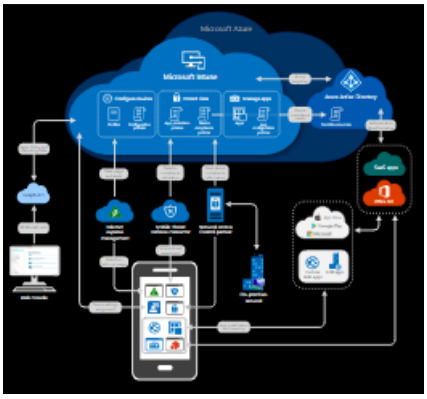
Contents

Microsoft Intune es un proveedor de MDM y MAM para los dispositivos.

14/05/2021 • 6 minutes to read

Microsoft Intune es un servicio basado en la nube que se centra en la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Puede controlar cómo se usan los dispositivos de la organización, incluidos los teléfonos móviles, las tabletas y los equipos portátiles. También puede configurar directivas específicas para controlar las aplicaciones. Por ejemplo, puede evitar que se envíen mensajes de correo electrónico a personas ajenas a la organización. Intune también permite que las personas de la organización usen sus dispositivos personales para la escuela o el trabajo. En los dispositivos personales, Intune ayuda a que los datos de la organización permanezcan protegidos., y puede aislar los datos de la organización de los datos personales.

Intune es parte del conjunto de aplicaciones Enterprise Mobility + Security (EMS) de Microsoft. Intune se integra con Azure Active Directory (Azure AD) para controlar quién tiene acceso y a qué se puede tener acceso. También se integra con Azure Information Protection para la protección de los datos. Se puede usar con el conjunto de productos de Microsoft 365. Por ejemplo, puede implementar Microsoft Teams, OneNote y otras aplicaciones de Microsoft 365 en los dispositivos. Esta característica permite que las personas de su organización sean productivas en todos sus dispositivos, a la vez que mantiene protegida la información de la organización con las directivas que crea.



Intune permite:

- Elegir estar al 100 % en una nube con Intune, o aplicar una administración conjunta con Configuration Manager e Intune.
- Establecer reglas y configurar los valores de los dispositivos personales y de la organización para tener acceso a los datos y las redes.
- Implementar y autenticar aplicaciones en dispositivos, tanto locales como móviles.
- Proteger la información de su empresa controlando el modo en que los usuarios acceden a la información y la comparten.
- Garantizar que los dispositivos y las aplicaciones sean compatibles con los requisitos de seguridad.

Administrar los dispositivos

En Intune, adoptará un enfoque adaptado a sus necesidades para administrar los dispositivos. En el caso de los dispositivos que pertenecen a la organización, puede que desee tener un control total sobre los dispositivos, incluida la configuración, las características y la seguridad. En este enfoque, los dispositivos y los usuarios de estos dispositivos "se inscriben" en Intune. Una vez inscritos, reciben las reglas y los valores de configuración a

través de las directivas configuradas en Intune. Por ejemplo, puede establecer requisitos de contraseña y PIN, crear una conexión VPN, configurar la protección contra amenazas y mucho más.

En el caso de dispositivos personales, o bring-your-own device (BYOD), es posible que los usuarios no quieran que los administradores de su organización tengan control total. En este enfoque, proporcione opciones a los usuarios. Por ejemplo, los usuarios inscriben sus dispositivos si desean tener acceso completo a los recursos de la organización. O bien, si estos usuarios solo quieren acceder al correo electrónico o a Microsoft Teams, use directivas de protección de aplicaciones que requieran autenticación multifactor (MFA) para usar estas aplicaciones.

Cuando los dispositivos se inscriben y administran en Intune, los administradores pueden:

- Ver los dispositivos inscritos y obtener un inventario de los dispositivos que acceden a los recursos de la organización.
- Configurar los dispositivos para que cumplan los estándares de seguridad y mantenimiento. Por ejemplo, es probable que desee bloquear dispositivos liberados.
- Inserte certificados en los dispositivos para que los usuarios puedan acceder fácilmente a la red Wi-Fi, o usar una VPN para conectarse a la red.
- Vea informes sobre usuarios y dispositivos que son compatibles y no compatibles.
- Quite los datos de la organización si un dispositivo se pierde, lo roban o ya no se usa.

Recursos en línea:

- ¿Qué es la inscripción de dispositivos?
- Aplicación de la configuración y características en dispositivos con perfiles de dispositivos
- Proteger dispositivos con Microsoft Intune

Pruebe la guía interactiva

La guía interactiva Administración de dispositivos con Microsoft Endpoint Manager le guiará a través del Centro de administración de Microsoft Endpoint Manager para mostrarle cómo administrar y proteger aplicaciones para dispositivos móviles y de escritorio.

https://mslearn.cloudguides.com/guides/Manage%20devices%20with%20Microsoft%20Endpoint%20Manager

Administrar aplicaciones

La administración de aplicaciones móviles (MAM) en Intune está diseñada para proteger los datos de la organización en el nivel de aplicación, incluidas las aplicaciones personalizadas y las aplicaciones de tienda. La administración de aplicaciones se puede usar en dispositivos propiedad de la organización y en dispositivos personales.

Cuando las aplicaciones se administran en Intune, los administradores pueden:

- Agregar y asignar aplicaciones móviles a grupos de usuarios y dispositivos, incluidos usuarios de grupos específicos, dispositivos en grupos específicos, etc.
- Configurar las aplicaciones para que se inicien o ejecuten con la configuración específica habilitada, y actualizar las aplicaciones existentes que ya están en el dispositivo.
- Ver los informes en los que se usan las aplicaciones y realizar un seguimiento de su uso.
- Realizar un borrado selectivo quitando únicamente los datos de la organización de las aplicaciones.

Una de las maneras en que Intune proporciona seguridad de aplicaciones móviles es a través de las **directivas de protección de aplicaciones** . Las directivas de protección de aplicaciones:

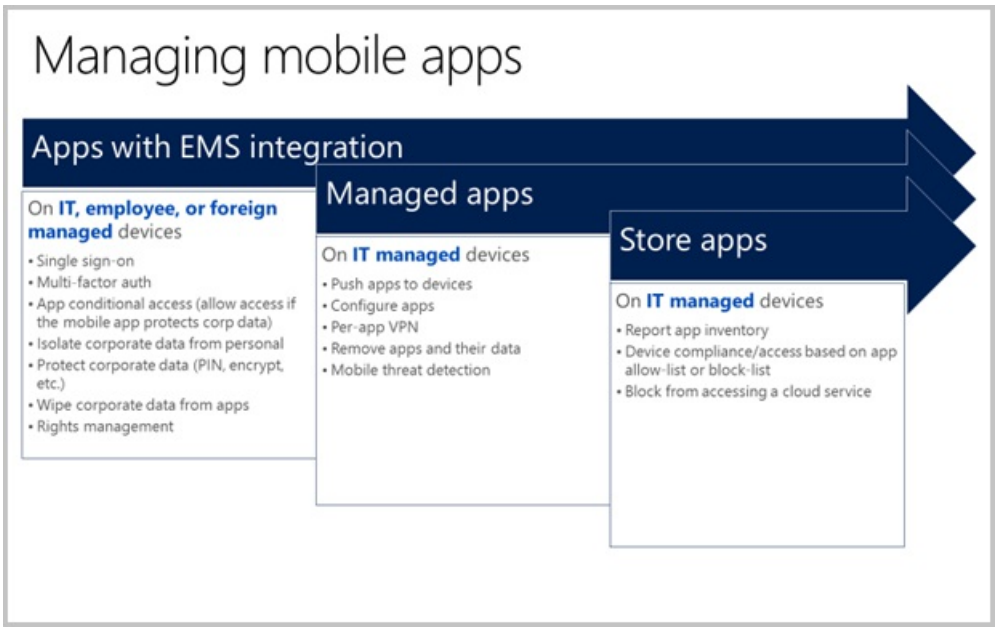
- Utilizan la identidad de Azure AD para aislar los datos de la organización de los datos personales. De este modo, la información personal se mantiene al margen del departamento de TI de la organización. A los datos

a los que se accede mediante credenciales de la organización se les proporciona protección de seguridad adicional.

- Ayudan a proteger el acceso a dispositivos personales mediante la restricción de las acciones que los usuarios pueden realizar, como copiar y pegar, guardar y ver.
- Pueden crearse e implementarse en dispositivos que estén inscritos en Intune, que estén inscritos en otro servicio MDM o que no estén inscritos en ningún servicio MDM. En los dispositivos inscritos, las directivas de protección de aplicaciones pueden agregar un nivel de protección adicional.

Por ejemplo, un usuario inicia sesión en un dispositivo con sus credenciales de organización. La identidad de su organización permite el acceso a los datos que se deniegan a su identidad personal. Dado que se usan datos de la organización, las directivas de protección de aplicaciones controlan cómo se guardan y se comparten los datos. Cuando los usuarios inician sesión con su identidad personal, no se aplican las mismas protecciones. De esta manera, el departamento de TI controla los datos de la organización, mientras que los usuarios finales mantienen el control y la privacidad de sus datos personales.

Además, puede usar Intune con los demás servicios de EMS. Esta característica proporciona la seguridad de la aplicación móvil de la organización más allá de lo que se incluye con el sistema operativo y las aplicaciones. Las aplicaciones administradas con EMS tienen acceso a un conjunto más amplio de características de protección de datos y aplicaciones móviles.



Cumplimiento y acceso condicional

Intune se integra con Azure AD para permitir una amplia gama de escenarios de control de acceso. Por ejemplo, requerir que los dispositivos móviles sean compatibles con los estándares de la organización definidos en Intune antes de tener acceso a los recursos de red, como el correo electrónico o SharePoint. También puede bloquear los servicios para que estén disponibles solo para un conjunto específico de aplicaciones móviles. Por ejemplo, puede bloquear Exchange Online de modo que solo Outlook o Outlook Mobile tengan acceso a él.

Recursos en línea:

- Establecimiento de reglas en los dispositivos para permitir el acceso a recursos de su organización
- Formas habituales de usar el acceso condicional con Intune

Obtención de Intune

Intune está disponible:

- Como un servicio de Azure independiente.
- Incluido con Microsoft 365 y Microsoft 365 Government.
- Como administración de dispositivos móviles en Microsoft 365 , que consta de algunas características limitadas de Intune.

Intune se usa en muchos sectores, como el administrativo o el educativo, así como en dispositivos de quiosco o dedicados, para la fabricación, la venta minorista, etc.

Pasos siguientes

- Estos son algunos de los problemas empresariales comunes que Intune ayuda a resolver.
- Comience con una prueba de 30 días de Intune.
- Planifique la migración a Intune .
- Con la evaluación gratuita o la suscripción, recorra el Inicio rápido: Crear un perfil de dispositivo de correo para iOS.

Información general sobre la administración de dispositivos

14/05/2021 • 6 minutes to read

Una tarea esencial de cualquier administrador es la de proteger los recursos y los datos de los dispositivos de la organización. Esta tarea se conoce como **administración de dispositivos**. Los usuarios reciben y envían correo electrónico de cuentas personales, exploran sitios web desde casa y restaurantes, e instalan aplicaciones y juegos. Estos usuarios también son empleados y alumnos que quieren usar sus dispositivos para acceder a recursos educativos y profesionales, como el correo electrónico y OneNote, rápidamente. Como administrador, el objetivo es proteger estos recursos y proporcionar un acceso fácil para los usuarios en sus muchos dispositivos, todos al mismo tiempo.

La administración de dispositivos permite a las organizaciones proteger y asegurar sus recursos y datos, y desde diferentes dispositivos.

Si la organización usa un proveedor de administración de dispositivos, tendrá la garantía de que solo acceden a la información de su propiedad aquellas personas y dispositivos que están autorizados. Del mismo modo, los usuarios de los dispositivos pueden acceder con tranquilidad a los datos de su trabajo desde la comodidad de su teléfono, porque saben que su dispositivo cumple los requisitos de seguridad de su organización. Las organizaciones se preguntarán: **¿qué debemos usar para proteger nuestros recursos?**

La respuesta es Microsoft Intune. Intune ofrece administración de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM). Estas son algunas tareas esenciales de cualquier solución de MDM o MAM:

- Admitir un entorno móvil variado y administrar dispositivos iOS/iPadOS, Android, Windows y macOS de forma segura.
- Garantizar que los dispositivos y las aplicaciones sean compatibles con los requisitos de seguridad de la organización.
- Crear directivas que ayuden a proteger los datos de la organización en dispositivos personales y corporativos.
- Usar una solución móvil única y unificada para aplicar estas directivas y ayudar a administrar dispositivos, aplicaciones, usuarios y grupos.
- Proteger la información de la empresa al ayudar a controlar la manera en que los empleados tienen acceso a sus datos y los comparten.

Intune se incluye con Microsoft Azure y Microsoft 365 y se integra con Azure Active Directory (Azure AD). Con Azure AD es más fácil controlar quién tiene acceso y a qué tiene acceso.

Microsoft Intune

Muchas organizaciones, como Microsoft, usan Intune para proteger datos de su propiedad a los que acceden los usuarios desde sus dispositivos propiedad de la empresa y de propiedad personal. Intune incluye directivas de configuración de dispositivos y aplicaciones, directivas de actualización de software y estados de instalación (gráficos, tablas e informes). Estos recursos le ayudan a proteger y supervisar el acceso a los datos.

Es habitual que las personas tengan varios dispositivos que usan plataformas distintas. Por ejemplo, es posible que un empleado use Surface Pro para el trabajo y un dispositivo móvil Android a nivel personal. Y es habitual que una persona acceda a los recursos de la organización, como Microsoft Outlook y SharePoint, desde distintos dispositivos.

Con Intune, es posible administrar varios dispositivos por persona y las distintas plataformas que se ejecutan en cada uno, como iOS/iPadOS, macOS, Android y Windows. Intune separa las directivas y la configuración por plataforma de dispositivo, para que resulte fácil administrar y ver los dispositivos de una plataforma específica.

Usos habituales de Microsoft Intune es un excelente recurso para ver cómo Intune responde ante preguntas comunes al trabajar con dispositivos móviles. Encontrará escenarios sobre:

- Protección del correo electrónico con Exchange local
- Acceso a Microsoft 365 de forma segura
- Uso de dispositivos personales para acceder a recursos de la organización

Para más información sobre Intune, consulte ¿Qué es Intune?

Administración conjunta y asociación de inquilinos

Muchas organizaciones usan Configuration Manager en el entorno local para administrar dispositivos, como equipos de escritorio y servidores. Puede asociar su instancia local de Configuration Manager a Microsoft Intune. Cuando se conecta en la nube, se obtienen las ventajas de Intune y la nube, incluidos el acceso condicional, la ejecución de acciones remotas, el uso de Windows Autopilot, etc.

Microsoft Endpoint Manager es una plataforma de soluciones que unifica varios servicios. Incluye Microsoft Intune para la administración de dispositivos basada en la nube y Configuration Manager e Intune para la administración de dispositivos que se conectan a la nube.

Si usa Configuration Manager y está listo para trasladar algunas tareas a la nube, la administración conjunta es la respuesta. Para obtener más información sobre cómo asociar la nube a Configuration Manager, consulte ¿Qué es administración conjunta?.

La asociación de inquilinos de Endpoint Manager también es una opción. Cargue sus dispositivos en el centro de administración de Endpoint Manager, sin habilitar la inscripción automática para la administración conjunta ni cambiar las cargas de trabajo a Intune. Puede ver los dispositivos y ejecutar acciones en dispositivos administrados para Configuration Manager. Para obtener más información, vea el artículo Asociación de inquilinos de Microsoft Endpoint Manager.

Integración con servicios de protección

Una tarea esencial de cualquier solución de administración de dispositivos consiste en proporcionar seguridad y protección. Intune se integra a la perfección con otros servicios para realizar esta tarea. Por ejemplo:

- **Microsoft 365** es un componente clave para simplificar las tareas comunes de TI. En el centro de administración de Microsoft 365, se crean usuarios y se administran grupos. También se puede acceder a otros servicios, como Intune, Azure AD y mucho más.

  Por ejemplo, cree un grupo de dispositivos iOS/iPadOS en Microsoft 365. Después, use Intune para insertar directivas en el grupo de dispositivos iOS/iPadOS que se centra en características de iOS/iPadOS, como acceder a la tienda de aplicaciones, usar AirDrop, hacer copias de seguridad en iCloud, usar el filtro web de Apple y mucho más.

- **Windows Defender** incluye muchas características de seguridad con las que puede proteger dispositivos Windows 10. Por ejemplo, con Intune y Windows Defender juntos puede hacer esto:

  - Habilitar Windows Defender SmartScreen para buscar actividades sospechosas en archivos y aplicaciones en dispositivos móviles.
  - Use Microsoft Defender para punto de conexión para ayudar a evitar infracciones de seguridad en dispositivos móviles, y limitar el impacto de una infracción de seguridad mediante el bloqueo de un usuario desde los recursos corporativos.

- **Acceso condicional** es una característica de Azure Active Directory que se integra perfectamente con Intune. Al usar el acceso condicional, asegúrese de que solo los dispositivos compatibles pueden acceder al correo electrónico, SharePoint y otras aplicaciones.

Elegir la solución de administración de dispositivos que más le conviene

Hay dos maneras de aproximarse a la administración de dispositivos. Primero, puede administrar diferentes aspectos de los dispositivos usando las características integradas en Intune. Este método se denomina **Administración de dispositivos móviles (MDM)** . Consiste en que los usuarios "inscriben" sus dispositivos y usan certificados para comunicarse con Intune. Como administrador de TI, puede insertar aplicaciones en dispositivos, restringir dispositivos a un sistema operativo específico, bloquear dispositivos personales y mucho más. Si alguna vez se pierde un dispositivo o lo roban, también puede quitar todos los datos del dispositivo.

El otro enfoque consiste en administrar las aplicaciones en los dispositivos. Este método se denomina **Administración de aplicaciones móviles (MAM)** . Con este método, los usuarios pueden usar sus dispositivos personales para acceder a recursos de la organización. Al abrir una aplicación, como el correo electrónico o SharePoint, se puede pedir a los usuarios que se autentiquen. Si alguna vez se pierde un dispositivo o lo roban, puede quitar todos los datos de la organización desde las aplicaciones administradas de Intune.

También puede usar una combinación de MDM y MAM juntos.

Simplificación de las tareas de TI mediante el centro de administración de Administración de dispositivos

El Centro de administración de Microsoft Endpoint Manager es un punto centralizado donde se pueden administrar y completar tareas para los dispositivos móviles. Este centro de administración incluye los servicios usados para la administración de dispositivos, incluido Intune y Azure Active Directory, y también para administrar aplicaciones cliente.

En el centro de administración de dispositivos, puede:

- Inscripción de dispositivos
- Establecimiento del cumplimiento de los dispositivos
- Administrar dispositivos
- Administración de aplicaciones
- eBooks de iOS
- Instalar el conector local de Exchange
- Administración de roles
- Administrar actualizaciones de software
  - Administrar actualizaciones de Windows 10
  - Administración de actualizaciones de iOS/iPadOS
- Azure Active Directory
- Administración de usuarios
- Administrar grupos y miembros
- Solución de problemas

Pasos siguientes

Cuando esté listo para empezar a trabajar con una solución de MDM o MAM, siga los distintos pasos para configurar Intune, inscribir dispositivos y empezar a crear directivas. La guía de planeamiento es un buen

recurso.

Caso práctico de Microsoft IT: Migración de administración de dispositivos móviles a Intune en Azure Portal

Novedades de Microsoft Intune

27/05/2021 • 62 minutes to read

Obtenga información sobre las novedades que se producen cada semana en Microsoft Intune en el Centro de administración de Microsoft Endpoint Manager. También puede encontrar notificaciones importantes, versiones anteriores e información sobre cómo se publican las actualizaciones del servicio de Intune.

> **NOTE**
>
> El lanzamiento de cada actualización mensual puede tardar hasta tres días y se realizará en el orden siguiente:
>
> - Día 1: Asia Pacífico (APAC)
> - Día 2: Europa, Oriente Medio y África (EMEA)
> - Día 3: América del Norte
> - Día 4+: Intune for Government
>
> Es posible que algunas características se implementen durante varias semanas y que no estén disponibles para todos los clientes la primera semana.
>
> Revise la página En desarrollo para ver una lista de las características que aparecerán en una versión próxima.

Fuente RSS: reciba notificaciones cuando esta página se actualice copiando y pegando la siguiente dirección URL en su lector de fuentes:

```
https://docs.microsoft.com/api/search/rss?search=%22What%27s+new+in+microsoft+intune%3F+-+Azure%22&locale=en-us
```

Semana del 10 de mayo de 2021

Administración de aplicaciones

Mensajería de acceso condicional mejorada para usuarios de Android e iOS/iPadOS

Azure Active Directory ha actualizado la redacción en una pantalla de acceso condicional para explicar mejor los requisitos de acceso y configuración a los usuarios. Los usuarios de Android e iOS/iPadOS verán esta pantalla cuando intenten acceder a los recursos corporativos desde un dispositivo que no esté inscrito en la administración de Intune.

Seguridad de dispositivos

Los perfiles de experiencia de seguridad de Windows admiten configuración de tres estados.

Para Windows 10 dispositivos, hemos actualizado la configuración de dos estado para que sea de tres estados en el perfil de experiencia de Seguridad de Windows para la directiva antivirus de seguridad de puntos de conexión.

La mayoría de las opciones del perfil solo admitían las dos opciones de **Sí** y **No configurado**. Ahora, esas mismas configuraciones incluyen las opciones **Sí, No configurado** y **No** (la nueva opción).

- En el caso de los perfiles existentes, los valores establecidos en *No configurado* permanecen como *No configurado*. Al crear perfiles o editar los existentes, ahora puede elegir especificar explícitamente *No*.

Además, lo siguiente se aplica a la configuración de la opción *Hide the Virus and threat protection area in the Windows Security app* (Ocultar el área de protección contra virus y amenazas en la aplicación Seguridad de Windows) y su configuración secundaria, *Hide the Ransomware data recovery option in the Windows Security app* (Ocultar la opción de recuperación de datos de ransomware en la aplicación Seguridad de Windows).

- Si la configuración principal (Ocultar el área de protección contra virus y amenazas) se ha establecido en *No*

configurado y la configuración secundaria se ha establecido en *Sí*, ambas configuraciones se establecerán en *No configurado*.

Administración de dispositivos

Uso de filtros para asignar directivas en el centro de administración de Endpoint Manager: versión preliminar pública

Hay una nueva opción, **Filtros**, que se puede usar al asignar aplicaciones o directivas a grupos. Para crear un filtro, vaya a estas ubicaciones:

- **Dispositivos** > **Filtros (versión preliminar)** > **Crear**
- **Aplicaciones** > **Filtros (versión preliminar)** > **Crear**
- **Administración de inquilinos** > **Filtros (vista previa)** > **Crear**.

Puede filtrar el ámbito de los dispositivos afectados mediante las propiedades de dispositivo. Por ejemplo, puede filtrar por la versión del sistema operativo, el fabricante del dispositivo, etc. Después de crear el filtro, puede usarlo al asignar una directiva o un perfil.

Para obtener más información, consulte Uso de filtros (versión preliminar) al asignar aplicaciones, directivas y perfiles en Microsoft Endpoint Manager.

Se aplica a:

- Administrador de dispositivos Android
- Android Enterprise
- iOS/iPadOS
- macOS
- Windows 10 y versiones posteriores

Uso de la directiva de Intune para acelerar la instalación de las actualizaciones de seguridad de Windows 10

En la versión preliminar pública, puede usar la directiva **Actualizaciones de calidad de Windows 10** de Intune para acelerar la instalación de las actualizaciones de seguridad más recientes de Windows 10 en los dispositivos que se administran en el servicio.

Al acelerar una actualización, los dispositivos pueden iniciar la descarga e instalación de la actualización lo antes posible, sin tener que esperar a que el dispositivo sincronice las actualizaciones. Aparte de acelerar la instalación de la actualización, al usar esta directiva, no se modifican los procesos ni las directivas de implementación de actualizaciones que ya tenga.

Si quiere supervisar las actualizaciones rápidas, puede usar las siguientes opciones:

- Informe de actualizaciones rápidas de Windows
- Informe de dispositivos con fallos en actualizaciones rápidas

Semana del 26 de abril de 2021 (versión del servicio 2104)

Administración de aplicaciones

Pantalla de privacidad actualizada en Portal de empresa para iOS

Hemos agregado texto adicional a la pantalla de privacidad de Portal de empresa para explicar el uso de los datos recopilados en la aplicación. Los usuarios pueden tener la certeza de que los datos recopilados solo se usan para comprobar que los dispositivos cumplen las directivas de la organización.

Estado de instalación de las aplicaciones necesarias asignadas a dispositivos

En la página **Aplicaciones instaladas** de la aplicación o el sitio web de Portal de empresa de Windows, los usuarios finales pueden ver el estado de instalación y los detalles de las aplicaciones necesarias asignadas a dispositivos. Además de esta funcionalidad, también se puede consultar el estado de la instalación y de los detalles de las aplicaciones necesarias asignadas a los usuarios. Para más información sobre el Portal de empresa de Intune, consulte Configuración de las aplicaciones del Portal de empresa de Intune, el sitio web del

Portal de empresa y la aplicación de Intune.

Visualización de la versión de aplicaciones Win32 en la consola

La versión de la aplicación Win32 ahora se muestra en el Centro de administración de Microsoft Endpoint Manager. La versión de las aplicaciones aparece en la lista **Todas las aplicaciones**, donde puede filtrar por aplicaciones Win32 y seleccionar la columna **versión** opcional. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Todas las aplicaciones** > **Columnas** > **Versión** para mostrar la versión en la lista de aplicaciones. Para obtener más información, consulte Administración de aplicaciones Win32 en Microsoft Intune.

Configuración de la versión máxima del sistema operativo para el inicio condicional de aplicación en dispositivos iOS

Con las directivas de protección de aplicaciones de Intune, se puede agregar una nueva configuración de inicio condicional para asegurarse de que los usuarios finales no usen ninguna versión previa ni compilación beta del sistema operativo para tener acceso a los datos de la cuenta profesional o educativa en dispositivos iOS. Esta configuración garantiza que se puedan examinar todas las versiones del sistema operativo antes de que los usuarios finales utilicen activamente las nuevas funciones del sistema operativo en dispositivos iOS. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Directivas de protección de aplicaciones**. Para obtener más información, consulte Creación y asignación de directivas de protección de aplicaciones.

Configuración del dispositivo

Actualización de los informes de directiva OEMConfig para dispositivos Android Enterprise

En dispositivos Android Enterprise, puede crear una directiva OEMConfig para agregar, crear y personalizar la configuración específica de OEM. Ahora, los informes de directiva se actualizan para que también se muestren correctamente en un usuario, un dispositivo y para cada opción de configuración de la directiva.

Para obtener más información, vea Uso y administración de dispositivos Android Enterprise con OEMConfig en Microsoft Intune.

Se aplica a:

- Android Enterprise

Deshabilitación del emparejamiento con NFC en dispositivos iOS/iPad con la versión 14.2 y posteriores

En los dispositivos iOS/iPadOS supervisados, puede crear un perfil de restricciones de dispositivos que deshabilite NFC (**Dispositivos** > **Perfiles de configuración**> **Crear perfil** > **iOS/iPadOS** como plataforma > **Restricciones de dispositivos** como perfil > **Dispositivos conectados** > **Disable near field communication (NFC)** [Deshabilitar NFC]). Cuando se deshabilita esta característica, se impide que los dispositivos se emparejen con otros dispositivos habilitados para NFC y se deshabilita NFC.

Para ver esta opción, vaya a Configuración de dispositivos iOS y iPadOS para permitir o restringir características mediante Intune.

Se aplica a:

- iOS/iPadOS 14.2 y versiones posteriores

Administración de dispositivos

Acción remota Buscar dispositivo para dispositivos Windows 10

Ahora puede usar una nueva acción remota Buscar dispositivo para obtener la ubicación geográfica de un dispositivo. Entre los dispositivos admitidos se incluyen:

- Windows 10, versión 20H2 (10.0.19042.789) o posteriores
- Windows 10, versión 2004 (10.0.19041.789) o posteriores
- Windows 10, versión 1909 (10.0.18363.1350) o posteriores
- Windows 10, versión 1809 (10.0.17763.1728) o posteriores

Para ver la nueva acción, inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft y elija **Dispositivos** > **Windows** > seleccione uno con Windows 10 > **Buscar dispositivo**.

Esta acción funcionará de manera similar a la acción actual Buscar dispositivo para los dispositivos Apple (pero no incluirá ninguna funcionalidad del modo Perdido).

Los servicios de ubicación deben estar habilitados en los dispositivos para que esta acción remota funcione. Si Intune no puede obtener la ubicación del dispositivo y el usuario ha establecido una ubicación predeterminada en la configuración del dispositivo, se mostrará la ubicación predeterminada.

Microsoft Endpoint Manager deja de ser compatible con Android 5.x

Microsoft Endpoint Manager ya no admite dispositivos Android 5.x.

Compatibilidad para mostrar los números de teléfono de los dispositivos corporativos con Android Enterprise

En el caso de los dispositivos corporativos con Android Enterprise (dedicados, totalmente administrados y totalmente administrados con un perfil de trabajo), los números de teléfono del dispositivo asociado ahora se muestran en el Centro de administración de Microsoft Endpoint Manager. Si hay varios números asociados al dispositivo, solo se mostrará un número.

Compatibilidad con la propiedad EID para dispositivos iOS/iPadOS

El identificador de eSIM (EID) es un identificador único para la SIM insertada (eSIM). La propiedad EID ahora aparece en la página de detalles de hardware para dispositivos iOS/iPadOS.

Compatibilidad de Intune con el aprovisionamiento de dispositivos compartidos de Azure Active Directory

La capacidad de aprovisionar dispositivos de Android Enterprise dedicados con Microsoft Authenticator configurado automáticamente en el modo de dispositivo compartido de Azure AD ya está disponible con carácter general. Para más información sobre cómo usar este tipo de inscripción, consulte Configuración de la inscripción en Intune de dispositivos dedicados de Android Enterprise.

Visualización de los detalles del final del soporte técnico para los perfiles de actualización de características

Para ayudarle a planear el fin del servicio para las actualizaciones de características de Windows 10 que implemente con Intune, hemos agregado dos nuevas columnas de información a los perfiles de actualizaciones de características en el Centro de administración de Microsoft Endpoint Manager.

La primera columna nueva muestra un estado que señala el momento en que la actualización del perfil está cerca o ha llegado a su fin de servicio, y la segunda columna muestra esa fecha de fin de servicio. Cuando una actualización llega a su fin de servicio, ya no se implementa en los dispositivos y la directiva se puede quitar de Intune.

Las nuevas columnas y detalles incluyen:

- **Soporte técnico** - Esta columna muestra el estado de la actualización de características:
  - **Con soporte**: la actualización tiene soporte para la distribución.
  - **Fin del soporte**: la actualización está a menos de dos meses de su fecha de fin de servicio.
  - **Sin soporte:** la actualización ya no tiene soporte, después de haber alcanzado su fecha de finalización del servicio.
- **Fecha de finalización del soporte técnico** -Esta columna muestra la fecha de fin del servicio para la actualización de características en el perfil.

Para obtener información sobre las fechas de fin de servicio de las versiones de Windows 10, consulte Información de versión de Windows 10 en la documentación sobre el estado de la versión de Windows.

Seguridad de dispositivos

Uso de perfiles de Antivirus para evitar o permitir la combinación de listas de exclusión de antivirus en dispositivos

Ahora puede configurar **Combinación de administradores locales de Defender** como parámetro en un perfil de *Antivirus de Microsoft Defender* para bloquear la combinación de listas de exclusión locales para

Antivirus de Microsoft Defender en dispositivos con Windows 10.

Las listas de exclusión de Antivirus de Microsoft Defender se pueden configurar localmente en un dispositivo y se especifican mediante la directiva de antivirus de Intune:

- Cuando se combinan listas de exclusión, las exclusiones definidas localmente se combinan con las de Intune.
- Cuando se bloquea la combinación, las exclusiones de la directiva serán las únicas efectivas en el dispositivo.

Para obtener más información sobre esta configuración y los valores relacionados, vea Exclusiones del antivirus de Microsoft Defender.

Flujo mejorado para el acceso condicional en dispositivos Surface Duo

Hemos optimizado el flujo de acceso condicional en dispositivos Surface Duo. Estos cambios se realizan automáticamente y no requieren ninguna actualización de la configuración por parte de los administradores. (**Seguridad de los puntos de conexión** > **Acceso condicional**)

En un dispositivo Duo:

- Cuando el acceso condicional bloquea el acceso a un recurso, ahora se redirige a los usuarios a la aplicación Portal de empresa que estaba preinstalada en el dispositivo. Anteriormente, se enviaban a la lista de aplicaciones de Google Play Store de la aplicación Portal de empresa.
- En el caso de los dispositivos inscritos como perfil de trabajo de propiedad personal, cuando un usuario intenta iniciar sesión en una versión personal de una aplicación con sus credenciales profesionales, ahora se les envía a la versión profesional de Portal de empresa en la que se muestran mensajes con instrucciones. Anteriormente, se enviaba al usuario al anuncio de la versión personal de la aplicación Portal de empresa en Google Play Store, donde tenía que volver a habilitarla para ver los mensajes con instrucciones.

Configuración de las opciones que se aplican a las actualizaciones del servidor de puerta de enlace de Tunnel

Hemos agregado opciones para ayudarle a administrar la actualización de los servidores de puerta de enlace de Microsoft Tunnel. Las nuevas opciones se aplican a la configuración de Sitios e incluyen:

- Establezca una ventana de mantenimiento para cada sitio de túnel. La ventana define cuándo los servidores de túnel asignados a ese sitio pueden empezar a actualizarse.
- Configure el tipo de actualización del servidor, que determina el modo en que todos los servidores del sitio proceden con las actualizaciones. Puede elegir entre:
  - **Automático**: todos los servidores del sitio se actualizarán lo antes posible después de que esté disponible una nueva versión del servidor.
  - **Manual**: los servidores del sitio solo se actualizarán después de que un administrador elija explícitamente permitir la actualización.
- La pestaña Comprobación de estado ahora muestra el estado de la versión de software del servidor para ayudarlo a comprender en qué momento el software del servidor de túnel está obsoleto. El estado incluye lo siguiente:
  - **Correcto**: actualizado con la versión de software más reciente.
  - **Advertencia**: una versión por detrás
  - **Incorrecto**: dos o más versiones por detrás

Aplicaciones de Intune

Nuevas aplicaciones protegidas disponibles para Intune

Las siguientes aplicaciones protegidas ya están disponibles para Microsoft Intune:

- Omnipresence Go de Omnipresence Technologies, Inc.
- Comfy de Building Robotics, Inc.
- M-Files for Intune de M-Files Corporation

Para obtener más información sobre las aplicaciones protegidas, vea Aplicaciones protegidas de Microsoft Intune.

Supervisión y solución de problemas

Nueva interfaz de usuario para filtrar los datos de nuevos informes operativos

Los nuevos informes operativos ahora admitirán una nueva interfaz de usuario para agregar filtros de datos. La nueva gama de filtros ofrece una experiencia mejorada para ayudar a segmentar, refinar y ver los datos de los informes. Para obtener más información sobre los informes en Intune, vea Informes de Intune.

El informe de frecuencia de reinicio de Windows en el análisis de puntos de conexión está disponible con carácter general

Actualmente, el rendimiento de inicio de análisis de puntos de conexión proporciona al equipo de TI información para medir y optimizar los tiempos de arranque del equipo. Sin embargo, la frecuencia de reinicio puede tener un gran impacto en la experiencia del usuario, en el sentido de que un dispositivo que se reinicia diariamente debido a las pantallas azules proporcionará una experiencia de usuario deficiente, incluso si los tiempos de arranque son rápidos. Ahora, hemos incluido un informe en las frecuencias de reinicio de la organización para ayudarle a identificar los dispositivos problemáticos. Para obtener más información, vea Frecuencia de reinicio en análisis de puntos de conexión.

Semana del 12 de abril de 2021

Configuración del dispositivo

Nuevo método de autenticación moderna con el Asistente para la configuración de Apple (versión preliminar pública)

Ahora, al crear un perfil de inscripción de dispositivos automatizada, puede elegir un nuevo método de autenticación: **Setup Assistant with modern authentication** (Asistente para configuración con autenticación moderna). Este método proporciona toda la seguridad del Asistente para configuración, pero evita el problema de que los usuarios finales no puedan usar el dispositivo mientras Portal de empresa se instala en el dispositivo. El usuario tiene que autenticarse mediante la autenticación multifactor de Azure AD durante las pantallas del Asistente para configuración. Para ello, se necesitará un inicio de sesión adicional de Azure AD después la inscripción en la aplicación Portal de empresa para acceder a los recursos corporativos protegidos por el acceso condicional. La versión de Portal de empresa correcta se enviará automáticamente como una aplicación obligatoria al dispositivo para iOS/iPadOS. Para macOS, estas son las opciones disponibles para obtener Portal de empresa en el dispositivo: Adición de la aplicación Portal de empresa para macOS.

La inscripción se completa cuando los usuarios llegan a la pantalla principal, y estos pueden usar libremente el dispositivo con los recursos que no están protegidos por el acceso condicional. La afinidad de usuario se establece cuando el usuario llega a la pantalla principal después de las pantallas de configuración; sin embargo, el dispositivo no se registrará completamente con AAD hasta el inicio de sesión en el Portal de empresa. El dispositivo no aparecerá en la lista de dispositivos de un usuario determinado en el portal de AAD hasta el inicio de sesión en el Portal de empresa. Si el inquilino tiene activada la autenticación multifactor para estos dispositivos o usuarios, se les pedirá que completen la autenticación multifactor durante la inscripción en el Asistente de configuración. La autenticación multifactor no es necesaria, pero está disponible para este método de autenticación dentro del acceso condicional si es necesario.

Este método tiene las siguientes opciones para instalar Portal de empresa:

- Para iOS/iPadOS: la opción **Instalar Portal de empresa** no se mostrará al elegir este flujo para iOS/iPad. Una vez que el usuario final llegue a la pantalla principal, Portal de empresa será una aplicación obligatoria en el dispositivo con la directiva de configuración de aplicaciones correcta aplicada. El usuario debe iniciar sesión con las credenciales de Azure AD en Portal de empresa después de inscribirse para obtener acceso a los recursos protegidos por el acceso condicional y estar plenamente registrado en AAD.
- Para macOS: los usuarios deben iniciar sesión en Portal de empresa para completar el registro de Azure AD y obtener acceso a los recursos protegidos por el acceso condicional. El usuario final podrá usar Portal de empresa sin problemas después de llegar a la página principal, pero tendrá que realizar un inicio de sesión

adicional en Portal de empresa para acceder a los recursos corporativos y cumplir las directivas. Para obtener más información, consulte Adición de la aplicación Portal de empresa de macOS.

Para obtener información sobre cómo usar este método de autenticación en dispositivos iOS/iPadOS, consulte Inscripción automática de dispositivos iOS/iPadOS mediante la inscripción de dispositivos automatizada de Apple.

Para obtener información sobre cómo usar este método de autenticación en dispositivos macOS, consulte Inscripción automática de dispositivos macOS con Apple Business Manager o Apple School Manager.

Semana del 29 de marzo de 2021 (versión del servicio 2103)

Administración de aplicaciones

El agente de administración de Intune para dispositivos macOS es ahora una aplicación universal.

Al implementar scripts de shell o atributos personalizados para dispositivos macOS desde Microsoft Endpoint Manager, se implementará la nueva versión universal de la aplicación del agente de administración de Intune que se ejecuta de forma nativa en máquinas Mac con Apple Silicon. La misma implementación instalará la versión x64 de la aplicación en máquinas Mac con Intel. Se requiere Rosetta 2 para ejecutar la versión x64 (Intel) de las aplicaciones en equipos Mac con Apple Silicon. Para instalar Rosetta 2 en los equipos Mac con Apple Silicon de forma automática, puede implementar un script de shell en Endpoint Manager. Para obtener más información, vea Agente de administración de Microsoft Intune para macOS.

Seguridad de dispositivos

Actualización de Microsoft Tunnel

Hemos publicado una nueva versión de Puerta de enlace de Microsoft Tunnel, que incluye los siguientes cambios:

- Varias mejoras y correcciones de errores.

El servidor de Puerta de enlace de Microsoft Tunnel se actualizará automáticamente a la nueva versión.

Semana del 22 de marzo de 2021 (versión del servicio 2103)

Administración de aplicaciones

Las aplicaciones de Microsoft 365 para dispositivos macOS son ahora aplicaciones universales

Al implementar aplicaciones de Microsoft 365 para dispositivos macOS desde Microsoft Endpoint Manager, ahora se implementará la nueva versión universal de la aplicación que se ejecuta de forma nativa en los equipos Mac con Apple Silicon. La misma implementación instalará las versiones x64 de la aplicación en los equipos Mac con Intel y macOS 10.14 y versiones posteriores. Para agregar aplicaciones de Microsoft 365 para macOS, en el Centro de administración de Microsoft Endpoint Manager > **Aplicaciones** > **Agregar todas las aplicaciones** > **Agregar**. Seleccione **macOS** en la lista **Tipo de aplicación**, en **Aplicaciones de Microsoft 365**. Para obtener información relacionada, consulte Asignación de Microsoft 365 a dispositivos macOS con Microsoft Intune.

Claves de configuración adicionales para la aplicación Microsoft Launcher

Ahora podrá establecer la configuración de la carpeta de Microsoft Launcher en los dispositivos totalmente administrados de propiedad corporativa con Android Enterprise. Al usar valores de claves de configuración y la directiva de configuración de aplicaciones, podrá establecer valores para la forma de carpeta, para la carpeta abierta en el modo de pantalla completa y para la dirección de desplazamiento de la carpeta. Además, ahora podrá situar la carpeta en la pantalla principal, además de colocar aplicaciones y vínculos web. Además, puede permitir que los usuarios finales modifiquen los valores de estilo de la carpeta desde la aplicación. Para obtener más información sobre Microsoft Launcher, consulte Configuración de Microsoft Launcher para Android Enterprise con Intune.

Configuración del dispositivo

Más opciones y categorías de Microsoft Edge quitadas del catálogo de configuración de macOS

En los dispositivos macOS, puede usar el catálogo de configuración para configurar Microsoft Edge, versión 77 y posteriores (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** en Plataforma > **Settings Catalog** [Catálogo de configuración]).

En esta versión:

- Se han agregado más opciones de configuración de Microsoft Edge.
- Las categorías de configuración se han quitado temporalmente. Para buscar una configuración concreta, use la categoría **Microsoft Edge - Todo** o busque el nombre de la configuración. Para ver una lista de opciones de configuración, Microsoft Edge: directivas es un buen recurso.

Para obtener más información sobre el catálogo de configuración, consulte Uso del catálogo de configuración para configurar opciones.

Se aplica a:

- macOS
- Microsoft Edge

La configuración de Windows 10 en la nube está disponible como un escenario guiado

La configuración de Windows 10 en la nube es una configuración de dispositivo para Windows 10 recomendada por Microsoft. La configuración de Windows 10 en la nube está optimizada para la nube y está diseñada para usuarios con necesidades de flujos de trabajo específicas.

Hay un escenario guiado que agrega las aplicaciones automáticamente y crea las directivas que configuran los dispositivos con Windows 10 en una configuración en la nube.

Para obtener más información, consulte Escenario guiado para la configuración de Windows 10 en la nube.

Se aplica a:

- Windows 10 y versiones posteriores

Administración de dispositivos

Aumento del número máximo recomendado de dispositivos iOS/iPadOS y macOS por token de inscripción

Anteriormente, se recomendaba no superar la cifra de 60 000 dispositivos iOS/iPadOS o macOS por token de inscripción de dispositivos automatizada (ADE). Este límite recomendado se ha aumentado a 200 000 dispositivos por token. Para obtener más información sobre los tokens de ADE, consulte Inscripción automática de dispositivos iOS/iPadOS mediante la inscripción de dispositivos automatizada de Apple.

Actualización de los nombres de columna en la vista Todos los dispositivos y en el informe de exportación

Para reflejar con precisión los datos en las columnas, hemos actualizado los nombres de columna en la vista Todos los dispositivos y en el informe de exportación para que "Primary User UPN" (UPN del usuario primario), "Dirección de correo electrónico del usuario primario" y "Nombre para mostrar del usuario primario".

Fin de la compatibilidad con Internet Explorer 11

Intune finalizará la compatibilidad con el acceso de administrador de Internet Explorer 11 a la interfaz de usuario de la aplicación web del portal de administración el 31 de marzo de 2021. Pásese a Edge u otro explorador compatible antes de ese momento para administrar cualquiera de los servicios de Microsoft basados en Azure.

Seguridad de dispositivos

Detalles del estado de mantenimiento de los servidores de puerta de enlace de Microsoft Tunnel

Hemos agregado la capacidad de ver información detallada del estado de mantenimiento de los servidores de puerta de enlace de Tunnel en el Centro de administración de Microsoft Endpoint Manager.

En la nueva pestaña nueva *Comprobación de estado*, verá la siguiente información:

- Última protección: la última vez que se protegió el servidor con Intune.

- Número de conexiones actuales: el número de conexiones activas en la última sincronización.
- Rendimiento: los megabits por segundo que atraviesan la NIC servidora en la última sincronización.
- Uso de CPU: el promedio de uso de CPU.
- Uso de memoria: el promedio de uso de memoria.
- Latencia: el tiempo promedio para que los paquetes IP atraviesen la NIC.
- Estado de expiración del certificado TLS y días antes de la expiración: cuánto tiempo el certificado TLS que protege la comunicación entre cliente y servidor para que el túnel siga siendo válido.

Versión preliminar pública de la funcionalidad de cliente de Tunnel en la aplicación Microsoft Defender para punto de conexión para Android

Tal como se anunció en Ignite, la funcionalidad de cliente de Microsoft Tunnel se está migrando a la aplicación Microsoft Defender para punto de conexión. Con esta versión preliminar, puede empezar a usar una versión preliminar de Microsoft Defender para punto de conexión como aplicación de Tunnel para los dispositivos compatibles. El cliente de Tunnel existente sigue estando disponible, pero finalmente se eliminará en favor de la aplicación Defender para punto de conexión.

Esta versión preliminar pública se aplica a:

- Android Enterprise
  - Totalmente administrado
  - Perfil de trabajo de propiedad corporativa
  - Perfil de trabajo de propiedad personal

En esta versión preliminar, debe participar para obtener acceso a la versión preliminar de Microsoft Defender para punto de conexión y, a continuación, migrar los dispositivos compatibles desde la aplicación cliente de Tunnel independiente a la aplicación en versión preliminar. Para obtener más información, consulte Migración a la aplicación Microsoft Defender para Endpoint.

Aplicaciones de Intune

Claves de configuración de Microsoft Launcher

En el caso de los dispositivos Android Enterprise totalmente administrados, la aplicación Microsoft Launcher para Intune proporcionará una personalización adicional. En el iniciador, puede configurar el conjunto de aplicaciones y vínculos web que se muestran, así como el orden de estas aplicaciones y vínculos web. La lista de aplicaciones y la posición (orden) de las configuraciones de la aplicación se han combinado para simplificar la personalización de la pantalla principal. Para obtener más información, vea Configuración de Microsoft Launcher.

Microsoft Edge para dispositivos macOS será una aplicación universal

Al implementar Microsoft Edge para dispositivos macOS desde Microsoft Endpoint Manager, se implementará la nueva versión universal de la aplicación que se ejecuta de forma nativa en los equipos Mac con Apple Silicon. La misma implementación instalará la versión x64 de la aplicación en los equipos Mac con Intel. Para agregar aplicaciones de Microsoft Edge para macOS, en el Centro de administración de Microsoft Endpoint Manager > **Aplicaciones** > **Agregar todas las aplicaciones** > **Agregar**. En la lista **Tipo de aplicación**, en **Microsoft Edge, versión 77 y posteriores**, seleccione **macOS**. Para obtener más información, consulte Adición de Microsoft Edge a dispositivos macOS con Microsoft Intune.

Nuevas aplicaciones protegidas disponibles para Intune

Las siguientes aplicaciones protegidas ya están disponibles para Microsoft Intune:

- FleetSafer de Cogosense Technology Inc.
- Senses de Mazrica Inc.
- Fuze Mobile para Intune de Fuze, Inc.
- MultiLine para Intune de Movius Interactive Corporation

Para obtener más información sobre las aplicaciones protegidas, vea Aplicaciones protegidas de Microsoft

Intune.

Mejora de la experiencia de notificación en la aplicación Portal de empresa de iOS/iPadOS

La aplicación Portal de empresa ahora puede almacenar y mostrar las notificaciones de inserción enviadas a los dispositivos iOS/iPadOS de los usuarios desde el Centro de administración de Microsoft Endpoint Manager. Los usuarios que hayan optado por recibir notificaciones de inserción del Portal de empresa pueden ver y administrar los mensajes almacenados personalizados que envíe a sus dispositivos en la pestaña **Notificaciones** del Portal de empresa. Para obtener información relacionada, vea Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune.

Scripting

Exportación de datos de informe localizados de Intune mediante Graph API

Ahora podrá especificar que los datos del informe que exporte mediante la API de exportación de informes de Microsoft Endpoint Manager solo pueden contener columnas localizadas, o bien columnas localizadas y no localizadas. La opción de columnas localizadas y no localizadas se seleccionará de forma predeterminada para la mayoría de los informes, lo que impedirá cambios importantes. Para obtener información relacionada sobre los informes, consulte Exportación de informes de Intune mediante Graph API e Informes y propiedades de Intune mediante Graph.

Semana del 8 de marzo de 2021

Configuración del dispositivo

Versión nueva del conector de certificados PFX

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2101.16.0**. Esta actualización agrega mejoras en el flujo de creación de PFX para evitar la duplicación de archivos de solicitud de certificado en servidores locales que hospedan el conector.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, consulte Conectores de certificados.

Semana del 1 de marzo de 2021 (versión del servicio 2102)

Administración de aplicaciones

Compatibilidad con la sustitución de aplicaciones Win32 en Intune

Hemos habilitado una versión preliminar pública de sustitución de aplicaciones en Intune. Ahora, se pueden crear relaciones de sustitución entre aplicaciones, lo que permite actualizar y reemplazar las aplicaciones Win32 existentes por versiones más recientes de esa misma aplicación o por aplicaciones Win32 completamente diferentes. Para obtener más información, vea Sustitución de aplicaciones Win32.

Configuración de la versión máxima del sistema operativo para el inicio condicional de aplicación en dispositivos Android

Con las directivas de protección de aplicaciones de Intune, se puede agregar una nueva configuración de inicio condicional para asegurarse de que los usuarios finales no usen ninguna versión previa ni compilación beta del sistema operativo para tener acceso a los datos de la cuenta profesional o educativa en dispositivos Android. Esta configuración garantiza que se puedan examinar todas las versiones del sistema operativo antes de que los usuarios finales utilicen activamente las nuevas funciones del sistema operativo en dispositivos Android. En el Centro de administración de Microsoft Endpoint Manager, podrá encontrar esta opción de configuración seleccionando **Aplicaciones** > **Directivas de protección de aplicaciones**. Para obtener más información, consulte Creación y asignación de directivas de protección de aplicaciones.

Configuración del dispositivo

Uso de Cisco AnyConnect como un tipo de conexión VPN para Windows 10 y Windows Holographic for Business

Se pueden crear perfiles de VPN mediante Cisco AnyConnect como un tipo de conexión (**Dispositivos** > **Configuración de dispositivo** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **VPN** para el perfil > **Cisco AnyConnect** para el tipo de conexión) sin necesidad de usar perfiles

personalizados.

Esta directiva usa la aplicación Cisco AnyConnect disponible en Microsoft Store, y no la aplicación de escritorio de Cisco AnyConnect.

Para obtener más información sobre los perfiles de VPN en Intune, consulte Creación de perfiles de VPN para conectarse a servidores VPN.

Se aplica a:

- Windows 10 y versiones posteriores
- Windows Holographic for Business

Ejecución de Microsoft Edge, versión 87 y versiones más recientes, en el modo de pantalla completa de una sola aplicación en dispositivos con Windows 10

En los dispositivos Windows 10 y versiones más recientes, configure un dispositivo para que se ejecute como una pantalla completa que ejecuta una o varias aplicaciones (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Windows 10 y versiones posteriores** > para la plataforma **Plantillas** > **Pantalla completa**). Al seleccionar el modo de aplicación única, puede:

- Ejecutar la versión 87 y posteriores de Microsoft Edge.
- Seleccione **Add Microsoft Edge legacy browser** (Agregar explorador de Microsoft Edge [versión heredada]) para ejecutar la versión 77 y anteriores de Microsoft Edge.

Para obtener más información sobre las opciones que puede configurar en el modo de pantalla completa, consulte Configuración de dispositivos con Windows 10 y versiones más recientes para ejecutarse como una pantalla completa.

Se aplica a:

- Windows 10 y versiones más recientes en el modo de pantalla completa de una sola aplicación
- Versión 87 de Microsoft Edge y versiones posteriores
- Microsoft Edge versión 77 y anteriores

Plantillas administrativas está disponible en el catálogo de configuración y tiene más opciones de configuración

En Intune, puede usar plantillas administrativas para crear directivas (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Plantillas administrativas** para el perfil).

En el catálogo de configuración, plantillas administrativas también están disponibles y tiene más opciones de configuración (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Catálogo de configuración** para el perfil).

Con esta versión, los administradores pueden configurar otras opciones que solo existían en la directiva de grupo local, y que no estaban disponibles en MDM basado en la nube. Estas opciones están disponibles para compilaciones de puntos de conexión del cliente **Windows Insider**, y tienen portabilidad con versiones anteriores de Windows en el mercado, como 1909, 2004 o 2010.

Si quiere crear plantillas administrativas y usar todas las opciones de configuración disponibles expuestas por Windows, use el catálogo de configuración.

Para más información, consulte:

- Uso de plantillas de Windows 10 para configurar los valores de directiva de grupo
- Uso del catálogo de configuración para configurar opciones

Se aplica a:

- Windows 10 y versiones posteriores

Inscripción de dispositivos

Estado de sincronización de tokens del programa de inscripción

Se ha quitado el estado de sincronización de los tokens de inscripción de dispositivos automatizados que figuran en el panel **Tokens del programa de inscripción** para evitar posibles confusiones. Sí se sigue mostrando la información por token. Los tokens del programa de inscripción se usan para administrar la inscripción automática de dispositivos con Apple Business Manager y Apple School Manager. En el centro de administración de Microsoft Endpoint Manager, encontrará la lista de tokens para dispositivos iOS/iPadOs si selecciona **Dispositivos** > **iOS/iPadOs** > **Inscripción de iOS/iPad** > **Tokens del programa de inscripción**. Para encontrar la lista de tokens para dispositivos macOS, seleccione **Dispositivos** > **macOS** > **Inscripción de macOS** > **Tokens del programa de inscripción**. Para obtener información relacionada, vea Inscripción automática de dispositivos iOS/iPadOs e Inscripción automática de dispositivos macOS.

Administración de dispositivos

Acción remota Recopilar diagnósticos

Una nueva acción remota, **Recopilar diagnósticos**, permite recopilar registros de los dispositivos corporativos sin interrumpir ni esperar al usuario final. Los registros recopilados engloban MDM, Autopilot, visores de eventos, claves, cliente de Configuration Manager, redes y otros registros de solución de problemas críticos. Para obtener más información, vea Recopilación de diagnósticos desde un dispositivo Windows.

Nuevas opciones para exportar datos de dispositivos

Estas son las nuevas opciones que hay disponibles al exportar datos de dispositivos:

- Solo se incluyen las columnas seleccionadas en el archivo exportado.
- Incluya todos los datos de inventario en el archivo exportado. Para ver estas opciones, vaya a Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **Todos los dispositivos** > **Exportar**.

Seguridad de los dispositivos

Uso de la variable CN={{UserPrincipalName}} en el asunto y la SAN de los perfiles de certificado SCEP y PKCS de dispositivos empresariales Android

Ahora, se puede usar la variable de atributo de usuario **CN={{UserPrincipalName}}** en el asunto o SAN de un perfil de certificado PKCS o un perfil de certificado SCEP de los dispositivos Android. Esta compatibilidad requiere que el dispositivo tenga un usuario, como los dispositivos inscritos del siguiente modo:

- Android Enterprise totalmente administrado
- Perfil de trabajo de propiedad personal de Android Enterprise

No se pueden usar atributos de usuario en dispositivos que carezcan de asociaciones de usuario, por ejemplo, en dispositivos que estén inscritos como dedicados de Android Enterprise. Por ejemplo, un perfil que use *CN={{UserPrincipalName}}* en el asunto o SAN no podrá obtener el nombre principal de usuario cuando no haya ningún usuario en el dispositivo.

Uso de directivas de protección de aplicaciones de Defender para punto de conexión en Android e iOS

Ahora, se puede usar Microsoft Defender para punto de conexión en las directivas de protección de aplicaciones de dispositivos que ejecutan Android o iOS.

- Configure la directiva de inicio condicional de MAM para incluir señales de **Nivel de amenaza máximo permitido** de Microsoft Defender para punto de conexión en dispositivos iOS y Android.
- Elija **Bloquear el acceso** o **Borrar datos** en función de si el dispositivo cumple el nivel de amenaza esperado.

Con esta configuración en vigor, se pedirá a los usuarios finales que instalen y configuren la aplicación **Microsoft Defender para punto de conexión** desde la tienda de aplicaciones correspondiente. Como requisito previo, debe configurar el conector de **Microsoft Defender para punto de conexión** y poner el conmutador en posición activa para enviar datos de riesgo a las directivas de protección de las aplicaciones. Para obtener información relacionada, vea Introducción general a las directivas de protección de aplicaciones y Uso de Microsoft Defender para punto de conexión en Microsoft Intune.

Configuración de reglas de reducción de la superficie expuesta a ataques para impedir que el malware obtenga persistencia a través de WMI

Ahora, la regla **Bloqueo de la persistencia a través de la suscripción de eventos WMI** se puede configurar como parte de un perfil de Reglas de reducción de la superficie expuesta a ataques en la seguridad del punto de conexión.

Esta regla impide que el malware abuse de WMI para lograr persistencia en un dispositivo. Las amenazas sin archivo emplean varias tácticas para permanecer ocultas, evitar ser detectadas en el sistema de archivos y obtener el control de la ejecución periódica. Algunas amenazas pueden abusar del repositorio WMI y el modelo de eventos para permanecer ocultas.

Si se configura como una configuración de la directiva *Reducción de la superficie expuesta a ataques* para la seguridad del punto de conexión, están disponibles las siguientes opciones:

- **Sin configurar** (valor predeterminado): la opción devuelve al valor predeterminado de Windows, que es desactivado y con la persistencia sin bloquear.
- **Bloquear**: se bloquea la persistencia a través de WMI.
- **Auditar**: evalúa cómo afecta esta regla a su organización si está habilitada (establecida en Bloquear).
- **Deshabilitar**: desactiva esta regla. La persistencia no está bloqueada.

Esta regla no admite la opción *WARN* y también está disponible como una opción de configuración de dispositivo en el catálogo de configuración.

Aplicaciones de Intune

Mejora del rendimiento de carga del sitio web del Portal de empresa

Para mejorar el rendimiento de la carga de página, ahora los iconos de la aplicación se cargarán en lotes. Los usuarios finales pueden ver un icono de marcador de posición para algunas de sus aplicaciones al visitar el sitio web del Portal de empresa. Los iconos relacionados se cargarán poco después. Para más información sobre el Portal de empresa de Intune, consulte Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune y Administrar aplicaciones desde el sitio web del Portal de empresa.

Supervisión y solución de problemas

Análisis de puntos de conexión en Puntuación de productividad de Microsoft

Hay una nueva página de análisis de puntos de conexión en Puntuación de productividad de Microsoft donde se comparte información de nivel de organización con los demás roles fuera del administrador de puntos de conexión de Microsoft. Es fundamental comprender el modo en que los dispositivos contribuyen a la experiencia de los usuarios finales para que estos puedan alcanzar sus objetivos. Para obtener más información, vea Análisis de puntos de conexión en Puntuación de productividad de Microsoft.

Informe de confiabilidad de la aplicación en análisis de puntos de conexión

Un nuevo informe, **Confiabilidad de la aplicación**, estará disponible en los análisis de puntos de conexión. En este informe, se proporciona información sobre los posibles problemas de las aplicaciones de escritorio en los equipos administrados. Permite identificar rápidamente las aplicaciones principales que afectan a la productividad del usuario final, así como ver métricas de uso de aplicaciones y de error de aplicación relativas a estas aplicaciones. Podrá solucionar problemas analizando un dispositivo específico y viendo una escala de tiempo de los eventos de confiabilidad de la aplicación. Se espera que este informe esté disponible como versión preliminar pública durante marzo de 2021. Para obtener más información, vea Confiabilidad de las aplicaciones de análisis de puntos de conexión.

Frecuencia de reinicio (versión preliminar) en análisis de puntos de conexión

Actualmente, el rendimiento de inicio de análisis de puntos de conexión proporciona al equipo de TI información para medir y optimizar los tiempos de arranque del equipo. Sin embargo, la frecuencia de reinicio puede tener un gran impacto en la experiencia del usuario, en el sentido de que un dispositivo que se reinicia diariamente debido a las pantallas azules proporcionará una experiencia de usuario deficiente, incluso si los tiempos de arranque son rápidos. Ahora, hemos incluido un informe de vista previa en las frecuencias de reinicio de la

organización para ayudarle a identificar los dispositivos problemáticos. Para obtener más información, vea Frecuencia de reinicio (versión preliminar) en análisis de puntos de conexión.

Control de acceso basado en rol

Actualización de los permisos de acceso basado en rol para la Puerta de enlace de Microsoft Tunnel

Para ayudar a controlar quién tiene derechos para administrar Microsoft Tunnel, hemos incluido **Puerta de enlace de Microsoft Tunnel** como un nuevo grupo de permisos para el control de acceso basado en roles de Intune. Este nuevo grupo incluye los siguientes permisos:

- **Crear**: permite configurar servidores de puerta de enlace de Microsoft Tunnel, configuraciones de servidor y sitios.
- **Actualizar** (modificar): permite actualizar servidores, configuraciones de servidor y sitios de puerta de enlace de Microsoft Tunnel.
- **Eliminar**: permite eliminar servidores, configuraciones de servidor y sitios de puerta de enlace de Microsoft Tunnel.
- **Leer**: permite ver servidores de puerta de enlace de Microsoft Tunnel, configuraciones de servidor y sitios.

Los administradores de Intune y los administradores de Azure Active Directory tienen estos permisos de forma predeterminada. Estos permisos también se pueden agregar a los roles personalizados que se hayan creado para el inquilino de Intune.

Compatibilidad de etiquetas de ámbito con las directivas de personalización de Intune para Government y 21Vianet

Ahora, se pueden asignar etiquetas de ámbito a directivas de personalización para Intune para Government e Intune a través de 21Vianet. Para ello, vaya al Centro de administración de Microsoft Endpoint Manager > **Administración de inquilinos** > **Personalización** donde verá las opciones de configuración de **Etiquetas de ámbito**.

Semana del 22 de febrero de 2021

Configuración del dispositivo

Versión nueva del conector de certificados PFX

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2101.13.0**. Esta nueva versión del conector incorpora mejoras de registro al conector PFX:

- Nueva ubicación de los registros de eventos, con los registros divididos como de administración, operativos o de depuración.
- Los registros operativos y de administración tienen un tamaño predeterminado de 50 MB cuando el archivado automático está habilitado.
- EventID de creación, importación y revocación de PKCS.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, consulte Conectores de certificados.

Semana del 8 de febrero de 2021

Administración de aplicaciones

Los usuarios finales pueden reiniciar la instalación de una aplicación en el Portal de empresa de Windows

Con el Portal de empresa de Windows, los usuarios finales pueden reiniciar la instalación de una aplicación si parece que el progreso se ha detenido o está inmovilizado. Esta funcionalidad se permite si el progreso de la instalación de la aplicación no ha cambiado en dos horas. Para más información, vea Incorporación de aplicaciones a Microsoft Intune.

Configuración del dispositivo

Las pantallas de cumplimiento de Google se muestran automáticamente en los dispositivos dedicados Android Enterprise 9.0 + que se ejecutan en pantalla completa.

En Intune, puede crear una directiva de contraseñas de configuración de dispositivos y una directiva de contraseñas de cumplimiento de dispositivos en dispositivos Android Enterprise.

Al crear las directivas, los dispositivos Android Enterprise dedicados que se ejecutan en el modo de pantalla completa usan automáticamente las pantallas de cumplimiento de Google. Estas pantallas guían a los usuarios y les obligan a establecer una contraseña que cumpla las reglas de la directiva.

Para obtener más información sobre la creación de directivas de contraseñas y pantallas completas, consulte:

- Configuración de Android Enterprise para marcar dispositivos como compatibles o no compatibles
- Configuración de dispositivos Android Enterprise para permitir o restringir características

Se aplica a:

- Android Enterprise 9 y versiones más recientes en el modo de pantalla completa

Semana del 1 de febrero de 2021 (versión del servicio 2101)

Administración de aplicaciones

Configuración de la opción de quitar o no una aplicación de iOS/iPadOS necesaria

Ahora puede configurar si los usuarios finales pueden instalar una aplicación de iOS/iPadOS necesaria como una aplicación que se puede quitar. La nueva configuración se aplicará a la tienda de iOS, la aplicación de línea de negocio y aplicaciones integradas. Puede encontrar esta opción en el Centro de administración de Microsoft Endpoint Manager; para ello, seleccione **Aplicaciones** > **iOS/iPadOS** > **Agregar**. Al establecer las asignaciones de la aplicación, puede seleccionar **Install as removable** (Instalar con la opción de quitar). El valor predeterminado es **Sí**, lo que significa que la aplicación se puede quitar. Las instalaciones necesarias existentes en iOS 14 se han actualizado al valor de configuración predeterminado (se puede quitar). Para obtener más información acerca de las aplicaciones de iOS/iPadOS, vea Administración de aplicaciones de Microsoft Intune.

Aplicaciones de línea de negocio admitidas en dispositivos iPad compartidos

Puede implementar aplicaciones de línea de negocio (LOB) en dispositivos iPad compartidos. La aplicación de línea de negocio debe estar asignada como **necesaria** a un grupo de dispositivos que contenga dispositivos iPad compartidos desde el Centro de administración de Microsoft Endpoint Manager. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Todas las aplicaciones** > **Agregar**. Para obtener información relacionada, vea Incorporación de una aplicación de línea de negocio iOS/iPadOS a Microsoft Intune.

Conector de Microsoft Endpoint Configuration Manager

El conector de Microsoft Endpoint Configuration Manager aparece ahora en el centro de administración. Para revisar el conector, vaya a **Administración de inquilinos** > **Conectores y tokens** > **Microsoft Endpoint Configuration Manager**. Seleccione una jerarquía de Configuration Manager que ejecute la versión 2006 o posterior para mostrar información adicional sobre ella.

Configuración del dispositivo

Versión nueva del conector de certificados PFX

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2009.2.0**. Esta nueva versión del conector:

- Mejora la actualización del conector para conservar las cuentas que ejecutan los servicios de conector.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, consulte Conectores de certificados.

Uso de la configuración del dispositivo para crear carpetas y establecer el tamaño de la cuadrícula en Managed Home Screen

En dispositivos Android Enterprise dedicados, puede configurar las opciones de configuración de Managed Home Screen (**Dispositivos** > **Configuración del dispositivo** > **Crear perfil** > **Android Enterprise** para la

plataforma > **Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado** para el perfil > **Experiencia del dispositivo**).

Al usar Managed Home Screen en el modo de pantalla completa de varias aplicaciones, existe un parámetro respecto al **diseño de aplicación personalizado**. Con este parámetro, puede:

- Cree carpetas, agregar aplicaciones a estas carpetas y colocar la carpeta en Managed Home Screen. No tiene que ordenar las carpetas.
- Elija si desea ordenar aplicaciones y carpetas en Managed Home Screen. Si lo hace, también puede:
  - Establecer el tamaño de la cuadrícula.
  - Agregar aplicaciones y carpetas a diferentes lugares de la cuadrícula.

Anteriormente, tenía que usar una directiva de configuración de la aplicación.

Para obtener más información, consulte la experiencia del dispositivo de dispositivos dedicados de Android Enterprise.

Se aplica a:

- Dispositivos Android Enterprise dedicados

Uso del catálogo de configuración para configurar el explorador Microsoft Edge en dispositivos macOS: versión preliminar pública

Actualmente, en los dispositivos macOS, el explorador Microsoft Edge se configura con un archivo de preferencias .plist (**Devices** [Dispositivos] > **Configuration profiles** [Perfiles de configuración] > **Create profile** [Crear perfil] > **macOS** para la plataforma > **Preference file** [Archivo de preferencias] para el perfil).

Hay una interfaz de usuario actualizada para configurar el explorador Microsoft Edge: **Devices** (Dispositivos) > **Configuration profiles** (Perfiles de configuración) > **Create profile** (Crear perfil) > **macOS** para la plataforma > **Settings catalog (preview)** (Catálogo de configuración [versión preliminar]) para el perfil. Seleccione los valores de Microsoft Edge que desee y, a continuación, configúrelos. Si quiere, en el perfil puede agregar opciones o quitar las existentes.

Para ver una lista de las opciones que se pueden configurar, vaya a Microsoft Edge: directivas. Asegúrese de que macOS aparezca como plataforma admitida. Si algunas opciones no están disponibles en el catálogo de configuración, se recomienda seguir usando solo el archivo de preferencias.

Para más información, consulte:

- Catálogo de configuración
- Adición de un archivo de lista de propiedades a dispositivos macOS con Intune

Para ver las directivas que ha configurado, abra Microsoft Edge y vaya a `edge://policy`.

Se aplica a:

- Explorador de Microsoft Edge, versión 77 y posteriores en macOS

Uso de NetMotion Mobility como tipo de conexión VPN para dispositivos Android Enterprise

Cuando se crea un perfil de VPN, NetMotion Mobility está disponible como un tipo de conexión VPN para Android Enterprise:

- **Dispositivos** > **Configuración del dispositivo de** > **Crear perfil** > **Android Enterprise** > **Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado Android** > **VPN** para el perfil > **NetMotion Mobility** para el tipo de conexión.
- **Dispositivos** > **Configuración del dispositivo** > **Crear perfil** > **Android Enterprise** > **Perfil de trabajo de propiedad personal** > **VPN** para el perfil > **NetMotion Mobility** para el tipo de conexión.

Para obtener más información sobre los perfiles de VPN en Intune, consulte Creación de perfiles de VPN para

conectarse a servidores VPN.

Se aplica a:

- Perfil de trabajo de propiedad personal de Android Enterprise
- Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado de Android Enterprise

Plantillas y catálogo de configuración al crear perfiles de configuración para dispositivos macOS y Windows 10

La interfaz de usuario se ha actualizado en relación con la creación de perfiles de configuración para dispositivos macOS y Windows 10 (**Devices** [Dispositivos] > **Configuration profiles** [Perfiles de configuración] > **Create profile** [Crear perfil] > **macOS** o **Windows 10 and later** [Windows 10 y versiones posteriores] para la plataforma).

En el perfil se muestra **Settings catalog - preview** (Catálogo de configuración: versión preliminar) y **Templates** (Plantillas):

- **Settings catalog - preview** (Catálogo de configuración: versión preliminar): utilice esta opción para empezar desde cero y seleccionar las opciones que quiera en la biblioteca de opciones disponibles. En macOS, el catálogo de configuraciones incluye valores para configurar la versión 77 y posteriores de Microsoft Edge. El catálogo de configuración de Windows 10 incluye muchas opciones existentes (y otras nuevas) en un solo lugar.
- **Templates** (Plantillas): utilice esta opción para configurar todos los perfiles existentes, como las restricciones de los dispositivos, las características de los dispositivos, las redes VPN o Wi-Fi, entre otras.

Este cambio solo concierne a la interfaz de usuario y no afecta a los perfiles existentes.

Para más información, consulte Catálogo de configuración.

Se aplica a:

- Configuración de dispositivos macOS
- Configuración de dispositivos Windows 10

Actualización del diseño de la pantalla de inicio en los dispositivos iOS/iPadOS supervisados

En los dispositivos iOS/iPadOS, puede configurar el diseño de la pantalla de inicio (**Devices** [Dispositivos] > **Device Configuration** [Configuración del dispositivo] > **Create profile** [Crear perfil] > **iOS/iPadOS** para la plataforma > **Device features** [Características del dispositivo] para el perfil > **Home screen layout** [Diseño de la pantalla de inicio]). En Intune se ha actualizado la característica Diseño de pantalla principal:

- El diseño de la pantalla principal tiene una nueva disposición. Esta característica permite a los administradores ver en tiempo real el aspecto que tendrán las aplicaciones y los iconos de aplicaciones en las páginas, el Dock y las carpetas. Al agregar aplicaciones en este nuevo diseñador, no se pueden agregar páginas independientes. Sin embargo, cuando se agregan nueve o más aplicaciones a una carpeta, esas aplicaciones pasan automáticamente a la página siguiente. Las directivas existentes no se ven afectadas y no es necesario cambiarlas. Los valores de configuración se transfieren a la nueva interfaz de usuario sin ningún tipo de problema. El comportamiento de la configuración en los dispositivos es el mismo.
- Agregue un vínculo web (aplicación web) a una página o al Dock. Asegúrese de agregar una dirección URL específica del vínculo web solo una vez. Las directivas existentes no se ven afectadas y no es necesario cambiarlas.

Para más información sobre las opciones que puede configurar, incluido el diseño de la pantalla principal, consulte Configuración de dispositivos iOS/iPadOS para usar las características comunes de iOS/iPadOS en Intune.

Se aplica a:

- Dispositivos iOS/iPadOS supervisados

Limitación de la publicidad personalizada de Apple en los dispositivos iOS/iPadOS

En los dispositivos iOS/iPadOS, puede configurar la publicidad personalizada de Apple. Cuando esta opción está habilitada, se limitan los anuncios personalizados en las aplicaciones de App Store, Apple News y Stocks (**Devices** [Dispositivos] > **Device Configuration** [Configuración del dispositivo] > **Create profile** [Crear perfil] > **iOS/iPadOS** para la plataforma > **Device restrictions** [Restricciones del dispositivo] para el perfil > **General** [General] > **Limit Apple personalized advertising** [Limitar la publicidad personalizada de Apple]).

Esta opción solo afecta a los anuncios personalizados. Al configurar esta opción se **desactiva** el parámetro de **Ajustes** > **Privacidad** > **Publicidad**. No afecta a los anuncios no personalizados de las aplicaciones de App Store, Apple News y Stocks. Para obtener más información sobre la directiva de publicidad de Apple, consulte el sitio web Publicidad y la privacidad de Apple.

Para ver las opciones que puede configurar actualmente en Intune, vaya a Configuración de dispositivos iOS e iPadOS para permitir o restringir características.

Se aplica a:

- Dispositivos iOS/iPadOS 14.0 y versiones más recientes inscritos con la inscripción de dispositivos o con la inscripción de dispositivos automatizada

Las plantillas administrativas incluyen nuevas directivas para la versión 88 de Microsoft Edge

Puede configurar e implementar la nueva configuración de ADMX que se aplica a la versión 88 de Microsoft Edge. Para ver las nuevas directivas, vaya a las notas de la versión de Microsoft Edge.

Para obtener más información sobre esta característica en Intune, consulte Configuración de opciones de directivas de Microsoft Edge.

Se aplica a:

- Windows 10 y versiones posteriores

Compatibilidad de la configuración regional en las notificaciones por correo electrónico en caso de incumplimiento

Las directivas de cumplimiento ahora admiten Plantillas de mensajes de notificación que incluyen mensajes independientes para diferentes configuraciones regionales. La compatibilidad con varios idiomas ya no requiere la creación de plantillas y directivas independientes para cada configuración regional.

Cuando se configuran mensajes específicos de una configuración regional en una plantilla, los usuarios finales no compatibles reciben el mensaje de notificación de correo electrónico localizado adecuado en función de su idioma preferido de O365. También se designa un mensaje localizado en la plantilla como *mensaje predeterminado*. El mensaje predeterminado se envía a los usuarios que no han establecido un idioma preferido o cuando la plantilla no incluye un mensaje específico para su configuración regional.

Inscripción de dispositivos

Ocultación de más pantallas del Asistente de configuración de inscripción de dispositivos automatizada de Apple

Ahora puede establecer perfiles de inscripción de dispositivos automatizada (ADE) para ocultar estas pantallas del asistente de configuración para dispositivos iOS/iPadOS 14.0 y macOS 11 o versiones posteriores:

- Restauración completada, para iOS/iPadOS 14.0 o versiones posteriores.
- Actualización de software completada, para iOS/iPadOS 14.0 o versiones posteriores.
- Accesibilidad, para macOS 11 o versiones posteriores (el dispositivo Mac debe estar conectado a una red Ethernet).

Administración de dispositivos

Migración de directivas de seguridad de dispositivos de Mobility + Security básico a Intune

La herramienta de migración de directivas le permite trasladar permanentemente las directivas de seguridad de los dispositivos de administración de dispositivos móviles (MDM) implementadas por Basic Mobility and Security (anteriormente MDM para Office 365 u Office MDM) a las directivas estándar de cumplimiento y los

perfiles de configuración de MDM de Intune. El uso de esta herramienta deshabilitará cualquier futura posibilidad de crear y editar las directivas de seguridad de los dispositivos de Mobility + Security básico.

Para usar la herramienta, debe:

- Haber comprado licencias de Intune para todos los usuarios de dispositivos administrados por Basic Mobility and Security (pero todavía no deben haberse asignado).
- Ponerse en contacto con soporte técnico para comprobar su idoneidad si ha adquirido una suscripción a Intune for Education.

Para obtener más información, consulte Migración de su administración de dispositivos móviles desde Basic Mobility and Security a Intune.

Id. de subred y direcciones IP en la página Propiedades de dispositivos Windows de propiedad corporativa

El id. de subred y las direcciones IP se muestra en la página **Propiedades** de los dispositivos Windows de propiedad corporativa. Para verlos, vaya al Centro de administración de Endpoint Manager > **Dispositivos** > **Todos los dispositivos** > elija un dispositivo Windows de propiedad corporativa > **Propiedades**.

Seguridad de dispositivos

La compatibilidad de Intune con Protección de aplicaciones de Microsoft Defender incluye ahora entornos aislados de Windows

Al configurar **Activar la protección de aplicaciones** en un perfil Aislamiento de aplicaciones y navegador de una directiva de reducción de la superficie de ataque de seguridad del punto de conexión de Intune, puede elegir entre las opciones siguientes:

- **Microsoft Edge** - *Disponible anteriormente*
- **Entornos de Windows aislados** - *Nuevo con esta actualización*
- **Microsoft Edge *y* _ _ Entornos de Windows aislados** - *Nuevo con esta actualización*

Antes de esta versión, esta opción se denominaba *Activación de la Protección de aplicaciones para Microsoft Edge (opciones)* .

Las nuevas opciones para esta configuración amplían la compatibilidad con Protección de aplicaciones más allá de la dirección URL para Edge. Ahora puede habilitar Protección de aplicaciones para ayudar a proteger los dispositivos mediante la apertura de amenazas potenciales en un entorno de máquina virtual Windows (contenedor) aislado de hardware. Por ejemplo, con la compatibilidad con entornos de Windows aislados, Protección de aplicaciones puede abrir documentos de Office que no son de confianza en una máquina virtual Windows aislada.

Con este cambio:

- Intune ahora admite toda la gama de valores que se encuentran en el CSP de MDM de Windows: AllowWindowsDefenderApplicationGuard.
- Para ayudarle a entender el efecto en los usuarios de dispositivos al usar entornos de Windows aislados, consulte Escenarios de prueba de Protección de aplicaciones en la documentación de seguridad de Windows.
- Obtenga más información sobre Protección de aplicaciones y la compatibilidad con aplicaciones de Office en Protección de aplicaciones para Office en la documentación de Microsoft 365.

Nueva configuración de protección de aplicaciones en la directiva de reducción de la superficie expuesta a ataques

Se han agregado dos nuevas opciones al perfil Aislamiento de aplicaciones y navegador de la directiva de reducción de la superficie expuesta a ataques para la seguridad de puntos de conexión de Intune:

- **Application Guard allow camera and microphone access** (Protección de aplicaciones permite el acceso a la cámara y el micrófono): administre el acceso de las aplicaciones de Protección de aplicaciones a la cámara y el micrófono de un dispositivo.
- **Application Guard allow use of Root Certificate Authorities from the user's device** (Protección de aplicaciones permite el uso de entidades de certificación raíz desde el dispositivo del usuario): cuando se

especifican una o varias huellas digitales del certificado raíz, los certificados coincidentes se transfieren al contenedor de Protección de aplicaciones de Microsoft Defender.

Para obtener más información, consulte la configuración del Aislamiento de aplicaciones y navegador.

Actualizaciones para líneas base de seguridad

Hay nuevas versiones disponibles para las siguientes líneas de base de seguridad:

- **Línea base de seguridad de MDM (Seguridad de Windows 10)**
- **Línea base de Microsoft Defender para punto de conexión**

Las versiones de línea base actualizadas proporcionan compatibilidad con los valores de configuración recientes para ayudarle a mantener las configuraciones que recomiendan los equipos de producto respectivos.

Para saber qué ha cambiado entre las versiones, en Comparación de versiones de línea de base aprenderá a exportar un archivo .CSV que muestre los cambios.

Informes del firewall de seguridad de los puntos de conexión

Se han agregado dos nuevos informes dedicados a las directivas del firewall en la seguridad de los puntos de conexión:

- Dispositivos MDM para Windows 10 con el firewall desactivado se encuentra en el nodo Seguridad del punto de conexión y muestra la lista de dispositivos Windows 10 con el firewall desactivado. Este informe identifica cada dispositivo por el nombre del dispositivo, el identificador del dispositivo, la información del usuario y el estado del firewall.
- Estado del firewall de los dispositivos MDM para Windows 10 es un informe organizativo que se encuentra en el nodo *Informes*, que muestra el estado de firewall de los dispositivos Windows 10. Este informe muestra la información de estado que incluye si el firewall está habilitado, deshabilitado, limitado o deshabilitado temporalmente.

Vista de resumen de los informes del Antivirus de Microsoft Defender

Hemos actualizado la vista de los informes del Antivirus de Microsoft Defender que se encuentran en el nodo **Informes** del centro de administración de Microsoft Endpoint Manager. Ahora, cuando seleccione Antivirus de Microsoft Defender en el nodo **Informes**, verá la vista predeterminada de la pestaña **Resumen** y una segunda pestaña para **Informes**. En la pestaña **Informes** es donde encontrará los informes organizativos anteriormente disponibles Estado del agente de antivirus y Malware detectado.

La nueva pestaña **Resumen** muestra la siguiente información:

- Muestra los detalles agregados de los informes del antivirus.
- Incluye una opción *Actualizar* que actualiza el número de dispositivos en cada uno de los estados del antivirus.
- Refleja los mismos datos que los que se encuentran en el informe organizativo Estado del agente de antivirus, al que ahora se tiene acceso desde la pestaña **Informes**.

Compatibilidad con directivas de protección de aplicaciones en Android y iOS/iPadOS para asociados adicionales de Mobile Threat Defense

En octubre de 2019, la directiva de protección de aplicaciones de Intune agregó la capacidad de usar datos de nuestros asociados de Microsoft Threat Defense.

Con esta actualización, ampliamos esta compatibilidad al asociado siguiente para usar una directiva de protección de aplicaciones a fin de bloquear o borrar de forma selectiva los datos corporativos de un usuario en función del estado del dispositivo:

- **McAfee MVision Mobile** en Android, iOS y iPadOS

Para más información, consulte Creación de una directiva de protección de aplicaciones de Mobile Threat Defense con Intune.

Aumento del período de validez de los certificados para los perfiles SCEP y PKCS

Intune admite ya un **período de validez de certificados** de hasta **24** meses en los perfiles de certificados para el Protocolo de inscripción de certificados simple (SCEP) y los estándares de criptografía de clave pública (PKCS). Este supone un aumento del período de soporte técnico anterior de hasta 12 meses.

Esta compatibilidad se aplica a Windows y Android. Los períodos de validez de los certificados se ignoran en iOS/iPadOS y macOS.

Supervisión y solución de problemas

Nuevo informe organizativo de idoneidad para la administración conjunta

El informe **Idoneidad para la administración conjunta** proporciona una evaluación de idoneidad para los dispositivos que se pueden administrar de manera conjunta. La administración conjunta permite administrar simultáneamente dispositivos Windows 10 mediante Configuration Manager y Microsoft Intune. Podrá ver un resumen de este informe en el Centro de administración de Microsoft Endpoint Manager si selecciona la pestaña **Informes** > **Cloud attached devices (Dispositivos conectados a la nube)** > **Informes** > **Co-management eligibility** (Idoneidad para la administración conjunta). Para obtener información relacionada con los informes, vea Informes de Intune.

Nuevo informe organizativo de cargas de trabajo de administración conjunta

El informe de **cargas de trabajo de administración conjunta** proporciona un informe de los dispositivos que se administran de forma conjunta en la actualidad. La administración conjunta permite administrar simultáneamente dispositivos Windows 10 mediante Configuration Manager y Microsoft Intune. Puede ver este informe en el Centro de administración de Microsoft Endpoint Manager si selecciona la pestaña **Informes** > **Cloud attached devices (Dispositivos conectados a la nube)** > **Informes** > **Co-Managed Workloads** (Cargas de trabajo de administración conjunta). Para más información, vea Informes de Intune.

Log Analytics incluirá registros de detalles del dispositivo.

Los registros detallados del dispositivo de Intune ya están disponibles. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Informes** > **Log Analytics**. Puede correlacionar un conjunto de detalles del dispositivo para compilar consultas personalizadas y libros de Azure. Para obtener más información, vea Informes de integración de Azure Monitor (especialista).

Control de acceso basado en roles.

Compatibilidad con etiquetas de ámbito para la página estado de inscripción

Ahora puede asignar etiquetas de ámbito a la página de estado de inscripción, de modo que solo los roles que defina puedan verlo. Para obtener más información, consulte Creación de un perfil de la página de estado de la inscripción y asignación a un grupo.

Scripts

Propiedades beta adicionales de Data Warehouse

Ya hay propiedades adicionales disponibles mediante la API beta Data Warehouse de Intune. Las propiedades siguientes se exponen a través de la entidad de dispositivos en la API beta:

- `SubnetAddressV4Wifi`: dirección de subred para la conexión Wi-Fi de IPV4.
- `IpAddressV4Wifi`: dirección IP para la conexión Wi-Fi de IPV4.

Para obtener información relacionada, vea API de Data Warehouse de Microsoft Intune.

Semana del 25 de enero de 2021

Administración de aplicaciones

Actualización del icono de la aplicación Portal de empresa para iOS, macOS y la Web

Hemos actualizado el icono de aplicación del Portal de empresa para iOS, macOS y web. Este icono también se usa en el Portal de empresa para Windows. Los usuarios finales verán el icono nuevo en el iniciador de aplicaciones y la pantalla principal del dispositivo, en App Store de Apple y en las experiencias de las

aplicaciones del Portal de empresa.

Compatibilidad con aplicaciones del sistema de Android Enterprise en perfiles de trabajo de propiedad personal

Ahora puede implementar aplicaciones del sistema de Android Enterprise en dispositivos de perfil de trabajo de propiedad personal de Android Enterprise. Las aplicaciones del sistema son aquellas que no aparecen en Google Play Store administrado y que están preinstaladas en el dispositivo. Una vez que se haya implementado una aplicación del sistema, no podrá desinstalarla, ocultarla ni quitarla. Para obtener información relacionada con las aplicaciones del sistema, vea Incorporación de aplicaciones del sistema Android Enterprise a Microsoft Intune.

Supervisión y solución de problemas

Actualización al exportar informes de Intune mediante Graph API

Cuando use `exportJobs` de Graph API para exportar informes de Intune sin seleccionar ninguna columna para el informe de dispositivos, recibirá el conjunto de columnas predeterminado. Para reducir la confusión, se han quitado las columnas del conjunto de columnas predeterminado. Las columnas eliminadas son `PhoneNumberE164Format`, `_ComputedComplianceState`, `_OS` y `OSDescription`. Estas columnas aún se podrán seleccionar si las necesita, pero solo de forma explícita y no de manera predeterminada. Si ha configurado alguna automatización en torno a las columnas predeterminadas de la exportación de dispositivos y usa alguna de ellas, deberá refactorizar los procesos para que esas columnas y cualquier otra pertinente se seleccionen de manera explícita. Para obtener información relacionada, consulte Exportación de informes de Intune mediante Graph API.

Semana del 18 de enero de 2021

Configuración del dispositivo

Microsoft Tunnel ahora admite Red Hat Enterprise Linux 8

Ahora puede usar Red Hat Enterprise Linux (RHEL) 8 con Microsoft Tunnel. Para usar RHEL 8, no es necesario realizar ninguna acción. Se ha agregado compatibilidad con los contenedores de Docker que se actualizan automáticamente. Además, esta actualización también suprime algunos registros superfluos.

Semana del 11 de enero de 2021

Administración de aplicaciones

Eliminación de aplicaciones Win32 en una relación de dependencia

Las aplicaciones Win32 agregadas a Intune no se pueden quitar si están en una relación de dependencia. Estas aplicaciones solo se pueden eliminar después de quitar la relación de dependencia. Este requisito se aplica a las aplicaciones primarias y secundarias con una relación de dependencia. Además, este requisito garantiza que las dependencias se apliquen correctamente y que el comportamiento de la dependencia sea más predecible. Para más información, consulte Administración de aplicaciones Win32 en Microsoft Intune.

Compatibilidad de etiquetas de ámbito con directivas de personalización

Ahora puede asignar etiquetas de ámbito a las directivas de personalización. Para ello, vaya al Centro de administración de Microsoft Endpoint Manager > **Administración de inquilinos** > **Personalización** donde verá las opciones de configuración de **Etiquetas de ámbito**. Esta característica ya está disponible con Intune para Government o Intune operado por 21Vianet.

Configuración del dispositivo

Versión nueva del conector de certificados PFX

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2009.1.9**. Esta nueva versión del conector:

- Mejoras en la renovación del certificado de conector.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, consulte Conectores de certificados.

Semana del 4 de enero de 2021

Administración de aplicaciones

Habilitación automática del acceso al explorador durante la inscripción de perfiles de trabajo Android

El acceso al explorador ya está habilitado automáticamente en el dispositivo durante la inscripción de perfiles de trabajo de propiedad personal de Android Enterprise. Con este cambio, los dispositivos compatibles pueden usar el explorador para tener acceso a los recursos protegidos por el acceso condicional sin necesidad de realizar acciones adicionales. Antes de este cambio, los usuarios tenían que iniciar el Portal de empresa, seleccionar **Configuración** > **Habilitar acceso al explorador** y hacer clic en **Habilitar**.

Este cambio no afecta a los dispositivos que ya están inscritos.

Barra de progreso de la descarga de aplicaciones Win32

Mientras se descarga una aplicación Win32, los usuarios finales verán ahora una barra de progreso en el Portal de empresa de Windows. Esta característica ayudará a los clientes a comprender mejor el progreso de la instalación de la aplicación.

Actualización del icono de la aplicación Portal de empresa para Android

Hemos actualizado el icono de la aplicación Portal de empresa para Android para crear una apariencia más moderna para los usuarios del dispositivo. Para ver el aspecto del nuevo icono, vaya a la lista de Portal de empresa de Intune en Google Play.

Semana del 7 de diciembre de 2020

Aplicaciones de Intune

Nuevas aplicaciones protegidas disponibles para Intune

Las siguientes aplicaciones protegidas ya están disponibles para Microsoft Intune:

- Dynamics 365 Remote Assist
- Box - Cloud Content Management
- STid Mobile ID
- FactSet 3.0
- Notate para Intune
- Field Service (Dynamics 365)

Para obtener más información sobre las aplicaciones protegidas, vea Aplicaciones protegidas de Microsoft Intune.

Archivo de novedades

Para ver los meses anteriores, consulte el archivo de novedades.

Notificaciones

Estos avisos proporcionan información importante que puede ayudarle a prepararse para las características y los cambios futuros de Intune.

Actualización de los perfiles antivirus de seguridad de puntos de conexión para Windows 10

Hemos realizado un pequeño cambio para mejorar la experiencia de los perfiles antivirus para Windows 10. Esto no afecta al usuario final, ya que solo se trata de un cambio en el contenido que se muestra en la interfaz de usuario.

¿Cómo me afecta esto?

Anteriormente, al configurar un perfil de seguridad de Windows para la directiva antivirus de seguridad de puntos de conexión, tenía dos opciones para la mayoría de las configuraciones: *Sí* y *No configurado*. Ahora, esas

mismas configuraciones incluyen las opciones *Sí, No configurado* y *No* (la nueva opción). Los valores configurados previamente que se hayan establecido en *No configurado* seguirán con la opción *No configurado*. Al crear perfiles o editar los existentes, ahora tiene la opción de especificar explícitamente *No*.

Además, la configuración *Hide the Virus and threat protection area in the Windows Security app* (Ocultar el área de protección contra virus y amenazas en la aplicación Seguridad de Windows) tiene una configuración secundaria, *Hide the Ransomware data recovery option in the Windows Security app* (Ocultar la opción de recuperación de datos de ransomware en la aplicación Seguridad de Windows). Si la configuración principal (Ocultar el área de protección contra virus y amenazas) se ha establecido en *No configurado* y la configuración secundaria se ha establecido en *Sí*, ambas configuraciones se establecerán en *No configurado*. Esto se aplicará al editar el perfil.

¿Qué acción debo llevar a cabo?

No se requiere ninguna acción. Sin embargo, es posible que quiera notificar este cambio a su departamento de soporte técnico.

Plan de cambio: Intune finaliza el soporte técnico del Portal de empresa en versiones no admitidas de Windows

Intune sigue el ciclo de vida de Windows 10 en las versiones compatibles de esta sistema operativo. Ahora, estamos retirando el soporte técnico de los portales de empresa de Windows 10 asociados en esas versiones de Windows que están fuera de la directiva de soporte técnico moderno.

¿Cómo me afecta esto?

Dado que Microsoft ya no admite estos sistemas operativos, puede que este cambio no le afecte, dado que es probable que ya haya actualizado el sistema operativo o los dispositivos. Este cambio solo le afectará si sigue administrando versiones de Windows 10 no admitidas. Las versiones de Windows y del Portal de empresa afectadas son:

- Windows 10, versión 1507, Portal de empresa, versión 10.1.721.0
- Windows 10, versión 1511, Portal de empresa, versión 10.1.1731.0
- Windows 10, versión 1607, Portal de empresa, versión 10.3.5601.0
- Windows 10, versión 1703, Portal de empresa, versión 10.3.5601.0
- Windows 10, versión 1709, cualquier versión del Portal de empresa

Aunque no vamos a desinstalar estas versiones del Portal de empresa mencionadas anteriormente, las retiraremos de Microsoft Store y dejaremos de probar nuestras versiones de servicio con ellas.

Efecto para el usuario: si sigue usando una versión no admitida de Windows 10, los usuarios no podrán obtener las últimas actualizaciones de seguridad, ni nuevas características, correcciones de errores, mejoras de latencia, mejoras de accesibilidad e inversiones en rendimiento. System Center Configuration Manager e Intune no podrán administrar conjuntamente a los usuarios.

¿Qué tengo que hacer?

En el centro de administración de Microsoft Endpoint Manager, use la característica Aplicaciones detectadas para buscar aplicaciones con estas versiones. En el dispositivo de un usuario, la versión del Portal de empresa se muestra en la página **Configuración** del Portal de empresa. Actualice a una versión admitida de Windows o del Portal de empresa.

Plan de cambio: Intune avanza para admitir Android 6.0 y versiones posteriores en abril de 2021

Como se mencionó en MC234534, Intune pasará a ser compatible con Android 6.0 (Marshmallow) y versiones posteriores en el lanzamiento del servicio de abril (2104).

Cómo afectará este cambio a su organización

Dado que las aplicaciones móviles de Office para Android finalizaron la compatibilidad con Android 5.x (Lollipop) el 30 de junio de 2019 (MC181101), es posible que este cambio no le afecte; es probable que ya haya actualizado el sistema operativo o los dispositivos. Sin embargo, si tiene un dispositivo que todavía está

ejecutando la versión 5.x de Android o decide inscribir cualquier dispositivo que ejecute la versión 5.x de Android, tenga en cuenta que estos dispositivos ya no se admitirán. Puede actualizarlos a la versión 6.0 de Android (Marshmallow) o una versión posterior o reemplazarlos por un dispositivo en la versión 6.0 o posterior de Android.

> **NOTE**
> Los dispositivos Android de Teams no se ven afectados por este anuncio y seguirán siendo compatibles con independencia de su versión del sistema operativo Android.

Lo que necesita para prepararse

Notifique a su departamento de soporte técnico, si procede, este próximo cambio en la compatibilidad. También tiene dos opciones de administración para ayudar a informar a los usuarios finales o a bloquear la inscripción.

1. A continuación se muestra cómo puede advertir a los usuarios finales:
   - Use una directiva de cumplimiento de dispositivos para el administrador de dispositivos Android o Android Enterprise y establezca la acción de incumplimiento para enviar un mensaje a los usuarios antes de marcarlos como no compatibles.
   - Configure una opción de inicio condicional para la directiva de protección de aplicaciones con un requisito de versión de SO mínima para advertir a los usuarios.
2. A continuación se muestra cómo puede bloquear dispositivos en versiones inferiores a Android 6.0:
   - Configuración de restricciones de inscripción para impedir que se inscriban dispositivos en Android 5.x
   - Use una directiva de cumplimiento de dispositivos para el administrador de dispositivos Android o Android Enterprise para que los dispositivos en Android 5.x no sean compatibles.
   - Configure una opción de inicio condicional para la directiva de protección de aplicaciones con un requisito de versión de SO mínima para bloquear el acceso a las aplicaciones de los usuarios.

Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune

14/05/2021 • 26 minutes to read

Obtenga información sobre las actualizaciones más recientes para las aplicaciones de Microsoft Intune. Periódicamente agregamos contenido y mejoras a la aplicación y el sitio web de Portal de empresa de Intune. Si es un administrador de Intune o un empleado de soporte técnico, en este artículo encontrará la información que necesita para:

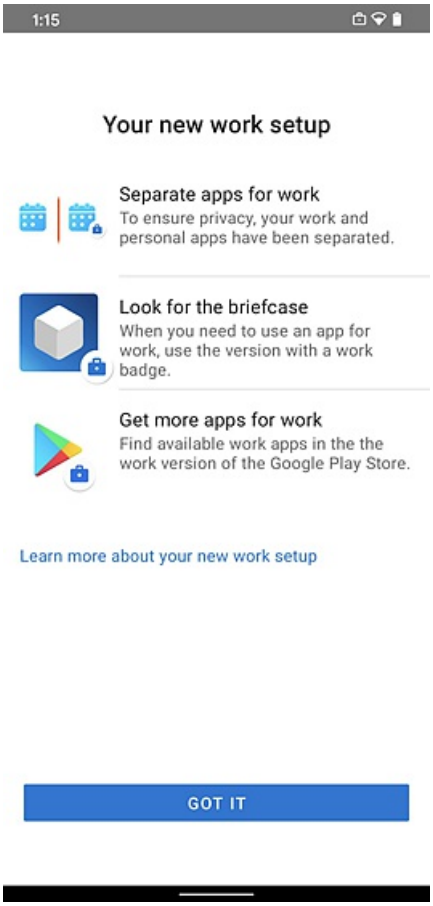
- Alertar a los alumnos y los empleados sobre cambios en la aplicación y la inscripción.
- Actualizar la documentación y los procedimientos del departamento de soporte técnico de la organización.

Si es un empleado o un alumno, asegúrese de consultar las capturas de pantalla y los vínculos de la documentación de ayuda del Portal de empresa. Para obtener más información sobre cómo usar la aplicación Portal de empresa, vea la documentación de ayuda al usuario del Portal de empresa.

Semana del 9 de noviembre de 2020

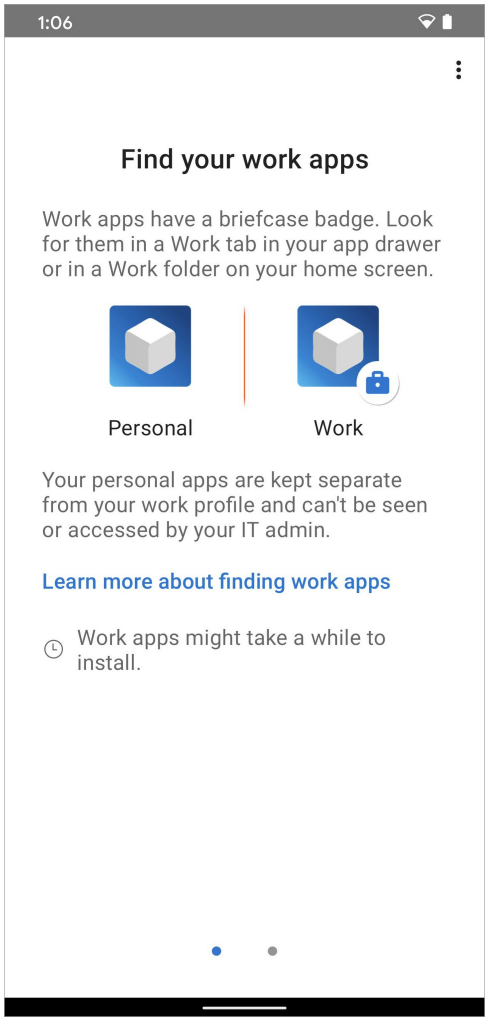
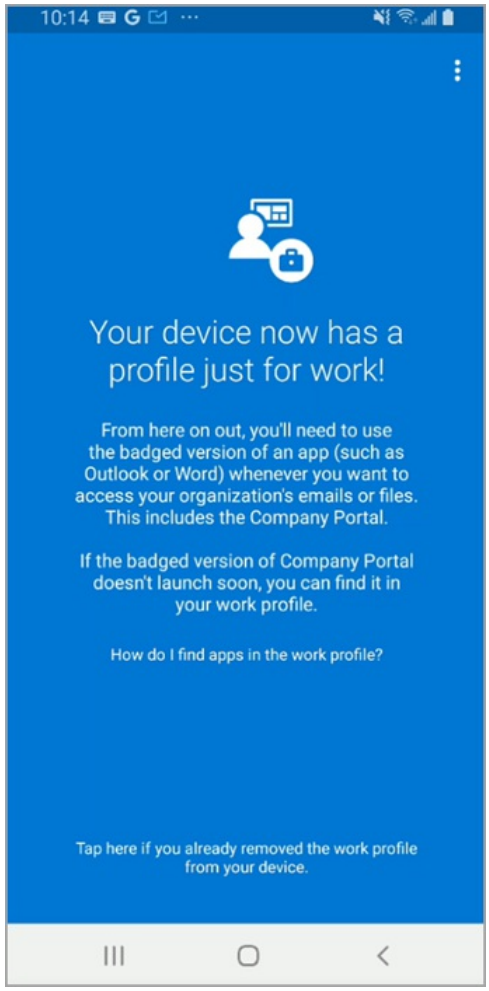
Mejoras en la mensajería del perfil de trabajo en el Portal de empresa para Android

Hemos actualizado la mensajería en el Portal de empresa para Android para presentar y explicar mejor cómo funciona el perfil de trabajo. Después del flujo de configuración del perfil de trabajo, los usuarios verán una nueva pantalla informativa en la que se explica dónde encontrar las aplicaciones de trabajo, con vínculos a la documentación de ayuda.

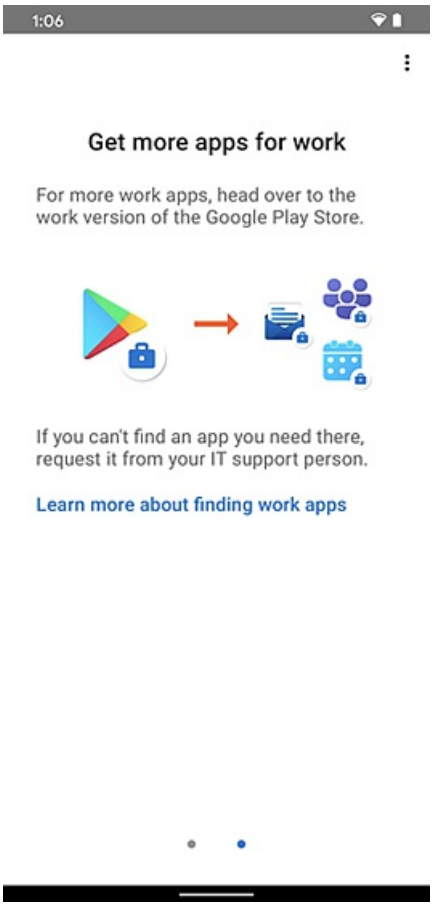


Cuando un usuario vuelve a habilitar accidentalmente la aplicación Portal de empresa en el perfil personal, verá

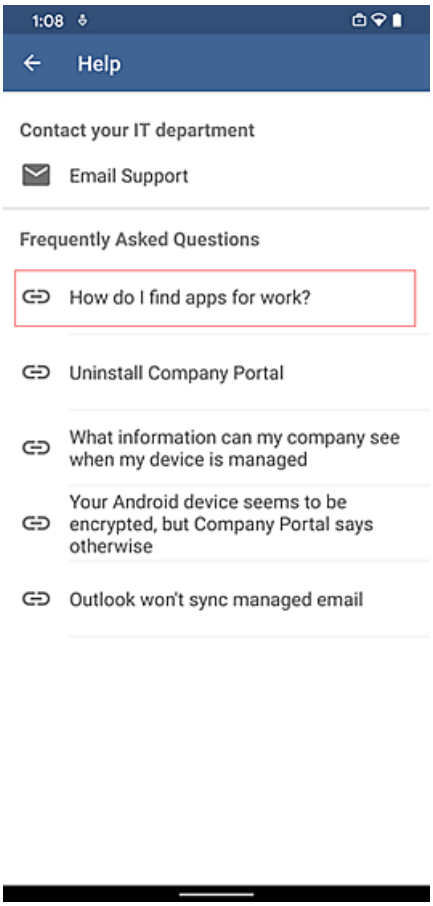
una pantalla (anteriormente, **ahora el dispositivo tiene un perfil solo para el trabajo**) que lo guía en sus aplicaciones de trabajo, con vínculos a la documentación de ayuda.

ACTUALIZADO	ANTERIOR
	

Cuando deslice el dedo hacia la derecha, aprenderá cómo obtener más aplicaciones de trabajo desde Google Play Store. `



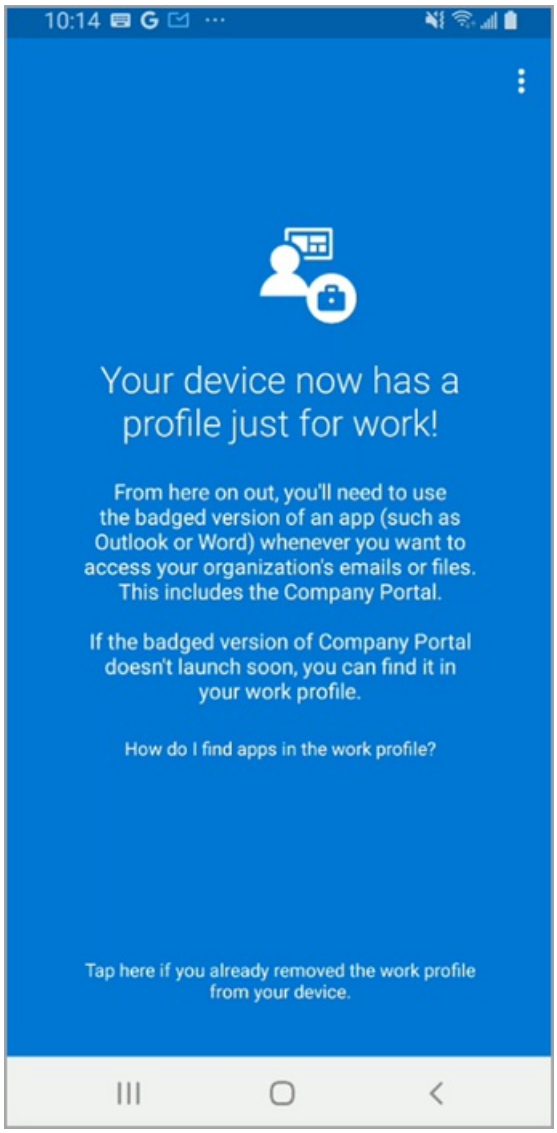
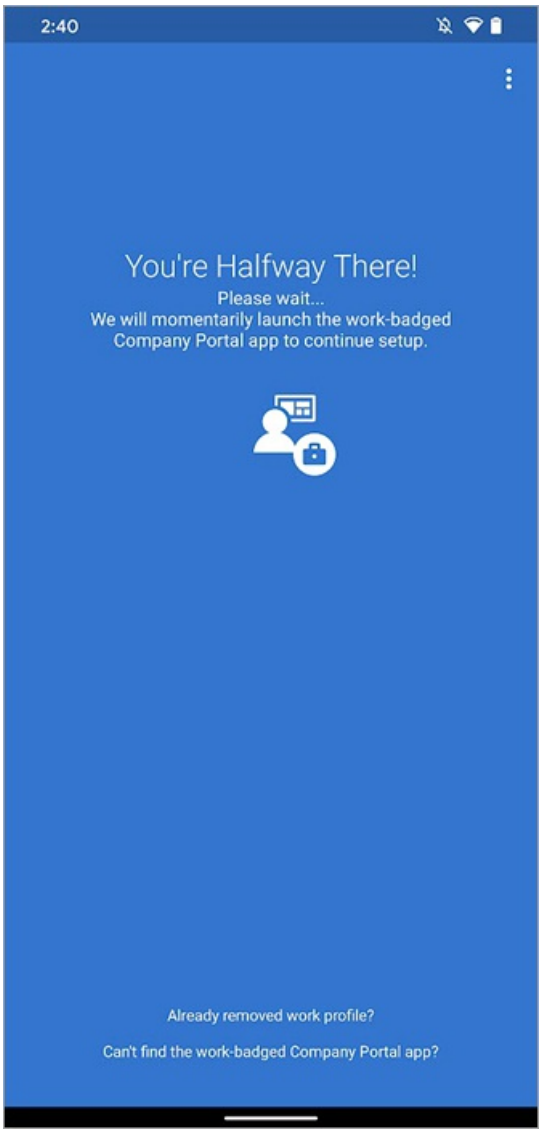
Por último, en la página **Ayuda** > sección **Preguntas más frecuentes**, hay un vínculo a un artículo de Microsoft Docs sobre como buscar aplicaciones del perfil de trabajo.



Semana del 28 de septiembre de 2020

Mejora en la mensajería del perfil de trabajo en el Portal de empresa para Android

La pantalla del Portal de empresa que antes se titulaba "Ya va por la mitad" se ha actualizado para que explique mejor cómo funciona la administración de perfiles de trabajo. Los usuarios verán esta pantalla si vuelven a habilitar el Portal de empresa en el perfil personal una vez que hayan realizado la inscripción del perfil de trabajo. También pueden ver esta pantalla durante la inscripción del perfil de trabajo en algunas versiones del sistema operativo Android, tal como se muestra en el documento de ayuda titulado Inscribir dispositivos con perfil profesional Android.

ACTUALIZADO	ANTERIOR
	

Semana del 10 de agosto de 2020

Mejora en la página Actualizar configuración del dispositivo de la aplicación Portal de empresa para Android para mostrar descripciones

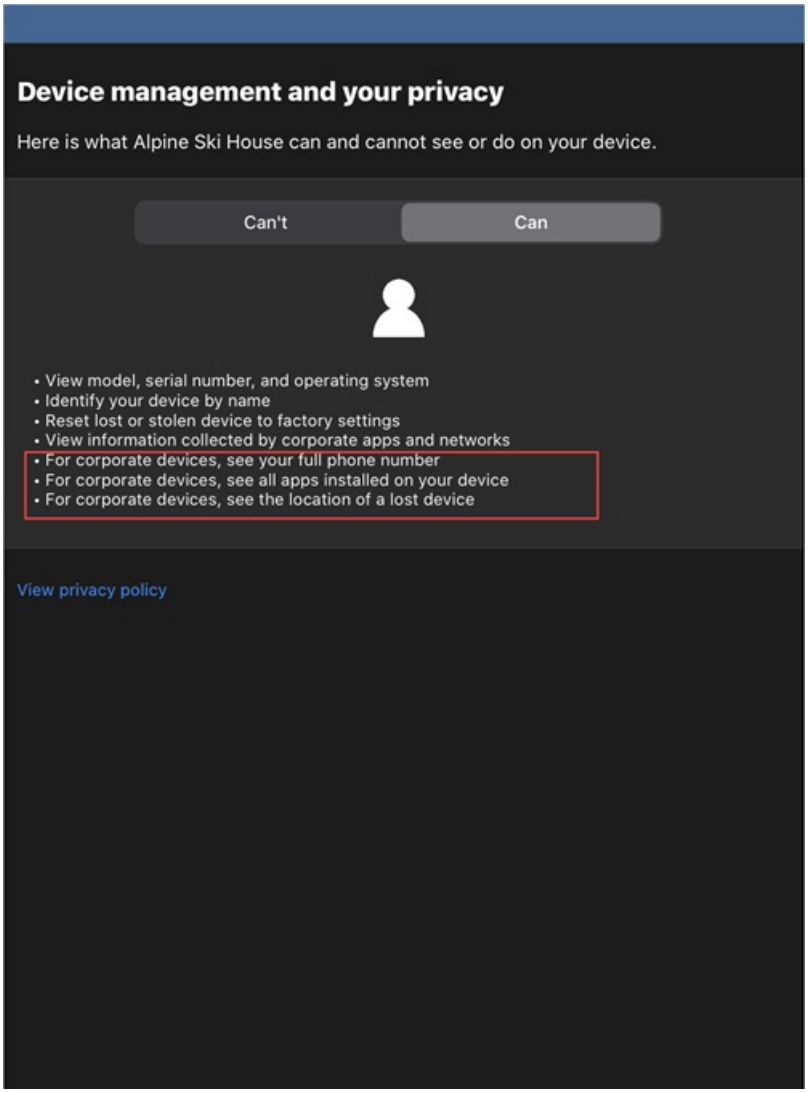
En la aplicación Portal de empresa de dispositivos Android, en la página **Actualizar configuración del dispositivo** se muestra la configuración que debe actualizar un usuario para que sea compatible. Los usuarios expanden el problema para ver más información y verán el botón **Resolver**.

Esta experiencia del usuario se ha mejorado. Las opciones enumeradas se expanden de forma predeterminada para mostrar la descripción y el botón **Resolver**, cuando proceda. Anteriormente, los problemas estaban contraídos de forma predeterminada. Este nuevo comportamiento predeterminado reduce el número de clics, por lo que los usuarios pueden resolver los problemas más rápidamente.

Semana del 8 de junio de 2020

Actualizaciones de la pantalla informativa en Portal de empresa para iOS/iPadOS

Hemos actualizado una pantalla informativa en Portal de empresa para iOS/iPadOS a fin de explicar mejor lo que un administrador puede ver y hacer en los dispositivos. Estas aclaraciones solo se aplican a los dispositivos corporativos. Solo se ha actualizado el texto, no se han realizado modificaciones reales de lo que el administrador puede ver o realizar en los dispositivos de usuario. Para obtener más información sobre lo que puede ver un administrador, vea ¿Qué información puede ver mi organización cuando inscribo mi dispositivo?

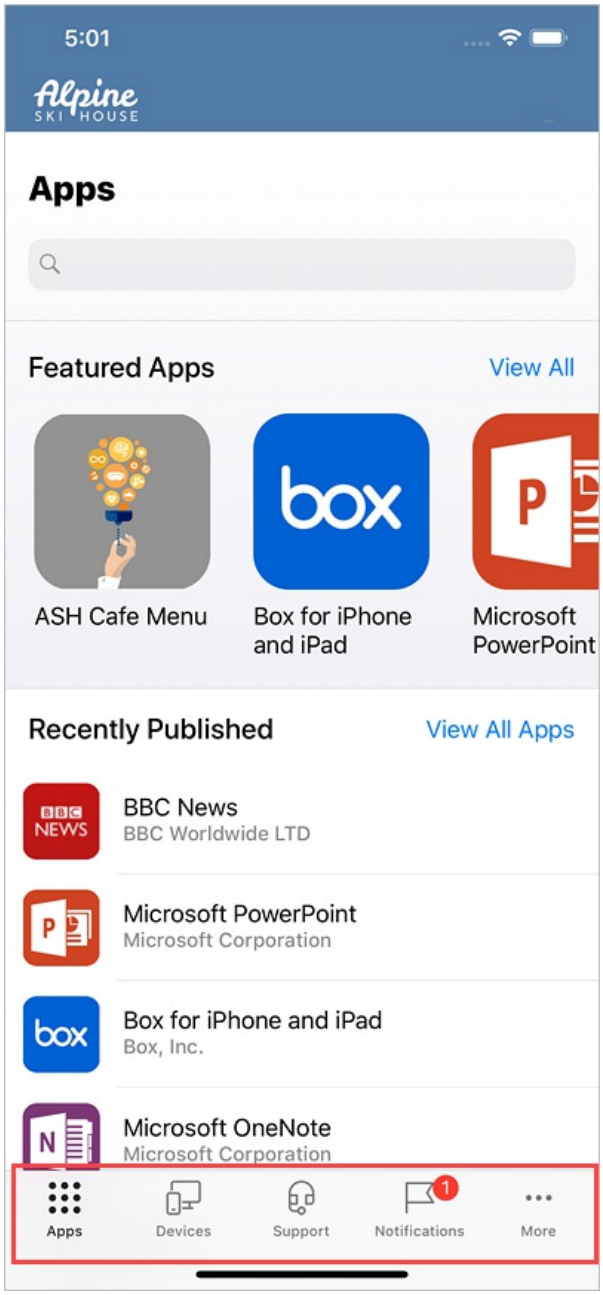


Semana del 18 de mayo de 2020

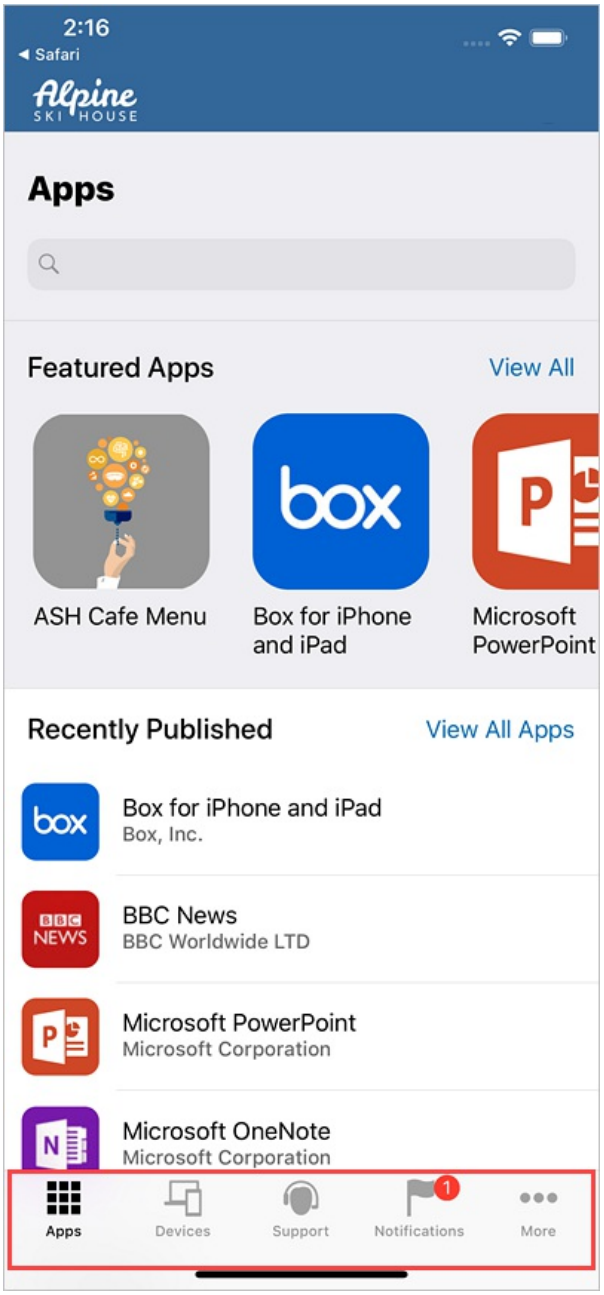
Actualización de iconos de la aplicación Portal de empresa para iOS/iPados y macOS

Actualizamos los iconos en Portal de empresa para crear una apariencia más moderna que sea compatible en dispositivos de pantalla doble y se alinee con Microsoft Fluent Design System.

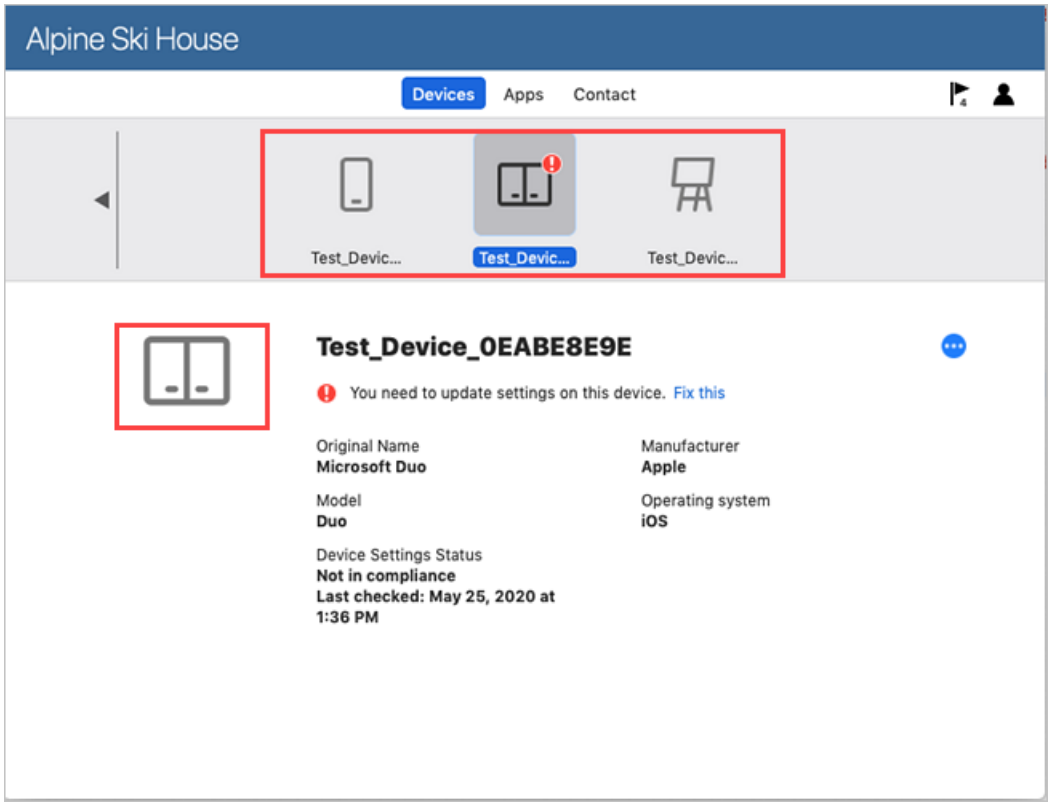
ACTUALIZADO PARA IOS/IPADOS



ANTERIORMENTE PARA IOS/IPADOS



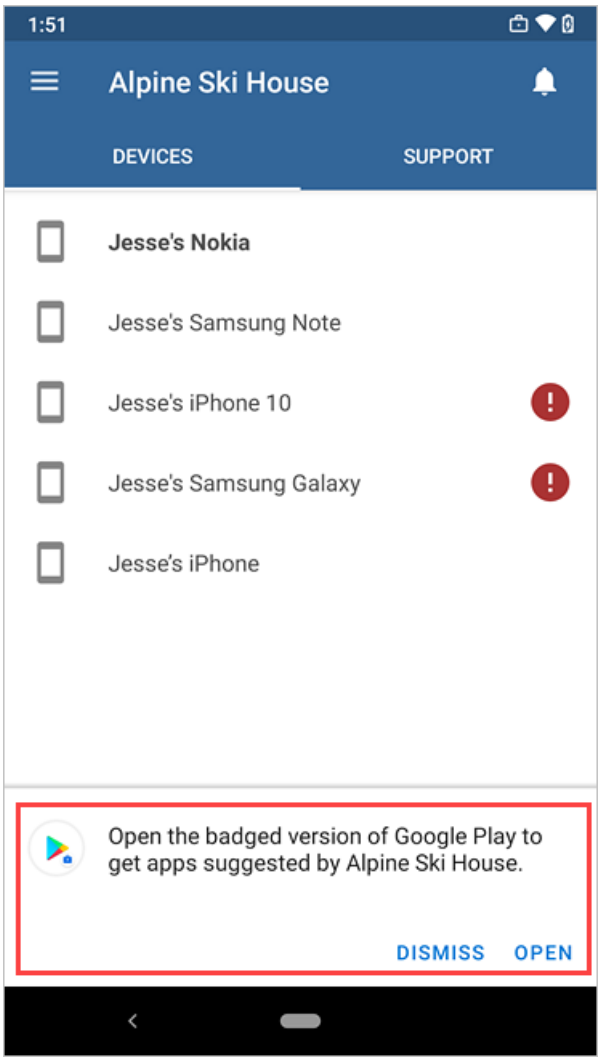
ACTUALIZADO PARA MACOS



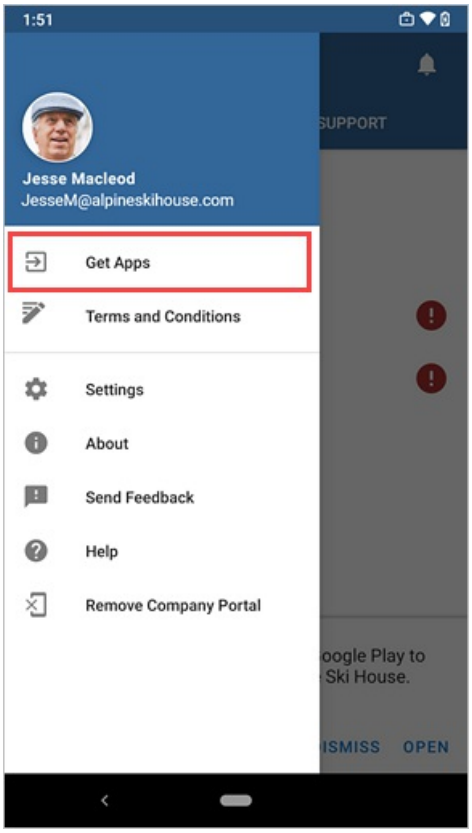
Semana del 4 de mayo de 2020

Portal de empresa para Android guía a los usuarios para obtener aplicaciones después de la inscripción del perfil de trabajo

Hemos mejorado las instrucciones en la aplicación del Portal de empresa para facilitar a los usuarios la búsqueda e instalación de aplicaciones. Después de la inscripción en la administración del perfil de trabajo, los usuarios recibirán un mensaje que explica cómo encontrar aplicaciones sugeridas en la versión con distintivo de Google Play. El último paso de Inscribir dispositivos con perfil Android se ha actualizado para mostrar el mensaje nuevo.

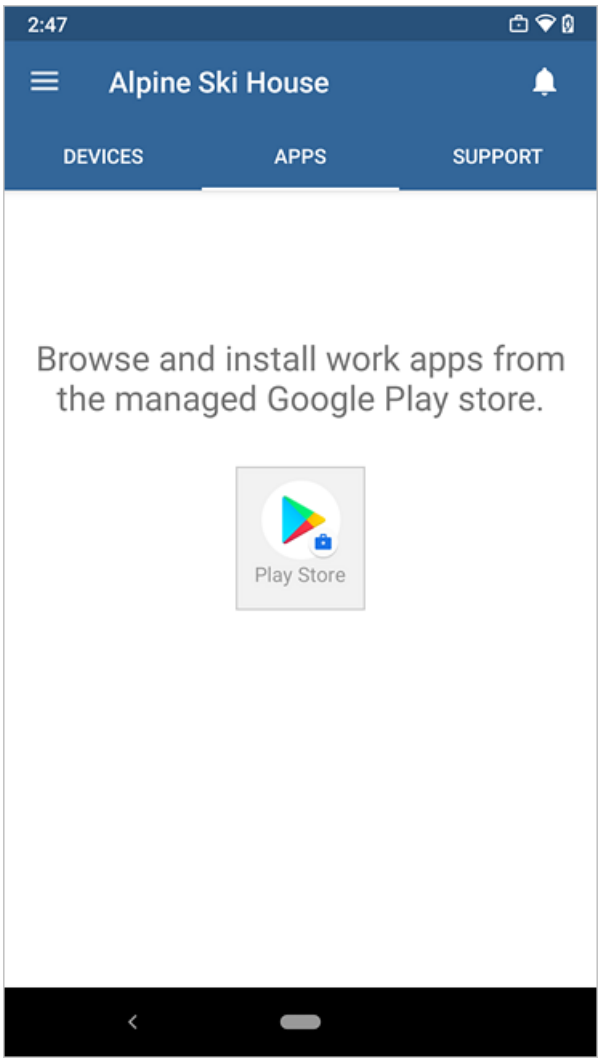


Los usuarios también verán un nuevo vínculo **Obtener aplicaciones** en el cajón de Portal de empresa de la izquierda.



Para dejar espacio a estas experiencias nuevas y mejoradas, se ha quitado la pestaña **APLICACIONES** que se

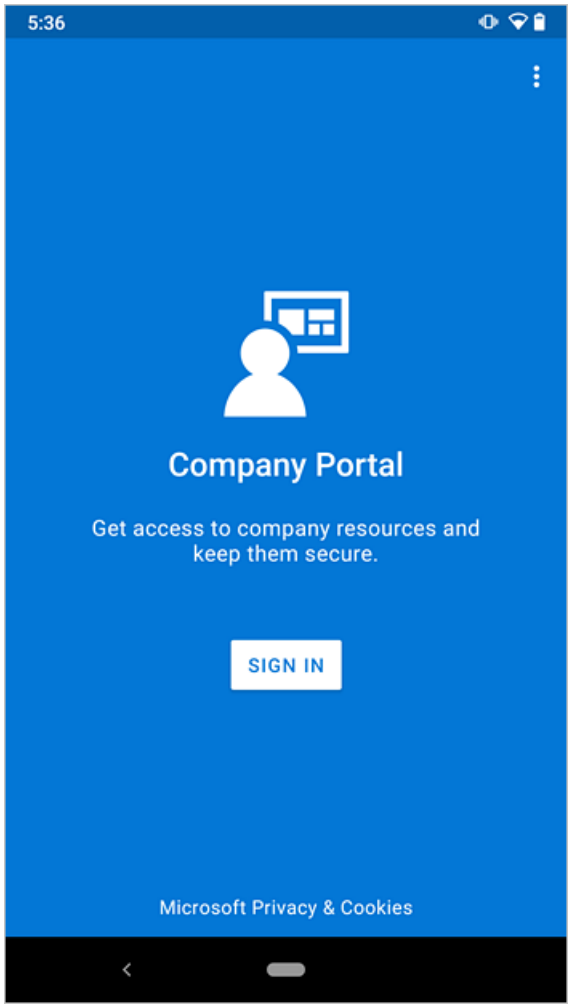
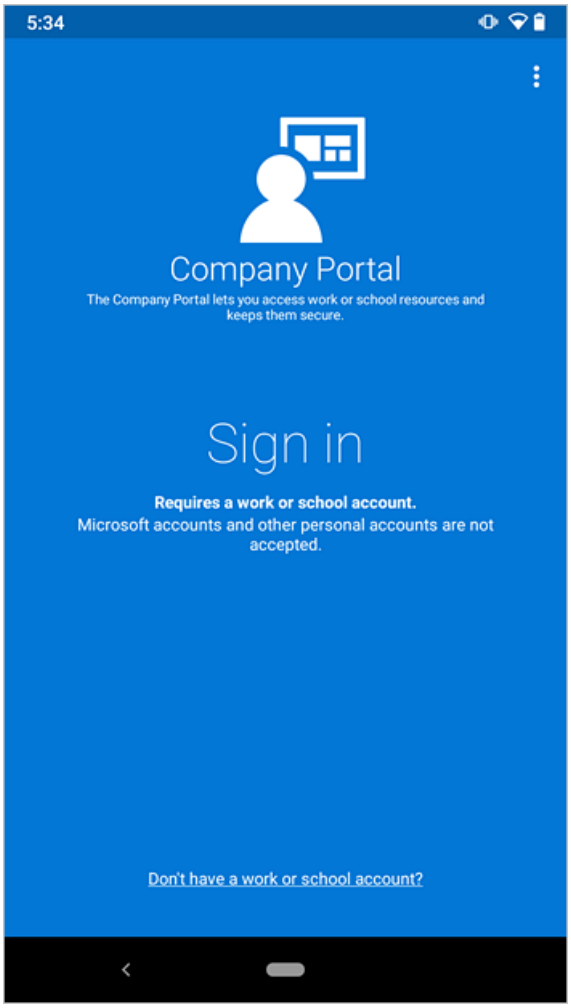
muestra en la siguiente imagen.

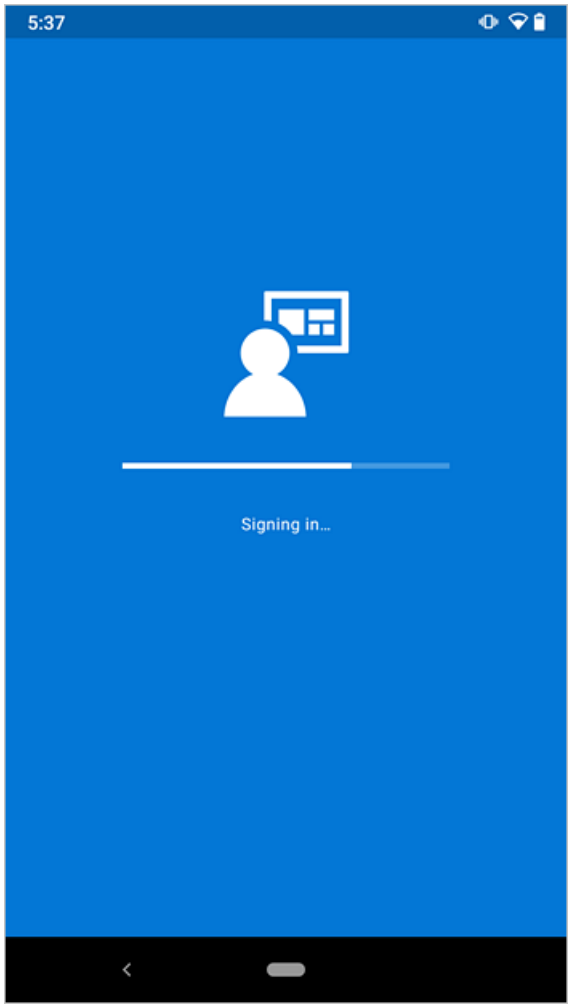
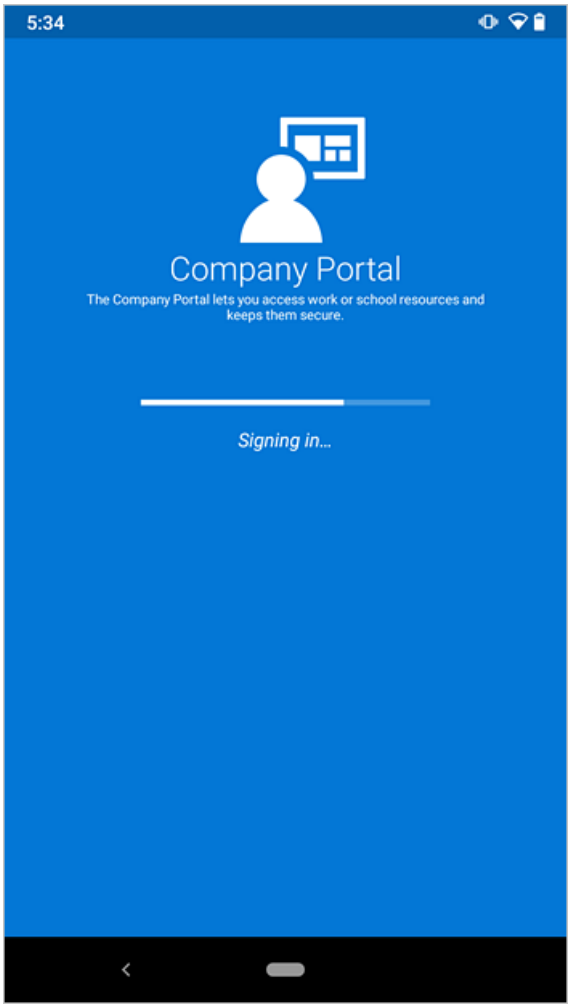


Semana del 2 de marzo de 2020

Experiencia de inicio de sesión mejorada en la aplicación Portal de empresa para Android

Hemos actualizado el diseño de varias pantallas de inicio de sesión en la aplicación Portal de empresa para Android a fin de que la experiencia sea más moderna, sencilla y limpia para los usuarios. Para ver todas las instrucciones de inscripción del Portal de empresa para Android, vaya a Inscripción de su dispositivo Android o Inscribir dispositivos con perfil profesional Android.

ACTUALIZADO	ANTERIOR
	

ACTUALIZADO	ANTERIOR
	

Semana del 3 de febrero de 2020

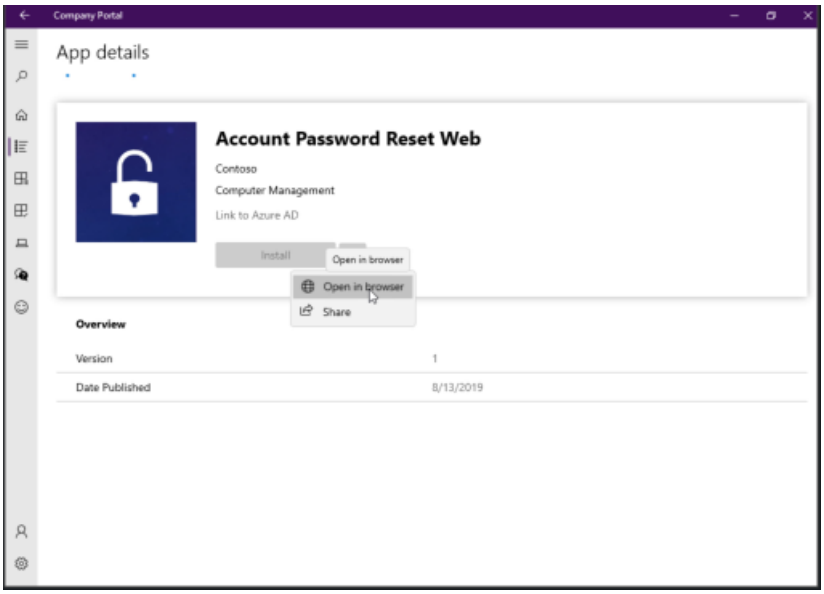
Pantalla quitada del Portal de empresa, inscripción del perfil de trabajo de Android

La pantalla **¿Cuál es el paso siguiente?** se ha quitado del flujo de inscripción del perfil de trabajo de Android en el Portal de empresa para simplificar la experiencia del usuario. Vaya a Inscripción con el perfil de trabajo de Android para ver el flujo de inscripción del perfil de trabajo de Android actualizado.

Semana del 11 de noviembre de 2019

Aplicaciones web iniciadas desde la aplicación Portal de empresa de Windows

Los usuarios finales ahora pueden iniciar aplicaciones web directamente desde la aplicación Portal de empresa de Windows. Los usuarios finales pueden seleccionar la aplicación web y, a continuación, elegir la opción **Abrir en el explorador**. La dirección URL web publicada se abre directamente en un explorador web. Esta funcionalidad se implementará durante la próxima semana. Para más información sobre las aplicaciones web, consulteAgregar aplicaciones web a Microsoft Intune.



Experiencia mejorada de inscripción de macOS en el Portal de empresa

La experiencia de inscripción del Portal de empresa para macOS cuenta con un proceso de inscripción más sencillo que es más coherente con la experiencia de inscripción en el Portal de empresa para iOS. Los usuarios del dispositivo ahora ven lo siguiente:

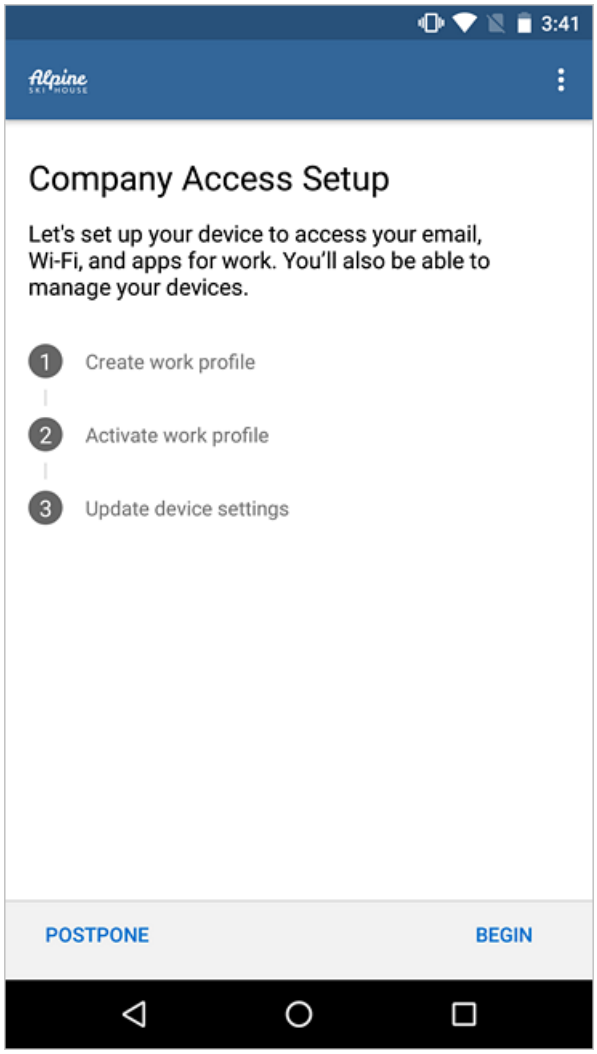
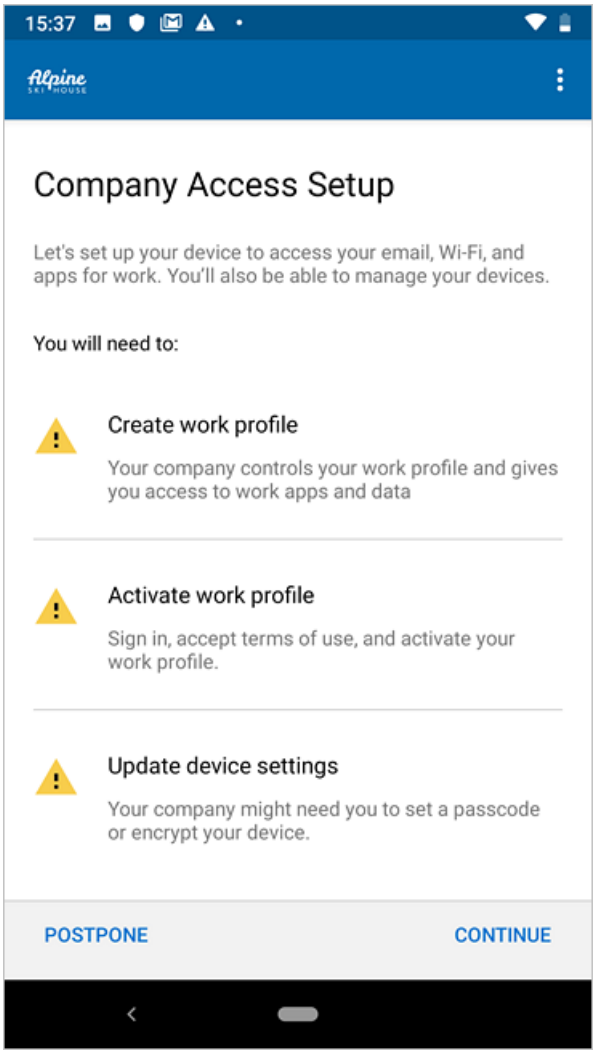
- Una interfaz de usuario más elegante.
- Una lista de comprobación de inscripción mejorada.
- Instrucciones más claras sobre cómo inscribir sus dispositivos.
- Mejores opciones de solución de problemas.

Semana del 28 de octubre de 2019

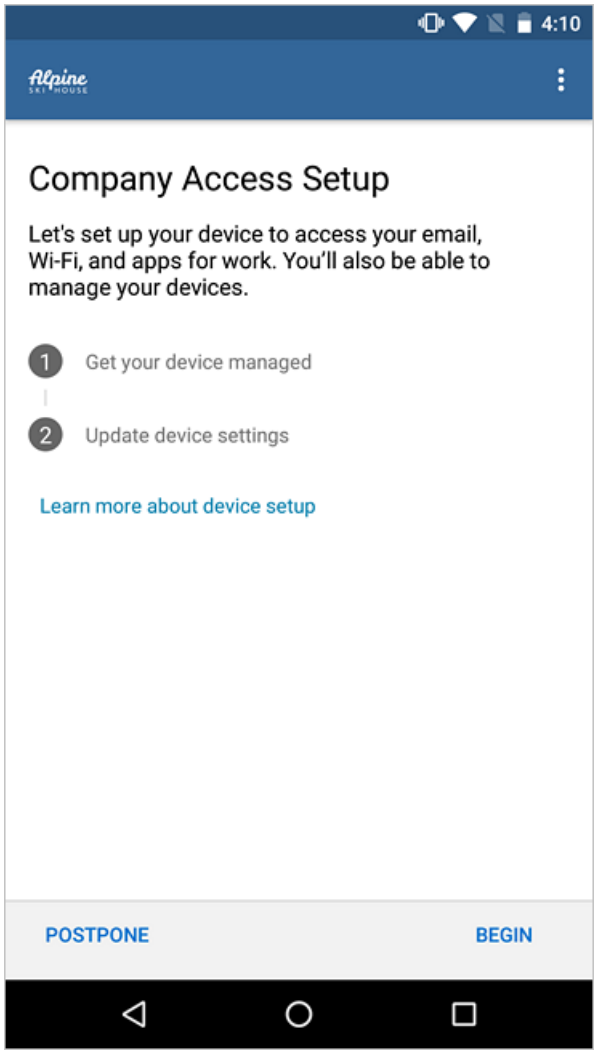
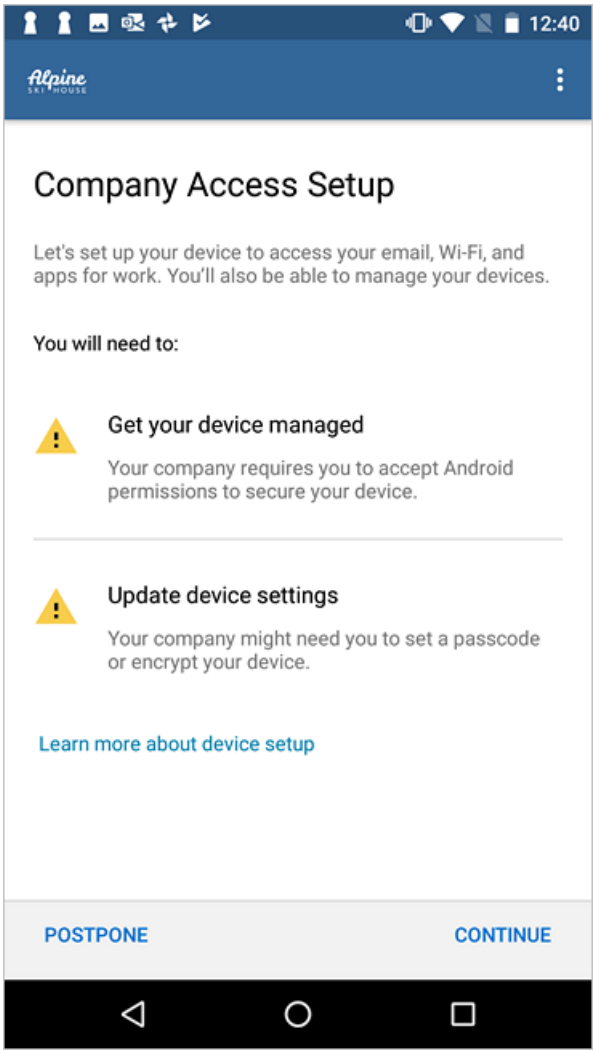
Diseño de la lista de comprobación mejorado en la aplicación Portal de empresa para Android

La lista de comprobación de configuración de la aplicación Portal de empresa para Android se ha actualizado con un diseño ligero y nuevos iconos. Los cambios se alinean con las actualizaciones recientes realizadas en la aplicación Portal de empresa para iOS/iPadOS. Para ver los pasos de inscripción actualizados, consulte Inscripción con el perfil de trabajo Android e Inscripción de su dispositivo Android.

En las pantallas siguientes se muestra la lista de comprobación actualizada para la inscripción del perfil de trabajo de Android:

ACTUALIZADO	ANTERIOR
	

En las pantallas siguientes se muestra la lista de comprobación actualizada para la inscripción del administrador de dispositivos Android:

ACTUALIZADO	ANTERIOR
	

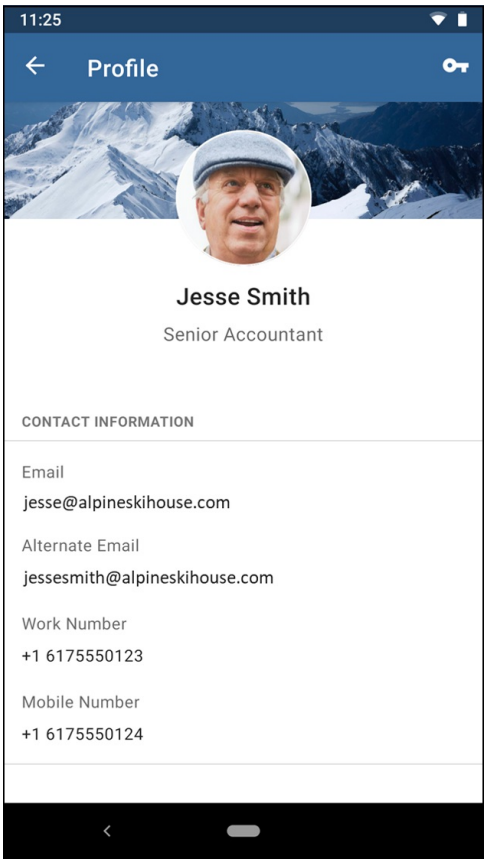
Semana del 9 de septiembre de 2019

Actualizaciones a la aplicación de Microsoft Intune

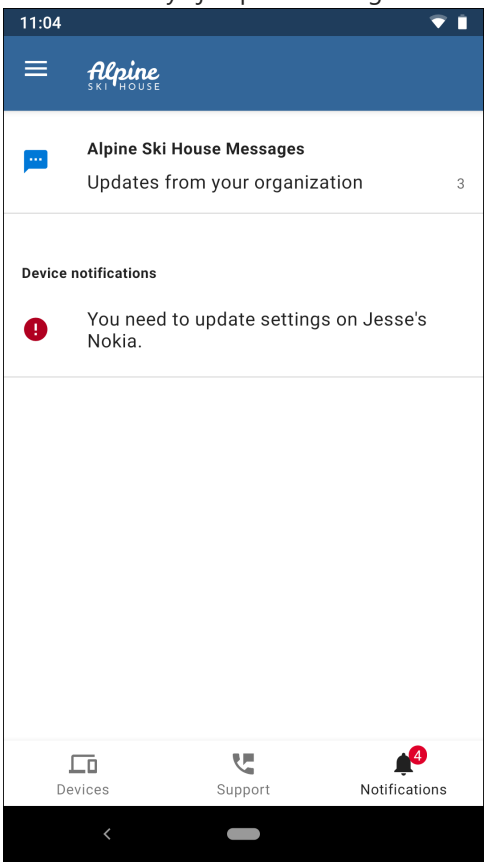
La aplicación de Microsoft Intune para Android se ha actualizado con las siguientes mejoras:

- Se ha actualizado y mejorado el diseño para incluir la navegación inferior para las acciones más importantes.
- Se ha agregado una página adicional que muestra el perfil del usuario.
- Se ha agregado la muestra de notificaciones interactivas en la aplicación para el usuario, como la necesidad de actualizar la configuración del dispositivo.
- Se ha agregado la muestra de notificaciones push personalizadas, alineando la aplicación con la compatibilidad agregada recientemente en la aplicación Portal de empresa para iOS y Android. Para más información, consulte Envío de notificaciones personalizadas en Intune.

  Ejemplo de perfil de usuario:



Notificaciones y ejemplo de navegación inferior:

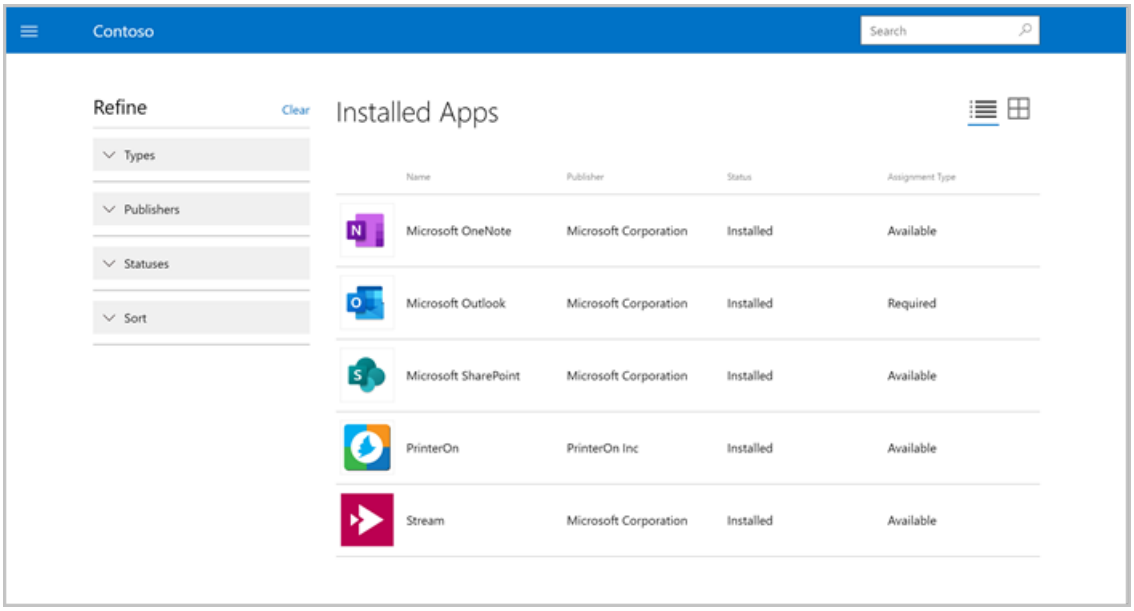


Semana del 24 de junio de 2019

Ver todas las aplicaciones instaladas desde la página web del Portal de empresa

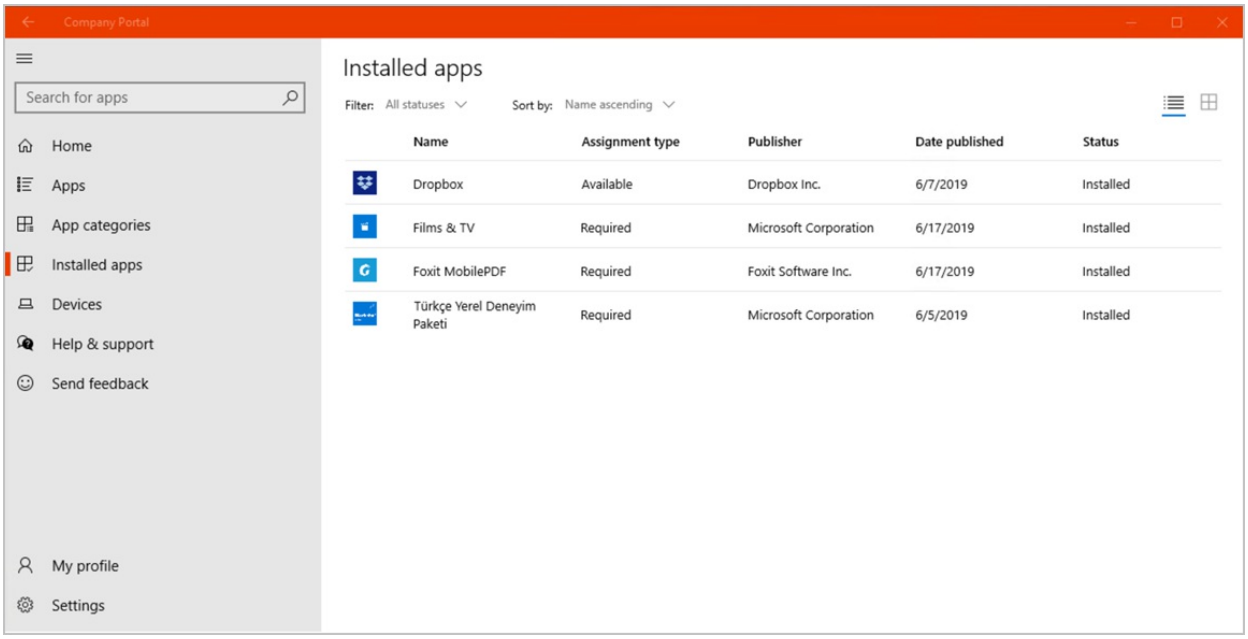
La nueva página **Aplicaciones instaladas** del sitio web del Portal de empresa muestra todas las aplicaciones administradas (requeridas y disponibles) que están instaladas en los dispositivos de un usuario. Además del tipo de asignación, los usuarios pueden ver el editor de la aplicación, la fecha de publicación y el estado de

instalación actual. Si todavía no hay ninguna aplicación requerida o disponible para los usuarios, estos verán un mensaje en el que se explica que no hay ninguna aplicación de la empresa instalada. Para ver la página nueva en la Web, vaya al sitio web del Portal de empresa y haga clic en **Aplicaciones instaladas**.



La vista nueva permite que los usuarios de las aplicaciones vean todas las aplicaciones administradas instaladas en el dispositivo

La aplicación Portal de empresa para Windows ahora muestra todas las aplicaciones administradas (tanto las requeridas como las disponibles) que están instaladas en el dispositivo de un usuario. Los usuarios también pueden ver las instalaciones de aplicaciones intentadas y pendientes, además de sus estados actuales. Si todavía no hay ninguna aplicación requerida o disponible para los usuarios, estos verán un mensaje en el que se explica que no hay ninguna aplicación de la empresa instalada. Para ver la vista nueva, vaya al panel de navegación del Portal de empresa y seleccione **Aplicaciones** > **Aplicaciones instaladas**.



Semana del 17 de junio de 2019

Características nuevas de la aplicación Microsoft Intune

Hemos agregado características nuevas a la aplicación Microsoft Intune (versión preliminar) para Android. Los usuarios de dispositivos Android totalmente administrados ahora pueden:

- Ver y administrar los dispositivos inscritos mediante la aplicación Portal de empresa de Intune o

Microsoft Intune.

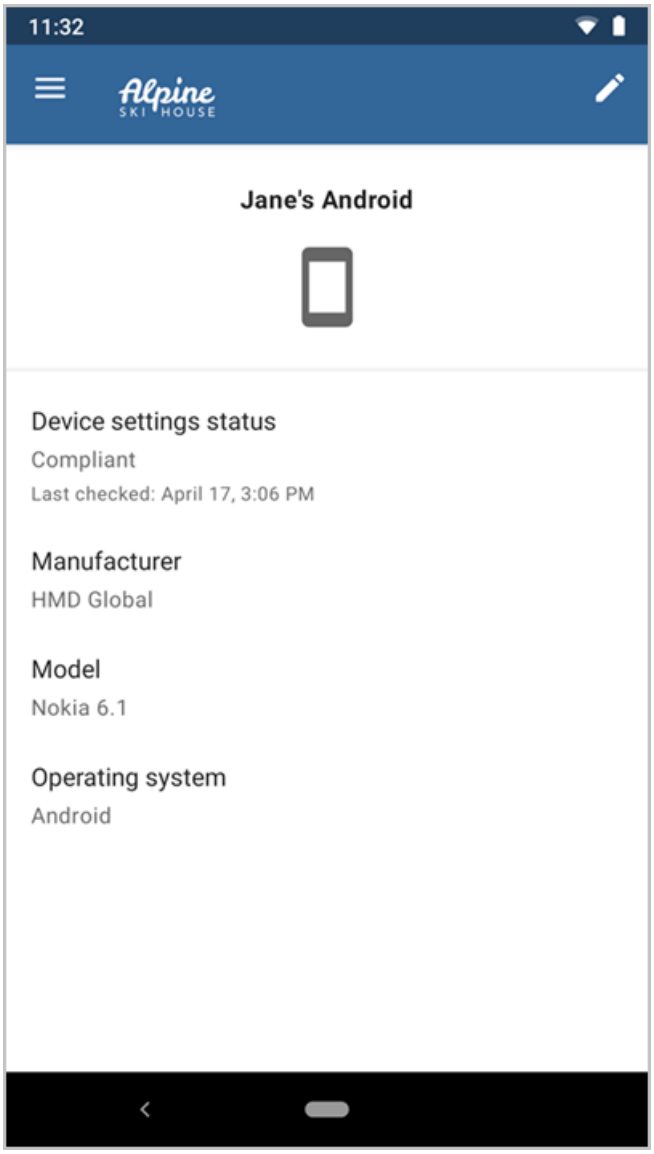
- Ponerse en contacto con su organización para obtener soporte técnico.
- Enviar comentarios a Microsoft.
- Consultar los términos y condiciones, si la organización los estableció.

Semana del 15 de abril de 2019

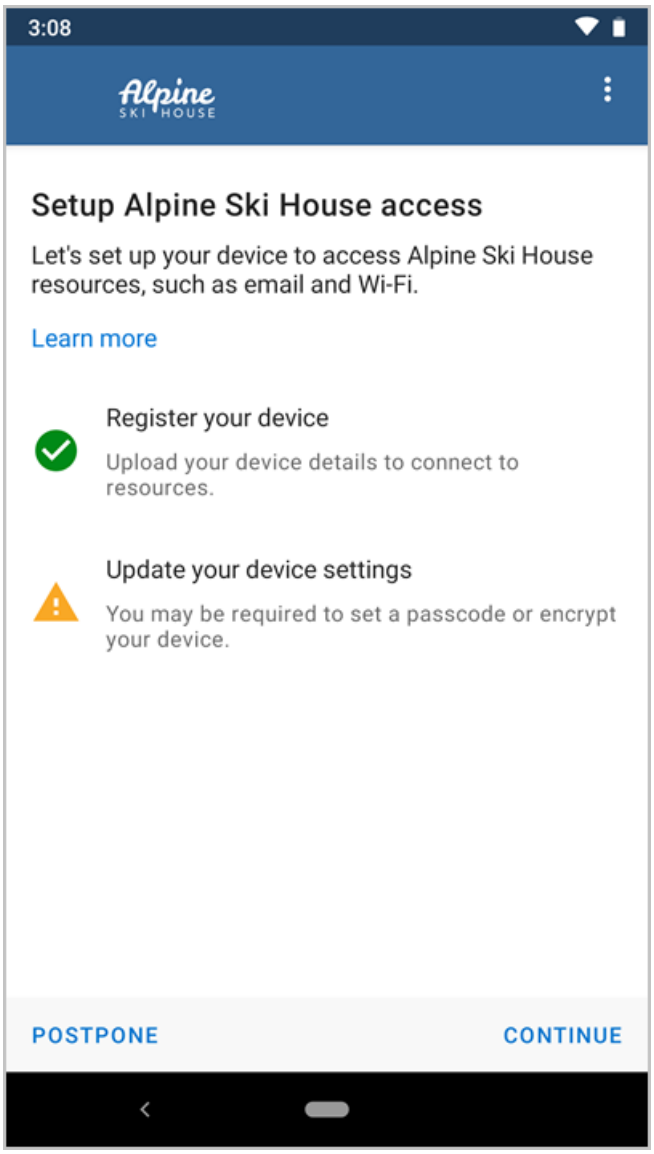
Nueva aplicación de usuario final (aplicación de Microsoft Intune)

Hay una nueva aplicación de usuario final para dispositivos Android totalmente administrados denominada **Microsoft Intune**. Esta nueva aplicación, ligera y moderna, proporciona una funcionalidad similar a la de la aplicación Portal de empresa, pero para dispositivos corporativos totalmente administrados. Para obtener más información, vea la aplicación Microsoft Intune en Google Play.

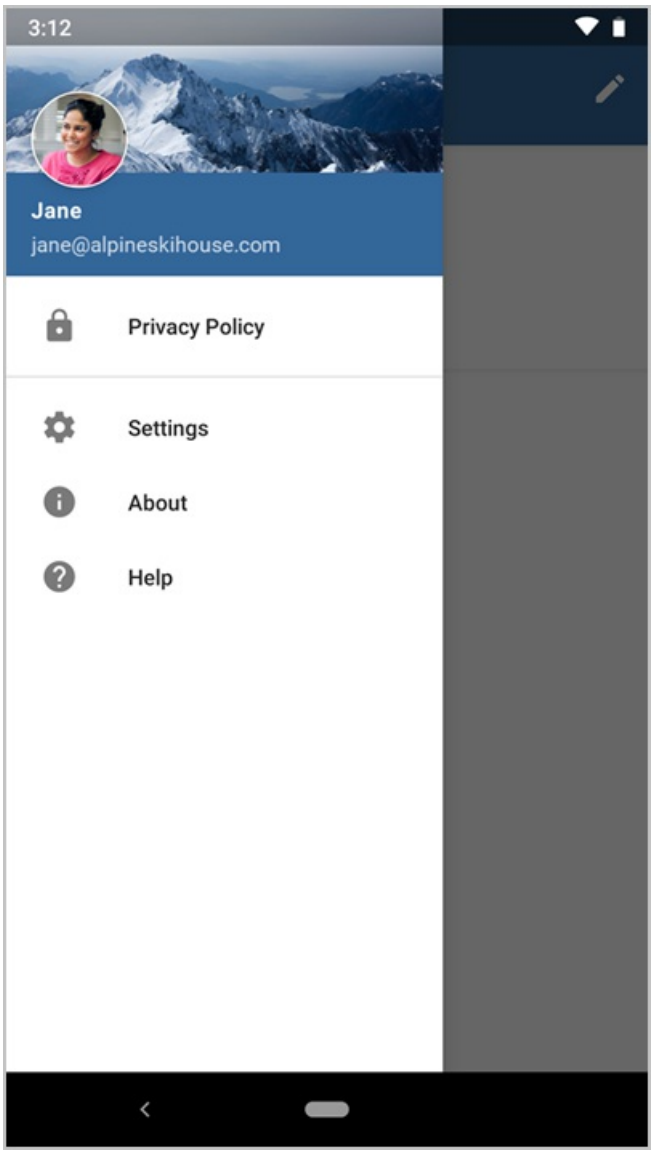
Captura de pantalla de ejemplo de la pantalla de detalles del dispositivo:



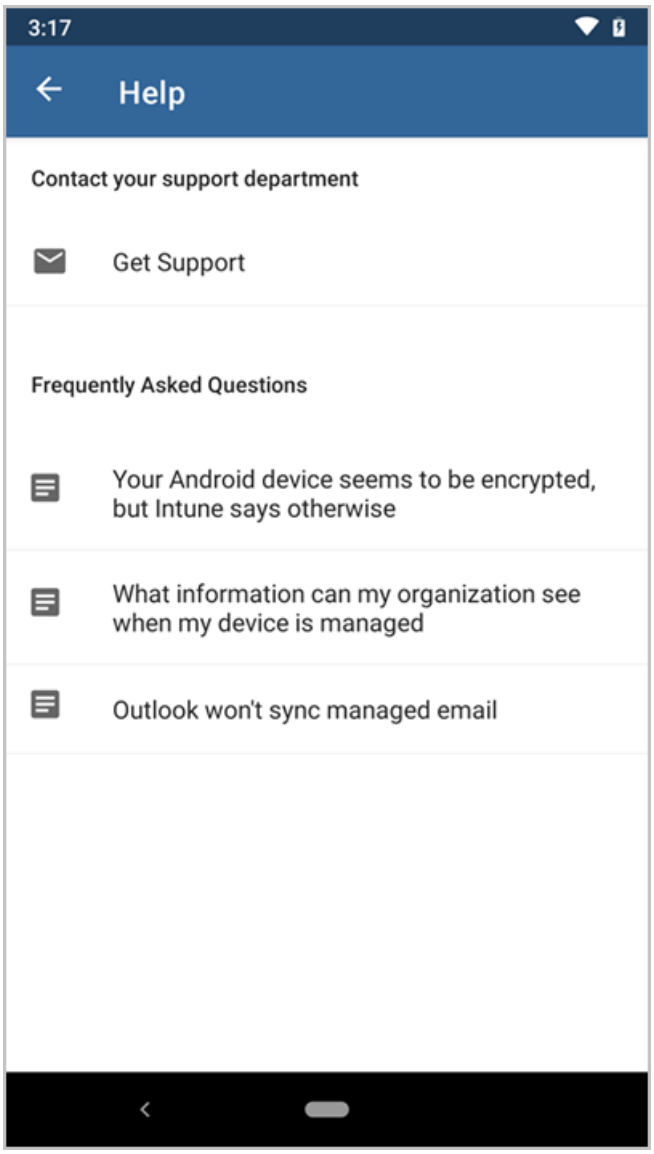
Captura de pantalla de ejemplo de la pantalla de **configuración del acceso**:



Captura de pantalla de ejemplo del menú de la aplicación:



Captura de pantalla de ejemplo de la pantalla de **ayuda**:



Semana del 1 de abril de 2019

Cambios en la inscripción del Portal de empresa para los usuarios de dispositivos iOS 12

Se han actualizado los pasos y las pantallas de inscripción del Portal de empresa para iOS con el fin de ajustarlos a los cambios en la inscripción de MDM que se introdujeron en Apple iOS 12.2. En el nuevo flujo de trabajo, se pide a los usuarios que hagan esto:

- Permitir que Safari abra el sitio web del Portal de empresa y descargue el perfil de administración antes de volver a la aplicación Portal de empresa.
- Abrir la aplicación Ajustes para instalar el perfil de administración en el dispositivo.
- Volver a la aplicación Portal de empresa para completar la inscripción.

Para conocer los pasos y las pantallas de inscripción actualizados, vea cómo inscribir dispositivos iOS en Intune.

Actualización de la experiencia de usuario para la aplicación Portal de empresa para iOS

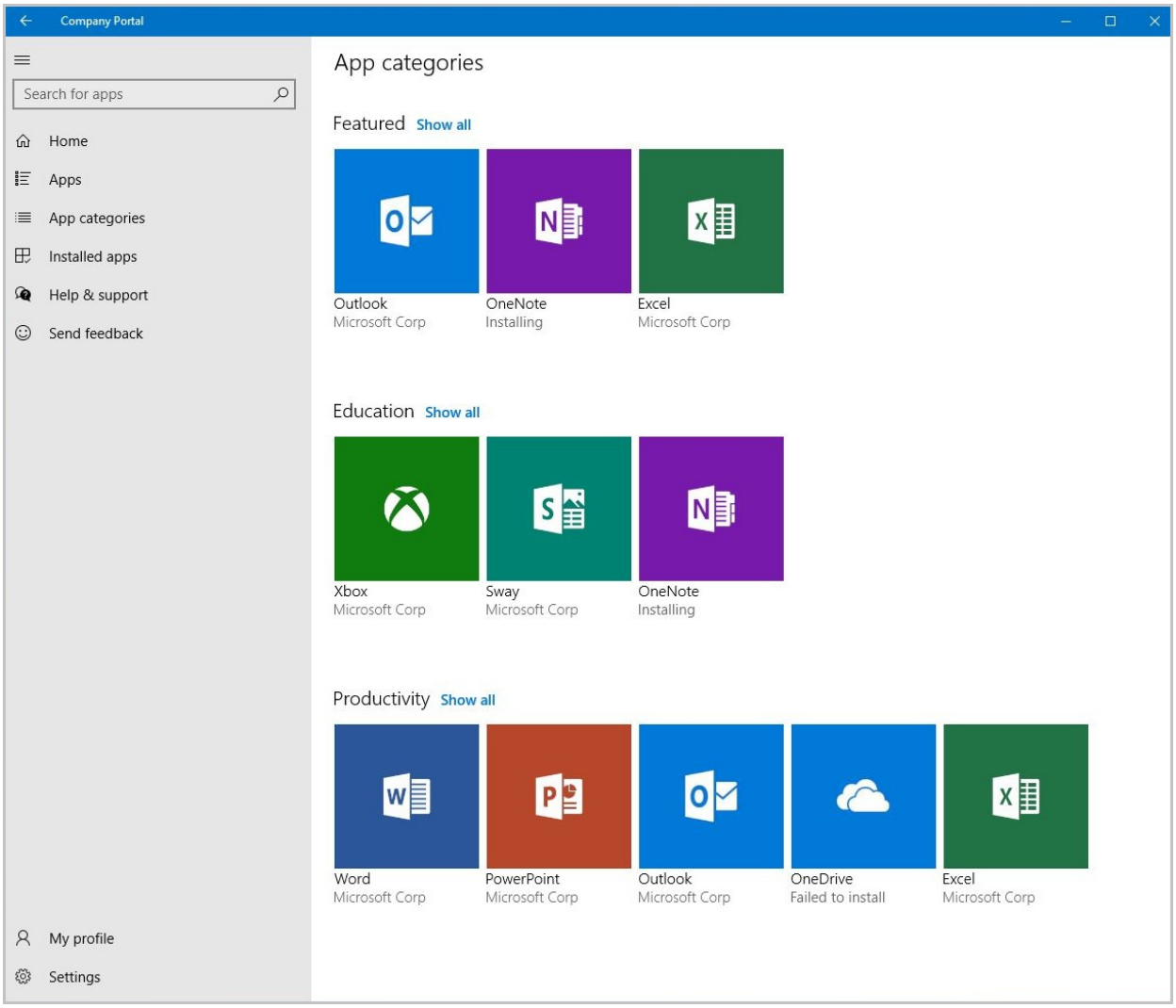
Se ha rediseñado la página principal de la aplicación Portal de empresa para dispositivos iOS. Con este cambio, la página principal seguirá mejor los patrones de la interfaz de usuario de iOS y ofrecerá una mejor detectabilidad para aplicaciones y libros electrónicos.

Semana del 19 de febrero de 2019

Nueva pantalla de categorías de aplicaciones en la aplicación Portal de empresa para Windows 10

Se ha agregado una nueva pantalla denominada **Categorías de aplicaciones** para mejorar la experiencia de

exploración y selección en la aplicación Portal de empresa para Windows 10. Los usuarios ahora verán sus aplicaciones ordenadas en categorías como **Destacadas**, **Educación** y **Productividad**. Este cambio aparece en las versiones 10.3.3451.0 y posteriores del Portal de empresa. Para obtener más información sobre cómo instalar aplicaciones en el Portal de empresa, vea Instalar y compartir aplicaciones en el dispositivo.



Semana del 12 de noviembre de 2018

Métodos abreviados de teclado del Portal de empresa de Windows

Ahora, los usuarios finales podrán desencadenar acciones de aplicación y dispositivo en el Portal de empresa de Windows mediante métodos abreviados de teclado (aceleradores).

Semana del 22 de octubre de 2018

Adición de una imagen de marca personalizada para la aplicación Portal de empresa

Como administrador de Microsoft Intune, puede cargar una imagen de marca personalizada que se mostrará como imagen de fondo en la página de perfil del usuario en la aplicación Portal de empresa de iOS. Para obtener más información sobre cómo configurar la aplicación Portal de empresa, vea How to configure the Microsoft Intune Company Portal app (Cómo configurar la aplicación Portal de empresa de Microsoft Intune).

Semana del 27 de agosto de 2018

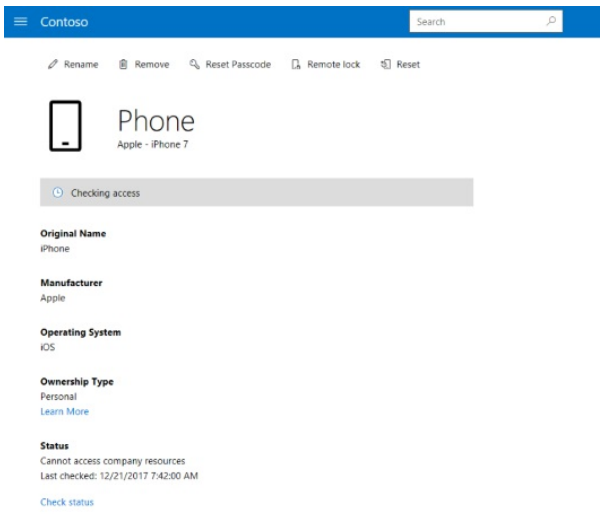
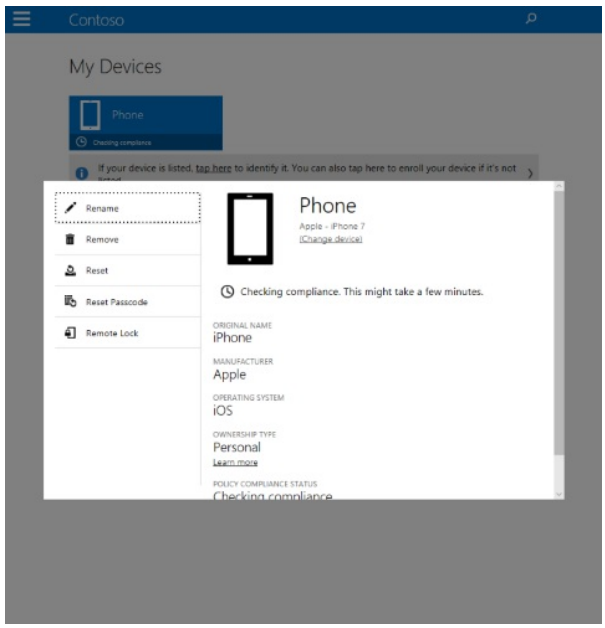
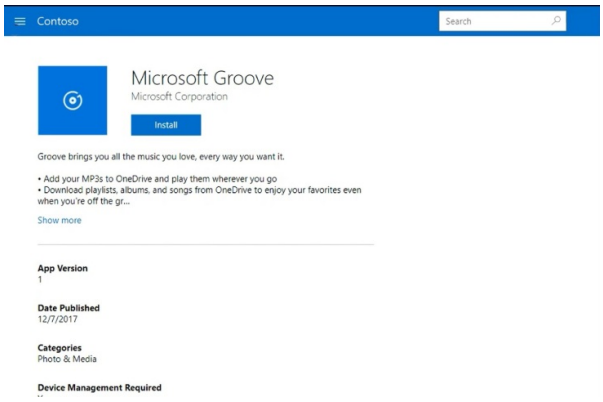
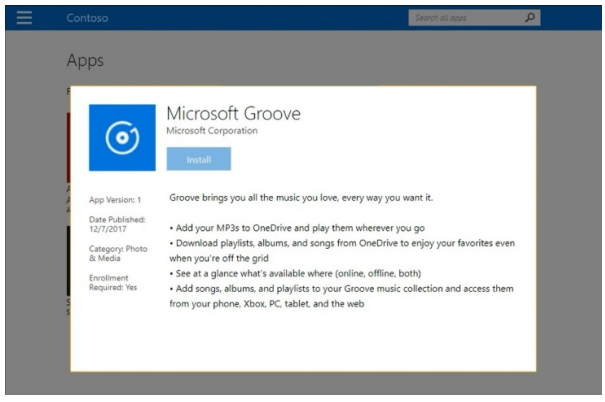
Nueva actualización de la experiencia de usuario para el sitio web del Portal de empresa

Tras escuchar los comentarios de los clientes, hemos agregado características nuevas al sitio web de Portal de empresa. Experimentará una mejora considerable en las funciones y la facilidad de uso actual de los

dispositivos. Determinadas áreas del sitio, como los detalles del dispositivo, los comentarios, el soporte técnico y la descripción general del dispositivo, tienen ahora un diseño nuevo, moderno y receptivo. Se ha actualizado la documentación del sitio web de Portal de empresa de Intune para reflejar estos cambios.

Las actualizaciones que verá incluyen las siguientes:

- Flujos de trabajo optimizados en todas las plataformas de dispositivo
- Flujos mejorados para la inscripción e identificación de dispositivos
- Mensajes de error más útiles
- Lenguaje más descriptivo y menos terminología técnica
- Capacidad de compartir vínculos directos a aplicaciones
- Rendimiento mejorado de los catálogos de aplicaciones de gran tamaño
- Aumento de accesibilidad para todos los usuarios

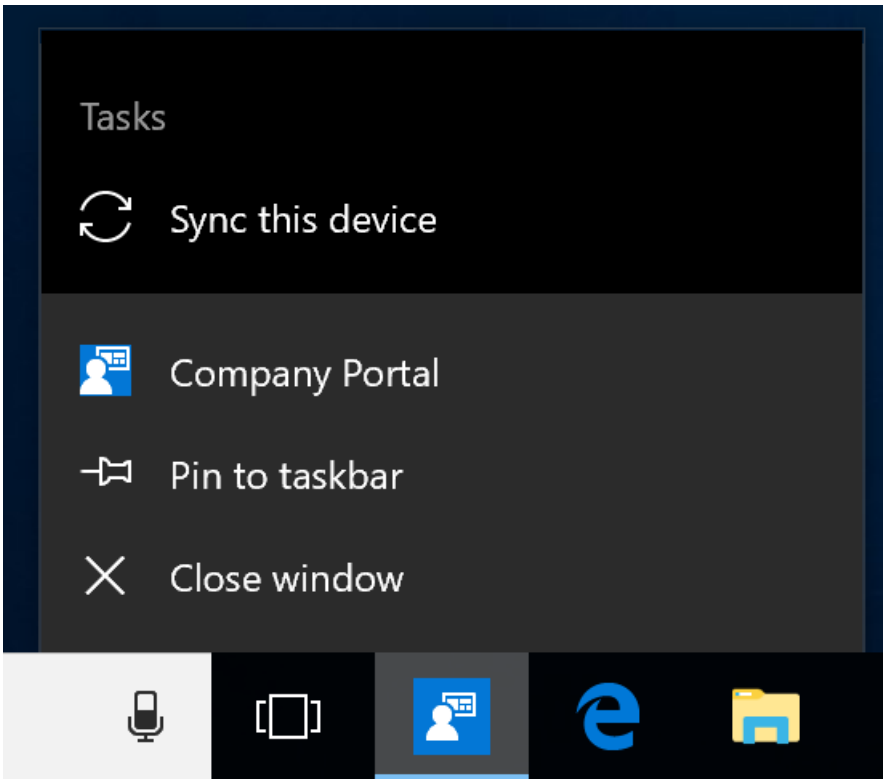
ACTUALIZADO	ANTERIOR
	
	

Semana del 16 de julio de 2018

Más oportunidades de sincronización en la aplicación Portal de empresa para Windows

La aplicación Portal de empresa para Windows ahora permite iniciar una sincronización directamente desde la barra de tareas de Windows y el menú Inicio. Esta característica es especialmente útil si la única tarea es sincronizar dispositivos y obtener acceso a recursos corporativos. Para acceder a la nueva característica, haga clic con el botón derecho en el icono de Portal de empresa que está anclado en la barra de tareas o el menú **Inicio**. En las opciones de menú (también denominada lista de accesos directos), seleccione **Sincronizar este**

dispositivo. El Portal de empresa se abrirá en la página **Configuración** e iniciará la sincronización.

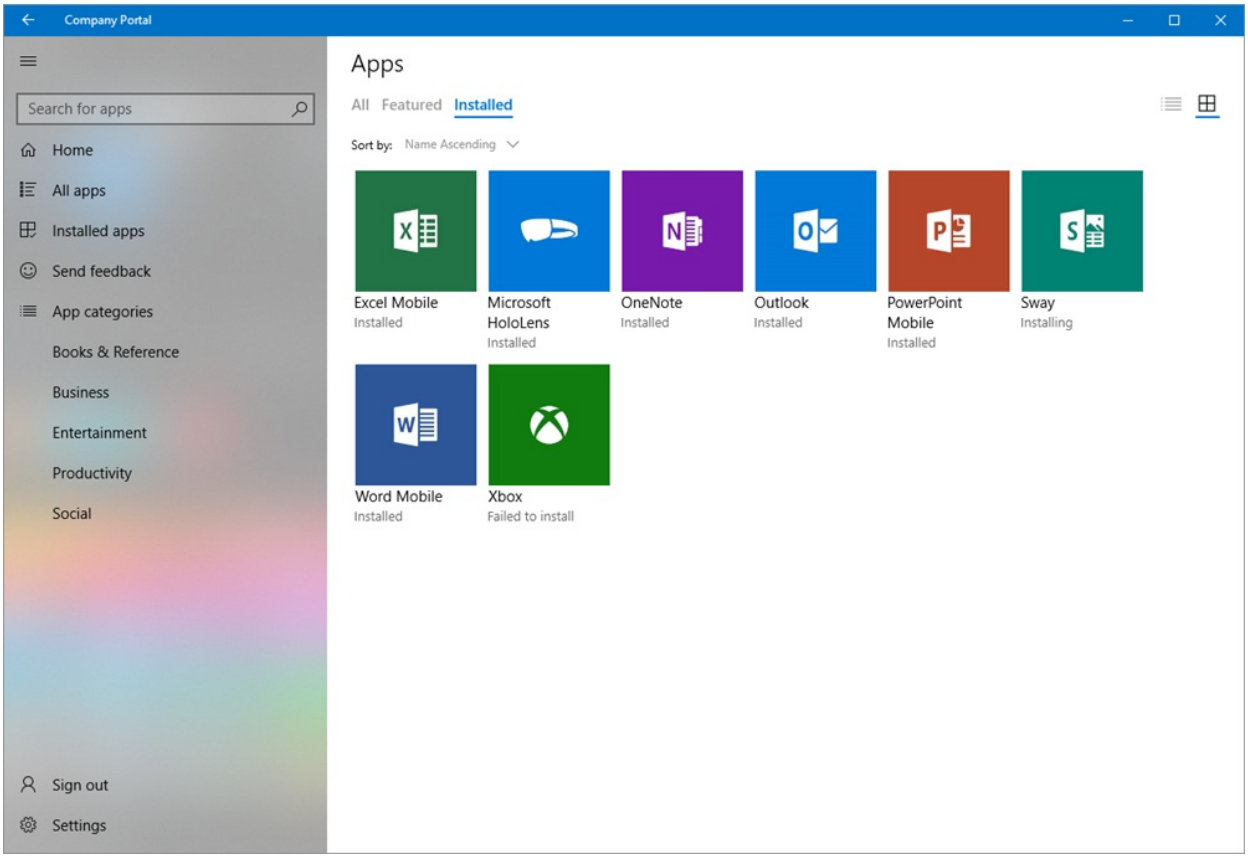


Nuevas experiencias de exploración en la aplicación de Portal de empresa para Windows

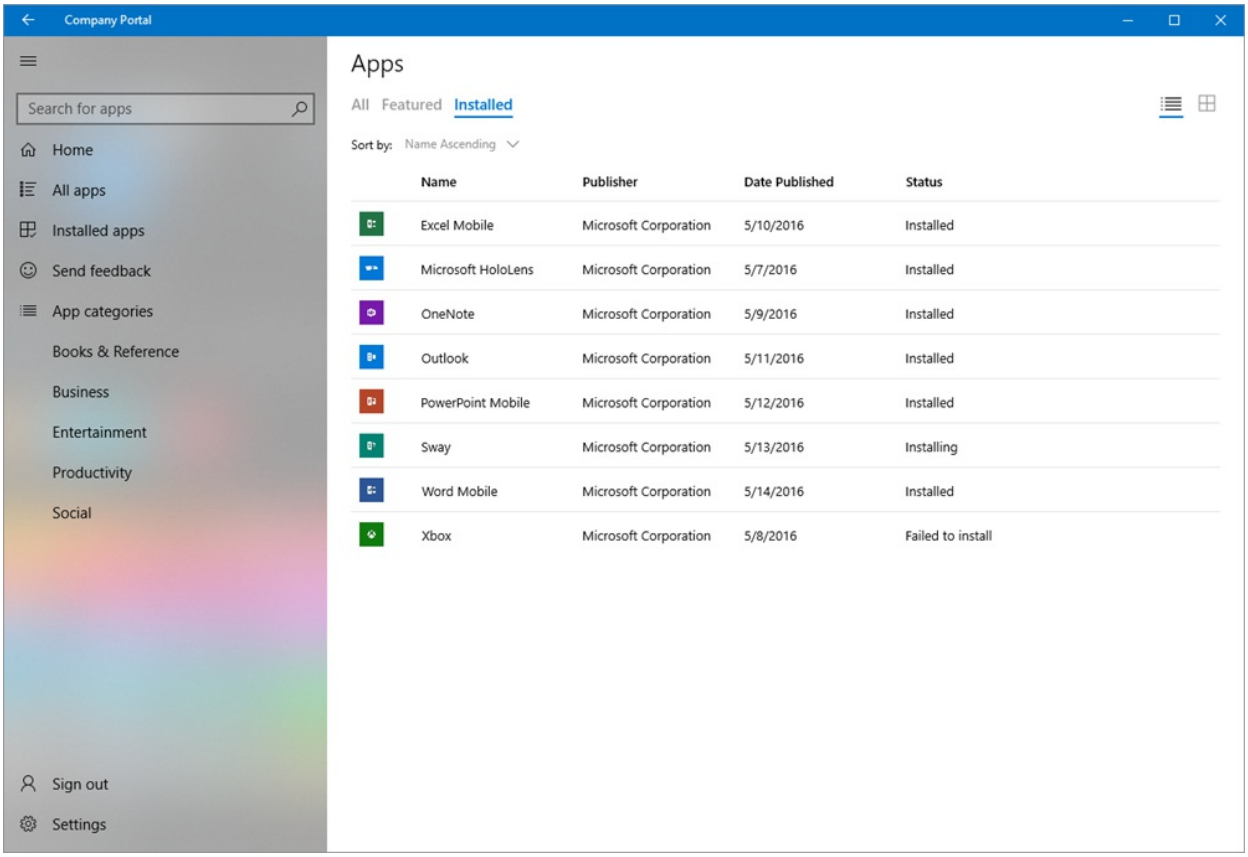
Ahora, al examinar o buscar aplicaciones en la aplicación Portal de empresa para Windows, puede alternar entre la vista **Iconos** existente y la nueva vista **Detalles**. En esta nueva vista se muestran detalles de la aplicación, como el nombre, el editor, la fecha de publicación y el estado de la instalación.

La vista **Instaladas** de la página **Aplicaciones** le permite ver detalles sobre las instalaciones de aplicaciones completadas y en curso.

Captura de pantalla de ejemplo en la que se muestra la vista de mosaico:



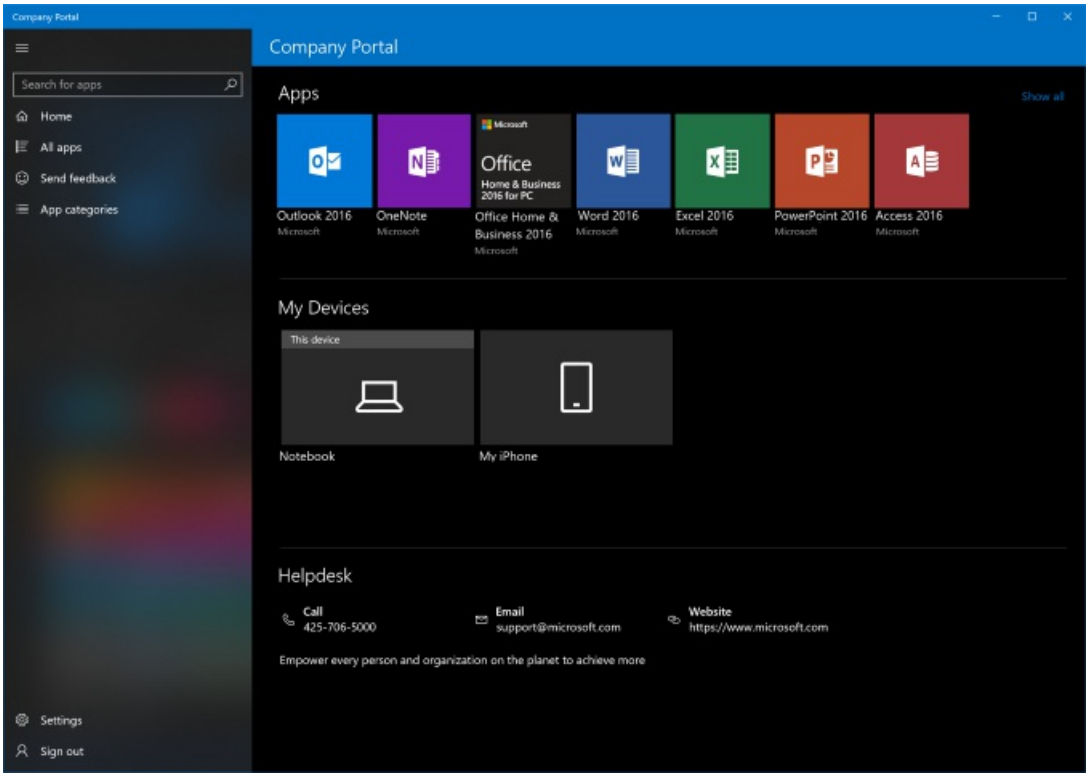
Captura de pantalla de ejemplo en la que se muestra la vista Detalles:



Semana del 23 de abril de 2018

Vista de navegación actualizada en la aplicación Portal de empresa para Windows 10

La aplicación Portal de empresa de Intune para Windows 10 se ha actualizado con la vista de navegación de Fluent Design System. En la parte lateral de la aplicación, verá una lista estática vertical de todas las páginas de nivel superior. Haga clic en cualquier vínculo para ver y cambiar entre páginas rápidamente. Esta es la primera de varias actualizaciones que verá como parte de nuestros esfuerzos para crear una experiencia más adaptable, empática y familiar en Intune.



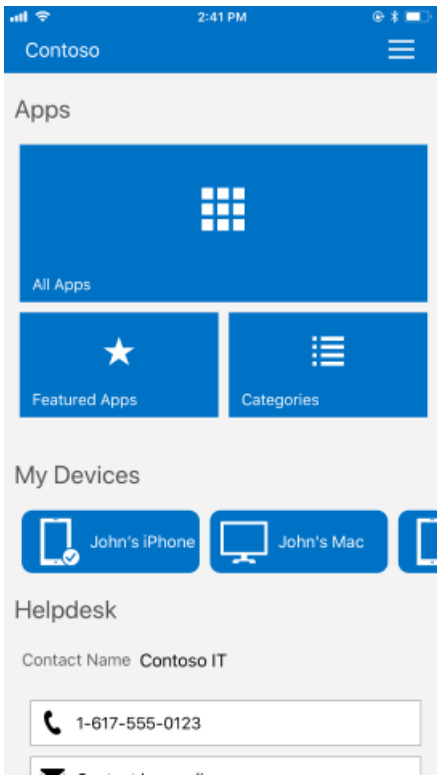
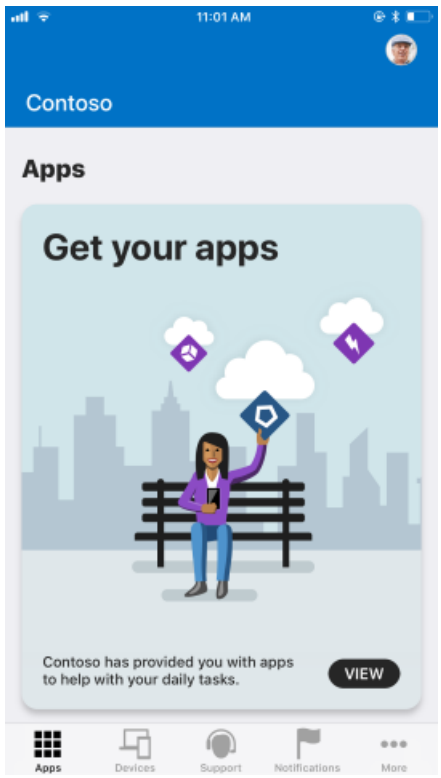
Semana del 2 de abril de 2018

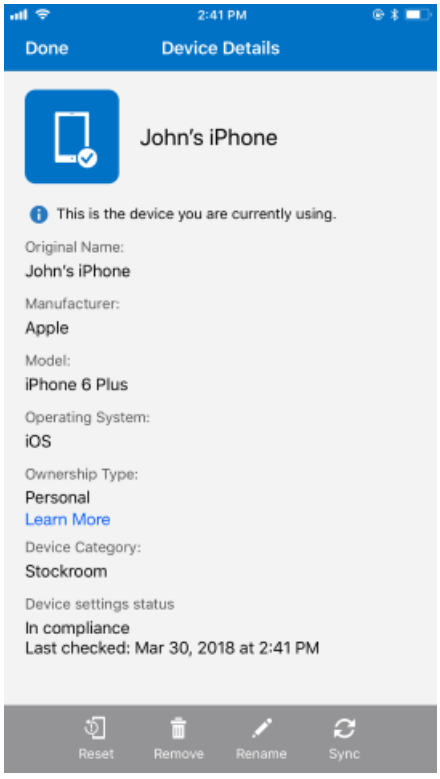
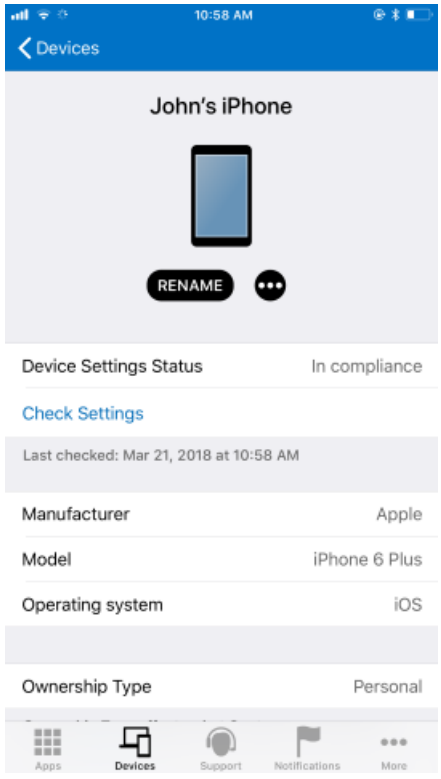
Actualización de la experiencia de usuario para la aplicación Portal de empresa para iOS

Se ha publicado una importante actualización de la experiencia de usuario para la aplicación Portal de empresa para iOS/iPadOS. La actualización incluye un completo cambio de diseño visual con una apariencia modernizada. Hemos mantenido la funcionalidad de la aplicación, pero hemos mejorado su facilidad de uso y accesibilidad.

También verá:

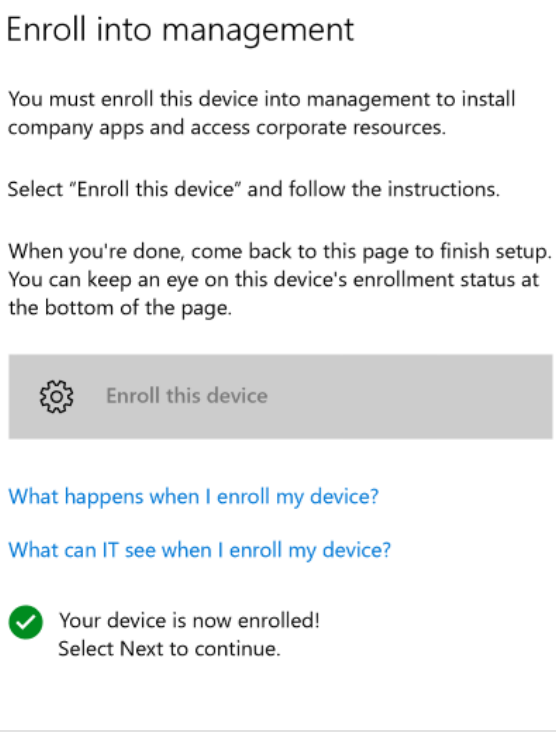
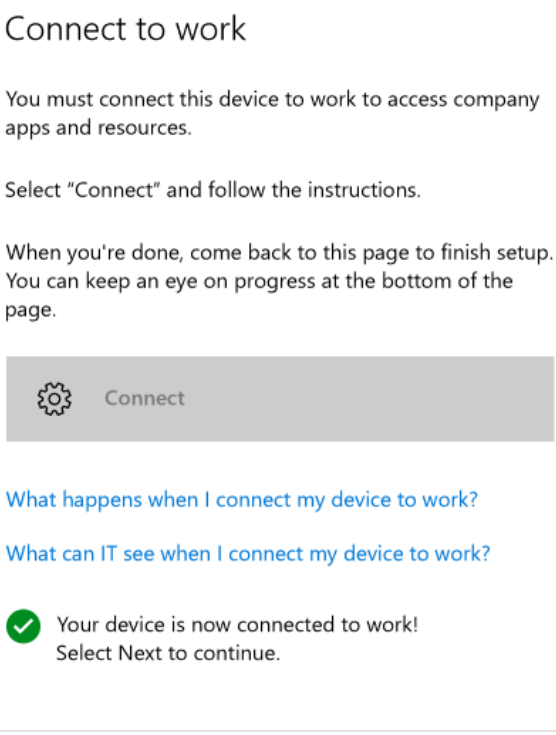
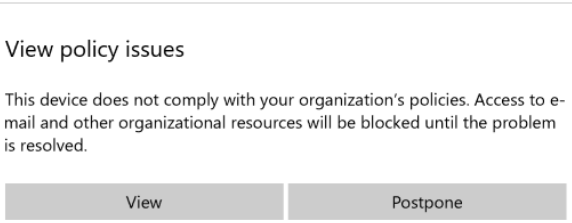
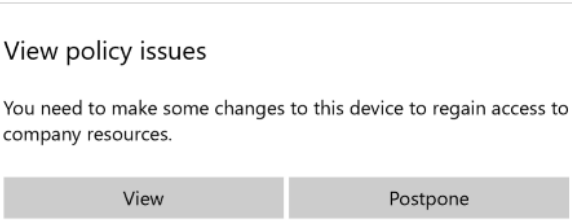
- Compatibilidad con el iPhone X.
- Inicio de la aplicación y carga de las respuestas más rápidos, para ahorrar tiempo a los usuarios.
- Barras de progreso adicionales para proporcionar a los usuarios la información de estado más reciente.
- Mejoras en la forma en que los usuarios cargan los registros, de modo que, si hay algún problema, sea más fácil de informar al respecto.

ANTES	DESPUÉS
	

ANTES	DESPUÉS
Combinado con el paso anterior	
	

Mejoras en el lenguaje de la aplicación Portal de empresa para Windows

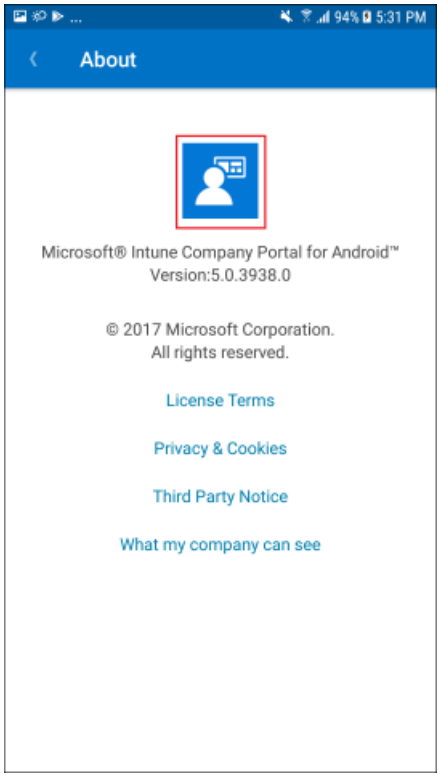
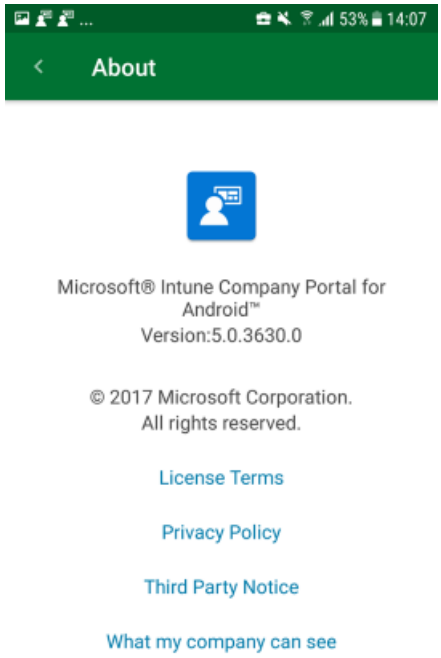
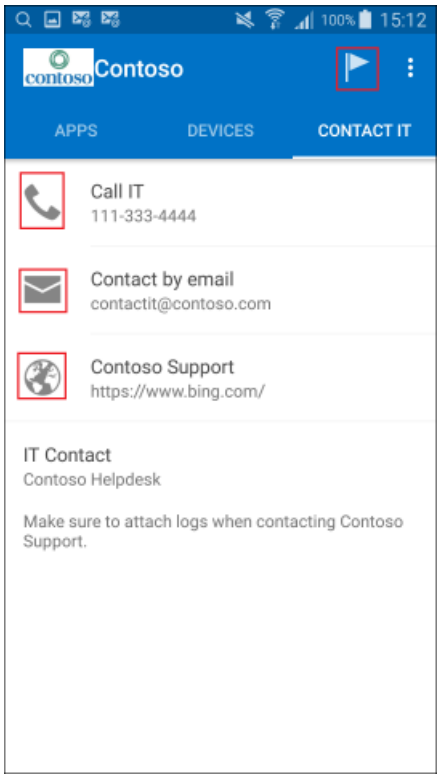
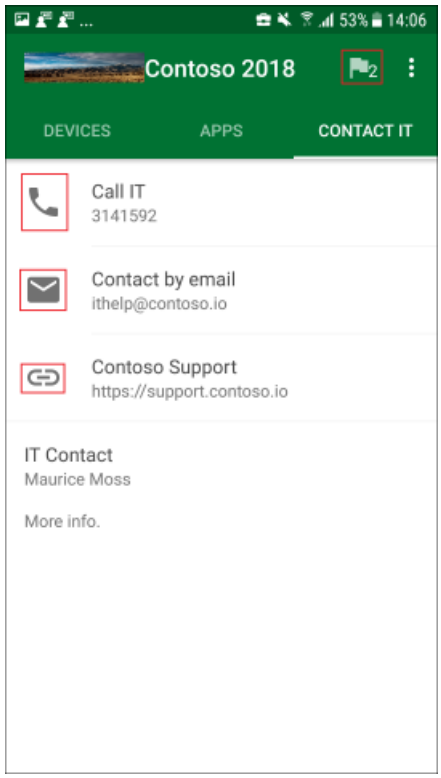
Se ha mejorado el lenguaje del Portal de empresa para Windows 10 para que sea más fácil de usar y más específico para la empresa.

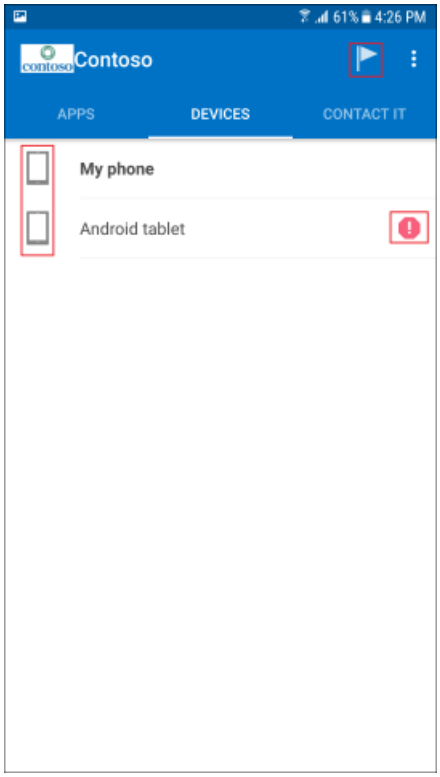
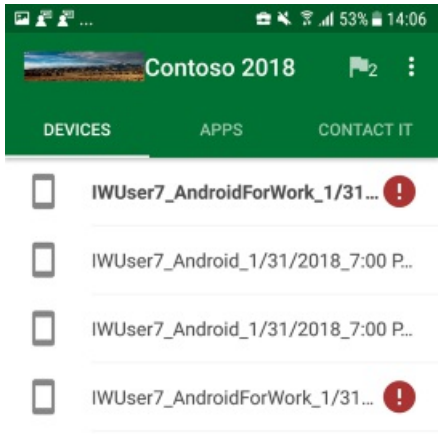
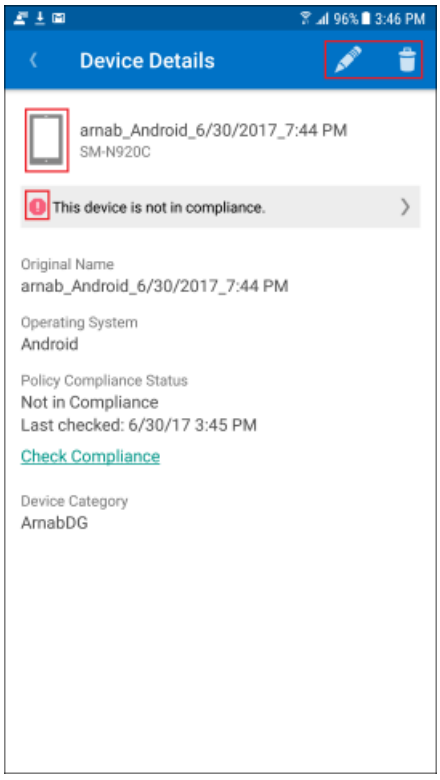
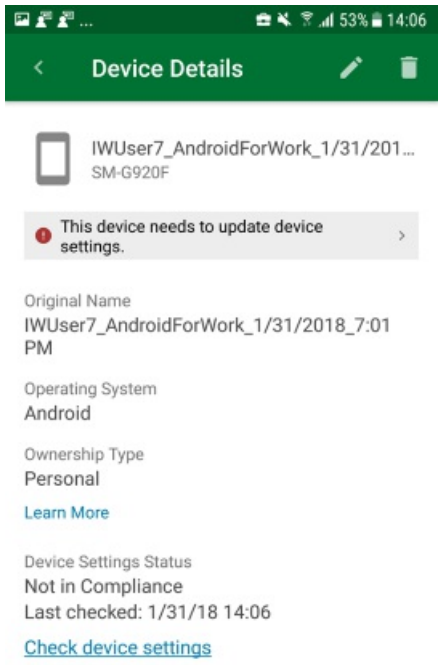
ANTES	DESPUÉS
	
	

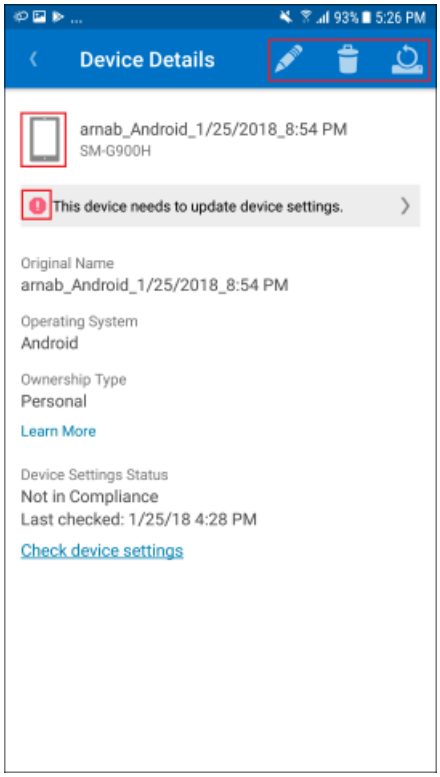
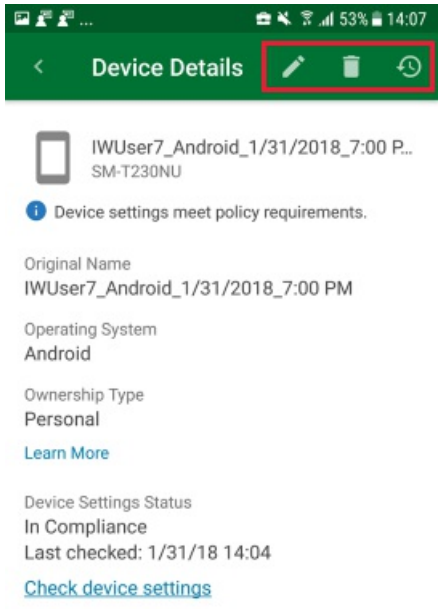
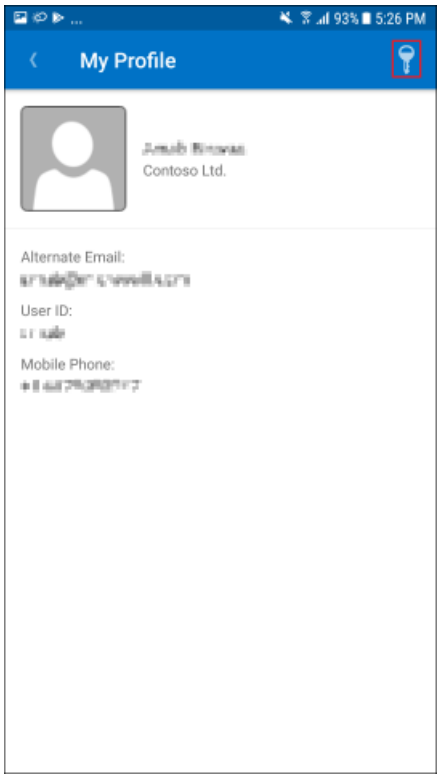
Semana del 12 de marzo de 2018

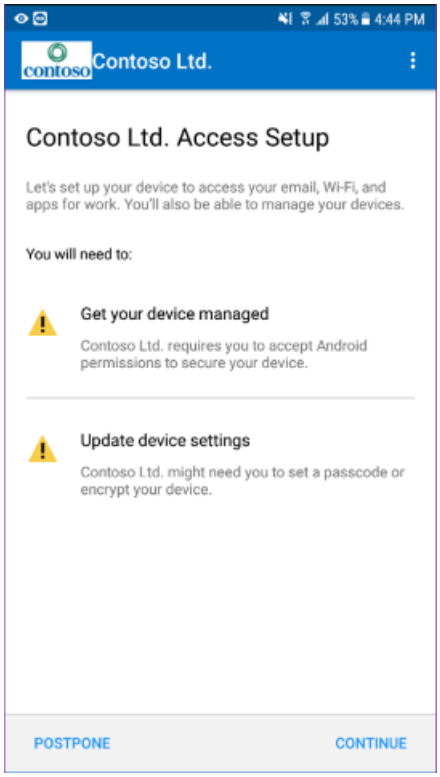
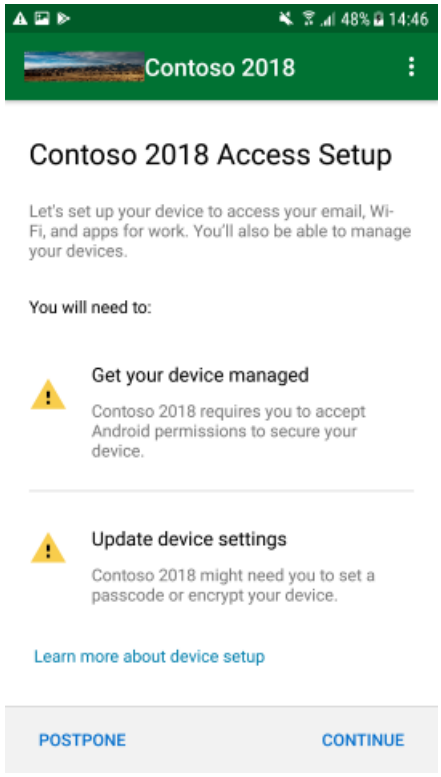
Actualizaciones visuales de Portal de empresa para Android

Hemos actualizado la aplicación Portal de empresa para Android para seguir las directrices de Material Design de Android.

ANTES	DESPUÉS
	
	

ANTES	DESPUÉS
	
	

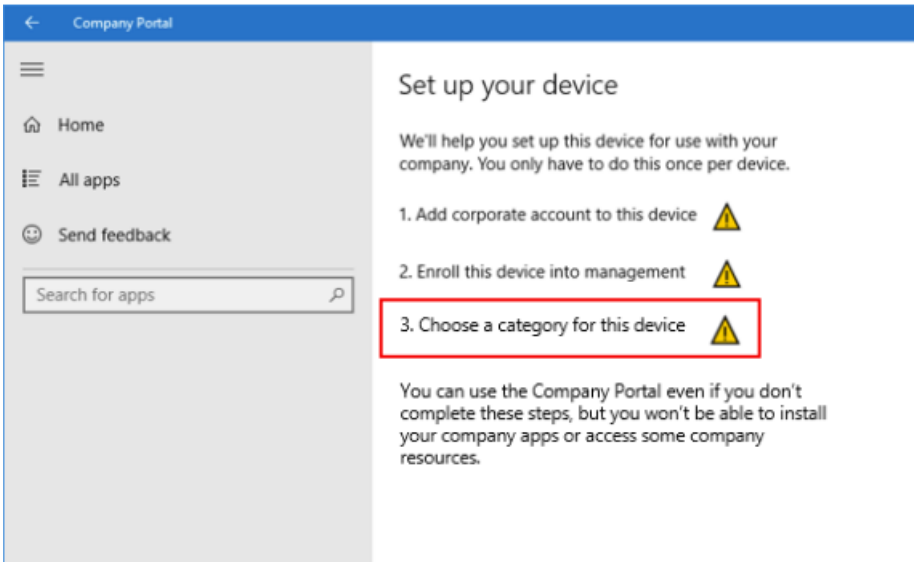
ANTES	DESPUÉS
	
	

ANTES	DESPUÉS
	

Semana del 27 de noviembre de 2017

Nuevo paso "Categorías de dispositivos" en la configuración guiada de la aplicación Portal de empresa para Windows 10

Si ha habilitado la asignación de grupos de dispositivos, la aplicación Portal de empresa para Windows 10 ahora guía a los usuarios a través de la selección de una categoría de dispositivo después de inscribir el dispositivo.



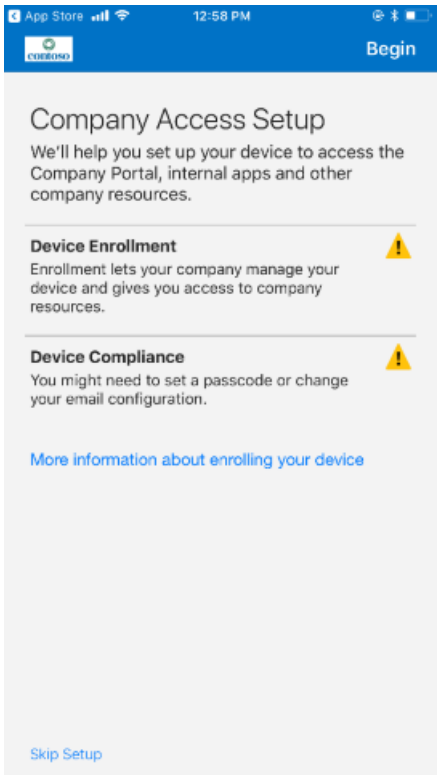
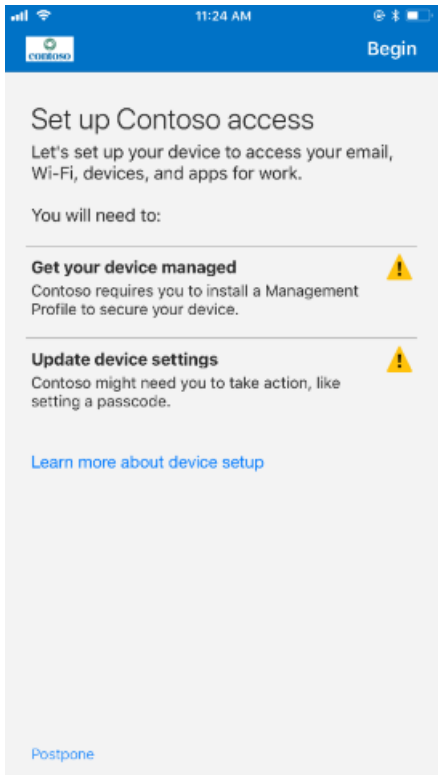
Semana del 13 de noviembre de 2017

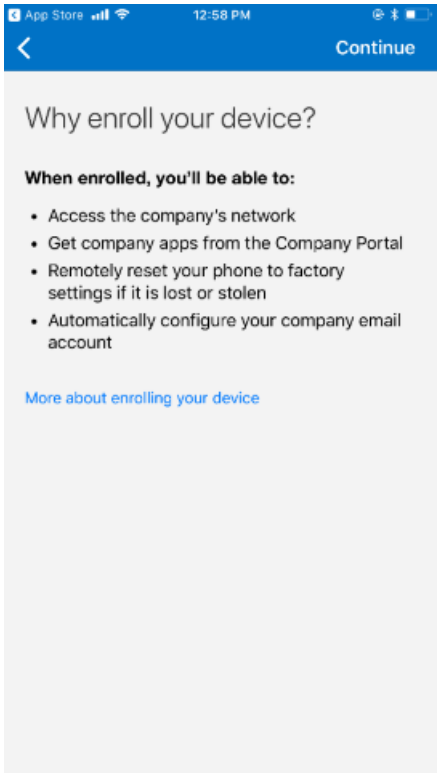
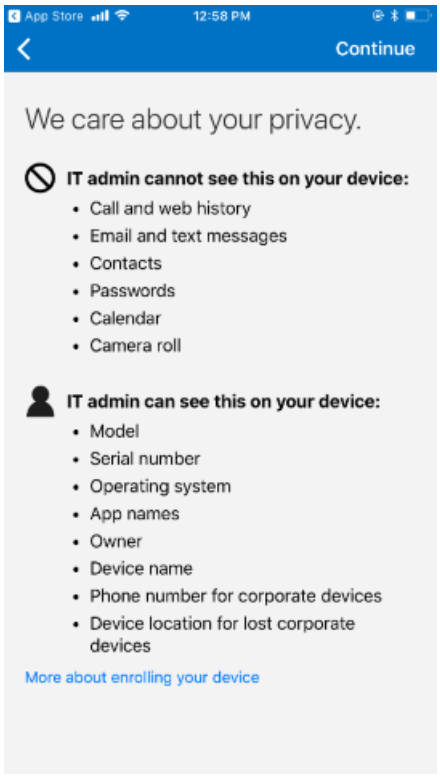
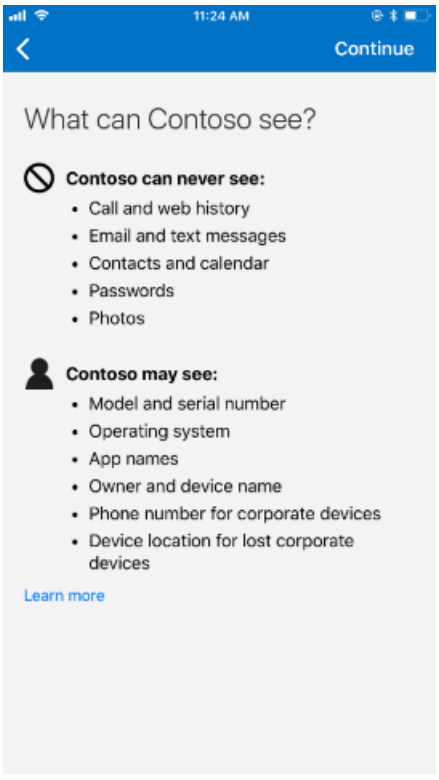
Mejoras en el flujo de trabajo de configuración de dispositivos en la versión 2.9.0 de Portal de empresa para iOS

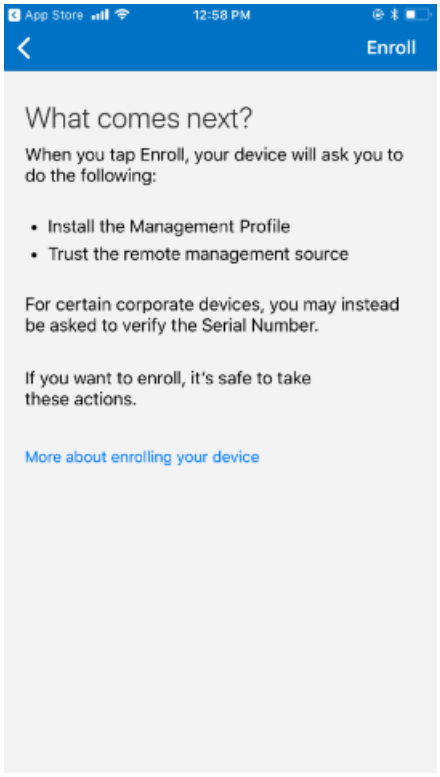
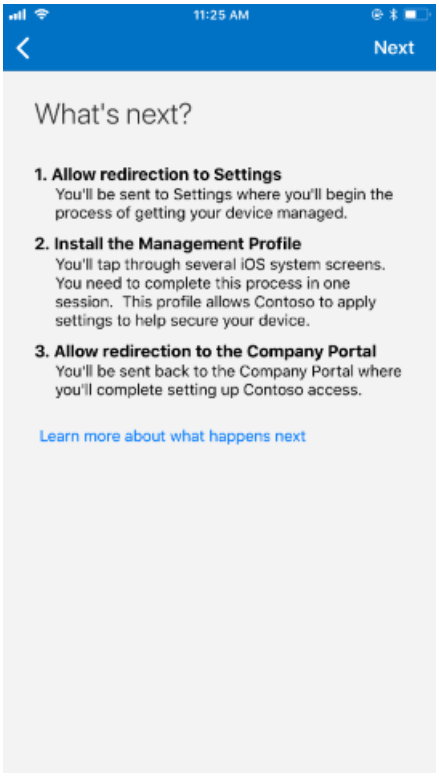
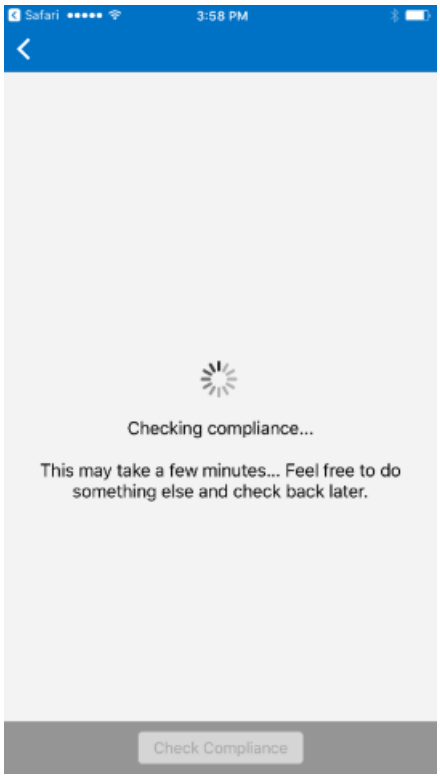
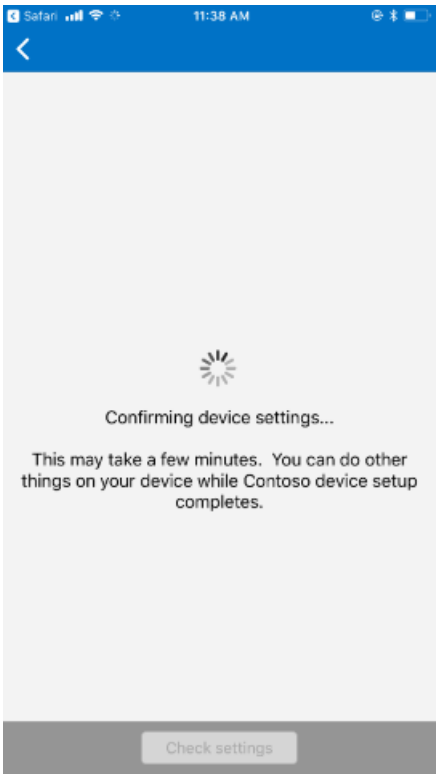
Se ha mejorado el flujo de trabajo de instalación de dispositivos en la aplicación Portal de empresa para iOS/iPadOS. El lenguaje resulta más fácil de usar y se han combinado pantallas donde era posible. El lenguaje también se ha hecho más específico para la empresa mediante el uso del nombre de la empresa en el texto de

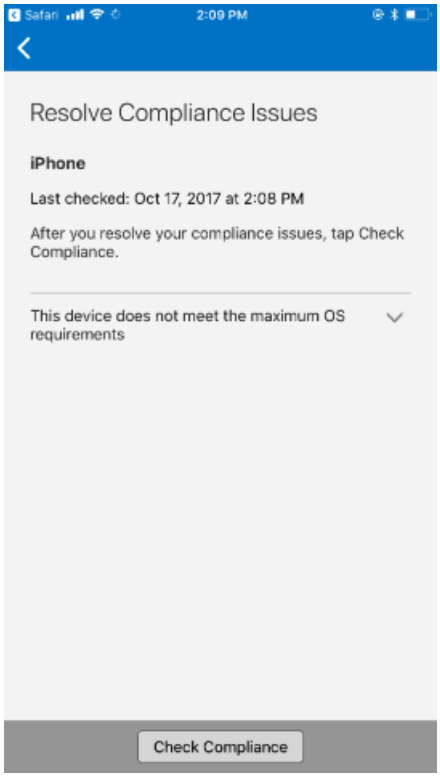
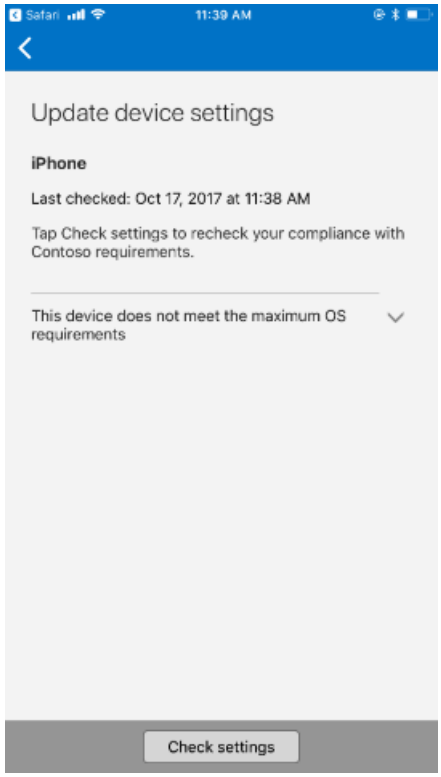
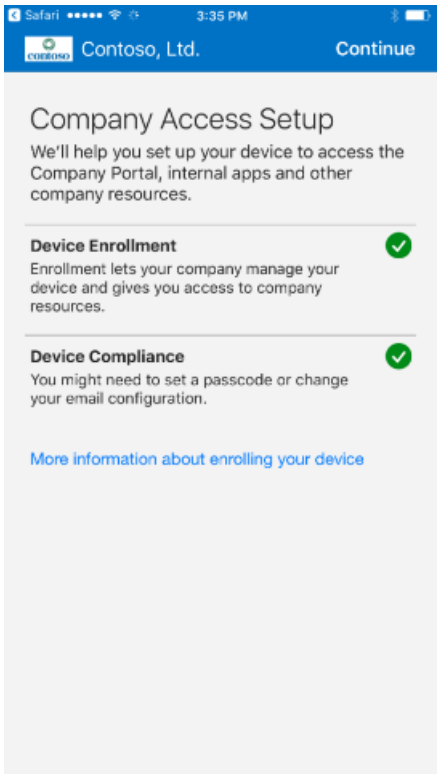
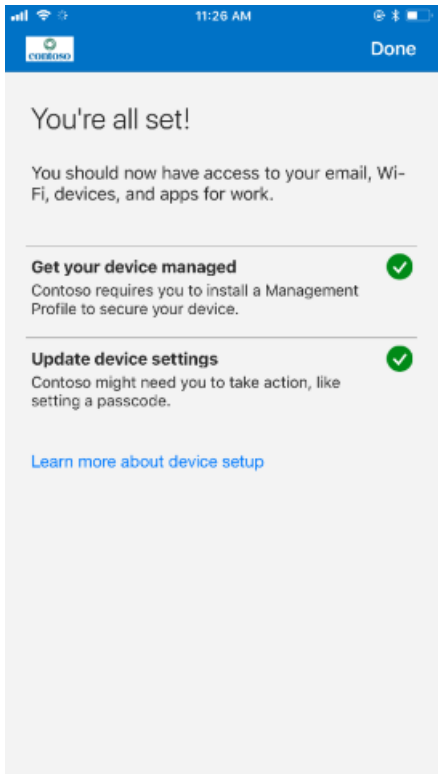
instalación.

> **NOTE**
>
> Se usa el nombre de empresa que ha establecido en Azure Portal, en **Microsoft Intune** > **Aplicaciones cliente** > **Personalización de marca del Portal de empresa** > **Nombre de la empresa**. Si no ha definido este valor, se usará el nombre del inquilino establecido en **Azure Active Directory** > **Propiedades** > **Nombre**. Si no ha establecido ningún nombre de empresa en Personalización de marca de Portal de empresa y no quiere que se muestre el del inquilino, se recomienda definir el nombre de la empresa en dicha pestaña. Si no quiere que esta cadena aparezca en el encabezado de Portal de empresa, puede anular la selección de la casilla "Mostrar nombre de la empresa junto al logotipo".

ANTES	DESPUÉS
	

ANTES	DESPUÉS
	*Combinado con el paso anterior*
	

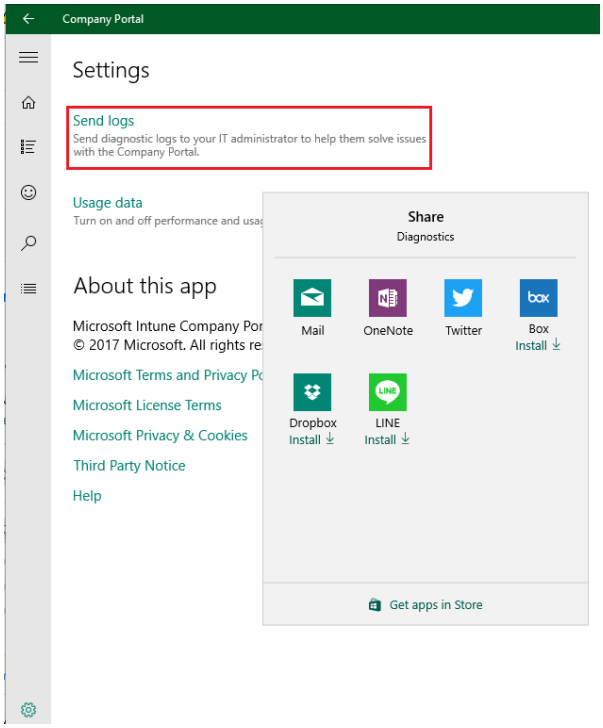
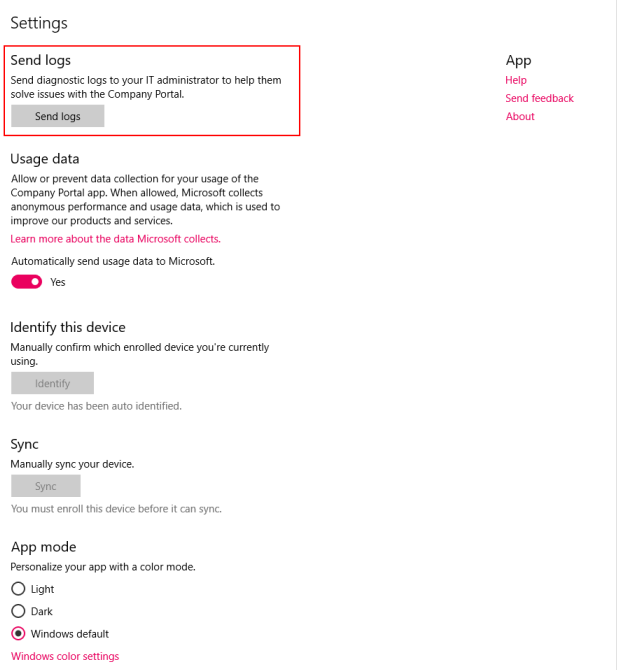
ANTES	DESPUÉS
	
	

ANTES	DESPUÉS
	
	

Semana del 6 de noviembre de 2017

Actualizaciones de la aplicación Portal de empresa para Windows 10

La página Configuración de la aplicación de Portal de empresa para Windows 10 se ha actualizado para que las opciones y las acciones de usuario previstas sean más coherentes en relación con el resto de opciones de configuración. También se ha actualizado para que el diseño coincida con el de otras aplicaciones de Windows.

ANTES	DESPUÉS
	

Mejoras de búsqueda en el sitio web y las aplicaciones del Portal de empresa

Ahora, las aplicaciones del Portal de empresa realizan búsquedas en categorías de aplicaciones, nombres y descripciones. Los resultados se ordenan en orden decreciente de relevancia. Estas actualizaciones también están disponibles en el sitio web del Portal de empresa.

Seguimos ajustando el modo de seguimiento de la relevancia, por lo que le agradeceríamos que nos hiciera saber si resulta útil mediante el vínculo "Comentarios" situado en la parte inferior del sitio web del Portal de empresa.

Semana del 16 de octubre de 2017

Mejoras de búsqueda en el sitio web del Portal de empresa

Estamos mejorando nuestras capacidades de búsqueda de aplicaciones, empezando por el sitio web del Portal de empresa. Las búsquedas ahora se efectuarán en categorías de aplicaciones, además de en los campos Nombre y Descripción. Los resultados se ordenarán, de forma predeterminada, en orden decreciente de relevancia.

Los usuarios de dispositivos iOS también recibirán este cambio, ya que el sitio web del Portal de empresa también se usa como parte de la aplicación del Portal de empresa para iOS/iPadOS. Las aplicaciones del Portal de empresa para Android y Windows recibirán actualizaciones similares en los próximos meses.

Seguimos ajustando el modo de seguimiento de la relevancia, por lo que le agradeceríamos que nos hiciera saber si resulta útil mediante el vínculo "Comentarios" situado en la parte inferior del sitio web del Portal de empresa.

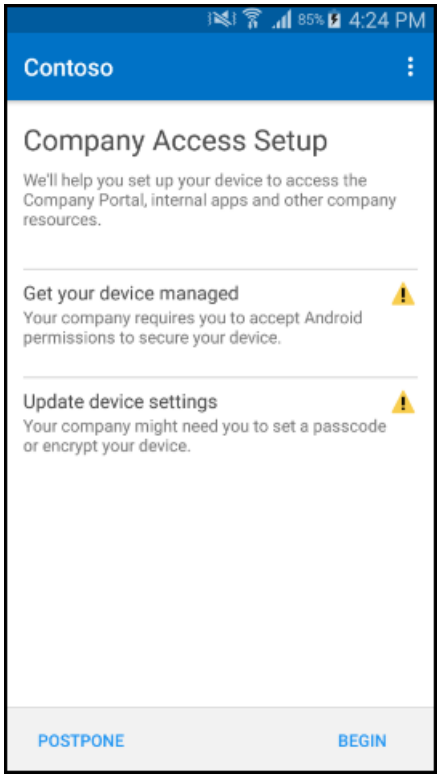
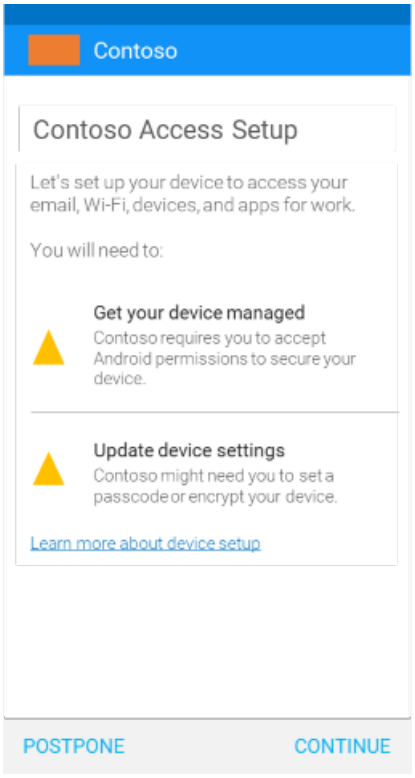
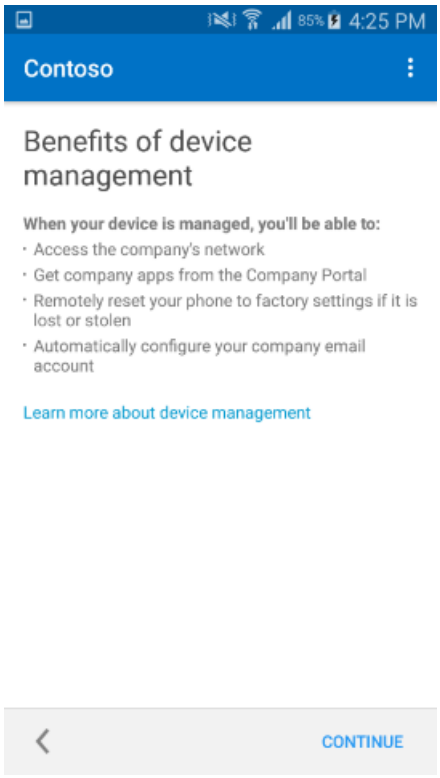
En el Portal de empresa de iOS se muestran iconos de gran tamaño

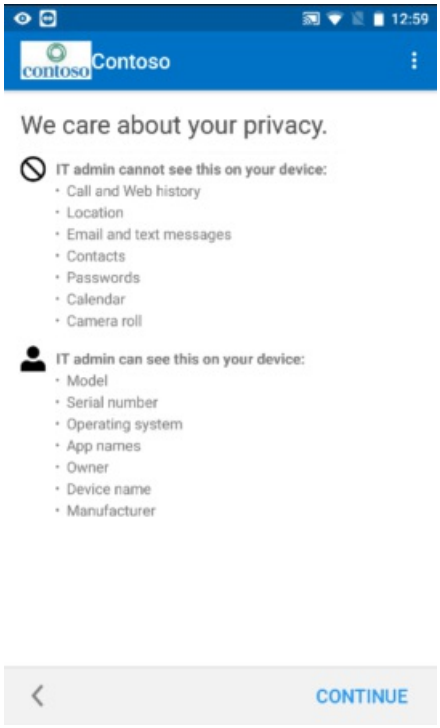
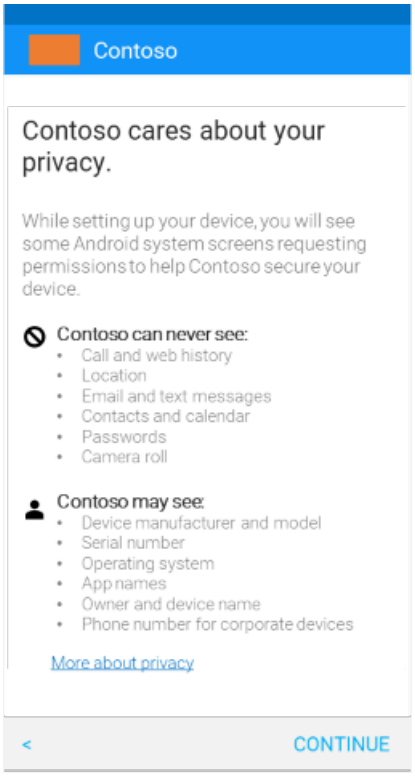
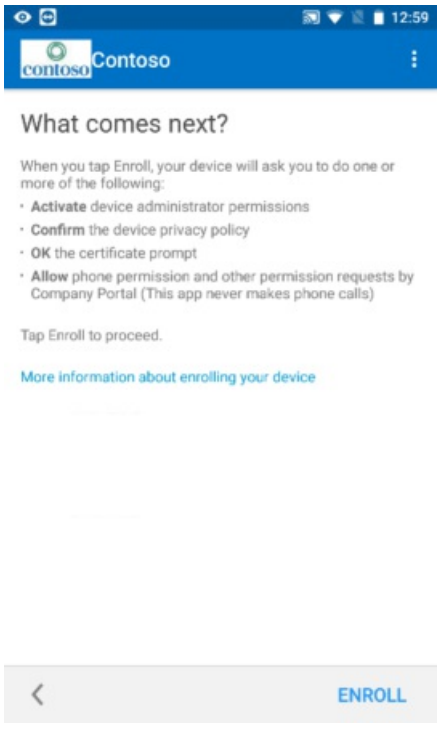
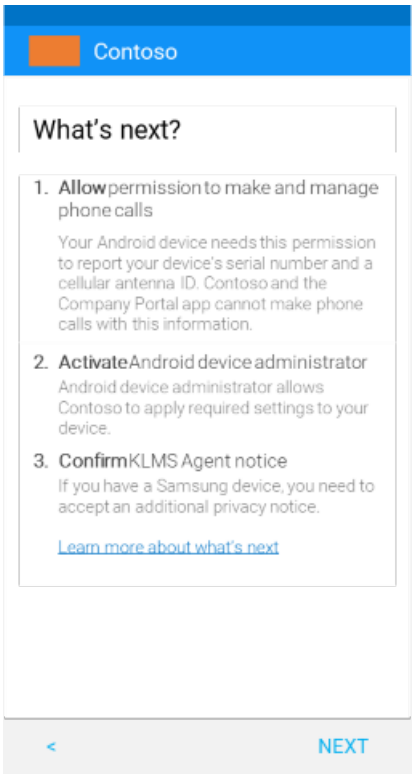
Con esta versión se soluciona un problema conocido en relación con el modo en que el portal de empresa de iOS muestra los iconos en el icono de la aplicación. Si carga iconos de aplicación de 120x120 píxeles o más, ahora se muestran en el sitio web del portal de empresa y las páginas de aplicaciones del Portal de empresa de iOS al tamaño completo del icono de aplicaciones.

Semana del 2 de octubre de 2017

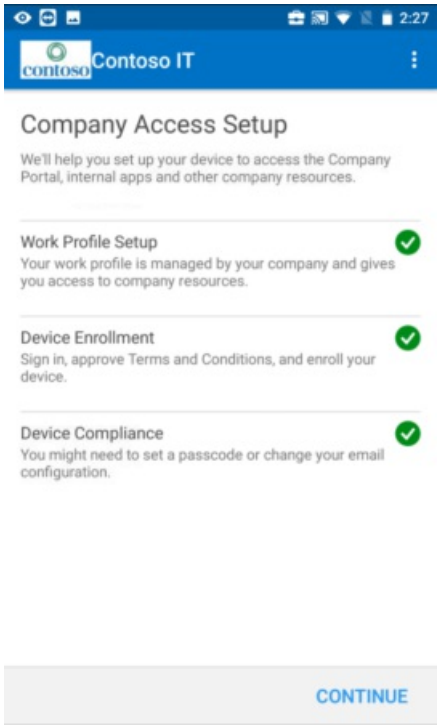
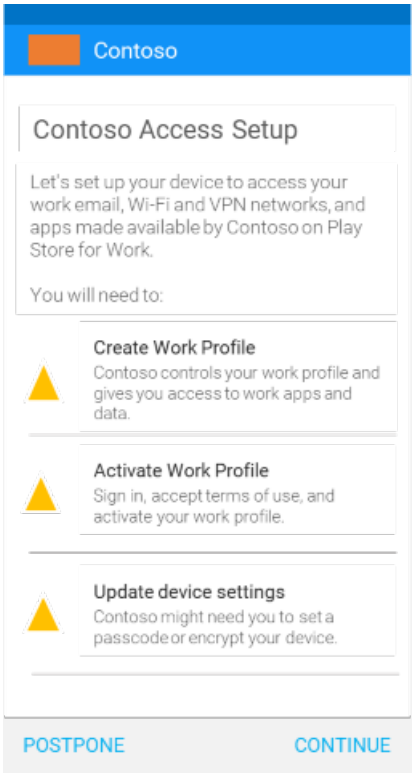
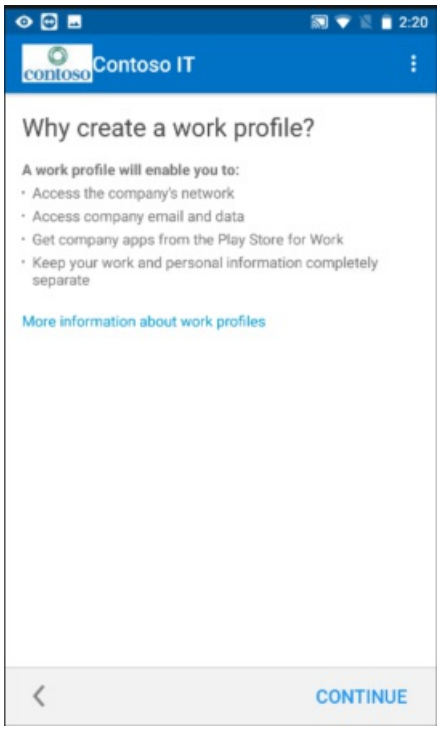
Mejoras en el flujo de trabajo de configuración de dispositivos en el Portal de empresa

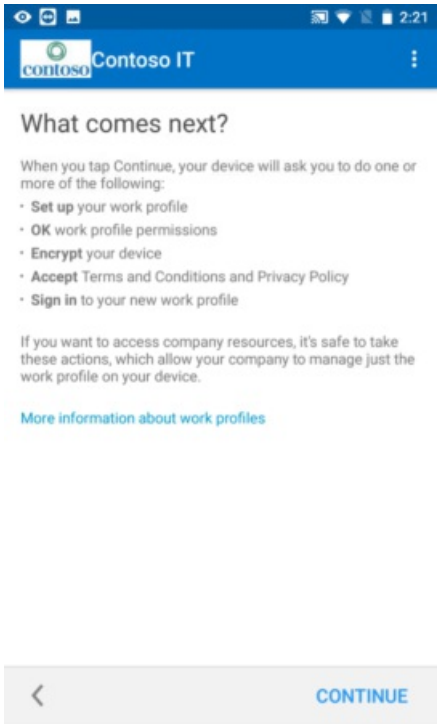
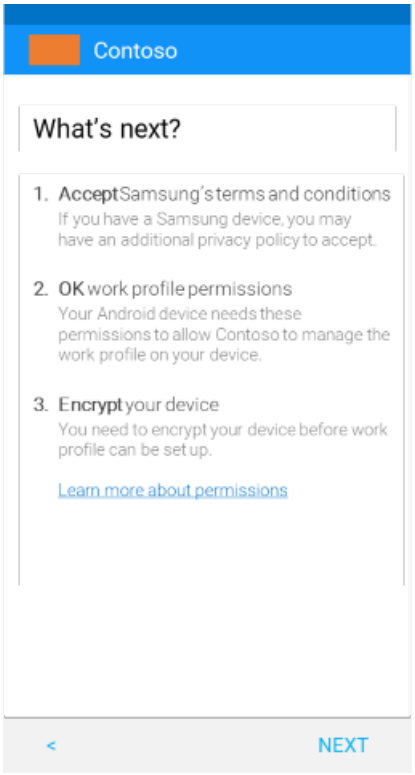
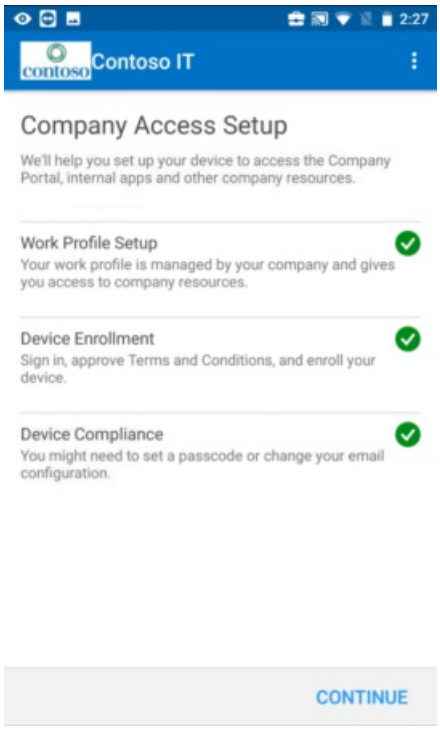
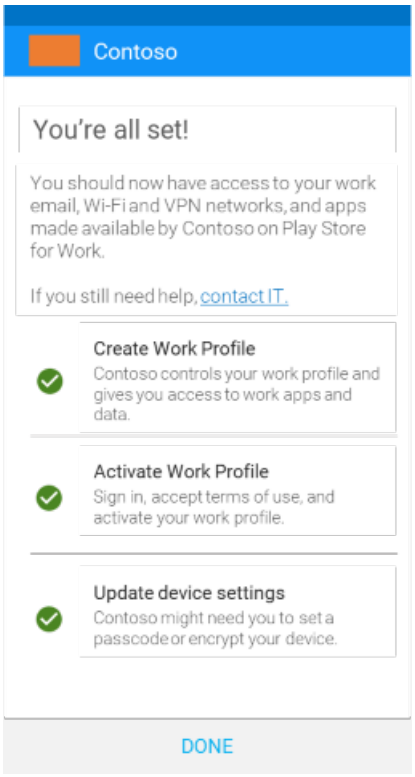
Se ha mejorado el flujo de trabajo de instalación de dispositivos en la aplicación del Portal de empresa para Android. El lenguaje resulta más fácil de usar y es específico de su empresa. Además, hemos combinado pantallas donde era posible.

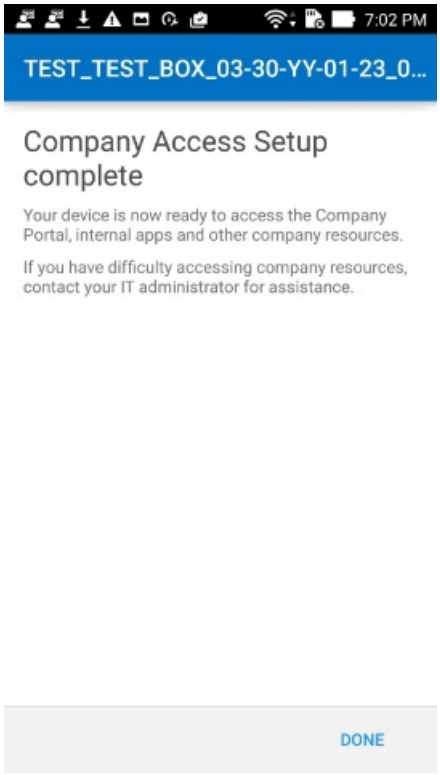
ANTES	DESPUÉS
	
	*Combinado con el paso anterior*

ANTES	DESPUÉS
	
	

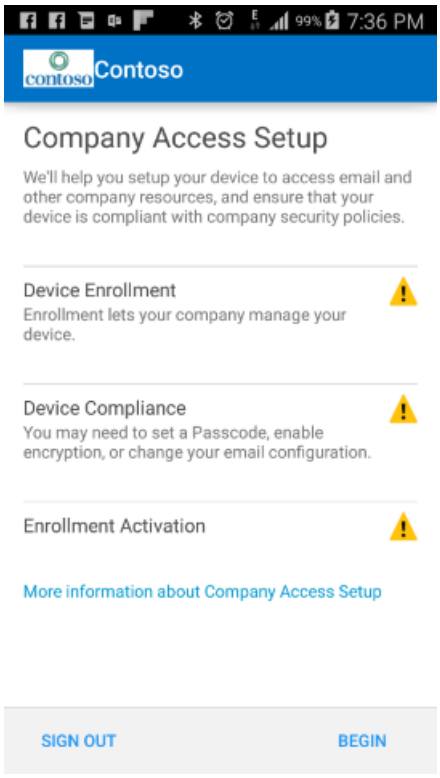
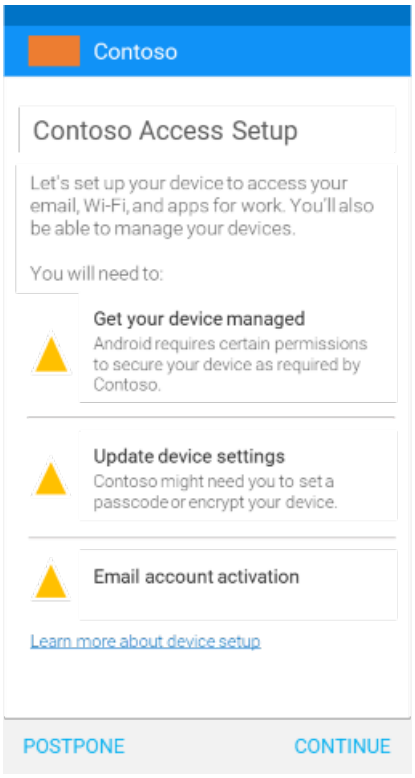
Se han mejorado los pasos adicionales en los dispositivos de perfil de trabajo Android.

ANTES	DESPUÉS
	
	*Combinado con el paso anterior*

ANTES	DESPUÉS
	
	

ANTES	DESPUÉS
	*Combinado con el paso anterior*

También hemos actualizado la pantalla de activación de correo electrónico de acceso condicional.

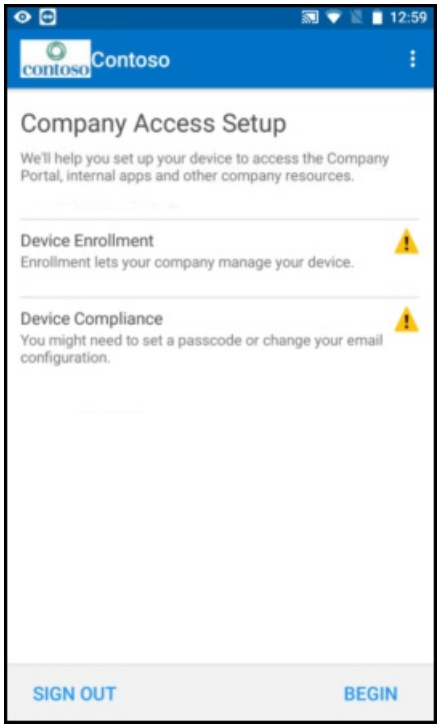
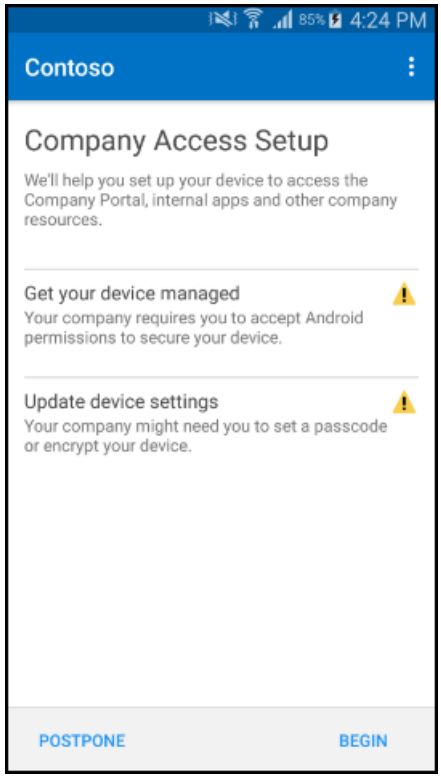
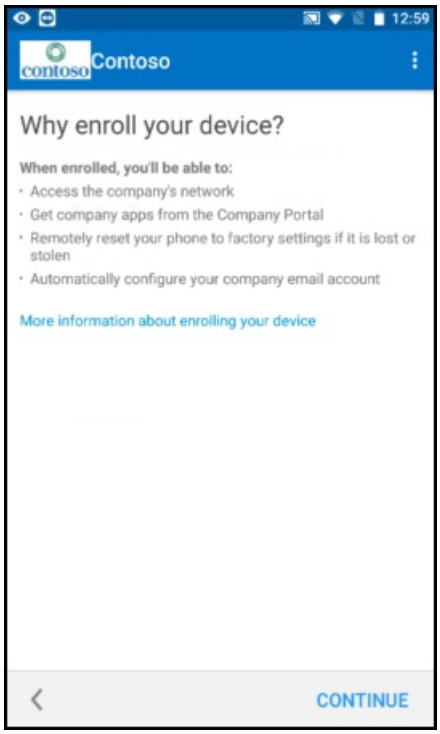
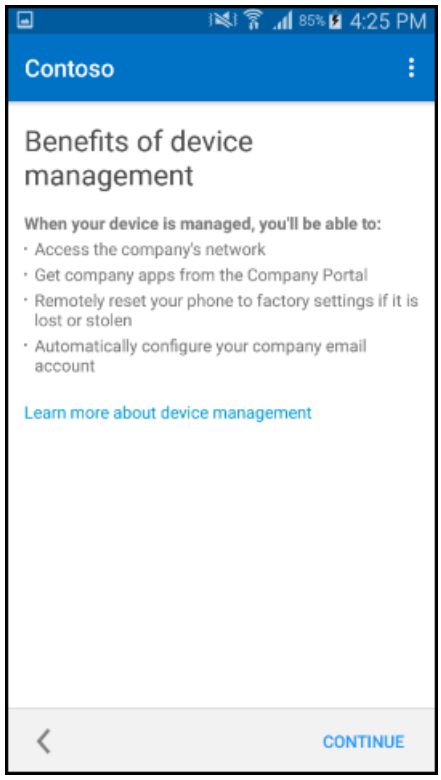
ANTES	DESPUÉS
	

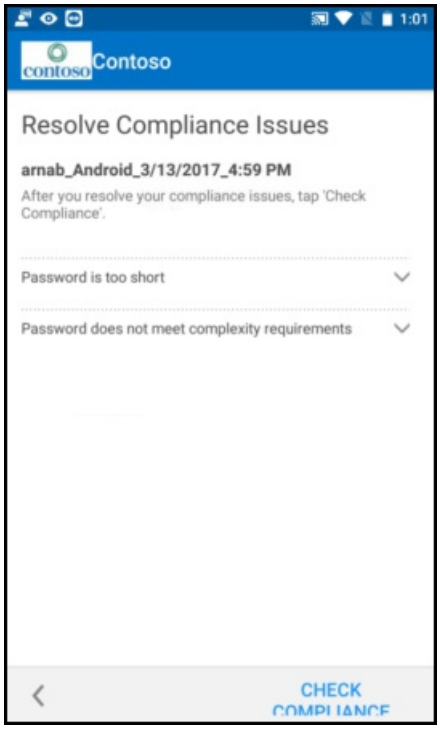
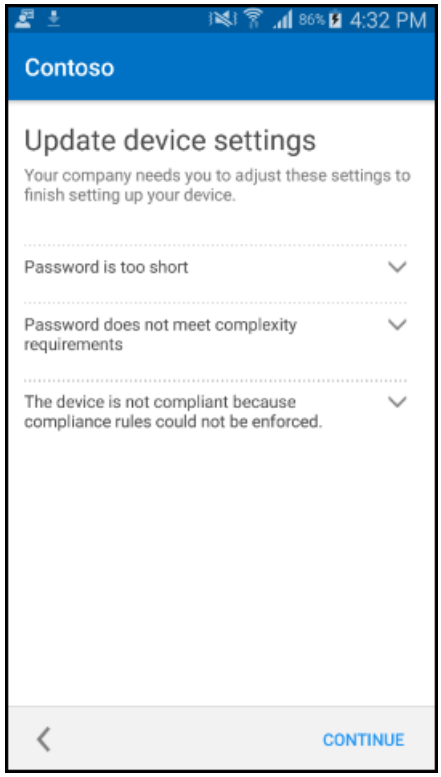
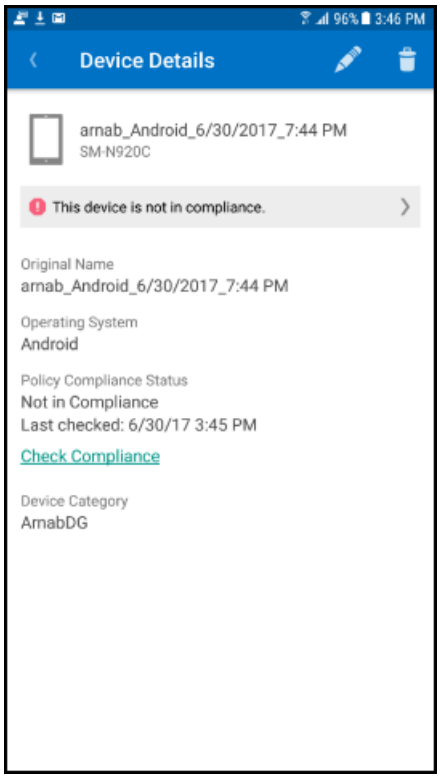
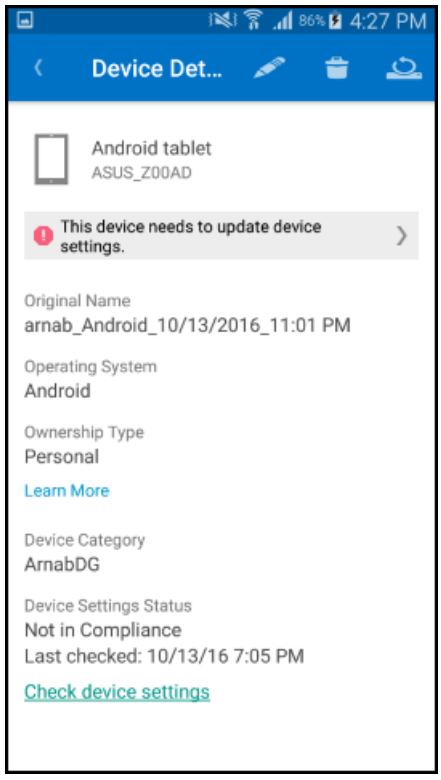
Semana del 11 de septiembre de 2017

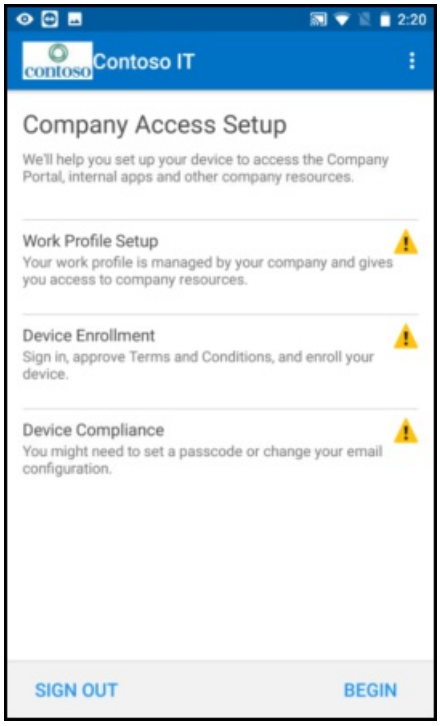
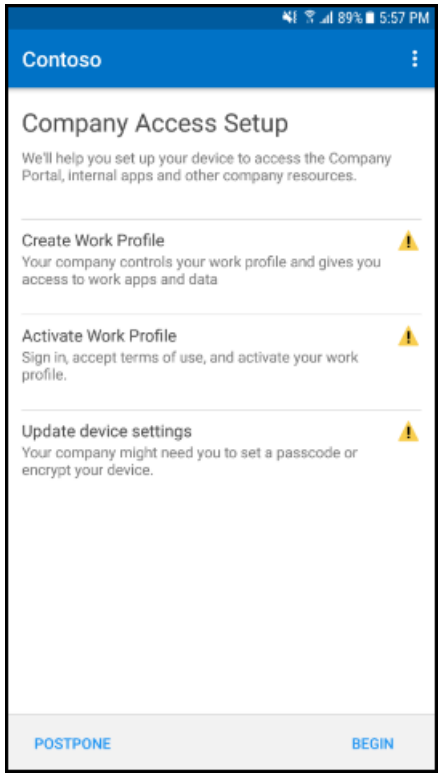
Frases más fáciles de entender para la aplicación Portal de empresa para Android

El proceso de inscripción para la aplicación de Portal de empresa para Android se ha simplificado con nuevo

texto para que resulte más sencillo para los usuarios finales. Si tiene documentación de inscripción personalizada, deberá actualizarla para reflejar las pantallas nuevas. Puede encontrar imágenes de muestra a continuación:

ANTES	DESPUÉS
	
	

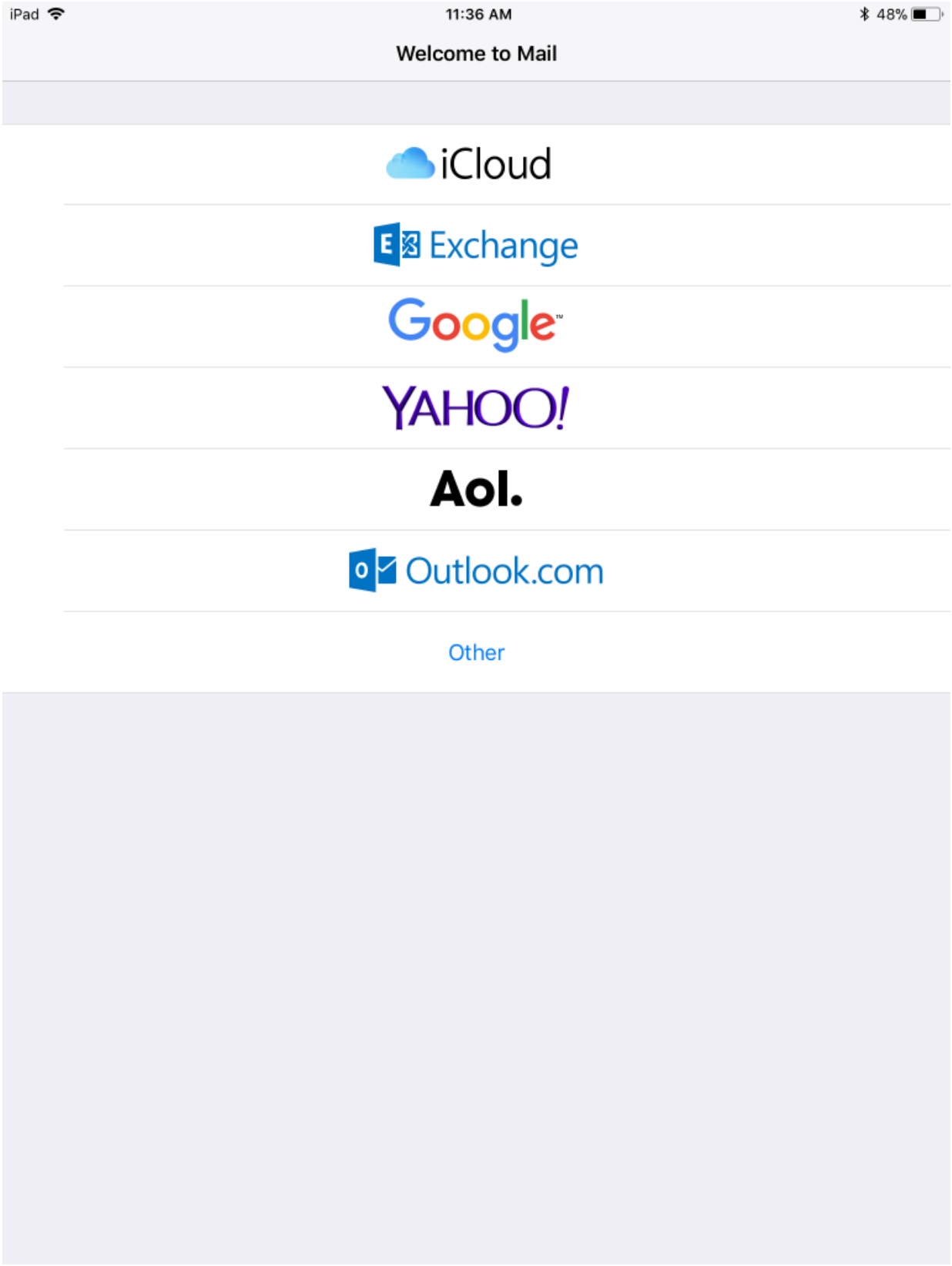
ANTES	DESPUÉS
	
	

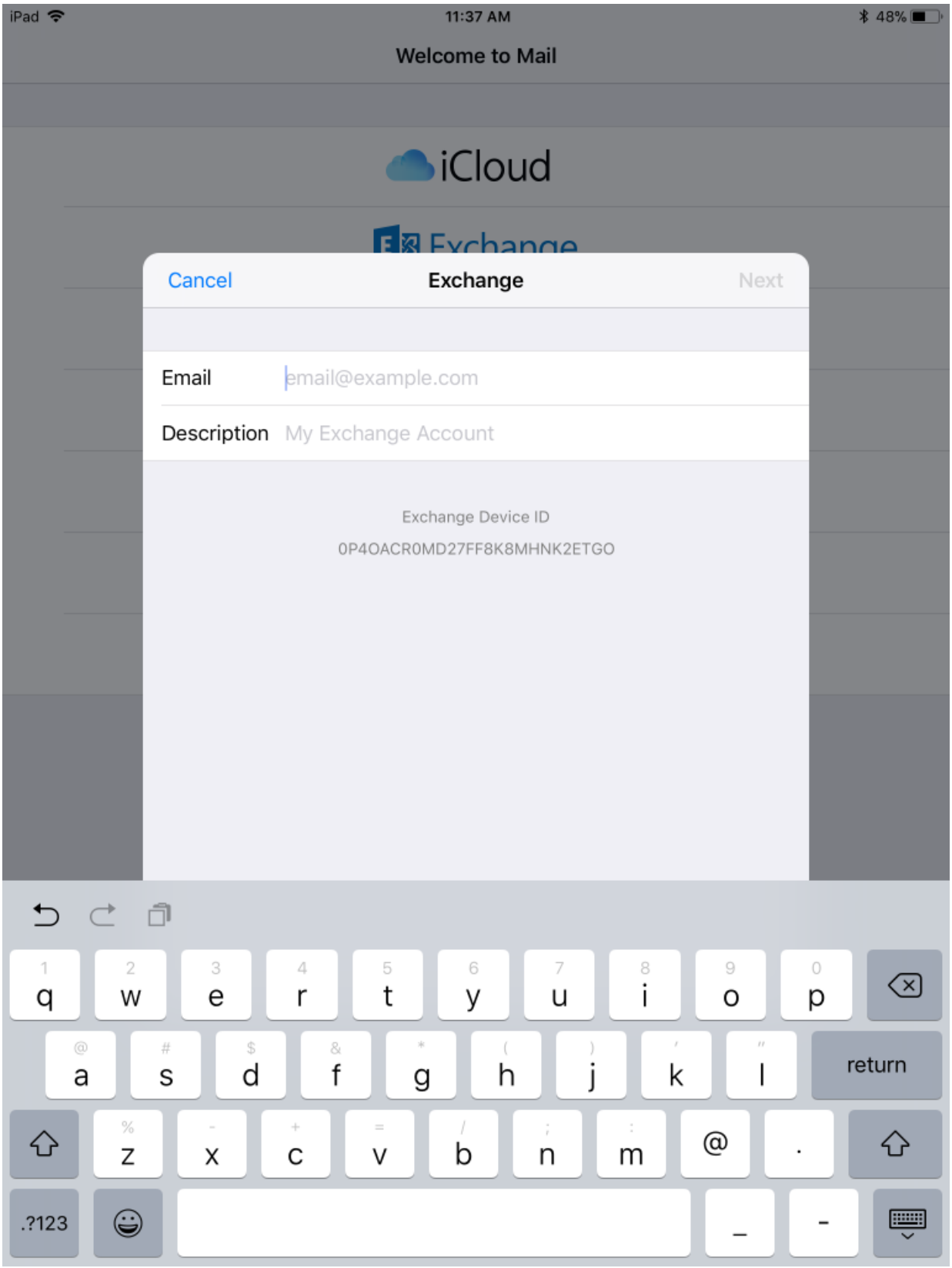
ANTES	DESPUÉS
	

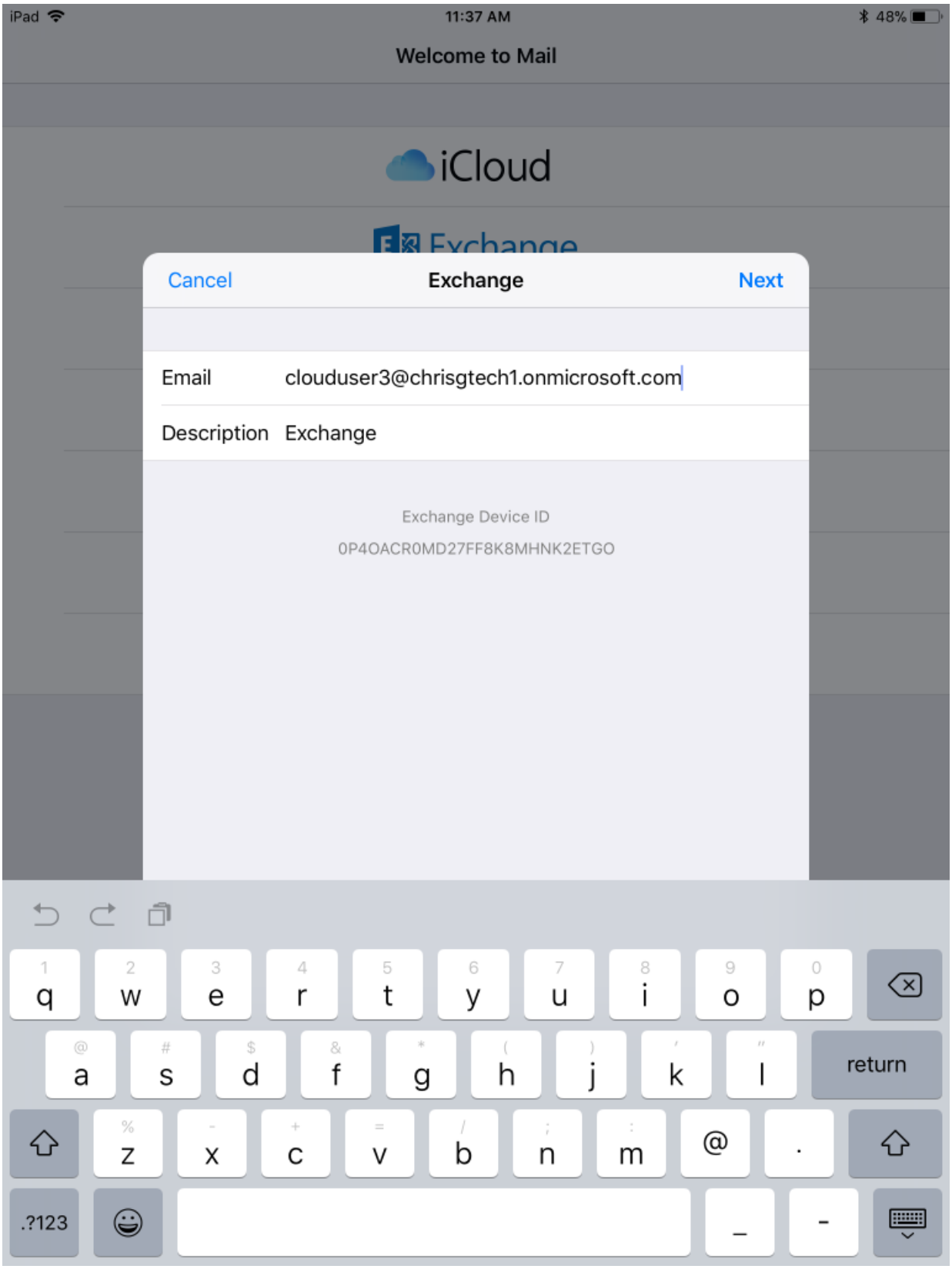
Agosto de 2017

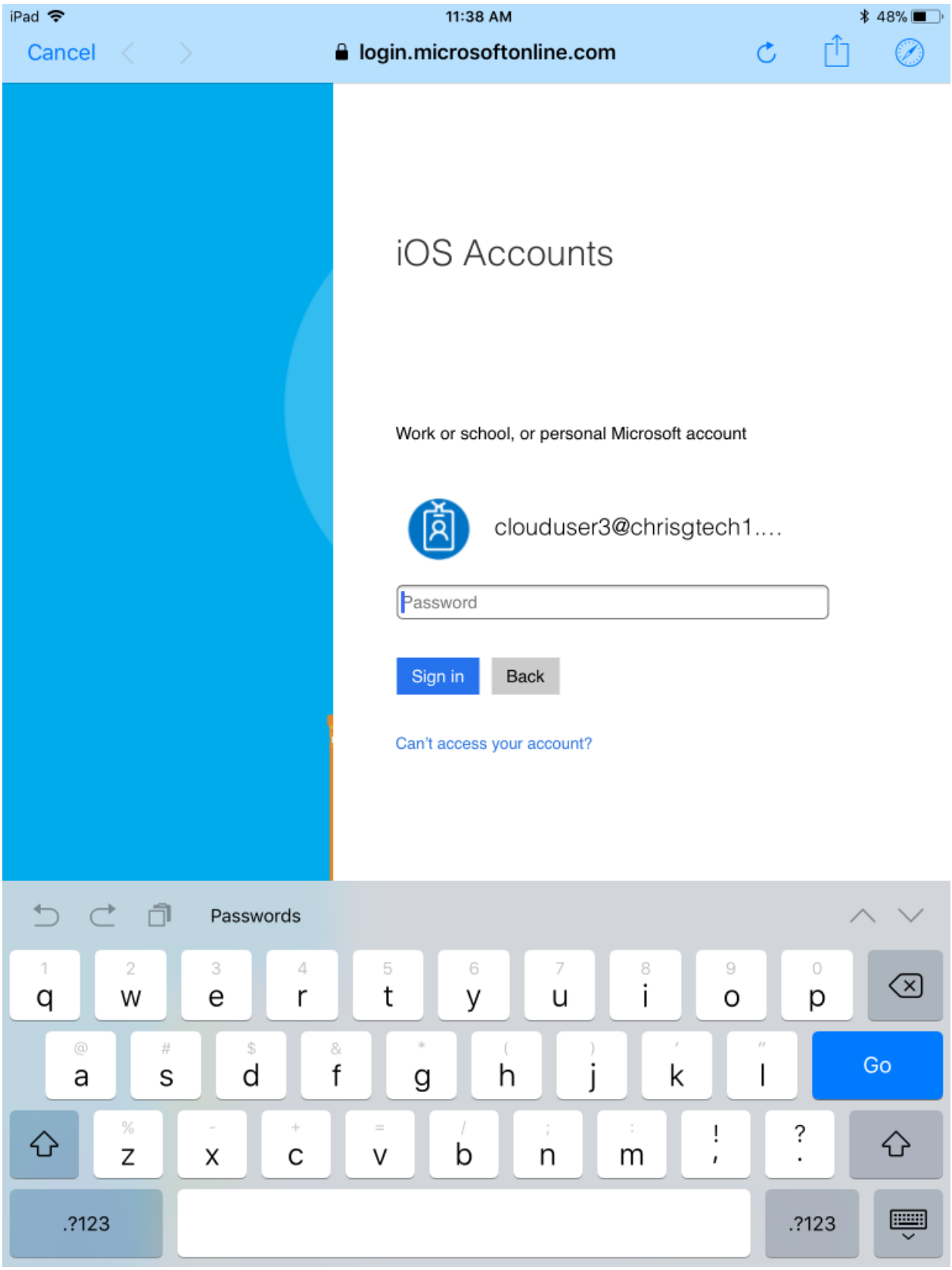
Compatibilidad de la aplicación Mail de iOS 11 con OAuth

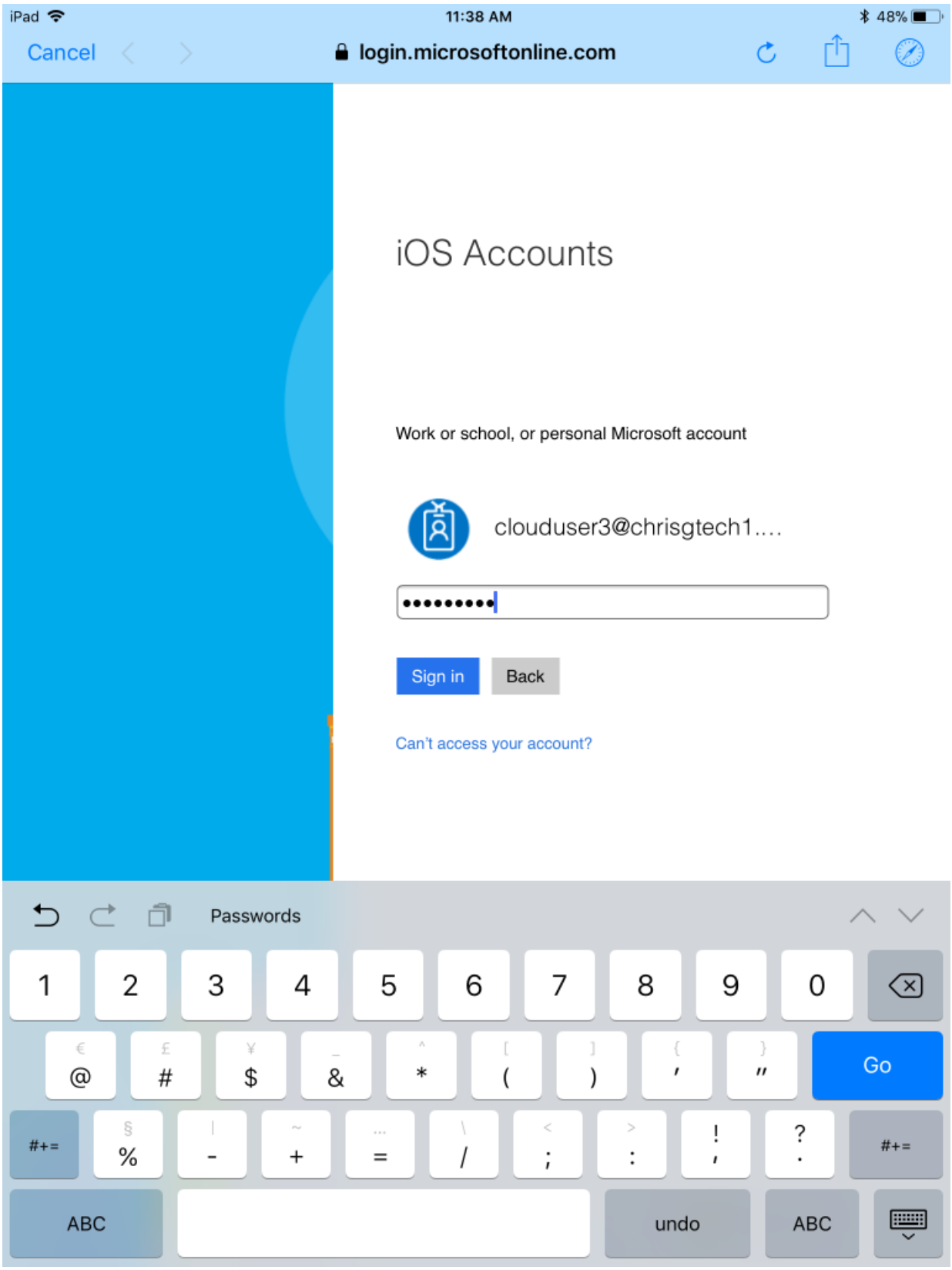
El acceso condicional con Intune es compatible con una autenticación más segura en dispositivos iOS con OAuth. Para lograr esta mayor seguridad en la autenticación, ahora habrá un flujo diferente en la aplicación Portal de empresa para iOS. Cuando los usuarios finales intenten iniciar sesión en una nueva cuenta de Exchange con la aplicación Mail, verán un mensaje de vista web. Tras la inscripción en Intune, los usuarios verán un mensaje para permitir que la aplicación nativa Mail acceda a un certificado. La mayoría de los usuarios finales no podrá ver correos electrónicos en cuarentena. Las cuentas de correo electrónico existentes continuarán usando el protocolo de autenticación básico, de modo que estos usuarios seguirán recibiendo correos electrónicos en cuarentena. Esta experiencia de inicio de sesión para los usuarios finales es similar a la de las aplicaciones móviles de Office.

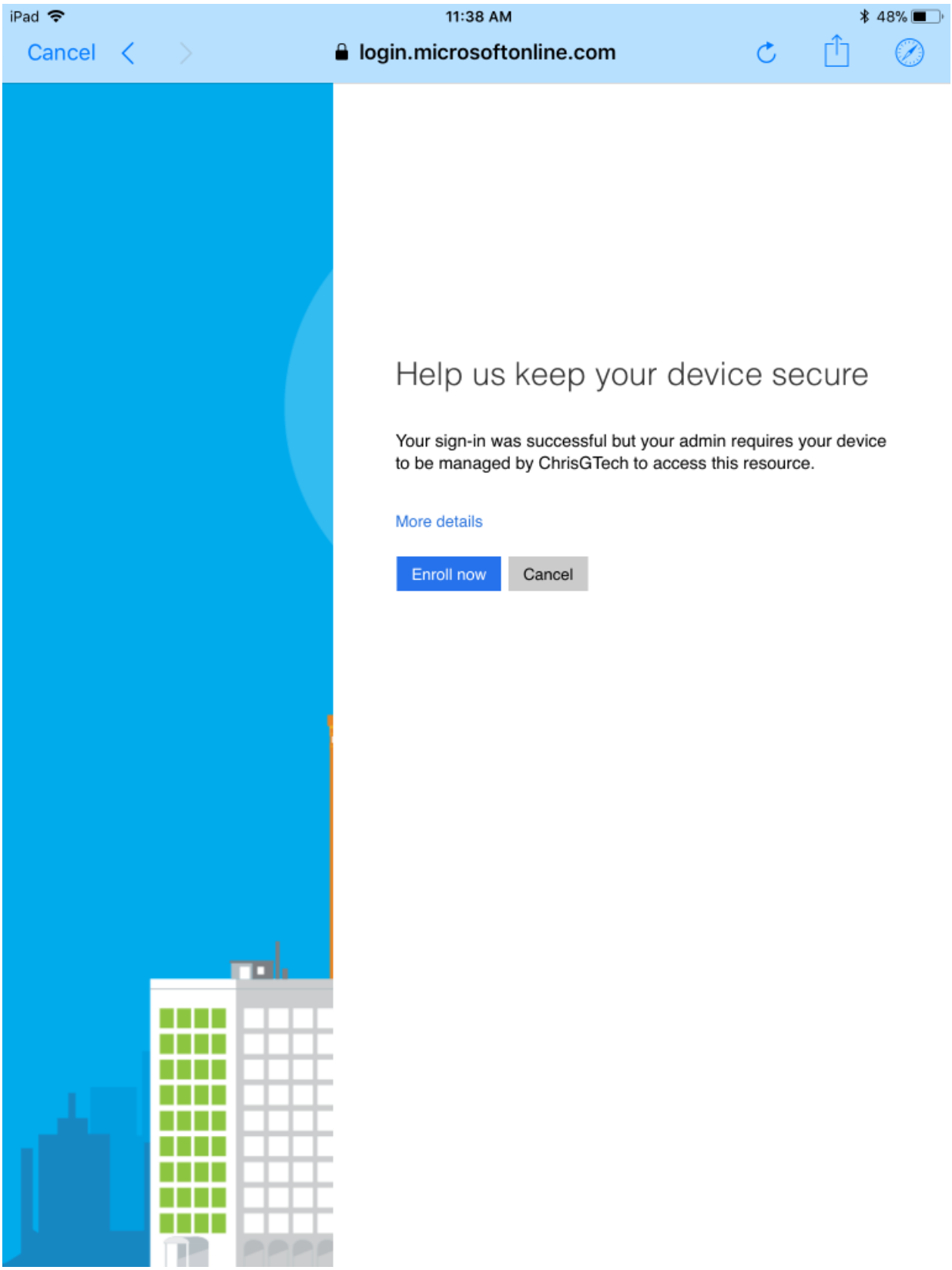

iPad
11:36 AM
48%
Welcome to Mail
iCloud
Exchange
Google
YAHOO!
Aol.
Outlook.com
Other

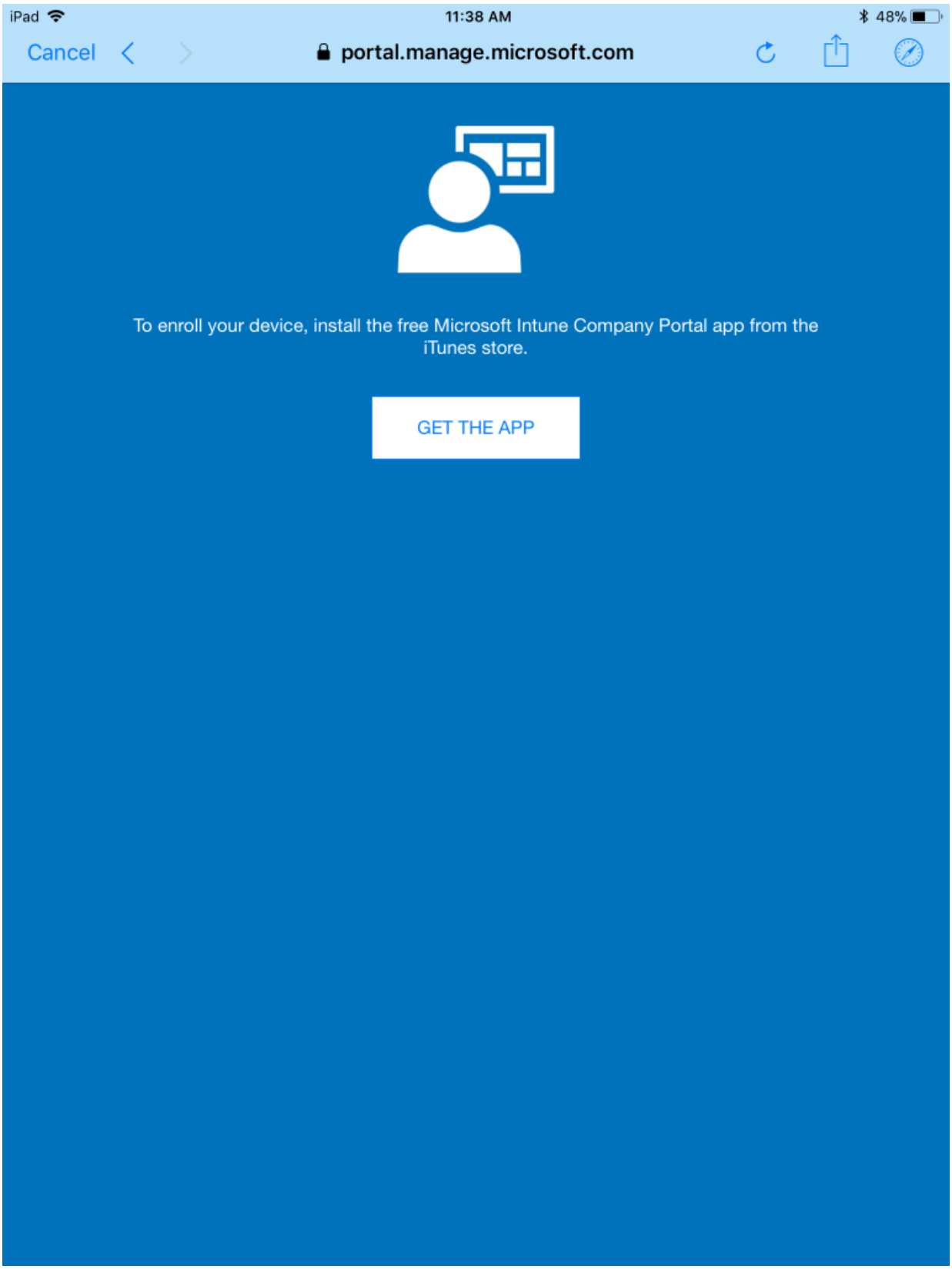

iPad
11:37 AM
48%
Welcome to Mail
iCloud
Exchange
Cancel
Exchange
Next
Email
email@example.com
Description
My Exchange Account
Exchange Device ID
0P4OACR0MD27FF8K8MHNK2ETGO
return
.?123


iPad
11:37 AM
48%
Welcome to Mail
iCloud
Exchange
Cancel
Exchange
Next
Email
clouduser3@chrisgtech1.onmicrosoft.com
Description
Exchange
Exchange Device ID
0P4OACR0MD27FF8K8MHNK2ETGO
return
.?123


iPad
11:38 AM
48%
Cancel
login.microsoftonline.com
iOS Accounts
Work or school, or personal Microsoft account
clouduser3@chrisgtech1....
Password
Sign in
Back
Can't access your account?
Passwords
Go
.?123
.?123


iPad
11:38 AM
48%
Cancel
login.microsoftonline.com
iOS Accounts
Work or school, or personal Microsoft account
clouduser3@chrisgtech1....
Sign in
Back
Can't access your account?
Passwords
Go
undo
ABC
ABC


iPad
11:38 AM
48%
Cancel
login.microsoftonline.com
Help us keep your device secure
Your sign-in was successful but your admin requires your device to be managed by ChrisGTech to access this resource.
More details
Enroll now
Cancel

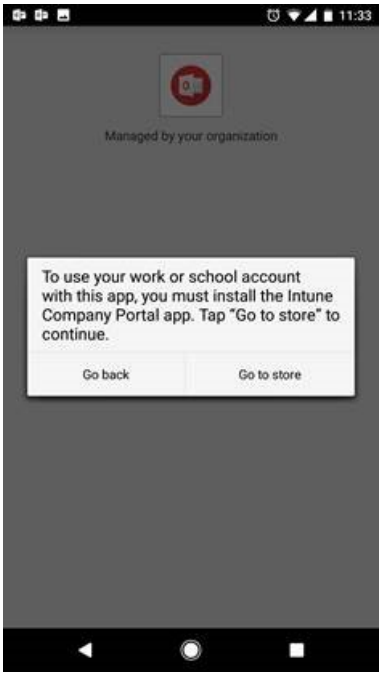


Los cuadros de diálogo de administración de aplicaciones móviles (MAM) de Intune tendrán ahora una interfaz moderna

Se actualizarán los cuadros de diálogo de administración de aplicaciones móviles (MAM) de Intune para tener un aspecto moderno. Los cuadros de diálogo funcionarán de la misma manera que con el estilo anterior.

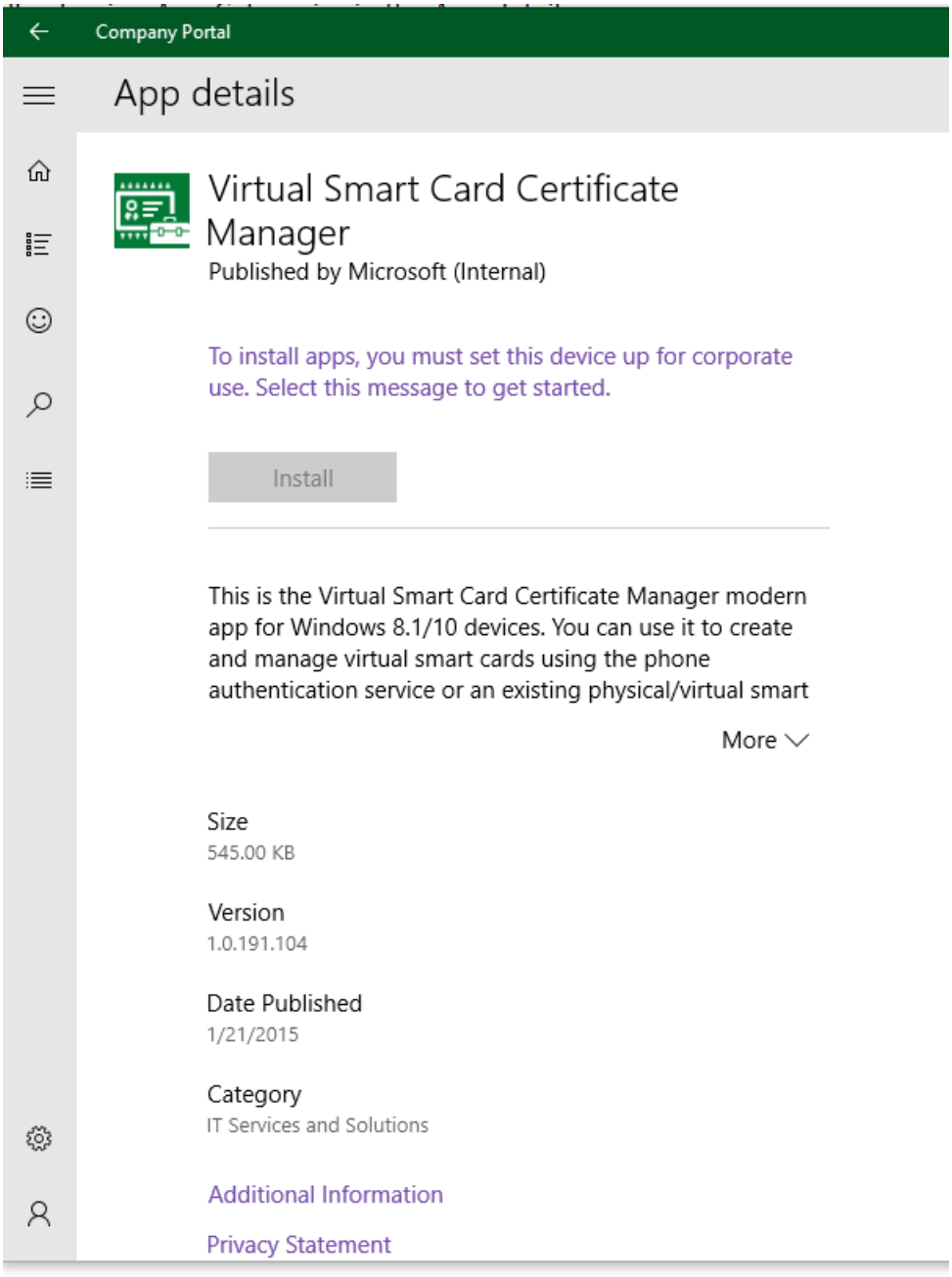
Experiencia anterior

Experiencia moderna



Actualizaciones en la página "Detalles del dispositivo" en la aplicación Portal de empresa para Windows 10

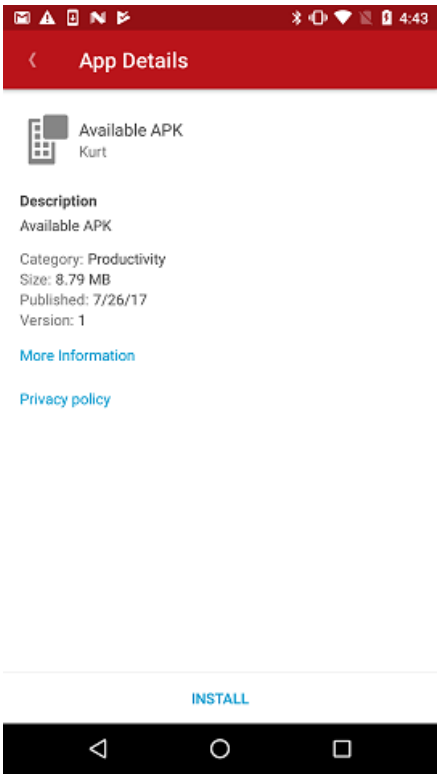
La etiqueta **Categoría** de la aplicación Portal de empresa para Windows 10 pasará de estar debajo del título a formar parte de una propiedad de la página **Detalles del dispositivo**.



Julio de 2017

Las páginas de información de aplicaciones mostrarán información nueva para los dispositivos Android

La página de información de aplicaciones de la aplicación Portal de empresa para Android mostrará las categorías de aplicaciones que el administrador de TI haya definido para esa aplicación.

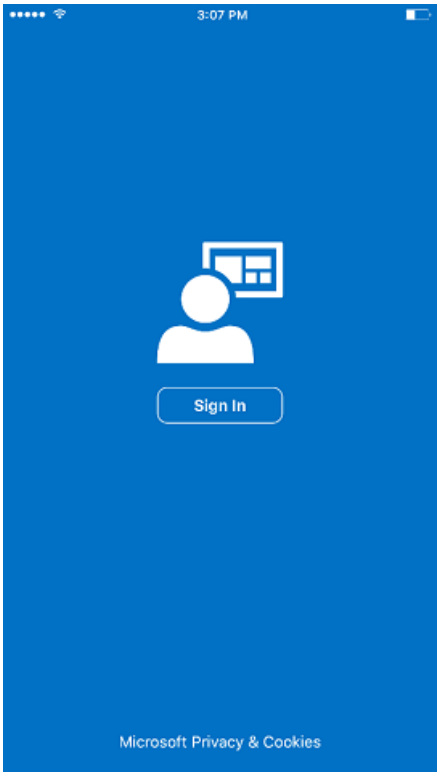


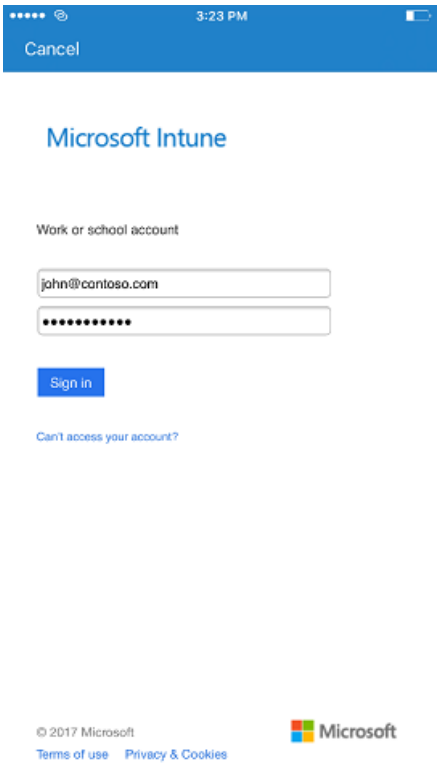
Mejora de la experiencia de inicio de sesión en todas las aplicaciones del Portal de empresa para todas las plataformas

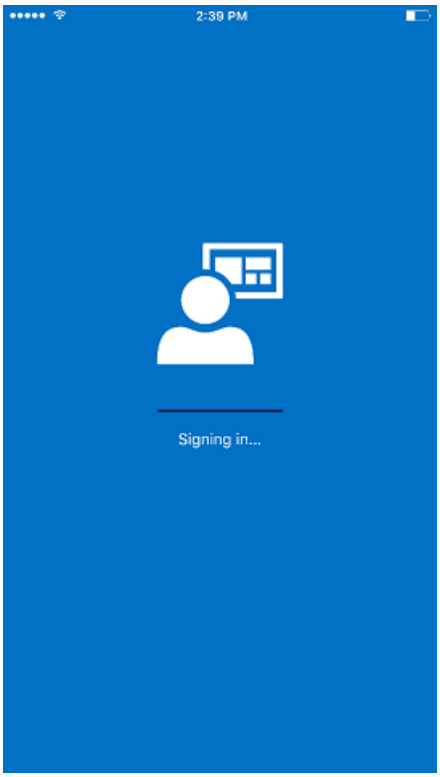
Se anuncia un cambio que aparecerá en los próximos meses y que mejorará la experiencia de inicio de sesión para las aplicaciones del Portal de empresa de Intune para Android, iOS/iPadOS y Windows. La nueva experiencia del usuario aparecerá automáticamente en todas las plataformas de la aplicación Portal de empresa cuando Azure AD haga este cambio. Además, los usuarios ahora pueden iniciar sesión en Portal de empresa desde otro dispositivo con un código generado de un solo uso. Esto resulta útil especialmente en casos en los que los usuarios necesitan iniciar sesión sin credenciales.

Aquí puede ver la experiencia de inicio de sesión anterior, la nueva experiencia de inicio de sesión con credenciales y la nueva experiencia de inicio de sesión desde otro dispositivo.

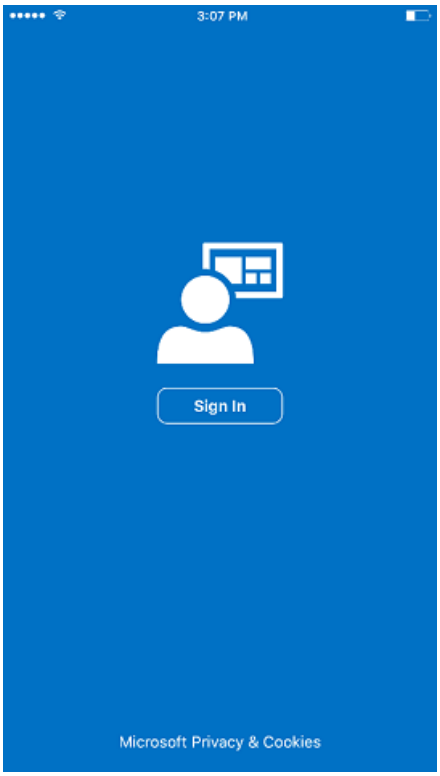
Experiencia de inicio de sesión anterior

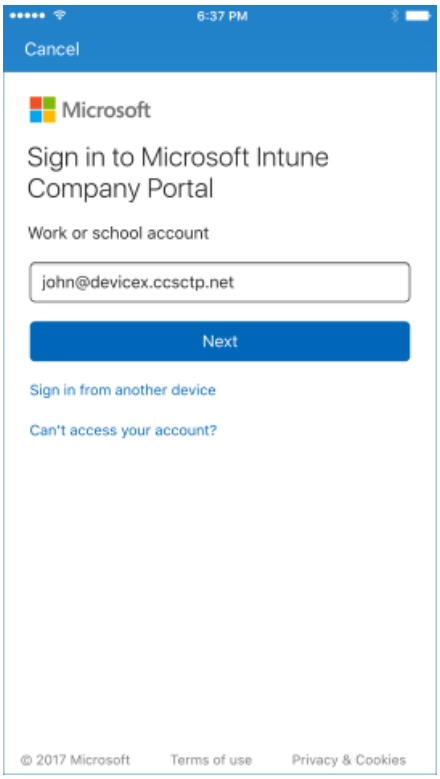


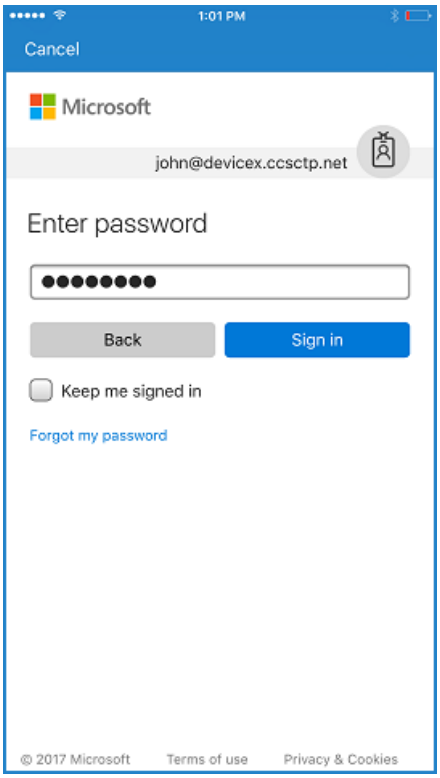


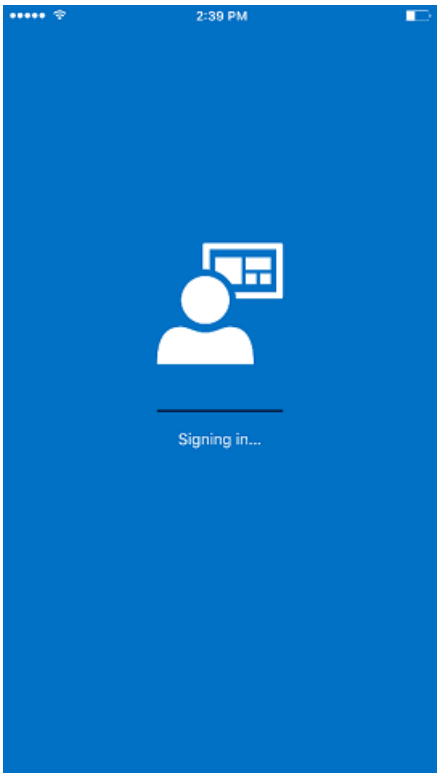


Nueva experiencia de inicio de sesión

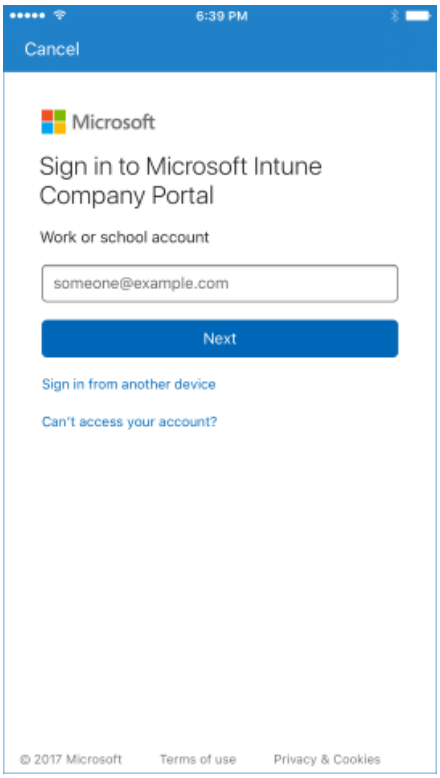

3:07 PM
Sign In
Microsoft Privacy & Cookies


6:37 PM
Cancel
Microsoft
Sign in to Microsoft Intune Company Portal
Work or school account
john@devicex.ccsctp.net
Next
Sign in from another device
Can't access your account?
© 2017 Microsoft
Terms of use
Privacy & Cookies



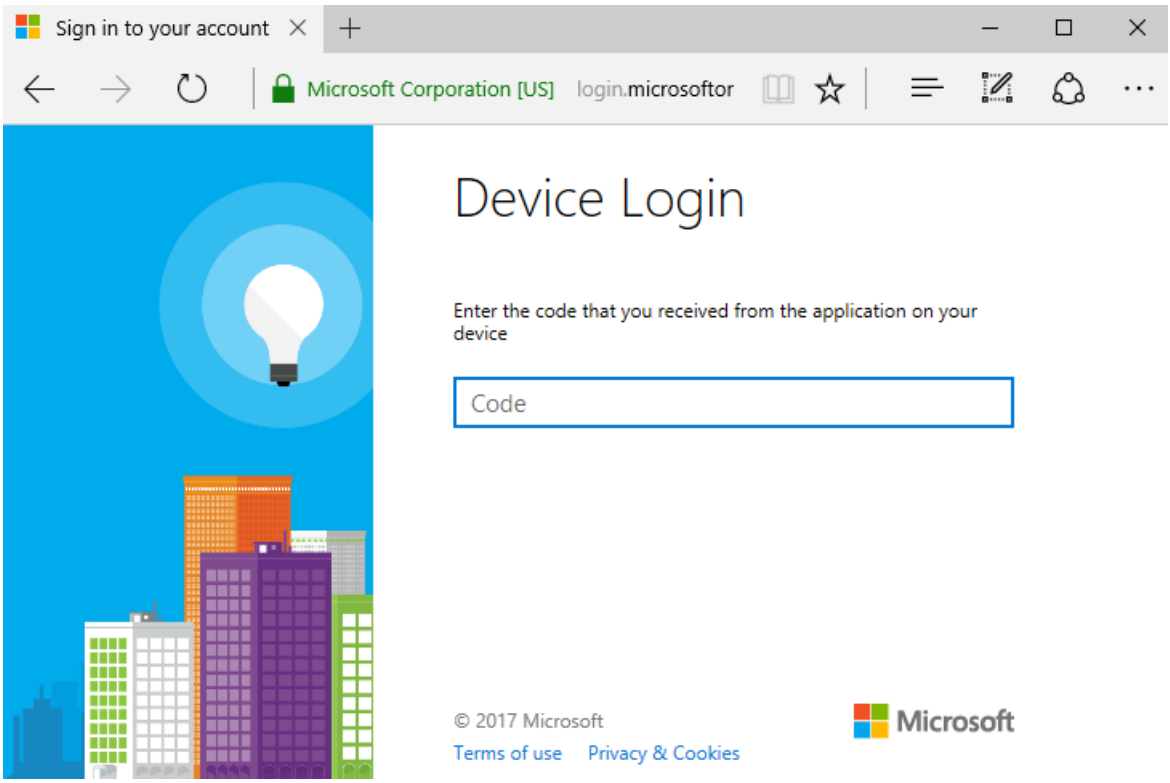


Nueva experiencia de inicio de sesión cuando se inicia sesión desde otro dispositivo

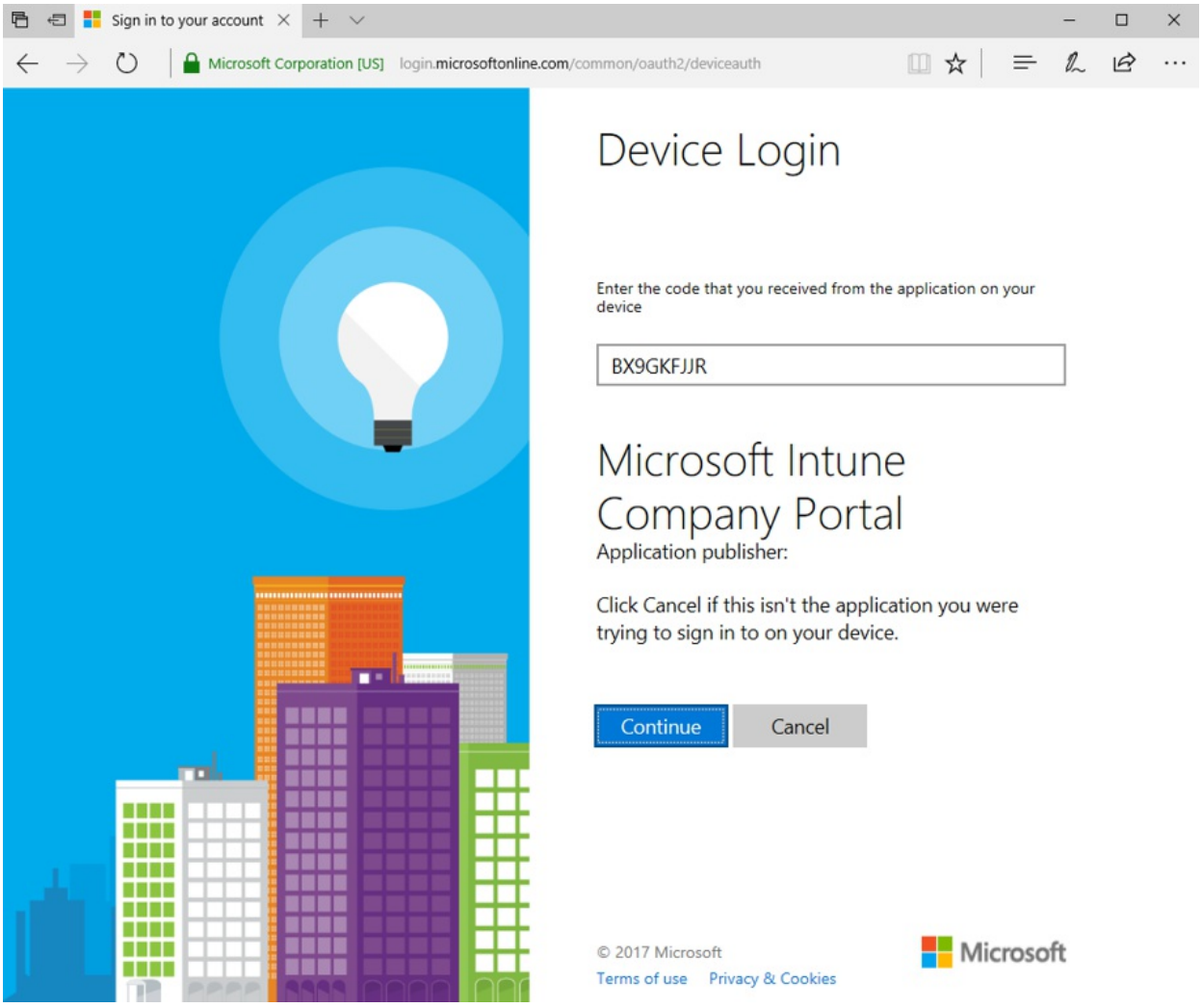


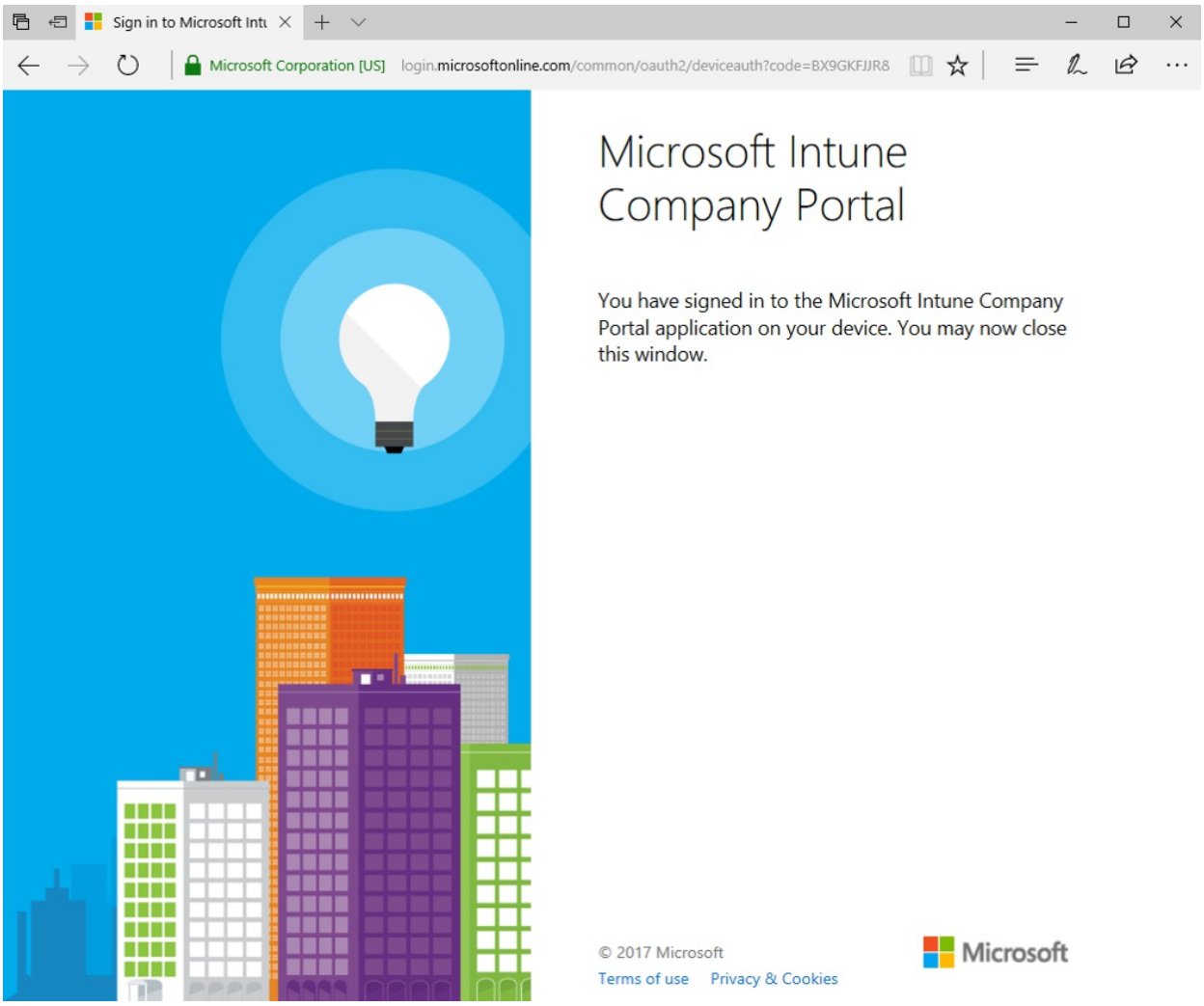
Pulse el vínculo **Iniciar sesión desde otro dispositivo**.

Abra un explorador y vaya a https://aka.ms/devicelogin.

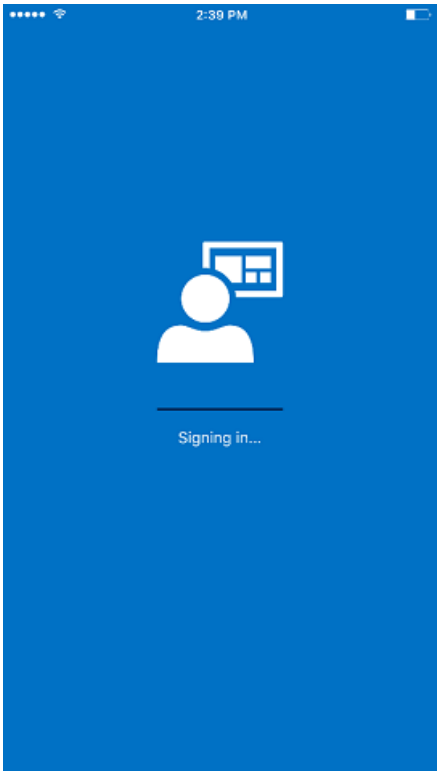


Escriba el código que vio en la aplicación Portal de empresa. Cuando seleccione **Continuar**, podrá autenticarse con cualquier método que admita su empresa, como una tarjeta inteligente.





La aplicación Portal de empresa comenzará a iniciar sesión.

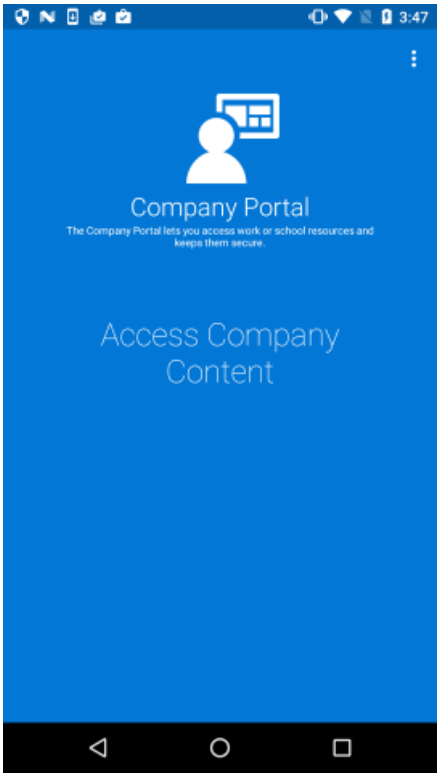


Junio de 2017

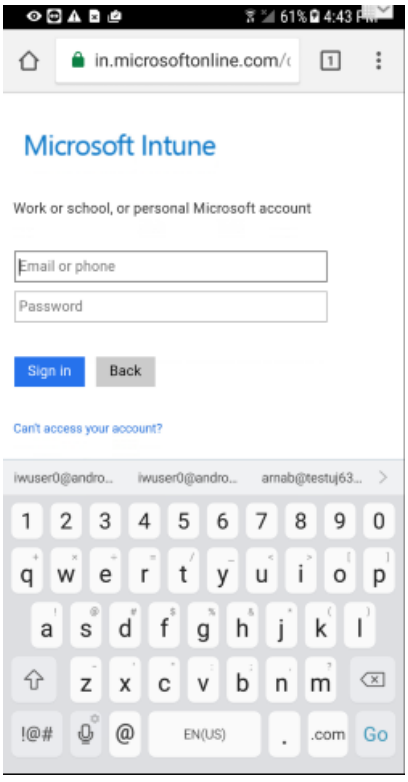
La aplicación Portal de empresa para Android ahora tiene una nueva experiencia de usuario final de las directivas de protección de aplicaciones.

Basándonos en los comentarios de los clientes, hemos modificado la aplicación del portal de empresa para Android para mostrar un botón **Acceso al contenido de la empresa**. El objetivo es impedir que los usuarios finales pasen innecesariamente por todo el proceso de inscripción cuando solo necesitan tener acceso a las aplicaciones que admiten las directivas de protección de aplicaciones, una característica de la administración de aplicaciones móviles de Intune.

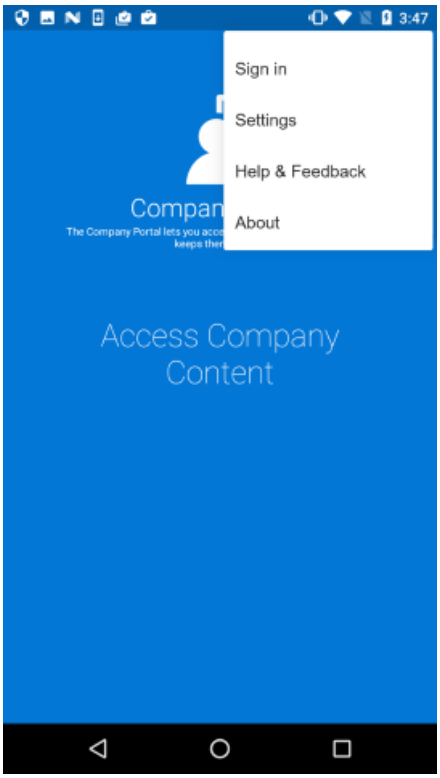
El usuario pulsará el botón **Acceso al contenido de la empresa** en lugar de comenzar a inscribir el dispositivo.



Después, al usuario se le redirige al sitio web del portal de empresa para autorizar la aplicación para su uso en el dispositivo, donde el sitio web del portal de empresa comprueba sus credenciales.

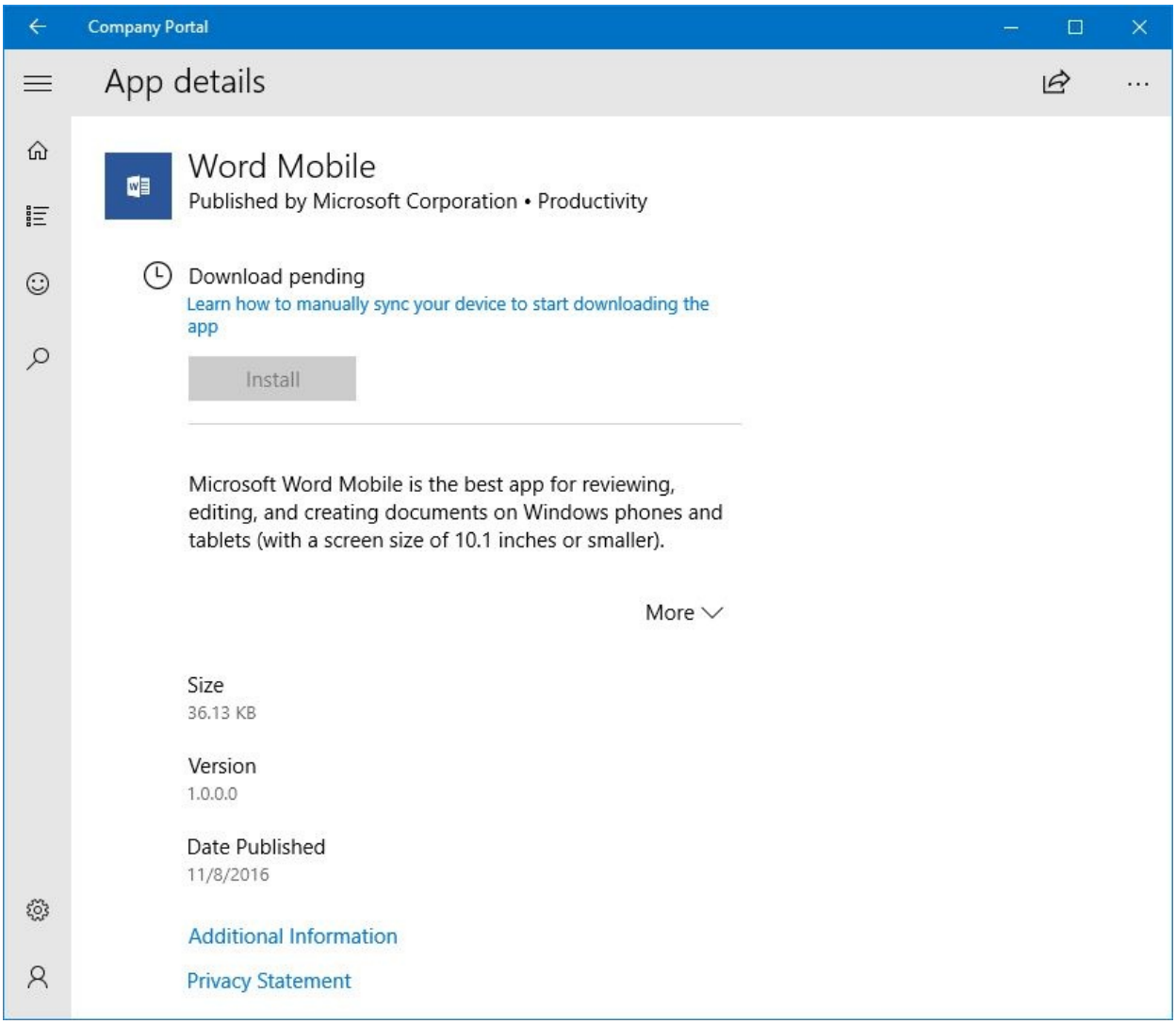


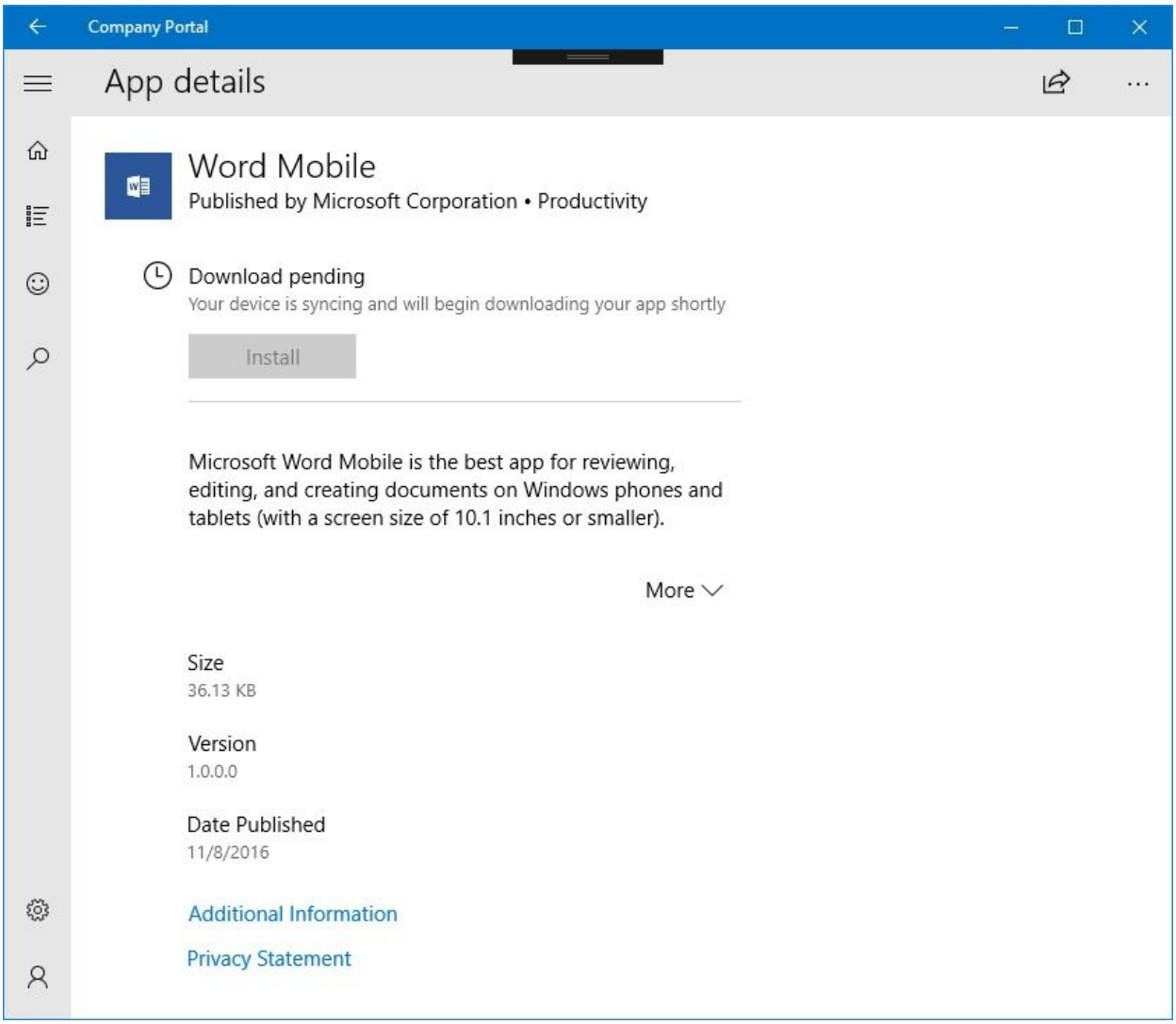
El dispositivo todavía puede inscribirse en la administración completa al pulsar el menú de **acción**.



Mejoras en la sincronización de aplicaciones con Windows 10 Creators Update

La aplicación Portal de empresa de Intune para Windows 10 ahora iniciará automáticamente una sincronización de las solicitudes de instalación de aplicaciones para dispositivos con Windows 10 Creators Update (versión 1709). De esta forma, se reducirá el problema de estancamiento de las instalaciones de aplicaciones durante el estado "Pending Sync" (Sincronización pendiente). Además, los usuarios podrán iniciar manualmente la sincronización desde dentro de la aplicación.

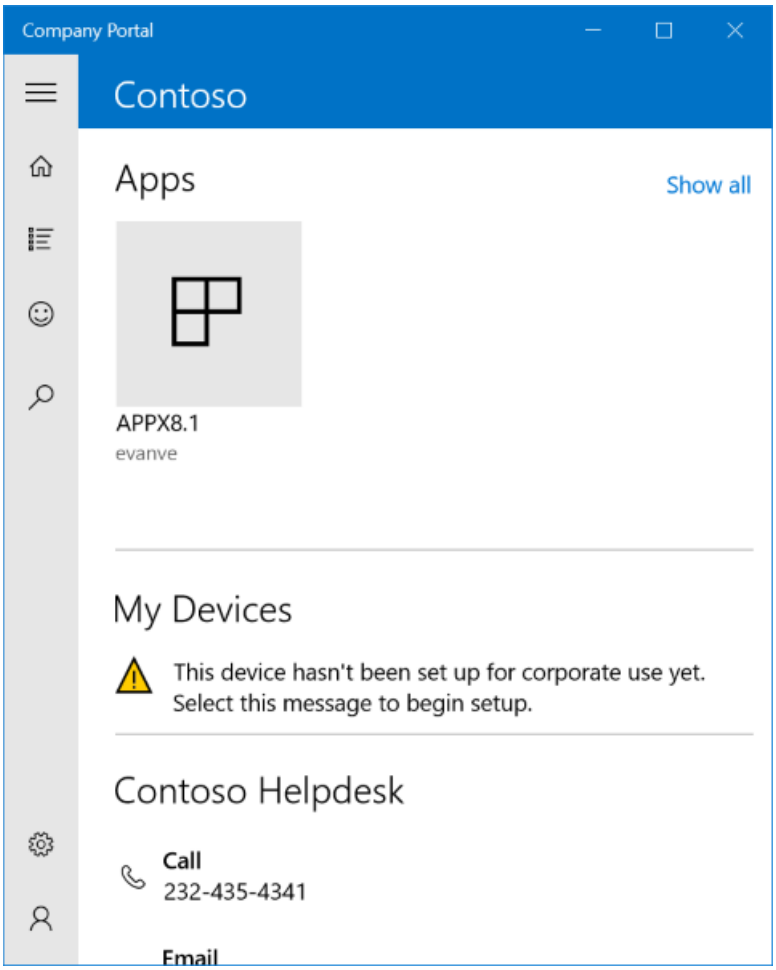

Company Portal
App details
Word Mobile
Published by Microsoft Corporation • Productivity
Download pending
Learn how to manually sync your device to start downloading the app
Install
Microsoft Word Mobile is the best app for reviewing, editing, and creating documents on Windows phones and tablets (with a screen size of 10.1 inches or smaller).
More
Size
36.13 KB
Version
1.0.0.0
Date Published
11/8/2016
Additional Information
Privacy Statement

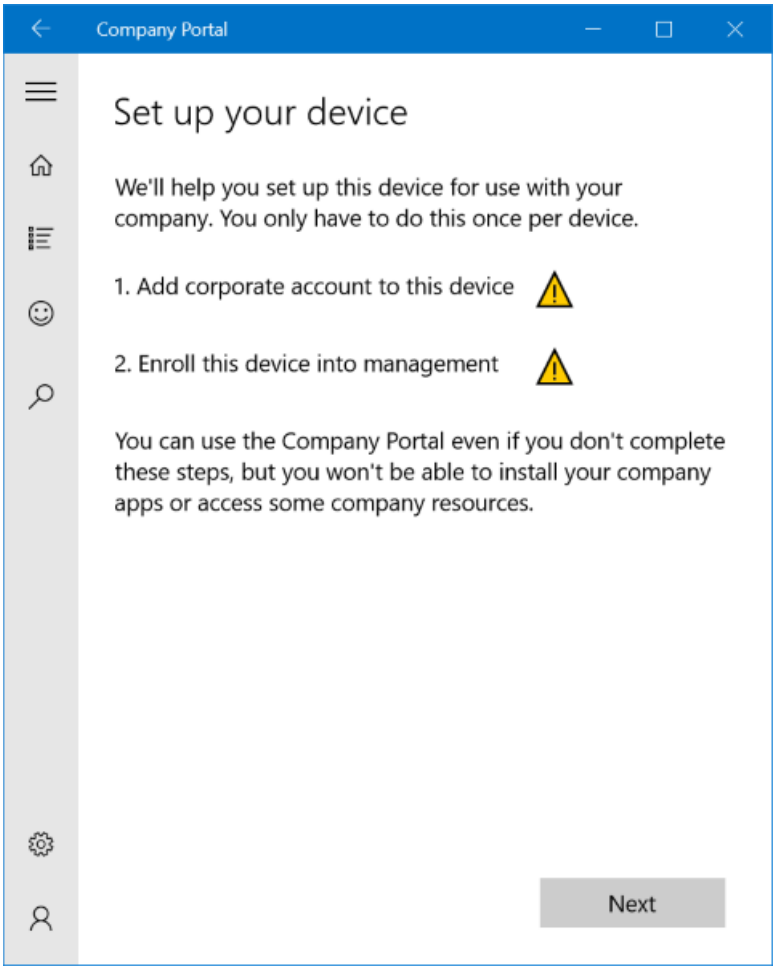


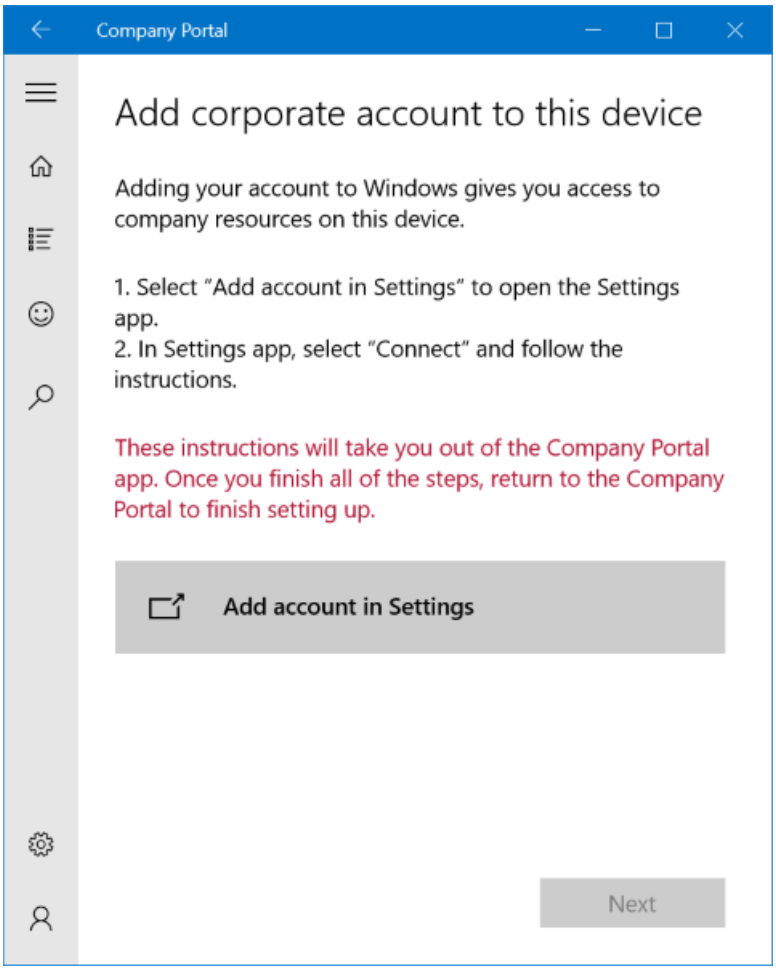
Nueva experiencia guiada del Portal de empresa de Windows 10 <!---1058938--->

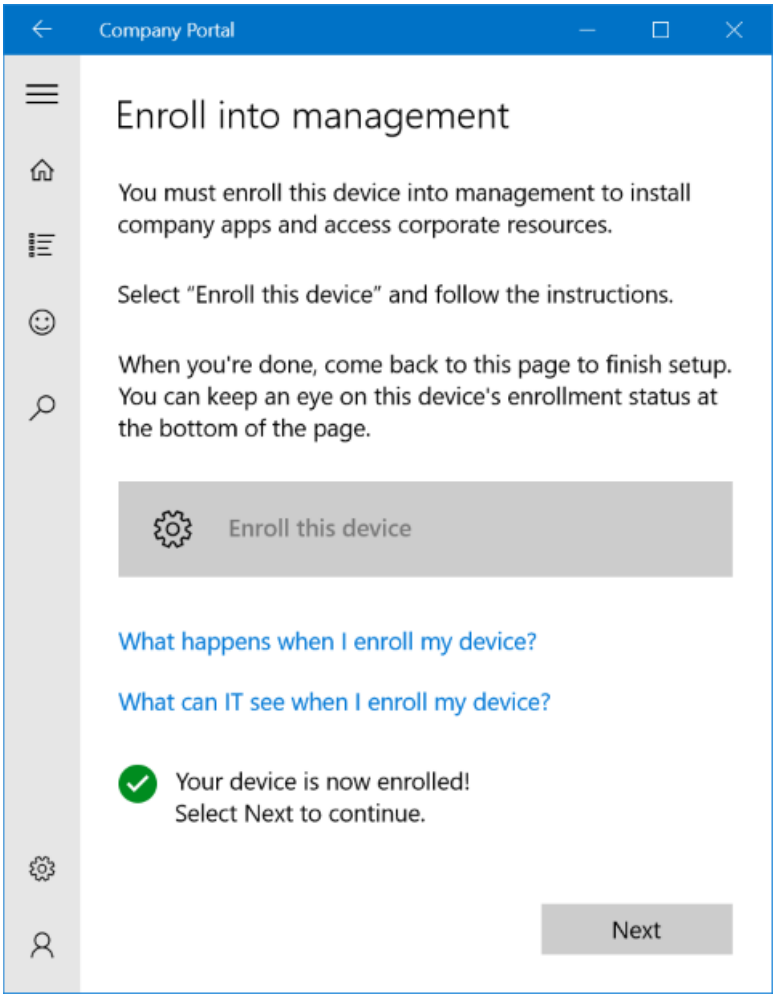
La aplicación del Portal de empresa para Windows 10 incluirá la experiencia de un tutorial de Intune guiado para dispositivos que no se han identificado ni inscrito. La nueva experiencia proporciona instrucciones paso a paso que llevan al usuario por el registro en Azure Active Directory (que es necesario para las características de acceso condicional) y la inscripción en MDM (que es necesaria para las características de administración de dispositivos). La experiencia guiada será accesible desde la página principal del Portal de empresa. Los usuarios pueden seguir utilizando la aplicación si no completan el registro y la inscripción, pero experimentarán una funcionalidad limitada.

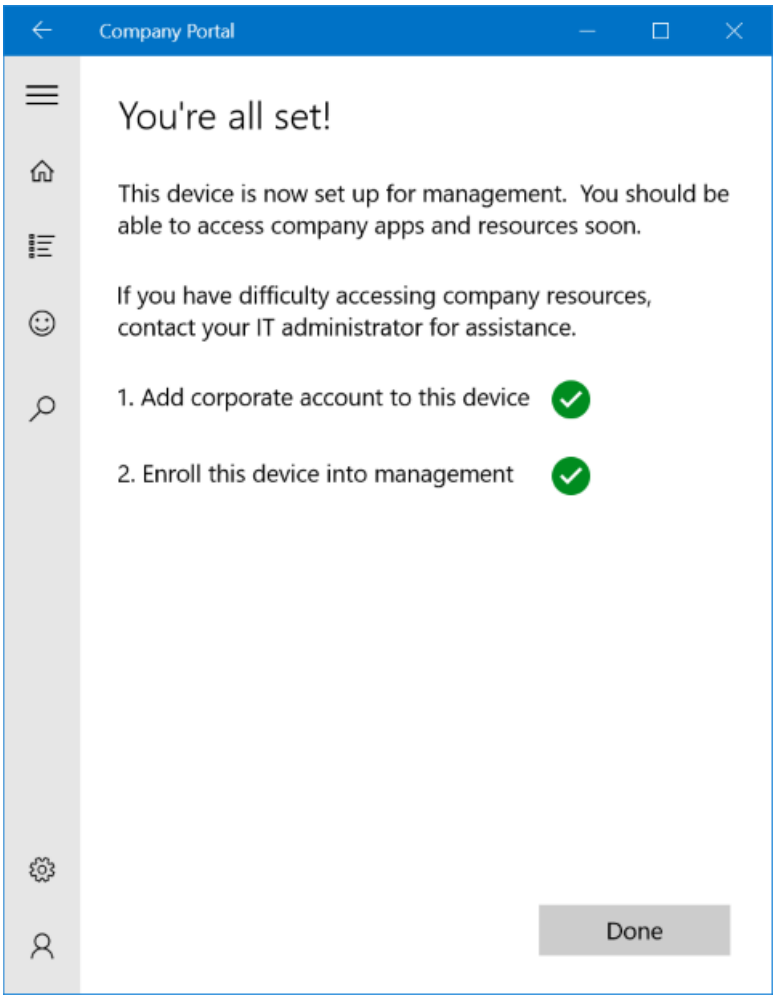
Esta actualización solo es visible en dispositivos que ejecuten la Actualización de aniversario de Windows 10 (compilación 1607) o superior.


Company Portal
Contoso
Apps
Show all
APPX8.1
evanve
My Devices
This device hasn't been set up for corporate use yet.
Select this message to begin setup.
Contoso Helpdesk
Call
232-435-4341
Email


Company Portal
Set up your device
We'll help you set up this device for use with your company. You only have to do this once per device.
1. Add corporate account to this device
2. Enroll this device into management
You can use the Company Portal even if you don't complete these steps, but you won't be able to install your company apps or access some company resources.
Next

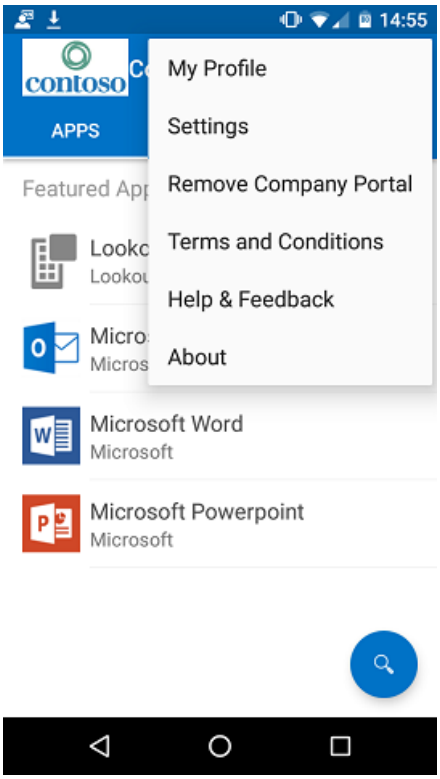

Company Portal
Add corporate account to this device
Adding your account to Windows gives you access to company resources on this device.
1. Select "Add account in Settings" to open the Settings app.
2. In Settings app, select "Connect" and follow the instructions.
These instructions will take you out of the Company Portal app. Once you finish all of the steps, return to the Company Portal to finish setting up.
Add account in Settings
Next

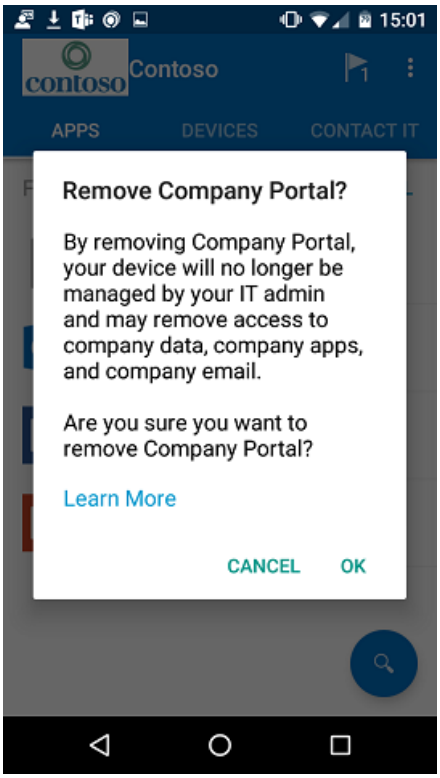

Company Portal
Enroll into management
You must enroll this device into management to install company apps and access corporate resources.
Select "Enroll this device" and follow the instructions.
When you're done, come back to this page to finish setup. You can keep an eye on this device's enrollment status at the bottom of the page.
Enroll this device
What happens when I enroll my device?
What can IT see when I enroll my device?
Your device is now enrolled!
Select Next to continue.
Next



Nueva acción de menú para quitar fácilmente Portal de empresa

Según los comentarios de los usuarios, se agregó una nueva acción de menú en la aplicación Portal de empresa de Intune para Android con el fin de iniciar su eliminación del dispositivo. Esta acción quita el dispositivo de la administración de Intune, por lo que el usuario puede quitar la aplicación del dispositivo.

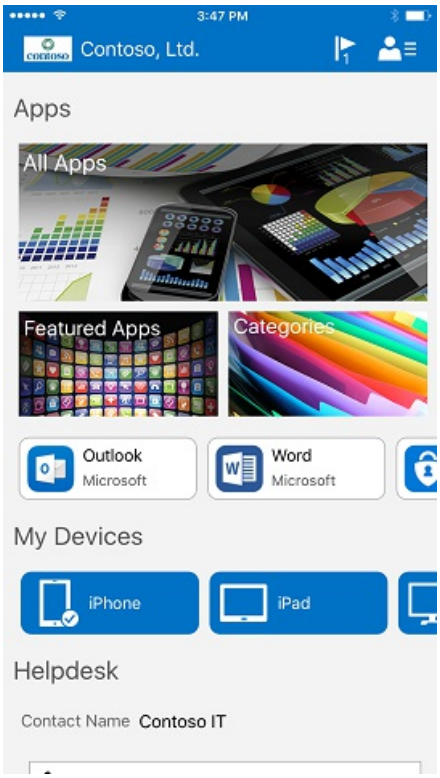




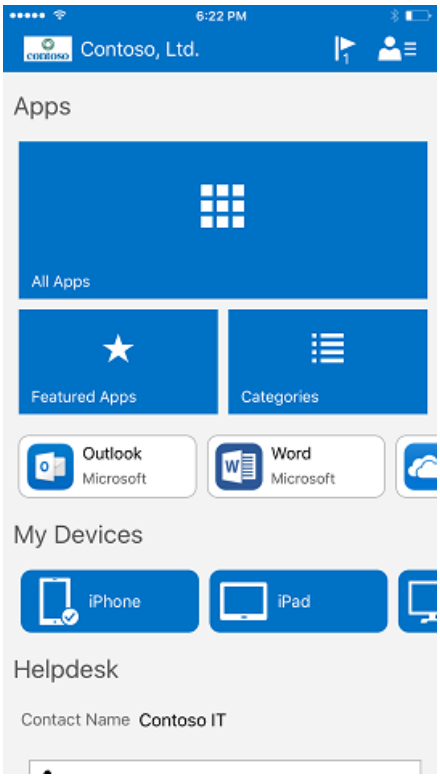
Mejoras de los iconos de aplicación en la aplicación Portal de empresa de Intune para iOS

Se actualizó el diseño de los iconos de aplicación en la página principal para reflejar el color de personalización de marca que estableció para Portal de empresa de Intune.

Antes

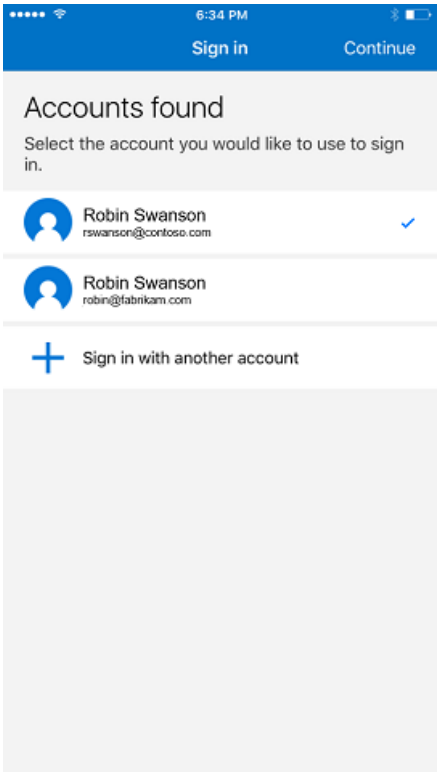


Después



Ahora el selector de cuenta está disponible en la aplicación Portal de empresa de Intune para iOS

Si los usuarios usaron su cuenta profesional o educativa para iniciar sesión en otras aplicaciones Microsoft en un dispositivo iOS, pueden ver el nuevo selector de cuenta cuando inician sesión por primera vez en Portal de empresa.



Abril de 2017

Nuevos iconos para Managed Browser y el Portal de empresa

Managed Browser está recibiendo iconos actualizados para las versiones de iOS y Android de la aplicación. El nuevo icono contendrá la notificación de Intune actualizada para que sea más coherente con otras aplicaciones de Enterprise Mobility + Security (EM+S).

El Portal de empresa también está recibiendo iconos actualizados para las versiones de Windows, iOS y Android de la aplicación con el objetivo de mejorar la coherencia con otras aplicaciones de EM+S. Estos iconos se lanzarán gradualmente en las distintas plataformas desde abril hasta finales de mayo.

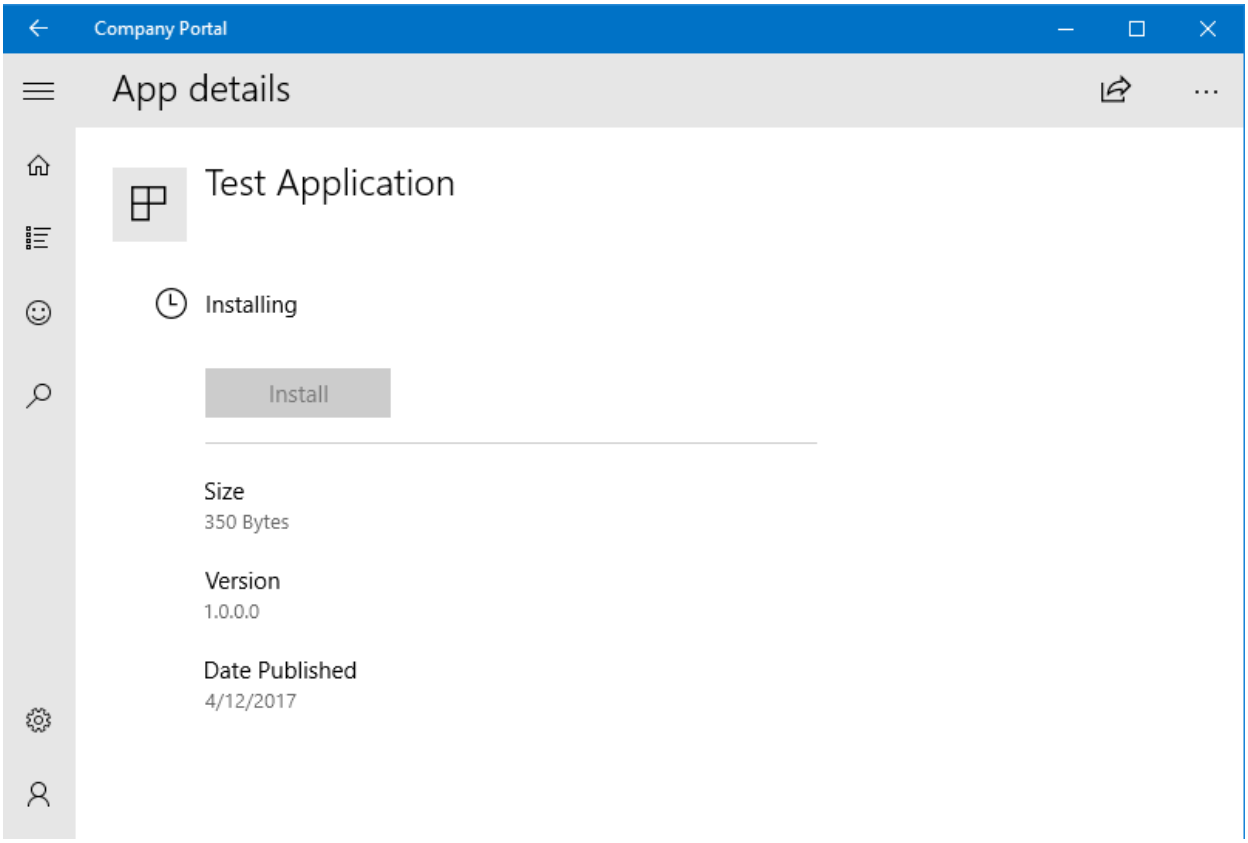
Indicador de progreso de inicio de sesión en Portal de empresa de Android

Una actualización de la aplicación Portal de empresa de Android muestra un indicador de progreso de inicio de sesión cuando el usuario inicia o reanuda la aplicación. El indicador avanza por los nuevos estados, desde "Conectando..." e "Iniciando sesión..." hasta "Comprobando los requisitos de seguridad...", antes de permitir que el usuario acceda a la aplicación.

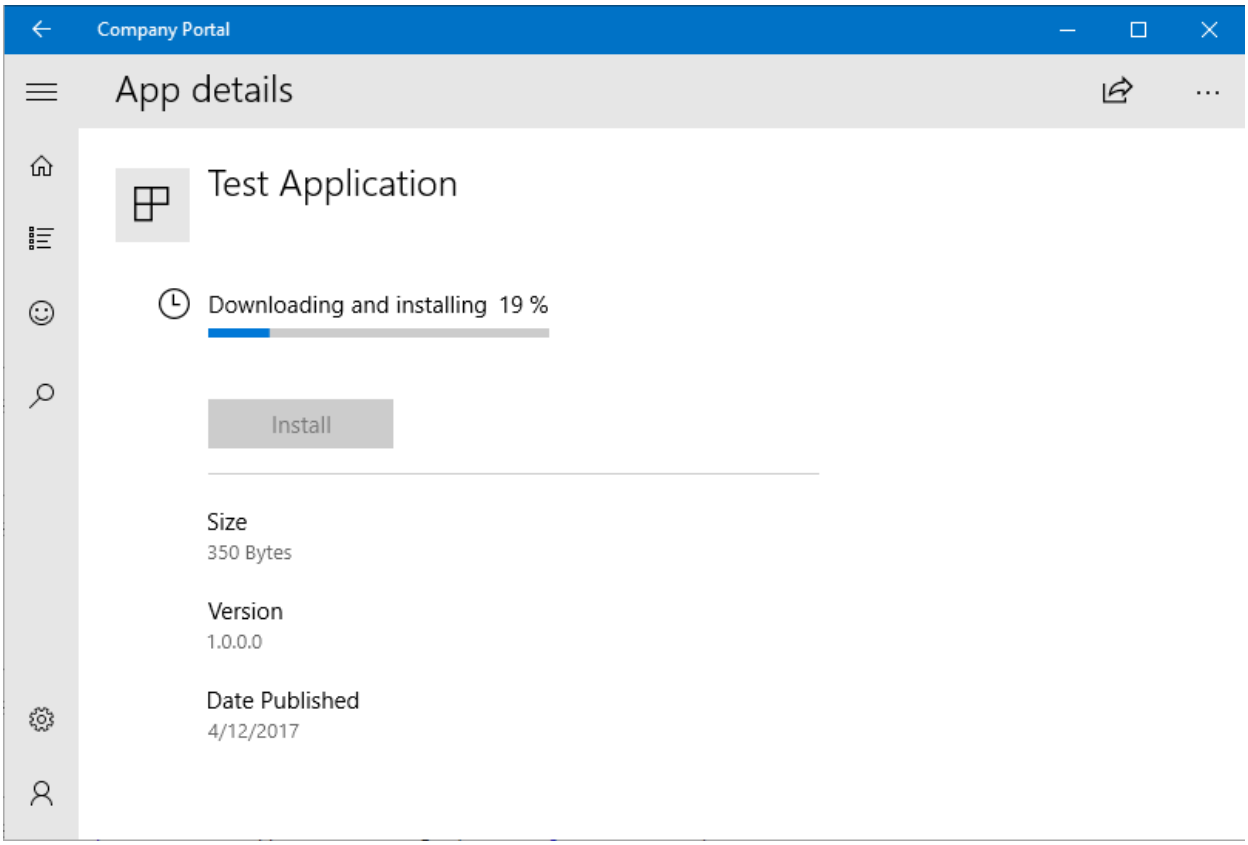
Mejora del estado de instalación de la aplicación para la aplicación Portal de empresa de Windows 10

La aplicación Portal de empresa para Windows 10 ahora proporciona una barra de progreso de la instalación en la página de detalles de la aplicación. Esto es posible en aplicaciones modernas en dispositivos que ejecutan la Actualización de aniversario de Windows 10 o superior.

Antes



Después

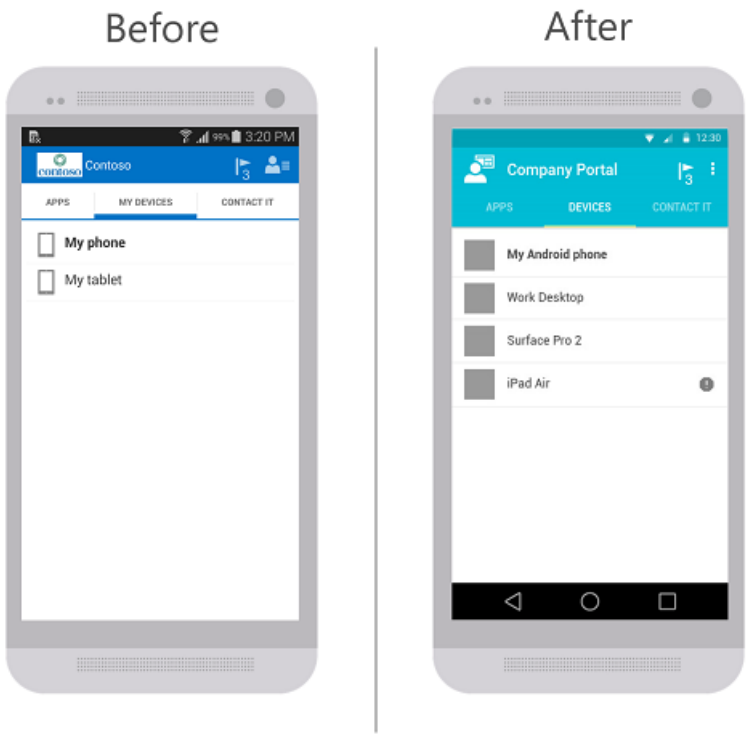


Febrero de 2017

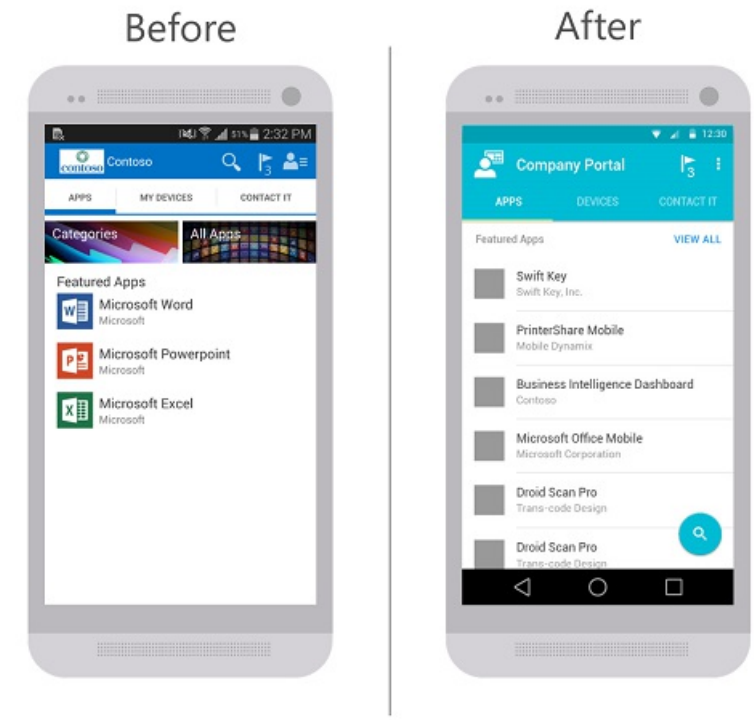
Nueva experiencia del usuario en la aplicación Portal de empresa para Android

A partir de marzo, la aplicación del portal de empresa para Android seguirá las directrices de Material Design para crear una apariencia más moderna. Esta experiencia del usuario mejorada incluye:

- **Colores**: los encabezados de pestaña pueden colorearse según la paleta de colores personalizada.



- **Interfaz**: los botones **Aplicaciones destacadas** y **Todas las aplicaciones** se han actualizado en la pestaña **Aplicaciones**. El botón **Buscar** ahora es un botón de acción flotante.

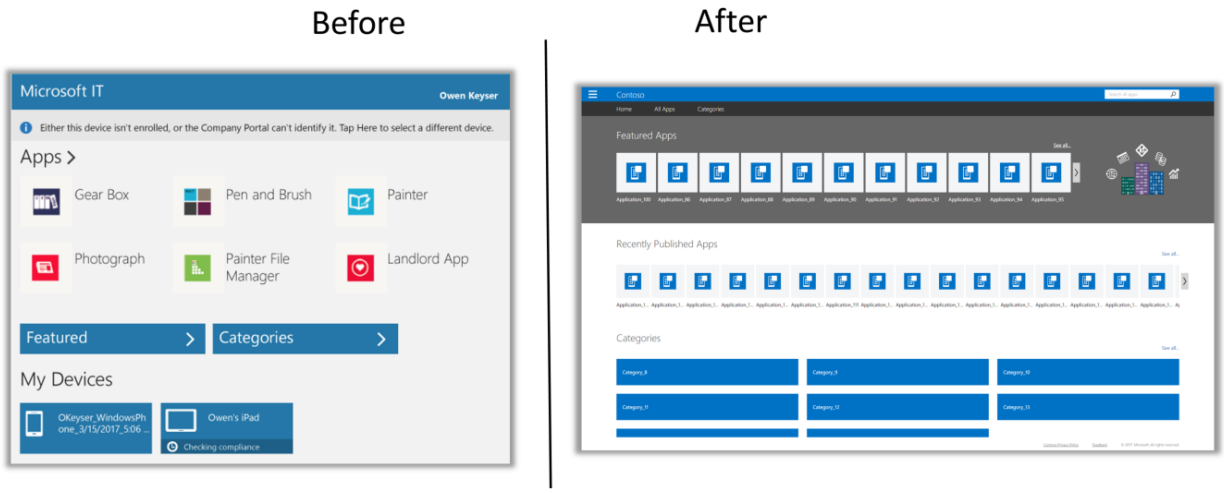


- **Navegación**: todas las aplicaciones muestran una vista con pestañas de **Destacadas**, **Todas** y **Categorías** para navegar más fácilmente. **Contactar con TI** se ha simplificado para mejorar la legibilidad.

Enero de 2017

Renovación del sitio web del portal de empresa

A partir de febrero, el sitio web del portal de empresa admitirá aplicaciones destinadas a aquellos usuarios que no tienen dispositivos administrados. El sitio web se asemejará a otros productos y servicios de Microsoft gracias a una nueva combinación de colores de contraste, ilustraciones dinámicas y un "menú hamburguesa", que contendrá los detalles de contacto del departamento de soporte técnico e información sobre los dispositivos administrados existentes. La página de inicio se reorganizará para destacar las aplicaciones que están disponibles para los usuarios, con carruseles para aplicaciones destacadas y actualizadas recientemente.



Próximamente en la interfaz de usuario

Estos son los planes para mejorar la experiencia del usuario mediante la actualización de nuestra interfaz de usuario.

> **NOTE**
> Las imágenes siguientes pueden corresponder a versiones preliminares y el producto anunciado puede diferir de las versiones presentadas.

Vea también

- Blog de Microsoft Intune
- Guía básica de la plataforma en la nube
- Novedades de Intune

En desarrollo para Microsoft Intune

14/05/2021 • 16 minutes to read

Para ayudarle con la preparación y planeación, en esta página se enumeran las actualizaciones y características de la interfaz de usuario de Intune que están en desarrollo, pero que aún no se han publicado. Además de la información de esta página:

- Si prevemos que tendrá que tomar medidas antes de realizar un cambio, haremos una publicación complementaria en el Centro de mensajes de Office.
- Cuando una característica entra en producción, ya sea una versión preliminar o disponible con carácter general, la descripción de la característica pasa de esta página a Novedades.
- Esta página y la página Novedades se actualizan periódicamente. Compruebe si hay actualizaciones adicionales.
- Consulte el plan de desarrollo de Microsoft 365 para conocer los plazos de tiempo y los productos estratégicos.

> **NOTE**
> Esta página refleja las expectativas actuales sobre las funciones de Intune en una versión futura. Las fechas y las características individuales pueden cambiar. En esta página no se describen todas las características en desarrollo.

Fuente RSS: para recibir notificaciones cuando esta página se actualice, copie y pegue la dirección URL siguiente en el lector de fuentes:

```
https://docs.microsoft.com/api/search/rss?search=%22in+development+-+microsoft+intune%22&locale=en-us
```

Este artículo se actualizó por última vez en la fecha que aparece bajo el título anterior.

Administración de aplicaciones

Exportación de los datos subyacentes de la lista de aplicaciones detectadas

Además de exportar un resumen de los datos de la lista de aplicaciones detectadas, también podrá exportar datos subyacentes más exhaustivos. La experiencia de exportación resumida actual ofrece datos agregados resumidos; sin embargo, la nueva experiencia adicional también proporcionará los datos sin procesar. Gracias a la exportación de datos sin procesar, podrá obtener todo el conjunto de datos, que se utiliza para crear el informe de datos agregados resumidos. Los datos sin procesar serán una lista de todos los dispositivos y las aplicaciones detectadas de ese dispositivo. Esta funcionalidad se va a agregar a la consola de Intune para reemplazar el conjunto de datos de inventarios de aplicaciones del almacenamiento de datos de Intune, que se quitará en la versión 2108. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Supervisar** > **Aplicaciones detectadas** > **Exportar** para mostrar las opciones de exportación. Para obtener información relacionada, consulte Aplicaciones descubiertas de Intune y Exportación de informes de Intune mediante Graph API.

Configuración de la versión máxima del sistema operativo para el inicio condicional de aplicación

Con las directivas de protección de aplicaciones de iOS de las directivas de protección de aplicaciones de Microsoft Intune, podrá agregar una nueva configuración de inicio condicional. De este modo, podrá asegurarse de que los usuarios finales no usen ninguna versión previa ni compilación beta del sistema operativo para tener acceso a los datos de la cuenta profesional o educativa. Esta configuración garantiza que se puedan examinar todas las versiones del sistema operativo antes de que los usuarios finales utilicen activamente las nuevas funciones del sistema operativo. En el Centro de administración de Microsoft Endpoint Manager, podrá

encontrar esta opción de configuración seleccionando **Aplicaciones** > **Directivas de protección de aplicaciones**. Para obtener más información, consulte Creación y asignación de directivas de protección de aplicaciones.

Configuración del dispositivo

Consulta del cumplimiento de directivas de dispositivos asociados a un inquilino en Endpoint Manager

Para administrar los dispositivos desde la nube, puede asociar la infraestructura de Configuration Manager a Endpoint Manager. Al implementar la directiva de seguridad de los puntos de conexión en los dispositivos asociados a un inquilino, podrá ver el estado de cumplimiento general de la directiva. Con los informes de nivel de dispositivo, podrá ver el estado de cumplimiento de una directiva en el nivel de dispositivo desde el Centro de administración de Microsoft Endpoint Manager.

Para obtener más información sobre lo que puede hacer en Endpoint Manager en una configuración de asociación de inquilinos, consulte Asociación de inquilinos de Microsoft Endpoint Manager.

Uso de una directiva del catálogo de configuración de un conjunto de directivas para dispositivos Windows y macOS

En Intune, puede crear una directiva mediante el catálogo de configuración, que enumera todas las opciones que puede configurar. Ahora, puede usar la directiva del catálogo de configuración dentro de un conjunto de directivas.

Para obtener más información, consulte Uso de conjuntos de directivas para agrupar colecciones de objetos de administración.

Se aplica a:

- macOS
- Windows 10 y versiones posteriores

Informe de estado por valor en el catálogo de configuración

Al usar el **catálogo de configuración**, puede ver cuántos dispositivos tienen cada uno de los estados, incluidos correcto, de conflicto y de error. Este informe incluirá un **estado por valor**, el cual:

- Mostrará el número total de dispositivos afectados por una configuración específica.
- Tendrá controles para buscar, ordenar, filtrar, exportar e ir a las páginas siguientes o anteriores.

Para obtener más información sobre el catálogo de configuración, consulte Uso del catálogo de configuración para configurar opciones en dispositivos Windows y macOS.

Nueva configuración para dispositivos iOS/iPadOS 14.5 y versiones más recientes

Al crear una directiva de restricciones de dispositivos para dispositivos iOS/iPadOS, hay nuevas opciones de configuración disponibles (Dispositivos > Perfiles de configuración > Crear perfil > iOS/iPadOS > Restricciones de dispositivos > Dispositivos conectados):

- **Block Apple Watch auto unlock** (Bloquear desbloqueo automático de Apple Watch): establezca en **Sí** para impedir que los usuarios desbloqueen su dispositivo con Apple Watch.
- **Allow users to boot devices into recovery mode with unpaired devices** (Permitir que los usuarios arranquen dispositivos en modo de recuperación con dispositivos no emparejados): establezca en **Sí** para permitir que los usuarios arranquen su dispositivo en recuperación con un dispositivo no emparejado.
- **Block Siri for dictation** (Bloquear Siri para el dictado): establezca en **Sí** para deshabilitar las conexiones a servidores de Siri para que los usuarios no puedan usar Siri para dictar texto.
- **Require devices to use Wi-Fi networks set up via configuration profiles** (Requerir que los dispositivos usen redes Wi-Fi configuradas a través de perfiles de configuración): establezca en **Sí** para requerir que los dispositivos usen solo redes Wi-Fi configuradas a través de perfiles de configuración.

Para ver las opciones que puede configurar en la actualidad, consulte Configuración de dispositivos iOS e iPadOS para permitir o restringir características mediante Intune.

Se aplica a:

- iOS/iPadOS 14.5 y versiones posteriores

Directivas del catálogo de configuración de los conjuntos de directivas

Además de los perfiles basados en plantillas, podrá agregar perfiles basados en el **catálogo de configuración** a los conjuntos de directivas. El **catálogo de configuración** es una lista de todas las opciones que puede configurar. Para crear un conjunto de directivas en el Centro de administración de Microsoft Endpoint Manager, seleccione **Dispositivos** > **Conjuntos de directivas** > **Conjuntos de directivas** > **Crear**. Para obtener más información, consulte Uso de conjuntos de directivas para agrupar colecciones de objetos de administración y Uso del catálogo de configuración para configurar las opciones de los dispositivos Windows y macOS (versión preliminar).

Administración de dispositivos

Compatibilidad con las sesiones múltiples de Windows 10 Enterprise (versión preliminar pública)

Esta compatibilidad proporcionará a los usuarios una experiencia de Windows 10 que ya conocen, quienes a su vez podrán disfrutar del mejor precio de las licencias existentes de Microsoft 365 por usuario y de sesiones múltiples. Esta próxima compatibilidad le permitirá lo siguiente:

- Hospedar varias sesiones de usuario simultáneas mediante el nuevo host de sesión de Escritorio remoto exclusivo de Windows Virtual Desktop en Azure.
- Administrar dispositivos de escritorio remotos de sesiones múltiples con configuraciones basadas en dispositivos, como un cliente de Windows 10 Enterprise compartido y sin usuario.
- Inscribir automáticamente máquinas virtuales unidas a Azure AD híbrido en Intune y establecerlas como destino mediante las aplicaciones y directivas de ámbito de sistema operativo.

Fin de la compatibilidad con la acción remota de reinicio en dispositivos Android Enterprise de propiedad corporativa con perfil de trabajo

La compatibilidad finalizará para la acción remota de **reinicio** en dispositivos de propiedad corporativa con un perfil de trabajo. El botón **Reiniciar** se quitará de la página **Dispositivo** para dispositivos de propiedad corporativa con un perfil de trabajo. Si intenta reiniciar dispositivos mediante acciones masivas de dispositivo, los dispositivos del perfil de trabajo de propiedad corporativa no se reiniciarán y esas acciones de dispositivo se notificarán como **No compatibles**. Otros tipos de dispositivos que se incluyen en la acción masiva de dispositivo se reiniciarán de forma normal para esa acción.

Asociación de inquilinos: retirada

Aunque sabemos que los clientes obtienen un gran valor al habilitar la asociación de inquilinos con Configuration Manager, hay casos excepcionales en los que es posible que tenga que retirar una jerarquía. Por ejemplo, puede que tenga que retirarse de la nube después de un escenario de recuperación ante desastres en el que se quitó el entorno local. Pronto podrá retirar un entorno de Configuration Manager del Centro de administración de Microsoft Endpoint Manager.

Aplicaciones de Intune

Los usuarios finales pueden reiniciar la instalación de una aplicación en el Portal de empresa

Con el Portal de empresa, los usuarios finales podrán reiniciar la instalación de una aplicación si parece que el progreso se ha detenido o está inmovilizado. Esta funcionalidad se permite si el progreso de la instalación de la aplicación no ha cambiado en dos horas.

El agente de administración de Intune para dispositivos macOS será una aplicación universal

Al implementar scripts de shell o atributos personalizados para dispositivos macOS desde Microsoft Endpoint Manager, se implementará la nueva versión universal de la aplicación del agente de administración de Intune que se ejecuta de forma nativa en máquinas Mac con Apple Silicon. La misma implementación instalará la versión x64 de la aplicación en máquinas Mac con Intel. Para obtener más información, consulte Agente de administración de Microsoft Intune para macOS.

Supervisión y solución de problemas

Cambios de la directiva de protección de cuentas en Seguridad de los puntos de conexión

Se va a modificar la directiva de protección de cuentas de Seguridad de los puntos de conexión para usar las nuevas API de Windows Hello para empresas. Las nuevas API darán lugar a una experiencia más coherente. La nueva API es *./Device/Vendor/MSFT/PassportForWork*, que incluye más opciones que pueden ayudar a reducir los conflictos. Esta API reemplaza el uso de *./User/Vendor/MSFT/PassportForWork*. (**Seguridad de los puntos de conexión** > **Protección de cuentas**)

Después del cambio, solo se usará la API nueva en las directivas que cree. Las directivas existentes no se verán afectadas por este cambio y seguirán usando la API anterior.

Informe organizativo centrado en la configuración del dispositivo

Vamos a publicar un nuevo informe organizativo sobre la **configuración de dispositivos**. Este informe reemplazará el informe de **estado de la asignación** del Centro de administración de Microsoft Endpoint Manager, en **Dispositivos** > **Monitor**. El informe sobre la **configuración de dispositivos** le permitirá generar una lista de perfiles en el inquilino que tengan dispositivos en un estado correcto, de error, de conflicto o no aplicable. Puede usar filtros para el tipo de perfil, el sistema operativo y el estado. Los resultados devueltos proporcionarán capacidades de búsqueda, ordenación, filtrado, paginación y exportación. Además de los detalles de configuración del dispositivo, este informe proporcionará detalles de acceso a los recursos y detalles del perfil del catálogo de nuevas opciones de configuración. Para obtener información relacionada, vea Informes de Intune.

Exportación de informes de Intune mediante la versión 1.0 de Graph API

La API de exportación de informes de Intune estará disponible en Graph v. 1.0, y seguirá estándolo en la versión beta. Para obtener información relacionada, consulte Informes de Intune y Exportación de informes de Intune mediante Graph API.

Scripting

Actualización al exportar informes de Intune mediante Graph API

Cuando use Graph API para exportar informes de Intune sin seleccionar ninguna columna para el informe de dispositivos, recibirá el conjunto de columnas predeterminado. Para reducir la confusión, a partir de enero de 2021 se quitarán algunas columnas del conjunto de columnas predeterminado. Las columnas que se quitarán son las siguientes: `PhoneNumberE164Format`, `_ComputedComplianceState`, `_OS` y `OSDescription`. Estas columnas se seguirán pudiendo seleccionar si las necesita, pero solo de forma explícita y no de manera predeterminada. Si ha configurado alguna automatización en torno a las columnas predeterminadas de la exportación de dispositivos y usa alguna de ellas, deberá refactorizar los procesos para que esas columnas y cualquier otra pertinente se seleccionen de manera explícita. Para obtener información relacionada, consulte Exportación de informes de Intune mediante Graph API.

Actualizaciones del almacenamiento de datos de Intune

La entidad `applicationInventory` se quitará del almacenamiento de datos de Intune con la actualización de servicio 2108 de Intune. Vamos a incorporar un conjunto de datos más completo y preciso que estará disponible en la interfaz de usuario y con nuestra API de exportación. Para obtener información relacionada, consulte Exportación de informes de Intune mediante Graph API.

El nuevo valor de propiedad se admitirá en la enumeración managementAgentType

El valor de propiedad `IntuneAosp` se admitirá en la enumeración `managementAgentType`. El valor `ManagementAgentTypeID` de esta propiedad será `2048`. Representa el tipo de dispositivo que administra la administración de dispositivos móviles (MDM) de Intune para dispositivos AOSP (Android Open Source Project). Para obtener información relacionada, consulte managementAgentType en la sección beta de la API de Almacenamiento de datos de Intune.

Seguridad

Nuevas opciones para las actualizaciones del servidor de puerta de enlace de Tunnel

Pronto podrá configurar algunos aspectos de las actualizaciones del servidor de puerta de enlace de Microsoft Tunnel. Podrá hacerlo en **Administración de inquilinos** > **Puerta de enlace de Microsoft Tunnel (versión preliminar)** .

Las opciones son:

- Restrinja el inicio de las actualizaciones de servidores a un período específico.
- Configure los servidores de un sitio para que se actualicen manualmente o solicite al administrador que apruebe una actualización antes de que se pueda iniciar.

También vamos a agregar una nueva configuración de comprobación del estado que lo ayudará a identificar cuándo un servidor está ejecutando la versión más reciente de la puerta de enlace de Tunnel.

Notificaciones

Estos avisos proporcionan información importante que puede ayudarle a prepararse para las características y los cambios futuros de Intune.

Actualización de los perfiles antivirus de seguridad de puntos de conexión para Windows 10

Hemos realizado un pequeño cambio para mejorar la experiencia de los perfiles antivirus para Windows 10. Esto no afecta al usuario final, ya que solo se trata de un cambio en el contenido que se muestra en la interfaz de usuario.

¿Cómo me afecta esto?

Anteriormente, al configurar un perfil de seguridad de Windows para la directiva antivirus de seguridad de puntos de conexión, tenía dos opciones para la mayoría de las configuraciones: *Sí* y *No configurado*. Ahora, esas mismas configuraciones incluyen las opciones *Sí, No configurado* y *No* (la nueva opción). Los valores configurados previamente que se hayan establecido en *No configurado* seguirán con la opción *No configurado*. Al crear perfiles o editar los existentes, ahora tiene la opción de especificar explícitamente *No*.

Además, la configuración *Hide the Virus and threat protection area in the Windows Security app* (Ocultar el área de protección contra virus y amenazas en la aplicación Seguridad de Windows) tiene una configuración secundaria, *Hide the Ransomware data recovery option in the Windows Security app* (Ocultar la opción de recuperación de datos de ransomware en la aplicación Seguridad de Windows). Si la configuración principal (Ocultar el área de protección contra virus y amenazas) se ha establecido en *No configurado* y la configuración secundaria se ha establecido en *Sí*, ambas configuraciones se establecerán en *No configurado*. Esto se aplicará al editar el perfil.

¿Qué acción debo llevar a cabo?

No se requiere ninguna acción. Sin embargo, es posible que quiera notificar este cambio a su departamento de soporte técnico.

Plan de cambio: Intune finaliza el soporte técnico del Portal de empresa en versiones no admitidas de Windows

Intune sigue el ciclo de vida de Windows 10 en las versiones compatibles de esta sistema operativo. Ahora,

estamos retirando el soporte técnico de los portales de empresa de Windows 10 asociados en esas versiones de Windows que están fuera de la directiva de soporte técnico moderno.

¿Cómo me afecta esto?

Dado que Microsoft ya no admite estos sistemas operativos, puede que este cambio no le afecte, dado que es probable que ya haya actualizado el sistema operativo o los dispositivos. Este cambio solo le afectará si sigue administrando versiones de Windows 10 no admitidas. Las versiones de Windows y del Portal de empresa afectadas son:

- Windows 10, versión 1507, Portal de empresa, versión 10.1.721.0
- Windows 10, versión 1511, Portal de empresa, versión 10.1.1731.0
- Windows 10, versión 1607, Portal de empresa, versión 10.3.5601.0
- Windows 10, versión 1703, Portal de empresa, versión 10.3.5601.0
- Windows 10, versión 1709, cualquier versión del Portal de empresa

Aunque no vamos a desinstalar estas versiones del Portal de empresa mencionadas anteriormente, las retiraremos de Microsoft Store y dejaremos de probar nuestras versiones de servicio con ellas.

Efecto para el usuario: si sigue usando una versión no admitida de Windows 10, los usuarios no podrán obtener las últimas actualizaciones de seguridad, ni nuevas características, correcciones de errores, mejoras de latencia, mejoras de accesibilidad e inversiones en rendimiento. System Center Configuration Manager e Intune no podrán administrar conjuntamente a los usuarios.

¿Qué tengo que hacer?

En el centro de administración de Microsoft Endpoint Manager, use la característica Aplicaciones detectadas para buscar aplicaciones con estas versiones. En el dispositivo de un usuario, la versión del Portal de empresa se muestra en la página **Configuración** del Portal de empresa. Actualice a una versión admitida de Windows o del Portal de empresa.

Plan de cambio: Intune avanza para admitir Android 6.0 y versiones posteriores en abril de 2021

Como se mencionó en MC234534, Intune pasará a ser compatible con Android 6.0 (Marshmallow) y versiones posteriores en el lanzamiento del servicio de abril (2104).

Cómo afectará este cambio a su organización

Dado que las aplicaciones móviles de Office para Android finalizaron la compatibilidad con Android 5.x (Lollipop) el 30 de junio de 2019 (MC181101), es posible que este cambio no le afecte; es probable que ya haya actualizado el sistema operativo o los dispositivos. Sin embargo, si tiene un dispositivo que todavía está ejecutando la versión 5.x de Android o decide inscribir cualquier dispositivo que ejecute la versión 5.x de Android, tenga en cuenta que estos dispositivos ya no se admitirán. Puede actualizarlos a la versión 6.0 de Android (Marshmallow) o una versión posterior o reemplazarlos por un dispositivo en la versión 6.0 o posterior de Android.

> **NOTE**
> Los dispositivos Android de Teams no se ven afectados por este anuncio y seguirán siendo compatibles con independencia de su versión del sistema operativo Android.

Lo que necesita para prepararse

Notifique a su departamento de soporte técnico, si procede, este próximo cambio en la compatibilidad. También tiene dos opciones de administración para ayudar a informar a los usuarios finales o a bloquear la inscripción.

1. A continuación se muestra cómo puede advertir a los usuarios finales:
   - Use una directiva de cumplimiento de dispositivos para el administrador de dispositivos Android o Android Enterprise y establezca la acción de incumplimiento para enviar un mensaje a los usuarios antes de marcarlos como no compatibles.

- Configure una opción de inicio condicional para la directiva de protección de aplicaciones con un requisito de versión de SO mínima para advertir a los usuarios.

2. A continuación se muestra cómo puede bloquear dispositivos en versiones inferiores a Android 6.0:
   - Configuración de restricciones de inscripción para impedir que se inscriban dispositivos en Android 5.x
   - Use una directiva de cumplimiento de dispositivos para el administrador de dispositivos Android o Android Enterprise para que los dispositivos en Android 5.x no sean compatibles.
   - Configure una opción de inicio condicional para la directiva de protección de aplicaciones con un requisito de versión de SO mínima para bloquear el acceso a las aplicaciones de los usuarios.

Vea también

Consulte Novedades de Microsoft Intune para obtener más información sobre los desarrollos recientes.

Novedades de Microsoft Intune

27/05/2021 • 62 minutes to read

Obtenga información sobre las novedades que se producen cada semana en Microsoft Intune en el Centro de administración de Microsoft Endpoint Manager. También puede encontrar notificaciones importantes, versiones anteriores e información sobre cómo se publican las actualizaciones del servicio de Intune.

> **NOTE**
>
> El lanzamiento de cada actualización mensual puede tardar hasta tres días y se realizará en el orden siguiente:
>
> - Día 1: Asia Pacífico (APAC)
> - Día 2: Europa, Oriente Medio y África (EMEA)
> - Día 3: América del Norte
> - Día 4+: Intune for Government
>
> Es posible que algunas características se implementen durante varias semanas y que no estén disponibles para todos los clientes la primera semana.
>
> Revise la página En desarrollo para ver una lista de las características que aparecerán en una versión próxima.

Fuente RSS: reciba notificaciones cuando esta página se actualice copiando y pegando la siguiente dirección URL en su lector de fuentes:

```
https://docs.microsoft.com/api/search/rss?search=%22What%27s+new+in+microsoft+intune%3F+-+Azure%22&locale=en-us
```

Semana del 10 de mayo de 2021

Administración de aplicaciones

Mensajería de acceso condicional mejorada para usuarios de Android e iOS/iPadOS

Azure Active Directory ha actualizado la redacción en una pantalla de acceso condicional para explicar mejor los requisitos de acceso y configuración a los usuarios. Los usuarios de Android e iOS/iPadOS verán esta pantalla cuando intenten acceder a los recursos corporativos desde un dispositivo que no esté inscrito en la administración de Intune.

Seguridad de dispositivos

Los perfiles de experiencia de seguridad de Windows admiten configuración de tres estados.

Para Windows 10 dispositivos, hemos actualizado la configuración de dos estado para que sea de tres estados en el perfil de experiencia de Seguridad de Windows para la directiva antivirus de seguridad de puntos de conexión.

La mayoría de las opciones del perfil solo admitían las dos opciones de **Sí** y **No configurado**. Ahora, esas mismas configuraciones incluyen las opciones **Sí, No configurado** y **No** (la nueva opción).

- En el caso de los perfiles existentes, los valores establecidos en *No configurado* permanecen como *No configurado*. Al crear perfiles o editar los existentes, ahora puede elegir especificar explícitamente *No*.

Además, lo siguiente se aplica a la configuración de la opción *Hide the Virus and threat protection area in the Windows Security app* (Ocultar el área de protección contra virus y amenazas en la aplicación Seguridad de Windows) y su configuración secundaria, *Hide the Ransomware data recovery option in the Windows Security app* (Ocultar la opción de recuperación de datos de ransomware en la aplicación Seguridad de Windows).

- Si la configuración principal (Ocultar el área de protección contra virus y amenazas) se ha establecido en *No*

configurado y la configuración secundaria se ha establecido en *Sí*, ambas configuraciones se establecerán en *No configurado*.

Administración de dispositivos

Uso de filtros para asignar directivas en el centro de administración de Endpoint Manager: versión preliminar pública

Hay una nueva opción, **Filtros**, que se puede usar al asignar aplicaciones o directivas a grupos. Para crear un filtro, vaya a estas ubicaciones:

- **Dispositivos** > **Filtros (versión preliminar)** > **Crear**
- **Aplicaciones** > **Filtros (versión preliminar)** > **Crear**
- **Administración de inquilinos** > **Filtros (vista previa)** > **Crear**.

Puede filtrar el ámbito de los dispositivos afectados mediante las propiedades de dispositivo. Por ejemplo, puede filtrar por la versión del sistema operativo, el fabricante del dispositivo, etc. Después de crear el filtro, puede usarlo al asignar una directiva o un perfil.

Para obtener más información, consulte Uso de filtros (versión preliminar) al asignar aplicaciones, directivas y perfiles en Microsoft Endpoint Manager.

Se aplica a:

- Administrador de dispositivos Android
- Android Enterprise
- iOS/iPadOS
- macOS
- Windows 10 y versiones posteriores

Uso de la directiva de Intune para acelerar la instalación de las actualizaciones de seguridad de Windows 10

En la versión preliminar pública, puede usar la directiva **Actualizaciones de calidad de Windows 10** de Intune para acelerar la instalación de las actualizaciones de seguridad más recientes de Windows 10 en los dispositivos que se administran en el servicio.

Al acelerar una actualización, los dispositivos pueden iniciar la descarga e instalación de la actualización lo antes posible, sin tener que esperar a que el dispositivo sincronice las actualizaciones. Aparte de acelerar la instalación de la actualización, al usar esta directiva, no se modifican los procesos ni las directivas de implementación de actualizaciones que ya tenga.

Si quiere supervisar las actualizaciones rápidas, puede usar las siguientes opciones:

- Informe de actualizaciones rápidas de Windows
- Informe de dispositivos con fallos en actualizaciones rápidas

Semana del 26 de abril de 2021 (versión del servicio 2104)

Administración de aplicaciones

Pantalla de privacidad actualizada en Portal de empresa para iOS

Hemos agregado texto adicional a la pantalla de privacidad de Portal de empresa para explicar el uso de los datos recopilados en la aplicación. Los usuarios pueden tener la certeza de que los datos recopilados solo se usan para comprobar que los dispositivos cumplen las directivas de la organización.

Estado de instalación de las aplicaciones necesarias asignadas a dispositivos

En la página **Aplicaciones instaladas** de la aplicación o el sitio web de Portal de empresa de Windows, los usuarios finales pueden ver el estado de instalación y los detalles de las aplicaciones necesarias asignadas a dispositivos. Además de esta funcionalidad, también se puede consultar el estado de la instalación y de los detalles de las aplicaciones necesarias asignadas a los usuarios. Para más información sobre el Portal de empresa de Intune, consulte Configuración de las aplicaciones del Portal de empresa de Intune, el sitio web del

Portal de empresa y la aplicación de Intune.

Visualización de la versión de aplicaciones Win32 en la consola

La versión de la aplicación Win32 ahora se muestra en el Centro de administración de Microsoft Endpoint Manager. La versión de las aplicaciones aparece en la lista **Todas las aplicaciones**, donde puede filtrar por aplicaciones Win32 y seleccionar la columna **versión** opcional. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Todas las aplicaciones** > **Columnas** > **Versión** para mostrar la versión en la lista de aplicaciones. Para obtener más información, consulte Administración de aplicaciones Win32 en Microsoft Intune.

Configuración de la versión máxima del sistema operativo para el inicio condicional de aplicación en dispositivos iOS

Con las directivas de protección de aplicaciones de Intune, se puede agregar una nueva configuración de inicio condicional para asegurarse de que los usuarios finales no usen ninguna versión previa ni compilación beta del sistema operativo para tener acceso a los datos de la cuenta profesional o educativa en dispositivos iOS. Esta configuración garantiza que se puedan examinar todas las versiones del sistema operativo antes de que los usuarios finales utilicen activamente las nuevas funciones del sistema operativo en dispositivos iOS. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Directivas de protección de aplicaciones**. Para obtener más información, consulte Creación y asignación de directivas de protección de aplicaciones.

Configuración del dispositivo

Actualización de los informes de directiva OEMConfig para dispositivos Android Enterprise

En dispositivos Android Enterprise, puede crear una directiva OEMConfig para agregar, crear y personalizar la configuración específica de OEM. Ahora, los informes de directiva se actualizan para que también se muestren correctamente en un usuario, un dispositivo y para cada opción de configuración de la directiva.

Para obtener más información, vea Uso y administración de dispositivos Android Enterprise con OEMConfig en Microsoft Intune.

Se aplica a:

- Android Enterprise

Deshabilitación del emparejamiento con NFC en dispositivos iOS/iPad con la versión 14.2 y posteriores

En los dispositivos iOS/iPadOS supervisados, puede crear un perfil de restricciones de dispositivos que deshabilite NFC (**Dispositivos** > **Perfiles de configuración**> **Crear perfil** > **iOS/iPadOS** como plataforma > **Restricciones de dispositivos** como perfil > **Dispositivos conectados** > **Disable near field communication (NFC)** [Deshabilitar NFC]). Cuando se deshabilita esta característica, se impide que los dispositivos se emparejen con otros dispositivos habilitados para NFC y se deshabilita NFC.

Para ver esta opción, vaya a Configuración de dispositivos iOS y iPadOS para permitir o restringir características mediante Intune.

Se aplica a:

- iOS/iPadOS 14.2 y versiones posteriores

Administración de dispositivos

Acción remota Buscar dispositivo para dispositivos Windows 10

Ahora puede usar una nueva acción remota Buscar dispositivo para obtener la ubicación geográfica de un dispositivo. Entre los dispositivos admitidos se incluyen:

- Windows 10, versión 20H2 (10.0.19042.789) o posteriores
- Windows 10, versión 2004 (10.0.19041.789) o posteriores
- Windows 10, versión 1909 (10.0.18363.1350) o posteriores
- Windows 10, versión 1809 (10.0.17763.1728) o posteriores

Para ver la nueva acción, inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft y elija **Dispositivos** > **Windows** > seleccione uno con Windows 10 > **Buscar dispositivo**.

Esta acción funcionará de manera similar a la acción actual Buscar dispositivo para los dispositivos Apple (pero no incluirá ninguna funcionalidad del modo Perdido).

Los servicios de ubicación deben estar habilitados en los dispositivos para que esta acción remota funcione. Si Intune no puede obtener la ubicación del dispositivo y el usuario ha establecido una ubicación predeterminada en la configuración del dispositivo, se mostrará la ubicación predeterminada.

Microsoft Endpoint Manager deja de ser compatible con Android 5.x

Microsoft Endpoint Manager ya no admite dispositivos Android 5.x.

Compatibilidad para mostrar los números de teléfono de los dispositivos corporativos con Android Enterprise

En el caso de los dispositivos corporativos con Android Enterprise (dedicados, totalmente administrados y totalmente administrados con un perfil de trabajo), los números de teléfono del dispositivo asociado ahora se muestran en el Centro de administración de Microsoft Endpoint Manager. Si hay varios números asociados al dispositivo, solo se mostrará un número.

Compatibilidad con la propiedad EID para dispositivos iOS/iPadOS

El identificador de eSIM (EID) es un identificador único para la SIM insertada (eSIM). La propiedad EID ahora aparece en la página de detalles de hardware para dispositivos iOS/iPadOS.

Compatibilidad de Intune con el aprovisionamiento de dispositivos compartidos de Azure Active Directory

La capacidad de aprovisionar dispositivos de Android Enterprise dedicados con Microsoft Authenticator configurado automáticamente en el modo de dispositivo compartido de Azure AD ya está disponible con carácter general. Para más información sobre cómo usar este tipo de inscripción, consulte Configuración de la inscripción en Intune de dispositivos dedicados de Android Enterprise.

Visualización de los detalles del final del soporte técnico para los perfiles de actualización de características

Para ayudarle a planear el fin del servicio para las actualizaciones de características de Windows 10 que implemente con Intune, hemos agregado dos nuevas columnas de información a los perfiles de actualizaciones de características en el Centro de administración de Microsoft Endpoint Manager.

La primera columna nueva muestra un estado que señala el momento en que la actualización del perfil está cerca o ha llegado a su fin de servicio, y la segunda columna muestra esa fecha de fin de servicio. Cuando una actualización llega a su fin de servicio, ya no se implementa en los dispositivos y la directiva se puede quitar de Intune.

Las nuevas columnas y detalles incluyen:

- **Soporte técnico** - Esta columna muestra el estado de la actualización de características:
  - **Con soporte**: la actualización tiene soporte para la distribución.
  - **Fin del soporte**: la actualización está a menos de dos meses de su fecha de fin de servicio.
  - **Sin soporte:** la actualización ya no tiene soporte, después de haber alcanzado su fecha de finalización del servicio.
- **Fecha de finalización del soporte técnico** -Esta columna muestra la fecha de fin del servicio para la actualización de características en el perfil.

Para obtener información sobre las fechas de fin de servicio de las versiones de Windows 10, consulte Información de versión de Windows 10 en la documentación sobre el estado de la versión de Windows.

Seguridad de dispositivos

Uso de perfiles de Antivirus para evitar o permitir la combinación de listas de exclusión de antivirus en dispositivos

Ahora puede configurar **Combinación de administradores locales de Defender** como parámetro en un perfil de *Antivirus de Microsoft Defender* para bloquear la combinación de listas de exclusión locales para

Antivirus de Microsoft Defender en dispositivos con Windows 10.

Las listas de exclusión de Antivirus de Microsoft Defender se pueden configurar localmente en un dispositivo y se especifican mediante la directiva de antivirus de Intune:

- Cuando se combinan listas de exclusión, las exclusiones definidas localmente se combinan con las de Intune.
- Cuando se bloquea la combinación, las exclusiones de la directiva serán las únicas efectivas en el dispositivo.

Para obtener más información sobre esta configuración y los valores relacionados, vea Exclusiones del antivirus de Microsoft Defender.

Flujo mejorado para el acceso condicional en dispositivos Surface Duo

Hemos optimizado el flujo de acceso condicional en dispositivos Surface Duo. Estos cambios se realizan automáticamente y no requieren ninguna actualización de la configuración por parte de los administradores. (**Seguridad de los puntos de conexión** > **Acceso condicional**)

En un dispositivo Duo:

- Cuando el acceso condicional bloquea el acceso a un recurso, ahora se redirige a los usuarios a la aplicación Portal de empresa que estaba preinstalada en el dispositivo. Anteriormente, se enviaban a la lista de aplicaciones de Google Play Store de la aplicación Portal de empresa.
- En el caso de los dispositivos inscritos como perfil de trabajo de propiedad personal, cuando un usuario intenta iniciar sesión en una versión personal de una aplicación con sus credenciales profesionales, ahora se les envía a la versión profesional de Portal de empresa en la que se muestran mensajes con instrucciones. Anteriormente, se enviaba al usuario al anuncio de la versión personal de la aplicación Portal de empresa en Google Play Store, donde tenía que volver a habilitarla para ver los mensajes con instrucciones.

Configuración de las opciones que se aplican a las actualizaciones del servidor de puerta de enlace de Tunnel

Hemos agregado opciones para ayudarle a administrar la actualización de los servidores de puerta de enlace de Microsoft Tunnel. Las nuevas opciones se aplican a la configuración de Sitios e incluyen:

- Establezca una ventana de mantenimiento para cada sitio de túnel. La ventana define cuándo los servidores de túnel asignados a ese sitio pueden empezar a actualizarse.
- Configure el tipo de actualización del servidor, que determina el modo en que todos los servidores del sitio proceden con las actualizaciones. Puede elegir entre:
  - **Automático**: todos los servidores del sitio se actualizarán lo antes posible después de que esté disponible una nueva versión del servidor.
  - **Manual**: los servidores del sitio solo se actualizarán después de que un administrador elija explícitamente permitir la actualización.
- La pestaña Comprobación de estado ahora muestra el estado de la versión de software del servidor para ayudarlo a comprender en qué momento el software del servidor de túnel está obsoleto. El estado incluye lo siguiente:
  - **Correcto**: actualizado con la versión de software más reciente.
  - **Advertencia**: una versión por detrás
  - **Incorrecto**: dos o más versiones por detrás

Aplicaciones de Intune

Nuevas aplicaciones protegidas disponibles para Intune

Las siguientes aplicaciones protegidas ya están disponibles para Microsoft Intune:

- Omnipresence Go de Omnipresence Technologies, Inc.
- Comfy de Building Robotics, Inc.
- M-Files for Intune de M-Files Corporation

Para obtener más información sobre las aplicaciones protegidas, vea Aplicaciones protegidas de Microsoft Intune.

Supervisión y solución de problemas

Nueva interfaz de usuario para filtrar los datos de nuevos informes operativos

Los nuevos informes operativos ahora admitirán una nueva interfaz de usuario para agregar filtros de datos. La nueva gama de filtros ofrece una experiencia mejorada para ayudar a segmentar, refinar y ver los datos de los informes. Para obtener más información sobre los informes en Intune, vea Informes de Intune.

El informe de frecuencia de reinicio de Windows en el análisis de puntos de conexión está disponible con carácter general

Actualmente, el rendimiento de inicio de análisis de puntos de conexión proporciona al equipo de TI información para medir y optimizar los tiempos de arranque del equipo. Sin embargo, la frecuencia de reinicio puede tener un gran impacto en la experiencia del usuario, en el sentido de que un dispositivo que se reinicia diariamente debido a las pantallas azules proporcionará una experiencia de usuario deficiente, incluso si los tiempos de arranque son rápidos. Ahora, hemos incluido un informe en las frecuencias de reinicio de la organización para ayudarle a identificar los dispositivos problemáticos. Para obtener más información, vea Frecuencia de reinicio en análisis de puntos de conexión.

Semana del 12 de abril de 2021

Configuración del dispositivo

Nuevo método de autenticación moderna con el Asistente para la configuración de Apple (versión preliminar pública)

Ahora, al crear un perfil de inscripción de dispositivos automatizada, puede elegir un nuevo método de autenticación: **Setup Assistant with modern authentication** (Asistente para configuración con autenticación moderna). Este método proporciona toda la seguridad del Asistente para configuración, pero evita el problema de que los usuarios finales no puedan usar el dispositivo mientras Portal de empresa se instala en el dispositivo. El usuario tiene que autenticarse mediante la autenticación multifactor de Azure AD durante las pantallas del Asistente para configuración. Para ello, se necesitará un inicio de sesión adicional de Azure AD después la inscripción en la aplicación Portal de empresa para acceder a los recursos corporativos protegidos por el acceso condicional. La versión de Portal de empresa correcta se enviará automáticamente como una aplicación obligatoria al dispositivo para iOS/iPadOS. Para macOS, estas son las opciones disponibles para obtener Portal de empresa en el dispositivo: Adición de la aplicación Portal de empresa para macOS.

La inscripción se completa cuando los usuarios llegan a la pantalla principal, y estos pueden usar libremente el dispositivo con los recursos que no están protegidos por el acceso condicional. La afinidad de usuario se establece cuando el usuario llega a la pantalla principal después de las pantallas de configuración; sin embargo, el dispositivo no se registrará completamente con AAD hasta el inicio de sesión en el Portal de empresa. El dispositivo no aparecerá en la lista de dispositivos de un usuario determinado en el portal de AAD hasta el inicio de sesión en el Portal de empresa. Si el inquilino tiene activada la autenticación multifactor para estos dispositivos o usuarios, se les pedirá que completen la autenticación multifactor durante la inscripción en el Asistente de configuración. La autenticación multifactor no es necesaria, pero está disponible para este método de autenticación dentro del acceso condicional si es necesario.

Este método tiene las siguientes opciones para instalar Portal de empresa:

- Para iOS/iPadOS: la opción **Instalar Portal de empresa** no se mostrará al elegir este flujo para iOS/iPad. Una vez que el usuario final llegue a la pantalla principal, Portal de empresa será una aplicación obligatoria en el dispositivo con la directiva de configuración de aplicaciones correcta aplicada. El usuario debe iniciar sesión con las credenciales de Azure AD en Portal de empresa después de inscribirse para obtener acceso a los recursos protegidos por el acceso condicional y estar plenamente registrado en AAD.
- Para macOS: los usuarios deben iniciar sesión en Portal de empresa para completar el registro de Azure AD y obtener acceso a los recursos protegidos por el acceso condicional. El usuario final podrá usar Portal de empresa sin problemas después de llegar a la página principal, pero tendrá que realizar un inicio de sesión

adicional en Portal de empresa para acceder a los recursos corporativos y cumplir las directivas. Para obtener más información, consulte Adición de la aplicación Portal de empresa de macOS.

Para obtener información sobre cómo usar este método de autenticación en dispositivos iOS/iPadOS, consulte Inscripción automática de dispositivos iOS/iPadOS mediante la inscripción de dispositivos automatizada de Apple.

Para obtener información sobre cómo usar este método de autenticación en dispositivos macOS, consulte Inscripción automática de dispositivos macOS con Apple Business Manager o Apple School Manager.

Semana del 29 de marzo de 2021 (versión del servicio 2103)

Administración de aplicaciones

El agente de administración de Intune para dispositivos macOS es ahora una aplicación universal.

Al implementar scripts de shell o atributos personalizados para dispositivos macOS desde Microsoft Endpoint Manager, se implementará la nueva versión universal de la aplicación del agente de administración de Intune que se ejecuta de forma nativa en máquinas Mac con Apple Silicon. La misma implementación instalará la versión x64 de la aplicación en máquinas Mac con Intel. Se requiere Rosetta 2 para ejecutar la versión x64 (Intel) de las aplicaciones en equipos Mac con Apple Silicon. Para instalar Rosetta 2 en los equipos Mac con Apple Silicon de forma automática, puede implementar un script de shell en Endpoint Manager. Para obtener más información, vea Agente de administración de Microsoft Intune para macOS.

Seguridad de dispositivos

Actualización de Microsoft Tunnel

Hemos publicado una nueva versión de Puerta de enlace de Microsoft Tunnel, que incluye los siguientes cambios:

- Varias mejoras y correcciones de errores.

El servidor de Puerta de enlace de Microsoft Tunnel se actualizará automáticamente a la nueva versión.

Semana del 22 de marzo de 2021 (versión del servicio 2103)

Administración de aplicaciones

Las aplicaciones de Microsoft 365 para dispositivos macOS son ahora aplicaciones universales

Al implementar aplicaciones de Microsoft 365 para dispositivos macOS desde Microsoft Endpoint Manager, ahora se implementará la nueva versión universal de la aplicación que se ejecuta de forma nativa en los equipos Mac con Apple Silicon. La misma implementación instalará las versiones x64 de la aplicación en los equipos Mac con Intel y macOS 10.14 y versiones posteriores. Para agregar aplicaciones de Microsoft 365 para macOS, en el Centro de administración de Microsoft Endpoint Manager > **Aplicaciones** > **Agregar todas las aplicaciones** > **Agregar**. Seleccione **macOS** en la lista **Tipo de aplicación**, en **Aplicaciones de Microsoft 365**. Para obtener información relacionada, consulte Asignación de Microsoft 365 a dispositivos macOS con Microsoft Intune.

Claves de configuración adicionales para la aplicación Microsoft Launcher

Ahora podrá establecer la configuración de la carpeta de Microsoft Launcher en los dispositivos totalmente administrados de propiedad corporativa con Android Enterprise. Al usar valores de claves de configuración y la directiva de configuración de aplicaciones, podrá establecer valores para la forma de carpeta, para la carpeta abierta en el modo de pantalla completa y para la dirección de desplazamiento de la carpeta. Además, ahora podrá situar la carpeta en la pantalla principal, además de colocar aplicaciones y vínculos web. Además, puede permitir que los usuarios finales modifiquen los valores de estilo de la carpeta desde la aplicación. Para obtener más información sobre Microsoft Launcher, consulte Configuración de Microsoft Launcher para Android Enterprise con Intune.

Configuración del dispositivo

Más opciones y categorías de Microsoft Edge quitadas del catálogo de configuración de macOS

En los dispositivos macOS, puede usar el catálogo de configuración para configurar Microsoft Edge, versión 77 y posteriores (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** en Plataforma > **Settings Catalog** [Catálogo de configuración]).

En esta versión:

- Se han agregado más opciones de configuración de Microsoft Edge.
- Las categorías de configuración se han quitado temporalmente. Para buscar una configuración concreta, use la categoría **Microsoft Edge - Todo** o busque el nombre de la configuración. Para ver una lista de opciones de configuración, Microsoft Edge: directivas es un buen recurso.

Para obtener más información sobre el catálogo de configuración, consulte Uso del catálogo de configuración para configurar opciones.

Se aplica a:

- macOS
- Microsoft Edge

La configuración de Windows 10 en la nube está disponible como un escenario guiado

La configuración de Windows 10 en la nube es una configuración de dispositivo para Windows 10 recomendada por Microsoft. La configuración de Windows 10 en la nube está optimizada para la nube y está diseñada para usuarios con necesidades de flujos de trabajo específicas.

Hay un escenario guiado que agrega las aplicaciones automáticamente y crea las directivas que configuran los dispositivos con Windows 10 en una configuración en la nube.

Para obtener más información, consulte Escenario guiado para la configuración de Windows 10 en la nube.

Se aplica a:

- Windows 10 y versiones posteriores

Administración de dispositivos

Aumento del número máximo recomendado de dispositivos iOS/iPadOS y macOS por token de inscripción

Anteriormente, se recomendaba no superar la cifra de 60 000 dispositivos iOS/iPadOS o macOS por token de inscripción de dispositivos automatizada (ADE). Este límite recomendado se ha aumentado a 200 000 dispositivos por token. Para obtener más información sobre los tokens de ADE, consulte Inscripción automática de dispositivos iOS/iPadOS mediante la inscripción de dispositivos automatizada de Apple.

Actualización de los nombres de columna en la vista Todos los dispositivos y en el informe de exportación

Para reflejar con precisión los datos en las columnas, hemos actualizado los nombres de columna en la vista Todos los dispositivos y en el informe de exportación para que "Primary User UPN" (UPN del usuario primario), "Dirección de correo electrónico del usuario primario" y "Nombre para mostrar del usuario primario".

Fin de la compatibilidad con Internet Explorer 11

Intune finalizará la compatibilidad con el acceso de administrador de Internet Explorer 11 a la interfaz de usuario de la aplicación web del portal de administración el 31 de marzo de 2021. Pásese a Edge u otro explorador compatible antes de ese momento para administrar cualquiera de los servicios de Microsoft basados en Azure.

Seguridad de dispositivos

Detalles del estado de mantenimiento de los servidores de puerta de enlace de Microsoft Tunnel

Hemos agregado la capacidad de ver información detallada del estado de mantenimiento de los servidores de puerta de enlace de Tunnel en el Centro de administración de Microsoft Endpoint Manager.

En la nueva pestaña nueva *Comprobación de estado*, verá la siguiente información:

- Última protección: la última vez que se protegió el servidor con Intune.

- Número de conexiones actuales: el número de conexiones activas en la última sincronización.
- Rendimiento: los megabits por segundo que atraviesan la NIC servidora en la última sincronización.
- Uso de CPU: el promedio de uso de CPU.
- Uso de memoria: el promedio de uso de memoria.
- Latencia: el tiempo promedio para que los paquetes IP atraviesen la NIC.
- Estado de expiración del certificado TLS y días antes de la expiración: cuánto tiempo el certificado TLS que protege la comunicación entre cliente y servidor para que el túnel siga siendo válido.

Versión preliminar pública de la funcionalidad de cliente de Tunnel en la aplicación Microsoft Defender para punto de conexión para Android

Tal como se anunció en Ignite, la funcionalidad de cliente de Microsoft Tunnel se está migrando a la aplicación Microsoft Defender para punto de conexión. Con esta versión preliminar, puede empezar a usar una versión preliminar de Microsoft Defender para punto de conexión como aplicación de Tunnel para los dispositivos compatibles. El cliente de Tunnel existente sigue estando disponible, pero finalmente se eliminará en favor de la aplicación Defender para punto de conexión.

Esta versión preliminar pública se aplica a:

- Android Enterprise
  - Totalmente administrado
  - Perfil de trabajo de propiedad corporativa
  - Perfil de trabajo de propiedad personal

En esta versión preliminar, debe participar para obtener acceso a la versión preliminar de Microsoft Defender para punto de conexión y, a continuación, migrar los dispositivos compatibles desde la aplicación cliente de Tunnel independiente a la aplicación en versión preliminar. Para obtener más información, consulte Migración a la aplicación Microsoft Defender para Endpoint.

Aplicaciones de Intune

Claves de configuración de Microsoft Launcher

En el caso de los dispositivos Android Enterprise totalmente administrados, la aplicación Microsoft Launcher para Intune proporcionará una personalización adicional. En el iniciador, puede configurar el conjunto de aplicaciones y vínculos web que se muestran, así como el orden de estas aplicaciones y vínculos web. La lista de aplicaciones y la posición (orden) de las configuraciones de la aplicación se han combinado para simplificar la personalización de la pantalla principal. Para obtener más información, vea Configuración de Microsoft Launcher.

Microsoft Edge para dispositivos macOS será una aplicación universal

Al implementar Microsoft Edge para dispositivos macOS desde Microsoft Endpoint Manager, se implementará la nueva versión universal de la aplicación que se ejecuta de forma nativa en los equipos Mac con Apple Silicon. La misma implementación instalará la versión x64 de la aplicación en los equipos Mac con Intel. Para agregar aplicaciones de Microsoft Edge para macOS, en el Centro de administración de Microsoft Endpoint Manager > **Aplicaciones** > **Agregar todas las aplicaciones** > **Agregar**. En la lista **Tipo de aplicación**, en **Microsoft Edge, versión 77 y posteriores**, seleccione **macOS**. Para obtener más información, consulte Adición de Microsoft Edge a dispositivos macOS con Microsoft Intune.

Nuevas aplicaciones protegidas disponibles para Intune

Las siguientes aplicaciones protegidas ya están disponibles para Microsoft Intune:

- FleetSafer de Cogosense Technology Inc.
- Senses de Mazrica Inc.
- Fuze Mobile para Intune de Fuze, Inc.
- MultiLine para Intune de Movius Interactive Corporation

Para obtener más información sobre las aplicaciones protegidas, vea Aplicaciones protegidas de Microsoft

Intune.

Mejora de la experiencia de notificación en la aplicación Portal de empresa de iOS/iPadOS

La aplicación Portal de empresa ahora puede almacenar y mostrar las notificaciones de inserción enviadas a los dispositivos iOS/iPadOS de los usuarios desde el Centro de administración de Microsoft Endpoint Manager. Los usuarios que hayan optado por recibir notificaciones de inserción del Portal de empresa pueden ver y administrar los mensajes almacenados personalizados que envíe a sus dispositivos en la pestaña **Notificaciones** del Portal de empresa. Para obtener información relacionada, vea Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune.

Scripting

Exportación de datos de informe localizados de Intune mediante Graph API

Ahora podrá especificar que los datos del informe que exporte mediante la API de exportación de informes de Microsoft Endpoint Manager solo pueden contener columnas localizadas, o bien columnas localizadas y no localizadas. La opción de columnas localizadas y no localizadas se seleccionará de forma predeterminada para la mayoría de los informes, lo que impedirá cambios importantes. Para obtener información relacionada sobre los informes, consulte Exportación de informes de Intune mediante Graph API e Informes y propiedades de Intune mediante Graph.

Semana del 8 de marzo de 2021

Configuración del dispositivo

Versión nueva del conector de certificados PFX

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2101.16.0**. Esta actualización agrega mejoras en el flujo de creación de PFX para evitar la duplicación de archivos de solicitud de certificado en servidores locales que hospedan el conector.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, consulte Conectores de certificados.

Semana del 1 de marzo de 2021 (versión del servicio 2102)

Administración de aplicaciones

Compatibilidad con la sustitución de aplicaciones Win32 en Intune

Hemos habilitado una versión preliminar pública de sustitución de aplicaciones en Intune. Ahora, se pueden crear relaciones de sustitución entre aplicaciones, lo que permite actualizar y reemplazar las aplicaciones Win32 existentes por versiones más recientes de esa misma aplicación o por aplicaciones Win32 completamente diferentes. Para obtener más información, vea Sustitución de aplicaciones Win32.

Configuración de la versión máxima del sistema operativo para el inicio condicional de aplicación en dispositivos Android

Con las directivas de protección de aplicaciones de Intune, se puede agregar una nueva configuración de inicio condicional para asegurarse de que los usuarios finales no usen ninguna versión previa ni compilación beta del sistema operativo para tener acceso a los datos de la cuenta profesional o educativa en dispositivos Android. Esta configuración garantiza que se puedan examinar todas las versiones del sistema operativo antes de que los usuarios finales utilicen activamente las nuevas funciones del sistema operativo en dispositivos Android. En el Centro de administración de Microsoft Endpoint Manager, podrá encontrar esta opción de configuración seleccionando **Aplicaciones** > **Directivas de protección de aplicaciones**. Para obtener más información, consulte Creación y asignación de directivas de protección de aplicaciones.

Configuración del dispositivo

Uso de Cisco AnyConnect como un tipo de conexión VPN para Windows 10 y Windows Holographic for Business

Se pueden crear perfiles de VPN mediante Cisco AnyConnect como un tipo de conexión (**Dispositivos** > **Configuración de dispositivo** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **VPN** para el perfil > **Cisco AnyConnect** para el tipo de conexión) sin necesidad de usar perfiles

personalizados.

Esta directiva usa la aplicación Cisco AnyConnect disponible en Microsoft Store, y no la aplicación de escritorio de Cisco AnyConnect.

Para obtener más información sobre los perfiles de VPN en Intune, consulte Creación de perfiles de VPN para conectarse a servidores VPN.

Se aplica a:

- Windows 10 y versiones posteriores
- Windows Holographic for Business

Ejecución de Microsoft Edge, versión 87 y versiones más recientes, en el modo de pantalla completa de una sola aplicación en dispositivos con Windows 10

En los dispositivos Windows 10 y versiones más recientes, configure un dispositivo para que se ejecute como una pantalla completa que ejecuta una o varias aplicaciones (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Windows 10 y versiones posteriores** > para la plataforma **Plantillas** > **Pantalla completa**). Al seleccionar el modo de aplicación única, puede:

- Ejecutar la versión 87 y posteriores de Microsoft Edge.
- Seleccione **Add Microsoft Edge legacy browser** (Agregar explorador de Microsoft Edge [versión heredada]) para ejecutar la versión 77 y anteriores de Microsoft Edge.

Para obtener más información sobre las opciones que puede configurar en el modo de pantalla completa, consulte Configuración de dispositivos con Windows 10 y versiones más recientes para ejecutarse como una pantalla completa.

Se aplica a:

- Windows 10 y versiones más recientes en el modo de pantalla completa de una sola aplicación
- Versión 87 de Microsoft Edge y versiones posteriores
- Microsoft Edge versión 77 y anteriores

Plantillas administrativas está disponible en el catálogo de configuración y tiene más opciones de configuración

En Intune, puede usar plantillas administrativas para crear directivas (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Plantillas administrativas** para el perfil).

En el catálogo de configuración, plantillas administrativas también están disponibles y tiene más opciones de configuración (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Catálogo de configuración** para el perfil).

Con esta versión, los administradores pueden configurar otras opciones que solo existían en la directiva de grupo local, y que no estaban disponibles en MDM basado en la nube. Estas opciones están disponibles para compilaciones de puntos de conexión del cliente **Windows Insider**, y tienen portabilidad con versiones anteriores de Windows en el mercado, como 1909, 2004 o 2010.

Si quiere crear plantillas administrativas y usar todas las opciones de configuración disponibles expuestas por Windows, use el catálogo de configuración.

Para más información, consulte:

- Uso de plantillas de Windows 10 para configurar los valores de directiva de grupo
- Uso del catálogo de configuración para configurar opciones

Se aplica a:

- Windows 10 y versiones posteriores

Inscripción de dispositivos

Estado de sincronización de tokens del programa de inscripción

Se ha quitado el estado de sincronización de los tokens de inscripción de dispositivos automatizados que figuran en el panel **Tokens del programa de inscripción** para evitar posibles confusiones. Sí se sigue mostrando la información por token. Los tokens del programa de inscripción se usan para administrar la inscripción automática de dispositivos con Apple Business Manager y Apple School Manager. En el centro de administración de Microsoft Endpoint Manager, encontrará la lista de tokens para dispositivos iOS/iPadOs si selecciona **Dispositivos** > **iOS/iPadOs** > **Inscripción de iOS/iPad** > **Tokens del programa de inscripción**. Para encontrar la lista de tokens para dispositivos macOS, seleccione **Dispositivos** > **macOS** > **Inscripción de macOS** > **Tokens del programa de inscripción**. Para obtener información relacionada, vea Inscripción automática de dispositivos iOS/iPadOs e Inscripción automática de dispositivos macOS.

Administración de dispositivos

Acción remota Recopilar diagnósticos

Una nueva acción remota, **Recopilar diagnósticos**, permite recopilar registros de los dispositivos corporativos sin interrumpir ni esperar al usuario final. Los registros recopilados engloban MDM, Autopilot, visores de eventos, claves, cliente de Configuration Manager, redes y otros registros de solución de problemas críticos. Para obtener más información, vea Recopilación de diagnósticos desde un dispositivo Windows.

Nuevas opciones para exportar datos de dispositivos

Estas son las nuevas opciones que hay disponibles al exportar datos de dispositivos:

- Solo se incluyen las columnas seleccionadas en el archivo exportado.
- Incluya todos los datos de inventario en el archivo exportado. Para ver estas opciones, vaya a Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **Todos los dispositivos** > **Exportar**.

Seguridad de los dispositivos

Uso de la variable CN={{UserPrincipalName}} en el asunto y la SAN de los perfiles de certificado SCEP y PKCS de dispositivos empresariales Android

Ahora, se puede usar la variable de atributo de usuario **CN={{UserPrincipalName}}** en el asunto o SAN de un perfil de certificado PKCS o un perfil de certificado SCEP de los dispositivos Android. Esta compatibilidad requiere que el dispositivo tenga un usuario, como los dispositivos inscritos del siguiente modo:

- Android Enterprise totalmente administrado
- Perfil de trabajo de propiedad personal de Android Enterprise

No se pueden usar atributos de usuario en dispositivos que carezcan de asociaciones de usuario, por ejemplo, en dispositivos que estén inscritos como dedicados de Android Enterprise. Por ejemplo, un perfil que use *CN={{UserPrincipalName}}* en el asunto o SAN no podrá obtener el nombre principal de usuario cuando no haya ningún usuario en el dispositivo.

Uso de directivas de protección de aplicaciones de Defender para punto de conexión en Android e iOS

Ahora, se puede usar Microsoft Defender para punto de conexión en las directivas de protección de aplicaciones de dispositivos que ejecutan Android o iOS.

- Configure la directiva de inicio condicional de MAM para incluir señales de **Nivel de amenaza máximo permitido** de Microsoft Defender para punto de conexión en dispositivos iOS y Android.
- Elija **Bloquear el acceso** o **Borrar datos** en función de si el dispositivo cumple el nivel de amenaza esperado.

Con esta configuración en vigor, se pedirá a los usuarios finales que instalen y configuren la aplicación **Microsoft Defender para punto de conexión** desde la tienda de aplicaciones correspondiente. Como requisito previo, debe configurar el conector de **Microsoft Defender para punto de conexión** y poner el conmutador en posición activa para enviar datos de riesgo a las directivas de protección de las aplicaciones. Para obtener información relacionada, vea Introducción general a las directivas de protección de aplicaciones y Uso de Microsoft Defender para punto de conexión en Microsoft Intune.

Configuración de reglas de reducción de la superficie expuesta a ataques para impedir que el malware obtenga persistencia a través de WMI

Ahora, la regla **Bloqueo de la persistencia a través de la suscripción de eventos WMI** se puede configurar como parte de un perfil de Reglas de reducción de la superficie expuesta a ataques en la seguridad del punto de conexión.

Esta regla impide que el malware abuse de WMI para lograr persistencia en un dispositivo. Las amenazas sin archivo emplean varias tácticas para permanecer ocultas, evitar ser detectadas en el sistema de archivos y obtener el control de la ejecución periódica. Algunas amenazas pueden abusar del repositorio WMI y el modelo de eventos para permanecer ocultas.

Si se configura como una configuración de la directiva *Reducción de la superficie expuesta a ataques* para la seguridad del punto de conexión, están disponibles las siguientes opciones:

- **Sin configurar** (valor predeterminado): la opción devuelve al valor predeterminado de Windows, que es desactivado y con la persistencia sin bloquear.
- **Bloquear**: se bloquea la persistencia a través de WMI.
- **Auditar**: evalúa cómo afecta esta regla a su organización si está habilitada (establecida en Bloquear).
- **Deshabilitar**: desactiva esta regla. La persistencia no está bloqueada.

Esta regla no admite la opción *WARN* y también está disponible como una opción de configuración de dispositivo en el catálogo de configuración.

Aplicaciones de Intune

Mejora del rendimiento de carga del sitio web del Portal de empresa

Para mejorar el rendimiento de la carga de página, ahora los iconos de la aplicación se cargarán en lotes. Los usuarios finales pueden ver un icono de marcador de posición para algunas de sus aplicaciones al visitar el sitio web del Portal de empresa. Los iconos relacionados se cargarán poco después. Para más información sobre el Portal de empresa de Intune, consulte Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune y Administrar aplicaciones desde el sitio web del Portal de empresa.

Supervisión y solución de problemas

Análisis de puntos de conexión en Puntuación de productividad de Microsoft

Hay una nueva página de análisis de puntos de conexión en Puntuación de productividad de Microsoft donde se comparte información de nivel de organización con los demás roles fuera del administrador de puntos de conexión de Microsoft. Es fundamental comprender el modo en que los dispositivos contribuyen a la experiencia de los usuarios finales para que estos puedan alcanzar sus objetivos. Para obtener más información, vea Análisis de puntos de conexión en Puntuación de productividad de Microsoft.

Informe de confiabilidad de la aplicación en análisis de puntos de conexión

Un nuevo informe, **Confiabilidad de la aplicación**, estará disponible en los análisis de puntos de conexión. En este informe, se proporciona información sobre los posibles problemas de las aplicaciones de escritorio en los equipos administrados. Permite identificar rápidamente las aplicaciones principales que afectan a la productividad del usuario final, así como ver métricas de uso de aplicaciones y de error de aplicación relativas a estas aplicaciones. Podrá solucionar problemas analizando un dispositivo específico y viendo una escala de tiempo de los eventos de confiabilidad de la aplicación. Se espera que este informe esté disponible como versión preliminar pública durante marzo de 2021. Para obtener más información, vea Confiabilidad de las aplicaciones de análisis de puntos de conexión.

Frecuencia de reinicio (versión preliminar) en análisis de puntos de conexión

Actualmente, el rendimiento de inicio de análisis de puntos de conexión proporciona al equipo de TI información para medir y optimizar los tiempos de arranque del equipo. Sin embargo, la frecuencia de reinicio puede tener un gran impacto en la experiencia del usuario, en el sentido de que un dispositivo que se reinicia diariamente debido a las pantallas azules proporcionará una experiencia de usuario deficiente, incluso si los tiempos de arranque son rápidos. Ahora, hemos incluido un informe de vista previa en las frecuencias de reinicio de la

organización para ayudarle a identificar los dispositivos problemáticos. Para obtener más información, vea Frecuencia de reinicio (versión preliminar) en análisis de puntos de conexión.

Control de acceso basado en rol

Actualización de los permisos de acceso basado en rol para la Puerta de enlace de Microsoft Tunnel

Para ayudar a controlar quién tiene derechos para administrar Microsoft Tunnel, hemos incluido **Puerta de enlace de Microsoft Tunnel** como un nuevo grupo de permisos para el control de acceso basado en roles de Intune. Este nuevo grupo incluye los siguientes permisos:

- **Crear**: permite configurar servidores de puerta de enlace de Microsoft Tunnel, configuraciones de servidor y sitios.
- **Actualizar** (modificar): permite actualizar servidores, configuraciones de servidor y sitios de puerta de enlace de Microsoft Tunnel.
- **Eliminar**: permite eliminar servidores, configuraciones de servidor y sitios de puerta de enlace de Microsoft Tunnel.
- **Leer**: permite ver servidores de puerta de enlace de Microsoft Tunnel, configuraciones de servidor y sitios.

Los administradores de Intune y los administradores de Azure Active Directory tienen estos permisos de forma predeterminada. Estos permisos también se pueden agregar a los roles personalizados que se hayan creado para el inquilino de Intune.

Compatibilidad de etiquetas de ámbito con las directivas de personalización de Intune para Government y 21Vianet

Ahora, se pueden asignar etiquetas de ámbito a directivas de personalización para Intune para Government e Intune a través de 21Vianet. Para ello, vaya al Centro de administración de Microsoft Endpoint Manager > **Administración de inquilinos** > **Personalización** donde verá las opciones de configuración de **Etiquetas de ámbito**.

Semana del 22 de febrero de 2021

Configuración del dispositivo

Versión nueva del conector de certificados PFX

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2101.13.0**. Esta nueva versión del conector incorpora mejoras de registro al conector PFX:

- Nueva ubicación de los registros de eventos, con los registros divididos como de administración, operativos o de depuración.
- Los registros operativos y de administración tienen un tamaño predeterminado de 50 MB cuando el archivado automático está habilitado.
- EventID de creación, importación y revocación de PKCS.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, consulte Conectores de certificados.

Semana del 8 de febrero de 2021

Administración de aplicaciones

Los usuarios finales pueden reiniciar la instalación de una aplicación en el Portal de empresa de Windows

Con el Portal de empresa de Windows, los usuarios finales pueden reiniciar la instalación de una aplicación si parece que el progreso se ha detenido o está inmovilizado. Esta funcionalidad se permite si el progreso de la instalación de la aplicación no ha cambiado en dos horas. Para más información, vea Incorporación de aplicaciones a Microsoft Intune.

Configuración del dispositivo

Las pantallas de cumplimiento de Google se muestran automáticamente en los dispositivos dedicados Android Enterprise 9.0 + que se ejecutan en pantalla completa.

En Intune, puede crear una directiva de contraseñas de configuración de dispositivos y una directiva de contraseñas de cumplimiento de dispositivos en dispositivos Android Enterprise.

Al crear las directivas, los dispositivos Android Enterprise dedicados que se ejecutan en el modo de pantalla completa usan automáticamente las pantallas de cumplimiento de Google. Estas pantallas guían a los usuarios y les obligan a establecer una contraseña que cumpla las reglas de la directiva.

Para obtener más información sobre la creación de directivas de contraseñas y pantallas completas, consulte:

- Configuración de Android Enterprise para marcar dispositivos como compatibles o no compatibles
- Configuración de dispositivos Android Enterprise para permitir o restringir características

Se aplica a:

- Android Enterprise 9 y versiones más recientes en el modo de pantalla completa

Semana del 1 de febrero de 2021 (versión del servicio 2101)

Administración de aplicaciones

Configuración de la opción de quitar o no una aplicación de iOS/iPadOS necesaria

Ahora puede configurar si los usuarios finales pueden instalar una aplicación de iOS/iPadOS necesaria como una aplicación que se puede quitar. La nueva configuración se aplicará a la tienda de iOS, la aplicación de línea de negocio y aplicaciones integradas. Puede encontrar esta opción en el Centro de administración de Microsoft Endpoint Manager; para ello, seleccione **Aplicaciones** > **iOS/iPadOS** > **Agregar**. Al establecer las asignaciones de la aplicación, puede seleccionar **Install as removable** (Instalar con la opción de quitar). El valor predeterminado es **Sí**, lo que significa que la aplicación se puede quitar. Las instalaciones necesarias existentes en iOS 14 se han actualizado al valor de configuración predeterminado (se puede quitar). Para obtener más información acerca de las aplicaciones de iOS/iPadOS, vea Administración de aplicaciones de Microsoft Intune.

Aplicaciones de línea de negocio admitidas en dispositivos iPad compartidos

Puede implementar aplicaciones de línea de negocio (LOB) en dispositivos iPad compartidos. La aplicación de línea de negocio debe estar asignada como **necesaria** a un grupo de dispositivos que contenga dispositivos iPad compartidos desde el Centro de administración de Microsoft Endpoint Manager. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Todas las aplicaciones** > **Agregar**. Para obtener información relacionada, vea Incorporación de una aplicación de línea de negocio iOS/iPadOS a Microsoft Intune.

Conector de Microsoft Endpoint Configuration Manager

El conector de Microsoft Endpoint Configuration Manager aparece ahora en el centro de administración. Para revisar el conector, vaya a **Administración de inquilinos** > **Conectores y tokens** > **Microsoft Endpoint Configuration Manager**. Seleccione una jerarquía de Configuration Manager que ejecute la versión 2006 o posterior para mostrar información adicional sobre ella.

Configuración del dispositivo

Versión nueva del conector de certificados PFX

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2009.2.0**. Esta nueva versión del conector:

- Mejora la actualización del conector para conservar las cuentas que ejecutan los servicios de conector.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, consulte Conectores de certificados.

Uso de la configuración del dispositivo para crear carpetas y establecer el tamaño de la cuadrícula en Managed Home Screen

En dispositivos Android Enterprise dedicados, puede configurar las opciones de configuración de Managed Home Screen (**Dispositivos** > **Configuración del dispositivo** > **Crear perfil** > **Android Enterprise** para la

plataforma > **Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado** para el perfil > **Experiencia del dispositivo**).

Al usar Managed Home Screen en el modo de pantalla completa de varias aplicaciones, existe un parámetro respecto al **diseño de aplicación personalizado**. Con este parámetro, puede:

- Cree carpetas, agregar aplicaciones a estas carpetas y colocar la carpeta en Managed Home Screen. No tiene que ordenar las carpetas.
- Elija si desea ordenar aplicaciones y carpetas en Managed Home Screen. Si lo hace, también puede:
  - Establecer el tamaño de la cuadrícula.
  - Agregar aplicaciones y carpetas a diferentes lugares de la cuadrícula.

Anteriormente, tenía que usar una directiva de configuración de la aplicación.

Para obtener más información, consulte la experiencia del dispositivo de dispositivos dedicados de Android Enterprise.

Se aplica a:

- Dispositivos Android Enterprise dedicados

Uso del catálogo de configuración para configurar el explorador Microsoft Edge en dispositivos macOS: versión preliminar pública

Actualmente, en los dispositivos macOS, el explorador Microsoft Edge se configura con un archivo de preferencias .plist (**Devices** [Dispositivos] > **Configuration profiles** [Perfiles de configuración] > **Create profile** [Crear perfil] > **macOS** para la plataforma > **Preference file** [Archivo de preferencias] para el perfil).

Hay una interfaz de usuario actualizada para configurar el explorador Microsoft Edge: **Devices** (Dispositivos) > **Configuration profiles** (Perfiles de configuración) > **Create profile** (Crear perfil) > **macOS** para la plataforma > **Settings catalog (preview)** (Catálogo de configuración [versión preliminar]) para el perfil. Seleccione los valores de Microsoft Edge que desee y, a continuación, configúrelos. Si quiere, en el perfil puede agregar opciones o quitar las existentes.

Para ver una lista de las opciones que se pueden configurar, vaya a Microsoft Edge: directivas. Asegúrese de que macOS aparezca como plataforma admitida. Si algunas opciones no están disponibles en el catálogo de configuración, se recomienda seguir usando solo el archivo de preferencias.

Para más información, consulte:

- Catálogo de configuración
- Adición de un archivo de lista de propiedades a dispositivos macOS con Intune

Para ver las directivas que ha configurado, abra Microsoft Edge y vaya a `edge://policy`.

Se aplica a:

- Explorador de Microsoft Edge, versión 77 y posteriores en macOS

Uso de NetMotion Mobility como tipo de conexión VPN para dispositivos Android Enterprise

Cuando se crea un perfil de VPN, NetMotion Mobility está disponible como un tipo de conexión VPN para Android Enterprise:

- **Dispositivos** > **Configuración del dispositivo de** > **Crear perfil** > **Android Enterprise** > **Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado Android** > **VPN** para el perfil > **NetMotion Mobility** para el tipo de conexión.
- **Dispositivos** > **Configuración del dispositivo** > **Crear perfil** > **Android Enterprise** > **Perfil de trabajo de propiedad personal** > **VPN** para el perfil > **NetMotion Mobility** para el tipo de conexión.

Para obtener más información sobre los perfiles de VPN en Intune, consulte Creación de perfiles de VPN para

conectarse a servidores VPN.

Se aplica a:

- Perfil de trabajo de propiedad personal de Android Enterprise
- Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado de Android Enterprise

Plantillas y catálogo de configuración al crear perfiles de configuración para dispositivos macOS y Windows 10

La interfaz de usuario se ha actualizado en relación con la creación de perfiles de configuración para dispositivos macOS y Windows 10 (**Devices** [Dispositivos] > **Configuration profiles** [Perfiles de configuración] > **Create profile** [Crear perfil] > **macOS** o **Windows 10 and later** [Windows 10 y versiones posteriores] para la plataforma).

En el perfil se muestra **Settings catalog - preview** (Catálogo de configuración: versión preliminar) y **Templates** (Plantillas):

- **Settings catalog - preview** (Catálogo de configuración: versión preliminar): utilice esta opción para empezar desde cero y seleccionar las opciones que quiera en la biblioteca de opciones disponibles. En macOS, el catálogo de configuraciones incluye valores para configurar la versión 77 y posteriores de Microsoft Edge. El catálogo de configuración de Windows 10 incluye muchas opciones existentes (y otras nuevas) en un solo lugar.
- **Templates** (Plantillas): utilice esta opción para configurar todos los perfiles existentes, como las restricciones de los dispositivos, las características de los dispositivos, las redes VPN o Wi-Fi, entre otras.

Este cambio solo concierne a la interfaz de usuario y no afecta a los perfiles existentes.

Para más información, consulte Catálogo de configuración.

Se aplica a:

- Configuración de dispositivos macOS
- Configuración de dispositivos Windows 10

Actualización del diseño de la pantalla de inicio en los dispositivos iOS/iPadOS supervisados

En los dispositivos iOS/iPadOS, puede configurar el diseño de la pantalla de inicio (**Devices** [Dispositivos] > **Device Configuration** [Configuración del dispositivo] > **Create profile** [Crear perfil] > **iOS/iPadOS** para la plataforma > **Device features** [Características del dispositivo] para el perfil > **Home screen layout** [Diseño de la pantalla de inicio]). En Intune se ha actualizado la característica Diseño de pantalla principal:

- El diseño de la pantalla principal tiene una nueva disposición. Esta característica permite a los administradores ver en tiempo real el aspecto que tendrán las aplicaciones y los iconos de aplicaciones en las páginas, el Dock y las carpetas. Al agregar aplicaciones en este nuevo diseñador, no se pueden agregar páginas independientes. Sin embargo, cuando se agregan nueve o más aplicaciones a una carpeta, esas aplicaciones pasan automáticamente a la página siguiente. Las directivas existentes no se ven afectadas y no es necesario cambiarlas. Los valores de configuración se transfieren a la nueva interfaz de usuario sin ningún tipo de problema. El comportamiento de la configuración en los dispositivos es el mismo.
- Agregue un vínculo web (aplicación web) a una página o al Dock. Asegúrese de agregar una dirección URL específica del vínculo web solo una vez. Las directivas existentes no se ven afectadas y no es necesario cambiarlas.

Para más información sobre las opciones que puede configurar, incluido el diseño de la pantalla principal, consulte Configuración de dispositivos iOS/iPadOS para usar las características comunes de iOS/iPadOS en Intune.

Se aplica a:

- Dispositivos iOS/iPadOS supervisados

Limitación de la publicidad personalizada de Apple en los dispositivos iOS/iPadOS

En los dispositivos iOS/iPadOS, puede configurar la publicidad personalizada de Apple. Cuando esta opción está habilitada, se limitan los anuncios personalizados en las aplicaciones de App Store, Apple News y Stocks (**Devices** [Dispositivos] > **Device Configuration** [Configuración del dispositivo] > **Create profile** [Crear perfil] > **iOS/iPadOS** para la plataforma > **Device restrictions** [Restricciones del dispositivo] para el perfil > **General** [General] > **Limit Apple personalized advertising** [Limitar la publicidad personalizada de Apple]).

Esta opción solo afecta a los anuncios personalizados. Al configurar esta opción se **desactiva** el parámetro de **Ajustes** > **Privacidad** > **Publicidad**. No afecta a los anuncios no personalizados de las aplicaciones de App Store, Apple News y Stocks. Para obtener más información sobre la directiva de publicidad de Apple, consulte el sitio web Publicidad y la privacidad de Apple.

Para ver las opciones que puede configurar actualmente en Intune, vaya a Configuración de dispositivos iOS e iPadOS para permitir o restringir características.

Se aplica a:

- Dispositivos iOS/iPadOS 14.0 y versiones más recientes inscritos con la inscripción de dispositivos o con la inscripción de dispositivos automatizada

Las plantillas administrativas incluyen nuevas directivas para la versión 88 de Microsoft Edge

Puede configurar e implementar la nueva configuración de ADMX que se aplica a la versión 88 de Microsoft Edge. Para ver las nuevas directivas, vaya a las notas de la versión de Microsoft Edge.

Para obtener más información sobre esta característica en Intune, consulte Configuración de opciones de directivas de Microsoft Edge.

Se aplica a:

- Windows 10 y versiones posteriores

Compatibilidad de la configuración regional en las notificaciones por correo electrónico en caso de incumplimiento

Las directivas de cumplimiento ahora admiten Plantillas de mensajes de notificación que incluyen mensajes independientes para diferentes configuraciones regionales. La compatibilidad con varios idiomas ya no requiere la creación de plantillas y directivas independientes para cada configuración regional.

Cuando se configuran mensajes específicos de una configuración regional en una plantilla, los usuarios finales no compatibles reciben el mensaje de notificación de correo electrónico localizado adecuado en función de su idioma preferido de O365. También se designa un mensaje localizado en la plantilla como *mensaje predeterminado*. El mensaje predeterminado se envía a los usuarios que no han establecido un idioma preferido o cuando la plantilla no incluye un mensaje específico para su configuración regional.

Inscripción de dispositivos

Ocultación de más pantallas del Asistente de configuración de inscripción de dispositivos automatizada de Apple

Ahora puede establecer perfiles de inscripción de dispositivos automatizada (ADE) para ocultar estas pantallas del asistente de configuración para dispositivos iOS/iPadOS 14.0 y macOS 11 o versiones posteriores:

- Restauración completada, para iOS/iPadOS 14.0 o versiones posteriores.
- Actualización de software completada, para iOS/iPadOS 14.0 o versiones posteriores.
- Accesibilidad, para macOS 11 o versiones posteriores (el dispositivo Mac debe estar conectado a una red Ethernet).

Administración de dispositivos

Migración de directivas de seguridad de dispositivos de Mobility + Security básico a Intune

La herramienta de migración de directivas le permite trasladar permanentemente las directivas de seguridad de los dispositivos de administración de dispositivos móviles (MDM) implementadas por Basic Mobility and Security (anteriormente MDM para Office 365 u Office MDM) a las directivas estándar de cumplimiento y los

perfiles de configuración de MDM de Intune. El uso de esta herramienta deshabilitará cualquier futura posibilidad de crear y editar las directivas de seguridad de los dispositivos de Mobility + Security básico.

Para usar la herramienta, debe:

- Haber comprado licencias de Intune para todos los usuarios de dispositivos administrados por Basic Mobility and Security (pero todavía no deben haberse asignado).
- Ponerse en contacto con soporte técnico para comprobar su idoneidad si ha adquirido una suscripción a Intune for Education.

Para obtener más información, consulte Migración de su administración de dispositivos móviles desde Basic Mobility and Security a Intune.

Id. de subred y direcciones IP en la página Propiedades de dispositivos Windows de propiedad corporativa

El id. de subred y las direcciones IP se muestra en la página **Propiedades** de los dispositivos Windows de propiedad corporativa. Para verlos, vaya al Centro de administración de Endpoint Manager > **Dispositivos** > **Todos los dispositivos** > elija un dispositivo Windows de propiedad corporativa > **Propiedades**.

Seguridad de dispositivos

La compatibilidad de Intune con Protección de aplicaciones de Microsoft Defender incluye ahora entornos aislados de Windows

Al configurar **Activar la protección de aplicaciones** en un perfil Aislamiento de aplicaciones y navegador de una directiva de reducción de la superficie de ataque de seguridad del punto de conexión de Intune, puede elegir entre las opciones siguientes:

- **Microsoft Edge** - *Disponible anteriormente*
- **Entornos de Windows aislados** - *Nuevo con esta actualización*
- **Microsoft Edge *y* _ _ Entornos de Windows aislados** - *Nuevo con esta actualización*

Antes de esta versión, esta opción se denominaba *Activación de la Protección de aplicaciones para Microsoft Edge (opciones)* .

Las nuevas opciones para esta configuración amplían la compatibilidad con Protección de aplicaciones más allá de la dirección URL para Edge. Ahora puede habilitar Protección de aplicaciones para ayudar a proteger los dispositivos mediante la apertura de amenazas potenciales en un entorno de máquina virtual Windows (contenedor) aislado de hardware. Por ejemplo, con la compatibilidad con entornos de Windows aislados, Protección de aplicaciones puede abrir documentos de Office que no son de confianza en una máquina virtual Windows aislada.

Con este cambio:

- Intune ahora admite toda la gama de valores que se encuentran en el CSP de MDM de Windows: AllowWindowsDefenderApplicationGuard.
- Para ayudarle a entender el efecto en los usuarios de dispositivos al usar entornos de Windows aislados, consulte Escenarios de prueba de Protección de aplicaciones en la documentación de seguridad de Windows.
- Obtenga más información sobre Protección de aplicaciones y la compatibilidad con aplicaciones de Office en Protección de aplicaciones para Office en la documentación de Microsoft 365.

Nueva configuración de protección de aplicaciones en la directiva de reducción de la superficie expuesta a ataques

Se han agregado dos nuevas opciones al perfil Aislamiento de aplicaciones y navegador de la directiva de reducción de la superficie expuesta a ataques para la seguridad de puntos de conexión de Intune:

- **Application Guard allow camera and microphone access** (Protección de aplicaciones permite el acceso a la cámara y el micrófono): administre el acceso de las aplicaciones de Protección de aplicaciones a la cámara y el micrófono de un dispositivo.
- **Application Guard allow use of Root Certificate Authorities from the user's device** (Protección de aplicaciones permite el uso de entidades de certificación raíz desde el dispositivo del usuario): cuando se

especifican una o varias huellas digitales del certificado raíz, los certificados coincidentes se transfieren al contenedor de Protección de aplicaciones de Microsoft Defender.

Para obtener más información, consulte la configuración del Aislamiento de aplicaciones y navegador.

Actualizaciones para líneas base de seguridad

Hay nuevas versiones disponibles para las siguientes líneas de base de seguridad:

- **Línea base de seguridad de MDM (Seguridad de Windows 10)**
- **Línea base de Microsoft Defender para punto de conexión**

Las versiones de línea base actualizadas proporcionan compatibilidad con los valores de configuración recientes para ayudarle a mantener las configuraciones que recomiendan los equipos de producto respectivos.

Para saber qué ha cambiado entre las versiones, en Comparación de versiones de línea de base aprenderá a exportar un archivo .CSV que muestre los cambios.

Informes del firewall de seguridad de los puntos de conexión

Se han agregado dos nuevos informes dedicados a las directivas del firewall en la seguridad de los puntos de conexión:

- Dispositivos MDM para Windows 10 con el firewall desactivado se encuentra en el nodo Seguridad del punto de conexión y muestra la lista de dispositivos Windows 10 con el firewall desactivado. Este informe identifica cada dispositivo por el nombre del dispositivo, el identificador del dispositivo, la información del usuario y el estado del firewall.
- Estado del firewall de los dispositivos MDM para Windows 10 es un informe organizativo que se encuentra en el nodo *Informes*, que muestra el estado de firewall de los dispositivos Windows 10. Este informe muestra la información de estado que incluye si el firewall está habilitado, deshabilitado, limitado o deshabilitado temporalmente.

Vista de resumen de los informes del Antivirus de Microsoft Defender

Hemos actualizado la vista de los informes del Antivirus de Microsoft Defender que se encuentran en el nodo **Informes** del centro de administración de Microsoft Endpoint Manager. Ahora, cuando seleccione Antivirus de Microsoft Defender en el nodo **Informes**, verá la vista predeterminada de la pestaña **Resumen** y una segunda pestaña para **Informes**. En la pestaña **Informes** es donde encontrará los informes organizativos anteriormente disponibles Estado del agente de antivirus y Malware detectado.

La nueva pestaña **Resumen** muestra la siguiente información:

- Muestra los detalles agregados de los informes del antivirus.
- Incluye una opción *Actualizar* que actualiza el número de dispositivos en cada uno de los estados del antivirus.
- Refleja los mismos datos que los que se encuentran en el informe organizativo Estado del agente de antivirus, al que ahora se tiene acceso desde la pestaña **Informes**.

Compatibilidad con directivas de protección de aplicaciones en Android y iOS/iPadOS para asociados adicionales de Mobile Threat Defense

En octubre de 2019, la directiva de protección de aplicaciones de Intune agregó la capacidad de usar datos de nuestros asociados de Microsoft Threat Defense.

Con esta actualización, ampliamos esta compatibilidad al asociado siguiente para usar una directiva de protección de aplicaciones a fin de bloquear o borrar de forma selectiva los datos corporativos de un usuario en función del estado del dispositivo:

- **McAfee MVision Mobile** en Android, iOS y iPadOS

Para más información, consulte Creación de una directiva de protección de aplicaciones de Mobile Threat Defense con Intune.

Aumento del período de validez de los certificados para los perfiles SCEP y PKCS

Intune admite ya un **período de validez de certificados** de hasta **24** meses en los perfiles de certificados para el Protocolo de inscripción de certificados simple (SCEP) y los estándares de criptografía de clave pública (PKCS). Este supone un aumento del período de soporte técnico anterior de hasta 12 meses.

Esta compatibilidad se aplica a Windows y Android. Los períodos de validez de los certificados se ignoran en iOS/iPadOS y macOS.

Supervisión y solución de problemas

Nuevo informe organizativo de idoneidad para la administración conjunta

El informe **Idoneidad para la administración conjunta** proporciona una evaluación de idoneidad para los dispositivos que se pueden administrar de manera conjunta. La administración conjunta permite administrar simultáneamente dispositivos Windows 10 mediante Configuration Manager y Microsoft Intune. Podrá ver un resumen de este informe en el Centro de administración de Microsoft Endpoint Manager si selecciona la pestaña **Informes** > **Cloud attached devices (Dispositivos conectados a la nube)** > **Informes** > **Co-management eligibility** (Idoneidad para la administración conjunta). Para obtener información relacionada con los informes, vea Informes de Intune.

Nuevo informe organizativo de cargas de trabajo de administración conjunta

El informe de **cargas de trabajo de administración conjunta** proporciona un informe de los dispositivos que se administran de forma conjunta en la actualidad. La administración conjunta permite administrar simultáneamente dispositivos Windows 10 mediante Configuration Manager y Microsoft Intune. Puede ver este informe en el Centro de administración de Microsoft Endpoint Manager si selecciona la pestaña **Informes** > **Cloud attached devices (Dispositivos conectados a la nube)** > **Informes** > **Co-Managed Workloads** (Cargas de trabajo de administración conjunta). Para más información, vea Informes de Intune.

Log Analytics incluirá registros de detalles del dispositivo.

Los registros detallados del dispositivo de Intune ya están disponibles. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Informes** > **Log Analytics**. Puede correlacionar un conjunto de detalles del dispositivo para compilar consultas personalizadas y libros de Azure. Para obtener más información, vea Informes de integración de Azure Monitor (especialista).

Control de acceso basado en roles.

Compatibilidad con etiquetas de ámbito para la página estado de inscripción

Ahora puede asignar etiquetas de ámbito a la página de estado de inscripción, de modo que solo los roles que defina puedan verlo. Para obtener más información, consulte Creación de un perfil de la página de estado de la inscripción y asignación a un grupo.

Scripts

Propiedades beta adicionales de Data Warehouse

Ya hay propiedades adicionales disponibles mediante la API beta Data Warehouse de Intune. Las propiedades siguientes se exponen a través de la entidad de dispositivos en la API beta:

- `SubnetAddressV4Wifi`: dirección de subred para la conexión Wi-Fi de IPV4.
- `IpAddressV4Wifi`: dirección IP para la conexión Wi-Fi de IPV4.

Para obtener información relacionada, vea API de Data Warehouse de Microsoft Intune.

Semana del 25 de enero de 2021

Administración de aplicaciones

Actualización del icono de la aplicación Portal de empresa para iOS, macOS y la Web

Hemos actualizado el icono de aplicación del Portal de empresa para iOS, macOS y web. Este icono también se usa en el Portal de empresa para Windows. Los usuarios finales verán el icono nuevo en el iniciador de aplicaciones y la pantalla principal del dispositivo, en App Store de Apple y en las experiencias de las

aplicaciones del Portal de empresa.

Compatibilidad con aplicaciones del sistema de Android Enterprise en perfiles de trabajo de propiedad personal

Ahora puede implementar aplicaciones del sistema de Android Enterprise en dispositivos de perfil de trabajo de propiedad personal de Android Enterprise. Las aplicaciones del sistema son aquellas que no aparecen en Google Play Store administrado y que están preinstaladas en el dispositivo. Una vez que se haya implementado una aplicación del sistema, no podrá desinstalarla, ocultarla ni quitarla. Para obtener información relacionada con las aplicaciones del sistema, vea Incorporación de aplicaciones del sistema Android Enterprise a Microsoft Intune.

Supervisión y solución de problemas

Actualización al exportar informes de Intune mediante Graph API

Cuando use `exportJobs` de Graph API para exportar informes de Intune sin seleccionar ninguna columna para el informe de dispositivos, recibirá el conjunto de columnas predeterminado. Para reducir la confusión, se han quitado las columnas del conjunto de columnas predeterminado. Las columnas eliminadas son `PhoneNumberE164Format`, `_ComputedComplianceState`, `_OS` y `OSDescription`. Estas columnas aún se podrán seleccionar si las necesita, pero solo de forma explícita y no de manera predeterminada. Si ha configurado alguna automatización en torno a las columnas predeterminadas de la exportación de dispositivos y usa alguna de ellas, deberá refactorizar los procesos para que esas columnas y cualquier otra pertinente se seleccionen de manera explícita. Para obtener información relacionada, consulte Exportación de informes de Intune mediante Graph API.

Semana del 18 de enero de 2021

Configuración del dispositivo

Microsoft Tunnel ahora admite Red Hat Enterprise Linux 8

Ahora puede usar Red Hat Enterprise Linux (RHEL) 8 con Microsoft Tunnel. Para usar RHEL 8, no es necesario realizar ninguna acción. Se ha agregado compatibilidad con los contenedores de Docker que se actualizan automáticamente. Además, esta actualización también suprime algunos registros superfluos.

Semana del 11 de enero de 2021

Administración de aplicaciones

Eliminación de aplicaciones Win32 en una relación de dependencia

Las aplicaciones Win32 agregadas a Intune no se pueden quitar si están en una relación de dependencia. Estas aplicaciones solo se pueden eliminar después de quitar la relación de dependencia. Este requisito se aplica a las aplicaciones primarias y secundarias con una relación de dependencia. Además, este requisito garantiza que las dependencias se apliquen correctamente y que el comportamiento de la dependencia sea más predecible. Para más información, consulte Administración de aplicaciones Win32 en Microsoft Intune.

Compatibilidad de etiquetas de ámbito con directivas de personalización

Ahora puede asignar etiquetas de ámbito a las directivas de personalización. Para ello, vaya al Centro de administración de Microsoft Endpoint Manager > **Administración de inquilinos** > **Personalización** donde verá las opciones de configuración de **Etiquetas de ámbito**. Esta característica ya está disponible con Intune para Government o Intune operado por 21Vianet.

Configuración del dispositivo

Versión nueva del conector de certificados PFX

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2009.1.9**. Esta nueva versión del conector:

- Mejoras en la renovación del certificado de conector.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, consulte Conectores de certificados.

Semana del 4 de enero de 2021

Administración de aplicaciones

Habilitación automática del acceso al explorador durante la inscripción de perfiles de trabajo Android

El acceso al explorador ya está habilitado automáticamente en el dispositivo durante la inscripción de perfiles de trabajo de propiedad personal de Android Enterprise. Con este cambio, los dispositivos compatibles pueden usar el explorador para tener acceso a los recursos protegidos por el acceso condicional sin necesidad de realizar acciones adicionales. Antes de este cambio, los usuarios tenían que iniciar el Portal de empresa, seleccionar **Configuración** > **Habilitar acceso al explorador** y hacer clic en **Habilitar**.

Este cambio no afecta a los dispositivos que ya están inscritos.

Barra de progreso de la descarga de aplicaciones Win32

Mientras se descarga una aplicación Win32, los usuarios finales verán ahora una barra de progreso en el Portal de empresa de Windows. Esta característica ayudará a los clientes a comprender mejor el progreso de la instalación de la aplicación.

Actualización del icono de la aplicación Portal de empresa para Android

Hemos actualizado el icono de la aplicación Portal de empresa para Android para crear una apariencia más moderna para los usuarios del dispositivo. Para ver el aspecto del nuevo icono, vaya a la lista de Portal de empresa de Intune en Google Play.

Semana del 7 de diciembre de 2020

Aplicaciones de Intune

Nuevas aplicaciones protegidas disponibles para Intune

Las siguientes aplicaciones protegidas ya están disponibles para Microsoft Intune:

- Dynamics 365 Remote Assist
- Box - Cloud Content Management
- STid Mobile ID
- FactSet 3.0
- Notate para Intune
- Field Service (Dynamics 365)

Para obtener más información sobre las aplicaciones protegidas, vea Aplicaciones protegidas de Microsoft Intune.

Archivo de novedades

Para ver los meses anteriores, consulte el archivo de novedades.

Notificaciones

Estos avisos proporcionan información importante que puede ayudarle a prepararse para las características y los cambios futuros de Intune.

Actualización de los perfiles antivirus de seguridad de puntos de conexión para Windows 10

Hemos realizado un pequeño cambio para mejorar la experiencia de los perfiles antivirus para Windows 10. Esto no afecta al usuario final, ya que solo se trata de un cambio en el contenido que se muestra en la interfaz de usuario.

¿Cómo me afecta esto?

Anteriormente, al configurar un perfil de seguridad de Windows para la directiva antivirus de seguridad de puntos de conexión, tenía dos opciones para la mayoría de las configuraciones: *Sí* y *No configurado*. Ahora, esas

mismas configuraciones incluyen las opciones *Sí, No configurado* y *No* (la nueva opción). Los valores configurados previamente que se hayan establecido en *No configurado* seguirán con la opción *No configurado*. Al crear perfiles o editar los existentes, ahora tiene la opción de especificar explícitamente *No*.

Además, la configuración *Hide the Virus and threat protection area in the Windows Security app* (Ocultar el área de protección contra virus y amenazas en la aplicación Seguridad de Windows) tiene una configuración secundaria, *Hide the Ransomware data recovery option in the Windows Security app* (Ocultar la opción de recuperación de datos de ransomware en la aplicación Seguridad de Windows). Si la configuración principal (Ocultar el área de protección contra virus y amenazas) se ha establecido en *No configurado* y la configuración secundaria se ha establecido en *Sí*, ambas configuraciones se establecerán en *No configurado*. Esto se aplicará al editar el perfil.

¿Qué acción debo llevar a cabo?

No se requiere ninguna acción. Sin embargo, es posible que quiera notificar este cambio a su departamento de soporte técnico.

Plan de cambio: Intune finaliza el soporte técnico del Portal de empresa en versiones no admitidas de Windows

Intune sigue el ciclo de vida de Windows 10 en las versiones compatibles de esta sistema operativo. Ahora, estamos retirando el soporte técnico de los portales de empresa de Windows 10 asociados en esas versiones de Windows que están fuera de la directiva de soporte técnico moderno.

¿Cómo me afecta esto?

Dado que Microsoft ya no admite estos sistemas operativos, puede que este cambio no le afecte, dado que es probable que ya haya actualizado el sistema operativo o los dispositivos. Este cambio solo le afectará si sigue administrando versiones de Windows 10 no admitidas. Las versiones de Windows y del Portal de empresa afectadas son:

- Windows 10, versión 1507, Portal de empresa, versión 10.1.721.0
- Windows 10, versión 1511, Portal de empresa, versión 10.1.1731.0
- Windows 10, versión 1607, Portal de empresa, versión 10.3.5601.0
- Windows 10, versión 1703, Portal de empresa, versión 10.3.5601.0
- Windows 10, versión 1709, cualquier versión del Portal de empresa

Aunque no vamos a desinstalar estas versiones del Portal de empresa mencionadas anteriormente, las retiraremos de Microsoft Store y dejaremos de probar nuestras versiones de servicio con ellas.

Efecto para el usuario: si sigue usando una versión no admitida de Windows 10, los usuarios no podrán obtener las últimas actualizaciones de seguridad, ni nuevas características, correcciones de errores, mejoras de latencia, mejoras de accesibilidad e inversiones en rendimiento. System Center Configuration Manager e Intune no podrán administrar conjuntamente a los usuarios.

¿Qué tengo que hacer?

En el centro de administración de Microsoft Endpoint Manager, use la característica Aplicaciones detectadas para buscar aplicaciones con estas versiones. En el dispositivo de un usuario, la versión del Portal de empresa se muestra en la página **Configuración** del Portal de empresa. Actualice a una versión admitida de Windows o del Portal de empresa.

Plan de cambio: Intune avanza para admitir Android 6.0 y versiones posteriores en abril de 2021

Como se mencionó en MC234534, Intune pasará a ser compatible con Android 6.0 (Marshmallow) y versiones posteriores en el lanzamiento del servicio de abril (2104).

Cómo afectará este cambio a su organización

Dado que las aplicaciones móviles de Office para Android finalizaron la compatibilidad con Android 5.x (Lollipop) el 30 de junio de 2019 (MC181101), es posible que este cambio no le afecte; es probable que ya haya actualizado el sistema operativo o los dispositivos. Sin embargo, si tiene un dispositivo que todavía está

ejecutando la versión 5.x de Android o decide inscribir cualquier dispositivo que ejecute la versión 5.x de Android, tenga en cuenta que estos dispositivos ya no se admitirán. Puede actualizarlos a la versión 6.0 de Android (Marshmallow) o una versión posterior o reemplazarlos por un dispositivo en la versión 6.0 o posterior de Android.

> **NOTE**
> Los dispositivos Android de Teams no se ven afectados por este anuncio y seguirán siendo compatibles con independencia de su versión del sistema operativo Android.

Lo que necesita para prepararse

Notifique a su departamento de soporte técnico, si procede, este próximo cambio en la compatibilidad. También tiene dos opciones de administración para ayudar a informar a los usuarios finales o a bloquear la inscripción.

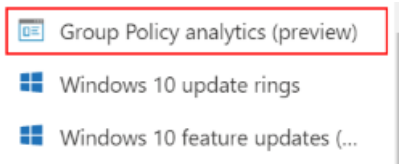
1. A continuación se muestra cómo puede advertir a los usuarios finales:
   - Use una directiva de cumplimiento de dispositivos para el administrador de dispositivos Android o Android Enterprise y establezca la acción de incumplimiento para enviar un mensaje a los usuarios antes de marcarlos como no compatibles.
   - Configure una opción de inicio condicional para la directiva de protección de aplicaciones con un requisito de versión de SO mínima para advertir a los usuarios.
2. A continuación se muestra cómo puede bloquear dispositivos en versiones inferiores a Android 6.0:
   - Configuración de restricciones de inscripción para impedir que se inscriban dispositivos en Android 5.x
   - Use una directiva de cumplimiento de dispositivos para el administrador de dispositivos Android o Android Enterprise para que los dispositivos en Android 5.x no sean compatibles.
   - Configure una opción de inicio condicional para la directiva de protección de aplicaciones con un requisito de versión de SO mínima para bloquear el acceso a las aplicaciones de los usuarios.

Versión preliminar pública en Microsoft Intune

14/05/2021 • 2 minutes to read

Microsoft Intune publica características en "versión preliminar pública". Estas características están en un proceso activo de desarrollo y es posible que no estén completas. Están disponibles como "versión preliminar". Puede probar y usar estas características en entornos y escenarios de producción, y proporcionar comentarios.

Las características en versión preliminar tienen una etiqueta **(versión preliminar)** en el centro de administración de Microsoft Endpoint Manager:



Aspectos que debe saber

Al trabajar con características en versión preliminar pública, estas características:

- Pueden tener una funcionalidad restringida o limitada. Por ejemplo, es posible que la característica solo se aplique a una plataforma.
- Las características suelen pasar por varios cambios antes de estar en disponibilidad general (GA).
- Son totalmente compatibles con Microsoft.
- Es posible que solo estén disponibles en determinadas regiones geográficas o entornos de nube. Por ejemplo, puede que la característica no exista en la nube de la administración pública.
- Las características individuales de la versión preliminar pueden tener más restricciones de uso y soporte técnico. Si es así, esta información se indica normalmente en la documentación de la característica.

Pasos siguientes

- Revise los avisos importantes.
- Vea lo que está en desarrollo.

Inicio rápido: Prueba gratuita de Microsoft Intune

14/05/2021 • 7 minutes to read

Microsoft Intune permite administrar los dispositivos y las aplicaciones para proteger los datos corporativos de los recursos. En este tutorial de inicio rápido, creará una suscripción gratuita para probar Intune en un entorno de prueba.

Intune proporciona administración de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM) desde un servicio seguro basado en la nube que se administra en el Centro de administración de Microsoft Endpoint Manager. Con Intune, se asegura de que los recursos corporativos de los empleados (datos, dispositivos y aplicaciones) están configurados correctamente y actualizados, se puede acceder a ellos y satisfacen las directivas de cumplimiento y los requisitos de su compañía.

Cuando complete el proceso de registro, tendrá un nuevo inquilino. Un inquilino es una instancia dedicada de Azure Active Directory (Azure AD) donde se hospeda la suscripción a Intune. A continuación, puede configurar el inquilino, agregar usuarios y grupos, y asignar licencias a los usuarios. Cuando esté listo, puede ayudar a los usuarios a inscribir sus dispositivos y agregar aplicaciones que necesitan para comenzar el proceso de administración de puntos de conexión moderno. A medida que continúe, puede establecer directivas de configuración y protección, así como otras funcionalidades de administración de puntos de conexión.

Requisitos previos

Antes de configurar Microsoft Intune, revise los siguientes requisitos:

- Exploradores y sistemas operativos compatibles
- Ancho de banda y requisitos de configuración de red de Intune

Suscríbase para disfrutar de una prueba gratuita de Microsoft Intune

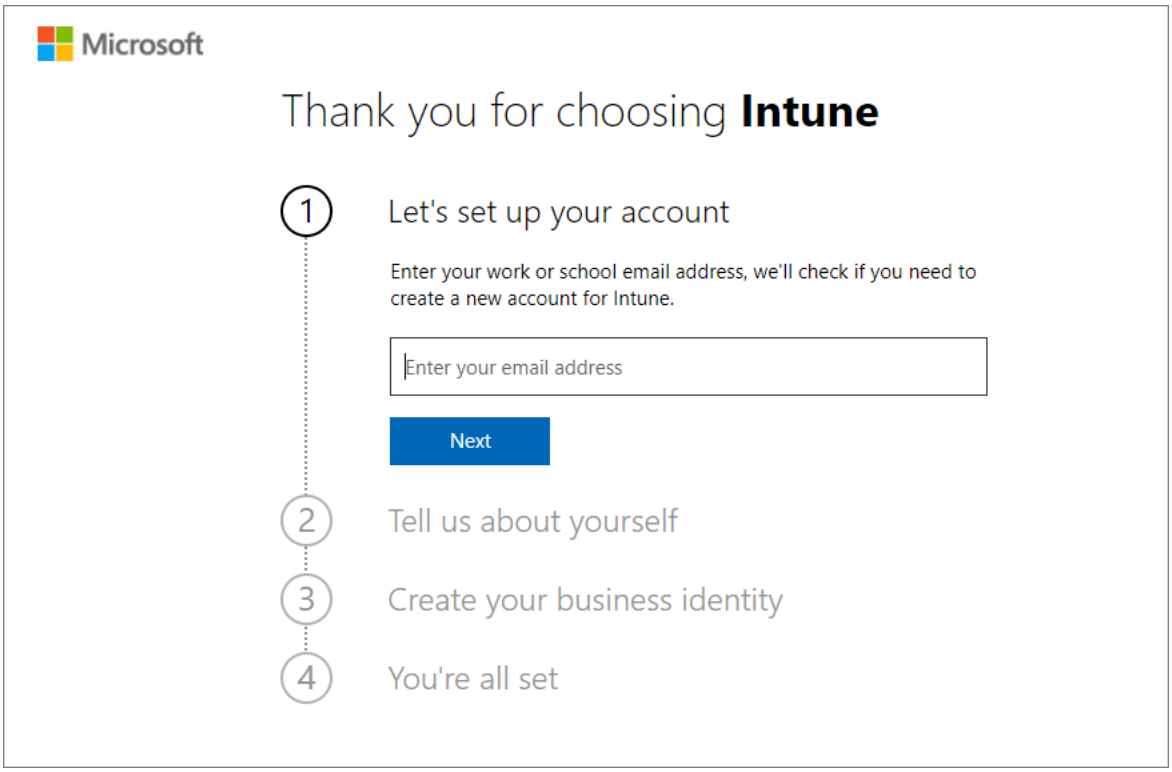
Probar Intune es gratis durante 30 días. Si ya dispone de una cuenta profesional o educativa, **inicie sesión** con dicha cuenta y agregue Intune a su suscripción. En caso contrario, puede **registrarse** para obtener una nueva cuenta y usar Intune para su organización.

> **IMPORTANT**
> No puede combinar una cuenta profesional o educativa existente después de registrarse con una cuenta nueva.

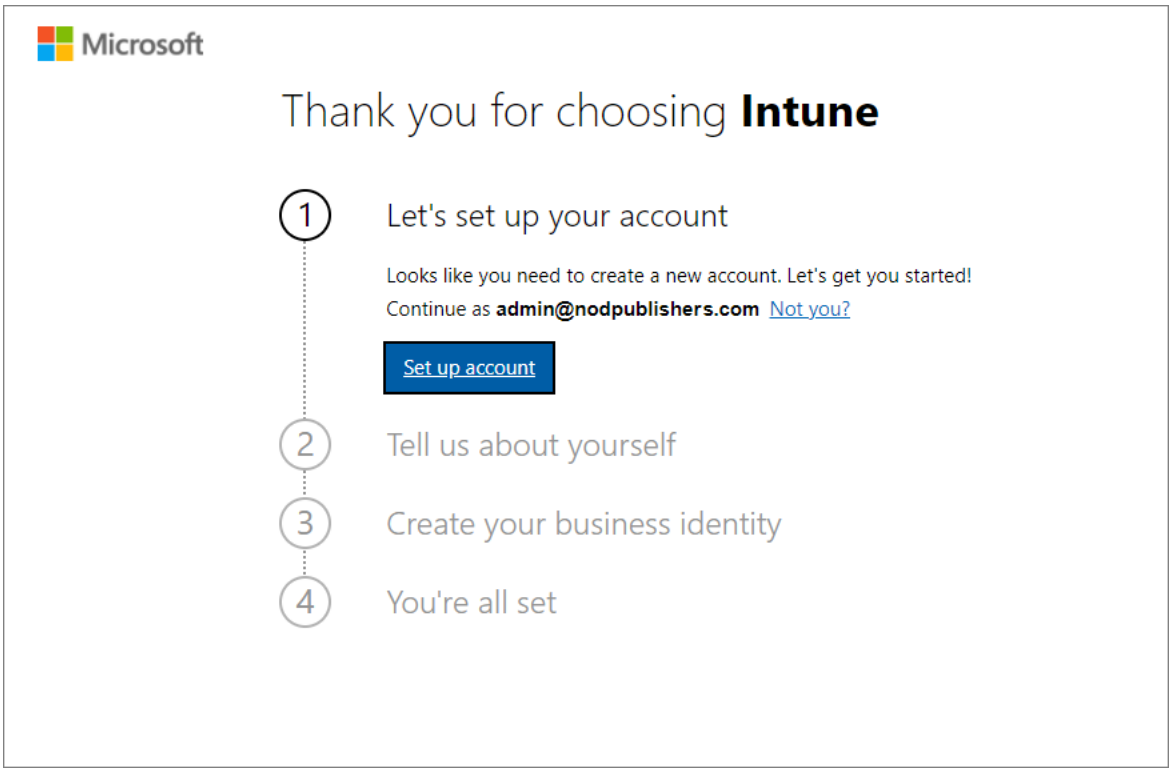
Para registrarse para una evaluación gratuita de Microsoft Intune, siga estos pasos:

1. Vaya a la página Cuenta de configuración de Intune.
2. Escriba la dirección de correo electrónico y haga clic en **Next** (Siguiente).

> **NOTE**
> Si ya tiene una cuenta configurada con otro servicio de Microsoft con su dirección de correo electrónico, puede optar por iniciar sesión para usar la cuenta con la evaluación de Intune o puede crear una cuenta nueva. En estos pasos se supone que va a crear una nueva cuenta.

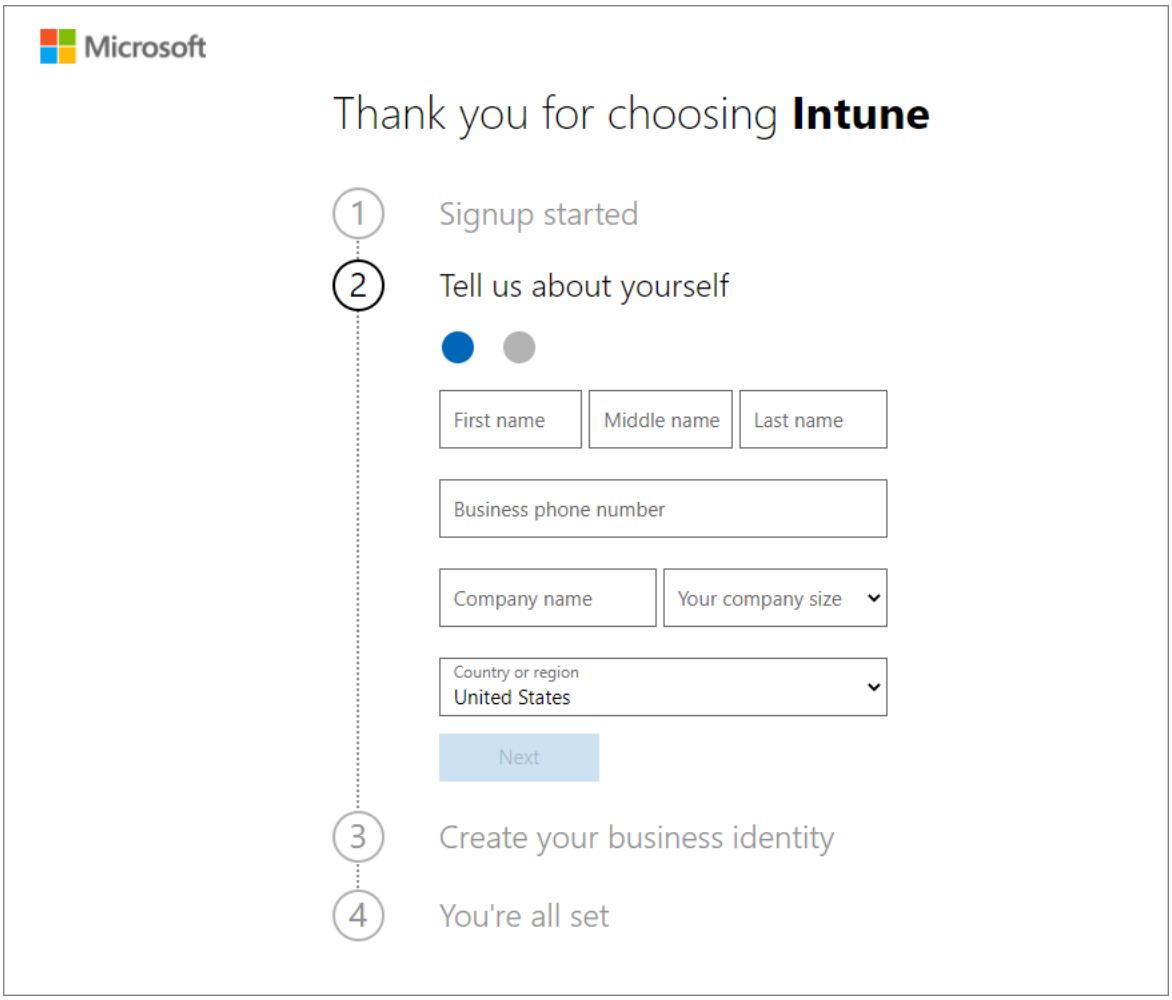


3. Haga clic en **Cuenta de configuración** para crear una nueva cuenta.

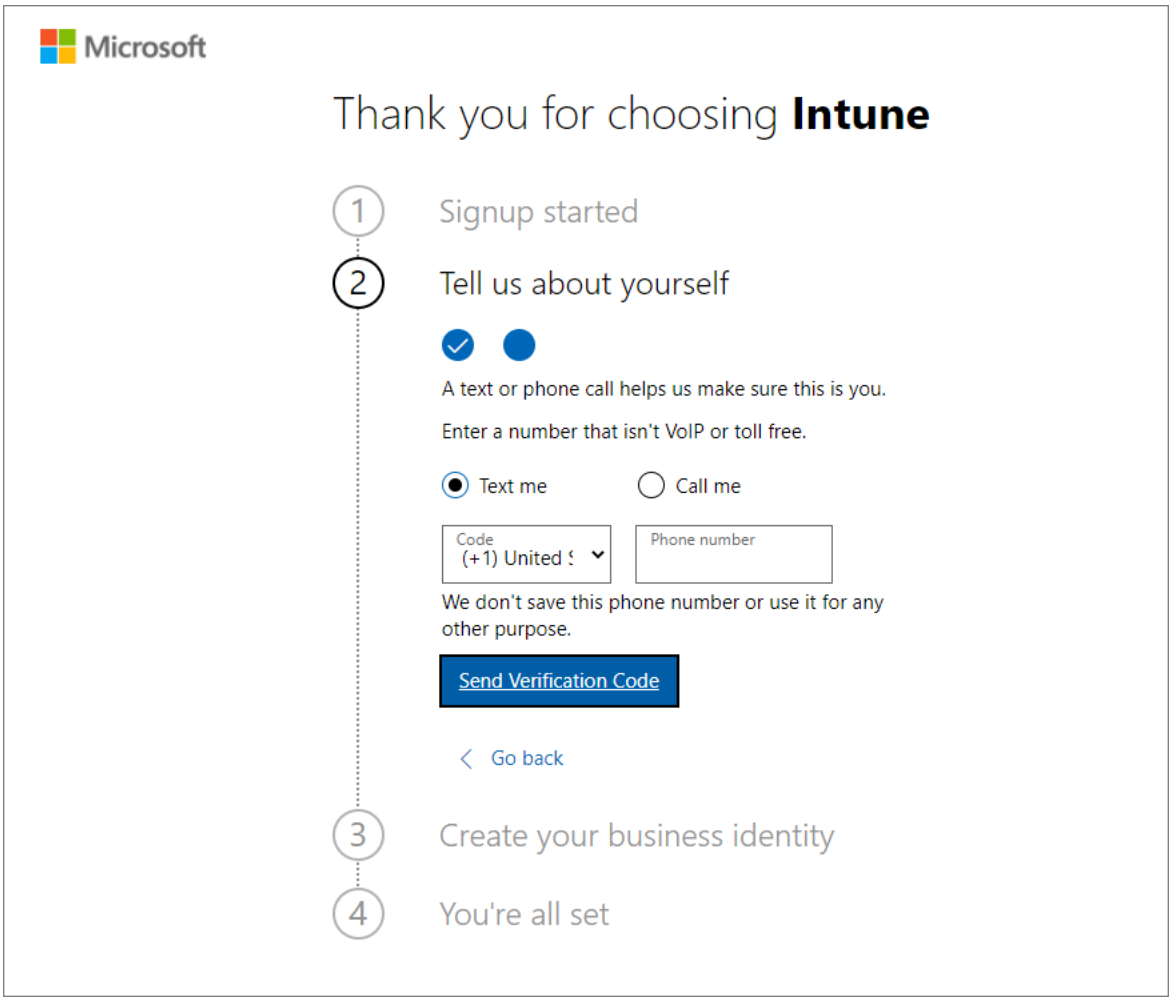


4. Agregue el nombre, el número de teléfono, el nombre de la empresa, el tamaño de la empresa y la región. A continuación, haga clic en **Siguiente**.

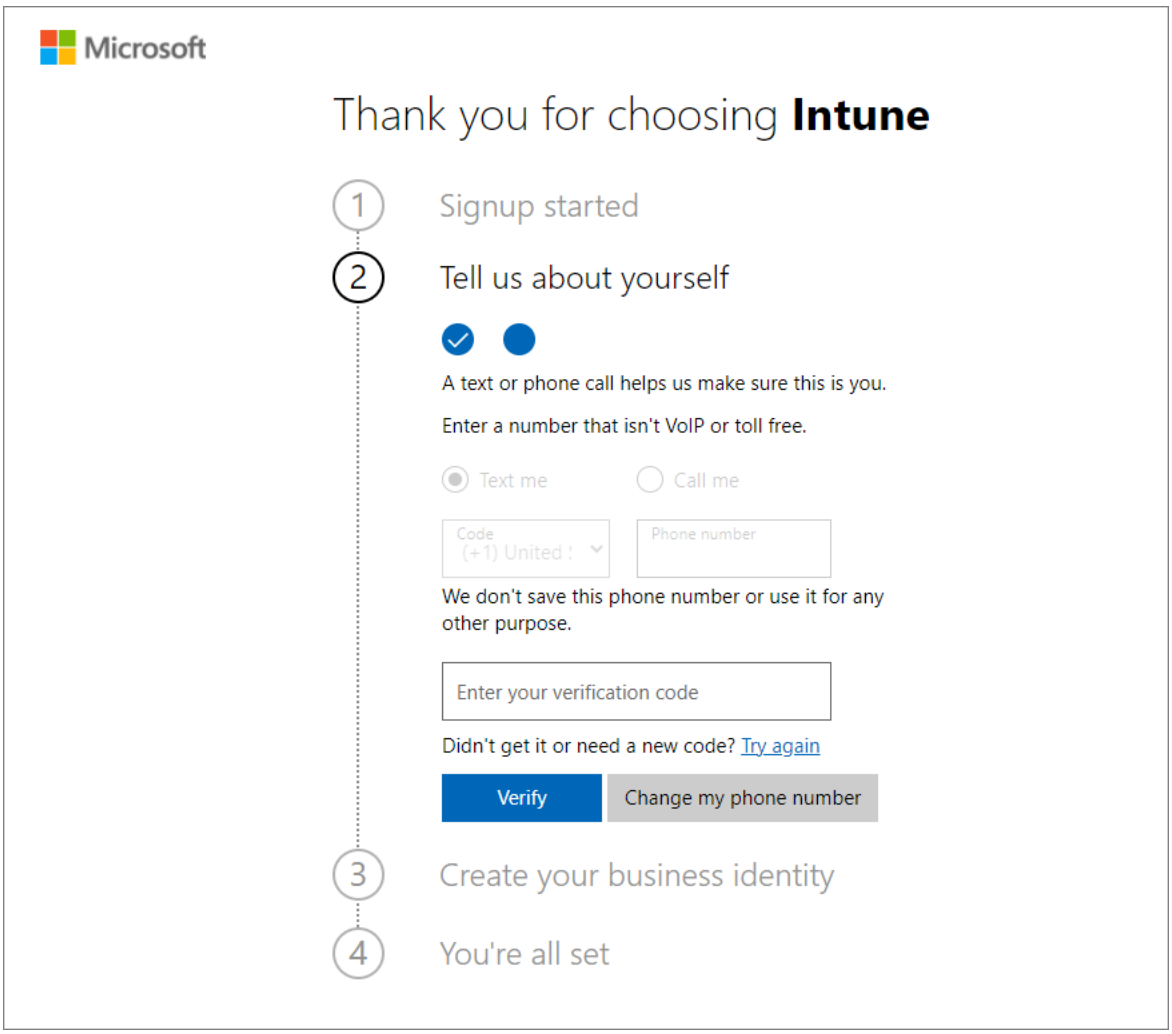
> **NOTE**
> Si la configuración regional de la mayoría de las operaciones de TI y de los usuarios es diferente a la suya, puede que quiera seleccionar esa configuración regional en **País o región**. Intune usa la información regional para ofrecer los servicios adecuados. Puede modificar esta configuración posteriormente.



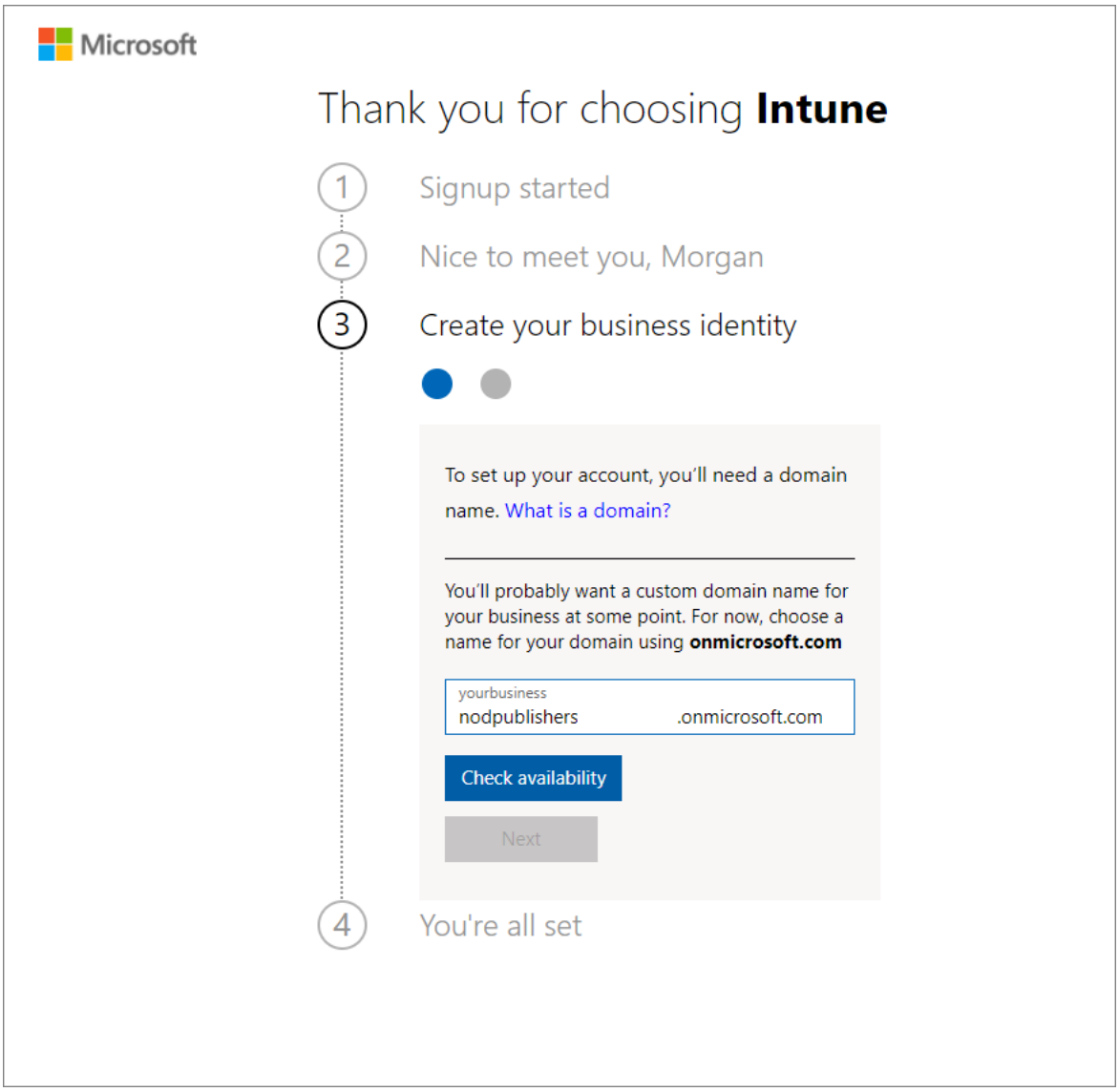
5. Haga clic en **Enviar código de verificación** para comprobar el número de teléfono que agregó.



6. Escriba el código de verificación que reciba en el dispositivo móvil y, a continuación, haga clic en **Comprobar**.



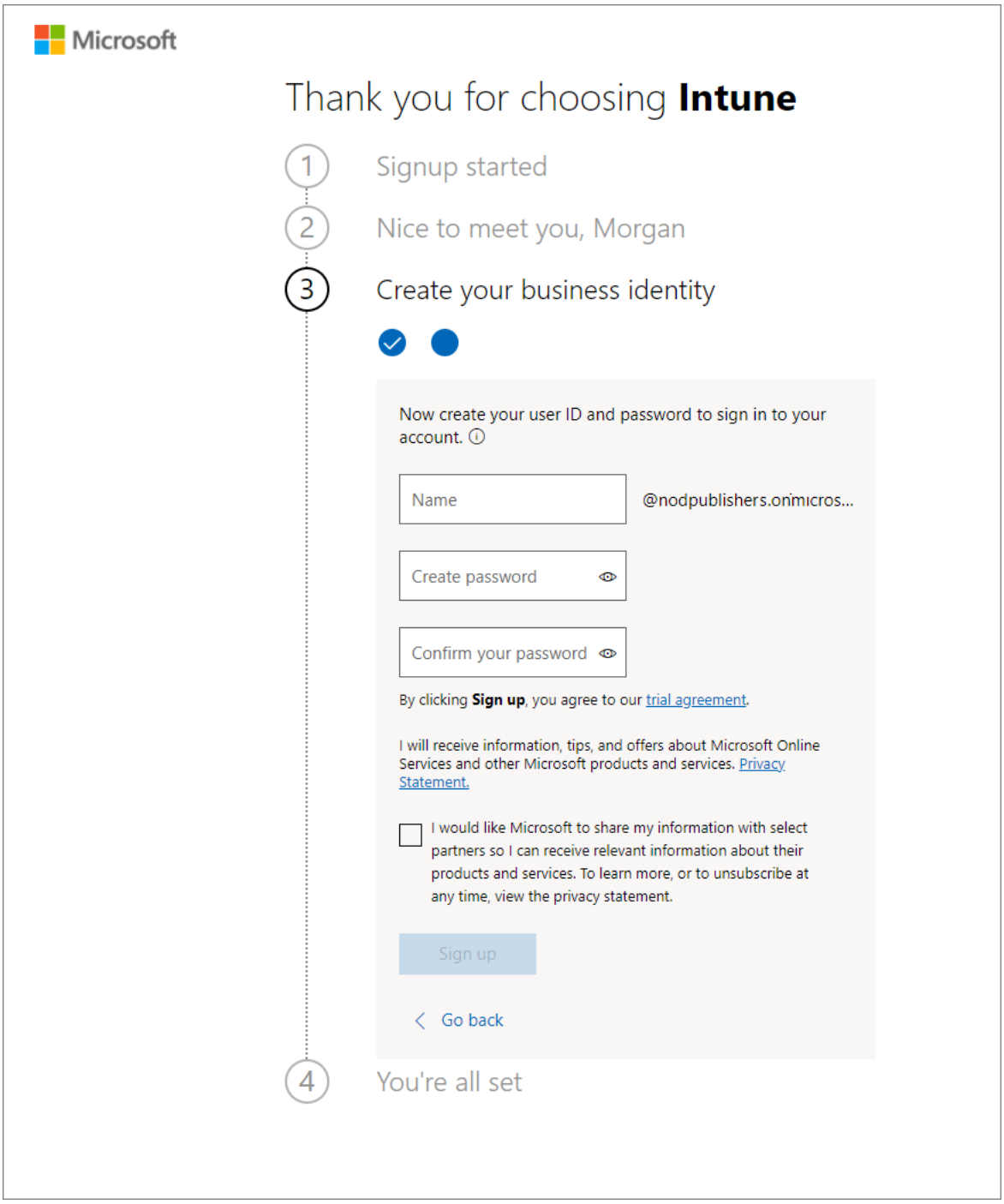
7. Agregue un nombre de dominio para su evaluación que represente su empresa u organización. Su nombre se agregará antes de *.onmicrosoft.com*. Haga clic en **Comprobar disponibilidad** > **Siguiente**. Si lo desea, puede cambiar este nombre de dominio posteriormente por su nombre de dominio personalizado.



> **NOTE**
>
> Si quiere usar el dominio personalizado de su organización sin *.onmicrosoft.com*, puede cambiarlo en el Centro de administración de Microsoft 365, tal como se describe más adelante en este artículo.

8. Agregue el nombre de usuario y la contraseña que usará para iniciar sesión en Microsoft Intune. Revise el contrato de evaluación y la declaración de privacidad. Haga clic en **Registrarse** para crear su cuenta.

> **IMPORTANT**
>
> Asegúrese de tomar nota de su nombre de usuario y contraseña.



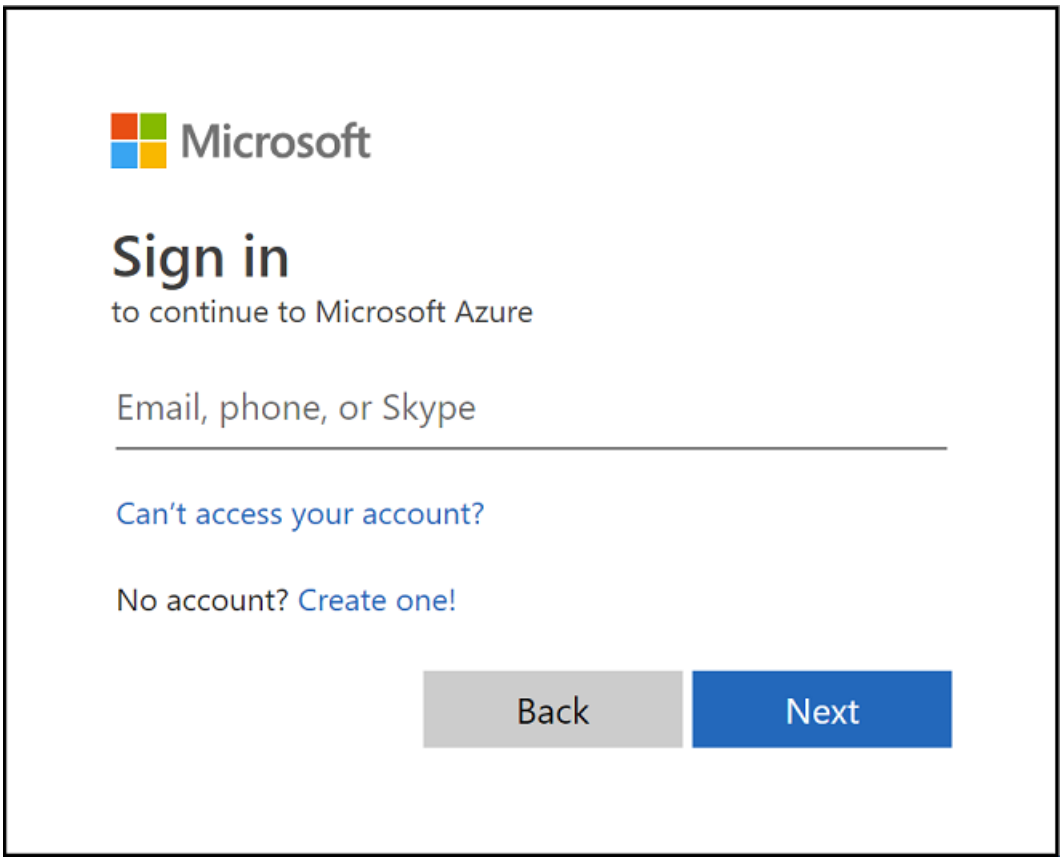
9. Una vez creada la cuenta, verá el nombre de usuario. Usará este nombre de usuario para iniciar sesión en Intune. Además, recibirá un mensaje de correo electrónico con la información de la cuenta en la dirección de correo electrónico que haya proporcionado durante el proceso de suscripción. Este mensaje confirma que la suscripción está activa.

Inicio de sesión en Intune en el centro de administración de Microsoft Endpoint Manager

Si aún no ha iniciado sesión en el portal, complete los pasos siguientes:

1. Abra una nueva ventana del explorador y escriba **https://endpoint.microsoft.com** en la barra de direcciones.

2. Use el identificador de usuario que recibió en los pasos anteriores para iniciar sesión. El identificador de usuario tendrá un aspecto similar al siguiente: *yourID@yourdomain.onmicrosoft.com* .



Si se registra en una versión de prueba, recibirá también un mensaje de correo electrónico con la información de la cuenta en la dirección que haya proporcionado durante el proceso de registro. Este mensaje confirma que la versión de prueba está activa.

> **TIP**
> Al trabajar con Microsoft Endpoint Manager, puede que obtenga mejores resultados si trabaja con un explorador en modo normal en lugar de en modo privado.

Confirmación de la entidad de MDM en Microsoft Endpoint Manager

De forma predeterminada, la entidad de administración de dispositivos móviles (MDM) se establece al crear la evaluación gratuita. Siga estos pasos para confirmar que la entidad de MDM está establecida:

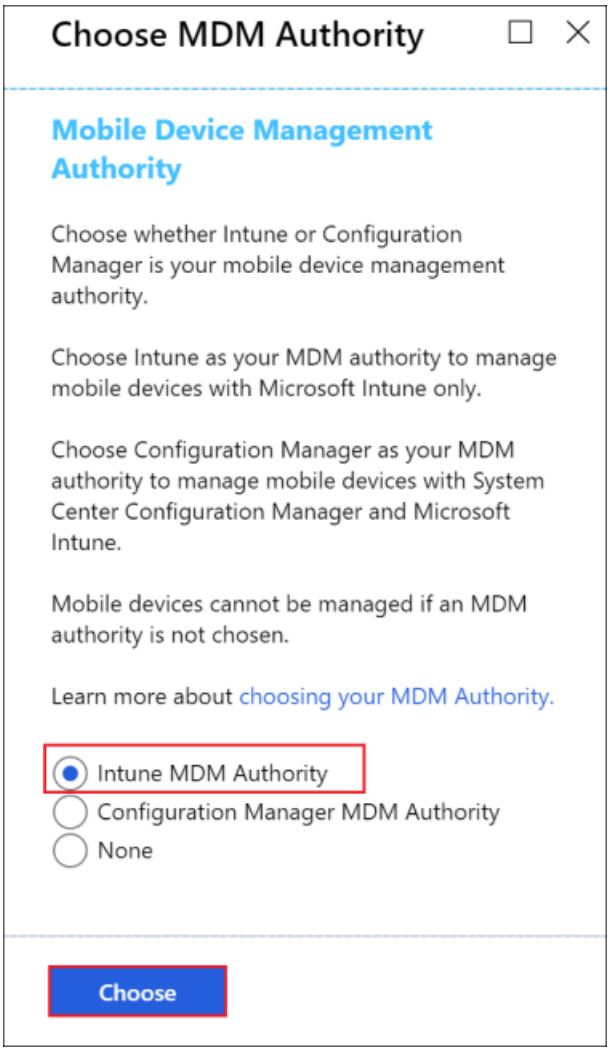
1. Si aún no lo ha hecho, inicie sesión en el centro de administración de Microsoft Endpoint Manager.
2. Haga clic en **Administración de inquilinos**.
3. Vea los detalles del inquilino. La **entidad de MDM** se debe establecer en **Microsoft Intune**.

Si después de iniciar sesión en Microsoft Endpoint Manager ve un banner de color naranja que indica que todavía no se estableció la entidad de MDM, puede activarla en este momento. La configuración de la entidad de administración de dispositivos móviles (MDM) determina cómo se administran los dispositivos. La entidad de MDM debe establecerse antes de que los usuarios puedan inscribir dispositivos para la administración.

Establecer la entidad de MDM en Intune

1. Si no tiene la entidad de MEM establecida, inicie sesión en el centro de administración de Microsoft Endpoint Manager.
2. Seleccione el banner de color naranja para abrir el ajuste **Entidad de administración de dispositivos móviles**. El banner naranja aparece únicamente si aún no ha establecido la entidad de MDM.

> **NOTE**
> Si ha establecido la entidad de MDM, verá el valor de dicha entidad en la hoja **Administración de inquilinos**. El banner naranja aparece únicamente si aún no ha establecido la entidad de MDM.



3. Si esa entidad no se ha establecido, en **Elegir entidad de MDM**, establézcala en **Entidad de MDM de Intune**.

Para obtener más información sobre la entidad de MDM, vea Establecer la entidad de administración de dispositivos móviles.

Configurar el nombre de dominio personalizado (opcional)

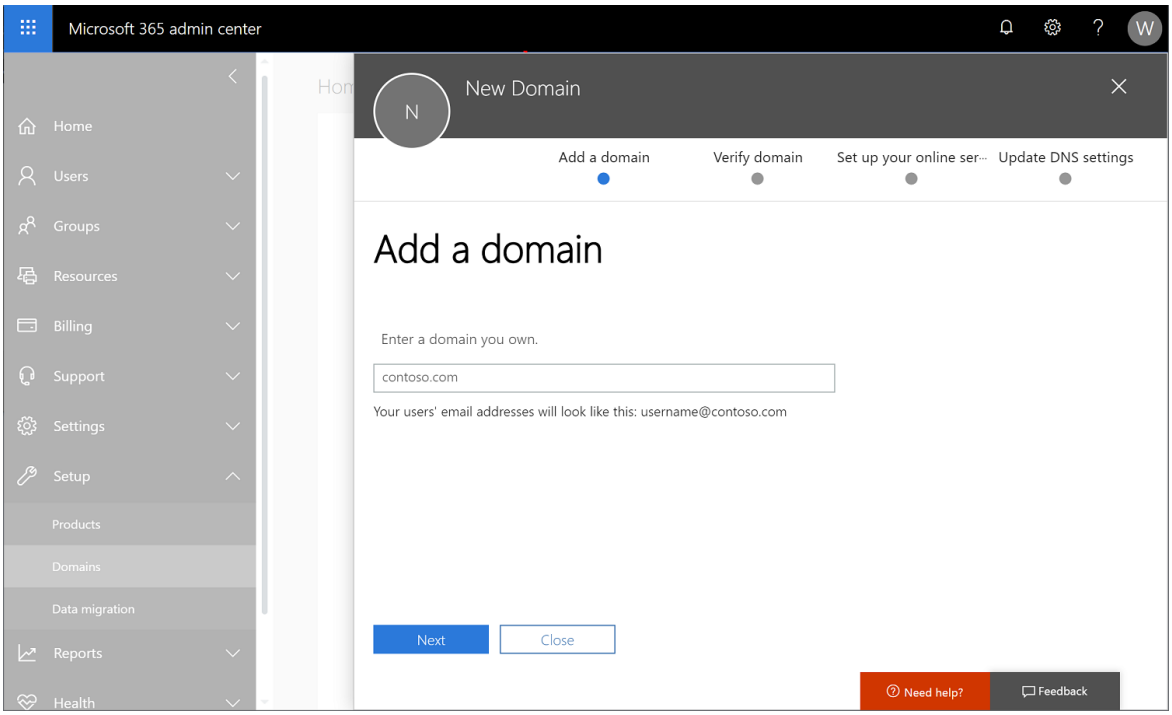
Tal como se mencionó anteriormente, si quiere usar el dominio personalizado de su organización sin **.onmicrosoft.com**, puede cambiarlo en el Centro de administración de Microsoft 365. Puede agregar, comprobar y configurar un nombre de dominio personalizado siguiendo los pasos que se indican a continuación.

> **IMPORTANT**
> No es posible cambiar la parte del nombre de dominio *onmicrosoft.com* **inicial**, ni tampoco quitarla. Sin embargo, se puede agregar, comprobar o quitar los nombres de dominio *personalizado* usados en Intune para identificar claramente su negocio. Para obtener más información, vea Configuración de un nombre de dominio personalizado.

1. Vaya al Centro de administración de Microsoft 365 e inicie sesión con su cuenta de administrador.

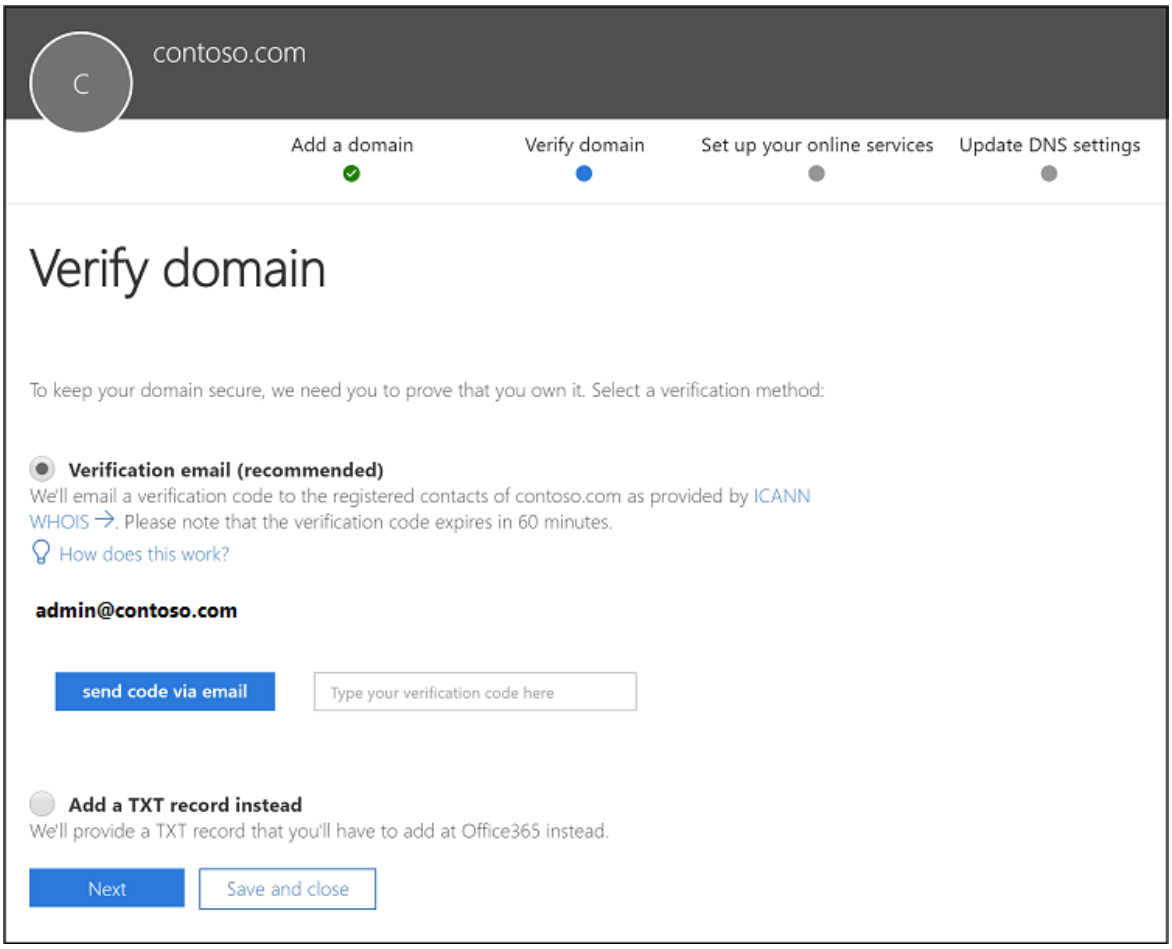
2. En el panel de navegación, seleccione **Configuración** > **Dominios** > **Agregar dominio**.

3. Escriba su nombre de dominio personalizado. A continuación, seleccione **Siguiente**.



4. Compruebe que es el propietario del dominio que escribió en el paso anterior.

   Si selecciona **enviar el código por correo electrónico**, recibirá un correo electrónico en la dirección de contacto registrada para el dominio. Después de recibir el correo electrónico, copie el código e introdúzcalo en el campo **Escriba aquí su código de verificación**. Si el código de verificación es correcto, el dominio se agregará a su inquilino. El correo electrónico que se muestra puede no resultarle familiar. Algunos registradores ocultan la dirección de correo electrónico real. Además, puede que la dirección de correo electrónico sea distinta de la que se proporcionó cuando se registró el dominio.



> **NOTE**
> Para obtener detalles de la comprobación de registros TXT, consulte Crear registros DNS en cualquier proveedor de hospedaje DNS para Microsoft 365.

Experiencias del administrador

Hay dos portales que usará con mayor frecuencia:

- El Centro de administración de Microsoft Endpoint Manager (https://endpoint.microsoft.com/) es donde puede explorar las funcionalidades de Intune. Aquí es donde un administrador puede trabajar con Intune.
- El Centro de administración de Microsoft 365 (https://admin.microsoft.com) es donde puede agregar y administrar usuarios si no usa Azure Active Directory para esta tarea. También puede administrar otros aspectos de su cuenta, como la facturación y el soporte técnico.

Pasos siguientes

En este tutorial de inicio rápido ha creado una suscripción gratuita para probar Intune en un entorno de prueba. Para obtener más información sobre cómo configurar Intune, vea Configurar Intune.

Para seguir esta serie de tutoriales de inicio rápido de Intune, pase al siguiente tutorial de inicio rápido.

Inicio rápido: Crear un usuario y asignarle una licencia

Inicio rápido: Creación de un usuario en Intune y asignación de una licencia

14/05/2021 • 2 minutes to read

En este inicio rápido, creará un usuario y le asignará una licencia de Intune. Al usar Intune, toda persona que necesite tener acceso a los datos de la empresa deberá tener su propia cuenta de usuario. Los administradores de Intune pueden configurar a los usuarios más adelante para administrar el control de acceso.

Requisitos previos

- Suscripción a Microsoft Intune. Suscríbase para disfrutar de una cuenta de prueba gratuita.

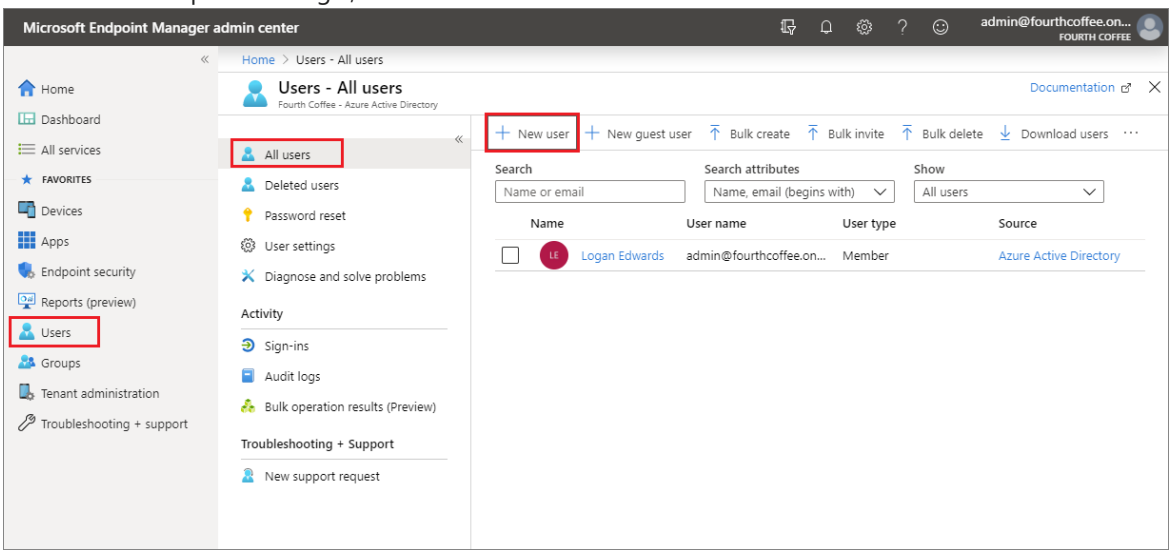
Inicio de sesión en Intune en Microsoft Endpoint Manager

Inicie sesión en el Centro de administración de Microsoft Endpoint Manager como administrador global o administrador de servicios de Intune. Si ha creado una suscripción de prueba de Intune, la cuenta con la que la haya creado es el administrador global.

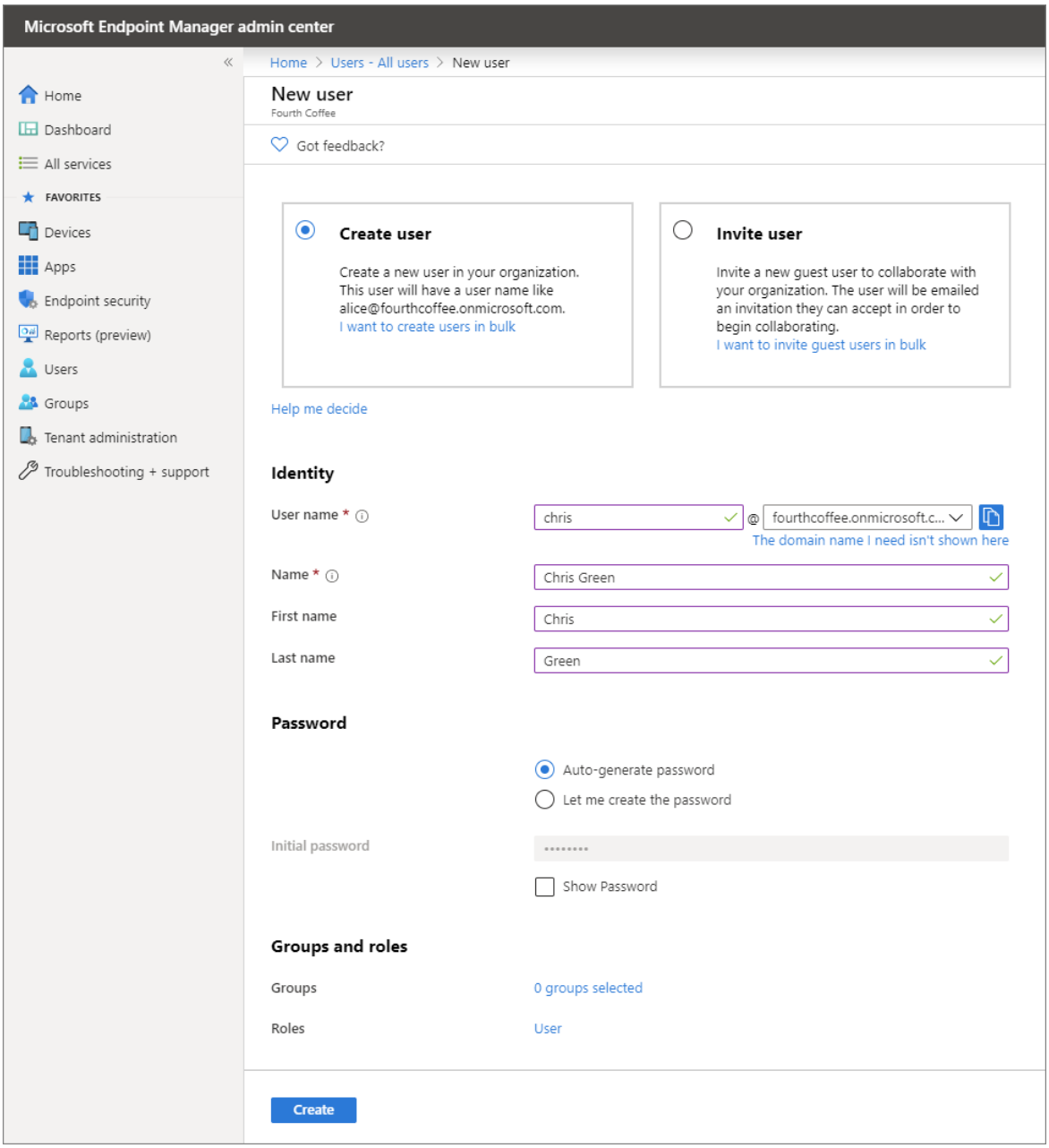
Creación de un usuario

Un usuario debe tener una cuenta de usuario para poder inscribirse en la administración de dispositivos de Intune. Para crear un usuario:

1. En Microsoft Endpoint Manager, seleccione **Usuarios** > **Todos los usuarios** > **Nuevo usuario**:



2. En el cuadro **Nombre**, escriba un nombre, como *Isabel Robledo*:



3. En el cuadro **Nombre de usuario**, escriba un identificador de usuario, como Dewey@contoso.onmicrosoft.com.

> **NOTE**
> Si no ha configurado el nombre de dominio del cliente, use el nombre de dominio comprobado que usó para crear la suscripción de Intune (o evaluación gratuita).

4. Seleccione **Mostrar contraseña** y asegúrese de recordar la contraseña generada automáticamente para que pueda iniciar sesión en un dispositivo de prueba.

5. Seleccione **Crear**.

Asignar una licencia a un usuario

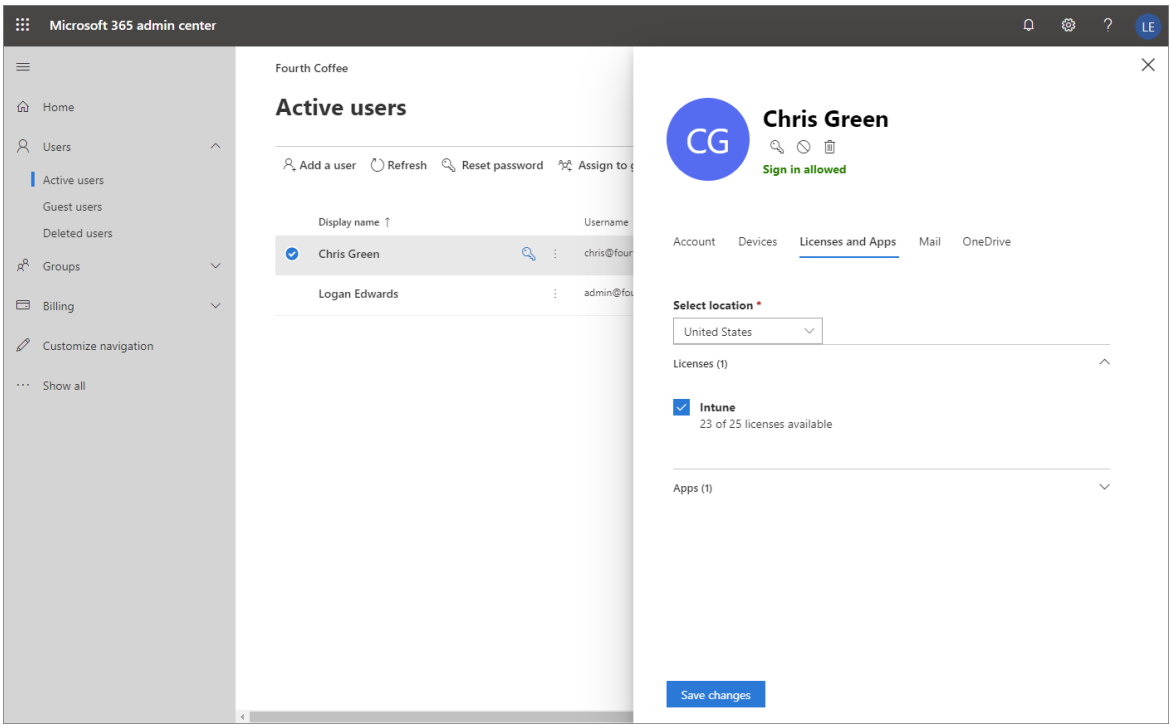
Después de crear un usuario, debe usar el Centro de administración de Microsoft 365 para asignarle una licencia de Intune. Si no se le asigna una licencia al usuario, no podrá inscribir su dispositivo en Intune.

Para asignar una licencia de Intune a un usuario:

1. Inicie sesión en el Centro de administración de Microsoft 365 con las mismas credenciales que ha usado

para iniciar sesión en Intune.

2. Seleccione **Usuarios** > **Usuarios activos** y, luego, seleccione el usuario que acaba de crear.
3. Seleccione la pestaña **Licencias y aplicaciones**.
4. En **Seleccionar ubicación**, seleccione una ubicación para el usuario, si todavía no se establece.
5. Active la casilla **Intune** en la sección **Licencias**. Si otra licencia incluye Intune, puede seleccionar esa licencia. El nombre de producto que se muestra se usa como plan de servicio en la administración de Azure.



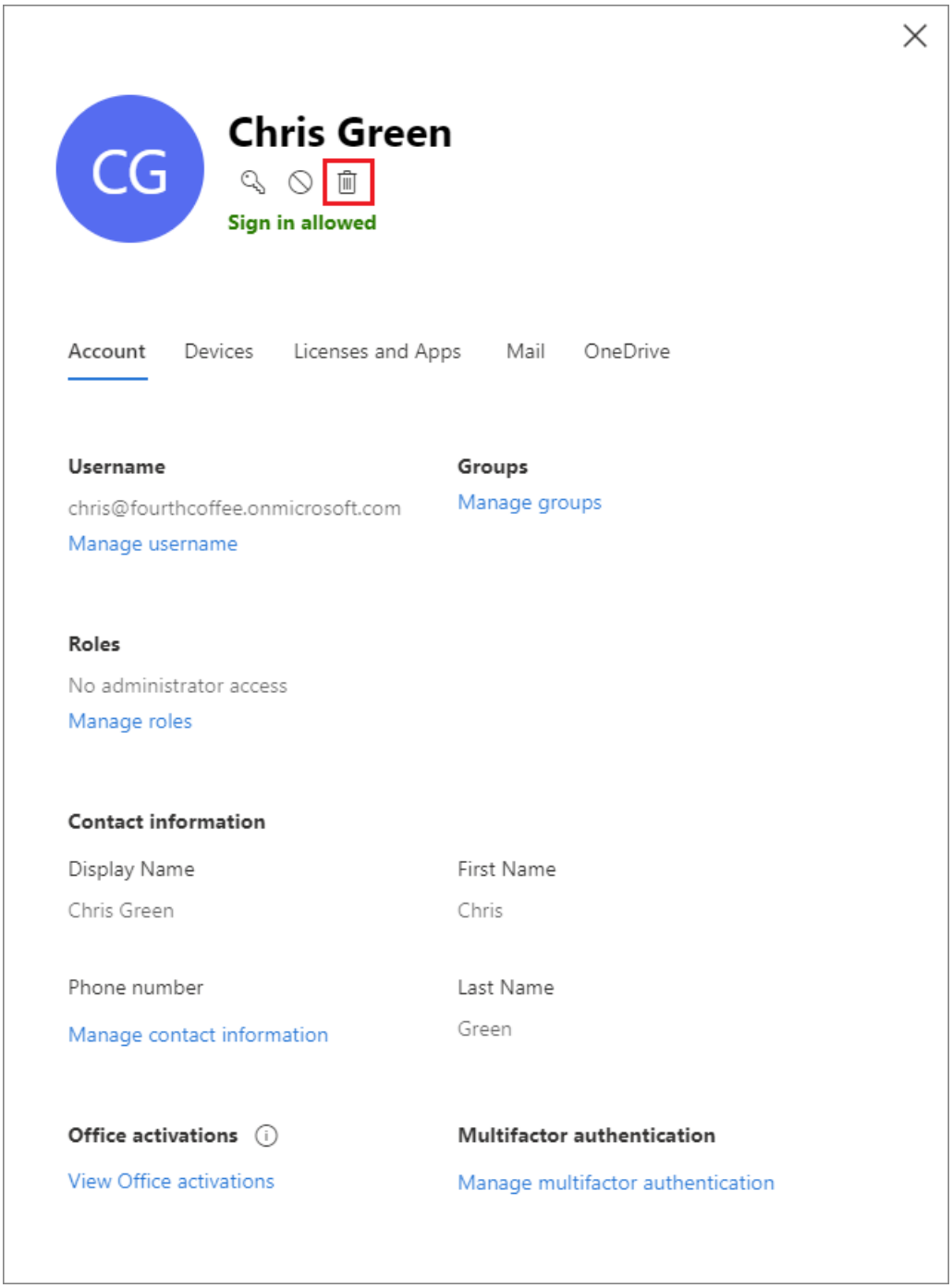
> **NOTE**
> Este valor usa una de las licencias del usuario. Si usa un entorno de evaluación, más tarde reasignará esta licencia a un usuario real en un entorno activo.

6. Seleccione **Guardar cambios**.

Ahora el nuevo usuario activo de Intune mostrará que está usando una licencia de **Intune**.

Limpieza de recursos

Si ya no necesita ese usuario, puede eliminarlo en el Centro de administración de Microsoft 365. Ahí, seleccione **Usuarios** > *el usuario* > *el icono de eliminación del usuario* > **Eliminar usuario** > **Cerrar**.



Pasos siguientes

En este inicio rápido, creó un usuario y le asignó una licencia de Intune. Para obtener más información sobre cómo agregar usuarios a Intune, consulte Adición de usuarios y concesión de permiso administrativo a Intune.

Para seguir esta serie de inicios rápidos de Intune, vaya al siguiente:

Inicio rápido: Crear un grupo para administrar usuarios

Inicio rápido: Crear un grupo para administrar usuarios

14/05/2021 • 2 minutes to read

En este inicio rápido, usará Intune para crear un grupo basado en un usuario existente. Los grupos se usan para administrar los usuarios y controlar el acceso de los empleados a los recursos de la empresa. Estos recursos pueden formar parte de la intranet de la empresa o ser recursos externos, como sitios de SharePoint, aplicaciones de SaaS o aplicaciones web.

Si no tiene una suscripción a Intune, regístrese para obtener una cuenta de prueba gratuita.

> **NOTE**
> Intune ofrece los grupos creados previamente **Todos los usuarios** y **Todos los dispositivos** en la consola con las optimizaciones integradas para su comodidad.

Requisitos previos

- Suscripción a Microsoft Intune: regístrese para obtener una cuenta de prueba gratuita.
- Para completar este inicio rápido, debe crear un usuario.

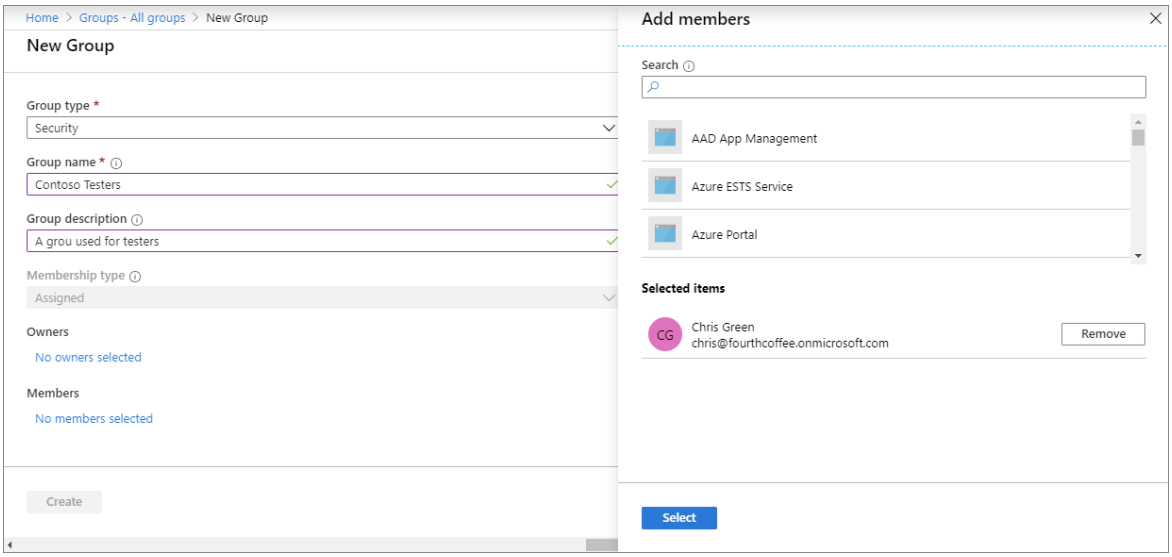
Inicio de sesión en Intune en Microsoft Endpoint Manager

Inicie sesión en el Centro de administración de Microsoft Endpoint Manager como administrador global o administrador de servicios de Intune. Si ha creado una suscripción de prueba de Intune, la cuenta con la que creó la suscripción es el administrador global.

Crear un grupo

Creará un grupo que se usará más adelante en esta serie de inicio rápido. Para crear un grupo:

1. Una vez que abra Microsoft Endpoint Manager, seleccione **Grupos** > **Nuevo grupo**.
2. En el cuadro desplegable **Tipo de grupo**, seleccione **Seguridad**.
3. En el campo **Nombre del grupo**, escriba el nombre del grupo nuevo (por ejemplo, **Contoso Testers** [Evaluadores de Contoso]).
4. Agregue una **descripción del grupo** para el grupo.
5. Establezca **Tipo de miembro** en **Asignado**.
6. En **Miembros**, seleccione el vínculo y agregue uno o más miembros para el grupo de la lista.



7. Haga clic en **Seleccionar** > **Crear**.

Cuando haya creado correctamente el grupo, aparecerá en la lista **Todos los grupos**.

Pasos siguientes

En este inicio rápido, usó Intune para crear un grupo basado en un usuario existente. Para obtener más información sobre cómo agregar grupos a Intune, consulte Agregar grupos para organizar usuarios y dispositivos.

Para seguir esta serie de tutoriales de inicio rápido de Intune, pase al siguiente tutorial de inicio rápido.

Inicio rápido: Configurar la inscripción automática para dispositivos Windows 10

Inicio rápido: Crear y asignar un rol personalizado

14/05/2021 • 2 minutes to read

En este inicio rápido de Intune, creará un rol personalizado con permisos específicos para un departamento de operaciones de seguridad. Después, asignará el rol a un grupo de operadores de este tipo. Hay varios roles predeterminados que puede usar de inmediato. Pero al crear roles personalizados como este, tendrá control de acceso preciso a todas las partes del sistema de administración de dispositivos móviles.

Si no dispone de ninguna suscripción a Intune, regístrese para obtener una cuenta de evaluación gratuita.

Requisitos previos

- Para completar este inicio rápido, debe crear un grupo.

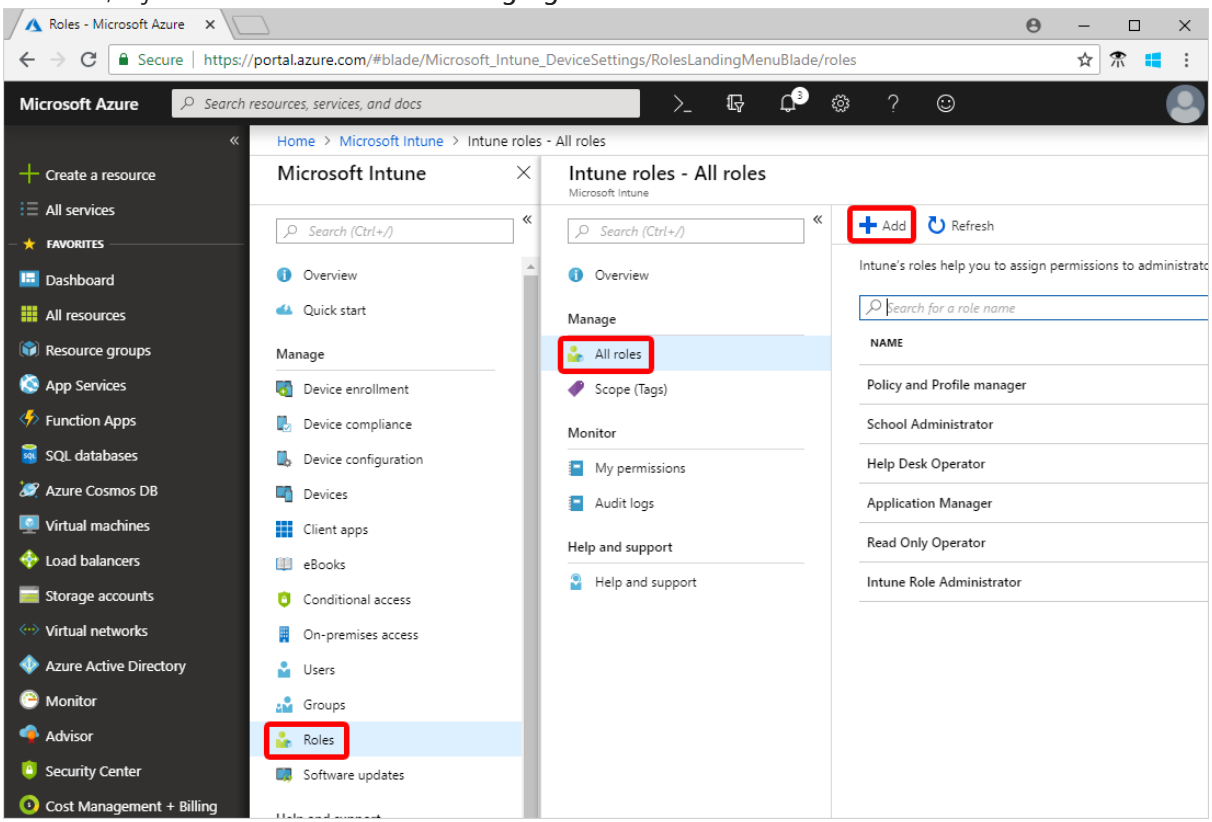
Iniciar sesión en Intune

Inicie sesión en Intune como administrador global o administrador de servicios de Intune. Si ha creado una suscripción de prueba de Intune, la cuenta con la que creó la suscripción es el administrador global.

Crear un rol personalizado

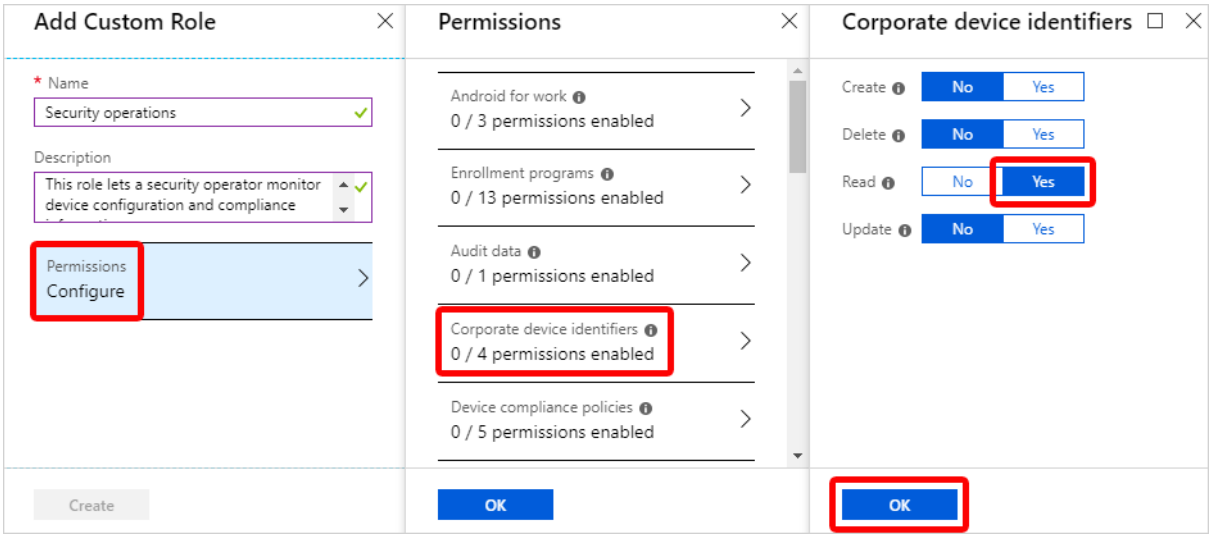
Cuando se crea un rol personalizado, se pueden establecer permisos para una amplia gama de acciones. Para el rol de operaciones de seguridad, estableceremos algunos permisos de lectura para que el operador pueda revisar las configuraciones y las directivas de un dispositivo.

1. En Intune, elija **Roles** > **Todos los roles** > **Agregar**.



2. En **Agregar rol personalizado**, en el cuadro **Nombre**, escriba *Operaciones de seguridad*.
3. En el cuadro **Descripción**, escriba *Este rol permite a un operador de seguridad supervisar la configuración del dispositivo y la información de cumplimiento.*

4. Elija **Configurar** > **Identificadores de dispositivo corporativos** > **Sí** junto a **Lectura** > **Aceptar**.



5. Elija **Todas las directivas de cumplimiento de los dispositivos** > **Sí** junto a **Lectura** > **Aceptar**.
6. Elija **Configuraciones de dispositivos** > **Sí** junto a **Lectura** > **Aceptar**.
7. Elija **Organización** > **Sí** junto a **Lectura** > **Aceptar**.
8. Elija **Aceptar** > **Crear**.

Asignar el rol a un grupo

Para que el operador de seguridad pueda usar los nuevos permisos, debe asignar el rol a un grupo que contenga el usuario de seguridad.

1. En Intune, elija **Roles** > **Todos los roles** > **Security operations** (Operaciones de seguridad).
2. En **Roles de Intune**, elija **Asignaciones** > **Asignar**.
3. En el cuadro **Nombre de asignación**, escriba *Oper. seg.*
4. Elija **Miembros (grupos)** > **Agregar**.
5. Elija el grupo **Contoso Testers** (Evaluadores de Contoso).
6. Elija **Seleccionar** > **Aceptar**.
7. Elija **Ámbito (grupos)** > **Seleccionar grupos para incluir** > **Contoso Testers** (Evaluadores de Contoso).
8. Elija **Seleccionar** > **Aceptar** > **Aceptar**.

Ahora, todos los miembros del grupo pertenecen al rol *Operaciones de seguridad* y pueden revisar esta información sobre un dispositivo: identificadores de dispositivos corporativos, directivas de cumplimiento de dispositivos, configuraciones de dispositivo e información de organización.

Limpieza de recursos

Si ya no quiere usar más el nuevo rol personalizado, puede eliminarlo. Elija **Roles** > **Todos los roles** > elija el botón de puntos suspensivos junto al rol > **Eliminar**.

Pasos siguientes

En este tutorial ha creado un rol de operaciones de seguridad personalizado y lo ha asignado a un grupo. Para obtener más información sobre los roles de Intune, consulte Control de administración basada en roles (RBAC) con Microsoft Intune

Para seguir esta serie de tutoriales de inicio rápido de Intune, pase al siguiente tutorial de inicio rápido.

Inicio rápido: Creación de un perfil de dispositivo de correo para iOS/iPadOS

Tutorial: Tutorial de Intune en Microsoft Endpoint Manager

14/05/2021 • 13 minutes to read

Microsoft Intune, que forma parte de Microsoft Endpoint Manager, proporciona la infraestructura en la nube, la administración de dispositivos móviles (MDM) basados en la nube, la administración de aplicaciones móviles (MAM) basadas en la nube y la administración de equipos basados en la nube para su organización. Intune ayuda a asegurarse de que los dispositivos, aplicaciones y datos empresariales cumplen los requisitos de seguridad de la empresa. Tiene el control para establecer qué requisitos se deben comprobar y qué sucede cuando no se cumplen. En el Centro de administración de Microsoft Endpoint Manager puede encontrar el servicio Microsoft Intune, así como otras opciones relacionadas con la administración de dispositivos. Comprender las características disponibles en Intune le ayudará a realizar diferentes tareas de administración de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM).

> **NOTE**
> Microsoft Endpoint Manager es una plataforma de administración de puntos de conexión única e integrada para la administración de todos los puntos de conexión. Este Centro de administración de Microsoft Endpoint Manager integra ConfigMgr y Microsoft Intune.

En este tutorial, aprenderá a:

- Recorrer el Centro de administración de Microsoft Endpoint Manager
- Personalizar la vista del Centro de administración de Microsoft Endpoint Manager

Si no tiene una suscripción a Intune, regístrese para obtener una cuenta de prueba gratuita.

Requisitos previos

Antes de configurar Microsoft Intune, revise los siguientes requisitos:

- Exploradores y sistemas operativos compatibles
- Ancho de banda y requisitos de configuración de red de Intune

Suscríbase para disfrutar de una prueba gratuita de Microsoft Intune

Probar Intune es gratis durante 30 días. Si ya dispone de una cuenta profesional o educativa, **inicie sesión** con dicha cuenta y agregue Intune a su suscripción. En caso contrario, puede registrarse para obtener una cuenta de evaluación gratuita para usar Intune en la organización.

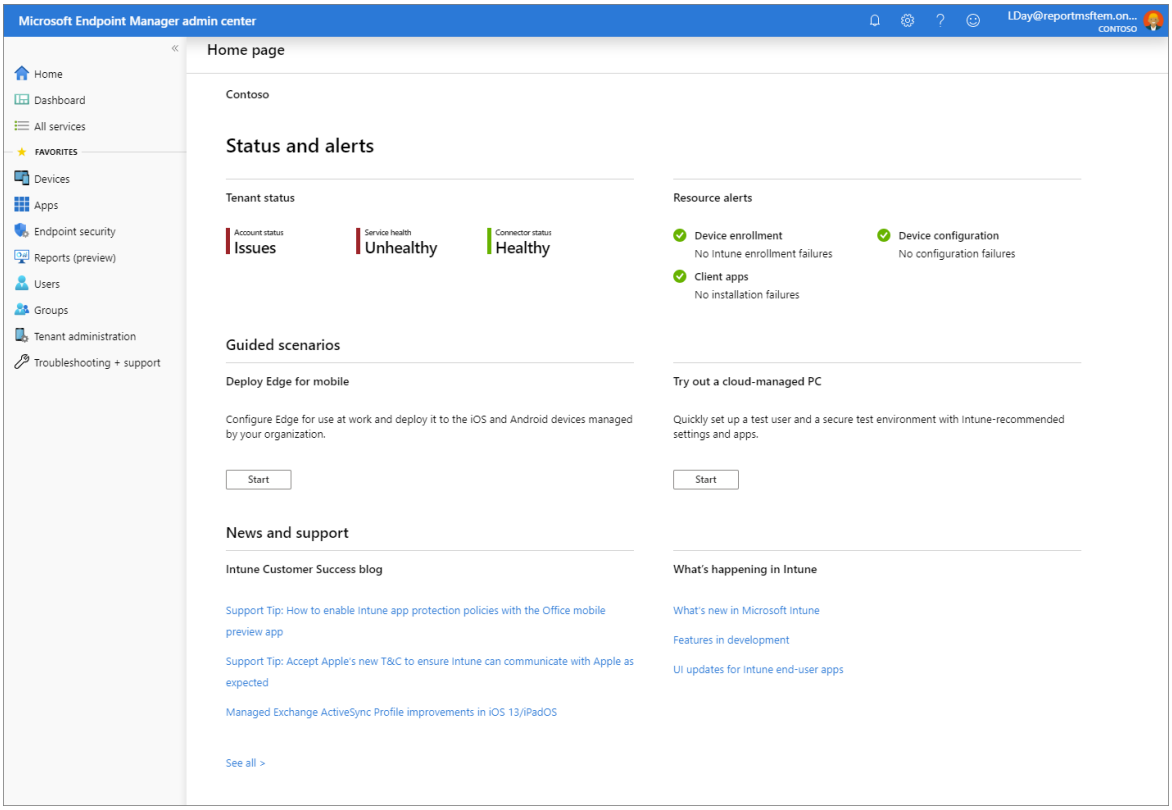
> **IMPORTANT**
> No puede combinar una cuenta profesional o educativa existente después de registrarse con una cuenta nueva.

Paseo por el Centro de administración de Microsoft Endpoint Manager Intune

Siga los pasos que se indican a continuación para comprender mejor Intune en el Centro de administración de

Microsoft Endpoint Manager. Cuando haya completado el paseo, comprenderá mejor algunas de las áreas principales de Intune.

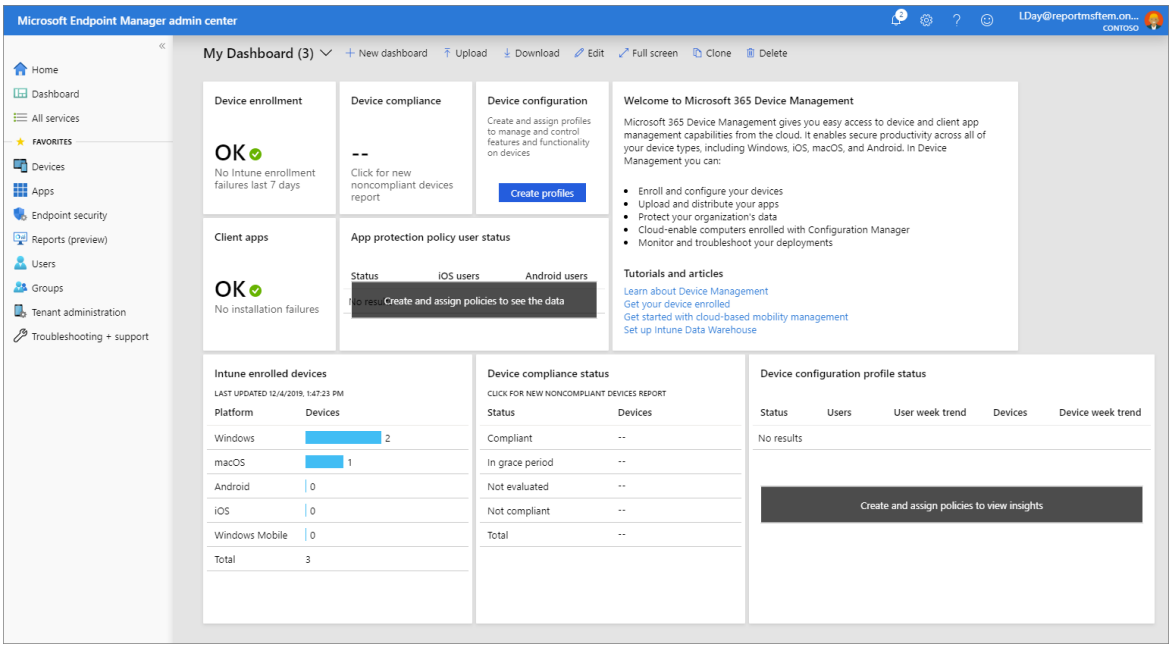
1. Abra un explorador e inicie sesión en el Centro de administración de Microsoft Endpoint Manager. Si es nuevo en Intune, use la suscripción de prueba gratuita.



   Al abrir Microsoft Endpoint Manager, el servicio se muestra en un panel del explorador. Algunas de las primeras cargas de trabajo que es posible que use en Intune incluyen **Dispositivos**, **Aplicaciones**, **Usuarios** y **Grupos**. Una carga de trabajo es simplemente una subárea de un servicio. Al seleccionar la carga de trabajo, el panel se abre como una página completa. Los demás paneles emergen del lado derecho del panel al abrirlos y se cierran para mostrar el panel anterior.

   De forma predeterminada, al abrir Microsoft Endpoint Manager, verá el panel **Página principal**. En este panel se proporciona una instantánea visual general del estado y cumplimiento de los inquilinos, así como otros vínculos relacionados muy útiles.

2. Desde el panel de navegación, seleccione **Panel** para mostrar los detalles generales sobre los dispositivos y las aplicaciones cliente en el inquilino de Intune. Si está empezando con un inquilino de Intune nuevo, todavía no tendrá ningún dispositivo inscrito.



Intune permite administrar los dispositivos y las aplicaciones de sus recursos, incluida la forma de acceder a los datos de la empresa. Para usar este servicio de administración de dispositivos móviles (MDM), primero es necesario inscribir los dispositivos en Intune. Al inscribir un dispositivo, se emite un certificado MDM. Dicho certificado se usa para la comunicación con el servicio de Intune.

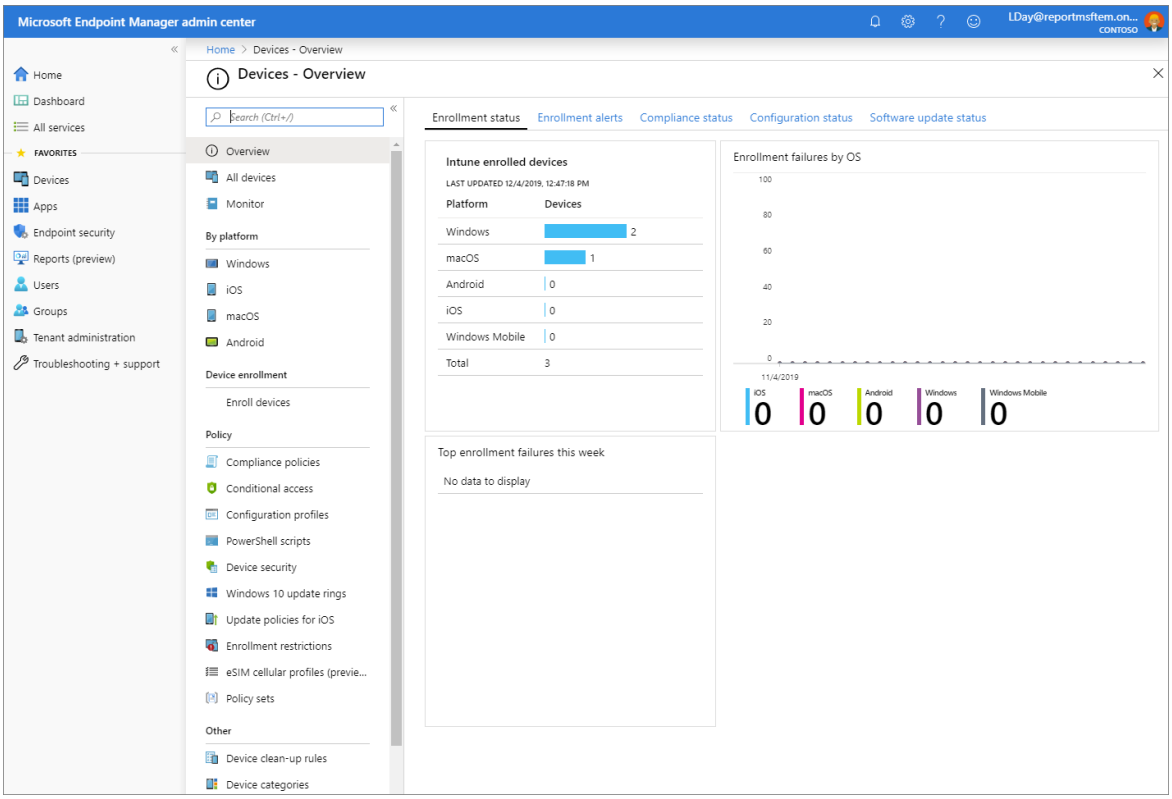
Hay varios métodos para inscribir los dispositivos de los recursos en Intune. Cada método depende de la propiedad del dispositivo (personal o corporativo), el tipo de dispositivo (iOS/iPadOS, Windows o Android) y los requisitos de administración (restablecimiento, afinidad o bloqueo). Pero antes de poder habilitar la inscripción de dispositivos, debe configurar la infraestructura de Intune. En concreto, la inscripción de dispositivos requiere que establezca su autoridad de MDM. Para más información sobre cómo preparar el entorno de Intune (el inquilino), vea Configurar Intune. Una vez que el inquilino de Intune esté listo, puede inscribir los dispositivos. Para obtener más información sobre la inscripción de dispositivos, consulte ¿Qué es la inscripción de dispositivos?

3. Desde el panel de navegación, seleccione **Dispositivos** para mostrar detalles sobre los dispositivos inscritos en el inquilino de Intune.

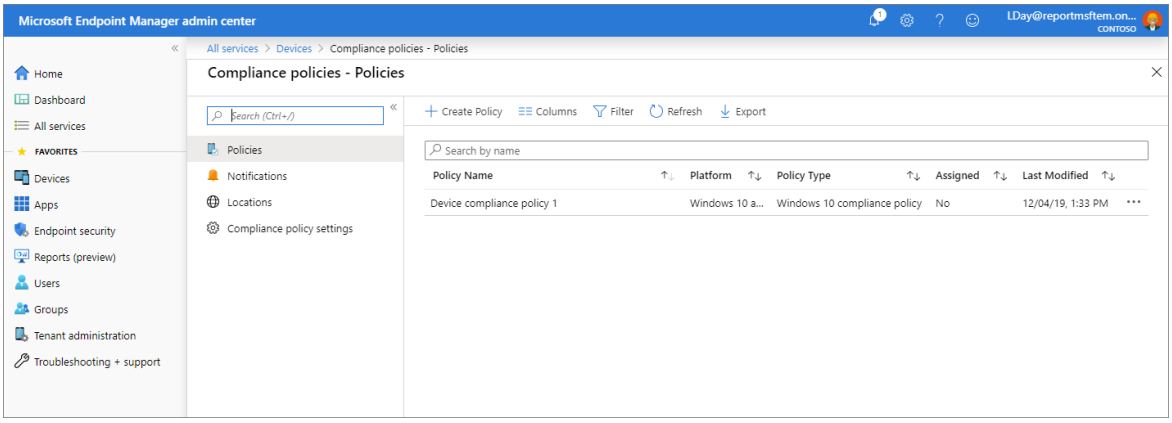
> **TIP**
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Dispositivos**.

El panel **Dispositivos - Información general** tiene varias pestañas que permiten ver un resumen de los siguientes estados y alertas:

- **Estado de inscripción**: revise los detalles de los dispositivos inscritos en Intune por plataforma e inscripción.
- **Alertas de inscripción**: busque más detalles sobre los dispositivos sin asignar por plataforma.
- **Estado de cumplimiento**: revise el estado de cumplimiento en función del dispositivo, la directiva, la configuración, las amenazas y la protección. Además, en este panel se proporciona una lista de dispositivos sin una directiva de cumplimiento.
- **Estado de la configuración**: revise el estado de configuración de los perfiles de dispositivo, así como la implementación del perfil, y
- **Estado de actualización de software**: vea una representación visual del estado de implementación para todos los dispositivos y usuarios.



4. Desde el panel **Dispositivos: Información general**, seleccione **Directivas de cumplimiento** para mostrar detalles sobre el cumplimiento de los dispositivos administrados por Intune. Verá información similar a la de la imagen siguiente.



> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Cumplimiento de dispositivos**.

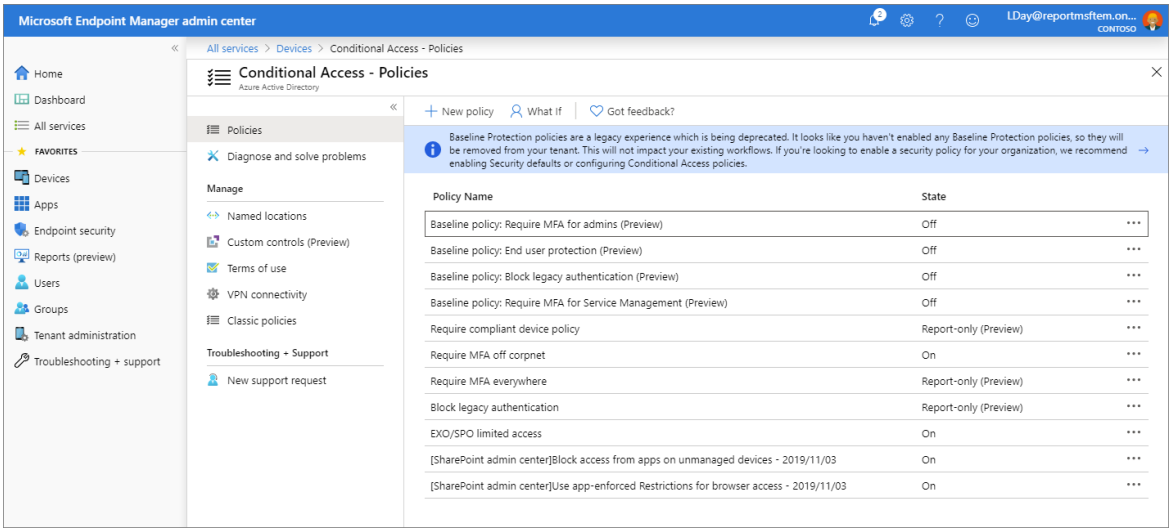
Los requisitos de cumplimiento son básicamente reglas, como requerir un PIN de dispositivo o el cifrado del dispositivo. Las directivas de cumplimiento de dispositivos definen las reglas y configuraciones que debe seguir un dispositivo para que se considere compatible. Para usar la conformidad de dispositivos, debe tener lo siguiente:

- Una suscripción a Intune y a Azure Active Directory (Azure AD) Premium.
- Dispositivos que ejecuten una plataforma admitida.
- Dispositivos inscritos en Intune.
- Dispositivos inscritos en un usuario o ningún usuario primario.

Para más información, vea Introducción a las directivas de cumplimiento de dispositivos de Intune.

5. Desde el panel **Dispositivos - Información general**, seleccione **Acceso condicional** para mostrar

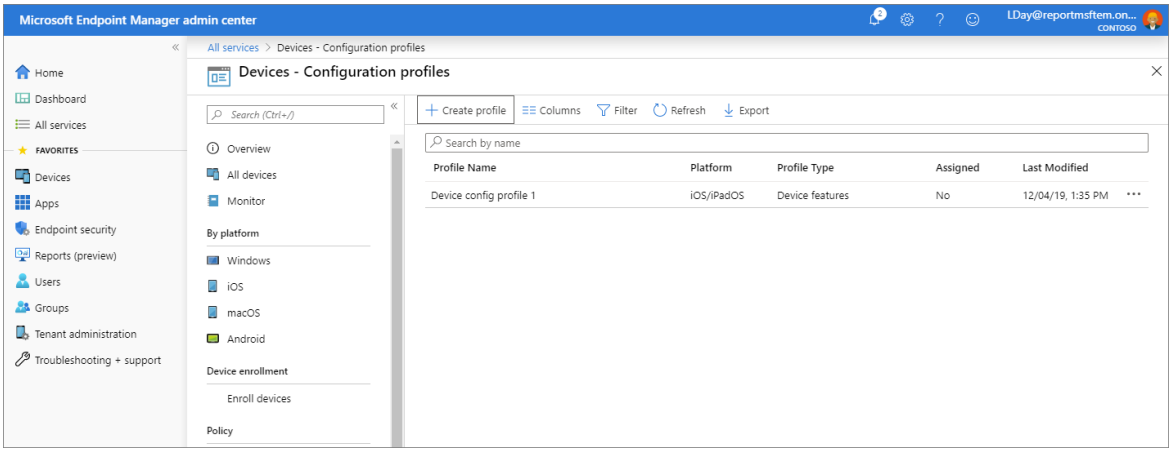
detalles sobre las directivas de acceso.



> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Acceso condicional**.

El acceso condicional hace referencia a las formas en que puede controlar los dispositivos y las aplicaciones que pueden conectarse a los recursos del correo electrónico y la empresa. Para información sobre el acceso condicional basado en dispositivos y aplicaciones y buscar escenarios comunes para usar el acceso condicional con Intune, consulte ¿Qué es el acceso condicional?

6. Desde el panel de navegación, seleccione **Dispositivos** > **Perfiles de configuración** para mostrar detalles sobre los perfiles de dispositivo en Intune.

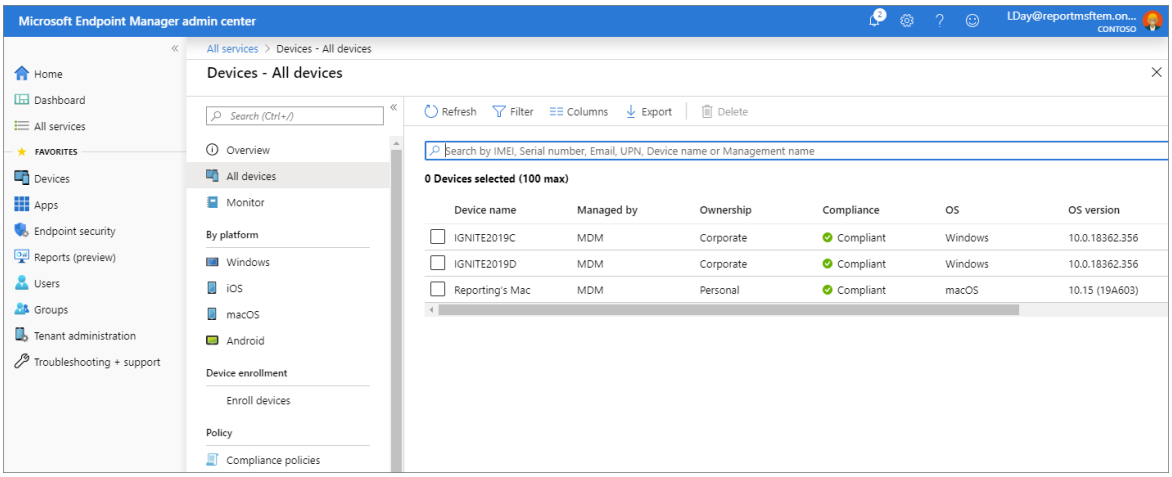


> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Configuración de dispositivos**.

Intune incluye opciones y características que se pueden habilitar o deshabilitar en distintos dispositivos dentro de la organización. Estas características y opciones de configuración se agregan a los "perfiles de configuración". Puede crear perfiles para otros dispositivos y plataformas, incluidas iOS/iPadOS, Android, macOS y Windows. Después, puede usar Intune para aplicar el perfil a los dispositivos de la organización.

Para más información sobre la configuración de dispositivos, vea Aplicación de la configuración de características en dispositivos con perfiles de dispositivos Microsoft Intune.

7. Desde el panel de navegación, seleccione **Dispositivos** > **Todos los dispositivos** para mostrar detalles sobre los dispositivos inscritos en el inquilino de Intune. Si está empezando con una inscripción de Intune nueva, todavía no tendrá dispositivos inscritos.



En esta lista de dispositivos se muestran detalles clave sobre el cumplimiento, la versión del sistema operativo y la última fecha de inserción en el repositorio.

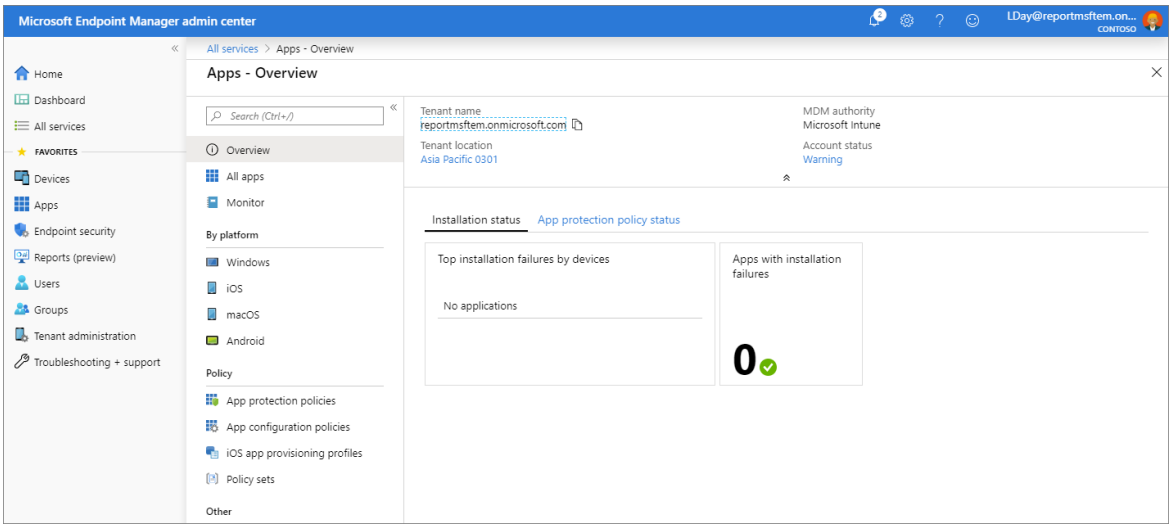
> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Dispositivos** > **Todos los dispositivos**.

8. En el panel de navegación, seleccione **Aplicaciones** para mostrar información general sobre el estado de la aplicación. En este panel se proporciona el estado de instalación de la aplicación en función de las pestañas siguientes:

> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Aplicaciones cliente**.

El panel **Aplicaciones - Información general** tiene dos pestañas que le permiten ver un resumen de los siguientes estados:

- **Estado de la instalación**: puede ver los principales errores de instalación por dispositivo, así como las aplicaciones con errores de instalación.
- **Estado de la directiva de protección de aplicaciones**: encuentre detalles sobre los usuarios asignados a las directivas de protección de aplicaciones, así como los usuarios marcados.



Como administrador de TI, puede usar Microsoft Intune para administrar las aplicaciones cliente que usan los trabajadores de su empresa. Esta funcionalidad se suma a la administración de dispositivos y la protección de datos. Una de las prioridades de un administrador es garantizar que los usuarios finales tengan acceso a las aplicaciones que necesitan para hacer su trabajo. Aparte de todo esto, puede que quiera asignar y administrar aplicaciones en dispositivos que no están inscritos en Intune. Intune ofrece diversas funcionalidades para ayudarle a conseguir las aplicaciones que necesita y en los dispositivos de su elección.

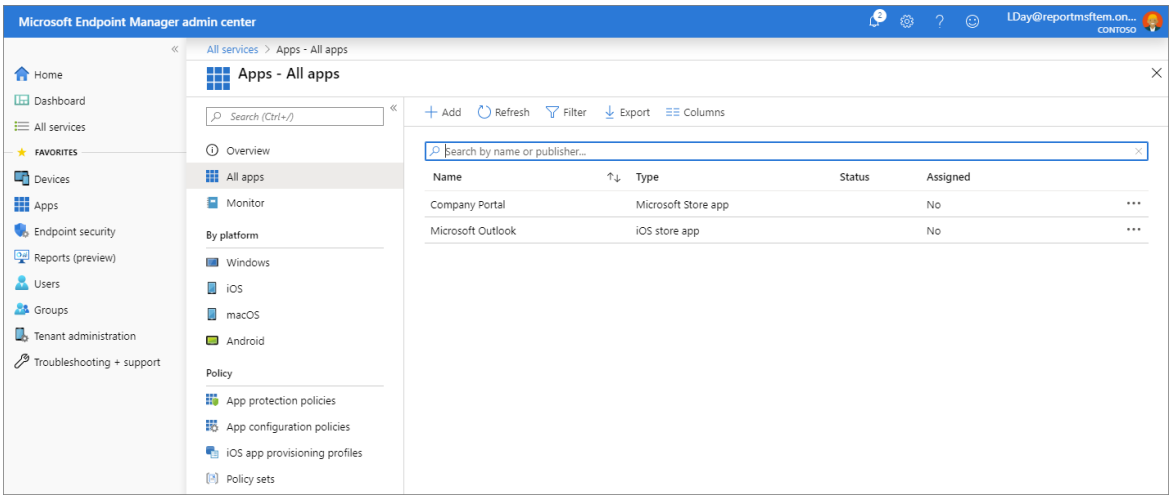
> **NOTE**
> En el panel **Aplicaciones - Información general** también se proporcionan detalles sobre el estado y la cuenta del inquilino.

Para más información sobre cómo agregar y asignar aplicaciones, vea Incorporación de aplicaciones a Microsoft Intune y Asignación de aplicaciones a grupos con Microsoft Intune.

9. En el panel **Aplicaciones - Información general**, seleccione **Todas las aplicaciones** para ver una lista de las aplicaciones que se han agregado a Intune.

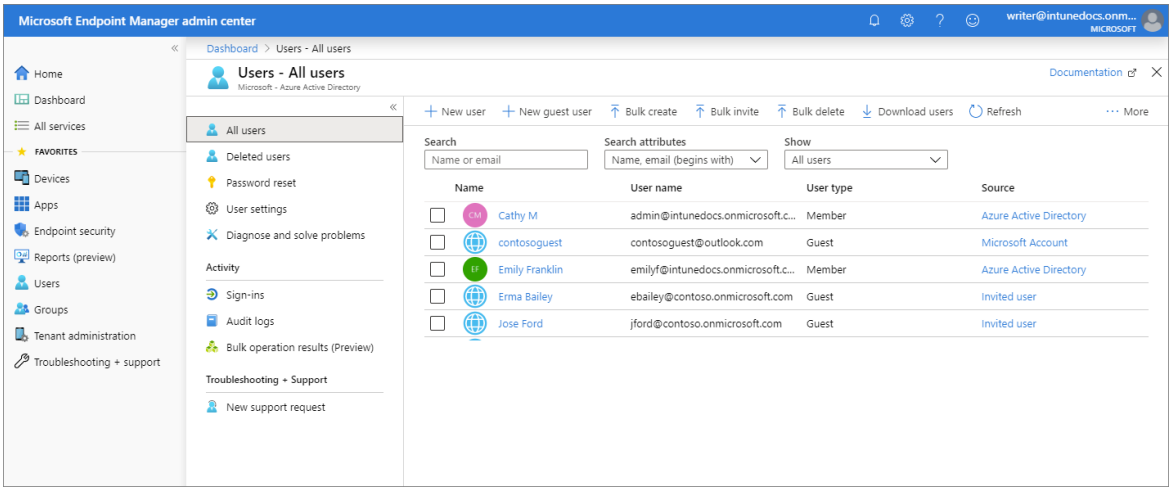
> **TIP**
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Aplicaciones cliente** > **Aplicaciones**.

Puede agregar a Intune una variedad de tipos de aplicación diferentes en función de la plataforma. Una vez que se ha agregado una aplicación, puede asignarla a grupos de usuarios.



Para más información, vea Agregar aplicaciones a Microsoft Intune.

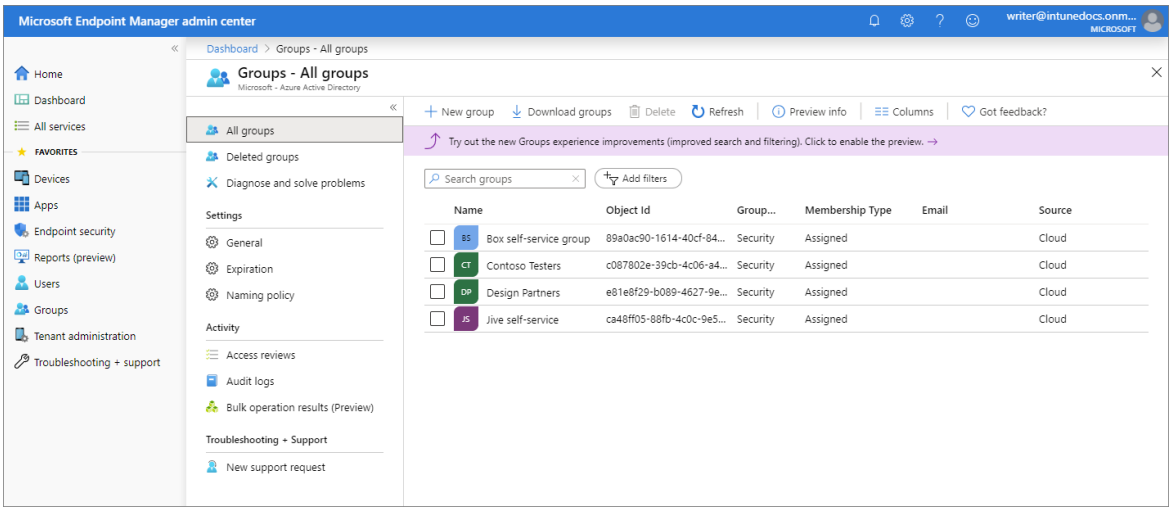
10. Desde el panel de navegación, seleccione **Usuarios** para mostrar detalles sobre los usuarios que haya incluido en Intune. Estos usuarios son los recursos de la empresa.



> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Usuarios**.

Puede agregar usuarios directamente a Intune o sincronizarlos desde la instancia local de Active Directory. Una vez agregados, los usuarios pueden inscribir dispositivos y obtener acceso a los recursos de la empresa. También puede asignar permisos adicionales a los usuarios para que accedan a Intune. Para más información, vea Adición de usuarios y concesión de permiso administrativo a Intune.

11. Desde el panel de navegación, seleccione **Grupos** para mostrar detalles sobre los grupos de Azure Active Directory (Azure AD) incluidos en Intune. Como administrador de Intune, los grupos se usan para administrar usuarios y dispositivos.



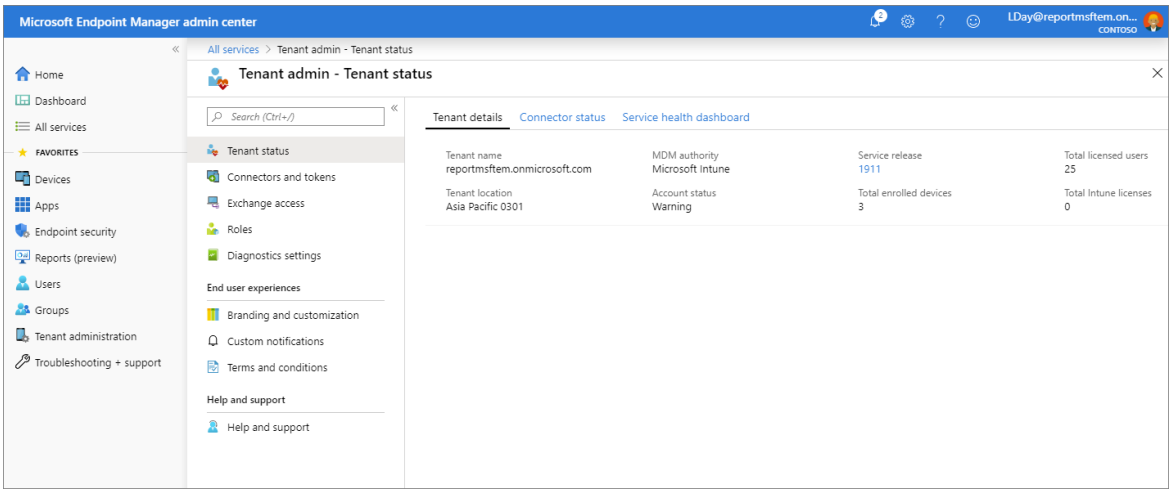
> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Grupos**.

Puede configurar grupos para satisfacer sus necesidades organizativas. Cree grupos para organizar a los usuarios o dispositivos por ubicación geográfica, departamento o características de hardware. Use los grupos para administrar tareas a escala. Por ejemplo, puede establecer directivas para muchos usuarios o implementar aplicaciones para un conjunto de dispositivos. Para más información sobre los grupos, vea Agregar grupos para organizar usuarios y dispositivos.

12. Desde el panel de navegación, seleccione **Administración de inquilinos** para mostrar detalles sobre el inquilino de Intune.

> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Estado de inquilino**.

En el panel **Administración de inquilinos - Estado de inquilino** se proporcionan pestañas para **Detalles del inquilino**, **Estado del conector** y **Panel de Service Health**. Si hay problemas con el inquilino o propios de Intune, encontrará los detalles en este panel.



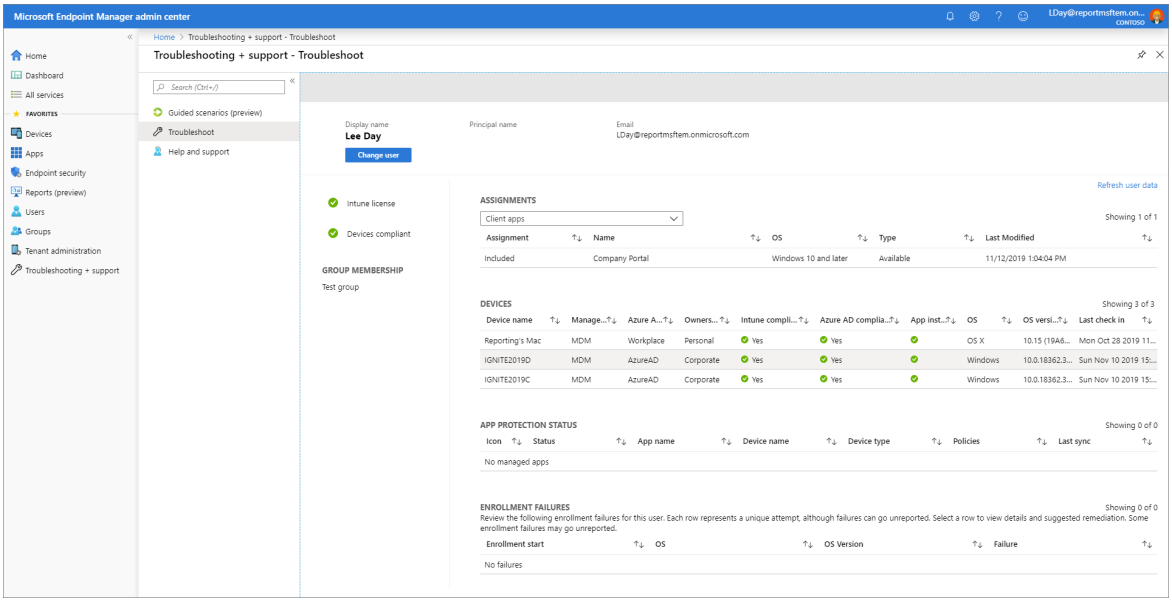
Para más información, vea Estado del inquilino de Intune.

13. Desde el panel de navegación, seleccione **Solución de problemas + soporte técnico** > **Solucionar**

problemas para comprobar los detalles de estado de un usuario específico.

> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Solucionar problemas**.

En la lista desplegable **Asignaciones**, puede elegir ver las asignaciones de destino de las aplicaciones cliente, las directivas, los anillos de actualización y las restricciones de inscripción. Además, en este panel se proporcionan detalles del dispositivo, el estado de protección de la aplicación y los errores de inscripción para un usuario específico.

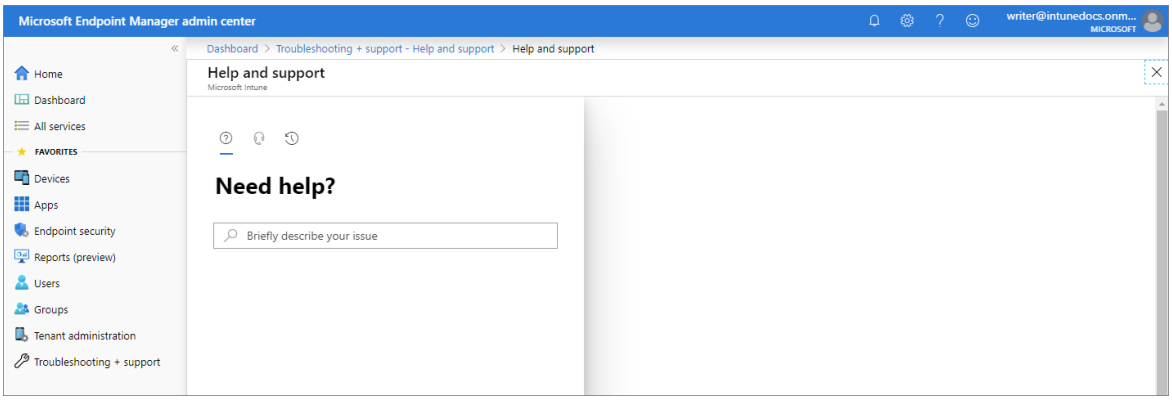


Para más información sobre la solución de problemas con Intune, vea Uso del portal de solución de problemas para ayudar a los usuarios de su empresa.

14. Desde el panel de navegación, seleccione **Solución de problemas + soporte técnico** > **Ayuda y soporte técnico** para solicitar ayuda.

> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Ayuda y soporte técnico**.

Como administrador de TI, puede usar la opción **Ayuda y soporte técnico** para buscar y ver soluciones, y también para registrar una incidencia de soporte técnico en línea sobre Intune.



Para crear una incidencia de soporte técnico, la cuenta debe tener asignado un rol de administrador en

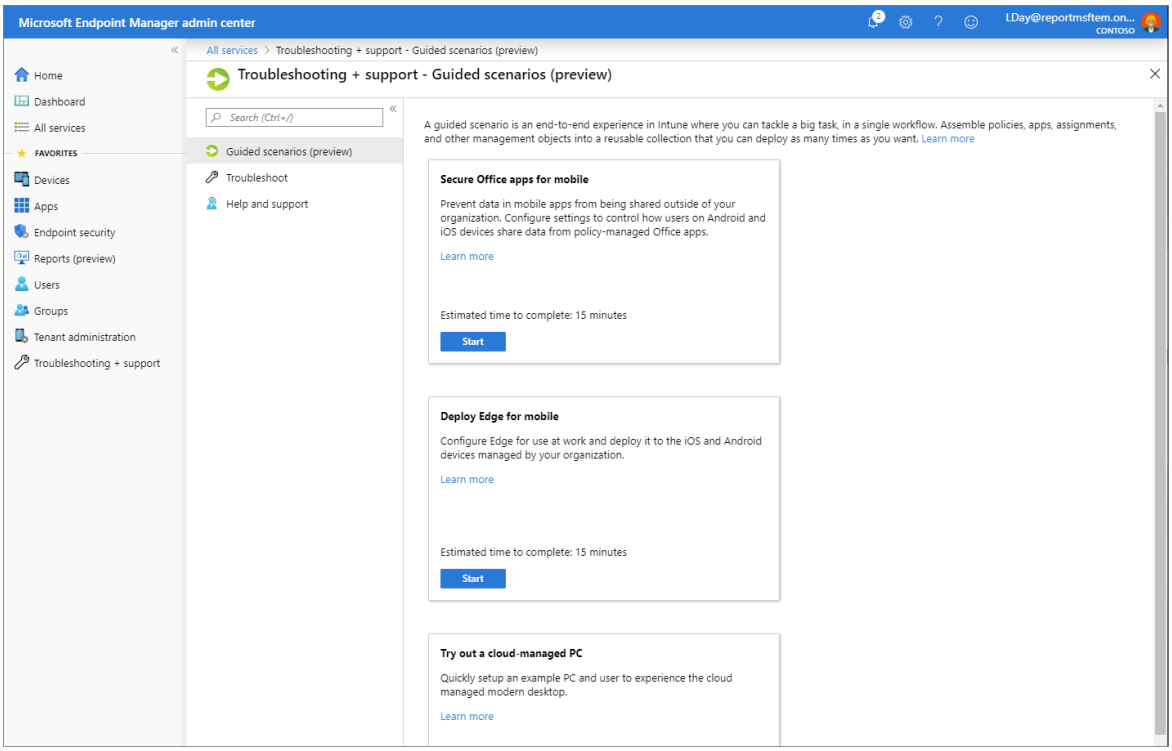
Azure Active Directory. Los roles de administrador incluyen **Administrador de Intune**, **Administrador Global** y **Administrador de servicios**.

Para más información, consulte el artículo sobre procedimientos para obtener soporte técnico en Microsoft Endpoint Manager.

15. Desde el panel de navegación, seleccione **Solución de problemas + soporte técnico** > **Escenarios guiados** para mostrar los escenarios de Intune disponibles.

    Un escenario guiado es una serie personalizada de pasos en torno a un caso de uso completo. Los escenarios más habituales se basan en el rol que un administrador, un usuario o un dispositivo desempeñan en la organización. Estos roles suelen requerir una colección de perfiles, opciones, aplicaciones y controles de seguridad cuidadosamente organizados para proporcionar la mejor experiencia de usuario y seguridad.

    Si no está familiarizado con todos los pasos y recursos necesarios para implementar un determinado escenario de Intune, los escenarios guiados pueden servir de punto de partida.



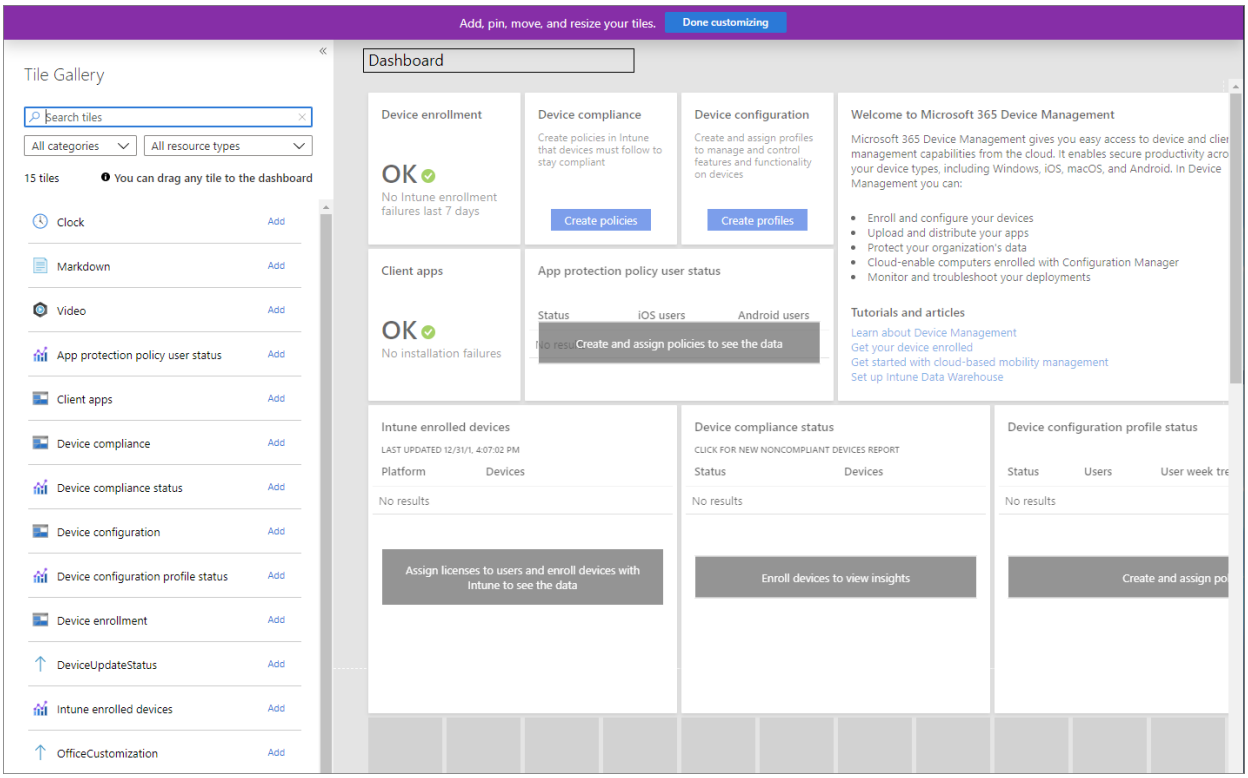
Para más información sobre los escenarios guiados, vea Introducción a los escenarios guiados de Intune.

Configuración del Centro de administración de Microsoft Endpoint Manager

El Centro de administración de Microsoft Endpoint Manager permite personalizar y configurar la vista del portal.

Cambio del panel

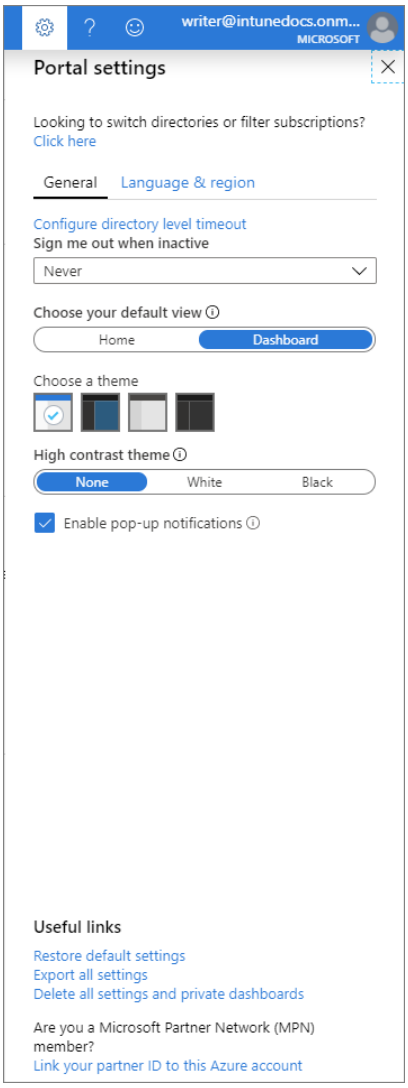
El **Panel** para mostrar los detalles generales sobre los dispositivos y las aplicaciones cliente en el inquilino de Intune. Los paneles proporcionan una manera de crear una vista centrada y organizada en el Centro de administración de Microsoft Endpoint Manager. Use los paneles como un área de trabajo donde puede iniciar rápidamente tareas para las operaciones cotidianas y supervisar los recursos. Cree paneles personalizados basados en proyectos, tareas o roles de usuario, por ejemplo. El Centro de administración de Microsoft Endpoint Manager proporciona un panel predeterminado como punto de partida. Puede editar el panel predeterminado, crear y personalizar paneles adicionales, y publicar y compartir paneles para ponerlos a disposición de otros usuarios.



Para modificar el panel actual, seleccione **Editar**. Si no quiere modificar el panel predeterminado, también puede crear un **panel nuevo**. Al crear un panel, se obtiene un panel vacío y privado que incluye la **Galería de iconos**, que le permite agregar o reorganizar iconos. Puede buscar iconos por categoría o tipo de recurso. También puede buscar iconos concretos. Seleccione **Mi panel** para seleccionar cualquiera de los paneles personalizados existentes.

Cambio de la configuración del portal

Puede personalizar el Centro de administración de Microsoft Endpoint Manager si selecciona la vista predeterminada, el tema y el período de tiempo de expiración de las credenciales, así como la configuración de idioma y región.



Pasos siguientes

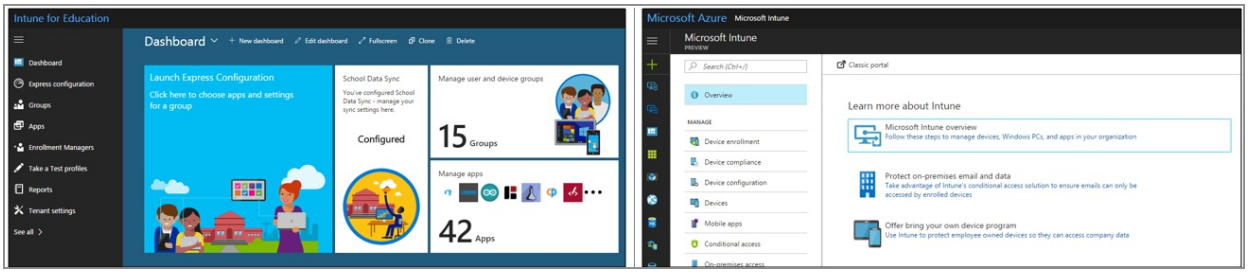
Para empezar a trabajar rápidamente en Microsoft Intune, puede consultar los inicios rápidos de Intune si primero configura una cuenta gratuita de Intune.

Inicio rápido: Prueba gratuita de Microsoft Intune

¿En qué se diferencia Intune for Education de la experiencia completa de administración de dispositivos en Intune?

14/05/2021 • 2 minutes to read

Intune for Education permite a profesores y estudiantes trabajar de forma productiva y mantener protegidos los datos del centro educativo. Intune for Education está basado en el servicio Intune de Microsoft, un servicio de administración de movilidad empresarial (EMM) basado en la nube.



Intune for Education permite administrar dispositivos iOS/iPadOS y Windows 10 mediante las funcionalidades de MDM completas disponibles en Intune. La experiencia de administración de dispositivos completa permite administrar dispositivos Windows, iOS/iPadOS y Android.

Intune for Education puede utilizarse por sí mismo o en armonía con la experiencia completa de administración de dispositivos disponible en Intune. También se puede utilizar junto con el resto de las herramientas disponibles en Microsoft Education, lo que facilita usar Intune for Education con otras herramientas educativas útiles de Microsoft.

Con Intune e Intune for Education, puede:

- Administrar los dispositivos móviles que el personal y los estudiantes usan para tener acceso a los datos.
- Administrar las aplicaciones móviles a las que los usuarios acceden a diario.
- Proteger la información corporativa al ayudar a controlar la manera en que los usuarios acceden a ella y la comparten.
- Garantizar que los dispositivos y las aplicaciones sean compatibles con los requisitos de seguridad.

Pasos siguientes

- Familiarícese con el producto con una evaluación de prueba de 90 días de Intune. Si ya tiene acceso, vaya a (https://intuneeducation.portal.azure.com) para empezar a trabajar.
- Obtenga información sobre la manera más rápida de comenzar a usar Intune for Education.
- Sumérjase en los requisitos técnicos y las funciones de Intune.

¿Qué es Intune for Government?

14/05/2021 • 2 minutes to read

Intune para Government es una plataforma de administración para dispositivos móviles y aplicaciones diseñada para ayudar a garantizar la seguridad, la privacidad y el control, el cumplimiento y la transparencia. Cumple con las necesidades federales, estatales y locales de la Administración Pública de Estados Unidos para las instancias de Azure lógicas y aisladas en redes. Son instancias dedicadas de la Administración Pública de Estados Unidos en las que todos los datos de clientes, las aplicaciones y el hardware residen en el territorio continental de Estados Unidos.

Intune para Government incluye una instancia físicamente aislada de Microsoft Intune que admite los requisitos de seguridad y cumplimiento normativo críticos de la Administración Pública de Estados Unidos. Intune es un servicio de administración de movilidad empresarial (EMM) basado en la nube que es la base de Intune for Government. Las agencias gubernamentales tendrán acceso a las mismas características disponibles para los clientes comerciales. Entre ellas se incluyen certificaciones de cumplimiento de FedRAMP y DoD, y están operadas por ciudadanos de EE. UU. selectos.

Con Intune for Government puede administrar dispositivos Windows 10, iOS y Android mediante las funciones de MDM completas disponibles en Intune. Por ejemplo, puede:

- Administrar los dispositivos móviles de los empleados públicos que se usan para acceder a los datos.
- Administrar las aplicaciones móviles a las que acceden los usuarios.
- Proteger los datos de la administración pública mediante el control del modo en que los usuarios acceden a ellos y los comparten.
- Garantizar que los dispositivos y las aplicaciones sigan los requisitos de seguridad.

Pasos siguientes

- Para obtener más información sobre Intune para la Administración Pública de EE. UU., vea Descripción del servicio Microsoft Intune for US Government GCC High y DoD.
- Sumérjase en los requisitos técnicos y las funciones de Intune.
- Vea diferencias de características entre Intune e Intune para la Administración Pública de EE. UU.

Arquitectura de alto nivel para Microsoft Intune

14/05/2021 • 2 minutes to read

Esta arquitectura de referencia muestra opciones para integrar Microsoft Intune en su entorno de Azure con Azure Active Directory.

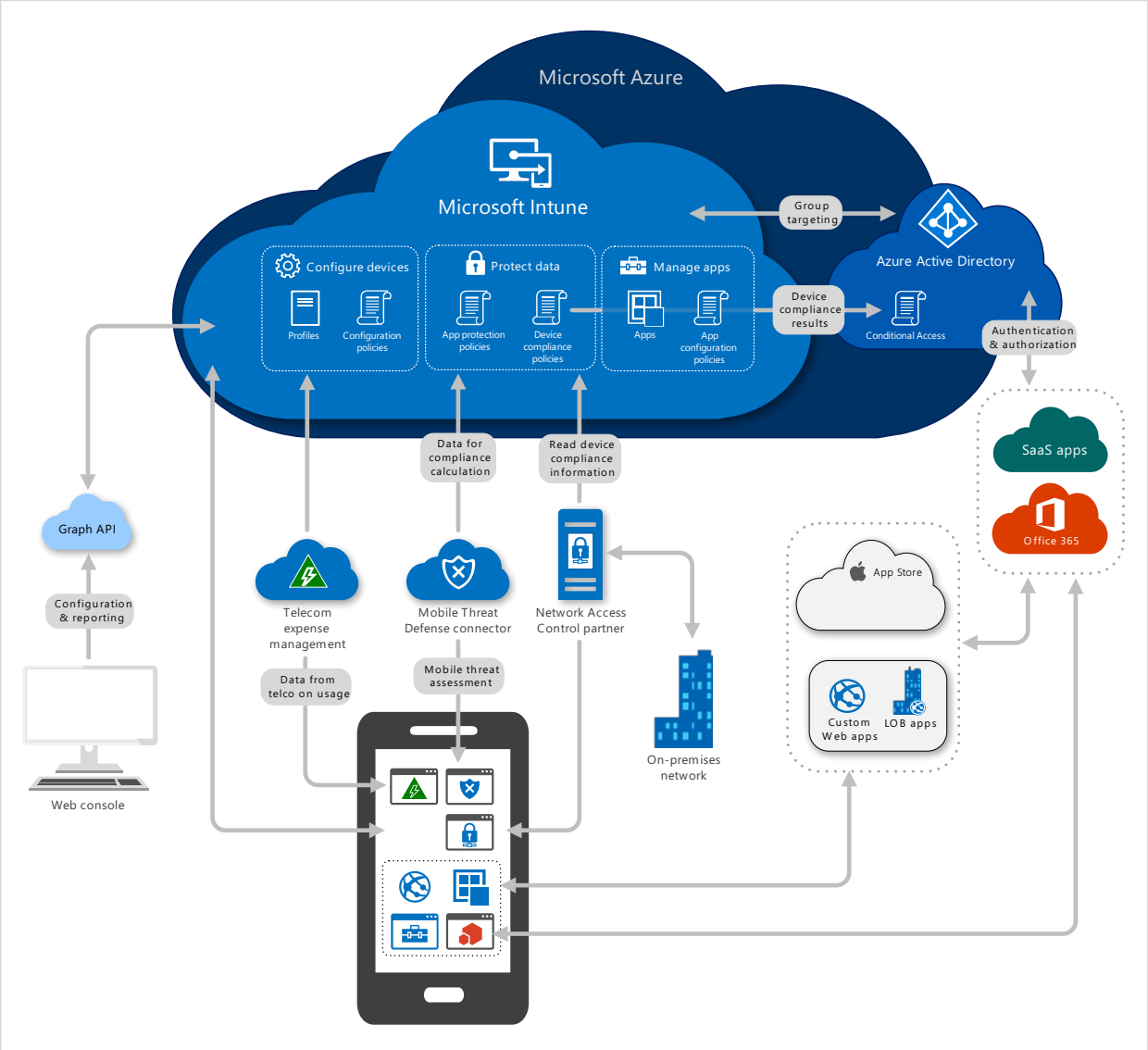
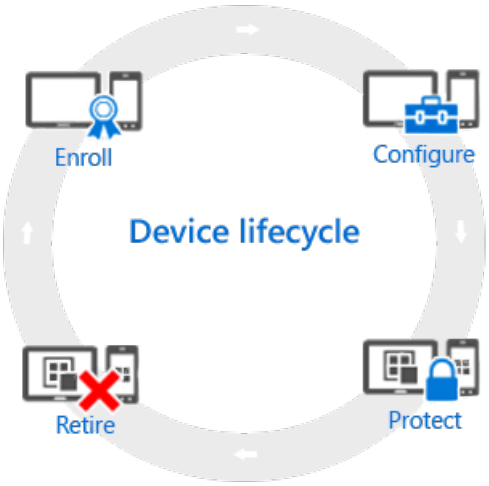


Imagen con contraste oscuro

Información general sobre el ciclo de vida de administración de dispositivos móviles (MDM) de Microsoft Intune

14/05/2021 • 3 minutes to read

Todos los dispositivos que administra tienen un *ciclo de vida*. Intune puede ayudarle a administrar su ciclo de vida: desde la inscripción, pasando por la configuración y la protección, hasta la retirada del dispositivo cuando ya no resulte necesario. Por ejemplo, si la empresa compra un iPad, primero hay que inscribirlo con una cuenta de Microsoft Intune para que la empresa pueda administrarlo; después, debe configurarse para adaptarlo a las necesidades de la empresa; luego, hay que proteger los datos que el usuario almacena en el iPad; y por último, cuando ya no se necesite el iPad, habrá que retirar o borrar todos los datos confidenciales que contenga el dispositivo.



Inscribir

Las estrategias actuales de administración de dispositivos móviles (MDM) se aplican a diferentes teléfonos, tabletas y equipos (iOS/iPadOS, Android, Windows y Mac OS X). Si tiene que administrar el dispositivo, lo que suele ser el caso de los dispositivos corporativos, el primer paso es configurar la inscripción del dispositivo. También puede administrar equipos Windows si los inscribe en Intune (MDM).

Configurar

La inscripción de los dispositivos es solo el primer paso. Para aprovechar todas las posibilidades que ofrece Intune y asegurarse de que los dispositivos sean seguros y conformes con los estándares de la empresa, puede elegir entre una amplia gama de directivas. Estas permiten configurar prácticamente todos los aspectos del funcionamiento de los dispositivos administrados. Por ejemplo, si los usuarios deben tener contraseñas en los dispositivos que contienen datos empresariales. Puede hacer que sea necesario disponer de una. ¿Tiene Wi-Fi corporativa? Puede configurarla automáticamente. Estos son los tipos de opciones de configuración disponibles:

- **Configuración de dispositivos**. Estas directivas permiten configurar las características y las funcionalidades de los dispositivos administrados. Por ejemplo, se podría exigir el uso de una contraseña en teléfonos Android o deshabilitar el uso de la cámara en dispositivos iPhone.
- **Acceso a los recursos de la empresa**. El hecho de permitir a los usuarios acceder al trabajo desde sus

dispositivos personales puede plantear retos. Por ejemplo, ¿cómo se garantiza que todos los dispositivos que necesitan acceder al correo electrónico de la empresa estén configurados correctamente? ¿Cómo se puede garantizar que los usuarios puedan tener acceso a la red corporativa con una conexión VPN si no conocen valores complejos? Intune puede ayudar a reducir esta carga; para conseguirlo, configura automáticamente los dispositivos administrados para acceder a recursos comunes de la empresa.

- **Directivas de administración de equipos Windows (con el software cliente de Intune)**. Aunque la inscripción de los equipos Windows con Intune ofrece el máximo de funcionalidades de administración de dispositivos, Intune sigue siendo compatible con la administración de equipos Windows con el software cliente de Intune. Si necesita información sobre algunas de las tareas que puede realizar con los equipos, empiece aquí.

Protección

En el actual sector de las TI, la protección de los dispositivos frente al acceso no autorizado es una de las tareas más importantes que se realizan. Además de los elementos del paso **Configurar** del ciclo de vida del dispositivo, Intune proporciona más funcionalidades que ayudan a proteger los dispositivos que se administran frente al acceso no autorizado o a los ataques malintencionados:

- **Autenticación multifactor**. La presencia de una capa adicional de autenticación para inicios de sesión de usuario puede ayudar a proteger aún más los dispositivos. Muchos dispositivos admiten la autenticación multifactor, que exige un segundo nivel de autenticación, como una llamada de teléfono o un mensaje de texto, para que los usuarios puedan acceder.
- **Configuración de Windows Hello para empresas**. Windows Hello para empresas es un método alternativo de inicio de sesión que permite a los usuarios usar un *gesto*, como una huella digital o Windows Hello, para iniciar sesión sin necesidad de una contraseña.
- **Directivas para proteger equipos Windows (con el software cliente de Intune)**. Al administrar equipos Windows con el software cliente de Intune, hay disponibles directivas que permiten controlar la configuración de Endpoint Protection, de las actualizaciones de software y de Firewall de Windows en los equipos que administra.

Retirar

Cuando un dispositivo se pierde o es robado, cuando es necesario reemplazarlo o cuando el usuario cambia de cargo en la empresa, suele ser necesario retirar o borrar el dispositivo. Hay varias maneras de hacerlo, como restablecer el dispositivo, quitarlo de la administración o borrar los datos corporativos que contiene.

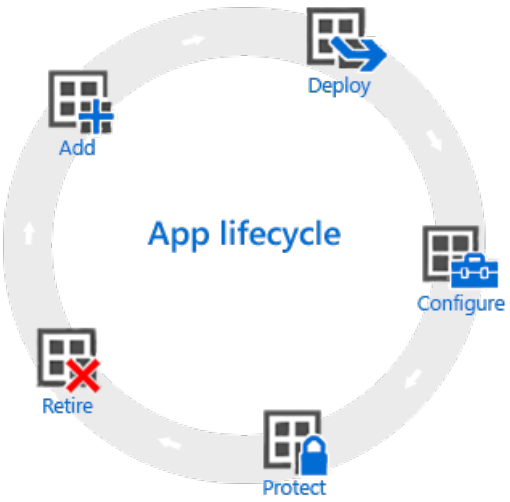
Pasos siguientes

- Obtenga información sobre la administración de dispositivos de Microsoft Intune

Información general sobre el ciclo de vida de la aplicación en Microsoft Intune

14/05/2021 • 2 minutes to read

El ciclo de vida de la aplicación de Microsoft Intune empieza cuando se agrega una aplicación, se extiende a través de otras fases y termina cuando se quita. Al comprender estas fases, tendrá los detalles que necesita para empezar a trabajar con la administración de aplicaciones de Intune.



Agregar

El primer paso en la implementación de la aplicación es agregar a Intune las aplicaciones que quiere administrar y asignar. Aunque hay muchos tipos diferentes de aplicaciones con las que puede trabajar, los procedimientos básicos son los mismos. Con Intune puede agregar tipos diferentes de aplicaciones, incluidas aplicaciones escritas internamente (línea de negocio), aplicaciones de la tienda, aplicaciones integradas y aplicaciones en la web. Para obtener más información sobre estos tipos de aplicaciones, consulte Agregar una aplicación a Microsoft Intune.

Implementar

Después de agregar la aplicación a Intune, puede asignarla a usuarios y dispositivos que administre. Intune facilita este proceso y, después de implementar la aplicación, puede supervisar que la implementación se haya realizado correctamente desde Intune en el portal. Además, en algunas tiendas de aplicaciones, como el App Store de Apple y la Tienda de aplicaciones Windows, puede comprar licencias de aplicación en masa para la empresa. Intune puede sincronizar datos con estas tiendas para permitirle implementar y realizar un seguimiento del uso de licencias de estos tipos de aplicaciones directamente desde la consola de administración de Intune.

Configurar

Como parte del ciclo de vida de la aplicación, periódicamente se publican nuevas versiones de aplicaciones. Intune proporciona herramientas para actualizar aplicaciones que haya implementado en una versión más reciente con facilidad. Además, puede configurar funcionalidad adicional para algunas aplicaciones, como:

- Las directivas de configuración de aplicaciones iOS/iPadOS proporcionan valores para aplicaciones

iOS/iPadOS compatibles que se usan cuando se ejecuta la aplicación. Por ejemplo, es posible que una aplicación necesite una configuración de marca concreta o el nombre de un servidor al que se debe conectar.

- Las directivas de explorador administrado ayudan a configurar los valores de Microsoft Edge, lo que reemplaza al explorador de dispositivos predeterminado y que permite restringir los sitios web que pueden visitar los usuarios.

Protección

Intune ofrece muchas maneras de ayudar a proteger los datos de las aplicaciones. Los métodos principales son:

- El acceso condicional, que controla el acceso al correo electrónico y otros servicios en función de las condiciones que especifique. Dichas condiciones incluyen tipos de dispositivos o el cumplimiento de una directiva de cumplimiento de dispositivos que haya implementado.
- Las directivas de protección de aplicaciones funcionan con aplicaciones individuales para ayudar a proteger los datos empresariales que usan. Por ejemplo, puede restringir la copia de datos entre las aplicaciones no administradas y las aplicaciones que administre o evitar que las aplicaciones se ejecuten en dispositivos con jailbreak o rooting.

Retirar

Por último, es probable que las aplicaciones que haya implementado queden obsoletas y tengan que quitarse. Intune permite desinstalar aplicaciones fácilmente. Para obtener más información, consulte Desinstalación de una aplicación.

Pasos siguientes

- Obtenga información sobre la administración de aplicaciones de Microsoft Intune

Introducción a los escenarios guiados de Intune

14/05/2021 • 4 minutes to read

Un escenario guiado es una serie personalizada de pasos en torno a un caso de uso completo. Los escenarios más habituales se basan en el rol que un administrador, un usuario o un dispositivo desempeñan en la organización. Estos roles suelen requerir una colección de perfiles, opciones, aplicaciones y controles de seguridad cuidadosamente organizados. para proporcionar la mejor experiencia de usuario y seguridad.

Si no está familiarizado con los pasos y recursos necesarios para implementar un escenario determinado, empiece con escenarios guiados. En el escenario guiado se ensamblarán directivas, aplicaciones, asignaciones y otras configuraciones de administración de manera automática. Asimismo, puede que en estos escenarios guiados se omitan deliberadamente ciertas opciones que no procedan o que sean poco frecuentes en el escenario en cuestión.

Los escenarios guiados no son un espacio de administración distinto de los flujos de trabajo de Intune habituales. Estos flujos de trabajo suelen usarse junto con los flujos de trabajo existentes de Intune de los perfiles, aplicaciones y directivas. Tras completar un escenario guiado, toda la administración futura del escenario debe realizarse en los menús existentes de las directivas, aplicaciones y perfiles. Un escenario guiado no guarda un tipo de recurso de "escenario guiado" ni realiza un seguimiento de los cambios futuros realizados en los recursos. Todos los recursos creados por un escenario guiado se muestran en su carga de trabajo respectiva. Todas las opciones del escenario guiado, incluso las omitidas, estarán disponibles para su edición en los menús existentes.

Tipos de escenarios guiados

Por motivos de simplicidad, en todos los escenarios guiados se omiten características de ámbito, como las etiquetas de ámbito, los grupos de exclusión y las asignaciones de grupo virtual. Todos los recursos creados en un escenario guiado heredarán todas las etiquetas de ámbito del administrador que complete el escenario. Algunos escenarios ofrecen cierto nivel de personalización de la configuración común para cubrir escenarios que están estrechamente relacionados. En estos escenarios solo se permite la asignación de grupos a grupos de inclusión. En otros escenarios guiados, todo el escenario garantiza una experiencia coherente al no ofrecer ninguna personalización, y se genera automáticamente un nuevo grupo para recibir todas las asignaciones. Una vez completado el escenario guiado, se pueden usar más características de asignaciones directamente a través de las cargas de trabajo de directivas, aplicaciones y perfiles existentes.

A continuación se describen los escenarios disponibles:

- Implementar Microsoft Edge para aplicaciones móviles
- Probar un equipo administrado en la nube
- Proteger Microsoft Office para móviles
- Windows 10 en configuración de nube

Funcionalidad de los escenarios guiados

Los escenarios guiados ofrecen una funcionalidad específica. Los siguientes detalles ayudan a explicar lo que se puede y no se puede hacer mientras se sigue un escenario guiado.

Inicio

Todos los escenarios guiados están disponibles en el **Centro de administración de Microsoft Endpoint Manager** > **Solución de problemas + soporte técnico** > **Escenarios guiados**.

Los escenarios guiados comienzan con una introducción. Se explica el propósito del escenario y los requisitos previos necesarios para completar la configuración. En ese momento, se comprueban sus permisos de administrador para corroborar que tiene todos los privilegios necesarios para completar el escenario.

Una vez superadas todas las comprobaciones de requisitos previos, el escenario ofrece la configuración adecuada de personalización. Los escenarios guiados solo requieren una entrada para un número mínimo de valores de configuración. Ocultan una configuración no habitual o avanzada hasta que sea necesaria o según circunstancias especiales. Cada escenario guiado incluye vínculos a la documentación que proporciona más información detallada.

Una vez especificados todos los valores obligatorios, el escenario guiado muestra un resumen de los valores especificados y los recursos que el escenario en cuestión requiere. En este momento, no se guarda nada a menos que se indique explícitamente.

El siguiente paso consiste en implementar el escenario. Con la implementación de un escenario se crean y guardan todos los recursos necesarios y la configuración seleccionada. El tiempo que se tarda en completar una implementación varía según el escenario. Una vez finalizada la implementación, el escenario guiado muestra una lista de los recursos creados. También tiene vínculos a la vista de administración de cada recurso, la carga de trabajo normal del recurso y la documentación.

> **IMPORTANT**
> La lista que se muestra al final del escenario guiado no se guarda y solo está visible mientras el escenario guiado está abierto.

Si se produce un error al implementar el escenario, se revertirán todos los cambios.

Edición

Los escenarios guiados no se pueden usar para editar los recursos existentes. Una vez creados, todos los recursos, grupos y asignaciones se deben editar con las cargas de trabajo existentes.

monitoring

Los escenarios guiados no se pueden usar para supervisar los recursos existentes aparte del proceso de creación inicial. Una vez creados, todos los recursos, grupos y asignaciones se deben supervisar con las cargas de trabajo existentes.

Retirada

Los escenarios guiados no se pueden usar para retirar los recursos existentes. Una vez creados, todos los recursos, grupos y asignaciones se deben retirar con las cargas de trabajo existentes.

Actualización

A medida que la tecnología avanza, Intune puede actualizar un escenario guiado para mejorar la experiencia de usuario, la seguridad u otros aspectos de ese escenario. Esta actualización solo afecta a las nuevas implementaciones de escenarios guiados. Intune no actualizará los recursos que generó anteriormente el escenario guiado.

Pasos siguientes

Para empezar a usar Microsoft Intune cuanto antes, recorra los escenarios guiados de Intune. Si no está familiarizado con Intune, configure un inquilino de Intune siguiendo el inicio rápido de prueba gratuita.

Escenario guiado: Implementación de Microsoft Edge para dispositivos móviles

14/05/2021 • 5 minutes to read

Al seguir este escenario guiado, puede asignar la aplicación Microsoft Edge a los usuarios de los dispositivos iOS/iPadOS o Android de la organización. La asignación de esta aplicación permitirá a los usuarios examinar contenido sin problemas con sus dispositivos corporativos.

Microsoft Edge permite a los usuarios abrirse camino a través del desorden de la web con características integradas que les ayudarán a consolidar, organizar y administrar el contenido de trabajo. Los usuarios de dispositivos iOS/iPadOS y Android que inician sesión con sus cuentas corporativas de Azure AD en la aplicación Microsoft Edge encontrarán el explorador precargado con los **favoritos** del lugar de trabajo y los filtros de sitios web que defina.

> **NOTE**
> Si ha bloqueado a usuarios para que no inscriban dispositivos iOS/iPadOS o Android, en este escenario no se habilitará la inscripción y los usuarios tendrán que instalar Edge por su cuenta. Están disponibles las características empresariales de Microsoft Edge siguientes habilitadas por directivas de Intune:

- **Identidad dual**: los usuarios pueden agregar una cuenta profesional, al igual que una cuenta personal, para realizar la exploración. Hay una separación total entre ambas identidades, que es similar a la arquitectura y experiencia existente en Microsoft 365 y Outlook. Los administradores de Intune podrán establecer las directivas deseadas para lograr una experiencia de exploración protegida dentro de la cuenta profesional.
- **Integración de directivas de protección de la aplicación Intune**: los administradores ahora pueden dirigir las directivas de protección de aplicación a Microsoft Edge, incluido el control de las acciones de cortar, copiar y pegar, lo que impide las capturas de pantalla y garantiza que los vínculos seleccionados por el usuario solo se abran en otras aplicaciones administradas.
- **Integración de proxy de la aplicación de Azure**: los administradores pueden controlar el acceso a las aplicaciones web y a las aplicaciones SaaS, lo que permite garantizar que las aplicaciones basadas en explorador solo se ejecuten en el explorador seguro de Microsoft Edge, ya sea que los usuarios finales se conecten desde la red corporativa o desde Internet.
- **Favoritos administrados y accesos directos a la página principal**: para facilitar el acceso, los administradores pueden establecer direcciones URL para que aparezcan en los favoritos cuando los usuarios finales estén en su contexto corporativo. Los administradores pueden establecer un acceso directo a la página principal, que se mostrará como el acceso directo principal cuando el usuario corporativo abra una página o una pestaña nueva en Microsoft Edge.

Requisitos previos

- Establecer la entidad de MDM en Intune: la configuración de la entidad de administración de dispositivos móviles (MDM) determina cómo se administran los dispositivos. Como administrador de TI, debe establecer una entidad de MDM antes de que los usuarios puedan inscribir dispositivos para la administración.
- Permisos de administrador de Intune necesarios:
  - Permisos de lectura, creación, eliminación y asignación de aplicaciones administradas
  - Permisos de lectura, creación y asignación de aplicaciones móviles
  - Permisos de lectura, creación y asignación de conjuntos de directivas

- Permiso de lectura y actualización de la organización

Paso 1: introducción

Al seguir el escenario guiado **Implementación de Microsoft Edge para dispositivos móviles**, configurará una implementación básica de Microsoft Edge para un grupo seleccionado de usuarios de iOS/iPadOS y Android. Esta implementación implementará una **identidad dual** y **accesos directos a los favoritos administrados y a la página de inicio**. Además, Intune instalará de forma automática la aplicación Microsoft Edge en los dispositivos inscritos por los usuarios seleccionados. Esta instalación automática se efectuará en todos los tipos de inscripción controlados por el usuario, entre los que se incluyen:

- Inscripción de iOS/iPadOS con la aplicación Portal de empresa
- Inscripción de afinidad de usuario de iOS/iPadOS mediante Apple Business Manager
- Inscripción de Android heredada con la aplicación Portal de empresa

En este escenario guiado se habilitará automáticamente **MyApps** para que aparezcan en los favoritos de Microsoft Edge y se configurará el explorador con la misma personalización de marca que haya definido para la aplicación Portal de empresa de Intune.

Qué se necesita para continuar

Le pediremos los favoritos del lugar de trabajo que necesitan sus usuarios y los filtros que necesita para la exploración web. Asegúrese de llevar a cabo las siguientes tareas antes de continuar:

- Agregue usuarios a los grupos de Azure AD. Para obtener más información, vea Creación de un grupo básico e incorporación de miembros con Azure Active Directory.
- Inscriba dispositivos iOS/iPadOS o Android en Intune. Para obtener más información, vea Inscripción de dispositivos.
- Recopile una lista de favoritos del lugar de trabajo para agregarlos a Microsoft Edge.
- Recopile una lista de filtros de sitios web para aplicarlos en Microsoft Edge.

Paso 2: aspectos básicos

En este paso debe especificar un nombre y una descripción de las nuevas directivas de Microsoft Edge. Se puede hacer referencia a estas directivas más adelante si necesita cambiar las asignaciones y configuraciones. El escenario guiado agregará y asignará la aplicación Microsoft Edge de iOS/iPadOS para dispositivos iOS/iPadOS y la aplicación Microsoft Edge de Android para dispositivos Android. Además, en este paso se crearán directivas de configuración para estas aplicaciones.

Paso 3: configuración

En este paso, el escenario guiado configurará Microsoft Edge para mostrar las demás aplicaciones asignadas a los usuarios a través de Intune y compartir la misma personalización de marca que la aplicación Portal de empresa de Microsoft Intune. Puede seguir configurando Microsoft Edge con una **dirección URL de acceso directo a la página de inicio**, una lista de **marcadores administrados** y una lista de **direcciones URL bloqueadas**. La **dirección URL de acceso directo a la página de inicio** se mostrará a los usuarios como el primer icono situado debajo de la barra de búsqueda cuando abran una nueva pestaña en Microsoft Edge en su dispositivo. Los **marcadores administrados** son una lista de direcciones URL favoritas que los usuarios tendrán disponibles al usar Microsoft Edge en su contexto de trabajo. Las **direcciones URL bloqueadas** especifican los sitios bloqueados para los usuarios mientras están en su contexto de trabajo. Se permitirán los demás sitios.

Paso 4: asignaciones

En este paso puede elegir los grupos de usuarios que desea incluir para que tengan configurado Microsoft Edge

para dispositivos móviles para el trabajo. Microsoft Edge también se instalará en todos los dispositivos iOS/iPadOS y Android inscritos por estos usuarios.

Paso 5: revisión y creación

El último paso permite revisar un resumen de los valores que ha configurado. Una vez que haya revisado las opciones, haga clic en **Crear** para completar el escenario guiado.

> **NOTE**
> Edge puede tardar hasta 12 horas en recibir la configuración. Para obtener más información, vea Directivas de configuración de aplicaciones para Microsoft Intune.

> **IMPORTANT**
> Cuando el escenario guiado se complete, se mostrará un resumen. Los recursos mencionados en este resumen se pueden modificar más adelante, pero la tabla en la que se muestran estos recursos no se guardará.

Pasos siguientes

- Mejorar la seguridad del uso de Microsoft Edge mediante la configuración de la integración de directivas de protección de aplicaciones de Intune. Para obtener más información, vea Creación de directivas de protección de aplicaciones de Intune.
- Si desea incluir sitios de intranet, explore la protección del acceso con la integración de proxy de la aplicación de Azure. Para obtener más información, vea Administración de la configuración del proxy.

Escenario guiado: Escritorio moderno administrado en la nube

14/05/2021 • 6 minutes to read

Escritorio moderno es la plataforma de productividad de vanguardia para el trabajador de la información. Aplicaciones de Microsoft 365 y Windows 10 son los componentes principales de Escritorio moderno junto con las líneas de base de seguridad más recientes para Windows 10 y Microsoft Defender para punto de conexión.

La administración de Escritorio moderno desde la nube aporta la ventaja adicional de las acciones remotas en toda Internet. La administración en la nube emplea las directivas de Administración de dispositivos móviles integradas de Windows y quita las dependencias de la directiva de grupo de Active Directory local.

Si quiere evaluar un escritorio moderno administrado en la nube en su propia organización, en este escenario guiado se predefinen todas las configuraciones necesarias para una implementación básica. En este escenario guiado, creará un entorno seguro en el que puede probar las funciones de administración de dispositivos de Intune.

Requisitos previos

- Establecer la entidad de MDM en Intune: la configuración de la entidad de administración de dispositivos móviles (MDM) determina cómo se administran los dispositivos. Como administrador de TI, debe establecer una entidad de MDM antes de que los usuarios puedan inscribir dispositivos para la administración.
- M365 E3 como mínimo (o M365 E5 para mayor seguridad)
- Dispositivo Windows 10 1903 (registrado con Windows Autopilot para la experiencia óptima del usuario final)
- Permisos de administrador de Intune necesarios para completar este escenario guiado:
  - Configuración del dispositivo, Leer, Crear, Eliminar, Asignar y Actualizar
  - Programas de inscripción Leer dispositivo, Leer perfil, Crear perfil, Asignar perfil, Eliminar perfil
  - Aplicaciones móviles, Leer, Crear, Eliminar, Asignar y Actualizar
  - Organización Leer y Actualizar
  - Líneas de base de seguridad, Leer, Crear, Eliminar, Asignar y Actualizar
  - Conjuntos de directivas Leer, Crear, Eliminar, Asignar y Actualizar

Paso 1: introducción

Con este escenario guiado, configurará un usuario de prueba, inscribirá un dispositivo en Intune y lo implementará con la configuración recomendada de Intune, así como con Windows 10 y Aplicaciones de Microsoft 365. El dispositivo también se configurará para Microsoft Defender para punto de conexión, si elige habilitar esta protección en Intune. El usuario que configure y el dispositivo que inscriba se agregarán a un nuevo grupo de seguridad y se configurarán con la configuración recomendada para la seguridad y la productividad.

Qué se necesita para continuar

En este escenario guiado debe proporcionar el dispositivo de prueba y el usuario de prueba. Asegúrese de completar las tareas siguientes:

- Configurar una cuenta de usuario de prueba en Azure Active Directory.
- Crear un dispositivo de prueba que ejecute Windows 10 versión, 1903 o posterior.

- (Opcional) Registrar el dispositivo de prueba con Windows Autopilot.
- (Opcional) Habilitar la personalización de marca en la página de inicio de sesión Azure Active Directory de la organización.

Paso 2: Usuario

Elija un usuario para configurar en el dispositivo. Será el usuario primario del dispositivo.

Si quiere agregar más usuarios o dispositivos a esta configuración, simplemente agréguelos a los grupos de seguridad de Azure AD generados por el asistente. A diferencia de otros escenarios guiados, no es necesario ejecutar el asistente más de una vez, ya que la configuración no se puede personalizar. Simplemente agregue más usuarios y dispositivos a los grupos de Azure AD creados. Después de completar el asistente, podrá ver el grupo generado con las directivas recomendadas implementadas.

Paso 3: Dispositivo

Asegúrese de que el dispositivo ejecuta Windows 10, versión 1903 o posterior. El usuario principal tendrá que configurar el dispositivo cuando lo reciba. Hay dos opciones de configuración disponibles para el usuario.

Opción A: Windows Autopilot

Windows Autopilot automatiza la configuración de dispositivos nuevos para que los usuarios puedan configurarlos de forma rápida, sin necesidad de ayuda de TI. Si el dispositivo ya está registrado en Windows Autopilot, selecciónelo por su número de serie. Para más información sobre el uso de Windows Autopilot, vea Registro del dispositivo con Windows Autopilot (opcional).

Opción B: Inscripción manual de dispositivos

Los usuarios instalarán e inscribirán de forma manual los dispositivos nuevos en la administración de dispositivos móviles. Después de completar este escenario, restablezca el dispositivo y proporcione al usuario principal las instrucciones de inscripción para los dispositivos Windows. Para más información, vea Unión de un dispositivo Windows 10 a Azure AD durante la experiencia de primera ejecución.

Paso 4: Revisión y creación

El último paso permite revisar un resumen de los valores que ha configurado. Una vez que haya revisado las opciones, haga clic en **Implementar** para completar el escenario guiado. Una vez completado el escenario guiado, se mostrará una tabla de recursos. Puede editar estos recursos más adelante, pero una vez que salga de la vista de resumen, la tabla no se guardará.

> **IMPORTANT**
> Cuando el escenario guiado se complete, se mostrará un resumen. Los recursos mencionados en este resumen se pueden modificar más adelante, pero la tabla en la que se muestran estos recursos no se guardará.

Comprobación

1. Compruebe que al usuario seleccionado se le ha asignado el ámbito de usuario de MDM.
   - Asegúrese de que Ámbito de usuario de MDM está:
     - Establecido en **Todo** para la aplicación **Microsoft Intune** o bien,
     - Establecido en **Algunos**. Además, agregue el grupo de usuarios creado por este escenario guiado.
2. Compruebe que el usuario seleccionado puede unir dispositivos a Azure Active Directory.
   - Asegúrese de que la unión a Azure AD esté:
     - Establecida en **Todos** o bien,

    - Establecida en **Algunos**. Además, agregue el grupo de usuarios creado por este escenario guiado.
3. Siga los pasos adecuados en el dispositivo para unirlo a Azure AD en función de lo siguiente:
    - Con Autopilot. Para más información, vea Modo controlado por el usuario de Windows Autopilot.
    - Sin Autopilot: Para más información, vea Unión de un dispositivo Windows 10 a Azure AD durante la experiencia de primera ejecución.

¿Qué ocurre cuando hago clic en Implementar?

El usuario y el dispositivo se agregarán a grupos de seguridad nuevos. También se configurarán con los valores recomendados por Intune para la seguridad y la productividad en el ámbito educativo o laboral. Después de que el usuario una el dispositivo a Azure AD, se agregarán más aplicaciones y configuraciones al dispositivo. Para obtener más información sobre estas configuraciones adicionales, vea Inicio rápido: Inscripción de dispositivos Windows 10.

Información adicional

Registro de dispositivos con Windows Autopilot (opcional)

Opcionalmente, puede optar por usar un dispositivo Autopilot registrado. Para Autopilot, este escenario guiado asignará un perfil de implementación de Autopilot y un perfil de página de estado de inscripción. El perfil de implementación de Autopilot se configurará de la siguiente manera:

- Modo controlado por el usuario: es decir, requerir que el usuario final escriba el nombre de usuario y la contraseña durante la configuración de Windows.
- Unión a Azure AD.
- Personalizar la configuración de Windows:
    - Ocultar la pantalla de términos de licencia de software de Microsoft
    - Ocultar la configuración de privacidad
    - Crear el perfil local del usuario sin privilegios de administrador local
    - Ocultar las opciones de cambio de cuenta en la página de inicio de sesión corporativa

La página Estado de inscripción se configurará para que solo se habilite para dispositivos Autopilot y no se bloqueará mientras espera a que se instalen todas las aplicaciones.

El escenario guiado también asignará el usuario al dispositivo Autopilot seleccionado para una experiencia de instalación personalizada.

Requisitos posteriores

Una vez que el usuario une el dispositivo a Azure Active Directory, se aplicarán las configuraciones siguientes al dispositivo:

1. Aplicaciones de Microsoft 365 se instalará de forma automática en el equipo administrado en la nube. Incluye las aplicaciones con las que está familiarizado, como Access, Excel, OneNote, Outlook, PowerPoint, Publisher, Skype Empresarial y Word. Puede usar estas aplicaciones para conectarse a servicios de Microsoft 365, como SharePoint Online, Exchange Online y Skype Empresarial Online. Aplicaciones de Microsoft 365 se actualiza periódicamente con nuevas características, a diferencia de las versiones de Office que no son de suscripción. Para obtener una lista de las características nuevas, vea Novedades de Microsoft 365.
2. Las líneas de base de seguridad de Windows se instalarán en el equipo administrado en la nube. Si ha configurado Microsoft Defender para punto de conexión, el escenario guiado también configurará las opciones de línea de base de Defender. Defender para punto de conexión proporciona una nueva capa de protección posterior a la infracción en la pila de seguridad de Windows 10. Con una combinación de tecnología cliente integrada en Windows 10 y un sólido servicio en la nube, ayudará a detectar las amenazas que han superado otras medidas de defensa.

Pasos siguientes

- Si usa Protección contra amenazas avanzada de Microsoft Defender, cree una directiva de cumplimiento de Intune para requerir que el análisis de amenazas de Defender satisfaga los requisitos de cumplimiento.
- Cree una directiva de acceso condicional basada en dispositivos para bloquear el acceso si el dispositivo no satisface los requisitos de cumplimiento de Intune.

Escenario guiado: Aplicaciones móviles seguras de Microsoft Office

14/05/2021 • 6 minutes to read

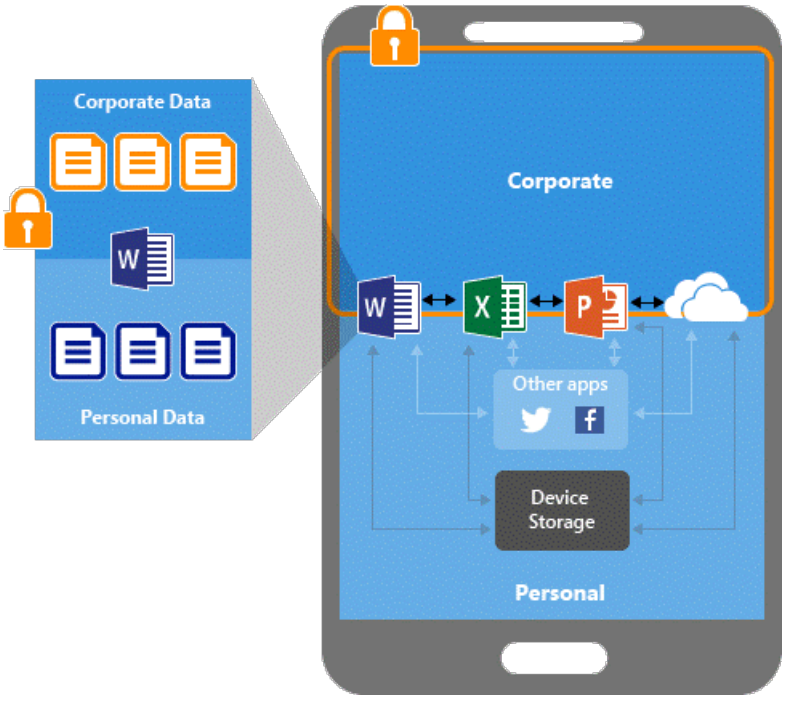
Si sigue este escenario guiado en el portal de administración de dispositivos, puede habilitar la protección de aplicaciones básica de Intune en dispositivos iOS/iPadOS y Android.

La protección de aplicaciones que se habilita aplicará las siguientes acciones:

- Cifrar los archivos de trabajo
- Requerir un PIN para acceder a los archivos de trabajo
- Requerir que se restablezca el PIN después de cinco intentos fallidos
- Impedir que se hagan copias de seguridad de los archivos de trabajo en los servicios de copia de seguridad de iTunes, iCloud y Android
- Requerir que los archivos de trabajo se guarden únicamente en OneDrive o SharePoint
- Impedir que las aplicaciones protegidas carguen archivos de trabajo en dispositivos con jailbreak o rooting
- Bloquear el acceso a los archivos de trabajo si el dispositivo lleva 720 minutos sin conectarse
- Quitar archivos de trabajo si el dispositivo lleva 90 días sin conectarse

Contexto

Las aplicaciones móviles de Office, así como Microsoft Edge para dispositivos móviles, admiten la identidad dual. La identidad dual permite a las aplicaciones administrar archivos de trabajo de forma independiente de los archivos personales.



Las directivas de protección de aplicaciones de Intune ayudan a proteger los archivos de trabajo almacenados en dispositivos inscritos en Intune. También puede usar directivas de protección de aplicaciones en dispositivos que poseen los empleados que no están inscritos para administración en Intune. En este caso, aunque la empresa no administre el dispositivo, deberá asegurarse de que los archivos de trabajo y los recursos de la empresa están protegidos.

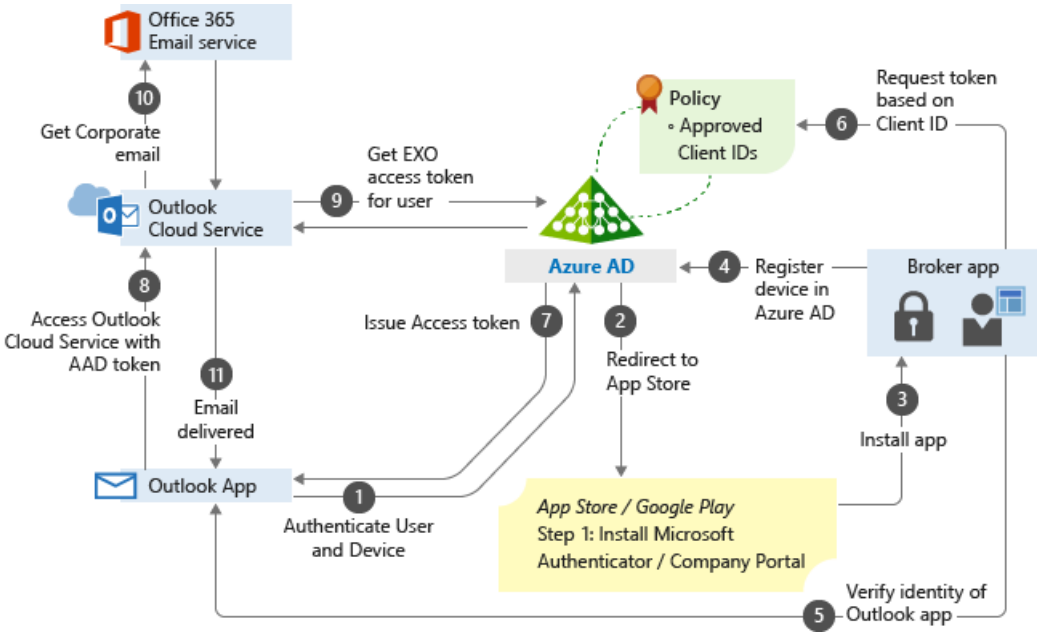
Puede usar directivas de protección de aplicaciones para impedir a los usuarios que guarden archivos de trabajo en ubicaciones desprotegidas. También puede restringir el movimiento de datos a otras aplicaciones que no estén protegidas por directivas de protección. La configuración de directivas de protección de aplicaciones incluye:

- Las directivas de reubicación de datos como **Guardar copias de los datos de la organización** y **Restringir funciones Cortar, Copiar y Pegar**.
- Opciones de directivas de acceso para requerir un PIN sencillo para el acceso o bloquear las aplicaciones administradas para que no se ejecuten en dispositivos con jailbreak o rooting

El acceso condicional basado en la aplicación y la administración de aplicaciones cliente agregan una capa de seguridad al garantizar que solo las aplicaciones cliente que admiten las directivas de protección de aplicaciones de Intune pueden acceder a Exchange Online y a otros servicios de Microsoft 365.

Puede bloquear las aplicaciones de correo electrónico integradas en iOS/iPadOS y Android cuando solo permita a la aplicación Microsoft Outlook acceder a Exchange Online. Además, puede bloquear las aplicaciones que no tienen directivas de protección de aplicaciones de Intune aplicadas para que no puedan acceder a SharePoint Online.

En este ejemplo, el administrador ha aplicado directivas de protección de aplicaciones a la aplicación Outlook, seguidas de una regla de acceso condicional que agrega la aplicación Outlook a una lista de aplicaciones admitidas que pueden usarse al obtener acceso al correo electrónico corporativo.



Requisitos previos

Necesitará los siguientes permisos de administrador de Intune:

- Permisos de lectura, creación, eliminación y asignación de aplicaciones administradas
- Permisos de lectura, creación y asignación de conjuntos de directivas
- Permiso de lectura de la organización

Paso 1: introducción

Si se sigue el escenario guiado de **protección de aplicaciones de Intune**, impedirá que los datos se compartan o se filtren fuera de la organización.

Los usuarios de iOS/iPadOS y Android asignados deben escribir un PIN cada vez que abren una aplicación de Office. Tras cinco intentos de PIN incorrectos, los usuarios deben restablecer el PIN. Si ya se requiere un PIN de

dispositivo, los usuarios no se verán afectados.

Qué se necesita para continuar

Le preguntaremos por las aplicaciones que los usuarios necesitan y lo que es necesario para acceder a ellas. Asegúrese de tener la siguiente información a mano:

- Lista de las aplicaciones de Office aprobadas para su uso corporativo
- Cualquier requisito de PIN para iniciar aplicaciones aprobadas en dispositivos no administrados

Paso 2: aspectos básicos

En este paso, debe especificar el **Prefijo** y una **Descripción** de la nueva directiva de protección de aplicaciones. Cuando agregue el **Prefijo**, se actualizarán los detalles relacionados con los recursos creados en el escenario guiado. Estos detalles permitirán encontrar más fácilmente las directivas más adelante por si necesita cambiar las asignaciones y la configuración.

> **TIP**
> Considere la posibilidad de tomar nota de los recursos que se crearán para, así, poder hacer referencia a ellos posteriormente.

Paso 3: aplicaciones

Para ayudarle a empezar, en este escenario guiado ya se han seleccionado previamente las siguientes aplicaciones móviles para protegerlas en dispositivos iOS/iPadOS y Android:

- Microsoft Excel
- Microsoft Word
- Microsoft Teams
- Microsoft Edge
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft OneDrive

En este escenario guiado también se configurarán estas aplicaciones para abrir vínculos web en Microsoft Edge con el fin de garantizar que los sitios de trabajo se abren en un explorador protegido.

Modifique la lista de aplicaciones administradas por directivas que quiera proteger. En la lista, agregue o quite aplicaciones.

Cuando termine de seleccionar las aplicaciones, haga clic en **Siguiente**.

Paso 4: configuración

En este paso, debe configurar los requisitos de acceso y uso compartido de los archivos y correos electrónicos corporativos en estas aplicaciones. Los usuarios pueden guardar los datos de forma predeterminada en las cuentas de OneDrive y SharePoint de la organización.

OPCIÓN	DESCRIPTION	VALOR PREDETERMINADO

OPCIÓN	DESCRIPTION	VALOR PREDETERMINADO
Tipo de PIN	Los PIN numéricos se componen únicamente de números, mientras que los códigos de acceso pueden contener caracteres alfanuméricos y caracteres especiales. Para configurar el tipo de código de acceso en iOS/iPadOS, es necesario que la aplicación tenga la versión 7.1.12 del SDK de Intune o una versión posterior. El tipo numérico no tiene ninguna restricción de versión para el SDK de Intune.	Numérico
Seleccionar la longitud mínima del PIN	especifique el número mínimo de dígitos en una secuencia de PIN.	6
Volver a comprobar los requisitos de acceso tras (minutos de inactividad)	Si la aplicación administrada por directivas lleva inactiva más tiempo que el número de minutos de inactividad aquí especificado, la aplicación pedirá que se vuelvan a comprobar los requisitos de acceso (esto es, el PIN, la configuración de inicio condicional) después de que se inicie la aplicación.	30
Impresión de datos de la organización	Si se establece en Bloquear, la aplicación no puede imprimir datos protegidos.	Bloquear
Abrir vínculos de aplicaciones administradas por directivas en exploradores no administrados	Si se establece en Bloquear, los vínculos de las aplicaciones administradas por directivas se deben abrir en un explorador administrado.	Bloquear
Copiar datos en aplicaciones no administradas	Si se establece en Bloquear, los datos administrados permanecerán en las aplicaciones administradas.	Allow

Paso 5: asignaciones

En este paso, puede elegir los grupos de usuarios que quiere incluir para asegurarse de que tienen acceso a los datos corporativos. La protección de aplicaciones se asigna a usuarios, no a dispositivos, por lo que los datos corporativos serán seguros independientemente del dispositivo que se use y su estado de inscripción.

Los usuarios que no tengan asignadas directivas de protección de aplicaciones ni una configuración de acceso condicional podrán guardar datos de su perfil corporativo en aplicaciones personales y en un almacenamiento local no administrado de sus dispositivos móviles. También podrán conectarse a servicios de datos corporativos (como, por ejemplo, Microsoft Exchange) con sus aplicaciones personales.

Paso 6: revisión y creación

El último paso permite revisar un resumen de los valores que ha configurado. Una vez que haya revisado las opciones, haga clic en **Crear** para completar el escenario guiado. Tras completar el escenario guiado, se muestra una tabla de recursos. Puede editar estos recursos más adelante, pero una vez que salga de la vista de resumen, la tabla no se guardará.

IMPORTANT

Cuando se haya completado el escenario guiado, se mostrará un resumen. Los recursos mencionados en este resumen se pueden modificar más adelante, pero la tabla en la que se muestran estos recursos no se guardará.

Pasos siguientes

- Para mejorar la seguridad de los archivos de trabajo, asigne a los usuarios una directiva de acceso condicional basado en aplicaciones que impida que los servicios en la nube envíen archivos de trabajo a aplicaciones sin protección. Para más información, vea Configuración de directivas de acceso condicional basado en la aplicación con Intune.

Escenario guiado: Configuración de Windows 10 en la nube

14/05/2021 • 10 minutes to read

Windows 10 en configuración de nube es una configuración de dispositivo recomendada por Microsoft. Puede convertir cualquier dispositivo con Windows 10 Professional, Enterprise y Education en un punto de conexión optimizado para la nube.

Esto es ideal para los siguientes usuarios:

- Trabajadores de primera línea
- Trabajadores remotos
- Otros usuarios con necesidades de flujo de trabajo específicas, como la productividad y la navegación

La configuración en la nube permite que sea más fácil usar estos dispositivos, y los protege con las características de seguridad recomendadas por Microsoft.

Con la configuración de Windows 10 en la nube conseguirá todo esto:

- Puede configurar nuevos dispositivos o reutilizar el hardware existente.
- Los usuarios finales obtienen una experiencia de Windows fácil de usar y familiar.
- Además, facilita la administración y la solución de problemas, ya que permite a los administradores aplicar una configuración de dispositivo uniforme en todos los dispositivos.
- Puede personalizar los nombres de los recursos, por lo que serán fáciles de ver y supervisar.

> **TIP**
> Para obtener más información sobre la configuración de Windows 10 en la nube, consulte Configuración de Windows 10 en la nube.

Funcionalidad de este escenario guiado

Con Microsoft Endpoint Manager, puede usar un escenario guiado para implementar una configuración en la nube. El escenario guiado crea automáticamente todos los recursos que necesita, incluidos los siguientes:

- Crea un grupo de seguridad de Azure AD o usa uno que ya exista.
- Implementa las aplicaciones Microsoft Edge y Microsoft Teams. Para obtener más información sobre la implementación de estas aplicaciones de forma individual, consulte los siguientes vínculos:
  - Adición de Microsoft Edge para Windows 10 a Microsoft Intune
  - Adición de aplicaciones de Microsoft 365 a dispositivos Windows 10 mediante Microsoft Intune
- Crea una directiva de línea de base de seguridad de Windows 10 con la configuración de seguridad recomendada que ya está configurada.

  Para obtener más información sobre las líneas de base de seguridad y lo que hacen, consulte Uso de líneas de base de seguridad para configurar dispositivos Windows 10 en Intune.
- Crea un perfil de inscripción de Windows Autopilot que inscribe automáticamente los dispositivos en Microsoft Intune.

Para obtener más información sobre cómo crear su propio perfil de Autopilot, consulte Configuración de perfiles de Autopilot.

- Activa y configura la página Estado de inscripción de Autopilot (ESP). En esta página se muestra el progreso de la inscripción de los usuarios.

  Para obtener más información acerca de ESP, consulte Configuración de la página de estado de la inscripción.

- Crea una plantilla administrativa que configura OneDrive con la configuración para mover carpetas conocidas. Con esta configuración, los datos y los archivos de usuario se guardan automáticamente en OneDrive.

  Para obtener más información sobre esta configuración, consulte Redirigir y mover carpetas conocidas de Windows a OneDrive.

- Crea una plantilla administrativa que configura algunos valores de SmartScreen en la aplicación Microsoft Edge. Para obtener más información sobre cómo crear su propio perfil, consulte Configuración de opciones de directivas de Microsoft Edge en Microsoft Intune.

- Crea una directiva de cumplimiento que supervisa el cumplimiento y el estado. Los usuarios pueden usar dispositivos no compatibles y acceder a los recursos. Si su organización bloquea el acceso a dispositivos no compatibles, cree otra directiva de cumplimiento que bloquee el acceso y asígnela al mismo grupo.

  Para obtener más información sobre la configuración de cumplimiento personalizable, consulte Configuración de Windows 10 y versiones posteriores para marcar dispositivos como compatibles o no compatibles con Intune.

- Implementa un script de Windows PowerShell que quita las aplicaciones integradas y simplifica el menú Inicio.

  Para obtener más información sobre PowerShell, consulte Uso de scripts de PowerShell para dispositivos Windows 10 en Intune.

- Crea una directiva de anillo de actualización de Windows 10. Esta directiva actualiza automáticamente los dispositivos, incluidas las actualizaciones del producto, los controladores y las actualizaciones de Windows.

  Para obtener más información sobre los anillos de actualización y la creación de la directiva, consulte Directiva de anillos de actualización de Windows 10 en Intune.

> **TIP**
> Este escenario guiado crea automáticamente todos estos recursos. Si desea crear sus propios recursos y no utilizar el escenario guiado, puede hacerlo. Para conocer los pasos específicos, consulte la guía de la configuración en la nube.

Requisitos previos

- Como mínimo, debe tener las siguientes licencias:
  - Azure Active Directory Premium P1
  - Microsoft Intune
  - Microsoft Teams
  - OneDrive para la Empresa
  - Windows 10 Pro

  Todos estos servicios se incluyen en la licencia Microsoft 365 E3. Para obtener más opciones y

características de seguridad, se recomienda usar la licencia Microsoft 365 E5. Para ayudar a decidir qué licencia es adecuada para su organización, consulte Transformar la empresa con Microsoft 365.

- Establecer la entidad de MDM en Intune. La configuración de la entidad de administración de dispositivos móviles (MDM) determina cómo se administran los dispositivos. Como administrador de TI, debe establecer una entidad de MDM antes de que los usuarios puedan inscribir dispositivos para la administración.
- Habilite la inscripción automática para dispositivos Windows 10. Para más información, consulte:
  - Inicio rápido: Configurar la inscripción automática para dispositivos Windows 10
  - Habilitar la inscripción automática de Windows 10
- Inicie sesión como administrador del servicio Intune (también conocido como "Administrador de Intune"). Para obtener más información sobre los roles de Intune, consulte Control de acceso basado en rol (RBAC) con Microsoft Intune.

Paso 1: introducción

1. Abra el Centro de administración de Microsoft Endpoint Manager.
2. Seleccione **Solución de problemas + soporte técnico** > **Escenarios guiados** > **Implementar configuración de Windows 10 en la nube** > **Iniciar**.
3. Seleccione **Next** (Siguiente).

Paso 2: aspectos básicos

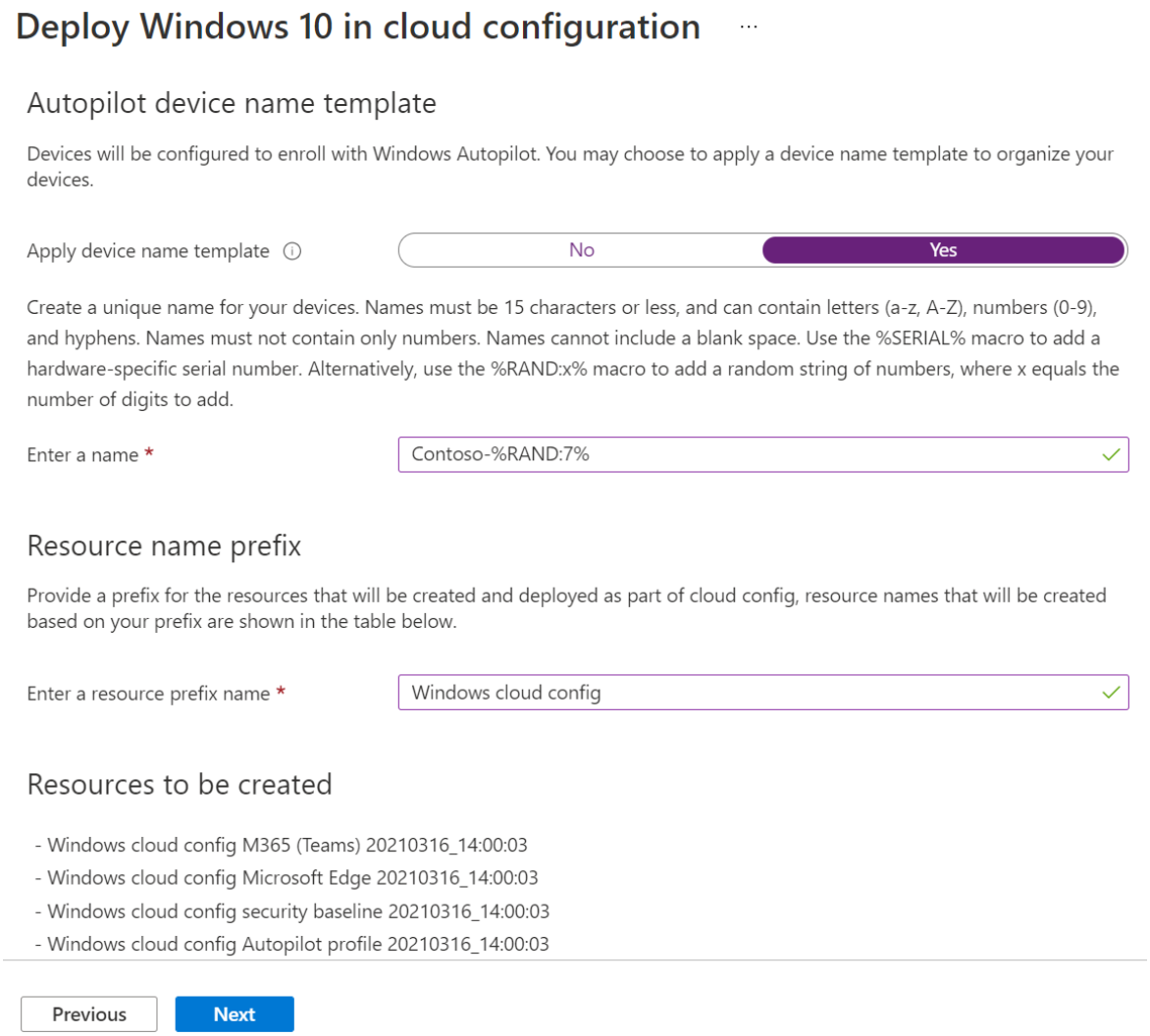
Elija cómo se asignarán los nombres a los dispositivos al inscribirse y elija el prefijo de todos los recursos creados.

- **Plantilla de nombre de dispositivo de Autopilot**: este escenario guiado inscribe los dispositivos en Windows Autopilot. Cuando se inscriben, si lo desea, puede asignar nombres a los dispositivos mediante un patrón único que se aplica a todos los dispositivos. Las opciones son:
  - **Aplicar plantilla de nombre de dispositivo**: **No** no crea una plantilla o un patrón al asignar nombres a los dispositivos. El dispositivo tendrá el nombre del OEM, como `DESKTOP-`, seguido de algunos caracteres aleatorios. Seleccione **Sí** para crear un modelo único para asignar un nombre a los dispositivos. Por ejemplo, escriba `Contoso-%RAND:7%` para asignar un nombre a todos los dispositivos **Contoso-** seguido de siete caracteres aleatorios.

    Los nombres deben cumplir estos requisitos:

    - Necesitan tener 15 caracteres o menos.
    - Pueden incluir letras (a-z, A-Z), números (0-9) y guiones.
    - No pueden ser solo números y no pueden incluir un espacio en blanco.
    - Pueden usar la macro `%SERIAL%` para agregar el número de serie de hardware específico.
    - Pueden usar la macro `%RAND:x%` para agregar una cadena de caracteres aleatoria, donde `x` equivale al número de dígitos para agregar.
- **Prefijo de nombre de recurso**: al implementar este escenario guiado, se crean automáticamente varios recursos. Para distinguir los elementos utilizados en esta implementación, agregue un prefijo:
  - **Escriba un nombre de prefijo de recurso**: escriba algún texto que vaya al principio de los elementos creados. Por ejemplo, escriba `Windows cloud config`. Todos los recursos creados se llamarán **Perfil de Autopilot de configuración de Windows en la nube** o **Directiva de cumplimiento de configuración de Windows en la nube**, o algo similar.

  La configuración será similar a la imagen siguiente:



- Seleccione **Next** (Siguiente).

Paso 3: aplicaciones

Seleccione las aplicaciones que desea implementar en los dispositivos. Microsoft recomienda implementar el menor número posible de aplicaciones. La idea es que los dispositivos de configuración en la nube sean sencillos y fáciles de administrar.

- **Valores predeterminados de configuración en la nube**: este escenario guiado incluye automáticamente las aplicaciones Microsoft Edge y Microsoft Teams. No se pueden quitar al crear el escenario guiado. Puede eliminar o desinstalar estas aplicaciones después de que finalice el escenario guiado.

  Para quitar la aplicación Microsoft Edge, consulte Desinstalación de la aplicación.

- **Seleccione más aplicaciones de Microsoft 365 (opcional)** : en la lista, agregue más aplicaciones de Microsoft 365 que desee en los dispositivos. Recuerde que la lista debe ser reducida y que tiene que incluir solo las aplicaciones que necesiten los usuarios. La idea es que los dispositivos sean sencillos.

> **TIP**
> Para agregar aplicaciones que no aparezcan en la lista o agregar aplicaciones de línea de negocio, complete este escenario guiado. En el Centro de administración de Endpoint Manager, vaya a **Aplicaciones** y cree una directiva. Implemente la directiva de aplicación en el mismo grupo en el que implementó este escenario de configuración en la nube. Para obtener más información sobre cómo agregar aplicaciones, consulte Incorporación de aplicaciones a Microsoft Intune.

- Seleccione **Next** (Siguiente).

Paso 4: asignaciones

Seleccione los grupos que recibirán este escenario guiado, y todos los recursos que cree.

- **Crear nuevo grupo**: crea un nuevo grupo e implementa las directivas de escenario guiado para este grupo. A medida que se agreguen dispositivos a este grupo, empezarán a recibir este escenario guiado.
  - **Nombre de grupo**: escriba el nombre del grupo. Por ejemplo, escriba `Cloud configured devices`.
- **Elegir un grupo existente**: seleccione un grupo que ya exista. Se han implementado las directivas del escenario guiado en este grupo.
- Seleccione **Next** (Siguiente).

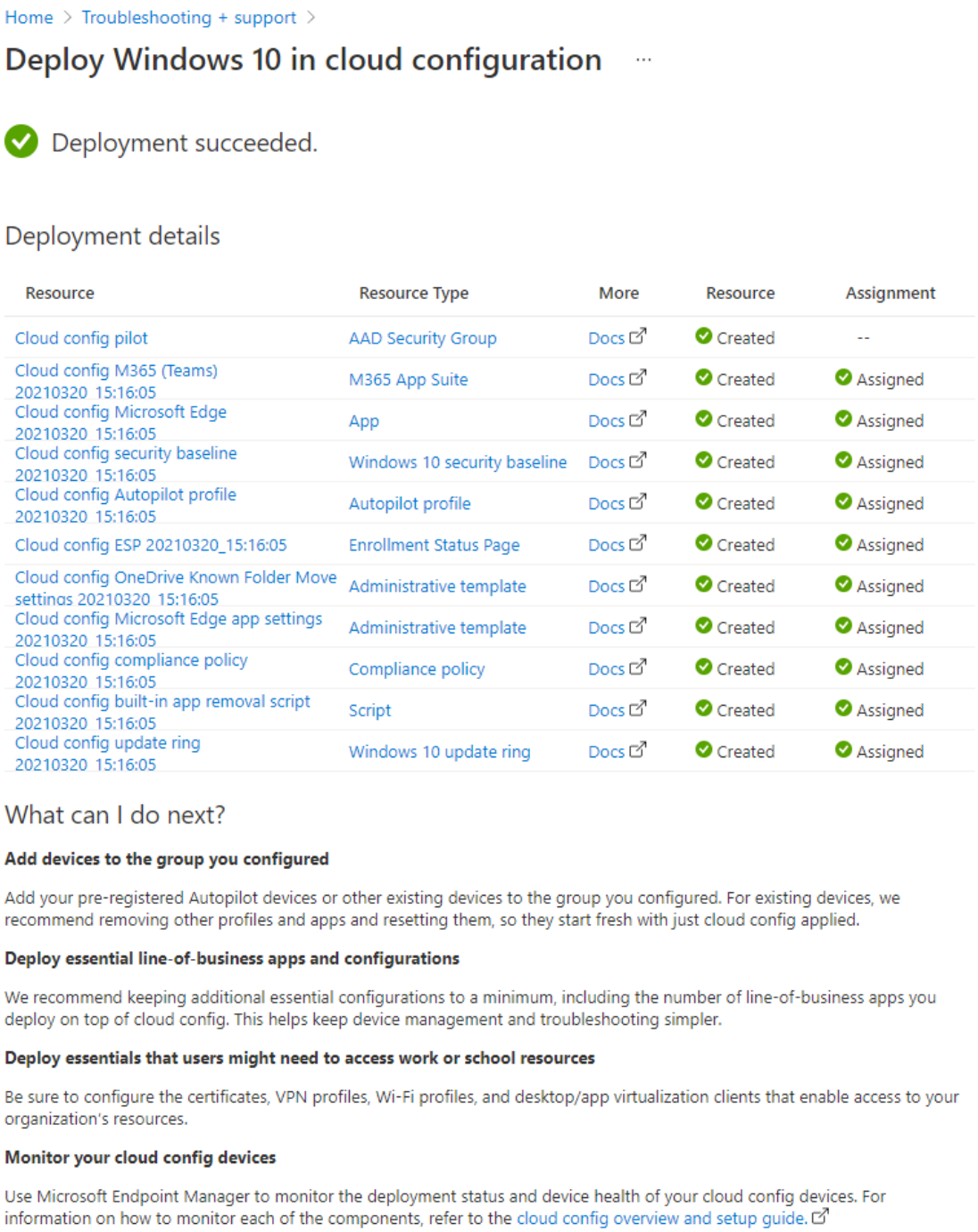
Paso 5: Revisión e implementación

Se muestra un resumen de la configuración y los valores que ha configurado. Puede volver a las otras pestañas y cambiar los valores agregados.

Observe las propiedades siguientes:

- **Configuraciones que se van a realizar**: expanda esta opción para ver todos los recursos que se crearán, incluidas las directivas.
- **Implementar**: seleccione esta opción para guardar los cambios e implementar el escenario guiado. Los grupos que ha agregado recibirán las directivas de este escenario guiado.

  A medida que se crean los recursos en el Centro de administración de Endpoint Manager, el estado se muestra de un modo similar a la siguiente imagen:



Si hay un error, el escenario guiado no se implementa y se revierten todos los cambios. La guía de la configuración en la nube también es un buen recurso.

Cuando se implementa correctamente, puede usar las características de supervisión y generación de informes en el Centro de administración de Endpoint Manager:

- Informes de Intune
- Supervisar perfiles de dispositivo
- Supervisión de las líneas base de seguridad y los perfiles

Aspectos que debe saber

- Puede completar el escenario guiado antes de que haya dispositivos en el grupo. Cuando los dispositivos se agregan al grupo y tienen acceso a Internet, empezarán a recibir automáticamente las directivas de este escenario guiado.

  También puede:

    - Agregar dispositivos de Windows Autopilot previamente registrados al grupo. Agréguelos al grupo antes de inscribir o aplicar directivas.
    - Agregar los dispositivos con Windows 10 que ya están inscritos. Microsoft recomienda quitar otras aplicaciones y perfiles destinados a estos dispositivos. Después de agregarlos al grupo, restablezca los dispositivos para que se inicien con solo la configuración en la nube aplicada.

  Para obtener información sobre los tiempos de actualización de las directivas, consulte las preguntas y respuestas frecuentes con las directivas de políticas en Microsoft Intune.

- Microsoft solo recomienda asignar opciones y aplicaciones de configuración en la nube. Después de implementar este escenario guiado, puede agregar cualquier otro recurso necesario, como certificados, perfiles de VPN, aplicaciones de línea de negocio, etc. Asegúrese de implementar estas directivas en el mismo grupo que este escenario guiado. Recuerde que la lista debe ser reducida y que tiene que incluir solo los recursos que necesiten los usuarios.

- Microsoft no recomienda usar la configuración de Windows 10 en la nube con dispositivos compartidos, debido a un problema de sincronización de OneDrive con los dispositivos compartidos. Los dispositivos compartidos suelen tener varios usuarios que inician y cierran sesión.

- Una vez implementado el escenario guiado, puede ir a una directiva y ver la configuración y los valores configurados. Puede cambiar cualquiera de estas opciones a otro valor, si lo desea.

- Para quitar la configuración del escenario guiado de los dispositivos, vaya a cada una de las directivas creadas en el escenario de configuración en la nube. Establezca la configuración en **No configurado**. Vuelva a implementar cada directiva en el mismo grupo que este escenario guiado.

  La próxima vez que el dispositivo se registre, la configuración ya no se bloqueará. La configuración se puede cambiar por otra directiva y, posiblemente, por el usuario final. Es posible que la configuración tenga el mismo valor establecido por el escenario guiado.

  Ahora, puede eliminar los elementos creados en este escenario guiado, incluidas las aplicaciones, las directivas, el script de Windows PowerShell y el grupo.

Pasos siguientes

- Para obtener más información sobre los escenarios guiados y ver los otros escenarios disponibles, consulte Introducción a los escenarios guiados de Intune.
- Para obtener más información sobre la configuración de Windows 10 en la nube, consulte Configuración de Windows 10 en la nube.

Usos habituales de Microsoft Intune

14/05/2021 • 7 minutes to read

Antes de sumergirse en las tareas de implementación, es importante poner de acuerdo a las partes interesadas de Enterprise Mobility en torno a los objetivos empresariales de utilización de Intune. El acuerdo de las partes interesadas es fundamental cuando se es totalmente profano en Enterprise Mobility o al migrar desde otro producto.

Las necesidades de Enterprise Mobilityestán en constante evolución y, en este sentido, los distintos métodos de Microsoft para abordar estas necesidades son a veces diferentes de los de otras soluciones del mercado. La mejor manera de ponerse de acuerdo en torno a los objetivos empresariales es expresar lo que se pretende lograr en lo relativo a los escenarios que se quieren habilitar para los empleados, los asociados y el departamento de TI.

A continuación se presentan brevemente los seis escenarios más comunes que se basan en Intune, así como vínculos para obtener más información sobre cómo planear e implementar cada uno de ellos.

NOTE

- ¿Quiere saber cómo usa Intune el equipo de TI de Microsoft para dar acceso corporativo a dispositivos móviles y, al mismo tiempo, tener protegidos los datos de la empresa? Consulte la biblioteca de TI y busque "Intune".
- Los blogs de seguridad y cumplimiento de Microsoft son un excelente recurso. Puede filtrar por las áreas que le interesen, como Enterprise Mobility + Security, la prevención de pérdida de datos, la administración de acceso e identidad, etc.

Proteger el correo electrónico y los datos locales para tener acceso a ellos sin riesgos desde un dispositivo móvil

La mayoría de las estrategias de Enterprise Mobility arranca con un plan que permite que los empleados tengan un acceso seguro al correo electrónico con dispositivos móviles conectados a Internet. Muchas organizaciones todavía tienen datos y servidores de aplicaciones locales, como Microsoft Exchange, que están hospedados en la red corporativa.

Intune y Microsoft Enterprise Mobility + Security (EMS) proporcionan una solución de acceso condicional integrada de manera exclusiva para Exchange Server, que garantiza que ninguna aplicación móvil puede tener acceso al correo electrónico hasta que el dispositivo esté inscrito con Intune. Puede implementar este tipo de dirección de correo electrónico sin implementar otra máquina de puerta de enlace en el extremo de la red corporativa.

Intune también permite el acceso a las aplicaciones móviles que requieren un acceso seguro a los datos locales, como servidores de aplicaciones de línea de negocio. Este tipo de acceso se suele llevar a cabo mediante certificados administrados por Intune para el control de acceso, combinado con un proxy o una puerta de enlace de VPN estándar en el perímetro (como, por ejemplo, el Proxy de aplicación de Microsoft Azure Active Directory).

En estos casos, la única manera de tener acceso a los datos corporativos es inscribir el dispositivo en la administración. Una vez que se han inscrito los dispositivos, el sistema de administración procura que los dispositivos cumplan con las directivas en vigor para que puedan tener acceso a los datos corporativos. Además, el SDK de aplicaciones y la herramienta de ajuste de aplicaciones de Intune pueden contener los datos a los que se ha tenido acceso dentro de la aplicación de línea de negocio, de forma que los datos corporativos no se

puedan pasar a servicios o aplicaciones de consumidor.

Protección del correo electrónico y los datos de Microsoft 365 para tener acceso a ellos sin riesgos desde un dispositivo móvil

La protección de los datos empresariales de Microsoft 365 (correo electrónico, documentos, mensajes instantáneos, contactos) no podría ser más sencilla o transparente para los usuarios.

Intune y Microsoft Enterprise Mobility + Security proporcionan una solución de acceso condicional integrada de forma única que garantiza que ningún usuario, aplicación o dispositivo pueda tener acceso a los datos de Microsoft 365, a menos que cumpla los requisitos de cumplimiento de la empresa (es decir, realizar una autenticación multifactor, estar inscrito con Intune, usar la aplicación administrada, disponer de una versión compatible del sistema operativo, tener un PIN de dispositivo, contar con un perfil de riesgo de usuario bajo, etc.).

Las aplicaciones móviles de Office que se encuentran en sus respectivas tiendas de aplicaciones están preparadas para adaptarse a las directivas de contención de datos que se pueden configurar mediante Intune. Esto permite evitar que los datos se compartan con aplicaciones (por ejemplo, aplicaciones de correo electrónico nativas) y con ubicaciones de almacenamiento (por ejemplo, Dropbox) que no administra el departamento de TI. Todas estas funciones están integradas en Microsoft 365 y EMS. No tendrá que implementar ninguna otra infraestructura para poder disfrutar de ellas.

Una práctica común de implementación de Microsoft 365 consiste en exigir que los dispositivos estén inscritos en la administración si se tienen que configurar completamente con las opciones de configuración de aplicaciones, certificados, Wi-Fi o VPN corporativos, un escenario habitual para dispositivos de propiedad corporativa.

En cambio, si el usuario solo necesita obtener acceso a los documentos y el correo electrónico corporativo (que suele ser el caso de los dispositivos de propiedad personal), puede exigir al usuario que use las aplicaciones móviles de Office (regidas por directivas de protección de datos) y no será preciso inscribir el dispositivo.

En cualquier caso, los datos de Microsoft 365 estarán protegidos por las directivas que haya definido usted.

Ofrecer un programa "Bring Your Own Device" a todos los empleados

Bring Your Own Device (BYOD) es cada vez más popular en las organizaciones como forma de reducir los gastos de hardware o de aumentar las opciones de productividad móvil de los empleados. A día de hoy, casi todo el mundo tiene un teléfono personal, así que, ¿qué necesidad hay de darles otro? El principal desafío siempre ha sido convencer a los empleados de que inscriban sus dispositivos personales en la administración, ya que les inquieta lo que el departamento de TI pueda ver en su dispositivo y hacer con él.

Cuando la inscripción de dispositivos no es una opción viable, Intune ofrece un método alternativo de BYOD con el que simplemente se administran las aplicaciones que contengan datos corporativos. Intune protege los datos corporativos incluso cuando la aplicación en cuestión tiene acceso a datos personales y a datos corporativos, como ocurre en las aplicaciones móviles de Office.

Como administrador, puede obligar a que los usuarios accedan a Microsoft 365 desde las aplicaciones móviles de Office, así como configurar las aplicaciones con directivas que mantengan los datos protegidos (por ejemplo, mediante el cifrado, la protección con PIN, etc.). Estas directivas de protección de aplicaciones evitan la pérdida de datos en aplicaciones y ubicaciones de almacenamiento no administradas, tanto dentro como fuera de esas aplicaciones. Por ejemplo, las directivas impiden que un usuario copie texto de un perfil de correo electrónico corporativo en un perfil de correo electrónico de consumidor, aun cuando ambos perfiles estén configurados en Outlook Mobile. Se pueden implementar configuraciones similares relativas a otros servicios y aplicaciones que los usuarios de BYOD necesiten.

Distribuir teléfonos de propiedad corporativa entre los empleados

En la actualidad, la mayoría de los empleados está en constante movimiento, de modo que la productividad de los dispositivos móviles es esencial para ser competitivos. Los empleados necesitan un acceso sin trabas a todas las aplicaciones y datos corporativos, en todo momento y estén donde estén. En este sentido, conviene garantizar que los datos corporativos estén protegidos y los costos administrativos sean bajos.

Intune ofrece soluciones de aprovisionamiento masivo y administración que se integran con las plataformas de administración de dispositivos corporativos más importantes del mercado de hoy día, incluidos el Programa de inscripción de dispositivos de Apple y la plataforma de seguridad móvil Samsung KNOX. La creación centralizada de configuraciones de dispositivos con Intune hace posible que el aprovisionamiento de dispositivos corporativos se automatice en un alto grado.

Imagínese: entrega una caja de iPhone sin abrir a un empleado. El empleado lo enciende y se le guía por un proceso de configuración de marca corporativa en el que debe autenticarse. El iPhone se configura a la perfección junto a las directivas de seguridad.

Después, el empleado inicia la aplicación de portal de empresa de Intune para tener acceso a una serie de aplicaciones corporativas opcionales disponibles.

Distribuir tabletas compartidas de uso limitado entre los empleados

Los empleados usan las tecnologías móviles con una frecuencia cada vez mayor. Por ejemplo, ahora las tabletas compartidas están a la orden del día entre los empleados de los comercios al por menor. Independientemente de si se usan para tramitar una venta o comprobar el inventario de forma inmediata, las tabletas ayudan a lograr una excelente interacción con los clientes.

En este caso, la simplicidad de la experiencia del usuario es fundamental. Por este motivo, las tabletas se suelen entregar a los empleados en un modo de uso limitado, de forma que solo puedan interactuar con una única aplicación de línea de negocio. Intune permite aprovisionar de forma masiva, proteger y administrar centralmente estas tabletas de iOS y Android compartidas que pueden configurarse para funcionar en este modo de uso limitado.

Concesión de permiso para que los empleados tengan acceso seguro a Microsoft 365 desde un quiosco público no administrado

A veces, los empleados necesitan usar dispositivos, aplicaciones o exploradores que no se pueden administrar, como los equipos públicos de ferias y hoteles.

¿Debe permitir que los empleados tengan acceso al correo electrónico de empresa desde ellos? Con Intune y Microsoft Enterprise Mobility + Security, puede decidir no hacerlo y limitar el acceso al correo electrónico a los dispositivos administrados por la organización. De este modo, se asegura de que un empleado con una autenticación sólida no deje accidentalmente datos corporativos en un equipo que no es de confianza.

Pasos siguientes

- Guía de planeamiento de Microsoft Intune
- Escenarios guiados de Intune

Decisiones de tecnología para habilitar BYOD con Microsoft Enterprise Mobility + Security (EMS)

14/05/2021 • 3 minutes to read

Cuando desarrolle su estrategia para permitir que los empleados trabajen de forma remota en sus propios dispositivos (BYOD), tiene que tomar importantes decisiones en los escenarios para habilitar BYOD y proteger los datos corporativos. Por suerte, EMS ofrece todas las capacidades necesarias en un conjunto completo de soluciones.

En este tema se analiza el caso de uso sencillo de habilitar el acceso BYOD al correo electrónico corporativo. Se centra en si es o no necesario administrar todo el dispositivo o solo las aplicaciones, ambas opciones totalmente válidas.

Suposiciones

- Tiene conocimientos básicos de Azure Active Directory y Microsoft Intune
- Las cuentas de correo electrónico están hospedadas en Exchange Online

Razones habituales para administrar el dispositivo (MDM)

Puede impulsar fácilmente a los usuarios a inscribir sus dispositivos en la administración de dispositivos si implementa una directiva de acceso condicional en Exchange Online. Estos son los motivos por los que es posible que quiera administrar los dispositivos personales:

Wi-Fi/VPN : si los usuarios necesitan un perfil de conectividad corporativo para ser productivos, se puede configurar sin problemas.

Aplicaciones : si los usuarios necesitan instalar un conjunto de aplicaciones en el dispositivo, se pueden entregar sin problemas. Esto incluye aplicaciones que se puedan exigir por motivos de seguridad, como Mobile Threat Defense.

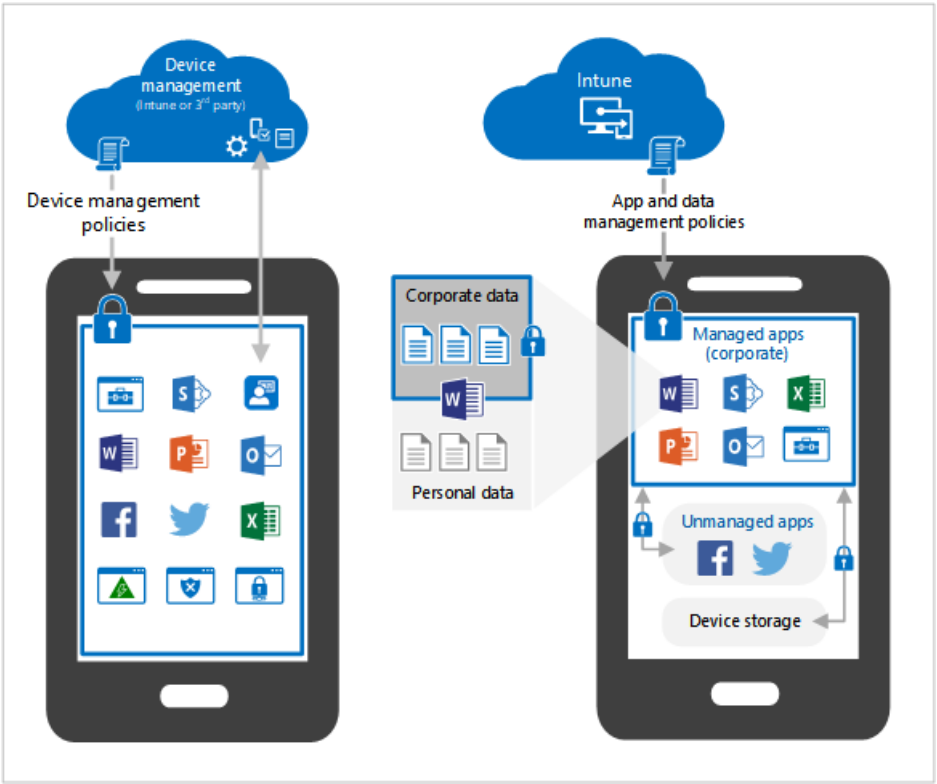
Cumplimiento : algunas organizaciones deben cumplir directivas reglamentarias u otras que exijan controles de MDM concretos. Por ejemplo, necesita que MDM cifre todo el dispositivo o elabore un informe de todas las aplicaciones del dispositivo.

Razones habituales para administrar solo las aplicaciones (MAM)

MAM sin MDM es muy popular en organizaciones que admiten BYOD. Puede sugerir a los usuarios que accedan al correo electrónico desde Outlook Mobile (compatible con las protecciones de MAM) implementando una directiva de acceso condicional en Exchange Online. Estos son los motivos por los que es posible que quiera administrar únicamente las aplicaciones de los dispositivos personales:

Experiencia de usuario : la inscripción de MDM incluye muchos mensajes de advertencia (aplicados por la plataforma) que suelen dar lugar a que el usuario desista de acceder al correo electrónico en el dispositivo personal después de todo. MAM es mucho menos alarmante para los usuarios, ya que simplemente aparece un mensaje emergente una vez para informar de que se han aplicado las protecciones de MAM.

Cumplimiento : algunas organizaciones deben cumplir directivas que exigen menos capacidades de administración en dispositivos personales. Por ejemplo, MAM solo puede quitar datos corporativos de las aplicaciones, a diferencia de MDM, que puede quitar todos los datos del dispositivo.



Más información sobre los ciclos de vida del dispositivo y la aplicación.

Comparación de capacidades de MDM y MAM

Como ya se ha mencionado, el acceso condicional puede llevar a un usuario a inscribir su dispositivo o a usar una aplicación administrada como Outlook Mobile. Se pueden aplicar muchas otras condiciones en cada caso, que incluyen:

- Qué usuario intenta acceder
- Si la ubicación es o no de confianza
- Nivel de riesgo de inicio de sesión
- Plataforma de dispositivo

Aun así, suele haber riesgos concretos que preocupan a muchas organizaciones. En la siguiente tabla se indican las preocupaciones comunes y la respuesta que ofrecen MDM y MAM.

PREOCUPACIÓN	MDM	MAM
Acceso a datos no autorizado	Exigir pertenencia a grupo	Exigir pertenencia a grupo
Acceso a datos no autorizado	Exigir inscripción del dispositivo	Exigir aplicación protegida
Acceso a datos no autorizado	Exigir ubicación determinada	Exigir ubicación determinada
Cuenta de usuario en peligro	Exigir MFA	Exigir MFA
Cuenta de usuario en peligro	Bloquear usuarios de alto riesgo	Bloquear usuarios de alto riesgo
Cuenta de usuario en peligro	PIN de dispositivo	PIN de aplicación

PREOCUPACIÓN	MDM	MAM
Dispositivo o aplicación en peligro	Exigir un dispositivo conforme	Comprobación de jailbreak/root al iniciar la aplicación
Dispositivo o aplicación en peligro	Cifrar datos de dispositivo	Cifrar datos de aplicación
Dispositivo extraviado o robado	Borrar todos los datos del dispositivo	Borrar todos los datos de la aplicación
Uso compartido de datos accidental o guardado en ubicaciones inseguras	Restricción de copias de seguridad de datos del dispositivo	Restricción de copias de seguridad de los datos de la organización
Uso compartido de datos accidental o guardado en ubicaciones inseguras	Restringir el guardado como	Restringir el guardado como
Uso compartido de datos accidental o guardado en ubicaciones inseguras	Deshabilitación de la impresión	Deshabilitación de la impresión de datos de la organización

Pasos siguientes

Es hora de decidir si va a habilitar BYOD en la organización al centrarse en la administración del dispositivo, de la aplicación o en una combinación de ambas. Usted elige la forma de implementación, aquella que le asegure que las características de identidad y seguridad disponibles en Azure AD siempre van a estar disponibles.

Use la guía de planeamiento de Intune para el siguiente nivel de planeamiento.

Administrar versiones de sistemas operativos con Intune

14/05/2021 • 6 minutes to read

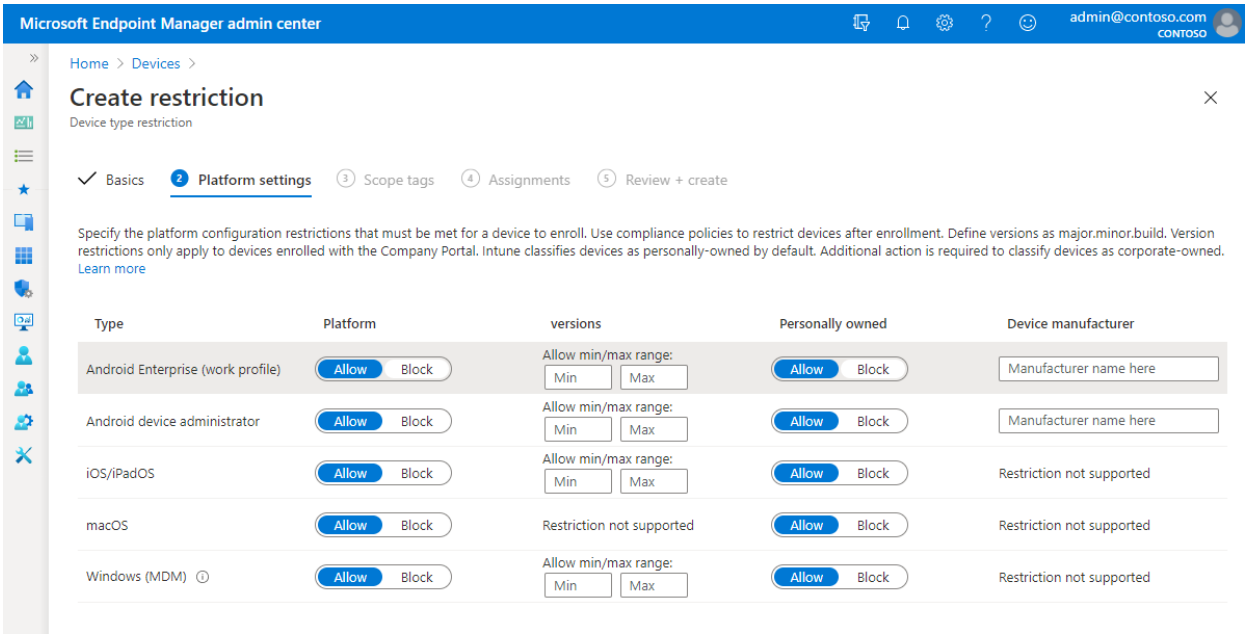
En las plataformas modernas de ordenadores y dispositivos móviles, podrá implementar rápidamente actualizaciones principales, revisiones y nuevas versiones. Tiene controles para administrar completamente las actualizaciones y revisiones en Windows, pero en otras plataformas, como iOS/iPadOS y Android, es necesario que los usuarios finales participen en el proceso. Microsoft Intune tiene las capacidades para ayudarle a estructurar la administración de versiones del sistema operativo en diferentes plataformas.

Intune puede ayudarle a resolver estos escenarios comunes:

- Determinar qué sistema operativo se ejecuta en los dispositivos de los usuarios finales
- Controlar el acceso a datos de la organización desde dispositivos mientras se valida una nueva versión del sistema operativo
- Inducir/requerir a los usuarios finales que actualicen la versión del sistema operativo a la más reciente aprobada por su organización
- Administrar el lanzamiento de una nueva versión del sistema operativo para toda la organización

Control de la versión del sistema operativo mediante las restricciones de inscripción de la administración de dispositivos móviles (MDM) de Intune

Las restricciones de inscripción de MDM de Intune le permiten definir los requisitos del dispositivo del cliente antes de permitir la inscripción del dispositivo. El objetivo es requerir que los usuarios finales inscriban solamente dispositivos compatibles para poder obtener acceso a los recursos de la organización. Los requisitos del dispositivo incluyen tanto las versiones del sistema operativo mínimas como las máximas admitidas para las plataformas compatibles.



A la práctica

Las organizaciones usan restricciones según el tipo de dispositivo para controlar el acceso a los recursos de la

organización mediante las siguientes opciones de configuración:

1. Usar la versión mínima del sistema operativo para que los usuarios finales usen plataformas actuales y compatibles en su organización.
2. No especificar la versión máxima del sistema operativo (sin límite) o establecerlo en la última versión validada en su organización para dar tiempo a que se prueben internamente las nuevas versiones del sistema operativo.

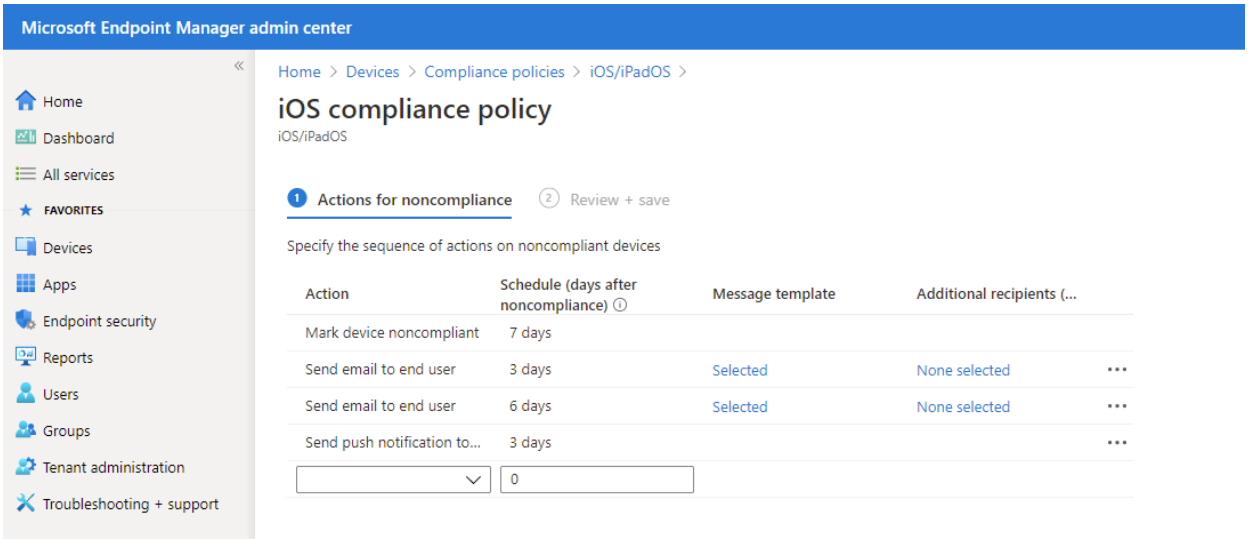
Para obtener información, consulte Establecer restricciones de tipo de dispositivo.

Informes de la versión del sistema operativo y cumplimiento de las directivas de cumplimiento de dispositivos de MDM de Intune

Las directivas de cumplimiento de dispositivos MDM de Intune proporcionan las siguientes herramientas:

- Especificar reglas de cumplimiento
- Ver el estado de cumplimiento mediante informes
- Actuar sobre los dispositivos no compatibles poniendo el dispositivo en cuarentena y ofreciéndole un acceso condicional

Igual que las restricciones de inscripción, las directivas de cumplimiento de dispositivos incluyen tanto la versión mínima como la máxima del sistema operativo. Las directivas también tienen una escala de tiempo de cumplimiento para ofrecer a los usuarios un período de gracia para cumplir con la directiva. Las directivas de cumplimiento del dispositivo hacen que los dispositivos de los usuarios finales inscritos cumplan con la directiva de la organización.



Para obtener información, consulte Introducción a las directivas de cumplimiento de dispositivos.

A la práctica

Las organizaciones usan las directivas de cumplimiento de dispositivos en los mismos escenarios que las restricciones de inscripción. Estas directivas hacen que los usuarios usen versiones actuales y validadas del sistema operativo en su organización. Si los dispositivos de los usuarios finales no cumplen las directivas, se puede bloquear el acceso a recursos de la organización mediante un acceso condicional hasta que los usuarios finales estén dentro del rango del sistema operativo compatible para su organización. A los usuarios finales se les informa de que no están cumpliendo con la directiva y se les explican los pasos para volver a obtener acceso.

Para obtener información, consulte Introducción a las directivas de cumplimiento de dispositivos.

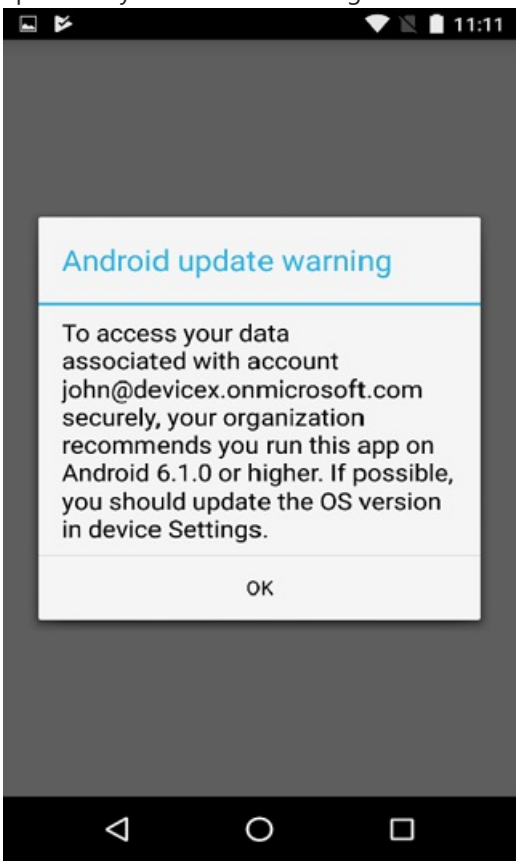
Controles de la versión del sistema operativo mediante directivas de

protección de aplicaciones de Intune

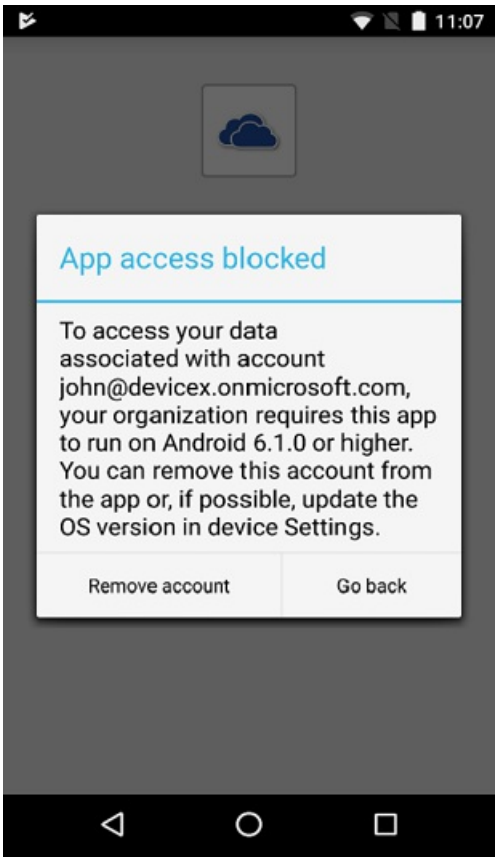
Las directivas de protección de aplicaciones de Intune y la configuración de acceso a la administración de aplicaciones móviles (MAM) le permiten especificar la versión mínima del sistema operativo en el nivel de aplicación. Esto le permite informar a los usuarios finales de que pueden actualizar su sistema operativo a una versión mínima especificada y fomentar o requerirles que lo hagan.

Tiene dos opciones:

- **Advertencia**: con la advertencia, se informa al usuario final de que debería actualizar la versión si abre una aplicación con una directiva de protección de aplicaciones o una configuración de acceso de MAM en un dispositivo con una versión de sistema operativo inferior a la especificada. Se permite el acceso a la aplicación y a los datos de la organización.



- **Bloqueo**: con el bloqueo, se informa al usuario final de que debe actualizar la versión si abre una aplicación con una directiva de protección de aplicaciones o una configuración de acceso de MAM en un dispositivo con una versión de sistema operativo inferior a la especificada. No se permite el acceso a la aplicación ni a los datos de la organización.



A la práctica

Al abrir o reanudar aplicaciones, las organizaciones usan la configuración de la directiva de protección de aplicaciones para explicar a los usuarios finales la necesidad de mantener las aplicaciones actualizadas. Por ejemplo, se podría establecer una configuración en la que a los usuarios finales se les advirtiera cuando estuvieran usando la versión actual menos uno y se les bloqueara cuando usaran la versión actual menos dos.

Para obtener información, consulte Creación y asignación de directivas de protección de aplicaciones.

Administrar el lanzamiento de una versión de sistema operativo

Puede usar las capacidades de Intune que se describen en este artículo para implementar una nueva versión de sistema operativo en su organización en la escala de tiempo que defina. En los pasos siguientes se ofrece un modelo de implementación de muestra para hacer que los usuarios de la versión 1 del sistema operativo pasen a la versión 2 en un plazo de siete días.

1. use las restricciones de lanzamiento para requerir la versión 2 del sistema operativo como versión mínima para inscribir el dispositivo. Esto garantiza que los dispositivos de los usuarios finales nuevos cumplan los requisitos a la hora de realizar la inscripción.
2. use las directivas de protección de aplicaciones de Intune para advertir a los usuarios de que se requiere la versión 2 del sistema operativo cuando la aplicación se abra o reanude.
3. use las directivas de cumplimiento de dispositivos para requerir la versión 2 del sistema operativo como versión mínima para que un dispositivo cumpla los requisitos. En los casos en que no se cumplan los requisitos, use **Acciones** para conceder un período de gracia de siete días y enviar una notificación por correo electrónico a los usuarios finales con la escala de tiempo y los requisitos.
   - En estas directivas se informará a los usuarios finales de que los dispositivos existentes deben actualizarse por correo electrónico, a través del Portal de empresa de Intune y, si la aplicación está abierta y tiene la función habilitada, con una directiva de protección de aplicaciones.
   - Puede ejecutar un informe de cumplimiento para identificar a los usuarios que no cumplan los requisitos.
4. use las directivas de protección de aplicaciones de Intune para bloquear a los usuarios que usen un

dispositivo en el que no se esté ejecutando la versión 2 del sistema operativo cuando se abra o reanude una aplicación.

5. use las directivas de cumplimiento de dispositivos para requerir la versión 2 del sistema operativo como versión mínima para que un dispositivo cumpla los requisitos.
    - Estas directivas requieren que los dispositivos estén actualizados para seguir teniendo acceso a datos de la organización. Los servicios protegidos se bloquean cuando se usan con acceso condicional al dispositivo. Las aplicaciones que disponen de una directiva de protección de aplicaciones se bloquean cuando se abren o cuando acceden a datos de la organización.

Pasos siguientes

Use los siguientes recursos para administrar las versiones del sistema operativo en su organización:

- Establecer restricciones de tipo de dispositivo
- Introducción al cumplimiento de dispositivos
- Creación y asignación de directivas de protección de aplicaciones

Administre y use diferentes características de administración de dispositivos en los dispositivos Windows Holographic y HoloLens con Intune

14/05/2021 • 8 minutes to read

Microsoft Intune incluye muchas características que ayudan a administrar los dispositivos que ejecutan Windows Holographic for Business, como Microsoft HoloLens. Con Intune, puede confirmar que los dispositivos cumplen con las reglas de su organización, y puede personalizar el dispositivo mediante la adición de un perfil de VPN o Wi-Fi. Otra característica importante es el uso del dispositivo como un quiosco, y ejecutar una aplicación específica o un conjunto determinado de aplicaciones.

Las tareas de este artículo le ayudan a administrar, personalizar y proteger los dispositivos que ejecutan Windows Holographic for Business, incluidas las actualizaciones de software y el uso de Windows Hello para empresas.

Para usar los dispositivos de Windows Holographic con Intune, cree un perfil de Actualización de edición. Este perfil de actualización actualiza los dispositivos de Windows Holographic a Windows Holographic for Business. Para Microsoft HoloLens, puede comprar Commercial Suite para obtener la licencia necesaria para la actualización. Para obtener más información, consulte Upgrade devices running Windows Holographic to Windows Holographic for Business (Actualizar dispositivos que ejecutan Windows Holographic a Windows Holographic for Business).

Azure Active Directory

Azure Active Directory (AD) es un excelente recurso para ayudar a administrar y controlar los dispositivos que ejecutan Windows Holographic for Business. Con Intune y Azure AD, puede:

- **Combinar dispositivos en Azure Active Directory** : en Azure Active Directory (AD), puede agregar los dispositivos de Windows 10 de trabajo, incluidos aquellos que ejecutan Windows Holographic for Business. Esta característica permite a Azure AD controlar el dispositivo. Ayuda a confirmar que los usuarios acceden a los recursos de la empresa desde dispositivos que cumplen los estándares de seguridad y cumplimiento.

  Administración de dispositivos en Azure AD proporciona más detalles.

- **Inscripción masiva para dispositivos Windows** : puede unir una gran cantidad de dispositivos Windows nuevos a Azure Active Directory (AD) e Intune. Esta característica se denomina inscripción masiva y usa paquetes de aprovisionamiento. Estos paquetes unen los dispositivos que ejecutan Windows Holographic for Business al inquilino de Azure AD y los inscriben en Intune.

Portal de empresa

Configurar la aplicación Portal de empresa

Intune incluye la aplicación Portal de empresa para que los usuarios accedan a los datos de la empresa, inscriban dispositivos, instalen aplicaciones, se pongan en contacto con el departamento de TI y mucho más. Puede personalizar la aplicación Portal de empresa para los dispositivos con Windows Holographic for Business.

En la aplicación Portal de empresa, también puede realizar las acciones siguientes:

- Quitar un dispositivo de Intune mediante la aplicación Configuración o la aplicación Portal de empresa

- Cambiar el nombre de un dispositivo
- Instalar aplicaciones en un dispositivo
- Sincronizar dispositivos manualmente desde la aplicación Configuración o la aplicación Portal de empresa

Directiva de cumplimiento

Crear una directiva de cumplimiento de dispositivos

Las directivas de cumplimiento son las reglas y la configuración que deben cumplir los dispositivos para ser conformes. Use estas directivas con el acceso condicional para bloquear el acceso a los recursos de la empresa a los dispositivos no conformes. En Intune, se crean directivas de cumplimiento para permitir o bloquear el acceso a dispositivos que ejecutan Windows Holographic for Business. Por ejemplo, se puede crear una directiva que exija la habilitación de BitLocker.

Vea también **Introducción a las directivas de cumplimiento de dispositivos de Microsoft Intune** .

Implementación y administración de aplicaciones

Agregar aplicaciones a Intune

Con Intune, puede agregar aplicaciones a los dispositivos con Windows Holographic for Business. Hay muchas maneras de implementar aplicaciones, por ejemplo:

- Agregar aplicaciones de Microsoft Store
- Agregar aplicaciones que cree
- Asignar aplicaciones a grupos

Microsoft Intune puede implementar aplicaciones universales de Windows en dispositivos con Microsoft HoloLens que ejecutan Windows Holographic for Business. Puede cargar directamente los paquetes de aplicaciones en Intune en Azure Portal, o bien implementarlos desde Microsoft Store para Empresas. Para obtener más información sobre las áreas relacionadas, vea los artículos siguientes:

- Para implementar aplicaciones de línea de negocio (LOB) mediante Azure Portal de Intune, consulte Adición de aplicaciones de línea de negocio (LOB) de Windows a Microsoft Intune.

  > **NOTE**
  > Intune permite a un tamaño de paquete máximo de 8 GB. Este tamaño de paquete solo está disponible para las aplicaciones LOB cargadas en Intune.

- Para implementar aplicaciones con Microsoft Store para Empresas, consulte Cómo administrar las aplicaciones adquiridas a través de la Microsoft Store para Empresas con Microsoft Intune.
- Para obtener información sobre la administración de aplicaciones con Microsoft Intune, consulte ¿Qué es la administración de aplicaciones de Microsoft Intune?.
- Para más información sobre el desarrollo de aplicaciones para Microsoft HoloLens, consulte Mixed reality apps for Microsoft HoloLens (Aplicaciones de realidad mixta para Microsoft HoloLens).

> **NOTE**
> Los dispositivos HoloLens que ejecutan Windows 10 Holographic for Business 1607 no son compatibles con las aplicaciones con licencia en línea de Microsoft Store para Empresas. Para más información, consulte Instalación de aplicaciones en HoloLens.

Acciones de dispositivo

Intune tiene algunas acciones integradas que permiten a los administradores de TI realizar diferentes tareas, en local en el dispositivo o de forma remota con Intune en Azure Portal. Los usuarios también pueden emitir un comando remoto desde el Portal de empresa de Intune para los dispositivos de propiedad privada que están inscritos en Intune.

Cuando se usan dispositivos que ejecutan Windows Holographic for Business, se pueden emplear las siguientes acciones:

- Borrar : la acción **Borrar** quita el dispositivo de Intune y lo restaura a la configuración predeterminada de fábrica. Use esta acción antes de entregar el dispositivo a un nuevo usuario o si se pierde o es robado.
- Retirar : la acción **Retirar** quita el dispositivo de Intune. También quita los datos de las aplicaciones administradas, la configuración y los perfiles de correo electrónico asignados por Intune. Los datos personales del usuario permanecen en el dispositivo.
- Sincronización de dispositivos para obtener las directivas y las acciones más recientes : la acción **Sincronizar** fuerza al dispositivo a registrarse inmediatamente en Intune. Cuando un dispositivo se registra, recibe de inmediato las acciones o las directivas pendientes que se le han asignado. Esta característica ayuda a validar y a solucionar problemas de directivas que se le han asignado, sin tener que esperar al siguiente registro programado.

¿Qué es la administración de dispositivos de Microsoft Intune? es un buen recurso para obtener información sobre la administración de dispositivos mediante Azure Portal.

Categorías de dispositivos y grupos

Clasificar dispositivos en grupos

Con Intune, puede crear categorías de dispositivos para agregar automáticamente los dispositivos a grupos en función de las categorías creadas, como Ventas, Contabilidad, Recursos humanos, etc. La idea es facilitar la administración de los dispositivos que ejecutan Windows Holographic for Business.

Perfiles de configuración de dispositivos

Introducción a los perfiles de configuración e Información general del perfil

Intune incluye opciones y características que se pueden habilitar o deshabilitar en distintos dispositivos dentro de la organización. Estos valores de configuración y características se administran mediante perfiles. Por ejemplo, puede crear un perfil que habilite Cortana o que use Microsoft Defender Smart Screen en los dispositivos con Windows Holographic for Business.

En los perfiles, puede usar OMA-URI para personalizar algunas opciones, crear restricciones de dispositivos y configurar una red privada virtual (VPN) y Wi-Fi.

Configuración de dispositivo personalizada

Para configurar las opciones de OMA-URI (Open Mobile Alliance Uniform Resource Identifier), puede crear un perfil personalizado en Intune. Use las opciones de OMA-URI para controlar diversas características de los dispositivos de Windows Holographic for Business, como habilitar una VPN o comprobar si hay actualizaciones en Microsoft Update.

Vea un ejemplo en el que se usa el CSP Control de aplicaciones de Windows Defender(WDAC) para permitir o impedir que las aplicaciones se abran en dispositivos HoloLens 2.

Configuración del modo de pantalla completa

Mediante las características de PC compartidas o de invitado disponibles en Intune, puede configurar los

dispositivos Windows Holographic for Business para que se ejecuten como un quiosco. Estos dispositivos pueden ejecutar una aplicación (modo de pantalla completa con una sola aplicación) o varias (modo de pantalla completa con varias aplicaciones).

Restricciones de dispositivos

Las restricciones de dispositivos permiten controlar distintas opciones y características de los dispositivos, como la exigencia de una contraseña, la instalación de aplicaciones desde Microsoft Store, la habilitación de Bluetooth, etc. Estas restricciones se crean en un perfil de Intune. Este perfil se puede aplicar a varios dispositivos con Windows Holographic for Business.

Configurar VPN

Las redes privadas virtuales (VPN) ofrecen a los usuarios un acceso remoto seguro a la red de la empresa. En Intune, puede crear un perfil de VPN que incluya opciones concretas para los dispositivos que ejecutan Windows Holographic for Business. Por ejemplo, puede crear un perfil de VPN para que todos los dispositivos de Windows Holographic for Business usen Citrix VPN como tipo de conexión.

Configurar Wi-Fi

Además, puede crear un perfil de Wi-Fi en Intune para asignar la configuración de red inalámbrica a los dispositivos de Windows Holographic for Business. Cuando se asigna un perfil de Wi-Fi, los usuarios finales obtienen acceso de red corporativo sin ninguna configuración de red. Por ejemplo, puede crear una red Wi-Fi dedicada exclusivamente a los dispositivos de Windows Holographic for Business.

Dispositivos multiusuario compartidos

Dispositivos compartidos

Los dispositivos que ejecutan Windows Holographic for Business, como Microsoft HoloLens, pueden tener varios usuarios. Intune incluye opciones de configuración para controlar distintas características en dichos dispositivos compartidos, como la administración de la energía, el uso del almacenamiento local y la administración de cuentas. Los perfiles de configuración también se pueden aplicar a dispositivos con distintos sistemas operativos. Por ejemplo, el grupo de dispositivos puede incluir dispositivos con RS2 y RS3 al mismo tiempo.

Actualizaciones de software

Administrar actualizaciones de software

Intune incluye una característica denominada anillos de actualización para dispositivos de Windows 10. Estos anillos de actualización incluyen un grupo de opciones que determinan cómo se instalan las actualizaciones. Por ejemplo, puede crear una ventana de mantenimiento para instalar actualizaciones u optar por reiniciar después de instalar las actualizaciones. Un anillo de actualización se puede aplicar a varios dispositivos con Windows Holographic for Business.

términos y condiciones

Establecer los términos y condiciones de la empresa para el acceso de los usuarios

Antes de que los usuarios inscriban dispositivos y accedan a las aplicaciones de la empresa, incluido el correo electrónico, puede exigirles que acepten los términos y condiciones de la empresa. En Intune, se define cómo se muestran en el Portal de empresa los términos y condiciones, además de asignarlos a los dispositivos que ejecutan Windows Holographic for Business.

Windows Hello para empresas

Usar Windows Hello para empresas

Hello para empresas es un método alternativo de inicio de sesión que emplea una cuenta de Azure Active Directory para reemplazar a una contraseña, una tarjeta inteligente o una tarjeta inteligente virtual. Con Hello para empresas, los dispositivos de Windows Holographic for Business pueden iniciar sesión con un PIN con una longitud mínima establecida por el usuario.

Pasos siguientes

Configurar Intune.

Implementación o traslado a Microsoft Intune

14/05/2021 • 2 minutes to read

Una adopción o migración correcta a Microsoft Intune comienza con un plan. Este plan depende de su entorno actual de administración de dispositivos móviles (MDM), los objetivos empresariales y los requisitos técnicos. Además, debe incluir las principales partes interesadas que apoyen el plan y colaboren con él.

Hemos creado algunas guías de planeamiento e implementación para ayudarle a planear su adopción o traslado a Intune.

> **TIP**
> Esta guía está en constante evolución. Así pues, no dude en agregar o actualizar las sugerencias e instrucciones existentes que le hayan parecido útiles.

Antes de empezar

- La implementación de Intune puede ser diferente de la implementación de MDM anterior. Intune usa el control de acceso controlado por identidades. No requiere un proxy de red para acceder a los datos de la organización desde dispositivos fuera de la red.

  Revise las formas más habituales de usar Intune.

- En estas guías se supone que ya ha evaluado Intune en un entorno de prueba de concepto (PoC) y ha decidido usarlo como la solución MDM de su organización. Está familiarizado con Intune y sus características.

Guías de planeamiento e implementación

- **Guía de planeamiento** : En esta guía se incluyen recomendaciones, sugerencias e instrucciones sobre las distintas tareas asociadas a las soluciones de MDM. Por ejemplo, obtenga orientación sobre:
  - Objetivos comunes
  - Administración de dispositivos personales y equipos de escritorio
  - Costos y licencias
  - Directivas y estructuras de grupo existentes
  - Creación de un plan de lanzamiento
  - Comunicación de cambios con los usuarios

    - Asistencia del departamento de soporte técnico
- **Guías y planes de implementación** : en estas guías se tratan varias áreas:
    - Configuración de Intune e impulso de la adopción de usuarios finales con acceso condicional: consulte las opciones para pasar a Intune o adoptar Intune. Obtenga más información sobre las ventajas de usar el acceso condicional y vea una lista de tareas.
    - Inscribir dispositivos: use estas guías para determinar el mejor método de inscripción para los dispositivos. Obtenga información general sobre las tareas de administración y las tareas de usuario final. En las guías de inscripción de implementación se tratan las siguientes áreas:
        - Administración de aplicaciones móviles sin necesidad de inscripción (MAM-WE)
        - Android
        - iOS/iPadOS
        - macOS
        - Windows
    - Administración de dispositivos y aplicaciones: implemente un conjunto básico de directivas de configuración de dispositivos y cumplimiento para usuarios y dispositivos. También puede implementar un conjunto específico de aplicaciones que se usan en su organización.
    - Protección de aplicaciones: en el caso de las aplicaciones de línea de negocio que necesitan un nivel de protección adicional, puede usar directivas de protección de aplicaciones.
- **Preparación de los usuarios** : obtenga orientación sobre la comunicación con los usuarios sobre mensajes de la aplicación Portal de empresa, la obtención de aplicaciones y la información que Apple y Google envían a Intune.

Pasos siguientes

Comience a planear la adopción de Intune mediante la guía de planeamiento.

Busque la configuración de Intune adecuada para su organización.

Guía de planeamiento de Microsoft Intune

17/05/2021 • 33 minutes to read

Una implementación o migración correcta de Microsoft Intune comienza con el planeamiento. Esta guía le orientará por los objetivos habituales de la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Además, contiene instrucciones sobre el inventario de los dispositivos, las licencias, la revisión de las directivas y la infraestructura actuales, la creación de un plan de lanzamiento y mucho más.

> **TIP**
>
> El kit de adopción de Intune incluye plantillas de correo electrónico y otra información útil.
>
> Esta guía está en constante evolución. Así pues, no dude en agregar o actualizar las sugerencias e instrucciones existentes que le hayan parecido útiles.

Tarea 1: determinación de los objetivos

Las organizaciones usan la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM) para controlar los datos de la organización de forma segura y con interrupciones mínimas para los usuarios. Al evaluar una solución de MDM o MAM, como Microsoft Intune, debe examinar cuál es el objetivo y qué quiere lograr.

En esta sección, se describen los objetivos comunes al usar Intune.

Objetivo: acceso al correo electrónico y las aplicaciones de la organización

Los usuarios esperan trabajar en dispositivos con aplicaciones de la organización, lo que incluye tareas como leer y responder correos electrónicos, actualizar y compartir datos, etc. En Intune, puede implementar diferentes tipos de aplicaciones, entre las que se incluyen las siguientes:

- Aplicaciones de Office 365
- Aplicaciones Win32
- Aplicaciones de línea de negocio (LOB)
- Aplicaciones personalizadas
- Habilitación (o bloqueo) del acceso a aplicaciones integradas o aplicaciones de la tienda

Tarea: haga una lista de las aplicaciones que los usuarios usan con regularidad. Estas aplicaciones son las que deben estar incluidas en sus dispositivos. Algunas consideraciones que hay que tener en cuenta:

- Muchas organizaciones implementan en equipos y tabletas el conjunto de aplicaciones de Office, como Word, Excel, OneNote, PowerPoint y Teams. En dispositivos más pequeños, como teléfonos móviles, se pueden instalar aplicaciones individuales, en función de los requisitos del usuario.

  Por ejemplo, el equipo de ventas podría necesitar Teams, Excel y SharePoint. En dispositivos móviles, solo se pueden implementar estas aplicaciones, en lugar de todo el conjunto de aplicaciones de Office.

- Los usuarios esperan poder leer y responder correos electrónicos y unirse a reuniones en todos los dispositivos, incluidos los personales. En los dispositivos propiedad de la organización, puede implementar Outlook y Teams. Además, puede administrar y controlar todas las opciones de configuración de los dispositivos y las aplicaciones, incluidos los requisitos de PIN y contraseña. En los dispositivos personales, no tiene este control. Por lo tanto, decida si quiere proporcionar a los usuarios acceso a las aplicaciones de la organización, como el correo electrónico y las reuniones.

Para conocer más detalles y consideraciones, consulte Dispositivos personales frente a dispositivos propiedad de la organización (en este artículo).

Objetivo: acceso seguro en todos los dispositivos

Los datos que se almacenan en los dispositivos móviles deben estar protegidos contra actividades malintencionadas.

Tarea: determine cómo quiere proteger los dispositivos y minimice el impacto de la actividades malintencionadas. Algunas consideraciones que hay que tener en cuenta:

- Es imprescindible contar con antivirus y protección contra el malware. Intune se integra con distintos asociados de Mobile Threat Defense (MTD) (Defensa contra amenazas móviles) para ayudar a proteger los dispositivos inscritos, los dispositivos personales y las aplicaciones. En los dispositivos Windows 10, puede usar Microsoft Defender para punto de conexión e Intune de manera conjunta.

  Microsoft Defender para punto de conexión incluye características de seguridad y un portal para supervisar las amenazas y reaccionar ante ellas.

- Si un dispositivo está en peligro, le interesará limitar el impacto mediante el acceso condicional. Por ejemplo:

  - Si un dispositivo cumple el nivel de amenaza que ha establecido, puede bloquear el acceso a los recursos de la organización. El acceso condicional le ayuda a impedir la propagación de actividades malintencionadas.

  - El acceso condicional contribuye a proteger la red y los recursos frente a los dispositivos, incluso los que no están inscritos en Intune.

    Por ejemplo, Intune se integra con Microsoft Defender para punto de conexión. Microsoft Defender para punto de conexión examina un dispositivo y determina si está en peligro. Después, el acceso condicional puede bloquear automáticamente el acceso a este dispositivo desde los recursos de la organización, incluido el correo electrónico.

- Las actualizaciones del dispositivo, el sistema operativo y las aplicaciones también ayudan a proteger los datos. Cree un plan en el que defina cómo y cuándo se instalan las actualizaciones. En Intune hay directivas que ayudan a administrar las actualizaciones, incluidas actualizaciones para aplicaciones de la tienda.

- Determine cómo se autenticarán los usuarios con los recursos de la organización desde sus diversos dispositivos. Por ejemplo, puede:

  - Use certificados en los dispositivos para autenticar características y aplicaciones, incluidas las que se conectan a una red privada virtual (VPN) y las que abren Outlook, entre otras. Estos certificados permiten una experiencia de usuario sin contraseña. El acceso sin contraseña se considera más seguro que pedirles a los usuarios que escriban su nombre de usuario y contraseña de la organización.

    Si está planeando usar certificados, asegúrese de que tiene una infraestructura de clave pública (PKI) admitida y lista para crear e implementar perfiles de certificado.

  - Use la autenticación multifactor (MFA) cuando necesite una capa adicional de autenticación en dispositivos propiedad de la organización. También puede emplear MFA para autenticar aplicaciones en dispositivos personales. Otra opción es usar datos biométricos, como el reconocimiento facial y las huellas digitales.

    Si va a usar biometría para la autenticación, asegúrese de que los dispositivos la admiten. La mayoría de los dispositivos modernos son compatibles con esta opción.

- Implemente una implementación de confianza cero. Con la confianza cero, se usan las características de Azure AD y Microsoft Intune para proteger todos los extremos, se usa la autenticación sin contraseña, etc. Para obtener más información, consulte Centro de implementación de confianza cero.

Objetivo: distribución de TI

Muchas organizaciones quieren conceder a distintos administradores el control de las ubicaciones, las divisiones, etc. Por ejemplo, el grupo **Administradores de TI de Charlotte** controla y supervisa las directivas del campus de Charlotte. Los administradores de TI de Charlotte solo pueden ver y administrar las directivas de esta ubicación. No pueden ver ni administrar directivas de la ubicación de Redmond. Este enfoque se denomina TI distribuida.

En Intune, la TI distribuida usa etiquetas de ámbito y categorías de inscripción de dispositivos. Las etiquetas de ámbito usan el control de acceso basado en roles (RBAC). Por lo tanto, solo los usuarios de un grupo específico tienen permiso para administrar las directivas y los perfiles de los usuarios y los dispositivos del ámbito.

Al usar categorías de dispositivos, estos se agregan automáticamente a grupos en función de las categorías que cree. Cuando los usuarios inscriben su dispositivo, eligen una categoría, como ventas, administrador de TI, dispositivo de punto de venta, etc. Estos grupos de dispositivos ya están listos para recibir los perfiles y las directivas que cree.

Para facilitar la administración de los dispositivos, puede usar las categorías de dispositivos de Intune para agregar automáticamente dispositivos a grupos en función de las categorías que defina.

Tarea: determine cómo quiere distribuir las reglas y los valores de configuración (directivas y perfiles). Algunas consideraciones que hay que tener en cuenta:

- Determine la estructura de administración. Por ejemplo, puede que le interese separar por ubicación, como **Administradores de TI de Charlotte** o **Administradores de TI de Redmond**. Es posible que prefiera separar por rol, por ejemplo, **Administradores de red** que controlan todo el acceso a la red, incluida la VPN.

  Estas categorías se convertirán en las etiquetas de ámbito.

- Muchas organizaciones separan grupos por tipo de dispositivo, como iOS, iPadOS, Android o Windows. He aquí algunos ejemplos:

  - Distribución de aplicaciones específicas en dispositivos específicos. Por ejemplo, puede implementar la aplicación de lanzadera de Microsoft en los dispositivos de la red de Redmond.
  - Implementación de directivas en ubicaciones específicas. Por ejemplo, puede implementar un perfil de VPN en los dispositivos de la red de Charlotte para que se conecten automáticamente cuando estén dentro del alcance.
  - Control de la configuración de dispositivos específicos. Por ejemplo, puede deshabilitar la cámara de los dispositivos Android Enterprise que se usan en una planta de fabricación, crear un perfil de antivirus de Windows Defender para todos los dispositivos Windows o agregar la configuración de correo electrónico de Exchange a todos los dispositivos iOS/iPadOS.

  Estas categorías se convertirán en las categorías de inscripción de dispositivos.

Objetivo: mantenimiento de los datos de la organización dentro de esta

Los datos que se almacenan en los dispositivos móviles deben estar protegidos contra la pérdida accidental o el uso compartido. Este objetivo incluye la eliminación de datos de la organización que están almacenados en dispositivos personales y de la organización.

Tarea: cree un plan para cubrir varios escenarios que afecten a la organización. Algunas consideraciones que hay que tener en cuenta:

- Se produce la pérdida o el robo de un dispositivo, o bien deja de usarse. Un usuario deja la organización.
    - En Intune, puede quitar dispositivos mediante el borrado, la retirada o la anulación manual de la inscripción. También puede quitar automáticamente los dispositivos que no se han protegido durante *x* días.
    - En el nivel de la aplicación, puede quitar los datos de la organización de las aplicaciones administradas por Intune. La eliminación selectiva es ideal para los dispositivos personales, ya que conserva los datos personales en el dispositivo y solo quita los datos de la organización.
- En los dispositivos personales, puede que le interese impedir que los usuarios realicen acciones de copiar y pegar, tomen capturas de pantalla o reenvíen correos electrónicos. Las directivas de protección de aplicaciones pueden bloquear estas características en los dispositivos que no administra usted. Para obtener más información, consulte Evitar fugas de datos en dispositivos no administrados con Intune.

  En los dispositivos administrados (inscritos en Intune), también puede controlar estas características mediante el uso de perfiles de configuración de dispositivos. Los perfiles de configuración de dispositivos controlan la configuración del dispositivo, no de la aplicación. En los dispositivos que acceden a datos altamente confidenciales, los perfiles de configuración de dispositivos pueden impedir realizar acciones de copiar y pegar, tomar capturas de pantalla, etc.
- En las aplicaciones de Office, impida el acceso no autorizado a los datos de la organización mediante Azure Information Protection. Esta característica usa etiquetas para clasificar los archivos, como los datos confidenciales.

Para conocer más detalles y consideraciones, consulte Dispositivos personales frente a dispositivos propiedad de la organización (en este artículo).

Tarea 2: inventario de los dispositivos

Las organizaciones tienen una gran variedad de dispositivos, como equipos de escritorio, portátiles, tabletas y teléfonos móviles. Estos dispositivos pueden ser propiedad de la organización o de los usuarios. Al planear la solución de administración de dispositivos, asegúrese de tener en cuenta todo lo que accederá a los recursos de la organización, incluidos los dispositivos personales de los usuarios.

En esta sección se incluye información relacionada con los dispositivos que debe tener en cuenta.

Plataformas compatibles

Intune es compatible con el administrador de dispositivos Android, Android Enterprise y dispositivos iOS, iPadOS, macOS y Windows. Para ver las versiones específicas, consulte las plataformas compatibles.

Tarea: si los dispositivos usan versiones no compatibles (generalmente, sistemas operativos más antiguos), ha llegado el momento de actualizar el sistema operativo o reemplazar los dispositivos. Estos dispositivos y sistemas operativos antiguos pueden tener una compatibilidad limitada y suponen un riesgo de seguridad potencial. En esta tarea se incluyen los equipos de escritorio que ejecutan Windows 7, los dispositivos iPhone 7 que ejecutan el sistema operativo original de la versión 10.0, etc.

Dispositivos personales frente a dispositivos propiedad de la organización

En los dispositivos personales, es normal que los usuarios consulten el correo electrónico, se unan a reuniones de Teams y actualicen archivos de SharePoint, entre otras cosas. Muchas organizaciones admiten los dispositivos personales, mientras que muchas otras solo permiten los que son propiedad de la organización.

Como organización y como administrador, usted decide si permitirá los dispositivos personales.

Tarea: determine cómo quiere controlar los dispositivos personales. Si la movilidad es importante para su organización, tenga en cuenta los enfoques siguientes:

- En los dispositivos personales, ofrezca a los usuarios la opción de inscribirse en Intune. Una vez que se

hayan inscrito, los administradores administrarán totalmente estos dispositivos, incluidas las directivas de inserción, el control de la configuración y las características de los dispositivos, e incluso la eliminación de los dispositivos. Como administrador, es posible que le interese tener este control, o tal vez *crea* que le interesa.

Cuando los usuarios inscriben sus dispositivos personales, probablemente no sepan o no entiendan que los administradores pueden hacer de todo en el dispositivo, incluido borrarlo o restablecerlo de manera accidental. Como administrador, puede que no le interese asumir esta responsabilidad o el impacto que podría tener en los dispositivos que no son propiedad de su organización.

Además, muchos usuarios se niegan a inscribirse y buscan otras maneras de acceder a los recursos de la organización. Por ejemplo, necesita que los dispositivos estén inscritos para usar la aplicación de Outlook y consultar el correo electrónico de la organización. Para omitir este requisito, los usuarios abren cualquier explorador web en el dispositivo e inician sesión en Outlook Web Access, lo que probablemente no sea el resultado esperado. También podrían realizar capturas de pantalla y guardar las imágenes en el dispositivo, algo que tal vez no le interese.

- En los dispositivos personales, use directivas de configuración de aplicaciones y directivas de protección de aplicaciones. Los usuarios no se inscriben en Intune y usted no administra estos dispositivos.

  Use una declaración de Términos y condiciones con una directiva de acceso condicional. Si los usuarios no la aceptan, no tendrán acceso a las aplicaciones. Si la aceptan, se agrega un registro de dispositivo en Azure AD y el dispositivo se convierte en una entidad conocida. Si el dispositivo es conocido, puede llevar un seguimiento de a qué recursos se accede desde el dispositivo.

  Después, controle el acceso y la seguridad mediante directivas de aplicación.

  Determine qué tareas usa más la organización, como el correo electrónico y la participación en reuniones. Use directivas de configuración de aplicaciones para configurar las opciones específicas de la aplicación. Use directivas de protección de aplicaciones para controlar la seguridad y el acceso a estas aplicaciones.

  Por ejemplo, los usuarios pueden usar la aplicación de Outlook en su dispositivo personal para consultar el correo electrónico del trabajo. Con Intune, los administradores crean una directiva de protección de aplicaciones de Outlook que usa la autenticación multifactor (MFA) cada vez que se abre la aplicación de Outlook, impide realizar acciones de copiar y pegar, etc.

- Quiere que todos los dispositivos estén totalmente administrados. En este escenario, proporcione a los usuarios todos los dispositivos que necesiten, incluidos teléfonos móviles. Invierta en un plan de actualización de hardware para que los usuarios sigan siendo productivos y eficaces. Inscriba en Intune estos dispositivos propiedad de la organización y adminístrelos mediante directivas.

  Esta opción impide el uso de dispositivos personales.

Se recomienda que siempre dé por supuesto que habrá datos que salgan del dispositivo. Asegúrese de contar con métodos de seguimiento y auditoría. Para obtener más información, consulte Centro de implementación de confianza cero.

Administración de equipos de escritorio

Intune puede administrar equipos de escritorio que ejecutan Windows 10 y versiones más recientes. El sistema operativo Windows 10 incluye características de administración de dispositivos modernas y quita las dependencias de la directiva de grupo de Active Directory (AD) local. Para disfrutar de las ventajas de la nube, cree reglas y configuraciones en Intune e implemente estas directivas en todos los dispositivos Windows 10, incluidos equipos de escritorio.

Para obtener más información, consulte Escenario guiado: escritorio moderno administrado en la nube.

Si los dispositivos Windows 10 se administran actualmente mediante Configuration Manager, puede inscribirlos igualmente en Intune. Este enfoque se conoce como "administración conjunta". La administración conjunta ofrece muchas ventajas, como la ejecución de acciones remotas en el dispositivo (reinicio, control remoto, restablecimiento de la configuración de fábrica), el acceso condicional con cumplimiento de dispositivos y mucho más. También puede asociar a la nube los dispositivos en Intune.

Para obtener más información, consulte ¿Qué es la administración conjunta?, Rutas hacia la administración conjunta y Asociación de inquilinos de Endpoint Manager.

Tarea: examine qué usa actualmente para la administración de dispositivos móviles y cuáles son los objetivos y determine la mejor ruta. Algunas consideraciones que hay que tener en cuenta:

- Si actualmente no usa nada, puede que lo mejor sea usar Intune directamente.
- En el caso de los dispositivos nuevos que no están inscritos en Configuration Manager, o en el caso de cualquier solución MDM, puede que lo mejor sea usar Intune directamente.
- Si actualmente usa Configuration Manager, dispone de las opciones siguientes:
  - Si quiere conservar la infraestructura existente y trasladar algunas cargas de trabajo a la nube, use la administración conjunta. Obtendrá las ventajas de ambos servicios. Los dispositivos existentes pueden recibir algunas directivas de Configuration Manager (local) y otras directivas de Intune (nube).
  - Si quiere conservar la infraestructura existente y usar Intune para ayudar a supervisar los dispositivos locales, use la asociación de inquilinos. Obtendrá las ventajas de usar el centro de administración de Endpoint Manager, pero seguirá usando Configuration Manager para administrar los dispositivos.
  - Si quiere una solución en la nube pura para administrar los dispositivos, trasládese a Intune. Este escenario no es habitual. Por lo general, los usuarios de Configuration Manager prefieren seguir usándolo. La guía de implementación de configuración contiene información útil.

  Para obtener más información, vea Administración conjunta de cargas de trabajo.

Tarea 3: determinación de los costos y las licencias

La administración de dispositivos consiste en una relación con diversos servicios. Intune incluye opciones de configuración y características que puede controlar en distintos dispositivos. También hay otros servicios que desempeñan un papel fundamental:

- **Azure Active Directory (AD) Premium** incluye varias características clave para la administración de dispositivos, entre las que se incluyen las siguientes:
  - Windows Autopilot: los dispositivos Windows 10 pueden inscribirse automáticamente en Intune y recibir las directivas también automáticamente.
  - Autenticación multifactor (MFA): los usuarios deben especificar dos o más métodos de verificación, como un PIN, una aplicación autenticadora, una huella digital, etc. MFA es una opción excelente al usar directivas de protección de aplicaciones para dispositivos personales o dispositivos propiedad de la organización que requieren seguridad adicional.
  - Acceso condicional: si los usuarios y los dispositivos cumplen las reglas, como proporcionar un código de acceso de seis dígitos, obtienen acceso a los recursos de la organización. En caso de que no las cumplan, no podrán acceder.
  - Grupos de usuarios dinámicos y grupos de dispositivos dinámicos: agregue usuarios o dispositivos automáticamente a grupos cuando cumplan ciertos criterios, por ejemplo, ciudad, puesto de trabajo, tipo de sistema operativo, versión del sistema operativo, etc.
- **Office 365** incluye aplicaciones de las que dependen los usuarios, como Outlook, Word, SharePoint, Teams, OneDrive, etc. Puede implementar estas aplicaciones en los dispositivos mediante Intune.
- **Microsoft Defender para punto de conexión** ayuda a supervisar y examinar dispositivos

Windows 10 para detectar actividades malintencionadas. También puede establecer un nivel de amenaza aceptable. Si lo combina con el acceso condicional, puede bloquear el acceso a los recursos de la organización cuando se supera el nivel de amenaza.

- **Azure Information Protection** clasifica y protege documentos y mensajes de correo electrónico mediante la aplicación de etiquetas. En las aplicaciones de Office, puede usar este servicio para impedir el acceso no autorizado a los datos de la organización, incluidas aplicaciones en dispositivos personales.

Todos estos servicios se incluyen en la licencia **Microsoft 365 E5**. Para obtener más información, consulte los planes de licencias de Microsoft 365.

Tarea: determine qué servicios y programas se necesitan y se usan en la organización para garantizar la productividad y la seguridad. Algunas consideraciones que hay que tener en cuenta:

- Si su objetivo es implementar directivas (reglas) y perfiles (configuración) sin ningún tipo de cumplimiento, necesita como mínimo Intune. Intune está disponible con distintas suscripciones, e incluso como servicio independiente. Para obtener más información, consulte Licencias de Microsoft Intune.

  Actualmente usa Configuration Manager y quiere configurar la administración conjunta de sus dispositivos. Intune ya está incluido en la licencia de Configuration Manager. Si le interesa que Intune administre por completo los dispositivos nuevos o administrados conjuntamente, necesitará una licencia de Intune independiente.

- Quiere aplicar las reglas de cumplimiento o de contraseña que cree en Intune. Como mínimo, necesita Intune y Azure AD Premium. Intune y Azure AD Premium están disponibles con **Enterprise Mobility + Security**.

  Para obtener más información, consulte Opciones de precios de Enterprise Mobility + Security.

- Solo quiere administrar aplicaciones de Office 365 en los dispositivos. Como mínimo, necesita Office 365. Para obtener más información, consulte MDM para Office 365 frente a Microsoft Intune y Preguntas más frecuentes sobre la administración de dispositivos móviles para Office 365.

- Quiere implementar aplicaciones de Office 365 en los dispositivos y crear directivas para ayudar a proteger los dispositivos que ejecutan estas aplicaciones. Como mínimo, necesita Intune y Office 365.

- Quiere crear directivas en Intune, implementar aplicaciones de Office 365 y aplicar sus propias reglas y opciones de configuración. Como mínimo, necesita Intune, Office 365 y Azure AD Premium. Dado que todos estos servicios se incluyen en Microsoft 365, puede ser más rentable usar la licencia de Microsoft 365.

  Para obtener más información, consulte los planes de licencias de Microsoft 365.

Tarea 4: revisión de las directivas e infraestructura existentes

Muchas organizaciones tienen una infraestructura de administración de dispositivos y directivas que simplemente se mantiene. Por ejemplo, podría tener directivas de grupo de 20 años de antigüedad, pero no saber lo que hacen. Al considerar la posibilidad de migrar a la nube, en lugar de centrarse en lo que ha hecho siempre, determine cuáles son sus objetivos.

Teniendo en cuenta estos objetivos, cree una línea base para las directivas. Si dispone de varias soluciones de administración de dispositivos, tal vez haya llegado el momento de empezar a usar una única solución de administración de dispositivos móviles.

Tarea: examine las tareas que se ejecutan de forma local y que podrían migrarse a la nube. Recuerde que, en lugar de centrarse en lo que ha hecho siempre, debe determinar cuáles son sus objetivos. Algunas consideraciones que hay que tener en cuenta:

- Revise las directivas existentes y su estructura. Algunas directivas pueden aplicarse de forma global, otras se aplican en el nivel de sitio y otras son específicas de un dispositivo. El objetivo consiste en conocer y comprender la intención de las directivas globales, de las directivas locales, etc.

  Las directivas de grupo de AD se aplican en este orden: local, sitio, dominio y unidad organizativa (UO). En esta jerarquía, las directivas de UO sobrescriben a las directivas locales, las de dominio sobrescriben a las de sitio, y así sucesivamente.

  En Intune, las directivas se aplican a los usuarios y a los grupos que se crean. No existe ninguna jerarquía. Si dos directivas actualizan el mismo valor, este se muestra como un conflicto. Para obtener más información, vea Preguntas comunes, problemas y su solución con perfiles y directivas de dispositivos.

  Al cambiar de una directiva de grupo de AD a Intune, las directivas globales de AD empezarán a aplicarse lógicamente a los grupos que tenga (o que necesite). Estos grupos incluirán los usuarios y los dispositivos que quiere que tengan como destino el nivel global, de sitio, etc. Esta tarea le permite hacerse una idea de la estructura de grupo que necesitará en Intune.

- Esté preparado para crear directivas y perfiles en Intune. Intune incluye varias características que cubren escenarios que podrían interesarle. He aquí algunos ejemplos:

  - **Líneas base de seguridad**: en los dispositivos Windows 10, las líneas base de seguridad son opciones de seguridad preconfiguradas para los valores recomendados. Si no está familiarizado con la protección de dispositivos, o si prefiere una línea base completa, consulte más información sobre las líneas base de seguridad.
  - **Plantillas administrativas**: en los dispositivos Windows 10, use plantillas ADMX para configurar opciones de directiva de grupo para Windows, Internet Explorer, Office y Microsoft Edge versión 77 y posteriores. Estas plantillas ADMX son las mismas que se usan en la directiva de grupo de AD, pero se basan al 100 % en la nube en Intune.
  - **Directiva de grupo**: use el análisis de directivas de grupo para importar y analizar los GPO. Esta característica ayuda a determinar cómo se traducen los GPO en la nube. La salida muestra qué valores se admiten en los proveedores de MDM, incluido Microsoft Intune. También se muestra cualquier configuración en desuso o la configuración que no está disponible para los proveedores de MDM.
  - **Escenarios guiados**: los escenarios guiados son una serie de pasos personalizada que se centra en casos de uso completos. Estos escenarios incluyen automáticamente directivas, aplicaciones, asignaciones y otras configuraciones de administración.
- Cree una línea base de directiva que incluya sus objetivos mínimos. Por ejemplo:

  - Correo electrónico seguro: como mínimo, probablemente le interesará lo siguiente:

    - Habilitar el acceso condicional para Exchange Online o mediante la conexión a una solución de correo electrónico local.
    - Crear directivas de protección de aplicaciones de Outlook.
  - Configuración del dispositivo: como mínimo, probablemente le interesará lo siguiente:

    - Requerir un PIN de seis caracteres para desbloquear el dispositivo.
    - Impedir las copias de seguridad en servicios personales en la nube, como iCloud o OneDrive.
  - Perfiles de dispositivo: como mínimo, probablemente le interesará lo siguiente:

    - Crear un perfil de Wi-Fi con la configuración predeterminada para conectarse a la red inalámbrica Contoso Wi-Fi.
    - Crear un perfil de VPN con un certificado para autenticarse automáticamente y conectarse a una VPN de la organización.
    - Crear un perfil de correo electrónico con la configuración predeterminada para conectarse a Office 365 o a una solución de correo electrónico de Gmail.

- Aplicaciones: como mínimo, probablemente le interesará lo siguiente:
  - Implementar Office 365 con directivas de protección de aplicaciones.
  - Implementar una línea de negocio (LOB) con directivas de protección de aplicaciones.
- Revise la estructura actual de los grupos. En Intune, puede crear y asignar directivas a grupos de usuarios, a grupos de dispositivos y a grupos de usuarios y dispositivos dinámicos (requiere Azure AD Premium).

  Al crear grupos en la nube, como Intune o Microsoft 365, se generan en Azure AD. No se ve la personalización de marca de Azure AD, pero es lo que está usando.

  - La creación de grupos es una tarea sencilla. Pueden crearse en el Centro de administración de Microsoft Endpoint Manager. Para obtener más información, consulte Agregar grupos para organizar usuarios y dispositivos.
  - El traslado de las listas de distribución existentes a Azure AD puede ser más complicado. Una vez que las listas de distribución se encuentran en Azure AD, Intune y Microsoft 365 ya pueden usar estos grupos. Para más información, consulte:
    - ¿Qué es la identidad híbrida con Azure Active Directory?
    - Sincronización de Azure AD Connect: comprender y personalizar la sincronización
  - Si ya tiene grupos de Office 365, puede pasar a usar Microsoft 365. Los grupos existentes se conservarán y podrá disfrutar de todos los servicios de características de Microsoft 365. Para más información, consulte:
    - ¿Qué es Microsoft 365?
    - Migración a Microsoft 365 Enterprise
    - Actualización a Microsoft 365 Empresa
- Si dispone de varias soluciones de administración de dispositivos, cambie a una única solución de administración de dispositivos móviles. Se recomienda usar Intune para ayudar a proteger los datos de la organización en aplicaciones y dispositivos.

Tarea 5: creación de un plan de lanzamiento

La siguiente tarea consiste en planear el modo y el momento en que los usuarios y los dispositivos recibirán las directivas. En esta tarea, tenga en cuenta también las siguientes consideraciones:

- Defina los objetivos y las métricas de éxito. Use estos puntos de datos para crear otras fases de lanzamiento. Asegurarse de que los objetivos sean específicos, mensurables, alcanzables, realistas y oportunos (SMART). Planee la medición en relación con los objetivos en cada fase para que el proyecto de lanzamiento se mantenga encarrilado.
- Tenga objetivos claramente definidos. Inclúyalos en todas las actividades de difusión y aprendizaje para que los usuarios entiendan por qué la organización ha elegido Intune.

Tarea: cree un plan para implementar las directivas y decida el modo en que los usuarios inscribirán sus dispositivos en Intune. Algunas consideraciones que hay que tener en cuenta:

- Implemente las directivas en fases. Por ejemplo:
  - Empiece con un grupo piloto o de prueba. Estos grupos deben saber que son los primeros usuarios y estar dispuestos a proporcionar comentarios. Use estos comentarios para mejorar la configuración, la documentación y las notificaciones y para facilitar el proceso a los usuarios en un lanzamiento futuro. Estos usuarios no deben ser ejecutivos ni personas VIP.

    Después de las pruebas iniciales, agregue más usuarios al grupo piloto. También puede crear más grupos piloto que se centren en un lanzamiento diferente, por ejemplo:

- **Departamentos**: Cada departamento puede ser una fase de lanzamiento. Puede centrarse en un departamento completo a la vez. En este lanzamiento, los usuarios de cada departamento podrían usar el dispositivo de la misma forma y acceder a las mismas aplicaciones. Los usuarios probablemente tendrán los mismos tipos de directivas.
- **Geografía**: implemente las directivas en todos los usuarios de una geografía determinada, ya sea el mismo continente, país, región o edificio de la organización. Este lanzamiento le permite centrarse en la ubicación específica de los usuarios. Podría proporcionar un entorno de Windows Autopilot para un enfoque de implementación previamente aprovisionado, ya que el número de ubicaciones que implementan Intune al mismo tiempo es menor. Es posible que existan departamentos o casos de uso diferentes en la misma ubicación. Por lo tanto, podría probar diferentes casos de uso al mismo tiempo.
- **Plataforma**: este lanzamiento implementa plataformas similares al mismo tiempo. Por ejemplo, podría implementar directivas en todos los dispositivos iOS/iPadOS en febrero, en todos los dispositivos Android en marzo y en todos los dispositivos Windows en abril. Este enfoque permitiría simplificar las solicitudes de ayuda al departamento de soporte técnico, ya que solo admiten una plataforma a la vez.

Con un enfoque por fases, puede recibir comentarios de tipos de usuarios muy diferentes.

- Tras una prueba piloto correcta, ya está listo para iniciar un lanzamiento de producción completo. El ejemplo siguiente consiste en un plan de lanzamiento de Intune que incluye grupos de destino y escalas de tiempo:

FASE DE IMPLEMENTACIÓN	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE
Piloto limitado	TI (50 usuarios)			
Piloto expandido	TI (200 usuarios), ejecutivos de TI (10 usuarios)			
Fase de implementación de producción 1		Ventas y marketing (2000 usuarios)		
Fase de implementación de producción 2			Venta al por menor (1000 usuarios)	
Fase de implementación de producción 3				Recursos humanos (50 usuarios), Finanzas (40 usuarios), Ejecutivos (30 usuarios)

Esta plantilla también está disponible para la descarga en Planeamiento, diseño e implementación de Intune: plantillas de tabla.

- Elija la manera en que los usuarios inscribirán los dispositivos personales y de la organización. Hay varios métodos de inscripción, entre los que se incluyen los siguientes:
  - **Autoservicio del usuario**: los usuarios inscriben sus propios dispositivos siguiendo los pasos que proporciona el departamento de TI de la organización. Este método es el que más se usa y es más escalable que la inscripción asistida por el usuario.

- **Inscripción asistida por el usuario**: con este método de implementación previamente aprovisionado, un miembro del departamento de TI guía a los usuarios por el proceso de inscripción, ya sea en persona o mediante Teams. Este método se usa normalmente con personal ejecutivo y otros grupos que pueden necesitar más ayuda.
- **Feria técnica de TI**: en este evento, el grupo de TI establece un área de asistencia de inscripción de Intune. Aquí, los usuarios reciben información sobre la inscripción de Intune, realizan preguntas y obtienen ayuda para inscribir los dispositivos. Esta opción resulta beneficiosa para los usuarios y el departamento de TI, sobre todo durante las primeras fases del lanzamiento de Intune.

En el ejemplo siguiente se incluyen los métodos de inscripción:

FASE DE IMPLEMENTACIÓN	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE
Piloto limitado				
Autoservicio	IT			
Piloto expandido				
Autoservicio	IT			
Previamente aprovisionado	Ejecutivos de TI			
Fase de implementación de producción 1		Ventas, Marketing		
Autoservicio		Ventas y marketing		
Fase de implementación de producción 2			Retail	
Autoservicio			Retail	
Fase de implementación de producción 3				Ejecutivos, recursos humanos, finanzas
Autoservicio				Recursos humanos, finanzas
Previamente aprovisionado				Ejecutivos

Tarea 6: comunicación de los cambios

La administración de los cambios se basa en comunicaciones claras y útiles sobre los cambios futuros. La idea consiste en facilitar la implementación de Intune, asegurarse de que los usuarios conozcan los cambios y evitar cualquier interrupción.

Tarea: el plan de comunicación de lanzamiento debe indicar qué información es importante, cómo se envían notificaciones a los usuarios y cuándo es necesario realizar comunicaciones. Algunas consideraciones que hay que tener en cuenta:

- Determine qué información se debe comunicar. Comuníquese en fases con los grupos y usuarios, comenzando con una puesta en marcha del lanzamiento de Intune, seguida de una inscripción previa y una posterior:
  - **Fase de puesta en marcha**: comunicación extensa en la que se presenta el proyecto de Intune. Debe aclarar cuestiones clave, como las siguientes:
    - ¿Qué es Intune?
    - ¿Por qué la organización usa Intune? (Deben incluirse las ventajas para la organización y los usuarios).
    - Proporcione un plan de alto nivel para la implementación y el lanzamiento.
    - Si no se permitirán dispositivos personales *a menos que* se inscriban, explique por qué ha tomado la decisión.
  - **Fase de inscripción previa**: comunicación extensa que incluye información sobre Intune y servicios adicionales (como Office, Outlook y OneDrive), recursos de usuario y plazos concretos en los que los usuarios y los grupos recibirán Intune.
  - **Fase de inscripción**: comunicación dirigida a los usuarios y los grupos de la organización que tienen previsto recibir Intune. Debe informar a los usuarios de que están listos para recibir Intune, así como incluir los pasos de inscripción y la persona de contacto para solicitar ayuda y solventar dudas.
  - **Fase de inscripción posterior**: comunicación dirigida a los usuarios y los grupos de la organización que se han inscrito en Intune. Debe proporcionar recursos adicionales que puedan resultar útiles al usuario y recopilar comentarios sobre su experiencia durante y después la inscripción.

  Es posible que el kit de adopción de Intune le resulte útil. Úselo tal como está o cámbielo para su organización.
- Elija cómo comunicar la información de lanzamiento de Intune a los usuarios y los grupos de destino. Por ejemplo:
  - Cree una reunión presencial de toda la organización o use Microsoft Teams.
  - Cree un correo electrónico para la inscripción previa, otro para la inscripción y otro para la inscripción posterior. Por ejemplo:
    - **Correo electrónico 1**: explique las ventajas, las expectativas y la programación. Aproveche la ocasión para mostrar otros servicios a los que se concede acceso en los dispositivos administrados por Intune.
    - **Correo electrónico 2**: anuncie que ahora hay servicios listos para su acceso a través de Intune. Indique a los usuarios que se inscriban ahora. proporcione a los usuarios una escala de tiempo antes de que su acceso se vea afectado. Recuerde a los usuarios las ventajas y las razones estratégicas para la migración.
  - Use un sitio web de la organización en el que se expliquen las fases de lanzamiento, lo que los usuarios pueden esperar y con quién deben ponerse en contacto para obtener ayuda.
  - Cree carteles, use las plataformas de redes sociales de la organización (como Yammer) o distribuya folletos para anunciar la fase de inscripción previa.
- Cree una escala de tiempo en la que se indiquen los plazos y las personas interesadas. Las primeras comunicaciones de puesta en marcha de Intune pueden dirigirse a toda la organización o solo a un subconjunto. Pueden prolongarse varias semanas antes de que comience el lanzamiento de Intune. Después de esto, la información puede comunicarse en fases a los usuarios y los grupos, y adaptarse a la programación de lanzamiento de Intune.

El ejemplo siguiente es un plan de comunicaciones de lanzamiento de Intune de alto nivel:

PLAN DE COMUNICACIÓN	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE
Fase 1	Todos			
Reunión de puesta en marcha	Primera semana			
Fase 2	TI	Ventas y marketing	Venta directa	Recursos humanos, finanzas y ejecutivos
Correo electrónico de implementación previa 1	Primera semana	Primera semana	Primera semana	Primera semana
Fase 3	TI	Ventas y marketing	Venta directa	Recursos humanos, finanzas y ejecutivos
Correo electrónico de implementación previa 2	Segunda semana	Segunda semana	Segunda semana	Segunda semana
Fase 4	TI	Ventas y marketing	Venta directa	Recursos humanos, finanzas y ejecutivos
Correo electrónico de inscripción	Tercera semana	Tercera semana	Tercera semana	Tercera semana
Fase 5	TI	Ventas y marketing	Venta directa	Recursos humanos, finanzas y ejecutivos
Correo electrónico de inscripción posterior	Cuarta semana	Cuarta semana	Cuarta semana	Cuarta semana

Tarea 7: Soporte técnico y usuarios finales

Incluya al departamento de soporte técnico de TI en las primeras fases de los esfuerzos piloto y el planeamiento de la implementación de Intune. La implicación temprana ayuda a los miembros del departamento a familiarizarse con Intune, lo que les permitirá obtener conocimientos y experiencia para identificar y resolver problemas de forma más eficaz. Además, los prepara para prestar asistencia durante todo el proceso de lanzamiento en producción dentro de la organización. Los equipos de soporte técnico y de asistencia experimentados son de gran ayuda para que los usuarios adopten estos cambios.

Tarea: incorporar cursos de aprendizaje para el personal de soporte técnico. Validar la experiencia del usuario final con métricas de éxito en el plan de implementación. Algunas consideraciones que hay que tener en cuenta:

- Determine quién prestará soporte técnico a los usuarios finales. Las organizaciones pueden tener diferentes niveles (de 1 a 3). Por ejemplo, los niveles 1 y 2 pueden formar parte del equipo de soporte técnico, mientras que el nivel 3 puede incluir miembros del equipo de MDM responsable de la implementación de Intune.

El nivel 1 suele ser el primer nivel de soporte técnico y el primero con el que los usuarios se ponen en contacto. Si el nivel 1 no es capaz de resolver el problema, lo deriva al nivel 2. El nivel 2 lo derivará al nivel 3 si es necesario. El Soporte técnico de Microsoft puede considerarse como el nivel 4.

  - En las fases iniciales de lanzamiento, asegúrese de que todos los niveles del equipo de soporte técnico documenten los problemas y las soluciones. Busque patrones y ajuste las comunicaciones para la siguiente fase de lanzamiento. Por ejemplo:
    - Si distintos usuarios o grupos tienen dudas sobre la inscripción de sus dispositivos personales, considere la posibilidad de realizar una llamada de Teams para responder a las preguntas más habituales.
    - Si los usuarios tienen los mismos problemas al inscribir dispositivos propiedad de la organización, organice un evento presencial para ayudar a los usuarios a inscribir los dispositivos.
- Cree un flujo de trabajo de asistencia y comunique constantemente los problemas de soporte técnico, las tendencias y otra información importante a todos los niveles del equipo de soporte técnico. Por ejemplo, puede celebrar reuniones diarias o semanales a través de Teams para que todos los niveles sean conscientes de las tendencias y los patrones y puedan obtener ayuda.

  En el ejemplo siguiente se muestra la manera en que Contoso implementa los flujos de trabajo de su departamento de soporte técnico de TI:

  1. El usuario final se pone en contacto con el nivel 1 del departamento de soporte técnico de TI con un problema de inscripción.
  2. El nivel 1 del departamento de soporte técnico de TI no puede determinar la causa principal y lo escala al nivel 2.
  3. El nivel 2 del departamento de soporte técnico de TI investiga el asunto. El nivel 2 no puede resolver el problema, de modo que lo deriva al nivel 3 y proporciona información adicional para ayudar.
  4. El nivel 3 del departamento de soporte técnico de TI investiga el problema, determina la causa principal y comunica la solución a los niveles 2 y 1.
  5. Después, el nivel 1 del departamento de soporte técnico de TI se pone en contacto con los usuarios y resuelve el problema.

  Este método, especialmente en las primeras fases del lanzamiento de Intune, aporta muchas ventajas, como las siguientes:

  - Ayuda en el aprendizaje tecnológico.
  - Identificación rápida de problemas y soluciones.
  - Mejora de la experiencia general del usuario.
- Entrene al departamento y a los equipos de soporte técnico. Pídales que inscriban dispositivos que ejecuten las diferentes plataformas que se usan en la organización (Android, iOS/iPadOS, macOS y Windows) para que se familiaricen con el proceso. Considere la posibilidad de usar los equipos de soporte técnico como grupo piloto para los escenarios.

  Hay recursos de aprendizaje disponibles, como vídeos de YouTube, tutoriales de Microsoft sobre la inscripción, el cumplimiento y la configuración, y cursos a través de asociados.

  A continuación se muestra un ejemplo de un programa de aprendizaje de soporte técnico de Intune:

  - Revisión de un plan de soporte técnico de Intune
  - Información general de Intune
  - Solucionar los problemas comunes
  - Herramientas y recursos
  - Q & A

La documentación sobre cómo presentar Intune a los usuarios finales, el foro de Intune basado en la comunidad y la documentación para el usuario final son también excelentes recursos.

Pasos siguientes

Cree directivas de dispositivo y de aplicación e inscriba los dispositivos.

Consulte el kit de adopción de Intune.

Guía de implementación: configuración o migración a Microsoft Intune

27/05/2021 • 17 minutes to read

En esta guía de implementación se incluye información sobre cómo migrar a Intune o cómo adoptar Intune como solución de MDM (administración de dispositivos móviles) y MAM (administración de aplicaciones móviles).

En esta guía se explica el proceso de registro en Intune, se agrega el nombre de dominio, se configura Intune como entidad de MDM, etc. Elija el enfoque de migración que sea más adecuado para las necesidades de su organización. Puede ajustar las tácticas de implementación en función de los requisitos de la organización.

> **TIP**
> Esta guía está en constante evolución. Así pues, no dude en agregar o actualizar las sugerencias e instrucciones existentes que le hayan parecido útiles.

Prerequisites

- **Suscripción a Intune**: Intune está disponible como un servicio de Azure independiente, como parte de Enterprise Mobility + Security (EMS) y, además, está incluido en Microsoft 365. Para obtener más información sobre cómo obtener Intune, vea Licencias de Intune.

  En la mayoría de los escenarios, Microsoft 365 puede ser la mejor opción, ya que proporciona EMS, Microsoft Endpoint Manager y Office 365.

  También puede suscribirse a una cuenta de evaluación gratuita.

- Inicie sesión como miembro del grupo de Azure AD **Administrador global**. Para implementar Intune, inicie sesión como miembro del grupo de Azure AD **Administrador global** o **Administrador del servicio Intune**.

Actualmente no se usa nada

Si actualmente no usa ningún proveedor de MDM o MAM, tiene algunas opciones:

- **Intune + Endpoint Manager**: si quiere una solución en la nube, considere la posibilidad de ir directamente a Intune. Se obtienen las características de cumplimiento, configuración, Windows Update aplicación en Intune. También se obtienen las ventajas del centro de administración de Endpoint Manager, que es una consola basada en web.

  Luego implemente Intune (en este artículo).

- **Configuration Manager + Endpoint Manager**: si quiere las características de Configuration Manager (local) combinadas con la nube, considere la posibilidad de usar asociación de inquilinos o administración conjunta. Con Configuration Manager puede:

  - Administrar dispositivos locales, incluidos dispositivos Windows Server o Windows 8.1.
  - Administración de actualizaciones de software de asociados o de terceros
  - Crear secuencias de tareas personalizadas al implementar sistemas operativos.
  - Implementar y administrar muchos tipos de aplicaciones.

Para poder decidir, vea Elegir una solución de administración de dispositivos.

Actualmente se usa un proveedor de MDM ajeno

Los dispositivos solo deberían tener un proveedor de MDM. Si usa otro proveedor de MDM, como Workspace ONE (anteriormente denominado AirWatch), MobileIron o MaaS360, puede migrar a Intune. El mayor desafío es que los usuarios deben anular la inscripción de los dispositivos en el proveedor de MDM actual y luego inscribirse en Intune.

> **IMPORTANT**
> No configure Intune ni la solución de MDM ajena existente para que apliquen controles de acceso a los recursos, incluidos Exchange o SharePoint Online.

Recomendaciones:

- Si va a migrar desde un proveedor de MDM/MAM asociado, anote las tareas que ejecuta y las características que usa. Esta información le da una idea de qué hacer o por dónde empezar en Intune.
- Cuando se anula la inscripción de los dispositivos, estos ya no reciben las directivas, incluidas las que proporcionan protección. Son vulnerables hasta que se inscriben en Intune. Al anular la inscripción de los dispositivos, se recomienda el Uso del acceso condicional para bloquearlos hasta que se inscriban en Intune.

  Asegúrese de conocer los pasos específicos de anulación de inscripción e inscripción. Incluya instrucciones del proveedor de MDM existente sobre cómo anular la inscripción de los dispositivos. Una comunicación clara y útil minimiza el descontento y el tiempo de inactividad de los usuarios finales.
- Use un método por fases. Comience con un pequeño grupo de usuarios piloto y agregue más grupos hasta llegar a la implementación completa.
- Supervise la carga del departamento de soporte técnico y el éxito de la inscripción en cada fase. Deje un tiempo en la programación para evaluar los criterios de éxito de cada grupo antes de migrar el siguiente. La implementación piloto debe validar las siguientes tareas:
  - Que las tasas de éxito y error de inscripción se encuentren dentro de lo esperado.
  - Productividad del usuario:
    - Que los recursos corporativos funcionan, lo que incluye VPN, Wi-Fi, correo electrónico y certificados.
    - Que se puede obtener acceso a las aplicaciones implementadas.
  - Seguridad de los datos:
    - Revise los informes de cumplimiento y busque tendencias y problemas comunes. Comunique problemas, resoluciones y tendencias al departamento de soporte técnico.
    - Que se han aplicado protecciones de aplicaciones móviles.
- Cuando esté satisfecho con la primera fase de las migraciones, repita el ciclo de migración en la siguiente fase.
  - Repita los ciclos por fases hasta que todos los usuarios se hayan migrado a Intune.
  - Confirme que el departamento de soporte técnico está preparado para asistir a los usuarios finales durante la migración. Ejecute una migración voluntaria hasta que pueda calcular la carga de trabajo de llamadas de soporte técnico.
  - No establezca fechas límite de inscripción hasta que el departamento de soporte técnico pueda controlar al resto de los usuarios.

Para obtener instrucciones de inscripción, vea la guía de implementación de la inscripción en Intune.

Luego implemente Intune (en este artículo).

Actualmente se usa Configuration Manager

Configuration Manager admite dispositivos Windows y macOS, y servidores Windows Server. Si usa otras plataformas, es posible que tenga que restablecer los dispositivos y luego inscribirlos en Intune. Una vez inscritos, reciben las directivas y los perfiles que se crean. Para obtener más información, vea la guía de implementación de la inscripción en Intune y la entrada de blog sobre conexión a la nube.

Si actualmente usa Configuration Manager y quiere usar Intune, tiene las siguientes opciones.

Opción 1: incorporación de la asociación de inquilinos

La asociación de inquilinos permite cargar los dispositivos de Configuration Manager en la organización en Intune, lo que también se conoce como "inquilino". Después de asociar los dispositivos, use el centro de administración de Microsoft Endpoint Manager para ejecutar acciones remotas, como sincronizar la máquina y la directiva de usuario. También puede ver los servidores locales y obtener información del sistema operativo.

La asociación de inquilinos está incluida en la licencia de administración conjunta de Configuration Manager sin costo adicional. Es la forma más sencilla de integrar la nube (Intune) con la instalación local de Configuration Manager.

Para obtener más información, vea Habilitación de la asociación de inquilinos.

Opción 2: configuración de la administración conjunta

Esta opción usa Configuration Manager para algunas cargas de trabajo e Intune para otras.

1. En Configuration Manager, configure la administración conjunta.
2. Implemente Intune (en este artículo), incluido el establecimiento de la entidad de MDM en Intune.

Entonces los dispositivos están listos para inscribirse y recibir las directivas.

Información de utilidad:

- ¿Qué es administración conjunta?
- Administración conjunta de cargas de trabajo
- Cambiar las cargas de trabajo de Configuration Manager a Intune
- Preguntas más frecuentes sobre productos y licencias de Configuration Manager

Opción 3: migración desde Configuration Manager a Intune

Este escenario no es habitual. La mayoría de los clientes existentes de Configuration Manager quieren seguir usándolo. Microsoft quiere que siga usando Configuration Manager. Incluye servicios que son beneficiosos para los dispositivos locales, como Análisis de escritorio, etc.

Estos pasos son una introducción que solo se incluye para aquellos usuarios que quieren una solución cien por cien en la nube. Con esta opción puede:

- Registrar los dispositivos locales existentes Windows 10 de Active Directory como dispositivos de Azure Active Directory (AD).
- Migrar las cargas de trabajo locales existentes de Configuration Manager a Intune.

Esta opción conlleva más trabajo para los administradores, pero puede crear una experiencia menos problemática para dispositivos existentes Windows 10. En el caso de los nuevos dispositivos Windows 10, se recomienda empezar desde cero con Microsoft 365 e Intune (en este artículo).

1. Configure Active Directory híbrido y Azure AD para los dispositivos. Los dispositivos unidos a Azure AD

híbrido se unen a Active Directory local y se registran en Azure AD. Cuando los dispositivos están en Azure AD, están disponibles para recibir las directivas y los perfiles que se crean en Intune.

Azure AD híbrido admite dispositivos Windows. Para conocer otros requisitos previos, incluidos los de inicio de sesión, vea Planeamiento de la implementación de la unión a Azure AD híbrido.

2. En Configuration Manager, configure la administración conjunta.
3. Implemente Intune (en este artículo), incluido el establecimiento de la entidad de MDM en Intune.
4. En Configuration Manager, realice el Cambio de las cargas de trabajo de Configuration Manager a Intune.
5. En los dispositivos, desinstale el cliente de Configuration Manager. Para obtener más información, vea Desinstalación del cliente.

   Una vez configurado Intune, puede crear una directiva de configuración de aplicaciones de Intune que desinstale el cliente de Configuration Manager. Por ejemplo, puede invertir los pasos de Instalación del cliente de Configuration Manager mediante Intune.

Entonces los dispositivos están listos para inscribirse y recibir las directivas.

> **IMPORTANT**
> Azure AD híbrido solo admite dispositivos Windows. Configuration Manager admite dispositivos Windows y macOS. En el caso de los dispositivos macOS administrados en Configuration Manager, puede:
>
> 1. Desinstalar el cliente de Configuration Manager. Cuando se anula la inscripción, los dispositivos ya no reciben las directivas, incluidas las que proporcionan protección. Son vulnerables hasta que se inscriben en Intune.
> 2. Inscribir los dispositivos en Intune para recibir directivas.
>
> Para ayudar a minimizar las vulnerabilidades, migre los dispositivos macOS una vez que Intune esté configurado y las directivas de inscripción estén listas para su implementación.

Opción 4: comienzo desde cero con Microsoft 365 e Intune

Esta opción se aplica a dispositivos Windows 10 y más recientes. Si emplea sistemas operativos Windows Server, como Windows Server 2016, no use esta opción. Use Configuration Manager.

1. Implemente Microsoft 365, lo que incluye la creación de usuarios y grupos.

   Vínculos útiles:

   - Guía de implementación de Microsoft 365 Enterprise
   - Configure Microsoft 365 Enterprise
2. Implemente Intune (en este artículo), incluido el establecimiento de la entidad de MDM en Intune.
3. En los dispositivos existentes, desinstale el cliente de Configuration Manager. Para obtener más información, vea Desinstalación del cliente.

Entonces los dispositivos están listos para inscribirse y recibir las directivas.

Actualmente se usa la directiva de grupo local

En la nube, los proveedores de MDM, como Intune, administran la configuración y las características de los dispositivos. No se usan objetos de directivas de grupo (GPO). Cuando se administran dispositivos, los perfiles de configuración de dispositivos de Intune reemplazan a los GPO locales. Estos perfiles usan la configuración expuesta por Apple, Google y Microsoft. Concretamente:

- En los dispositivos Android, estos perfiles usan Management API y EMM API de Android.

- En los dispositivos Apple, estos perfiles usan las cargas de administración de dispositivos.
- En los dispositivos Windows, estos perfiles usan los proveedores de servicios de configuración (CSP) de Windows.

Al migrar dispositivos desde la directiva de grupo, use Análisis de directiva de grupo. En Endpoint Manager, importe los GPO y vea qué directivas hay disponibles (y no disponibles) en Intune.

Luego implemente Intune (en este artículo).

Migración de inquilino a inquilino

Un inquilino es su organización en Azure Active Directory (AD), como Contoso. Incluye una instancia de servicio de Azure AD dedicada que Contoso recibe cuando obtiene un servicio en la nube de Microsoft, como Microsoft Intune o Microsoft 365. Azure AD lo utiliza Intune y Microsoft 365 para identificar a los usuarios y dispositivos, controlar el acceso a las directivas creadas y mucho más.

En Intune, puede exportar e importar algunas de las directivas mediante Microsoft Graph y Windows PowerShell.

Por ejemplo, cree una suscripción de Microsoft Intune de prueba. En este inquilino de prueba de suscripción, tiene directivas que configuran aplicaciones y características, comprueban el cumplimiento y mucho más. Le gustaría mover estas directivas a otro inquilino.

> **IMPORTANT**
>
> - En estos pasos se usan los ejemplos de Graph beta de Intune en GitHub. Los scripts de ejemplo hacen cambios en el inquilino. Están disponibles tal y como están y deben validarse con una cuenta de inquilino que no sea de producción o de "prueba". Asegúrese de que los scripts cumplen las directrices de seguridad de la organización.
> - Los scripts no exportan ni importan todas las directivas, como los perfiles de certificado. Prepárese para realizar más tareas de las que están disponibles en estos scripts. Tendrá que volver a crear algunas directivas.
> - Para migrar el dispositivo de un usuario, este debe deshacer la inscripción del dispositivo del inquilino anterior y, a continuación, volver a inscribirlo en el nuevo inquilino.

Lo que no se puede hacer

Hay algunos tipos de directiva que no se pueden exportar. Hay algunos tipos de directiva que se pueden exportar, pero no se pueden importar a un inquilino diferente. Use la siguiente tabla como guía. Sepa que hay otros tipos de directivas que no aparecen en la lista.

TIPO DE PERFIL O DIRECTIVA	INFORMATION
Aplicaciones	
Aplicaciones Android de línea de negocio	✕ Exportar ✕ Importar Para agregar la aplicación de LOB a un nuevo inquilino, también necesita los archivos de origen de la aplicación `.apk` originales.
Apple: Programa de Compras por Volumen de Apple (VPP)	✕ Exportar ✕ Importar Estas aplicaciones se sincronizan con el VPP de Apple. En el nuevo inquilino, agregue el token de VPP, que muestra las aplicaciones disponibles.

TIPO DE PERFIL O DIRECTIVA	INFORMATION
Aplicaciones de línea de negocio de iOS/iPadOS	✕ Exportar ✕ Importar Para agregar la aplicación de LOB a un nuevo inquilino, también necesita los archivos de origen de la aplicación `.ipa` originales.
Google Play administrado	✕ Exportar ✕ Importar Estas aplicaciones y vínculos web se sincronizan con Google Play administrado. En el nuevo inquilino, agregue la cuenta de Google Play administrado, que muestra las aplicaciones disponibles.
Microsoft Store para Empresas	✕ Exportar ✕ Importar Estas aplicaciones se sincronizan con Microsoft Store para Empresas. En el nuevo inquilino, agregue la cuenta de Microsoft Store para Empresas, que muestra las aplicaciones disponibles.
Aplicación Windows (Win32)	✕ Exportar ✕ Importar Para agregar la aplicación de LOB a un nuevo inquilino, también necesita los archivos de origen de la aplicación `.intunewin` originales.
Directivas de cumplimiento	
Las acciones de no cumplimiento	✕ Exportar ✕ Importar Es posible que haya un vínculo a una plantilla de correo electrónico. Al importar una directiva que tiene acciones de no cumplimiento, en su lugar se agregan las acciones predeterminadas de no cumplimiento.
Assignments	✔ Exportar ✕ Importar Las asignaciones se dirigen a un identificador de grupo. En un nuevo inquilino, el identificador de grupo es diferente.
Perfiles de configuración	
Correo electrónico	✔ Exportar ✔ Si un perfil de correo electrónico no usa certificados, la importación debería funcionar. ✕ Si un perfil de correo electrónico usa un certificado raíz, el perfil no se puede importar a un nuevo inquilino. El identificador del certificado raíz es diferente en un nuevo inquilino.

TIPO DE PERFIL O DIRECTIVA	INFORMATION
Certificado SCEP	✔ Exportar ✘ Importar Los perfiles de certificado SCEP usan un certificado raíz. El identificador del certificado raíz es diferente en un nuevo inquilino.
VPN	✔ Exportar ✔ Si un perfil de VPN no usa certificados, la importación debería funcionar. ✘ Si un perfil de VPN usa un certificado raíz, el perfil no se puede importar a un nuevo inquilino. El identificador del certificado raíz es diferente en un nuevo inquilino.
Wi-Fi	✔ Exportar ✔ Si un perfil Wi-Fi no usa certificados, la importación debería funcionar. ✘ Si un Wi-Fi utiliza un certificado raíz, el perfil no se puede importar a un nuevo inquilino. El identificador del certificado raíz es diferente en un nuevo inquilino.
Assignments	✔ Exportar ✘ Importar Las asignaciones se dirigen a un identificador de grupo. En un nuevo inquilino, el identificador de grupo es diferente.
seguridad de los puntos de conexión	
Detección de puntos de conexión y respuesta	✘ Exportar ✘ Importar Esta directiva está vinculada a Microsoft Defender para punto de conexión. En el nuevo inquilino, configurará Microsoft Defender para punto de conexión, que incluye automáticamente la directiva de **detección y respuesta de puntos de conexión**.

Descargue los ejemplos y ejecute el script.

En esta sección se incluye información general sobre estos pasos. Siga estos pasos como guía y tenga en cuenta que los pasos específicos pueden ser diferentes.

1. Descargue los ejemplos y utilice Windows PowerShell para exportar las directivas:

   a. Vaya a microsoftgraph/powershell-intune-samples y seleccione **Código** > **Descargar archivo Zip**. Extraiga el contenido del archivo `.zip`.

   b. Abra la aplicación de Windows PowerShell como administrador y cambie el directorio a su carpeta. Por ejemplo, escriba el siguiente comando:

   ```
   cd C:\psscripts\powershell-intune-samples-master
   ```

   c. Instale el módulo de PowerShell de Azure AD:

   ```
   Install-Module AzureAD
   ```

Seleccione **Y** para instalar el módulo desde un repositorio que no es de confianza. Esta comprobación puede tardar unos minutos.

d. Cambie el directorio a la carpeta con el script que desea ejecutar. Por ejemplo, cambie el directorio a la carpeta `CompliancePolicy`:

```
cd C:\psscripts\powershell-intune-samples-master\powershell-intune-samples-master\CompliancePolicy
```

e. Ejecute el script de exportación. Por ejemplo, escriba el siguiente comando:

```
.\CompliancePolicy_Export.ps1
```

Inicie sesión con su cuenta. Cuando se le solicite, escriba la ruta de acceso para colocar las directivas. Por ejemplo, escriba:

```
C:\psscripts\ExportedIntunePolicies\CompliancePolicies
```

En la carpeta, se exportan las directivas.

2. Importe las directivas en el nuevo inquilino:

a. Cambie el directorio a la carpeta de PowerShell con el script que desea ejecutar. Por ejemplo, cambie el directorio a la carpeta `CompliancePolicy`:

```
cd C:\psscripts\powershell-intune-samples-master\powershell-intune-samples-master\CompliancePolicy
```

b. Ejecute el script de importación. Por ejemplo, escriba el siguiente comando:

```
.\CompliancePolicy_Import_FromJSON.ps1
```

Inicie sesión con su cuenta. Cuando se le solicite, escriba la ruta de acceso al archivo `.json` de la directiva que desea importar. Por ejemplo, escriba:

```
C:\psscripts\ExportedIntunePolicies\CompliancePolicies\PolicyName.json
```

3. Inicie sesión en el Centro de administración de Endpoint Manager. Se muestran las directivas que ha importado.

Implementación de Intune

1. Inicie sesión en el centro de administración de Endpoint Manager y luego en Intune. Si tiene una suscripción existente, también puede iniciar sesión en ella.

   Para obtener más información, vea Suscribirse o iniciar sesión en Microsoft Intune.

2. Establezca **Intune independiente** como entidad de MDM. Para obtener más información, vea Establecimiento de la entidad de MDM.

3. Agregue la cuenta de dominio, como `contoso.com`. De lo contrario, se usa `your-domain.onmicrosoft.com` automáticamente para el dominio. Por ejemplo, si no agrega la cuenta de dominio, es posible que se use `contoso.onmicrosoft.com`.

   Si va a migrar a Microsoft 365 desde una suscripción de Office 365, es posible que el dominio ya esté en Azure AD. Intune usa la misma instancia de Azure AD y puede emplear el dominio existente.

   Para más información, vea Incorporación de un nombre de dominio personalizado.

4. Agregue usuarios y grupos. Estos usuarios y grupos reciben las directivas que se crean en Endpoint Manager.

Los usuarios y los grupos se almacenan en Azure AD, que está incluido en Microsoft 365. Es posible que no vea la personalización de marca de Azure AD, pero es lo que está usando. Azure AD es el sistema de back-end que almacena usuarios, grupos y dispositivos. También controla el acceso a los recursos y autentica a los usuarios y dispositivos. Asegúrese de que los administradores de AD tengan acceso a la suscripción de Azure AD y que sepan realizar tareas comunes de AD.

Si va a migrar a Microsoft 365 desde una suscripción de Office 365, los usuarios y los grupos ya están en Azure AD. Intune usa la misma instancia de Azure AD y puede emplear los usuarios y los grupos existentes.

Si quiere migrar usuarios existentes desde Active Directory local a Azure AD, puede configurar la identidad híbrida. Las identidades híbridas existen en ambos servicios: AD local y Azure AD. También puede exportar usuarios de Active Directory mediante la interfaz de usuario o por medio de scripts. Realice una búsqueda en Internet para conocer las opciones.

Puede crear **grupos de dispositivos** cuando tenga que realizar tareas administrativas en función de la identidad del dispositivo y no de la del usuario. Son útiles para administrar dispositivos que no tienen usuarios dedicados, como dispositivos de pantalla completa, compartidos entre trabajadores por turnos o asignados a una ubicación concreta. Por ejemplo, cree `Charlotte, NC distribution center - Android Enterprise inventory scanning devices` o `All Windows 10 Surface devices`.

Si configura grupos de dispositivos antes de la inscripción de dispositivos, puede usar categorías de dispositivos para unir dispositivos automáticamente a los grupos durante la inscripción. Luego estos reciben las directivas de dispositivo de su grupo automáticamente. Para obtener más información, vea la guía de implementación de la inscripción en Intune.

5. Asigne licencias de Intune a los usuarios. Cuando se asignan las licencias, los dispositivos de los usuarios pueden inscribirse en Intune.

   Para obtener más información, vea Asignar licencias.

6. De manera predeterminada, todas las plataformas de dispositivos se pueden inscribir en Intune. Si quiere evitar plataformas concretas, cree una restricción.

   Para obtener más información, vea Creación de una restricción de tipo de dispositivo.

7. Personalice la aplicación Portal de empresa de modo que incluya los detalles de la organización. Los usuarios van a usar esta aplicación para inscribir sus dispositivos, instalar aplicaciones y obtener soporte técnico del departamento de TI.

   Para obtener más información, vea Configuración de la aplicación Portal de empresa.

8. Cree el equipo administrativo. Intune usa control de acceso basado en rol para controlar lo que los usuarios pueden ver y cambiar. Como administrador global, puede asignar roles a los usuarios, como operador del departamento de soporte técnico, administrador de aplicaciones, administrador de roles de Intune, etc.

   Para más información, vea Control de acceso basado en rol (RBAC) con Microsoft Intune.

Pasos siguientes

Vea las guías de implementación de la inscripción, Administración de dispositivos y aplicaciones y Protección de aplicaciones.

Migración de su administración de dispositivos móviles desde Basic Mobility and Security a Intune

14/05/2021 • 9 minutes to read

Este artículo le ayudará a migrar la administración de dispositivos móviles (MDM) desde Basic Mobility and Security (Office 365) al portal del administrador de Microsoft Endpoint Manager (Intune).

Al pasar a Intune, se combina toda su MDM en una solución. Permite que todos los usuarios se beneficien del conjunto más amplio de características que ofrece Intune. Para ver una comparación de las características disponibles en los dos servicios, consulte Elección entre Basic Mobility and Security o Intune.

Después de migrar a Intune, las directivas de seguridad de dispositivos existentes implementadas con Basic Mobility and Security se inmovilizarán de forma permanente.

La migración a Intune requiere los tres pasos principales siguientes:

1. **Preparar**: Revise las licencias de Intune, las directivas de Basic Mobility and Security, las pertenencias a grupos y los dispositivos para simplificar la migración.
2. **Migrar directivas**: Use la herramienta de evaluación de la migración para obtener recomendaciones de grupos y directivas de Intune para reemplazar las directivas de Basic Mobility and Security.
3. **Migrar usuarios y dispositivos**: Asigne licencias a usuarios o grupos, que pasarán automáticamente a los usuarios a la administración de dispositivos de Intune en el siguiente ciclo de actualización.

Para obtener una referencia de la asignación de las directivas migradas por esta herramienta, consulte Asignación de directivas entre Basic Mobility and Security e Intune.

Preparación

Antes de migrar la administración de dispositivos desde Basic Mobility and Security a Intune, siga estos pasos:

1. Asegúrese de tener suficientes licencias de Intune para cubrir todos los usuarios administrados por Basic Mobility and Security.
2. Revise las directivas de seguridad de dispositivos en el portal de seguridad y cumplimiento de Office 365 y elimine las que ya no necesite. La eliminación de directivas innecesarias reduce el número de recomendaciones creadas por la herramienta de migración, por lo que tendrá menos para revisar después de la migración.
3. Revise la pertenencia a grupos en las directivas de seguridad de dispositivos asignadas actualmente. Si estos grupos contienen usuarios que ya tienen licencia para Intune, debe crear nuevos grupos para separar los usuarios con licencia de Intune de los grupos sin licencias de Intune. Asigne solo las directivas de seguridad de dispositivos a los usuarios que no tengan asignadas licencias de Intune.
4. Revise los tipos de dispositivos inscritos actualmente en Basic Mobility and Security. Es posible que las versiones de sistema operativo y las variantes no admitidas sigan funcionando, pero no se admitirán si se migran a Intune. Por ejemplo, la configuración aplicada a un teléfono de Windows 8.1 no se moverá a Intune. Si el usuario tiene licencia para Intune, el teléfono perderá cualquier configuración establecida por las directivas de seguridad del dispositivo en el portal de seguridad y cumplimiento de Office 365.
5. Antes de la migración, no asigne licencias de Intune a los usuarios cuyos dispositivos estén administrados por Basic Mobility and Security. No asigne licencias de Intune para habilitar la protección de aplicaciones de Intune sin inscripción (MAM-WE). Solo debe asignar licencias de Intune a los usuarios una vez completado el paso de migración de directivas. La asignación de licencias controla la migración de dispositivos desde Basic Mobility and Security a Intune. Antes de que se mueva el primer dispositivo, asegúrese de que se han creado

directivas de Intune suficientes para reemplazar a Basic Mobility and Security.

Una vez que se activa el proceso de evaluación de la migración, no podrá realizar cambios en las directivas de seguridad del dispositivo en el portal de seguridad y cumplimiento de Office 365. Se aplicarán las directivas existentes, pero no se guardarán los cambios que se realicen en ellas.

IMPORTANT

Póngase en contacto con el soporte técnico antes de continuar si tiene alguno de los siguientes productos:

- Enterprise Mobility + Security A3 for Faculty
- Enterprise Mobility + Security A3 for Students
- Ventaja para uso de Enterprise Mobility + Security A3 for Students
- Enterprise Mobility + Security A5 for Faculty
- Enterprise Mobility + Security A5 for Students
- Ventaja para uso de Enterprise Mobility + Security A5 for Students
- Intune para educación
- Complemento de Intune for Education
- Microsoft Intune for Education for Faculty
- Microsoft Intune for Education for Student
- Dispositivo de prepago de Microsoft Intune for Education

Migración de directivas

Una vez que haya preparado las licencias y las directivas de Basic Mobility and Security como se describe en la sección anterior, puede usar la herramienta de evaluación de la migración para obtener recomendaciones sobre directivas de Intune. La herramienta migrará las directivas de seguridad de dispositivos de Basic Mobility and Security existentes a Intune como directivas de cumplimiento y perfiles de configuración y recomendaciones para los grupos a los que deben asignarse.

Estas recomendaciones de Intune están diseñadas para replicar las directivas de Basic Mobility and Security. Deberá revisar estas recomendaciones para asegurarse de que reflejan las directivas antiguas.

- No necesitará revisar ni hacer cambios en la configuración que controla el acceso condicional a los servicios de Office 365 porque está respaldada por las directivas de acceso condicional de Azure Active Directory clásicas y están disponibles directamente a través del portal de Azure AD. Estas son exactamente las mismas directivas subyacentes administradas indirectamente a través de las directivas de seguridad de los dispositivos en el portal de seguridad y cumplimiento de Office 365, por lo que no es necesario revisarlas o cambiarlas.
- No todas las configuraciones de dispositivos que se ofrecen en las directivas de seguridad de dispositivos se corresponden exactamente con los valores y la configuración de Intune. Por lo tanto, no se pueden cambiar con una asignación precisa de una a una. Tendrá que revisar y posiblemente ajustar estas configuraciones.

Después de revisar y posiblemente cambiar las directivas migradas, puede asignar las directivas a los grupos de Intune. Las nuevas directivas entrarán en vigor una vez que se hayan asignado y los dispositivos administrados por Basic Mobility and Security se migrarán después de asignar licencias de Intune a los usuarios y se produzca el siguiente ciclo de actualización.

NOTE

En el caso del sistema operativo Windows, solo se migrarán las directivas de los dispositivos de escritorio de Windows 10. No se migrarán las directivas de otras versiones de Windows y Windows Phone. Para obtener más información, consulte Asignación de directivas para los requisitos de acceso y Asignación de directivas para la configuración.

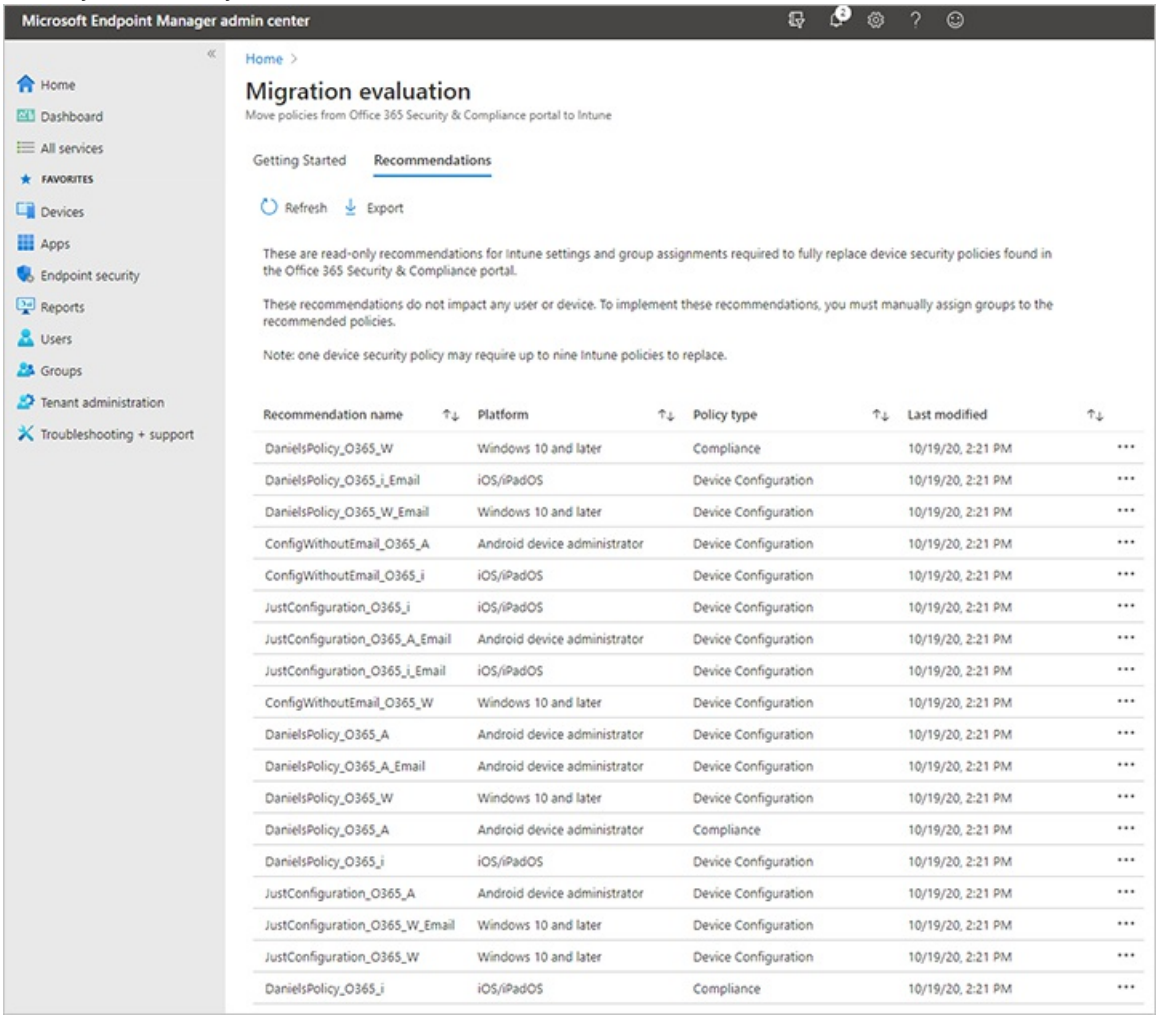
Para migrar directivas desde Basic Mobility and Security a Intune, siga estos pasos:

1. Complete los pasos descritos en la sección Preparar más arriba.
2. Abra la herramienta de evaluación de la migración > **Inicio**. La evaluación tardará unos minutos en completarse.

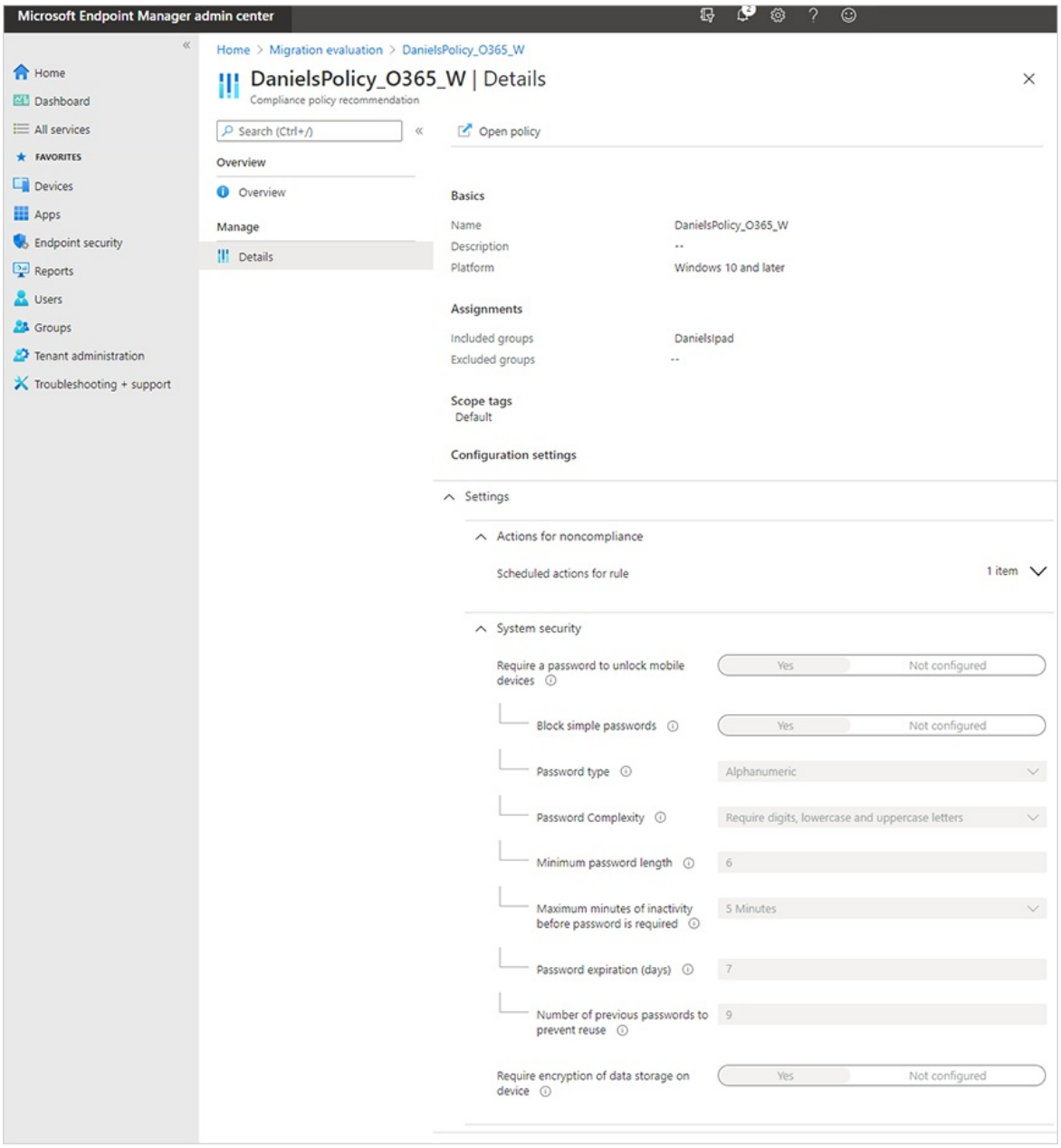
> **NOTE**
> Si sale de la herramienta de evaluación de la migración, la única manera de volver es usar el vínculo anterior.

> **IMPORTANT**
> Después de iniciar la evaluación de la migración, ya no podrá crear nuevas directivas de seguridad de dispositivos o editar las existentes en el portal de seguridad y cumplimiento de Office 365.

3. Seleccione **Recomendaciones**. En esta página se muestran las recomendaciones de directivas de Intune en función de las directivas de Basic Mobility and Security. Las recomendaciones son de solo lectura y no cambiarán. El nombre de cada recomendación tiene un prefijo basado en el nombre de directiva de Basic Mobility and Security. Deberá revisar cada elemento de la lista como se indica a continuación.



4. Seleccione un elemento de la lista para abrir la página de **información general de recomendaciones sobre directivas de cumplimiento** y revise las instrucciones.
5. Seleccione **Detalles** para revisar la configuración y las asignaciones de grupo recomendadas.



La recomendación de directiva de esta página no es una directiva de Intune. Solo es un informe de solo lectura que documenta la configuración y las asignaciones para usar recomendadas. Al revisar las recomendaciones, tenga en cuenta estos puntos:

- Si los grupos enumerados en la recomendación ya tienen directivas de Intune asignadas, pueden entrar en conflicto con la configuración recomendada. Para obtener información sobre cómo se administran los conflictos para una configuración específica, consulte la documentación de la configuración del dispositivo o el cumplimiento del dispositivo.

> **NOTE**
> Si realiza cambios en los perfiles de correo electrónico migrados o no puede asignarlos a grupos recomendados, es posible que se pida a los usuarios que vuelvan a escribir su nombre de usuario y contraseña para acceder al correo electrónico en sus dispositivos cuando el dispositivo migre a Intune. Consulte [asignación de directivas para configuración] (https://docs.microsoft.com/mem/intune/fundamentals/policy-map-configurations

- Si ya hay usuarios con licencia de Intune en los grupos recomendados, compruebe que las directivas recomendadas también serán adecuadas para ellos. Después de asignar las directivas a estos grupos, todos los usuarios con licencia de Intune las recibirán, incluso los usuarios que no se administraban previamente con Basic Mobility and Security.

6. Si desea implementar la directiva recomendada, elija **Abrir directiva**. Se abrirá la página de directivas real. Inicialmente, la directiva no tiene ningún grupo asignado. Esto significa que no afecta a ningún usuario con licencia para Intune que se encuentre en los mismos grupos asignados a la directiva de seguridad del dispositivo original. Deberá asignar los grupos recomendados a la directiva de Intune para reemplazar a la configuración del dispositivo establecida en Basic Mobility and Security. Si no lo hace, los dispositivos administrados por Basic Mobility and Security podrían perder los ajustes y la configuración del correo electrónico cuando sus usuarios obtengan la licencia de Intune, provocando la migración de sus dispositivos.

   > **NOTE**
   > Si elimina la directiva, el vínculo **Abrir directiva** de la página recomendación no funcionará.

7. Para asignar los grupos recomendados a la directiva, elija **Propiedades** > **Editar** (junto a **Asignaciones**) > use el flujo de trabajo de asignaciones para asignar los grupos.

   - Opcionalmente, puede asignar primero un grupo de usuarios de prueba que tengan dispositivos inscritos en Basic Mobility and Security. En este caso, en lugar de asignar los grupos sugeridos reales a la directiva, asigne un grupo de prueba y confirme que las directivas se comportan según lo previsto.

8. Habilite la coexistencia. Después de habilitar la coexistencia, todos los usuarios a los que se les ha asignado una licencia de Intune se migrarán inmediatamente a Intune.

9. Asigne licencias de Intune a los usuarios. Las nuevas directivas comenzarán a afectar a los dispositivos de los usuarios después del siguiente ciclo de actualización.

Problemas conocidos

El botón Iniciar aparece siempre.

El botón **Iniciar** aparecerá cada vez que visite la página evaluación de la migración, incluso si ya se ha generado la evaluación. Si descarta la indicación **Iniciar**, las recomendaciones generadas anteriormente no se cargarán. **Solución alternativa**: vuelva a iniciar la evaluación. No creará recomendaciones ni directivas adicionales o duplicadas. Al volver a ejecutar la migración, se detecta que la evaluación ya se realizó correctamente y se cargan las recomendaciones anteriores.

El número de errores de inicio de sesión antes borrar el dispositivo no se migra.

La opción **Número de errores de inicio de sesión antes borrar el dispositivo** no se migra a Intune. **Solución alternativa**: esta opción debe agregarse manualmente a los perfiles de configuración de dispositivos de Intune si se ha habilitado en la directiva de Basic Mobility and Security.

Migración de usuarios y dispositivos

Para migrar un usuario y sus dispositivos a Intune desde Basic Mobility and Security, siga estos pasos:

1. Habilite la coexistencia. La habilitación de la coexistencia migrará inmediatamente todos los dispositivos a los que se haya asignado una licencia de Intune.
2. Inicie sesión en el centro de administración de Microsoft Endpoint Manager con derechos de administrador global o de licencias de Azure AD.
3. Asigne licencias de Intune a los usuarios que desea migrar mediante Usuarios o Grupos:
   - Asigne licencias a **Usuarios**. Para obtener más información, vea Asignación de licencias a usuarios.
   - Asigne licencias a **Grupos**. Para obtener más información, vea Asignación de licencias a un grupo.
4. Una vez que un usuario tiene licencia para Intune, sus dispositivos cambiarán automáticamente a la administración de Intune en el siguiente ciclo de actualización del dispositivo. Consulte Ciclos de actualización.

Pasos siguientes

Administración de dispositivos en Intune.

Impulso de la adopción de usuarios finales con acceso condicional en Microsoft Intune

14/05/2021 • 2 minutes to read

La habilitación de las características de acceso condicional con Intune, como el bloqueo de correo electrónico para dispositivos no inscritos, puede contribuir a impulsar la inscripción y el cumplimiento, pero no son necesarios para una correcta migración. Los requisitos de seguridad y los objetivos de adopción de la migración deben determinar el éxito.

Campaña de migración con acceso condicional

Este es un método típico para mejorar una campaña de migración con acceso condicional:

1. Establezca reglas de acceso condicional que se apliquen a todos los usuarios, pero excluya específicamente los usuarios que tengan que migrar desde el proveedor de MDM antiguo. Puede crear un grupo de usuarios de Azure AD con todos los usuarios excluidos del acceso condicional.
2. A medida que se migren, quite los usuarios del grupo de exclusión de acceso condicional.
3. Una vez finalizada la migración, configure todas las directivas de acceso condicional para que se bloqueen de forma predeterminada a menos que Intune permita el acceso.

Ventajas

- Ofrece control de acceso para nuevas cuentas de usuario o cuentas de usuario que no se administraban mediante la solución anterior.
- Ofrece un período de gracia para los usuarios de la solución anterior a la migración.
- Minimiza la pérdida de productividad.

Desventajas

- Los usuarios de la solución anterior posiblemente puedan obtener acceso a recursos mediante dispositivos no administrados hasta que se habilite el acceso condicional para esos usuarios.

Se trata de un método entre otros. Es posible elegir un proceso más sencillo que aplace todo el acceso condicional hasta después de que se dé orden de inscripción a cada fase o un proceso más estricto que exija el acceso condicional desde el mismo principio y requiera compatibilidad completa para todos los accesos.

- Más información sobre el acceso condicional.

Lista de tareas para acceso condicional

Tarea 1: determinación de cómo se va a implementar el acceso condicional

Formas comunes de usar el acceso condicional.

Tarea 2: configuración del acceso condicional de Intune

Elija una de las siguientes opciones:

- Configurar el acceso condicional en Azure Active Directory
- Configuración de la autenticación moderna híbrida
- Configurar directivas de acceso condicional basado en la aplicación para Exchange Online

- Configurar directivas de acceso condicional basado en la aplicación para SharePoint Online
- Bloquear las aplicaciones que no usan la autenticación moderna (ADAL o MSAL)

Pasos siguientes

Asegúrese de crear un plan de lanzamiento.

Guía de implementación: Inscripción de dispositivos en Microsoft Intune

14/05/2021 • 4 minutes to read

Azure AD es el pilar de Intune y de Endpoint Manager. Cuando los usuarios y dispositivos se registran en Azure AD (también conocido como inquilino), estarán disponibles también en Intune y Endpoint Manager. Esta característica se denomina "inscripción".

La inscripción de dispositivos les permite recibir las directivas que creamos, como las siguientes:

- Directivas de cumplimiento que sirven para que usuarios y dispositivos cumplan las reglas
- Perfiles de configuración que establecen las características y la configuración de los dispositivos

Muchas organizaciones crean una línea de base de lo que todos los usuarios y dispositivos deben tener. Normalmente, estas directivas se implementan durante la inscripción. Por ejemplo, se podría crear una conexión VPN, instalar un certificado de autenticación o requerir un PIN de Windows Hello. Para obtener más información sobre la inscripción, vea ¿Qué es la inscripción de dispositivos?

Al inscribir un dispositivo, se emite un certificado MDM. Dicho certificado se comunica con el servicio de Intune.

Se pueden inscribir dispositivos en las siguientes plataformas (para consultar versiones concretas, vea las Sistemas operativos compatibles):

- Android
- iOS/iPadOS
- macOS
- Windows

En este artículo se enumeran los requisitos previos de inscripción, se ofrece información sobre el uso de otros proveedores de MDM y se incluyen vínculos a guías de inscripción específicas de cada plataforma.

> **TIP**
> Esta guía está en constante evolución. Así pues, no dude en agregar o actualizar las sugerencias e instrucciones existentes que le hayan parecido útiles.

Requisitos previos

- Tener Intune configurado y listo para inscribir usuarios y dispositivos. No olvide lo siguiente:
  - Tener la entidad de MDM establecida en Intune, incluso cuando use la administración conjunta con Intune + Configuration Manager.
  - Tener licencias de Intune asignadas.

  Para obtener más información, vea Guía de implementación de la configuración de Intune.
- Asegurarse de que sus dispositivos son compatibles. Este requisito engloba a los dispositivos que se administran de manera conjunta o dispositivos híbridos unidos a Azure Active Directory (Azure AD).
- Iniciar sesión como miembro de los roles de Azure AD **Administrador global** o **Administrador del servicio Intune**. En Control de acceso basado en rol (RBAC) con Intune encontrará más información. Si ha creado una suscripción de prueba de Intune, la cuenta con la que la haya creado será el

administrador global.

- Cada plataforma puede tener requisitos adicionales. Por ejemplo, los dispositivos iOS/iPadOS y macOS requieren un certificado push MDM de Apple. Aquí se muestran los requisitos de plataforma adicionales.

PLATAFORMA	REQUISITOS ADICIONALES
Android	ninguno
Android Enterprise	ninguno
iOS/iPadOS	Certificado push MDM de Apple Identificador de Apple
macOS	Certificado push MDM de Apple
Windows	ninguno

- Tenga los grupos de usuarios y de dispositivos listos para recibir las directivas de inscripción. Si no ha revisado o creado la estructura de grupos y le gustaría recibir orientación al respecto, vea Guía de planificación: Tarea 4: revisión de las directivas e infraestructura existentes.

- Si va a inscribir dispositivos de forma masiva, considere la posibilidad de crear una cuenta de **administrador de inscripción de dispositivos** (DEM). Esta cuenta es un permiso de Intune que se aplica a una cuenta de usuario de Azure AD. La cuenta DEM tiene capacidad para inscribir hasta 1000 dispositivos móviles. Use esta cuenta para inscribir y configurar los dispositivos antes de suministrarlos a los usuarios.

  Para obtener más información, vea Inscripción de dispositivos en Intune mediante una cuenta de administrador de inscripción de dispositivos.

Anulación de una inscripción de un proveedor de MDM existente y restablecimiento de fábrica

Si los dispositivos están inscritos actualmente en otro proveedor de MDM, anule la inscripción de dichos dispositivos de ese proveedor de MDM existente. Normalmente, la anulación de la inscripción no quita las características y las configuraciones existentes que se hayan establecido. La mayoría de los proveedores de MDM tienen acciones remotas que quitan los datos específicos de la organización de los dispositivos. Antes de inscribirlos en Intune, puede quitar los datos específicos de la organización de esos dispositivos, aunque no es necesario.

Dependiendo de la plataforma, es posible que se requiera un restablecimiento de fábrica antes de realizar la inscripción en Intune.

PLATAFORMA	¿SE NECESITA UN RESTABLECIMIENTO DE FÁBRICA?
Dispositivos Android Enterprise de propiedad personal con un perfil de trabajo (BYOD)	No
Perfil de trabajo corporativo de Android Enterprise (COPE)	Sí
Android Enterprise totalmente administrado (COBO)	Sí
Dispositivos Android Enterprise dedicados (COSU)	Sí

PLATAFORMA	¿SE NECESITA UN RESTABLECIMIENTO DE FÁBRICA?
Administrador de dispositivos Android (DA)	No
iOS/iPadOS	Sí
macOS	Sí
Windows	No

En las plataformas que no requieran un restablecimiento de fábrica, cuando estos dispositivos se inscriban en Intune, empezarán a recibir directivas de Intune. Si no establece una configuración en Intune, Intune no cambiará ni actualizará esa configuración. Por lo tanto, es posible que las configuraciones establecidas previamente permanezcan así en los dispositivos.

Elección de la guía de inscripción de la plataforma

Hay una guía de inscripción de cada plataforma. Elíjala según su escenario y empiece a trabajar:

- Administración de aplicaciones sin necesidad de inscripción (MAM-WE)
- Android
- iOS/iPadOS
- macOS
- Windows

Grupos piloto

Al asignar sus perfiles, empiece desde abajo y vaya avanzando por fases. Asigne el perfil de inscripción a un grupo piloto o de prueba. Después de las pruebas iniciales, agregue más usuarios al grupo piloto. Después, asigne el perfil de inscripción a más grupos piloto.

Para obtener más información y sugerencias, vea Guía de planificación: Tarea 5: creación de un plan de lanzamiento.

Informes y solución de problemas

- Informe de inscripciones de usuario incompletas
- Solucionar problemas de inscripción de dispositivos

Pasos siguientes

Elija la plataforma y empiece a trabajar:

- MAM-WE
- Guía de inscripción de Android
- Guía de inscripción de iOS/iPadOS
- Guía de inscripción de macOS
- Guía de inscripción de Windows

Guía de implementación: Inscripción de dispositivos mediante la administración de aplicaciones sin inscripción (MAM-WE) en Microsoft Intune

14/05/2021 • 3 minutes to read

MAM-WE no es un método tradicional de "inscripción", ya que usa el perfil de configuración de aplicaciones para implementar o configurar aplicaciones en los dispositivos. Los dispositivos no se inscriben. Cuando se combina con las directivas de protección de aplicaciones, puede proteger los datos en una aplicación.

MAM-WE suele usarse para dispositivos personales o BYOD. También pueden usarse para dispositivos administrados que necesitan seguridad adicional. También es una opción para los usuarios que no inscriben sus dispositivos personales pero que, aun así, necesitan acceder al correo electrónico de la organización, a las reuniones de Teams y mucho más.

MAM-WE se encuentra disponible en las plataformas siguientes:

- Android
- iOS/iPadOS
- Windows

En este artículo se proporcionan recomendaciones sobre cuándo usar MAM-WE. También se incluye información general de las tareas del administrador y el usuario. Para obtener información más específica sobre MAM-WE, vea Administración de aplicaciones de Microsoft Intune.

> **TIP**
> Esta guía está en constante evolución. Así pues, no dude en agregar o actualizar las sugerencias e instrucciones existentes que le hayan parecido útiles.

Antes de empezar

Para obtener información general, incluidos los requisitos previos específicos de Intune, vea Guía de implementación: Inscripción de dispositivos en Microsoft Intune.

Inscripción de MAM-WE

Úsela para dispositivos personales o BYOD. También puede usarla en dispositivos propiedad de la organización que necesiten una configuración de aplicaciones específica o seguridad de aplicaciones adicional.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Quiere configurar aplicaciones específicas y controlar el acceso a estas aplicaciones, como Outlook o Microsoft Teams.	✔
Los dispositivos son personales o BYOD.	✔
Tiene dispositivos nuevos o existentes.	✔

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Necesita administrar un número pequeño de dispositivos o un gran número de dispositivos (inscripción masiva).	✔
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos los administra otra solución de MDM.	✔
Usa la cuenta del administrador de inscripción de dispositivos (DEM).	✔
Los dispositivos pertenecen a la organización o la escuela.	✘ No se recomienda como el *único* método de inscripción para dispositivos propiedad de la organización. Este tipo de dispositivos deben inscribirse y administrarse mediante Intune. Si quiere seguridad adicional para aplicaciones específicas, use la inscripción y MAM-WE de forma conjunta.
Los dispositivos son sin usuario como, por ejemplo, pantalla completa o un dispositivo dedicado.	✘ Normalmente, los dispositivos sin usuario o compartidos son propiedad de la organización. Estos dispositivos deben inscribirse y administrarse mediante Intune.

Tareas del administrador de MAM-WE

Esta lista de tareas proporciona información general. Para obtener información más específica, vea Administración de aplicaciones de Microsoft Intune.

- Asegúrese de que los dispositivos sean compatibles.
- En el centro de administración de Endpoint Manager, agregue las aplicaciones o configure las aplicaciones. Cuando las aplicaciones están en el dispositivo, Intune las considera "administradas". Después de agregar o configurar la aplicación, cree una directiva de protección de aplicaciones. Por ejemplo, cree una directiva que permita o bloquee las características en la aplicación, tales como copiar y pegar.
- Indique a los usuarios cómo obtener la aplicación. Por ejemplo, puede:
  - Dirigir a los usuarios al sitio web de Portal de empresa en `portal.manage.microsoft.com`. Cuando inicien sesión con las credenciales de su organización, verán una lista de aplicaciones, incluidas las aplicaciones necesarias. Pueden obtener las aplicaciones de este sitio.
  - Pedir a los usuarios que descarguen e instalen la aplicación Portal de empresa en la Tienda de aplicaciones. Una vez autenticados, los usuarios pueden instalar aplicaciones, incluidas las necesarias.

Tareas del usuario final de MAM-WE

Las tareas específicas dependen de la forma en que indique a los usuarios que instalen las aplicaciones.

- Para instalar las aplicaciones, los usuarios pueden realizar lo siguiente:
  - Ir a la tienda de aplicaciones y descargar la aplicación.
  - Ir a la tienda de aplicaciones y descargar la aplicación Portal de empresa. La aplicación Portal de empresa autentica al usuario. Abrir la aplicación Portal de empresa e iniciar sesión con las credenciales de su organización (`user@contoso.com`). Verán una lista de aplicaciones disponibles, incluidas las aplicaciones requeridas.

    - Ir al sitio web de Portal de empresa en `portal.manage.microsoft.com` e iniciar sesión con las credenciales de su organización (`user@contoso.com`). Una vez que hayan iniciado sesión, verán una lista de aplicaciones disponibles, incluidas las aplicaciones requeridas.
- Una vez instalada la aplicación, deberán abrir la aplicación y se les pedirá que inicien sesión con las credenciales de su organización (`user@contoso.com`). Cuando los usuarios inicien sesión, es posible que tengan que reiniciar la aplicación. Después del reinicio, Intune "administra" los datos de la aplicación.
- Algunas plataformas pueden requerir aplicaciones específicas para instalar otras aplicaciones, como Outlook o Teams. Por ejemplo, en los dispositivos iOS, los usuarios deben instalar una aplicación de agente, como la aplicación Microsoft Authenticator. En los dispositivos Android, los usuarios deben instalar la aplicación Portal de empresa.

Pasos siguientes

- Guía de inscripción de Android
- Guía de inscripción de iOS/iPadOS
- Guía de inscripción de macOS
- Guía de inscripción de Windows

Guía de implementación: Inscripción de dispositivos Android en Microsoft Intune

14/05/2021 • 13 minutes to read

Los dispositivos personales y propiedad de la organización se pueden inscribir en Intune. Una vez inscritos, reciben las directivas y los perfiles que se crean. Al inscribir dispositivos Android, dispone de las siguientes opciones:

- BYOD: Dispositivos Android Enterprise de propiedad personal con un perfil de trabajo
- Dispositivos Android Enterprise dedicados de propiedad corporativa (COSU)
- Dispositivos Android Enterprise de propiedad corporativa totalmente administrados (COBO)
- Perfil de trabajo de propiedad corporativa de Android Enterprise (COPE)
- Administrador de dispositivos Android (DA)

En este artículo se proporcionan recomendaciones sobre los métodos de inscripción de dispositivos Android. También se incluye información general de las tareas del administrador y el usuario final para cada tipo de inscripción.

Para obtener información específica, vea Inscripción de dispositivos Android.

> **TIP**
> Esta guía está en constante evolución. Así pues, no dude en agregar o actualizar las sugerencias e instrucciones existentes que le hayan parecido útiles.

Antes de empezar

Para obtener información general, incluidos los requisitos previos específicos de Intune, vea Guía de implementación: Inscripción de dispositivos en Microsoft Intune.

BYOD: Dispositivos Android Enterprise de propiedad personal con un perfil de trabajo

Estos dispositivos son dispositivos Android personales o BYOD (Bring Your Own Device) con acceso al correo electrónico, las aplicaciones y otros datos de la organización.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos son personales o BYOD.	✔ Estos dispositivos se pueden marcar como corporativos o personales.
Tiene dispositivos nuevos o existentes.	✔
Necesita inscribir un número pequeño de dispositivos o un gran número de dispositivos (inscripción masiva).	✔

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos están asociados a un único usuario.	✔
Usa la cuenta opcional del administrador de inscripción de dispositivos (DEM).	✔
Los dispositivos los administra otro proveedor de MDM.	✕ Cuando se inscribe un dispositivo, los proveedores de MDM instalan certificados y otros archivos. Estos archivos se deben quitar. La forma más rápida puede consistir en la anulación de la inscripción o el restablecimiento de fábrica de los dispositivos. Si no quiere llevar a cabo el restablecimiento de fábrica, póngase en contacto con el proveedor de MDM.
Los dispositivos pertenecen a la organización o la escuela.	✕ No recomendado en el caso de los dispositivos propiedad de la organización. Los dispositivos propiedad de la organización se deben inscribir con Android Enterprise totalmente administrado (en este artículo), o bien un perfil de trabajo de propiedad corporativa de Android Enterprise (en este artículo).
Los dispositivos son sin usuario como, por ejemplo, pantalla completa, dedicado o compartido.	✕ Los dispositivos sin usuario o compartidos deben ser propiedad de la organización. Estos dispositivos se deben inscribir con dispositivos Android Enterprise dedicados.

Tareas de administrador de dispositivos de propiedad personal de Android Enterprise con un perfil de trabajo

Esta lista de tareas contiene información general. Para obtener información más específica, vea Configuración de la inscripción de dispositivos de perfil de trabajo de propiedad personal de Android Enterprise.

- Asegúrese de que los dispositivos son compatibles.
- En el centro de administración de Endpoint Manager, conecte la cuenta de la organización de Intune a su cuenta de Google Play administrada. Al conectar, Intune agrega automáticamente a los dispositivos tanto la aplicación Portal de empresa como otras aplicaciones de Android Enterprise habituales. Para conocer el procedimiento detalladamente, vea Conexión de una cuenta de Intune a una cuenta de Google Play administrado.

Tareas de usuario final de dispositivos de propiedad personal de Android Enterprise con un perfil de trabajo

Los usuarios deben realizar los pasos siguientes. Para obtener más información sobre la experiencia de usuario, vea Inscribir dispositivos.

1. Vaya a Google Play Store e instale la aplicación Portal de empresa.
2. Los usuarios abren la aplicación Portal de empresa e inician sesión con sus credenciales de la organización (`user@contoso.com`). Tras iniciar sesión, el perfil de inscripción se aplica al dispositivo.

   Es posible que los usuarios tengan que especificar más información. Para conocer el procedimiento más detalladamente, vea Inscribir dispositivos.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para

obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

> **TIP**
> Hay un vídeo breve con instrucciones paso a paso para ayudar a los usuarios a inscribir sus dispositivos en Intune:
>
> Inscripción de su dispositivo Android

Dispositivos Android Enterprise dedicados

Anteriormente se conocían como COSU. Estos dispositivos son propiedad de la organización y se admiten en Zero Touch de Google. Su único propósito es actuar como dispositivos de tipo pantalla completa. No están asociados a ningún usuario único o específico. Estos dispositivos se suelen usar para escanear elementos, imprimir vales, obtener firmas digitales, administrar inventarios, etc.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos pertenecen a la organización o la escuela.	✔
Tiene dispositivos nuevos o existentes.	✔
Necesita inscribir un número pequeño de dispositivos o un gran número de dispositivos (inscripción masiva).	✔
Los dispositivos son sin usuario como, por ejemplo, pantalla completa, dedicado o compartido.	✔
Los dispositivos son personales o BYOD.	✖ Los dispositivos BYOD o personales se deben inscribir mediante dispositivos Android Enterprise de propiedad personal con un perfil de trabajo (en este artículo).
Los dispositivos están asociados a un único usuario.	✖ No se recomienda. Estos dispositivos se deben inscribir con un dispositivo Android Enterprise totalmente administrado.
Usa la cuenta opcional del administrador de inscripción de dispositivos (DEM).	✖ No se puede usar la cuenta DEM.
Los dispositivos los administra otro proveedor de MDM.	✖ Para que se administren completamente con Intune, los usuarios deben anular la inscripción del proveedor de MDM actual y, luego, inscribirlos en Intune.

Tareas de administrador de dispositivos Android Enterprise dedicados

Esta lista de tareas contiene información general. Para obtener información más específica, vea Configuración de la inscripción en Intune de dispositivos dedicados de Android Enterprise.

- Asegúrese de que los dispositivos son compatibles.

- Restablezca los dispositivos a los valores de fábrica. Este paso es obligatorio.
- En el centro de administración de Endpoint Manager, conecte la cuenta de la organización de Intune a su cuenta de Google Play administrada. Al conectar, Intune agrega automáticamente a los dispositivos tanto la aplicación Intune como otras aplicaciones de Android Enterprise habituales. Para conocer el procedimiento detalladamente, vea Conexión de una cuenta de Intune a una cuenta de Google Play administrado.
- En el centro de administración de Endpoint Manager, cree un perfil de inscripción y tenga listos los grupos de dispositivos dedicados. Para conocer el procedimiento específico, vea Configuración de la inscripción en Intune de dispositivos dedicados de Android Enterprise.
- Inscriba los dispositivos en Intune. Para conocer el procedimiento específico, vea Inscripción de los dispositivos de Android Enterprise.

  En los dispositivos Samsung Knox, se puede inscribir automáticamente un gran número de dispositivos Android Enterprise usando Samsung Knox Mobile Enrollment (KME). Para más información, vea Automatically enroll Android devices by using Samsung's Knox Mobile Enrollment (Inscripción automática de dispositivos Android mediante Samsung Knox Mobile Enrollment).

Tareas de usuario final de dispositivos Android Enterprise dedicados

No es aconsejable que los usuarios inscriban dispositivos Android Enterprise dedicados. Es preferible que se encarguen de esto los administradores.

Android Enterprise totalmente administrado

Anteriormente se conocía como COBO. Estos dispositivos son propiedad de la organización y tienen un usuario. Se usan única y exclusivamente para desarrollar el trabajo de la organización; no tienen un uso personal.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos pertenecen a la organización o la escuela.	✔
Tiene dispositivos nuevos o existentes.	✔
Necesita inscribir un número pequeño de dispositivos o un gran número de dispositivos (inscripción masiva).	✔
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos son sin usuario como, por ejemplo, pantalla completa, dedicado o compartido.	✕ Los dispositivos sin usuario se deben inscribir con dispositivos Android Enterprise dedicados.
Los dispositivos son personales o BYOD.	✕ Los dispositivos BYOD o personales se deben inscribir mediante dispositivos Android Enterprise de propiedad personal con un perfil de trabajo (en este artículo).
Los dispositivos los administra otro proveedor de MDM.	✕ Para que se administren completamente con Intune, los usuarios deben anular la inscripción del proveedor de MDM actual y, luego, inscribirlos en Intune.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Usa la cuenta opcional del administrador de inscripción de dispositivos (DEM).	✕ No se puede usar la cuenta DEM.

Tareas de administrador de dispositivos Android Enterprise totalmente administrado

Esta lista de tareas contiene información general. Para obtener información más específica, vea Configuración de la inscripción en Intune de dispositivos Android Enterprise totalmente administrados.

- Asegúrese de que los dispositivos son compatibles.
- Restablezca los dispositivos a los valores de fábrica. Este paso es obligatorio.
- En el centro de administración de Endpoint Manager, conecte la cuenta de la organización de Intune a su cuenta de Google Play administrada. Al conectar, Intune agrega automáticamente a los dispositivos tanto la aplicación Portal de empresa como otras aplicaciones de Android Enterprise habituales. Para conocer el procedimiento detalladamente, vea Conexión de una cuenta de Intune a una cuenta de Google Play administrado.
- En el centro de administración de Endpoint Manager, habilite los dispositivos de usuario totalmente administrados. Para conocer el procedimiento específico, vea Configuración de la inscripción en Intune de dispositivos Android Enterprise totalmente administrados.
- Inscriba los dispositivos en Intune. Para conocer el procedimiento específico, vea Inscripción de los dispositivos de Android Enterprise.
- Explique a los usuarios con qué método deben inscribirse: una transmisión de datos en proximidad (NFC), un token, un código QR, Google Zero Touch o Samsung Knox Mobile Enrollment (KME).

  Si se usa Samsung Knox Mobile Enrollment (KME), se puede inscribir automáticamente un gran número de dispositivos de Android Enterprise de Samsung Knox. Para más información, vea Automatically enroll Android devices by using Samsung's Knox Mobile Enrollment (Inscripción automática de dispositivos Android mediante Samsung Knox Mobile Enrollment).

Tareas de usuario final de dispositivos Android Enterprise totalmente administrados

Los pasos específicos dependen de cómo se haya configurado el perfil de inscripción. Para obtener más información sobre la experiencia de usuario, vea Inscribir dispositivos.

1. Los usuarios encienden el dispositivo y se les solicita información, incluido el método de inscripción: NFC, token, código QR o Google Zero Touch. Puede que se les pida que inicien sesión con sus credenciales de la organización (`user@contoso.com`).
2. Tras especificar la información necesaria, el perfil de inscripción se aplica al dispositivo.

   Es posible que los usuarios tengan que especificar más información. Para conocer el procedimiento más detalladamente, vea Inscribir dispositivos.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

Perfil de trabajo de propiedad corporativa de Android Enterprise

Anteriormente se conocían como COPE. Estos dispositivos son propiedad de la organización y tienen un usuario.

Se usan para desarrollar el trabajo de la organización y se puede hacer un uso personal de ellos.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos pertenecen a la organización o la escuela.	✔
Tiene dispositivos nuevos o existentes.	✔
Necesita inscribir un número pequeño de dispositivos o un gran número de dispositivos (inscripción masiva).	✔
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos son sin usuario como, por ejemplo, pantalla completa, dedicado o compartido.	✘ Los dispositivos sin usuario se deben inscribir con dispositivos Android Enterprise dedicados. Además, se puede inscribir un administrador de la organización. Cuando el dispositivo esté inscrito, cree un perfil de dispositivo dedicado y asigne este perfil al dispositivo.
Los dispositivos son personales o BYOD.	✘ Los dispositivos BYOD o personales se deben inscribir mediante dispositivos Android Enterprise de propiedad personal con un perfil de trabajo (en este artículo).
Los dispositivos los administra otro proveedor de MDM.	✘ Para que se administren completamente con Intune, los usuarios deben anular la inscripción del proveedor de MDM actual y, luego, inscribirlos en Intune.
Usa la cuenta opcional del administrador de inscripción de dispositivos (DEM).	✘ No se puede usar la cuenta DEM.

Tareas de administrador de perfil de trabajo de propiedad corporativa de Android Enterprise

Esta lista de tareas contiene información general. Para obtener información más específica, vea Configuración de la inscripción de Intune de perfiles de trabajo de propiedad corporativa de Android Enterprise.

- Asegúrese de que los dispositivos son compatibles.
- Restablezca los dispositivos a los valores de fábrica. Este paso es obligatorio.
- En el centro de administración de Endpoint Manager, conecte la cuenta de la organización de Intune a su cuenta de Google Play administrada. Al conectar, Intune agrega automáticamente a los dispositivos tanto la aplicación Portal de empresa como otras aplicaciones de Android Enterprise habituales. Para conocer el procedimiento detalladamente, vea Conexión de una cuenta de Intune a una cuenta de Google Play administrado.
- En el centro de administración de Endpoint Manager, habilite los dispositivos de perfil personal de propiedad corporativa. Para conocer el procedimiento específico, vea Configuración de la inscripción de Intune para dispositivos corporativos de Android Enterprise con un perfil de trabajo.
- Inscriba los dispositivos en Intune. Para conocer el procedimiento específico, vea Inscripción de los dispositivos de Android Enterprise.

- Explique a los usuarios con qué método deben inscribirse: una transmisión de datos en proximidad (NFC), un token, un código QR, Google Zero Touch o Samsung Knox Mobile Enrollment (KME).

  Si se usa Samsung Knox Mobile Enrollment (KME), se puede inscribir automáticamente un gran número de dispositivos de Android Enterprise de Samsung Knox. Para más información, vea Automatically enroll Android devices by using Samsung's Knox Mobile Enrollment (Inscripción automática de dispositivos Android mediante Samsung Knox Mobile Enrollment).

Tareas de usuario final del perfil de trabajo de propiedad corporativa de Android Enterprise

Los pasos específicos dependen de cómo se haya configurado el perfil de inscripción. Para obtener más información sobre la experiencia de usuario, vea Inscribir dispositivos.

1. Los usuarios encienden el dispositivo y se les solicita información, incluido el método de inscripción: NFC, token, código QR o Google Zero Touch. Puede que se les pida que inicien sesión con sus credenciales de la organización (`user@contoso.com`).

2. Tras especificar la información necesaria, el perfil de inscripción se aplica al dispositivo.

   Es posible que los usuarios tengan que especificar más información. Para conocer el procedimiento más detalladamente, vea Inscribir dispositivos.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

Administrador de dispositivos Android

Estos dispositivos Android son dispositivos corporativos o personales/BYOD (Bring Your Own Device) con acceso al correo electrónico, las aplicaciones y otros datos de la organización.

Google está reduciendo la compatibilidad de administradores de dispositivos en las nuevas versiones de Android. Para no ver las funcionalidades reducidas, Microsoft recomienda hacer lo siguiente:

- Inscriba los dispositivos nuevos mediante dispositivos Android Enterprise de propiedad personal con un perfil de trabajo (en este artículo). No los inscriba con el administrador de dispositivos Android.
- Crear una restricción de inscripción de dispositivos para bloquear la inscripción de administradores de dispositivos. Puede que los dispositivos Android intenten inscribirse con el administrador de dispositivos antes de probar con otros métodos de inscripción. Por lo tanto, conviene crear esta restricción para evitar este comportamiento. Para obtener más información, consulte Establecer restricciones de inscripción.
- Si los dispositivos se van a actualizar a Android 10, mígrelos fuera de la administración del administrador de dispositivos.
- Mueva los dispositivos de administrador de dispositivos Android existentes a dispositivos de propiedad personal de Android Enterprise con un perfil de trabajo (en este artículo), o bien a perfiles de trabajo de propiedad corporativa (en este artículo). Para obtener más información, vea Transferencia de dispositivos Android desde el administrador de dispositivos a la administración de perfiles de trabajo.
- La inscripción del administrador de dispositivos está bloqueada de forma predeterminada en los nuevos inquilinos.

Hay algunas situaciones en las que debe usar la inscripción del administrador de dispositivos:

- Android Enterprise necesita acceder a los servicios de Google. Es posible que los servicios de Google no estén disponibles debido a la geografía o al fabricante del dispositivo. Por ejemplo:
  - Hay lugares en los que los servicios de Google no están disponibles, como China. En ese caso, use la inscripción del administrador de dispositivos Android.

- Algunos dispositivos se basan en Android, pero no tienen acceso a los servicios de Google, como las tabletas Amazon Fire. En ese caso, use la inscripción del administrador de dispositivos Android.

- Las versiones del sistema operativo Android anteriores a la 5.0 deben usar la inscripción de administrador de dispositivos Android. La inscripción de Android Enterprise no es una opción.

Pasos siguientes

- MAM-WE
- Guía de inscripción de iOS/iPadOS
- Guía de inscripción de macOS
- Guía de inscripción de Windows

Guía de implementación: Inscripción de dispositivos iOS y iPadOS en Microsoft Intune

14/05/2021 • 28 minutes to read

Los dispositivos personales y propiedad de la organización se pueden inscribir en Intune. Una vez inscritos, recibirán las directivas y los perfiles que se creen. Al inscribir dispositivos iOS/iPadOS, dispone de las opciones siguientes:

- Inscripción de dispositivo automatizada (ADE)
- Apple Configurator
- BYOD: inscripción de usuario y de dispositivo

En este artículo se proporcionan recomendaciones sobre el método de inscripción de iOS/iPadOS que se va a usar. También se incluye información general de las tareas del administrador y el usuario final para cada tipo de inscripción. Para obtener información más específica, vea Inscripción de dispositivos macOS.

> **TIP**
> Esta guía está en constante evolución. Así pues, no dude en agregar o actualizar las sugerencias e instrucciones existentes que le hayan parecido útiles.

Antes de empezar

Para obtener información general, incluidos los requisitos previos específicos de Intune, vea Guía de implementación: Inscripción de dispositivos en Microsoft Intune.

Inscripción de dispositivo automatizada (ADE) (supervisado)

Anteriormente llamado Programa de inscripción de dispositivos (DEP) de Apple. Úselo en dispositivos propiedad de su organización. Esta opción configura las opciones de configuración con Apple Business Manager (ABN) o Apple School Manager (ASM). Inscribe un gran número de dispositivos, sin necesidad de tocar los dispositivos. Estos dispositivos se adquieren en Apple, tienen sus opciones preconfiguradas y se pueden enviar directamente a usuarios o escuelas. Cree un perfil de inscripción en el centro de administración de Endpoint Manager e inserte este perfil en los dispositivos.

Para obtener información más específica sobre este tipo de inscripción, vea:

- Inscripción de Apple Business Manager
- Inscripción de Apple School Manager: para obtener más información sobre Apple School Manager, vea Educación de Apple (se abrirá un sitio web de Apple).

CARACTERÍSTICA	USAR ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Quiere el modo de supervisión.	✔ El modo supervisado implementa las actualizaciones de software, restringe características, permite y bloquea aplicaciones, etc.

CARACTERÍSTICA	USAR ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos pertenecen a la organización o centro educativo.	✔
Tiene nuevos dispositivos.	✔
Necesita inscribir un pequeño número de dispositivos, o bien un gran número de dispositivos (inscripción masiva).	✔
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos son sin usuario, como pantalla completa o un dispositivo dedicado.	✔
Los dispositivos son personales o BYOD.	✘ No se recomienda. Los dispositivos BYOD o personales deben inscribirse mediante MAM-WE (se abre otro artículo de Microsoft) o la inscripción de usuarios y dispositivos (cubierta en este artículo).
Tiene dispositivos existentes.	✘ Los dispositivos actuales deben inscribirse con Apple Configurator (cubierto en este artículo).
Los dispositivos los administra otra solución de MDM.	✘ Para que se administren completamente con Intune, los usuarios deben anular la inscripción del proveedor de MDM actual y, luego, inscribirlos en Intune. También puede usar MAM-WE para administrar aplicaciones específicas en el dispositivo. Dado que estos dispositivos son propiedad de la organización, recomendamos inscribirlos en Intune.
Usa la cuenta del administrador de inscripción de dispositivos (DEM).	✘ No se puede usar la cuenta DEM.

Tareas del administrador de ADE

Esta lista de tareas contiene información general. Para obtener información más específica, vea Inscripción de Apple Business Manager o Inscripción de Apple School Manager.

- Asegúrese de que los dispositivos son compatibles.
- Se necesita acceso al portal Apple Business Manager (ABM) o Apple School Manager (ASM).
- Asegúrese de que el token de Apple (.p7m) está activo. Para obtener información más específica, vea Obtención de un token de ADE de Apple.
- Asegúrese de que el Certificado push MDM de Apple se ha agregado a Endpoint Manager y está activo. Este certificado es necesario para inscribir dispositivos iOS/iPadOS. Para obtener más información, vea Obtener un certificado push MDM de Apple.
- Decida cómo se autenticarán los usuarios en sus dispositivos: la aplicación **Portal de empresa**, el **Asistente para la configuración (heredado)** o el **Setup Assistant with modern authentication**

(Asistente para la configuración con autenticación moderna) (versión preliminar pública). Tome esta decisión antes de crear el perfil de inscripción. El uso de la aplicación **Portal de empresa** o el **Setup Assistant with modern authentication** (Asistente para la configuración con autenticación moderna) forma parte de lo que se considera autenticación moderna.

- Seleccione la aplicación **Portal de empresa** en los siguientes casos:
  - Quiere borrar el dispositivo.
  - Quiere usar la autenticación multifactor (MFA).
  - Quiere pedir a los usuarios que actualicen la contraseña expirada la primera vez que inicien sesión.
  - Quiere pedir a los usuarios que restablezcan sus contraseñas expiradas durante la inscripción.
  - Quiere que los dispositivos se registren en Azure AD. Al registrarlos ahí, se pueden usar las características disponibles en Azure AD, como el acceso condicional.
  - Quiere instalar automáticamente la aplicación **Portal de empresa** durante la inscripción. Si la compañía usa el Programa de Compras por Volumen de Apple (VPP), puede instalar automáticamente la aplicación **Portal de empresa** durante la inscripción sin necesidad de usar los ID de Apple de los usuarios.
  - Quiere bloquear el dispositivo hasta que se instale la aplicación **Portal de empresa**. Una vez instalada, los usuarios inician sesión en ella con su cuenta de organización de Azure AD. Después, el dispositivo se desbloquea, y los usuarios pueden usarlo.
- Seleccione el **Asistente para la configuración (heredado)** en los siguientes casos:
  - Quiere borrar el dispositivo.
  - No quiere usar características de autenticación modernas, como MFA.
  - No quiere que los dispositivos se registren en Azure AD. El Asistente para la configuración (heredado) autentica al usuario con el token `.p7m` de Apple. Si se admite no registrar dispositivos en Azure AD, no es necesario instalar la aplicación Portal de empresa. Siga usando el Asistente para la configuración (heredado).

    Si quiere que los dispositivos estén registrados en Azure AD, instale la aplicación **Portal de empresa**. Al crear el perfil de inscripción y seleccionar el Asistente para la configuración (heredado), puede instalar la aplicación Portal de empresa. Recomendamos instalar la aplicación **Portal de empresa** durante la inscripción.
- Seleccione el **Setup Assistant with modern authentication** (Asistente para la configuración con autenticación moderna) en los siguientes casos:
  - Quiere borrar el dispositivo.
  - Quiere usar la autenticación multifactor (MFA).
  - Quiere pedir a los usuarios que actualicen la contraseña expirada la primera vez que inicien sesión.
  - Quiere pedir a los usuarios que restablezcan sus contraseñas expiradas durante la inscripción.
  - Quiere que los dispositivos se registren en Azure AD. Al registrarlos ahí, se pueden usar las características disponibles en Azure AD, como el acceso condicional.
  - Quiere instalar automáticamente la aplicación **Portal de empresa** durante la inscripción. Si la compañía usa el Programa de Compras por Volumen de Apple (VPP), puede instalar automáticamente la aplicación **Portal de empresa** durante la inscripción sin necesidad de usar los ID de Apple de los usuarios.
  - Quiere que los usuarios usen el dispositivo, incluso cuando la aplicación Portal de empresa no esté instalada.

> **NOTE**
>
> Para autenticar a los usuarios, Microsoft recomienda usar la aplicación **Portal de empresa** o el **Setup Assistant with modern authentication** (Asistente para la configuración con autenticación moderna).
>
> ¿Qué opción debería usar? Depende de lo siguiente:
>
> - Si quiere usar el dispositivo antes de que se instale la aplicación Portal de empresa, use el **Setup Assistant with modern authentication** (Asistente para la configuración con autenticación moderna).
>
> Durante el Asistente de configuración, los usuarios deben especificar las credenciales de su organización de Azure AD (`user@contoso.com`). Tras especificar las credenciales, se inicia la inscripción y se instala la aplicación Portal de empresa. Si así lo quiere, los usuarios también pueden especificar su ID de Apple para acceder a características específicas de esta empresa, como Apple Pay.
>
> Una vez completado el Asistente de configuración, los usuarios pueden usar el dispositivo. Cuando se muestra la pantalla principal, la inscripción está completada y se ha establecido la afinidad de usuario. El dispositivo no está totalmente registrado en Azure AD y no aparece en la lista de dispositivos de un usuario en Azure AD.
>
> Tras instalar la aplicación Portal de empresa, un proceso que tarda un tiempo, los usuarios la abren y vuelven a iniciar sesión con las credenciales de su organización de Azure AD (`user@contoso.com`). Durante este segundo inicio de sesión, se evalúan las directivas de acceso condicional y el registro de Azure AD se completa. Los usuarios pueden instalar y usar los recursos de la organización, incluidas las aplicaciones de línea de negocio.
>
> - Elija la opción de la aplicación **Portal de empresa** si no quiere usar el dispositivo antes de que se instale. Con la opción de la aplicación **Portal de empresa**, se bloquea el dispositivo hasta la instalación de esta. Cuando se completa la instalación, la aplicación Portal de empresa se abre automáticamente. Los usuarios inician sesión con la cuenta de su organización de Azure AD (`user@contoso.com`) y pueden usar el dispositivo.

- Si usa la aplicación Portal de empresa, decida cómo se va a instalar en los dispositivos. Tome esta decisión antes de crear el perfil de inscripción.

  > **NOTE**
  >
  > Microsoft recomienda usar el Programa de Compras por Volumen de Apple (VPP) cuando se utiliza la aplicación Portal de empresa para la autenticación. ya que proporciona una mejor experiencia de usuario final.

  No instale la aplicación Portal de empresa desde la tienda de aplicaciones directamente en los dispositivos inscritos con ADE; instálela mejor con una de las siguientes opciones:

  - **Token de VPP + inscripción de nuevos dispositivos**: si tiene el Programa de Compras por Volumen de Apple (VPP) y está inscribiendo nuevos dispositivos, la aplicación Portal de empresa estará incluida. Cuando cree el perfil de inscripción en el centro de administración de Endpoint Manager, seleccione **Instalar Portal de empresa con VPP**. No es necesario ningún paso más.

    Esta opción:

    - Incluye la versión correcta de la aplicación Portal de empresa.
    - No tiene que crear otra directiva para implementar la aplicación Portal de empresa en los dispositivos.
    - La actualización de la aplicación Portal de empresa deberá ser manual y correrá a su cargo o de los usuarios.
  - **Sin token de VPP + inscripción de nuevos dispositivos**: no hay tareas del administrador. Asegúrese de que los usuarios indican su identificador de Apple en el Asistente para la instalación.

Cuando el Asistente para la instalación finalice, la aplicación Portal de empresa intenta instalarse automáticamente. Si los usuarios no especifican su identificador de Apple (`user@iCloud.com` o `user@gmail.com`), se les pedirá constantemente que lo hagan. Deben especificarlo para tener la aplicación Portal de empresa en sus dispositivos. Cuando la aplicación Portal de empresa se instala, los usuarios la abren y escriben sus credenciales de la organización (`user@contoso.com`). Cuando se autentican, los usuarios pueden instalar y usar las aplicaciones usadas en la organización, incluidas las aplicaciones de línea de negocio.

- **Dispositivos ya inscritos**: si los dispositivos ya están inscritos (con o sin VPP), use una directiva de configuración de aplicaciones:

  1. En el centro de administración de Endpoint Manager, agregue la aplicación Portal de empresa como una aplicación necesaria y como una aplicación con licencia de dispositivo.
  2. Cree una directiva de configuración de aplicaciones que incluya la aplicación Portal de empresa como aplicación con licencia de dispositivo. Para obtener información más específica, vea Configuración de la aplicación Portal de empresa para que admita dispositivos iOS e iPadOS de DEP.
  3. Implemente la directiva de configuración de aplicaciones en el mismo grupo de dispositivos que el perfil de inscripción.
  4. Cuando los dispositivos se registran con el servicio de Intune, reciben su perfil y la aplicación Portal de empresa se instala.

  Esta opción:

  - Incluye la versión correcta de la aplicación Portal de empresa.
  - Requiere crear un perfil de inscripción y una directiva de configuración de aplicaciones. En la directiva de configuración de aplicaciones, establezca Portal de empresa como una aplicación necesaria para que sepa que se implementa en todos los dispositivos.
  - La aplicación Portal de empresa se puede actualizar automáticamente cambiando la directiva de configuración de aplicaciones existente.

- En el centro de administración de Endpoint Manager, cree un perfil de inscripción:

  - Elija **Inscribir con afinidad de usuario** (asociar un usuario al dispositivo) o **Inscribir sin afinidad de usuario** (dispositivos sin usuario o compartidos).
  - Elija dónde deben autenticarse los usuarios: la aplicación **Portal de empresa**, el **Asistente para la configuración (heredado)** o el **Setup Assistant with modern authentication** (Asistente para la configuración con autenticación moderna).

  Para obtener información y sugerencias más específicas, vea Inscripción de dispositivos automatizada de Apple.

Tareas del usuario final de ADE

Cuando cree un perfil de inscripción en el centro de administración de Endpoint Manager, elija asociar un usuario al dispositivo (**Inscribir con afinidad de usuario**) o que los dispositivos se compartan (**Inscribir sin afinidad de usuario**). Los pasos específicos dependen de cómo se haya configurado el perfil de inscripción.

- **Inscripción con afinidad de usuario + aplicación Portal de empresa**:

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican su identificador de Apple (`user@iCloud.com` o `user@gmail.com`). Tras especificarlo, la aplicación Portal de empresa se instala automáticamente desde el perfil de inscripción. La aplicación Portal de empresa puede tardar algo de tiempo en instalarse automáticamente.
  2. Los usuarios abren la aplicación Portal de empresa e inician sesión con sus credenciales de la organización (`user@contoso.com`). Tras iniciar sesión, arranca el proceso de inscripción. Cuando la inscripción finalice, los usuarios pueden instalar y usar las aplicaciones usadas en la organización,

incluidas las aplicaciones de línea de negocio.

Es posible que los usuarios tengan que especificar más información. Para conocer el procedimiento en mayor profundidad, vea Inscripción de un dispositivo con iOS proporcionado por la organización.

- **Inscripción con afinidad de usuario + Asistente para la configuración (heredado) + aplicación Portal de empresa**:

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican su identificador de Apple (`user@iCloud.com` o `user@gmail.com`).
  2. El Asistente para la instalación solicita información al usuario.
  3. La aplicación Portal de empresa se abre automáticamente y debe bloquear el dispositivo en un modo de tipo pantalla completa. La aplicación Portal de empresa puede tardar algo de tiempo en abrirse. Los usuarios inician sesión con sus credenciales de la organización (`user@contoso.com`) y el dispositivo se inscribe en Intune.

     En este paso, el dispositivo se registra en Azure AD. Los usuarios pueden instalar y usar las aplicaciones usadas en la organización, incluidas las aplicaciones de línea de negocio.

- **Inscripción con afinidad de usuario + Asistente para la configuración (heredado) - aplicación Portal de empresa**:

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican su identificador de Apple (`user@iCloud.com` o `user@gmail.com`).
  2. El Asistente para la instalación solicita información al usuario e inscribe el dispositivo en Intune. El dispositivo no está registrado en Azure AD.

- **Inscripción con afinidad de usuario + Setup Assistant with modern authentication (Asistente para la configuración con autenticación moderna) + aplicación Portal de empresa**:

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican su ID de Apple (`user@iCloud.com` o `user@gmail.com`) y las credenciales de su organización de Azure AD (`user@contoso.com`).

     Cuando los usuarios especifican sus credenciales de Azure AD, se inicia la inscripción.
  2. El Asistente de configuración solicita información adicional al usuario. Tras completar el proceso, los usuarios pueden usar el dispositivo. Cuando se muestra la pantalla principal, la inscripción está completada. Los usuarios verán las aplicaciones y directivas en el dispositivo.
  3. La aplicación Portal de empresa se instala automáticamente; este proceso tarda un tiempo. Los usuarios abren la aplicación Portal de empresa y vuelven a iniciar sesión con las credenciales de su organización (`user@contoso.com`).

- **Inscripción con afinidad de usuario + Setup Assistant with modern authentication (Asistente para la configuración con autenticación moderna) - aplicación Portal de empresa**:

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican su ID de Apple (`user@iCloud.com` o `user@gmail.com`) y las credenciales de su organización de Azure AD.

     Cuando los usuarios especifican sus credenciales de Azure AD, se inicia la inscripción.
  2. El Asistente de configuración solicita información adicional al usuario. Tras completar el proceso, los usuarios pueden usar el dispositivo. Cuando se muestra la pantalla principal, la inscripción está completada. Los usuarios verán las aplicaciones y directivas en el dispositivo.
  3. La aplicación Portal de empresa se instala automáticamente. Los usuarios no necesitan abrir la

aplicación Portal de empresa ni iniciar sesión en ella. Si no inician sesión, el dispositivo no se registra en Azure AD y no aparece en la lista de dispositivos de un usuario en Azure AD. Los recursos que dependen del acceso condicional no están disponibles.

- **Inscripción sin afinidad de usuario**: no hay acciones. Asegúrese de que la aplicación Portal de empresa no se instala desde la App Store de Apple.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

Inscribir Apple Configurator

Se usa en los dispositivos propiedad de la organización, e incluye la inscripción directa. Esta opción requiere conectar los dispositivos macOS físicamente a un equipo Mac a través de un puerto USB.

Para obtener información más específica sobre este tipo de inscripción, vea Inscripción de Apple Configurator.

CARACTERÍSTICA	USAR ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Necesita una conexión con cable o tiene un problema de red.	✔
Su organización no quiere que los administradores usen los portales de ABN o ASM, o bien no quiere configurar todos los requisitos.	✔ Lo que se pretende al *no* permitir el uso de los portales de ABN o ASM es que los administradores tengan menos control.
Un país no admite el uso de Apple Business Manager (ABN) o Apple School Manager (ASM).	✔ Si su país admite el uso de ABS o ASM, lo más aconsejable es que los dispositivos se inscriban con la inscripción automática de dispositivos.
Los dispositivos pertenecen a la organización o centro educativo.	✔
Tiene dispositivos nuevos o existentes.	✔
Necesita inscribir un pequeño número de dispositivos, o bien un gran número de dispositivos (inscripción masiva).	✔ Si tiene una gran cantidad de dispositivos, este método tardará un tiempo.
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos son sin usuario, como pantalla completa o un dispositivo dedicado.	✔
Los dispositivos son personales o BYOD.	✘ No se recomienda. Los dispositivos BYOD o personales deben inscribirse mediante MAM-WE (se abre otro artículo de Microsoft) o la inscripción de usuarios y dispositivos (cubierta en este artículo).

CARACTERÍSTICA	USAR ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos los administra otra solución de MDM.	✕ Para que se administren completamente con Intune, los usuarios deben anular la inscripción del proveedor de MDM actual y, luego, inscribirlos en Intune. También puede usar MAM-WE para administrar aplicaciones específicas en el dispositivo. Dado que estos dispositivos son propiedad de la organización, recomendamos inscribirlos en Intune.
Usa la cuenta del administrador de inscripción de dispositivos (DEM).	✕ No se puede usar la cuenta DEM.

Tareas de administrador de Apple Configurator

Esta lista de tareas contiene información general. Para obtener información más específica, vea Inscripción de Apple Configurator.

- Se necesita acceso a un equipo Mac con un puerto USB.
- Asegúrese de que los dispositivos son compatibles.
- Asegúrese de que el Certificado push MDM de Apple se ha agregado a Endpoint Manager y está activo. Este certificado es necesario para inscribir dispositivos iOS/iPadOS. Para obtener más información, vea Obtener un certificado push MDM de Apple.
- Decida cómo se autenticarán los usuarios en sus dispositivos: mediante la aplicación **Portal de empresa** o el **Asistente para la instalación**. Tome esta decisión antes de crear el perfil de inscripción. El uso de la aplicación Portal de empresa se considera autenticación moderna. Recomendamos usar la aplicación Portal de empresa.
  - Seleccione la aplicación **Portal de empresa** en los siguientes casos:
    - Quiere usar la autenticación multifactor (MFA).
    - Quiere pedir a los usuarios que actualicen la contraseña expirada la primera vez que inicien sesión.
    - Quiere pedir a los usuarios que restablezcan sus contraseñas expiradas durante la inscripción.
    - Quiere que los dispositivos se registren en Azure AD. Al registrarlos ahí, se pueden usar las características disponibles en Azure AD, como el acceso condicional.
    - Quiere instalar automáticamente la aplicación **Portal de empresa** durante la inscripción. Si la compañía usa el Programa de Compras por Volumen de Apple (VPP), puede instalar automáticamente la aplicación **Portal de empresa** durante la inscripción.
  - Seleccione el **Asistente para la instalación** en los siguientes casos:
    - No quiere usar características de autenticación modernas, como MFA.
    - Quiere borrar el dispositivo.
    - Quiere importar los números de serie.
    - No quiere que los dispositivos se registren en Azure AD. El Asistente para la instalación autentica al usuario con el perfil de inscripción exportado que se haya copiado en el dispositivo. Si se admite no registrar dispositivos en Azure AD, no es necesario instalar la aplicación Portal de empresa. Siga usando el Asistente para la instalación.

      Si quiere que los dispositivos estén registrados en Azure AD, instale la aplicación **Portal de**

empresa. Al crear el perfil de inscripción y seleccionar el Asistente para la instalación, puede instalar la aplicación Portal de empresa. Recomendamos instalar la aplicación **Portal de empresa** durante la inscripción.

- Si usa la aplicación Portal de empresa, esta se debe instalar en los dispositivos con una directiva de configuración de aplicaciones. Se recomienda crear esta directiva antes de crear el perfil de inscripción.

  No instale la aplicación Portal de empresa desde la tienda de aplicaciones directamente en los dispositivos inscritos con Apple Configurator; instálela mejor con una de las siguientes opciones:

  - **Inscripción de nuevos dispositivos**: no hay tareas del administrador. Asegúrese de que los usuarios indican su identificador de Apple en el Asistente para la instalación.

    Cuando el Asistente para la instalación finalice, la aplicación Portal de empresa intenta instalarse automáticamente. Si los usuarios no especifican su identificador de Apple (`user@iCloud.com` o `user@gmail.com`), se les pedirá constantemente que lo hagan. Deben especificarlo para tener la aplicación Portal de empresa en sus dispositivos. Cuando la aplicación Portal de empresa se instala, los usuarios la abren y escriben sus credenciales de la organización (`user@contoso.com`). Cuando se autentican, los usuarios pueden instalar y usar las aplicaciones usadas en la organización, incluidas las aplicaciones de línea de negocio.

  - **Dispositivos ya inscritos**: si los dispositivos ya están inscritos, use una directiva de configuración de aplicaciones:

    1. En el centro de administración de Endpoint Manager, agregue la aplicación Portal de empresa como una aplicación necesaria y como una aplicación con licencia de dispositivo.
    2. Cree una directiva de configuración de aplicaciones que incluya la aplicación Portal de empresa como aplicación con licencia de dispositivo. Para obtener información más específica, vea Configuración de la aplicación Portal de empresa para que admita dispositivos iOS e iPadOS de DEP.
    3. Implemente la directiva de configuración de aplicaciones en el mismo grupo de dispositivos que el perfil de inscripción.
    4. Cuando los dispositivos se registran con el servicio de Intune, reciben su perfil y la aplicación Portal de empresa se instala.

    Esta opción:

    - Incluye la versión correcta de la aplicación Portal de empresa.
    - Requiere crear un perfil de inscripción y una directiva de configuración de aplicaciones. En la directiva de configuración de aplicaciones, establezca Portal de empresa como una aplicación necesaria para que sepa que se implementa en todos los dispositivos.
    - La aplicación Portal de empresa se puede actualizar automáticamente cambiando la directiva de configuración de aplicaciones existente.

- En el centro de administración de Endpoint Manager, cree un perfil de inscripción:

  - Elija **Inscribir con afinidad de usuario** (asociar un usuario al dispositivo) o **Inscribir sin afinidad de usuario** (dispositivos sin usuario o compartidos).

  - Si elige **Inscribir sin afinidad de usuario**, se usará automáticamente la **inscripción directa**. Recuerde:

    - Está usando la configuración de un perfil de inscripción de macOS existente.
    - Los usuarios no pueden usar aplicaciones que requieran un usuario, incluida la aplicación Portal de empresa. La aplicación Portal de empresa no se usa y no es necesaria ni compatible con las inscripciones sin afinidad de usuario. Asegúrese de que la aplicación Portal de empresa no se instala desde la App Store de Apple.

- Cuando el perfil de inscripción esté listo, conecte los dispositivos al equipo Mac a través de un puerto USB y abra la aplicación **Apple Configurator**. Al abrirla, detecta el dispositivo conectado al puerto USB e implementa el perfil de inscripción de Intune que ha creado.

Para obtener más información sobre esta opción de inscripción y los requisitos previos correspondientes, vea Inscripción de Apple Configurator.

Tareas de usuario final de Apple Configurator

Las tareas dependen de la opción que se haya configurado en el perfil de inscripción.

- **Inscripción con afinidad de usuario + aplicación Portal de empresa**:

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican su identificador de Apple (`user@iCloud.com` o `user@gmail.com`). Tras especificarlo, la aplicación Portal de empresa se instala automáticamente desde la tienda de aplicaciones. La aplicación Portal de empresa puede tardar algo de tiempo en instalarse automáticamente.
  2. Abra la aplicación Portal de empresa e inicie sesión con sus credenciales de organización (`user@contoso.com`). Tras iniciar sesión, arranca el proceso de inscripción. Cuando la inscripción finalice, los usuarios pueden instalar y usar las aplicaciones usadas en la organización, incluidas las aplicaciones de línea de negocio.

  Es posible que los usuarios tengan que especificar más información. Para conocer el procedimiento más detalladamente, vea Inscripción de un dispositivo iOS proporcionado por la organización.

- **Inscripción con afinidad de usuario +Asistente para la instalación + aplicación Portal de empresa**:

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican sus credenciales de la organización (`user@contoso.com`). Durante este paso, el dispositivo se inscribe en Intune.
  2. El Asistente para la instalación solicita información al usuario, incluido el identificador de Apple (`user@iCloud.com` o `user@gmail.com`).
  3. La aplicación Portal de empresa se instala automáticamente desde la tienda de aplicaciones. Los usuarios abren la aplicación Portal de empresa e inician sesión con sus credenciales de la organización (`user@contoso.com`). En este paso, el dispositivo se registra en Azure AD. Los usuarios pueden instalar y usar las aplicaciones usadas en la organización, incluidas las aplicaciones de línea de negocio.
- **Inscripción con afinidad de usuario +Asistente para la instalación - aplicación Portal de empresa**:

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican sus credenciales de la organización (`user@contoso.com`). Durante este paso, el dispositivo se inscribe en Intune.
  2. El Asistente para la instalación solicita información al usuario, incluido el identificador de Apple (`user@iCloud.com` o `user@gmail.com`). Durante este paso, el perfil de administración de Intune se envía al dispositivo.
  3. Los usuarios instalan el perfil de administración. El perfil se registra en el servicio de Intune e inscribe el dispositivo. El dispositivo no está registrado en Azure AD.
- **Inscripción sin afinidad de usuario**: se usa la inscripción directa. Ninguna acción. Asegúrese de que la aplicación Portal de empresa no se instala desde la App Store de Apple.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

BYOD: Inscripción de usuarios y dispositivos

Estos dispositivos iOS/iPadOS son dispositivos personales o BYOD (Bring Your Own Device) con acceso al correo electrónico, las aplicaciones y otros datos de la organización. A partir de iOS 13 y versiones más recientes, esta opción de inscripción se dirige bien a los usuarios, bien a los dispositivos. No es necesario restablecer los dispositivos.

Al crear el perfil de inscripción, se le pedirá que elija **Inscripción de usuario**, **Inscripción de dispositivos** o **Determinar según la elección del usuario**.

Para conocer los pasos de inscripción específicos y los requisitos previos correspondientes, vea Configuración de la Inscripción de usuario de iOS/iPadOS y iPadOS.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos son personales o BYOD.	✔
Quiere ayudar a proteger una característica específica en el dispositivo, como VPN por aplicación.	✔
Tiene dispositivos nuevos o existentes.	✔
Necesita inscribir un pequeño número de dispositivos, o bien un gran número de dispositivos (inscripción masiva).	✔
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos los administra otra solución de MDM.	✕ Cuando se inscribe un dispositivo, los proveedores de MDM instalan certificados y otros archivos. Estos archivos se deben quitar. La forma más rápida puede consistir en la anulación de la inscripción o el restablecimiento de fábrica de los dispositivos. Si no quiere llevar a cabo el restablecimiento de fábrica, póngase en contacto con el proveedor de MDM.
Usa la cuenta del administrador de inscripción de dispositivos (DEM).	✔
Los dispositivos pertenecen a la organización o la escuela.	✕ No se recomienda. Los dispositivos que son propiedad de la organización debe inscribirse con el perfil Inscripción de dispositivos automatizada (cubierto en este artículo) o Apple Configurator (también cubierto en este artículo).
Los dispositivos son sin usuario, como pantalla completa o un dispositivo dedicado.	✕ Normalmente, los dispositivos sin usuario o compartidos son propiedad de la organización. Estos dispositivos deben inscribirse con el perfil Inscripción de dispositivos automatizada (cubierto en este artículo) o Apple Configurator (cubierto en este artículo).

Tareas del administrador de inscripción de usuario y de dispositivo

Esta lista de tareas contiene información general. Para obtener información más específica, vea Configuración de

la Inscripción de usuario de iOS/iPadOS y iPadOS.

- Asegúrese de que los dispositivos son compatibles.
- Asegúrese de que el Certificado push MDM de Apple se ha agregado a Endpoint Manager y está activo. Este certificado es necesario para inscribir dispositivos iOS/iPadOS. Para obtener más información, vea Obtener un certificado push MDM de Apple.
- En el centro de administración de Endpoint Manager, cree el perfil de inscripción. Al crearlo, dispone de las siguientes opciones:
  - **Inscripción de dispositivos**: esta opción es una inscripción típica de los dispositivos personales. Se administra el dispositivo, no solo características o aplicaciones concretas. Al usar esta opción, tenga en cuenta lo siguiente:
    - Puede implementar certificados que se apliquen a todo el dispositivo.
    - Los usuarios deben instalar las actualizaciones. Solo los dispositivos inscritos con la inscripción de dispositivos automatizada (ADE) pueden recibir actualizaciones a través de perfiles o directivas de MDM.
    - Debe haber un usuario asociado al dispositivo. Este usuario puede ser una cuenta de administrador de inscripción de dispositivos (DEM).
  - **Determinar según la opción del usuario**: se ofrece una opción a los usuarios finales cuando se inscriben. En función de su elección, se usa **Inscripción de usuario** o **Inscripción de dispositivos**.
  - **Inscripción de usuarios**: a partir de iOS 13 y versiones más recientes. Con esta opción se configura un conjunto específico de características y aplicaciones de la organización, como una contraseña, VPN por aplicación, Wi-Fi y Siri. Si se usa la inscripción de usuario, y a fin de ayudar a proteger las aplicaciones y sus datos, recomendamos usar también directivas de protección de aplicaciones.

    Para obtener una lista completa de lo que se puede y no se puede hacer, vea Acciones y opciones de Intune compatibles con la inscripción de usuarios de Apple. Para conocer el procedimiento detallado de inscripción de usuarios, vea Configuración de la Inscripción de usuario de iOS/iPadOS y iPadOS.

    > **NOTE**
    > Los dispositivos BYOD pueden pasar a ser dispositivos propiedad de la organización. Para hacer que estos dispositivos sean corporativos, vea Identificar dispositivos como corporativos.

    La inscripción de usuario se considera más sencilla de realizar para los usuarios finales, pero puede que no proporcione el conjunto de características ni las características de seguridad que los administradores necesitan. En algunos casos, puede que la inscripción de usuario no sea la mejor opción. Considere los siguientes escenarios:

    - La inscripción de usuario crea una partición de trabajo en los dispositivos. Las características y la seguridad configuradas en el perfil de inscripción de usuario existen solamente en la partición de trabajo. No existirán en la partición de usuario. Los usuarios no podrán restablecer la partición de trabajo a los valores de fábrica, pero sí los administradores. Los usuarios podrán restablecer su partición personal a los valores de fábrica, pero no los administradores.
    - Si los usuarios usan eminentemente aplicaciones de Microsoft o aplicaciones creadas con el SDK de aplicaciones de Intune, deberán descargar esas aplicaciones desde el App Store de

Apple. Después, se deben usar directivas de protección de aplicaciones para proteger esas aplicaciones. En este caso, no se necesita la inscripción de usuario.

  - En cuanto a las aplicaciones de línea de negocio, la inscripción de usuario puede ser una opción, ya que implementará estas aplicaciones en la partición de trabajo. La administración de aplicaciones (MAM) no admite aplicaciones de línea de negocio, de modo que si se necesitan este tipo de aplicaciones, use la inscripción de usuario.

  - Si los dispositivos están inscritos con la inscripción de usuario, no se podrá cambiar a inscripción de dispositivos. Con la inscripción de usuario, una aplicación no puede cambiar de no administrada a administrada. Los usuarios deberán anular la inscripción de usuario y volver a inscribirse con la inscripción de dispositivos.

  - Si instala aplicaciones antes de aplicar el perfil de inscripción de usuarios, este no las protegerá ni administrará.

    Por ejemplo, un usuario descarga la aplicación Outlook desde el App Store de Apple. La aplicación se instala automáticamente en la partición de usuario en el dispositivo. El usuario configura Outlook como correo electrónico personal. Al configurar su correo electrónico de la organización, el acceso condicional se lo impide y le pide que se inscriba. Se inscribe, y se implementa un perfil de inscripción de usuario.

    Como la aplicación Outlook se instaló antes que el perfil de inscripción de usuario, se produce un error en el perfil de inscripción de usuario. La aplicación Outlook no se puede administrar porque está instalada y configurada en la partición de usuario, y no en la partición de trabajo. La aplicación Outlook se deberá desinstalar manualmente.

    Una vez desinstalado, el usuario puede sincronizar el dispositivo manualmente y, posiblemente, volver a aplicar el perfil de inscripción de usuario. También puede que haya que crear una directiva de configuración de aplicaciones para implementar Outlook y convertirla en una aplicación requerida. Tras ello, implemente una directiva de protección de aplicaciones para proteger la aplicación y sus datos.

- Asigne el perfil de inscripción a grupos de usuarios, no a grupos de dispositivos.

Tareas del usuario final de inscripción de usuario y de dispositivo

Los usuarios deben realizar los pasos siguientes. Para obtener más información sobre la experiencia de usuario, vea Inscribir dispositivos.

1. Vaya al App Store de Apple e instale la aplicación Portal de empresa de Intune.
2. Abra la aplicación Portal de empresa e inicie sesión con sus credenciales de organización (`user@contoso.com`). Tras iniciar sesión, el perfil de inscripción se aplica al dispositivo.

   Es posible que los usuarios tengan que especificar más información. Para conocer el procedimiento más detalladamente, vea Inscribir dispositivos.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

> **TIP**
> Hay un vídeo breve con instrucciones paso a paso para ayudar a los usuarios a inscribir sus dispositivos en Intune:
>
> Inscripción de dispositivos iOS/iPadOS

Pasos siguientes

- MAM-WE
- Guía de inscripción de Android
- Guía de inscripción de macOS
- Guía de inscripción de Windows

Guía de implementación: Inscripción de dispositivos macOS en Microsoft Intune

14/05/2021 • 12 minutes to read

Los dispositivos personales y propiedad de la organización se pueden inscribir en Intune. En los dispositivos macOS, la aplicación Portal de empresa o el Asistente para la instalación de Apple autentica a los usuarios e inicia la inscripción. Una vez que están inscritos, reciben las directivas y los perfiles que se crean.

Al inscribir dispositivos macOS, dispone de las opciones siguientes:

- BYOD: inscripción de dispositivos
- Inscripción de dispositivos automatizada (ADE)

> **NOTE**
> La inscripción mediante Apple Configurator está disponible para dispositivos iOS/iPadOS. Sin embargo, no está disponible para dispositivos macOS. Cuando se crea un perfil de inscripción de macOS, Apple Configurator aparece como opción. Este comportamiento es un problema conocido y se corregirá en una versión futura (sin ETA). No cree un perfil de inscripción de macOS con Apple Configurator. No funciona.

En este artículo:

- Se describen las opciones de la aplicación Portal de empresa para cada método de inscripción.
- Se proporcionan recomendaciones sobre el método de inscripción de macOS que se va a usar.
- Se incluye información general de las tareas del administrador y el usuario final para cada tipo de inscripción.

Para obtener información más específica, vea Inscripción de dispositivos macOS.

> **TIP**
> Esta guía está en constante evolución. Así pues, no dude en agregar o actualizar las sugerencias e instrucciones existentes que le hayan parecido útiles.

Antes de empezar

Para obtener información general, incluidos los requisitos previos específicos de Intune, vea Guía de implementación: Inscripción de dispositivos en Microsoft Intune.

BYOD: Inscripción de dispositivos

Úsela para dispositivos personales o BYOD. No es un método tradicional de "inscripción", ya que usa un perfil de configuración de aplicaciones. Esta opción administra las aplicaciones en el dispositivo. Los dispositivos no se inscriben.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos son personales o BYOD.	✔

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Necesita inscribir un pequeño número de dispositivos, o bien un gran número de dispositivos (inscripción masiva).	✔
Tiene dispositivos nuevos o existentes.	✔
Los dispositivos están asociados a un único usuario.	✔
Usa la cuenta del administrador de inscripción de dispositivos (DEM).	✔ Tenga en cuenta el impacto y las limitaciones con la cuenta DEM.
Los dispositivos los administra otra solución de MDM.	✘ Cuando se inscribe un dispositivo, los proveedores de MDM instalan certificados y otros archivos. Estos archivos se deben quitar. La forma más rápida puede consistir en la anulación de la inscripción o el restablecimiento de fábrica de los dispositivos. Si no quiere llevar a cabo el restablecimiento de fábrica, póngase en contacto con el proveedor de MDM.
Los dispositivos pertenecen a la organización o la escuela.	✘ No recomendado en el caso de los dispositivos propiedad de la organización. Los dispositivos que son propiedad de la organización debe inscribirse con el perfil Inscripción de dispositivos automatizada (cubierto en este artículo) o Apple Configurator. Puede agregar los números de serie de MacBook a los identificadores de dispositivos corporativos para marcar los dispositivos como corporativos. No obstante, de forma predeterminada los dispositivos están marcados como personales.
Los dispositivos son sin usuario como, por ejemplo, pantalla completa, dedicado o compartido.	✘ Estos dispositivos son propiedad de la organización. Los dispositivos sin usuario deben inscribirse con el perfil Inscripción de dispositivos automatizada (cubierto en este artículo) o Apple Configurator.

Tareas del administrador de inscripción de dispositivos

Esta lista de tareas proporciona información general.

- Asegúrese de que los dispositivos sean compatibles.
- Asegúrese de que el Certificado push MDM de Apple se agrega a Endpoint Manager y está activo. Este certificado es necesario para inscribir dispositivos macOS. Para obtener más información, vea Obtener un certificado push MDM de Apple.
- No existe una aplicación Portal de empresa para dispositivos macOS en el App Store de Apple o a través de VPP. Los usuarios deben descargar y ejecutar manualmente el paquete del instalador de la aplicación Portal de empresa. Inician sesión con su cuenta de organización (`user@contoso.com`) y, después, recorren la inscripción paso a paso. Una vez que se inscriben, deben aprobar el perfil de inscripción.

Cuando lo aprueban, el dispositivo se agrega al servicio Azure AD de la organización. Después, está disponible en Intune para recibir las directivas y los perfiles.

Asegúrese de comunicar esta información con los usuarios.

Tareas del usuario final de inscripción de dispositivos

Los usuarios deben realizar los pasos siguientes. Para obtener información más específica acerca de los pasos de usuario final, vea Inscripción de un dispositivo macOS con Portal de empresa.

1. Descargue y ejecute el paquete del instalador de la aplicación Portal de empresa.
2. Abra la aplicación Portal de empresa e inicie sesión con su cuenta de organización (`user@contoso.com`). Una vez que inicien sesión, deben aprobar el perfil de inscripción (preferencias del sistema). Cuando los usuarios lo aprueban, el dispositivo se inscribe y se considera administrado. Si no lo aprueban, no se inscriben y no recibirán la directiva y los perfiles.

Para obtener información más específica acerca de los pasos de usuario final, vea Inscripción de un dispositivo macOS con Portal de empresa.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

Inscripción de dispositivo automatizada (ADE) (supervisado)

Anteriormente llamado Programa de inscripción de dispositivos (DEP) de Apple. Úselo en dispositivos propiedad de su organización. Esta opción configura las opciones de configuración con Apple Business Manager (ABN) o Apple School Manager (ASM). Inscribe un gran número de dispositivos, sin necesidad de tocar los dispositivos. Estos dispositivos se adquieren en Apple, tienen sus opciones preconfiguradas y se pueden enviar directamente a usuarios o escuelas. Cree un perfil de inscripción en el centro de administración de Endpoint Manager e inserte este perfil en los dispositivos.

Para obtener información específica sobre este tipo de inscripción, vea Inscripción automática de dispositivos macOS con Apple Business Manager o Apple School Manager.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos pertenecen a la organización o la escuela.	✔
Tiene nuevos dispositivos.	✔
Tiene dispositivos existentes.	✔ Para inscribir dispositivos existentes, vea Inscripción del dispositivo macOS registrado en ABN/ASM con la inscripción de dispositivo automatizada después del Asistente para la configuración (se abre otro artículo de Microsoft).
Necesita inscribir un pequeño número de dispositivos, o bien un gran número de dispositivos (inscripción masiva).	✔
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos son sin usuario, como pantalla completa o un dispositivo dedicado.	✔

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos son personales o BYOD.	✕ No se recomienda. Los dispositivos BYOD o personales deben inscribirse con la inscripción de dispositivos (cubierto en este artículo).
Los dispositivos los administra otra solución de MDM.	✕ Para estar totalmente administrado por parte de Intune, los usuarios deben anular la inscripción del proveedor de MDM actual y luego inscribirse en Intune. También puede usar la inscripción de dispositivos para administrar aplicaciones específicas en el dispositivo. Dado que estos dispositivos son propiedad de la organización, se recomienda inscribirse en Intune.
Usa la cuenta del administrador de inscripción de dispositivos (DEM).	✕ No se puede usar la cuenta DEM.

Tareas del administrador de ADE

Esta lista de tareas proporciona información general. Para obtener información específica, vea Inscripción automática de dispositivos macOS con Apple Business Manager o Apple School Manager.

- Asegúrese de que los dispositivos sean compatibles.
- Se necesita acceso al portal Apple Business Manager (ABM) o Apple School Manager (ASM).
- Asegúrese de que el token de Apple (.p7m) está activo. Para obtener información más específica, vea Obtención de un token de ADE de Apple.
- Asegúrese de que el Certificado push MDM de Apple se agrega a Endpoint Manager y está activo. Este certificado es necesario para inscribir dispositivos macOS. Para obtener más información, vea Obtener un certificado push MDM de Apple.
- Decida cómo se autenticarán los usuarios en sus dispositivos: **Asistente para la configuración (heredado)** o **Asistente para la configuración con autenticación moderna** (versión preliminar pública). Tome esta decisión antes de crear el perfil de inscripción. El uso del **Asistente para la configuración con autenticación moderna** se considera autenticación moderna. Microsoft recomienda usar el **Asistente para la configuración con autenticación moderna**.

  En todos los dispositivos macOS propiedad de la organización, el **Asistente para la instalación (heredado)** se usa siempre y de forma automática, incluso si no ve el texto "Asistente para la configuración" en Endpoint Manager. El Asistente para la configuración (heredado) autentica al usuario e inscribe el dispositivo.

  - Seleccione el **Asistente para la configuración (heredado)** en los siguientes casos:
    - Quiere borrar el dispositivo.
    - No quiere usar características de autenticación modernas, como MFA.
    - No quiere que los dispositivos se registren en Azure AD. El Asistente para la configuración (heredado) autentica al usuario con el token `.p7m` de Apple. Si se admite no registrar dispositivos en Azure AD, no es necesario instalar la aplicación Portal de empresa. Siga usando el Asistente para la configuración (heredado).

Si desea usar la aplicación Portal de empresa para la autenticación en lugar de usar el Asistente para la configuración, o quiere que los dispositivos se registren en Azure AD, instale la aplicación **Portal de empresa**. **Después** de que el dispositivo esté inscrito, puede instalar la aplicación Portal de empresa.

Para instalar la aplicación Portal de empresa en dispositivos, vea agregar la aplicación Portal de empresa. Establezca la aplicación Portal de empresa como una aplicación necesaria.

Una vez instalada, los usuarios abren la aplicación Portal de empresa e inician sesión con su cuenta de Azure AD (`user@contoso.com`). Una vez que han iniciado sesión, se autentican y están a punto para recibir las directivas y los perfiles.

- Seleccione el **Setup Assistant with modern authentication** (Asistente para la configuración con autenticación moderna) en los siguientes casos:
  - Quiere borrar el dispositivo.
  - Quiere usar la autenticación multifactor (MFA).
  - Quiere pedir a los usuarios que actualicen la contraseña expirada la primera vez que inicien sesión.
  - Quiere pedir a los usuarios que restablezcan sus contraseñas expiradas durante la inscripción.
  - Quiere que los dispositivos se registren en Azure AD. Al registrarlos ahí, se pueden usar las características disponibles en Azure AD, como el acceso condicional.

> **NOTE**
> Durante el Asistente de configuración, los usuarios deben especificar las credenciales de su organización de Azure AD (`user@contoso.com`). Cuando escriben sus credenciales, se inicia la inscripción. Si así lo quiere, los usuarios también pueden especificar su ID de Apple para acceder a características específicas de esta empresa, como Apple Pay.
>
> Una vez completado el Asistente de configuración, los usuarios pueden usar el dispositivo. Cuando se muestra la pantalla principal, la inscripción está completada y se ha establecido la afinidad de usuario. El dispositivo no está totalmente registrado en Azure AD y no aparece en la lista de dispositivos de un usuario en Azure AD.
>
> Si los usuarios necesitan acceso a los recursos protegidos por el acceso condicional o deben estar totalmente registrados con Azure AD, instale la aplicación Portal de empresa. Una vez instalada, los usuarios abren la aplicación Portal de empresa e inician sesión con su cuenta de Azure AD (`user@contoso.com`). Durante este segundo inicio de sesión, se evalúan las directivas de acceso condicional y el registro de Azure AD se completa. Los usuarios pueden instalar y usar los recursos de la organización, incluidas las aplicaciones de línea de negocio.

- En el centro de administración de Endpoint Manager, deben crear un perfil de inscripción. Elija **Inscribir con afinidad de usuario** (asociar un usuario al dispositivo) o **Inscribir sin afinidad de usuario** (dispositivos sin usuario o compartidos).
  - **Inscribir con afinidad de usuario**: el Asistente para la instalación autentica al usuario e inscribe el dispositivo en Intune. Elija también si los usuarios pueden eliminar el perfil de administración, llamado **Inscripción bloqueada**.
  - **Inscribir sin afinidad de usuario**: el Asistente para la instalación autentica al usuario y lo inscribe en Intune. Elija también si los usuarios pueden eliminar el perfil de administración, llamado **Inscripción bloqueada**. La aplicación Portal de empresa no se usa y no es necesaria ni compatible con las inscripciones sin afinidad de usuario.

Tareas del usuario final de ADE

Estas tareas dependen de cómo los administradores indican a los usuarios que instalen la aplicación Portal de empresa. Normalmente, cuantos menos usuarios finales deban realizar la inscripción, más probabilidades habrá de que quieran inscribirse.

Para obtener información más específica sobre los pasos de usuario final, vea Inscripción de un dispositivo macOS con Portal de empresa.

- **Inscripción con afinidad de usuario + Asistente para la configuración (heredado)** :

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican su identificador de Apple (`user@iCloud.com` o `user@gmail.com`).
  2. El Asistente para la instalación solicita información al usuario e inscribe el dispositivo en Intune. El dispositivo no está registrado en Azure AD.

     Si utiliza el Asistente para la instalación en la autenticación, deténgase en este punto.
  3. Opcional. Si usa la aplicación Portal de empresa para la autenticación (en lugar del Asistente para la instalación), esta se instala con la opción configurada.

     Los usuarios abren la aplicación Portal de empresa e inician sesión con las credenciales de su organización (`user@contoso.com`). Cuando han iniciado sesión, los usuarios se autentican y pueden acceder a los recursos de la organización.

     Recuerde que la instalación de la aplicación Portal de empresa es opcional. Si quiere que los usuarios se autentiquen mediante la aplicación Portal de empresa, en lugar de usar el Asistente para la instalación, agregue la aplicación Portal de empresa.

- **Inscripción con afinidad de usuario + Asistente para la configuración con autenticación moderna**:

  1. Cuando se enciende el dispositivo, se ejecutará el Asistente para la instalación de Apple. Los usuarios especifican su ID de Apple (`user@iCloud.com` o `user@gmail.com`) y las credenciales de su organización de Azure AD (`user@contoso.com`).

     Cuando los usuarios especifican sus credenciales de Azure AD, se inicia la inscripción.
  2. El Asistente para la configuración puede solicitar al usuario información adicional. Tras completar el proceso, los usuarios pueden usar el dispositivo. Cuando se muestra la pantalla principal, la inscripción está completada y se ha establecido la afinidad entre usuario y dispositivo. Los usuarios verán las aplicaciones y directivas en el dispositivo.
  3. Los usuarios abren la aplicación Portal de empresa que instaló y vuelven a iniciar sesión con las credenciales de su organización (`user@contoso.com`).

- **Inscribir sin afinidad de usuario**: no hay acciones. Asegúrese de que los usuarios no instalen la aplicación Portal de empresa.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

Pasos siguientes

- MAM-WE
- Guía de inscripción de Android
- Guía de inscripción de iOS/iPadOS

- Guía de inscripción de Windows

Guía de implementación: Inscripción de dispositivos Windows en Microsoft Intune

14/05/2021 • 20 minutes to read

Los dispositivos personales y propiedad de la organización se pueden inscribir en Intune. Una vez que están inscritos, reciben las directivas y los perfiles que se crean.

Al inscribir dispositivos Windows, dispone de las opciones siguientes:

- Inscripción automática de Windows 10
- Windows Autopilot:
- Directiva de grupo
- Administración conjunta

En este artículo se proporcionan recomendaciones sobre el método de inscripción de Windows que se va a usar. También se incluye información general de las tareas del administrador y el usuario final para cada tipo de inscripción. Para obtener información más específica, vea Inscripción de dispositivos Windows.

> **TIP**
> Esta guía está en constante evolución. Así pues, no dude en agregar o actualizar las sugerencias e instrucciones existentes que le hayan parecido útiles.

Antes de empezar

Para obtener información general, incluidos los requisitos previos específicos de Intune, vea Guía de implementación: Inscripción de dispositivos en Microsoft Intune.

Inscripción automática de Windows 10

Se usa para dispositivos personales o BYOD, y propiedad de la organización, que ejecutan Windows 10 y versiones más recientes. La inscripción automática:

- Usa la característica **Obtener acceso a trabajo o escuela** en los dispositivos.
- Usa las opciones de inscripción que se configuran en el centro de administración de Endpoint Manager.

En función de las opciones que se configuren, es posible que Azure AD Premium sea necesario.

También puede usar este método de inscripción para inscribir dispositivos de forma masiva automáticamente con la aplicación Diseñador de configuración de Windows.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Tiene Azure AD Premium.	✔

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Usará el Acceso condicional (CA) en los dispositivos inscritos mediante inscripción masiva.	✔ En Windows 10 1803 y versiones más recientes, CA está disponible para dispositivos Windows inscritos mediante inscripción masiva. ✖ En Windows 10 1709 y versiones más antiguas, CA no está disponible para dispositivos Windows inscritos mediante inscripción masiva.
Los dispositivos son personales o BYOD.	✔
Los dispositivos pertenecen a la organización o la escuela.	✔
Tiene dispositivos nuevos o existentes.	✔
Necesita inscribir un número pequeño de dispositivos o un gran número de dispositivos (inscripción masiva).	✔ La inscripción masiva está disponible para dispositivos propiedad de la organización, pero no para los personales o BYOD.
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos son sin usuario como, por ejemplo, pantalla completa, dedicado o un dispositivo compartido.	✔ Estos dispositivos son propiedad de la organización. Este método de inscripción requiere que los usuarios inicien sesión con su cuenta de organización. Un administrador de la organización puede iniciar sesión e inscribirse de forma automática. Cuando el dispositivo esté inscrito, cree un perfil de pantalla completa y asigne este perfil al dispositivo. También puede crear un perfil para dispositivos compartidos con muchos usuarios.
Usa la cuenta opcional del administrador de inscripción de dispositivos (DEM).	✔
Los dispositivos los administra otro proveedor de MDM.	✖ Para estar totalmente administrados por parte de Intune, los usuarios deben anular la inscripción del proveedor de MDM actual y luego inscribirse en Intune.

Tareas del administrador de inscripción automática

- Asegúrese de que los dispositivos ejecutan Windows 10 y versiones más recientes. Para obtener una lista completa, vea plataformas de dispositivos compatibles.
- Opcional. En lugar de que los usuarios escriban el nombre del servidor de Intune, puede crear un registro CNAME que sea más fácil de escribir, como `EnterpriseEnrollment.contoso.com`. Los registros CNAME asocian un nombre de dominio con un servidor específico. En el centro de administración de Endpoint Manager, pruebe el registro CNAME para asegurarse de que está configurado correctamente. Para obtener más información, vea Creación de un registro CNAME.
- En el centro de administración de Endpoint Manager, seleccione **inscripción de Windows** > **Inscripción automática**. En la configuración, establezca el **Ámbito de usuario de MDM** y el **Ámbito de usuario de MAM**:

- **Ámbito de usuario de MDM**: cuando se establece en **Algunos** o **Todos**, los dispositivos se unen a Azure AD y los administra Intune. No importa quién haya iniciado sesión en el dispositivo o si los dispositivos son personales o BYOD. Cuando se establece en **Ninguno**, los dispositivos no se unen a Azure AD y no los administra Intune.

  Por ejemplo:

  - Si quiere administrar el dispositivo, elija **Algunos** o **Todos**.
  - Si no quiere administrar el dispositivo, elija **Ninguno**.
  - Si solo quiere administrar la cuenta de organización en el dispositivo, elija **Ninguno** y configure el **Ámbito de usuario de MAM**.
  - Si quiere administrar el dispositivo *y* la cuenta de organización en el dispositivo, elija **Algunos** o **Todos** y configure el **Ámbito de usuario de MAM**.
- **Ámbito de usuario de MAM**: cuando se establece en **Algunos** o **Todos**, Intune administra la cuenta de organización en el dispositivo. Los dispositivos se "registran" en Azure AD. No se "unen" a Azure AD y no los administra Intune. Esta opción está diseñada para dispositivos BYOD o personales.

  Por ejemplo:

  - Si quiere administrar la cuenta de organización en el dispositivo, elija **Algunos** o **Todos**.
  - Si no quiere administrar la cuenta de organización en el dispositivo, entonces elija **Ninguno**.
  - Si solo quiere administrar el dispositivo, elija **Ninguno** y configure el **Ámbito de usuario de MDM**.
  - Si quiere administrar el dispositivo *y* la cuenta de organización en el dispositivo, elija **Algunos** o **Todos** y configure el **Ámbito de usuario de MDM**.

  Para obtener más información sobre los dispositivos unidos frente a los registrados, vea lo siguiente:

  - Identidad del dispositivo de Azure AD
  - Dispositivos registrados en Azure AD
  - Dispositivos unidos a Azure AD
- Para la inscripción masiva, vaya a Microsoft Store y descargue la aplicación Diseñador de configuración de Windows (WCD). Configure la aplicación Diseñador de configuración de Windows y elija inscribir dispositivos en Azure AD. Se crea un archivo de paquete. Coloque el archivo de paquete en una unidad USB o en un recurso compartido de red.

  En la configuración de la cuenta del dispositivo, los usuarios inician sesión con su cuenta de organización y seleccionan este archivo de paquete. Después, los usuarios se inscriben automáticamente.

  Si los usuarios finales están familiarizados con la ejecución de un archivo desde estas ubicaciones, pueden completar la inscripción. Para obtener más información, vea la inscripción masiva automática.

Tareas del usuario final para la inscripción automática

Cuando los usuarios encienden el dispositivo, los pasos siguientes determinan cómo están inscritos. Asegúrese de comunicar claramente las opciones que los usuarios deben elegir en los dispositivos personales y propiedad de la organización.

- **Dispositivos propiedad de la organización**: los usuarios encienden el dispositivo, recorren la experiencia integrada (OOB) paso a paso e inician sesión con su cuenta de organización. Este paso une el dispositivo en Azure AD y el dispositivo se considera propiedad de la organización. El dispositivo está totalmente administrado, independientemente de quién haya iniciado sesión. Los usuarios pueden abrir la aplicación **Configuración** > **Cuentas** > **Obtener acceso a trabajo o escuela**. Muestra que están conectados.

  Si los usuarios inician sesión con una cuenta personal durante la experiencia de OOB, todavía pueden

unir los dispositivos a Azure AD mediante los pasos siguientes:

1. Abrir la aplicación **Configuración** > **Cuentas** > **Obtener acceso a trabajo o escuela** > **Conectar**.
2. En **Acciones alternativas:** , seleccionar **Unir este dispositivo a Azure Active Directory** y escribir la información que se les solicita.

Cuando se unen, en el centro de administración de Endpoint Manager los dispositivos se muestran como propiedad de la organización y unidos a Azure AD. Intune administra los dispositivos, independientemente de quién haya iniciado sesión.

- **Dispositivos BYOD o personales**: los usuarios encienden el dispositivo, recorren la experiencia integrada (OOB) paso a paso e inician sesión con su cuenta personal. Para registrar el dispositivo en Azure AD:

  1. Abra la aplicación **Configuración** > **Cuentas** > **Obtener acceso a trabajo o escuela** > **Conectar**.
  2. En **Conectar**, los usuarios optan por escribir una **Dirección de correo electrónico** o eligen **Unir este dispositivo a Azure Active Directory**:
     - **Dirección de correo electrónico**: los usuarios escriben la dirección de correo electrónico de su organización. Se les pide más información, incluido el nombre del servidor de Intune o el registro CNAME. Asegúrese de proporcionarles toda la información que necesiten introducir.

       Esta opción registra el dispositivo en Azure AD. En el centro de administración de Endpoint Manager, se muestra como personal y registrado en Azure AD. Intune administra el usuario de la organización, no el dispositivo.

       Si no quiere administrar dispositivos BYOD o personales, asegúrese de que los usuarios seleccionan **Dirección de correo electrónico** y escriben la dirección de correo electrónico de su organización.

     - **Unir este dispositivo a Azure Active Directory**: los usuarios escriben la información que se les solicita, incluida la dirección de correo electrónico de su organización.

       Esta opción une el dispositivo en Azure AD. En el centro de administración de Endpoint Manager, se muestra como propiedad de la organización y unido a Azure AD. Intune administra los dispositivos, independientemente de quién haya iniciado sesión.

       Si quiere administrar dispositivos BYOD o personales, asegúrese de que los usuarios seleccionan **Unir este dispositivo a Azure Active Directory**. Los usuarios también deben saber que sus dispositivos personales los administrará su propio equipo de TI.

  Para obtener más información sobre la experiencia del usuario final, vea inscribir dispositivos Windows 10.

- Si usa la inscripción masiva y los usuarios finales están familiarizados con la ejecución de archivos desde un recurso compartido de red o una unidad USB, podrán completar la inscripción. Si no están familiarizados con este paso, se recomienda que el administrador realice la inscripción.

- En los dispositivos personales o BYOD que no son Windows 10, los usuarios deben instalar la aplicación Portal de empresa desde Microsoft Store. Una vez instalada, deben abrir la aplicación Portal de empresa e iniciar sesión con las credenciales de su organización (`user@contoso.com`). Se les pedirá más información, incluido el nombre del servidor de Intune. Asegúrese de proporcionarles toda la información que necesiten introducir.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para

obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

Windows Autopilot

Se usa en dispositivos propiedad de la organización, que ejecutan Windows 10 y versiones más recientes. Windows Autopilot usa la versión OEM de Windows 10 que está preinstalada en el dispositivo. No tiene que borrar los dispositivos ni usar imágenes de SO personalizadas. También requiere la Inscripción automática y usa el centro de administración de Endpoint Manager para crear un perfil de inscripción. Cuando los usuarios inician sesión con su cuenta de organización, se inscriben automáticamente.

Para obtener más información sobre Windows Autopilot, vea Información general de Windows Autopilot o el Tutorial: Uso de Autopilot para la inscripción de dispositivos Windows.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos se compran a través de un OEM que admite el servicio de implementación de Windows Autopilot, o en revendedores o distribuidores que estén en el programa de Asociados de soluciones en la nube de (CSP).	✔
Los dispositivos están unidos a Azure AD híbrido.	✔ Los dispositivos unidos a Azure AD híbrido están unidos a su entorno local de Active Directory y registrados en Azure AD. Los dispositivos de Azure AD están disponibles en Intune. Los dispositivos que no están registrados en Azure AD no están disponibles en Intune.
Tiene trabajadores remotos y quiere enviar dispositivos directamente a estos usuarios.	✔
Los dispositivos pertenecen a la organización o la escuela.	✔
Tiene dispositivos nuevos o existentes.	✔ Puede actualizar los escritorios existentes que ejecutan versiones anteriores de Windows, como Windows 7 y hasta Windows 10. Esta opción también usa Microsoft Endpoint Configuration Manager.
Necesita inscribir un número pequeño de dispositivos o un gran número de dispositivos (inscripción masiva).	✔
Tiene Azure AD Premium.	✔ Windows Autopilot usa la inscripción automática. La inscripción automática requiere Azure AD Premium.
Los dispositivos están asociados a un único usuario.	✔

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos son sin usuario como, por ejemplo, pantalla completa, dedicado o compartido.	✔ Estos dispositivos son propiedad de la organización. Este método de inscripción requiere que los usuarios inicien sesión con su cuenta de organización. Un administrador de la organización puede iniciar sesión e inscribirse de forma automática. Cuando el dispositivo esté inscrito, cree un perfil de pantalla completa y asigne este perfil al dispositivo. También puede crear un perfil para dispositivos compartidos con muchos usuarios.
Los dispositivos son personales o BYOD.	✘ Windows Autopilot es solo para dispositivos propiedad de la organización. En el caso de dispositivos personales o BYOD, use la inscripción automática o la inscripción de usuario.
Los dispositivos los administra otra solución de MDM.	✘ Para estar totalmente administrados por parte de Intune, los usuarios deben anular la inscripción del proveedor de MDM actual y luego inscribirse en Intune.
Usa la cuenta del administrador de inscripción de dispositivos (DEM).	✘ Las cuentas DEM no se aplican a Windows Autopilot. Si el administrador va a inscribir y preparar los dispositivos antes de asignarlos a los usuarios, puede usar una cuenta DEM.

Tareas del administrador de Windows Autopilot

- Asegúrese de que los dispositivos ejecutan Windows 10 y versiones más recientes. Para obtener una lista completa, vea requisitos de software.
- En el Centro de administración de Endpoint Manager, registre los dispositivos en Windows Autopilot. Este paso une los dispositivos a Azure AD. Para obtener información más específica, consulte Introducción al registro de Windows Autopilot e Información general sobre el registro manual.
- Cree un perfil de implementación de Autopilot. Para obtener información más específica, vea Crear un perfil de implementación de Autopilot.

  Al crear el perfil, también puede hacer lo siguiente:

  - Configurar la experiencia del usuario de implementación integrada, incluidas las opciones controlada por el usuario, aprovisionamiento previo y mucho más. Para obtener información más específica, vea Configuración de perfiles de Autopilot.
  - Configurar los comportamientos de inicio, como deshabilitar el administrador local y omitir el CLUF.
  - Asigne el perfil de implementación de Autopilot a los grupos de seguridad de Azure AD. También puede excluir grupos de seguridad.
  - En el caso de los dispositivos unidos a Azure AD híbrido, registre los dispositivos, cree el perfil de implementación y asigne el perfil. También instalará el conector de Intune para Active Directory. Este conector se comunica entre el entorno local de Active Directory y Azure AD.

  Para obtener información más específica, vea Implementación de dispositivos unidos a Azure AD híbrido

mediante Intune y Windows Autopilot.

Una vez asignado el perfil, los dispositivos empiezan a mostrarse en el centro de administración de Endpoint Manager (**Dispositivos** > **Windows**).

Tareas del usuario final de Windows Autopilot

La experiencia del usuario final depende de la opción de implementación de Windows Autopilot que elija, como controlada por el usuario o aprovisionamiento previo.

- **Modo de autoimplementación**: no hay acciones. Esta opción no asocia un usuario con el dispositivo. Los usuarios simplemente encienden el dispositivo y la inscripción se inicia automáticamente.

  Para obtener información más específica, vea autoimplementación.

- **Aprovisionamiento previo**: los usuarios encienden el dispositivo e inician sesión con su cuenta profesional o educativa. La inscripción se inicia automáticamente. Dado que los administradores aprovisionan previamente el dispositivo, la inscripción es más rápida en comparación con la opción **controlada por el usuario**.

  Para obtener información más específica, vea implementación con aprovisionamiento previo.

- **Dispositivos existentes**: los usuarios deben realizar los pasos siguientes:

  1. Abra la aplicación del Centro de software y seleccione **Sistemas operativos**.
  2. Seleccione **Windows Autopilot para dispositivos existentes** > **Instalar**. Se descarga el contenido, las unidades se formatean y se instala Windows 10.

     Este paso puede tardar algún tiempo y los usuarios deben esperar.
  3. Autopilot se ejecuta y los usuarios inician sesión con su cuenta profesional o educativa. La inscripción se puede iniciar automáticamente. Para obtener información más específica, vea implementación de dispositivos existentes.

- **Controlada por el usuario**: los usuarios encienden el dispositivo e inician sesión con su cuenta profesional o educativa. La inscripción se inicia automáticamente. Para obtener información más específica, vea implementación controlada por el usuario.

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

Directiva de grupo

Esta opción de inscripción está disponible para los dispositivos unidos a un dominio que quiere administrar mediante Intune. Antes de realizar la inscripción, los dispositivos deben estar unidos a Azure AD híbrido. Es decir, los dispositivos están registrados en el entorno local de Active Directory (AD) y en Azure AD. Una vez registrados en Azure AD, están disponibles para inscribirse en Intune y recibir la configuración y las características de los dispositivos que se configuren.

Se debe crear una directiva de grupo en AD local. Cuando se produce una actualización de directiva de grupo en el dispositivo, se notifica a los usuarios para que completen la configuración. La configuración usa la cuenta de Azure AD del usuario para inscribir automáticamente el dispositivo en Intune.

Para obtener información más específica, vea Inscripción automática de un dispositivo Windows 10 con directiva de grupo.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos están unidos a Azure AD híbrido.	✔ Los dispositivos unidos a Azure AD híbrido están unidos a su entorno local de Active Directory y registrados en Azure AD. Los dispositivos de Azure AD están disponibles en Intune. Los dispositivos que no están registrados en Azure AD no están disponibles en Intune.
Tiene Azure AD Premium.	✔ La inscripción con directiva de grupo requiere Azure AD Premium.
Tiene trabajadores remotos.	✔
Los dispositivos pertenecen a la organización o la escuela.	✔
Tiene dispositivos nuevos o existentes.	✔
Necesita inscribir un número pequeño de dispositivos o un gran número de dispositivos (inscripción masiva).	✔
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos son sin usuario como, por ejemplo, pantalla completa, dedicado o compartido.	✔ Estos dispositivos son propiedad de la organización. Este método de inscripción requiere que los usuarios inicien sesión con su cuenta de organización. Un administrador de la organización puede iniciar sesión e inscribirse de forma automática. Cuando el dispositivo esté inscrito, cree un perfil de pantalla completa y asigne este perfil al dispositivo. También puede crear un perfil para dispositivos compartidos con muchos usuarios.
Los dispositivos son personales o BYOD.	✘ En el caso de dispositivos personales o BYOD, use la inscripción automática o la inscripción de usuario.
Los dispositivos los administra otra solución de MDM.	✘ Para estar totalmente administrados por parte de Intune, los usuarios deben anular la inscripción del proveedor de MDM actual y luego inscribirse en Intune. No deben inscribirse con los agentes clásicos de Intune.
Usa la cuenta del administrador de inscripción de dispositivos (DEM).	✘ Las cuentas DEM no se aplican en directiva de grupo.

Tareas del administrador de directivas de grupo

Para obtener información más específica sobre este método de inscripción, vea Inscripción automática de un dispositivo Windows 10 con directiva de grupo.

- Asegúrese de que los dispositivos Windows 10 se admiten en Intune y son compatibles con la inscripción de

directiva de grupo.

- Registre AD en Azure AD. Para obtener información más específica, vea Integración de Azure AD con MDM.
- Asegúrese de que son dispositivos unidos a Azure AD híbrido. Los dispositivos se deben registrar en AD local y en Azure AD.
- En AD local, cree una Directiva de grupo **Habilitar la inscripción automática de MDM con las credenciales de Azure AD predeterminadas**. Cuando se actualiza la directiva de grupo, esta directiva se inserta en los dispositivos y los usuarios completan la configuración mediante su cuenta de dominio (`user@contoso.com`).

Normalmente, los usuarios no quieren inscribirse y es posible que no estén familiarizados con la aplicación Portal de empresa. Asegúrese de proporcionar instrucciones, incluida la información que se va a introducir. Para obtener instrucciones sobre cómo comunicarse con los usuarios, vea Guía de planeamiento: Tarea 5: Creación de un plan de lanzamiento.

Tareas del usuario final de directiva de grupo

- A los usuarios se les notifica que hay cambios de configuración. Puede que la actualización de la directiva requiera que los usuarios inicien sesión con su cuenta profesional o educativa (`user@contoso.com`). La inscripción se inicia automáticamente.

Inscripción de administración conjunta

Si usa Configuration Manager y quiere seguir usándolo, la inscripción de administración conjunta es lo que buscaba. La administración conjunta administra los dispositivos Windows 10 mediante Configuration Manager y Microsoft Intune a la vez. Asocie en la nube el entorno de Configuration Manager existente a Endpoint Manager. Esta opción de inscripción ejecuta algunas cargas de trabajo en Configuration Manager y otras en Endpoint Manager.

Para obtener información más específica sobre la administración conjunta, vea ¿Qué es administración conjunta?.

> **NOTE**
> La Asociación de inquilinos también es una opción cuando se usa Configuration Manager. No inscribe dispositivos, pero puede cargar los dispositivos de Configuration Manager en el centro de administración de Endpoint Manager. Usar el centro de administración para ejecutar algunas acciones remotas, ver los servidores locales y obtener información del sistema operativo. Para obtener más información, vea habilitación de la asociación de inquilinos.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Use Configuration Manager.	✔
Los dispositivos están unidos a Azure AD híbrido.	✔ Los dispositivos unidos a Azure AD híbrido están unidos a su entorno local de Active Directory y registrados en Azure AD. Los dispositivos de Azure AD están disponibles en Intune. Los dispositivos que no están registrados en Azure AD no están disponibles en Intune.

CARACTERÍSTICA	USE ESTA OPCIÓN DE INSCRIPCIÓN CUANDO
Los dispositivos están inscritos en Intune.	✔ Tiene dispositivos que quiere incorporar a la administración conjunta. Estos dispositivos pueden haberse inscrito mediante Windows Autopilot o proceder directamente de su OEM de hardware.
Tiene Azure AD Premium.	✔ Es posible que Azure AD Premium sea necesario en función de la configuración de la administración conjunta. Para obtener información más específica, vea Rutas hacia la administración conjunta.
Tiene trabajadores remotos.	✔
Los dispositivos pertenecen a la organización o la escuela.	✔
Los dispositivos son personales o BYOD.	✔
Tiene dispositivos nuevos o existentes.	✔ En el caso de los dispositivos que no ejecutan Windows 10 y versiones más recientes, como Windows 7, se deberán actualizar. Para obtener información más específica, vea Actualización de Windows 10 para la administración conjunta.
Necesita inscribir un número pequeño de dispositivos o un gran número de dispositivos (inscripción masiva).	✔
Los dispositivos están asociados a un único usuario.	✔
Los dispositivos son sin usuario como, por ejemplo, pantalla completa, dedicado o compartido.	✔ Estos dispositivos son propiedad de la organización. Este método de inscripción requiere que los usuarios inicien sesión con su cuenta de organización. Un administrador de la organización puede iniciar sesión e inscribirse de forma automática. Cuando el dispositivo esté inscrito, cree un perfil de pantalla completa y asigne este perfil al dispositivo. También puede crear un perfil para dispositivos compartidos con muchos usuarios.
Los dispositivos los administra otra solución de MDM.	✘ Para ser administrados conjuntamente, los usuarios deben anular la inscripción del proveedor de MDM actual. No deben inscribirse con los agentes clásicos de Intune.
Usa la cuenta del administrador de inscripción de dispositivos (DEM).	✘ Las cuentas DEM no se aplican en la administración conjunta.

Tareas del administrador de administración conjunta

Las tareas y los requisitos del administrador dependen de la opción de administración conjunta que se elija. Para obtener información más específica, vea Rutas hacia la administración conjunta.

Al configurar la administración conjunta, se elige lo siguiente:

- Inscribir de forma automática los dispositivos existentes administrados de Configuration Manager en Intune. Esta opción requiere dispositivos unidos a Azure AD híbrido. Para obtener información más específica, vea Tutorial: Habilitación de la administración conjunta para clientes existentes de Configuration Manager.
- Incorpore los dispositivos Windows 10 existentes inscritos en Intune para que también los administre Configuration Manager. En esta situación, estos dispositivos no están unidos a Azure AD híbrido. Es decir, los dispositivos están registrados en Azure AD. No están registrados en el entorno local de Active Directory.

  Para obtener información más específica, vea Tutorial: Habilitación de la administración conjunta para nuevos dispositivos basados en Internet.

Tareas del usuario final de administración conjunta

Ambas opciones usan la inscripción automática. Con la inscripción automática, los usuarios inician sesión con su cuenta de organización (`user@contoso.com`) y, después, se inscriben automáticamente. También pueden abrir la aplicación **Configuración** > **Cuentas** > **Obtener acceso a trabajo o escuela** > **Conectar** e iniciar sesión con la dirección de correo electrónico y la contraseña de la organización.

Configuration Manager puede aleatorizar la inscripción, por lo que puede que no se produzca de inmediato. Cuando se completa la inscripción, está listo para recibir las directivas y los perfiles que se creen.

Pasos siguientes

- MAM-WE
- Guía de inscripción de Android
- Guía de inscripción de iOS/iPadOS
- Guía de inscripción de macOS

Guía de implementación: Administración de dispositivos iOS/iPadOS en Microsoft Intune

20/05/2021 • 15 minutes to read

Intune admite la administración de dispositivos móviles (MDM) de iPads y iPhones para conceder acceso seguro a los usuarios al correo electrónico, los datos y las aplicaciones profesionales. En esta guía se proporcionan instrucciones específicas de iOS para ayudarle a configurar la inscripción e implementar aplicaciones y directivas en usuarios y dispositivos.

Requisitos previos

Antes de comenzar, complete estos requisitos previos para habilitar la administración de dispositivos iOS/iPadOS en Intune. Para obtener información más detallada sobre cómo configurar Intune, incorporar dispositivos o trasladarlos a esta plataforma, consulte la guía de implementación de la configuración de Intune.

- Agregar usuarios y grupos
- Asignar licencias a usuarios
- Establecer la entidad de administración de dispositivos móviles
- Tener permisos de Administrador global o Administrador de Intune en Azure Active Directory
- Configurar el certificado push MDM de Apple (APN)

Planificación de la implementación

La guía de planeamiento de Microsoft Intune proporciona instrucciones y consejos para ayudarlo a determinar los objetivos, los casos de uso y los requisitos. También se describe cómo crear planes de implementación, comunicación, soporte técnico, pruebas y validación.

Aprovechamiento del marco de configuración de seguridad de iOS/iPadOS

El marco de configuración de seguridad de iOS/iPadOS consta de una serie de recomendaciones de configuración de las directivas de configuración y cumplimiento de los dispositivos. Estas recomendaciones le ayudan a adaptar la protección de seguridad de los dispositivos móviles de la organización a sus necesidades específicas.

Microsoft Intune usa una taxonomía para este marco que es similar a la que se usa para las configuraciones de seguridad en Windows 10. Se aplica tanto a dispositivos de propiedad personal como supervisados, e incluye la configuración recomendada para una seguridad básica, mejorada y de alto nivel. Cada nivel de seguridad se basa en el anterior y ofrece más protección que el último.

Los niveles de seguridad de los dispositivos de propiedad personal son:

- Seguridad básica (nivel 1): esta configuración se recomienda como configuración de seguridad mínima para los dispositivos personales utilizados para acceder a datos profesionales o educativos. Esta configuración aplica directivas de contraseña, define las características de bloqueo del dispositivo y deshabilita determinadas funciones de dispositivo (como certificados que no son de confianza).
- Seguridad mejorada (nivel 2): esta configuración se recomienda para los dispositivos utilizados para acceder a información confidencial. Esta configuración establece controles de uso compartido de datos. Es aplicable a la mayoría de los usuarios de dispositivos móviles que acceden a los datos profesionales o

educativos en un dispositivo.

- Seguridad alta (nivel 3): esta configuración se recomienda para los dispositivos de usuarios o grupos específicos que son de alto riesgo. Por ejemplo, usuarios que controlan datos muy delicados cuya divulgación no autorizada causaría pérdidas materiales considerables a la organización. Esta configuración aplica directivas de contraseña más seguras que los niveles anteriores, deshabilita más funciones del dispositivo y establece restricciones de transferencia de datos adicionales.

Los niveles de seguridad de los dispositivos supervisados son:

- Seguridad básica (nivel 1): esta configuración se recomienda como configuración de seguridad mínima para los dispositivos supervisados utilizados para acceder a datos profesionales o educativos. Este nivel se alcanza aplicando directivas de contraseñas, definiendo características de bloqueo de dispositivo y deshabilitando determinadas funciones de los dispositivos (como certificados que no son de confianza).
- Seguridad mejorada (nivel 2): esta configuración se recomienda para los dispositivos utilizados para acceder a información confidencial. Esta configuración aplica controles de uso compartido de datos y bloquea el acceso a dispositivos USB. Es aplicable a la mayoría de los usuarios de dispositivos móviles que acceden a los datos profesionales o educativos en un dispositivo.
- Seguridad alta (nivel 3): esta configuración se recomienda para los dispositivos de usuarios o grupos específicos que son de alto riesgo. Por ejemplo, usuarios que controlan datos muy delicados cuya divulgación no autorizada causaría pérdidas materiales considerables a la organización. Esta configuración aplica directivas de contraseñas más seguras, deshabilita más funciones del dispositivo, establece restricciones de transferencia de datos adicionales y requiere que las aplicaciones se instalen a través del Programa de Compras por Volumen de Apple (VPP).

Para obtener más información sobre el marco de seguridad, incluidas recomendaciones específicas y las aplicaciones mínimas que deben protegerse, consulte los artículos que se enumeran en la tabla siguiente.

TAREA	DETAIL
Conocer la metodología de implementación del marco de iOS/iPadOS	Obtenga información sobre la metodología recomendada por Microsoft para implementar el marco de configuración de seguridad.
No permitir cuentas personales de aplicaciones de Microsoft en dispositivos iOS/iPadOS	Configure una directiva de aplicación que impida que los usuarios inicien sesión en una cuenta personal en un dispositivo profesional o educativo.
Configurar las opciones de seguridad de cumplimiento de dispositivos	Aplique esta configuración de seguridad para establecer un nivel de seguridad básico o alto en dispositivos de propiedad personal y corporativos.
Configurar las opciones de seguridad de dispositivos para dispositivos personales	Aplique esta configuración para establecer un nivel de seguridad básico, mejorado o alto en dispositivos de propiedad personal.
Configurar las opciones de seguridad de dispositivos para dispositivos supervisados	Aplique esta configuración para establecer un nivel de seguridad básico, mejorado o alto en dispositivos supervisados.

Creación de reglas de cumplimiento

Use directivas de cumplimiento para definir las reglas y condiciones que deben cumplir los usuarios y dispositivos para acceder a los recursos protegidos. Si usa el acceso condicional, las directivas de acceso

condicional pueden usar los resultados de cumplimiento de dispositivos para bloquear el acceso a los recursos desde dispositivos no compatibles. Para obtener una explicación detallada sobre las directivas de cumplimiento y cómo empezar, consulte Uso de directivas de cumplimiento para establecer reglas para los dispositivos que administra con Intune.

TAREA	DETAIL
Cree una directiva de cumplimiento.	Obtenga instrucciones paso a paso sobre cómo crear y asignar una directiva de cumplimiento a grupos de usuarios y dispositivos.
Adición de acciones en caso de incumplimiento	Elija lo que sucede cuando los dispositivos ya no cumplen las condiciones de la directiva de cumplimiento. Se pueden agregar acciones en caso de incumplimiento cuando se configure la directiva de cumplimiento de dispositivos o, más adelante, editando la directiva.
Crear una directiva de acceso condicional basada en dispositivo o basada en la aplicación	Especifique la aplicación o los servicios que desea proteger y defina las condiciones de acceso.
Bloquear el acceso a aplicaciones que no usan la autenticación moderna	Cree una directiva de acceso condicional basada en aplicaciones para bloquear las aplicaciones que usan métodos de autenticación distintos de OAuth2; por ejemplo, las aplicaciones que usan la autenticación básica y basada en formularios. Sin embargo, antes de bloquear el acceso, inicie sesión en Azure AD y revise el informe de actividad de métodos de autenticación para ver si los usuarios usan la autenticación básica para acceder a elementos esenciales que ha olvidado o desconoce. Por ejemplo, elementos como los quioscos de calendario de las salas de reuniones usan la autenticación básica.

Configuración de la seguridad del punto de conexión

Use las características de seguridad del punto de conexión de Intune para configurar la seguridad de los dispositivos y administrar las tareas de seguridad de los dispositivos en riesgo.

TAREA	DETAIL
Administrar dispositivos con características de seguridad del punto de conexión	Use la configuración de seguridad del punto de conexión en Intune para administrar de forma eficaz la seguridad de los dispositivos y corregir los problemas de los dispositivos.
Habilitar el conector Mobile Threat Defense (MTD) para dispositivos no inscritos	Habilite la conexión de MTD en Intune para que las aplicaciones asociadas de MTD puedan funcionar con Intune y sus directivas. Si no usa Microsoft Defender para punto de conexión, considere la posibilidad de habilitar el conector para que pueda usar otra solución de Mobile Threat Defense.
Crear una directiva de protección de aplicaciones de MTD	Cree una directiva de protección de aplicaciones de Intune que evalúe el riesgo y limite el acceso corporativo de un dispositivo en función del nivel de amenaza.
Incorporación de aplicaciones de MTD a dispositivos no inscritos	Ponga las aplicaciones de MTD a disposición de los usuarios de su organización y configure Microsoft Authenticator para iOS/iPadOS.

TAREA	DETAIL
Usar el acceso condicional para limitar el acceso a Microsoft Tunnel	Utilice las directivas de acceso condicional para regular el acceso de los dispositivos a su puerta de enlace de VPN de Microsoft Tunnel.

Configuración de dispositivo

Use Microsoft Intune para habilitar o deshabilitar la configuración y las características en dispositivos iOS/iPadOS. Para configurar y aplicar estas opciones, cree un perfil de configuración de dispositivo y, a continuación, asigne el perfil a los grupos de su organización. Los dispositivos reciben el perfil una vez que se inscriben.

TAREA	DETAIL
Creación de un perfil de dispositivo en Microsoft Intune	Obtenga información sobre los diferentes tipos de perfiles de dispositivo que puede crear para su organización.
Configurar características de dispositivo	Configure características y funcionalidades comunes de iOS/iPadOS para un contexto profesional o educativo. Para obtener una descripción de la configuración de esta área, consulte la referencia de características del dispositivo.
Configurar perfil Wi-Fi	Este perfil permite a los usuarios buscar la red Wi-Fi de su organización y conectarse a ella. Para obtener una descripción de la configuración de esta área, consulte la referencia de la configuración de la red Wi-Fi.
Configurar el perfil de VPN	Configure una opción de VPN segura, como Microsoft Tunnel, para las personas que se conectan a la red de su organización. También puede crear una directiva de VPN por aplicación para exigir a los usuarios que inicien sesión en determinadas aplicaciones a través de una conexión VPN. Para obtener una descripción de la configuración de esta área, consulte la referencia de la configuración de VPN.
Configurar el perfil de correo electrónico	Configure los valores de correo electrónico para que los usuarios puedan conectarse a un servidor de correo electrónico y acceder a su dirección de correo electrónico profesional o educativa. Para obtener una descripción de la configuración de esta área, consulte la referencia de la configuración de correo electrónico.
Restringir las características del dispositivo	Proteja a los usuarios contra el acceso no autorizado y las distracciones limitando las características del dispositivo que pueden usar en su entorno profesional o educativo. Para obtener una descripción de la configuración de esta área, consulte la referencia de las restricciones del dispositivo.
Configurar perfil personalizado	Agregue y asigne configuraciones y características del dispositivo que no están integradas en Intune.
Personalizar la marca y la experiencia de inscripción	Personalice el Portal de empresa de Intune y la experiencia de la aplicación Microsoft Intune con sus propias palabras, la personalización de marca, las preferencias de pantalla y la información de contacto de su organización.

TAREA	DETAIL
Configurar la directiva de actualización de software	Programe actualizaciones e instalaciones automáticas del sistema operativo para dispositivos iOS/iPadOS supervisados.

Configuración de métodos de autenticación seguros

Configure métodos de autenticación en Intune para asegurarse de que solo las personas autorizadas acceden a los recursos internos. Intune admite la autenticación multifactor, los certificados y las credenciales derivadas. Los certificados también se usan para firmar y cifrar el correo electrónico mediante S/MIME.

TAREA	DETAIL
Requerir autenticación multifactor (MFA)	Obligue a las personas a proporcionar dos formas de credenciales en el momento de la inscripción.
Creación de un perfil de certificado de confianza	Cree e implemente un perfil de certificado de confianza antes de crear un perfil de certificado SCEP, PKCS o PKCS importado. El perfil de certificado de confianza implementa el certificado raíz de confianza en dispositivos y usuarios mediante certificados SCEP, PKCS y PKCS importados.
Usar certificados SCEP con Intune	Obtenga información sobre lo que se necesita para usar certificados SCEP con Intune y configure la infraestructura necesaria. Después de hacerlo, puede crear un perfil de certificado SCEP o configurar una entidad de certificación de terceros con SCEP.
Usar certificados PKCS con Intune	Configure la infraestructura necesaria (por ejemplo, los conectores de certificados locales), exporte un certificado PKCS y agregue el certificado a un perfil de configuración de dispositivos de Intune.
Usar certificados PKCS importados con Intune	Configure los certificados PKCS importados, que le permiten configurar y usar S/MIME para cifrar el correo electrónico.
Configurar un emisor de credenciales derivadas	Aprovisione dispositivos iOS/iPadOS con certificados derivados de tarjetas inteligentes de usuario.

Implementación de aplicaciones

Al configurar aplicaciones y directivas de aplicaciones, piense en los requisitos de su organización, como las plataformas que admitirá, las tareas que realizan los usuarios, el tipo de aplicaciones que necesitan para completar esas tareas y, por último, quién las necesita. Puede usar Intune para administrar todo el dispositivo (incluidas las aplicaciones) o para administrar solo las aplicaciones.

TAREA	DETAIL
Agregar aplicaciones de Store	Agregue aplicaciones de iOS/iPadOS desde el App Store a Intune y asígnelas a grupos.
Agregar aplicaciones web	Agregue aplicaciones web a Intune y asígnelas a grupos.

TAREA	DETAIL
Agregar aplicaciones integradas	Agregue aplicaciones integradas a Intune y asígnelas a grupos.
Agregar aplicaciones de línea de negocio	Agregue aplicaciones de línea de negocio (LOB) de iOS/iPadOS a Intune y asígnelas a grupos.
Asignar aplicaciones a grupos	Asigne aplicaciones a usuarios y dispositivos.
Incluir y excluir asignaciones de aplicaciones	Controle el acceso y la disponibilidad de una aplicación mediante la inclusión y exclusión de grupos seleccionados de la asignación.
Administrar aplicaciones de iOS/iPadOS adquiridas a través de Apple Business Manager	Sincronice, administre y asigne aplicaciones adquiridas a través de Apple Business Manager.
Administrar eBooks de iOS/iPadOS adquiridos a través de Apple Business Manager	Sincronice, administre y asigne libros adquiridos a través de Apple Business Manager.
Crear una directiva de protección de aplicaciones de iOS/iPadOS	Mantenga los datos de su organización dentro de aplicaciones administradas como Outlook y Word. Consulte Configuración de directivas de protección de aplicaciones de iOS/iPadOS para obtener más información sobre cada opción de configuración.
Crear un perfil de aprovisionamiento de aplicaciones	Evite que los certificados de aplicaciones expiren mediante la asignación proactiva de nuevos perfiles de aprovisionamiento a dispositivos que tienen aplicaciones que están a punto de expirar.
Crear una directiva de configuración de aplicaciones	Aplique opciones de configuración personalizadas a aplicaciones de iOS/iPadOS en dispositivos inscritos. También puede aplicar estos tipos de directivas a aplicaciones administradas sin inscripción de dispositivos.
Configuración de Microsoft Edge	Use las directivas de configuración y protección de aplicaciones de Intune con Edge para iOS/iPadOS a fin de garantizar que se apliquen medidas de seguridad al acceder a los sitios web corporativos.
Configurar aplicaciones de Microsoft Office	Use las directivas de configuración y protección de aplicaciones de Intune con aplicaciones de Office a fin de garantizar que se apliquen medidas de seguridad al acceder a los archivos corporativos.
Configuración de Microsoft Teams	Use las directivas de configuración y protección de aplicaciones de Intune con Teams a fin de garantizar que se apliquen medidas de seguridad al acceder a experiencias de colaboración en equipo.
Configurar Microsoft Outlook	Use las directivas de configuración y protección de aplicaciones de Intune con Outlook a fin de garantizar que se apliquen medidas de seguridad al acceder al correo electrónico y los calendarios corporativos.

Inscribir dispositivos

La inscripción de dispositivos les permite recibir las directivas que cree, por lo que debe tener listos los grupos de usuarios y los grupos de dispositivos de Azure AD.

Para obtener información sobre cada método de inscripción y cómo elegir el adecuado para su organización, consulte la guía de inscripción de dispositivos de iOS/iPadOS para Microsoft Intune.

TAREA	DETAIL
Configurar la inscripción de dispositivos automatizada (ADE) de Apple en Intune	Configure una experiencia de inscripción inmediata para dispositivos corporativos adquiridos a través de Apple School Manager o Apple Business Manager. Para ver un tutorial detallado de este proceso, consulte Tutorial: Uso de las características de inscripción de dispositivos corporativos de Apple en Apple Business Manager (ABM) para inscribir dispositivos iOS/iPadOS en Intune.
Configurar Apple School Manager en Intune	Configure Intune para inscribir los dispositivos que adquiera mediante el programa de Apple School Manager.
Configurar la inscripción de dispositivos con Apple Configurator	Cree un perfil de Apple Configurator para inscribir dispositivos corporativos (sin afinidad de usuario) a través de la inscripción directa, o para inscribir dispositivos borrados o nuevos (con afinidad de usuario) a través del Asistente para la configuración. Tendrá que exportar el perfil de Apple Configurator desde Intune, lo cual requiere una conexión USB a un equipo Mac que ejecute Apple Configurator.
Identificar dispositivos como corporativos	Asigne el estado de propiedad corporativa a los dispositivos para habilitar más funcionalidades de administración e identificación en Intune. El estado de propiedad corporativa no se puede asignar a los dispositivos inscritos a través de Apple Business Manager.
Configurar la inscripción de usuarios de Apple (en versión preliminar)	Cree un perfil de inscripción de usuario para implementar la experiencia de inscripción de usuarios de Apple en dispositivos mediante un Apple ID administrado. La compatibilidad con esta característica está actualmente en versión preliminar.
Configurar dispositivos iPad compartidos	Configure los dispositivos para que más de una persona los pueda usar (el tipo de configuración que vería en una biblioteca o entorno educativo).
Hacer copia de seguridad de dispositivo y restaurarlo	Haga una copia de seguridad de un dispositivo y restáurelo para prepararlo para la inscripción o la migración en Intune, como durante la configuración de la inscripción de dispositivo automatizada.
Cambiar la propiedad del dispositivo	Una vez inscrito un dispositivo, puede cambiar su etiqueta de propiedad en Intune a propiedad corporativa o personal. Este ajuste cambia la forma en que puede administrar el dispositivo.
Solución de problemas de inscripción	Solucione los problemas que se producen durante la inscripción o busque opciones para resolverlos.

Ejecución de acciones remotas

Una vez configurados los dispositivos, podrá usar acciones remotas en Intune para administrar los dispositivos

y solucionar sus problemas a distancia. La disponibilidad varía según la plataforma del dispositivo. Si una acción falta en el portal o está deshabilitada, no se admite en el dispositivo.

TAREA	DETAIL
Realizar acciones remotas en dispositivos	Obtenga información sobre cómo explorar en profundidad dispositivos individuales en Intune, así como administrarlos de forma remota y solucionar sus problemas. En este artículo se enumeran todas las acciones remotas disponibles en Intune y los vínculos a esos procedimientos.
Uso de TeamViewer para administrar dispositivos de Intune de forma remota	Configure TeamViewer en Intune y aprenda a administrar un dispositivo de forma remota.
Corregir las vulnerabilidades que identifica Microsoft Defender para punto de conexión	Integre Intune con Microsoft Defender para punto de conexión para aprovechar las ventajas de Administración de amenazas y vulnerabilidades de Defender para punto de conexión y usar Intune para corregir las debilidades de los puntos de conexión que se han identificado con la funcionalidad de administración de vulnerabilidades de Defender.

Pasos siguientes

Consulte estos tutoriales de inscripción para aprender a realizar algunas de las tareas principales en Intune. Los tutoriales son contenidos de nivel 100 - 200 para usuarios nuevos en Intune o en un escenario específico.

- Tutorial: Tutorial de Intune en Microsoft Endpoint Manager
- Tutorial: Uso de las características de inscripción de dispositivos corporativos de Apple en Apple Business Manager (ABM) para inscribir dispositivos iOS/iPadOS en Intune
- Protección del correo electrónico de Exchange Online en dispositivos administrados
- Protección del correo electrónico de Exchange Online en dispositivos no administrados
- Configuración de Slack para usar Intune para EMM y la configuración de aplicaciones

Para obtener la versión de Android de esta guía, consulte Guía de implementación: Administración de dispositivos Android en Microsoft Intune.

Guía de implementación: Administración de dispositivos Android en Microsoft Intune

20/05/2021 • 17 minutes to read

Intune admite la administración de dispositivos móviles (MDM) de Android para conceder acceso seguro a los usuarios al correo electrónico, los datos y las aplicaciones profesionales. En esta guía se proporcionan recursos específicos de Android para ayudarle a configurar la inscripción en Intune e implementar aplicaciones y directivas en usuarios y dispositivos.

Requisitos previos

Antes de comenzar, complete estos requisitos previos para habilitar la administración de dispositivos Android en Intune. Para obtener información más detallada sobre cómo configurar Intune, incorporar dispositivos o trasladarlos a esta plataforma, consulte la guía de implementación de la configuración de Intune.

- Agregar usuarios y grupos
- Asignar licencias a usuarios
- Establecer la entidad de administración de dispositivos móviles
- Tener permisos de Administrador global o Administrador de Intune en Azure Active Directory

Planificación de la implementación

Use la Guía de planificación de Microsoft Intune para obtener ayuda con la planificación, el diseño y la implementación de Microsoft Intune en su organización. La guía proporciona información para ayudarle a:

- Determinar los objetivos, los escenarios de casos de uso y los requisitos.
- Crear planes de implementación y comunicación.
- Crear planes de compatibilidad, pruebas y validación.

Aprovechamiento del marco de configuración de seguridad de Android Enterprise

El marco de configuración de seguridad de Android Enterprise consta de una serie de recomendaciones de configuración de las directivas de configuración y cumplimiento de los dispositivos. Estas recomendaciones le pueden ayudar a adaptar la protección de seguridad de los dispositivos móviles de la organización a sus necesidades específicas. Puede aplicarlas a dispositivos totalmente administrados o de propiedad personal con perfiles de trabajo.

La taxonomía para este marco es similar a la que se usa para las configuraciones de seguridad en iOS. Incluye opciones de configuración recomendadas para seguridad de nivel básico, mejorado y alto. Cada nivel de seguridad se basa en el anterior para ofrecer más protección que el último.

Los niveles de seguridad de los dispositivos de propiedad personal con perfil de trabajo son:

- Seguridad básica (nivel 1): esta configuración se recomienda como configuración de seguridad mínima para los dispositivos personales donde los usuarios acceden a datos profesionales o educativos. Esta configuración presenta los requisitos de contraseña, separa los datos profesionales y personales y valida la atestación de dispositivos Android.
- Seguridad alta (nivel 3): esta configuración se recomienda para los dispositivos de usuarios o grupos

específicos que son de alto riesgo. Por ejemplo, usuarios que controlan datos muy delicados cuya divulgación no autorizada causaría pérdidas materiales considerables a la organización. Esta configuración presenta la defensa contra amenazas móviles o la Protección contra amenazas avanzada (ATP) de Microsoft Defender, aplica requisitos de versión de Android más estrictos, aplica directivas de contraseñas más seguras y restringe aún más la separación personal y profesional.

Los niveles de seguridad de los dispositivos totalmente administrados son:

- Seguridad básica (nivel 1): esta configuración se recomienda como configuración de seguridad mínima para los dispositivos supervisados utilizados para acceder a datos profesionales o educativos. Aplica los requisitos de contraseña, la versión mínima de Android y ciertas restricciones de dispositivos.
- Seguridad mejorada (nivel 2): esta configuración se recomienda para los dispositivos utilizados para acceder a información confidencial. Aplica directivas de contraseñas más seguras y deshabilita las funcionalidades de usuario y cuenta. Es aplicable a la mayoría de los usuarios de dispositivos móviles que acceden a los datos profesionales o educativos en un dispositivo.
- Seguridad alta (nivel 3): esta configuración se recomienda para los dispositivos de usuarios o grupos específicos que son de alto riesgo. Por ejemplo, usuarios que controlan datos muy delicados cuya divulgación no autorizada causaría pérdidas materiales considerables a la organización. Esta configuración aplica requisitos de versión de Android más estrictos y otras restricciones de dispositivos, e introduce la defensa contra amenazas móviles o ATP de Microsoft Defender.

Para obtener más información sobre el marco de seguridad, consulte los artículos que se enumeran en la siguiente tabla.

TAREA	DETAIL
Obtener información sobre la metodología de implementación del marco de Android Enterprise	Obtenga información sobre la metodología recomendada por Microsoft para implementar el marco de configuración de seguridad.
Configurar restricciones de inscripción de dispositivos para dispositivos de propiedad personal	Aplique estas restricciones para establecer un nivel de seguridad básico o alto en dispositivos de propiedad personal con perfil de trabajo.
No permitir cuentas personales en dispositivos Android Enterprise	Impida que las personas inicien sesión en aplicaciones de Microsoft con una cuenta personal en dispositivos profesionales o educativos.
Configurar las opciones de seguridad para dispositivos de propiedad personal	Aplique esta configuración para establecer un nivel de seguridad básico o alto en dispositivos de propiedad personal con perfil de trabajo.
Configurar las opciones de seguridad para dispositivos totalmente administrados	Aplique esta configuración para establecer un nivel de seguridad básico, mejorado o alto en dispositivos de propiedad corporativa y totalmente administrados.

Creación de reglas de cumplimiento

Use directivas de cumplimiento para definir las reglas y condiciones que deben cumplir los usuarios y dispositivos para acceder a los recursos protegidos de la organización. También puede crear directivas de acceso condicional, que funcionan junto con los resultados de cumplimiento de dispositivos para bloquear el acceso a los recursos desde dispositivos no compatibles. Para obtener una explicación detallada sobre las directivas de cumplimiento y cómo empezar, consulte Uso de directivas de cumplimiento para establecer reglas para los dispositivos que administra con Intune.

Las siguientes tareas se aplican a las plataformas de Android Enterprise y Administrador de dispositivos Android.

TAREA	DETAIL
Cree una directiva de cumplimiento.	Obtenga instrucciones paso a paso sobre cómo crear y asignar una directiva de cumplimiento a grupos de usuarios y dispositivos.
Adición de acciones en caso de incumplimiento	Elija lo que sucede cuando los dispositivos ya no cumplen las condiciones de la directiva de cumplimiento. Se pueden agregar acciones en caso de incumplimiento cuando se configure la directiva de cumplimiento de dispositivos o, más adelante, editando la directiva.
Crear una directiva de acceso condicional basada en dispositivos o basada en aplicaciones.	Especifique la aplicación o los servicios que desea proteger y defina las condiciones de acceso.
Bloquear el acceso a aplicaciones que no usan la autenticación moderna	Cree una directiva de acceso condicional basada en aplicaciones para bloquear las aplicaciones que usan métodos de autenticación distintos de OAuth2. Por ejemplo, puede bloquear las aplicaciones que usan la autenticación básica y basada en formularios. Antes de bloquear el acceso, inicie sesión en Azure AD y revise el informe de actividad de métodos de autenticación para ver si los usuarios usan la autenticación básica para acceder a elementos esenciales (como los quioscos de calendario de las salas de reuniones) que ha olvidado o desconoce.

Configuración de la seguridad del punto de conexión

Use las características de seguridad del punto de conexión de Intune para configurar la seguridad de los dispositivos y administrar las tareas de seguridad de los dispositivos en riesgo.

Las siguientes tareas se aplican a las plataformas de Android Enterprise y Administrador de dispositivos Android.

TAREA	DETAIL	PLATAFORMA
Administrar dispositivos con características de seguridad del punto de conexión	Use la configuración de **seguridad de puntos de conexión** en Intune para administrar de forma eficaz la seguridad de los dispositivos y corregir los problemas de los dispositivos.	
Habilitar el conector de defensa contra amenazas móviles (MTD) para dispositivos inscritos	Habilite la conexión de MTD en Intune para que las aplicaciones asociadas de MTD puedan funcionar con Intune y sus directivas de cumplimiento de dispositivos de MTD. Si no usa Microsoft Defender para punto de conexión, considere la posibilidad de habilitar el conector para que pueda usar otra solución de Mobile Threat Defense. También puede habilitar el conector MTD para dispositivos no inscritos en Intune.	

TAREA	DETAIL	PLATAFORMA
Crear una directiva de protección de aplicaciones de MTD	Cree una directiva de protección de aplicaciones de Intune que evalúe los riesgos y limite el acceso de un dispositivo a aplicaciones profesionales o educativas.	
Crear una directiva de cumplimiento de dispositivos de MTD	Cree una directiva de protección de aplicaciones de Intune que evalúe el riesgo y limite el acceso corporativo de un dispositivo en función del nivel de amenaza.	
Agregar y asignar aplicaciones de MTD	Agregue e implemente aplicaciones de MTD en Intune. Estas aplicaciones funcionan con las directivas de cumplimiento de dispositivos y de protección de aplicaciones para identificar y ayudar a corregir las amenazas de los dispositivos. También puede asignar aplicaciones de MTD a dispositivos no inscritos en Intune.	

Configuración de dispositivo

Use Microsoft Intune para habilitar o deshabilitar la configuración y las características en dispositivos. Para configurar y aplicar estas opciones, cree un perfil de dispositivo y, a continuación, asigne el perfil a los grupos de su organización. Los dispositivos reciben el perfil una vez que se inscriben.

TAREA	DETAIL	PLATAFORMA
Creación de un perfil de dispositivo en Microsoft Intune	Obtenga información sobre los diferentes tipos de perfiles de dispositivo que puede crear para su organización.	Android Enterprise, Administrador de dispositivos Android
Configurar perfil Wi-Fi	Este perfil permite a los usuarios buscar la red Wi-Fi de su organización y conectarse a ella. Para obtener una descripción de la configuración de esta área, consulte la referencia de configuración de Wi-Fi para la configuración de Wi-Fi de Android Enterprise o la configuración de Wi-Fi del Administrador de dispositivos Android.	Android Enterprise, Administrador de dispositivos Android
Configurar el perfil de VPN	Configure una opción de VPN segura, como Microsoft Tunnel, para las personas que se conectan a la red de su organización. Para obtener una descripción de la configuración de esta área, consulte la referencia de configuración de VPN para la configuración de VPN de Android Enterprise o la configuración de VPN del Administrador de dispositivos Android.	Android Enterprise, Administrador de dispositivos Android

TAREA	DETAIL	PLATAFORMA
Configurar el perfil de correo electrónico	Configure los valores de correo electrónico para que los usuarios puedan conectarse a un servidor de correo electrónico y acceder a su dirección de correo electrónico profesional o educativa. Para obtener una descripción de la configuración de esta área, consulte la configuración de correo electrónico de Android Enterprise o la configuración de correo electrónico del Administrador de dispositivos Android.	Android Enterprise, Administrador de dispositivos Android
Restringir las características del dispositivo	Proteja a los usuarios contra el acceso no autorizado y las distracciones limitando las características del dispositivo que pueden usar en su entorno profesional o educativo. Para obtener una descripción de la configuración de esta área, consulte la configuración de dispositivo Android Enterprise o la configuración de dispositivo del Administrador de dispositivos Android.	Android Enterprise, Administrador de dispositivos Android
Configurar opciones personalizadas para el Administrador de dispositivos Android	Agregue o cree opciones personalizadas que no están integradas en Intune, como un perfil de VPN por aplicación y la protección web con Microsoft Defender para punto de conexión.	Administrador de dispositivos Android
Configurar aplicaciones Samsung Knox	Cree un perfil personalizado para permitir y bloquear aplicaciones para dispositivos Samsung Knox Standard.	Administrador de dispositivos Android
Crear un perfil personalizado para Android Enterprise	Agregue o cree opciones personalizadas que no están integradas en Intune para dispositivos de propiedad personal.	Android Enterprise
Configurar un perfil de Mobility Extensions (MX) de Zebra	Use perfiles de Mobility Extensions (MX) de Zebra para personalizar o agregar más ajustes específicos de Zebra en Intune.	Administrador de dispositivos Android
Crear un perfil de configuración de OEMConfig	Use OEMConfig para agregar, crear y personalizar la configuración específica de OEM para dispositivos Android Enterprise.	Android Enterprise
Personalizar la marca y la experiencia de inscripción	Personalice el Portal de empresa de Intune y las aplicaciones de Microsoft Intune con la personalización de marca de su organización para crear una experiencia familiar para las personas que inscriban sus dispositivos.	Android Enterprise, Administrador de dispositivos Android

Configuración de métodos de autenticación seguros

Configure métodos de autenticación en Intune para asegurarse de que solo las personas autorizadas acceden a los recursos internos. Intune admite la autenticación multifactor, los certificados SCEP y PKCS y las credenciales derivadas. Los certificados también se usan para firmar y cifrar el correo electrónico mediante S/MIME.

TAREA	DETAIL	PLATAFORMA
Requerir autenticación multifactor (MFA)	Obligue a las personas a proporcionar dos formas de credenciales en el momento de la inscripción.	Android Enterprise
Creación de un perfil de certificado de confianza	Cree e implemente un perfil de certificado de confianza antes de crear un perfil de certificado SCEP, PKCS o PKCS importado. El perfil de certificado de confianza implementa el certificado raíz de confianza en dispositivos mediante certificados SCEP, PKCS y PKCS importados.	Android Enterprise, Administrador de dispositivos Android
Usar certificados SCEP con Intune	Obtenga información sobre lo que se necesita para usar certificados SCEP con Intune y configure la infraestructura necesaria. Después de hacerlo, puede crear un perfil de certificado SCEP o configurar una entidad de certificación de terceros con SCEP.	Android Enterprise
Usar certificados PKCS con Intune	Configure la infraestructura necesaria (por ejemplo, los conectores de certificados locales), exporte un certificado PKCS y agregue el certificado a un perfil de configuración de dispositivos de Intune.	Android Enterprise, Administrador de dispositivos Android
Usar certificados PKCS importados con Intune	Configure los certificados PKCS importados, que le permiten configurar y usar S/MIME para cifrar el correo electrónico.	Android Enterprise, Administrador de dispositivos Android
Configurar un emisor de credenciales derivadas	Aprovisione dispositivos Android con certificados derivados de tarjetas inteligentes de usuario.	Android Enterprise

Implementación de aplicaciones

Al configurar aplicaciones y directivas de aplicaciones, piense en los requisitos de su organización, como las plataformas que admitirá, las tareas que realizan los usuarios, el tipo de aplicaciones que necesitan para completar esas tareas y, por último, quién las necesita. Puede usar Intune para administrar todo el dispositivo (incluidas las aplicaciones) o para administrar solo las aplicaciones.

TAREA	DETAIL	PLATAFORMA
Agregar aplicaciones de Google Play Store	Agregue aplicaciones de Android desde Google Play Store.	Administrador de dispositivos Android

TAREA	DETAIL	PLATAFORMA
Agregar aplicaciones de Google Play administrado	Agregue aplicaciones de la tienda, aplicaciones de línea de negocio (LOB) y aplicaciones web a través de Google Play Store administrado.	Android Enterprise
Agregar aplicaciones del sistema de Android Enterprise	Use Intune para habilitar y deshabilitar aplicaciones del sistema de Android Enterprise.	Android Enterprise
Agregar aplicaciones web	Agregue aplicaciones web a Intune y asígnelas a grupos.	Administrador de dispositivos Android
Agregar aplicaciones integradas	Agregue aplicaciones integradas a Intune y asígnelas a grupos.	Android Enterprise, Administrador de dispositivos Android
Agregar aplicaciones de línea de negocio	Agregue aplicaciones de línea de negocio (LOB) de Android a Intune y asígnelas a grupos.	Administrador de dispositivos Android
Asignar aplicaciones a grupos	Asigne aplicaciones a usuarios y dispositivos.	Android Enterprise, Administrador de dispositivos Android
Incluir y excluir asignaciones de aplicaciones	Controle el acceso y la disponibilidad de una aplicación mediante la inclusión y exclusión de grupos seleccionados de la asignación.	Android Enterprise, Administrador de dispositivos Android
Crear una directiva de protección de aplicaciones de Android	Mantenga los datos de su organización dentro de aplicaciones administradas como Outlook y Word. Para obtener más información sobre cada opción de configuración, consulte la configuración de directivas de protección de aplicaciones de Android.	Android Enterprise, Administrador de dispositivos Android
Validar la directiva de protección de aplicaciones	Compruebe que su directiva de protección de aplicaciones esté configurada y funcione correctamente antes de implementarla en toda la organización.	Android Enterprise, Administrador de dispositivos Android
Crear una directiva de configuración de aplicaciones	Aplique opciones de configuración personalizadas a aplicaciones de Android en dispositivos inscritos. También puede aplicar estos tipos de directivas a aplicaciones administradas sin inscripción de dispositivos.	Android Enterprise, Administrador de dispositivos Android
Configuración de Microsoft Edge	Use las directivas de configuración y protección de aplicaciones de Intune con Microsoft Edge para Android a fin de garantizar que se apliquen medidas de seguridad al acceder a los sitios web corporativos.	Android Enterprise, Administrador de dispositivos Android

TAREA	DETAIL	PLATAFORMA
Configurar Google Chrome	Use una directiva de configuración de aplicaciones de Intune para configurar Google Chrome en dispositivos Android inscritos en Intune.	Android Enterprise
Configurar la aplicación Managed Home Screen de Microsoft	Configure Managed Home Screen en dispositivos Android Enterprise de propiedad corporativa, dedicados, inscritos mediante Intune y ejecutados en modo de pantalla completa con varias aplicaciones.	Android Enterprise
Configurar la aplicación Microsoft Launcher	Configure Microsoft Launcher para personalizar la experiencia de pantalla principal en los dispositivos totalmente administrados de la organización.	Android Enterprise
Configurar aplicaciones de Microsoft Office	Use las directivas de configuración y protección de aplicaciones de Intune con aplicaciones de Office a fin de garantizar que se apliquen medidas de seguridad al acceder a los archivos corporativos.	Android Enterprise
Configuración de Microsoft Teams	Use las directivas de configuración y protección de aplicaciones de Intune con Teams a fin de garantizar que se apliquen medidas de seguridad al acceder a experiencias de colaboración en equipo.	Android Enterprise
Configurar Microsoft Outlook	Use las directivas de configuración y protección de aplicaciones de Intune con Outlook a fin de garantizar que se apliquen medidas de seguridad al acceder al correo electrónico y los calendarios corporativos.	Android Enterprise

Inscribir dispositivos

La inscripción de dispositivos les permite recibir las directivas que cree, por lo que debe tener listos los grupos de usuarios y los grupos de dispositivos de Azure AD.

Intune admite los siguientes métodos de inscripción para dispositivos Android:

- Bring-your-own-device (BYOD): dispositivos Android Enterprise de propiedad personal con un perfil de trabajo
- Dispositivos Android Enterprise dedicados de propiedad corporativa
- Dispositivos Android Enterprise de propiedad corporativa totalmente administrados
- Perfil de trabajo de propiedad corporativa de Android Enterprise
- Administrador de dispositivos Android

Para obtener información sobre cada método de inscripción y cómo elegir el adecuado para su organización, consulte la Guía de inscripción de dispositivos Android para Microsoft Intune.

TAREA	DETAIL	PLATAFORMA
Conectar una cuenta de Intune a una cuenta de Google Play administrado	Para habilitar la administración de Android Enterprise en Intune, conecte la cuenta de inquilino de Intune a la cuenta de Google Play administrado.	Android Enterprise
Configurar la inscripción de perfiles de trabajo para dispositivos de propiedad personal	Configure la administración de perfiles de trabajo para dispositivos de propiedad personal. Este método de inscripción crea un área independiente en el dispositivo para los datos relacionados con el trabajo, de modo que las cosas personales no se ven afectadas.	Android Enterprise
Configurar la inscripción de perfiles de trabajo para dispositivos de propiedad corporativa	Configure la administración de perfiles de trabajo para dispositivos de propiedad corporativa diseñados para uso personal y profesional. Este método de inscripción crea un área independiente en el dispositivo para los datos relacionados con el trabajo, de modo que las cosas personales no se ven afectadas.	Android Enterprise
Configurar la inscripción para dispositivos dedicados	Configure la inscripción para dispositivos de propiedad corporativa de tipo pantalla completa de un solo uso.	Android Enterprise
Configurar la inscripción para dispositivos totalmente administrados	Configure la inscripción para dispositivos de propiedad corporativa asociados a un único usuario y utilizados exclusivamente para el trabajo.	Android Enterprise
Inscribir dispositivos de perfil de trabajo de propiedad corporativa, dedicados y totalmente administrados	Después de configurar Intune para la inscripción de Android Enterprise, inscriba dispositivos mediante uno de los cinco métodos de inscripción admitidos.	Android Enterprise
Configuración de la inscripción del administrador de dispositivos	Configure la inscripción del Administrador de dispositivos Android. Android Enterprise ha reemplazado este método de administración de dispositivos, por lo que no se recomienda inscribir nuevos dispositivos de esta manera.	Administrador de dispositivos Android
Usar Samsung Knox Mobile Enrollment para inscribir automáticamente dispositivos Android	Configure Intune para Samsung Knox Mobile Enrollment (KME), que le permite inscribir automáticamente un gran número de dispositivos Android de propiedad corporativa.	Android Enterprise, Administrador de dispositivos Android

TAREA	DETAIL	PLATAFORMA
Identificar dispositivos como corporativos	Asigne el estado de propiedad corporativa a los dispositivos para habilitar más funcionalidades de administración e identificación en Intune. El estado de propiedad corporativa no se puede asignar a los dispositivos inscritos a través de Apple Business Manager.	Android Enterprise, Administrador de dispositivos Android
Cambiar la propiedad del dispositivo	Una vez inscrito un dispositivo, puede cambiar su etiqueta de propiedad en Intune a propiedad corporativa o personal. Este ajuste cambia la forma en que puede administrar el dispositivo.	Android Enterprise, Administrador de dispositivos Android
Solución de problemas de inscripción	Solucione los problemas que se producen durante la inscripción o busque opciones para resolverlos.	Android Enterprise, Administrador de dispositivos Android

Ejecución de acciones remotas

Una vez configurados los dispositivos, podrá usar acciones remotas en Intune para administrar los dispositivos y solucionar sus problemas a distancia. La disponibilidad varía según la plataforma del dispositivo. Si una acción falta en el portal o está deshabilitada, no se admite en el dispositivo.

TAREA	DETAIL
Ejecutar acciones remotas en Intune	Obtenga información sobre cómo explorar en profundidad dispositivos individuales en Intune, así como administrarlos de forma remota y solucionar sus problemas. En este artículo se enumeran todas las acciones remotas disponibles en Intune y los vínculos a esos procedimientos.
Corregir las vulnerabilidades que identifica Microsoft Defender para punto de conexión	Integre Intune con Microsoft Defender para punto de conexión para aprovechar las ventajas de la administración de amenazas y vulnerabilidades de Defender y usar Intune para corregir las debilidades de los puntos de conexión que se han identificado con la funcionalidad de administración de vulnerabilidades de Defender.
Borrar datos corporativos desde aplicaciones administradas por Intune	De forma selectiva, quite los datos relacionados con el trabajo de un dispositivo.

Pasos siguientes

Consulte estos tutoriales de inscripción para aprender a realizar algunas de las tareas principales en Intune. Los tutoriales son contenidos de nivel 100 - 200 para usuarios nuevos en Intune o en un escenario específico.

- Tutorial: Tutorial de Intune en Microsoft Endpoint Manager
- Configurar Slack para usar Intune para la administración de movilidad empresarial (EMM) y la configuración de aplicaciones

Para obtener la versión de iOS/iPadOS de esta guía, consulte Guía de implementación: Administración de dispositivos iOS/iPadOS en Microsoft Intune.

Configurar directivas administración de aplicaciones y cumplimiento de los dispositivos al migrar a Microsoft Intune

14/05/2021 • 3 minutes to read

El objetivo principal al migrar a Intune es que todos los dispositivos estén inscritos en Intune y cumplan con sus directivas. Las directivas de dispositivos no solo ayudan a administrar dispositivos de usuario único de propiedad corporativa, sino también dispositivos personales (BYOD) y compartidos, como pantallas completas, máquinas de punto de venta, tabletas compartidas entre varios alumnos en un aula o dispositivos sin usuario (solo iOS).

Puede que cada plataforma de dispositivo ofrezca una configuración diferente, pero las directivas de dispositivos de Intune funcionan con cada plataforma de dispositivo proporcionando las siguientes capacidades de administración de dispositivos móviles:

- Regular el número de dispositivos que cada usuario inscribe.
- Administrar la configuración de dispositivos (por ejemplo, cifrado de nivel de dispositivo, longitud de la contraseña, uso de la cámara).
- Entregar aplicaciones, perfiles de correo electrónico y perfiles de VPN, entre otros.
- Evaluar los criterios de nivel de dispositivo para las directivas de cumplimiento de seguridad.

> **IMPORTANT**
> Las directivas de administración de dispositivos no se asignan directamente a usuarios o dispositivos individuales, sino que se asignan a grupos de usuarios. Las directivas pueden aplicarse directamente a un grupo de usuarios y, por lo tanto, al dispositivo del usuario. También pueden aplicarse a un grupo de dispositivos y, por lo tanto, a los miembros del grupo.

Lista de tareas para directivas de cumplimiento de dispositivos

Tarea 1: Agregar grupos de dispositivos (opcional)

Puede crear grupos de dispositivos cuando tenga que realizar tareas administrativas en función de la identidad del dispositivo y no de la identidad del usuario.

Los grupos de dispositivos resultan prácticos para administrar dispositivos que no tienen usuarios dedicados, como dispositivos de pantalla completa, dispositivos compartidos entre trabajadores por turnos o dispositivos asignados a una ubicación concreta.

Si configura grupos de dispositivos antes de la inscripción de dispositivos, puede usar las categorías de dispositivos para unir dispositivos automáticamente a los grupos tras la inscripción. Después, recibirán las directivas de sus dispositivos de grupo automáticamente. Introducción a los grupos

Tarea 2: Usar perfiles de acceso a recursos (certificados de Wi-Fi, VPN y correo electrónico)

Los perfiles de acceso a recursos proporcionan configuraciones de acceso y certificados para dispositivos inscritos. Si está usando autenticación basada en certificados, configure los certificados.

Tarea 3: Crear e implementar perfiles de configuración de dispositivos

Tiene que crear un perfil de configuración de dispositivos para aplicar la configuración de nivel de dispositivo,

como, por ejemplo: deshabilitar la cámara, la tienda de aplicaciones, configurar el modo de aplicación sencilla y la pantalla principal, entre otros. Aprenda sobre los perfiles de dispositivo.

Importación directa de perfiles de configuración de iOS/iPadOS (opcional)

- **Perfiles de iOS de Apple Configurator (iOS 7.1 y posterior):** si la solución MDM existente usa perfiles de Apple Configurator (archivos .mobileconfig), Intune puede importarlos directamente como directivas de configuración personalizadas.
- **Directivas de configuración de aplicaciones móviles de iOS:** si la solución MDM existente usa directivas de configuración de aplicaciones móviles de iOS/iPadOS, Intune puede importarlas directamente siempre que cumplan con el formato XML especificado por Apple para las listas de propiedades.
- Obtenga información sobre cómo agregar una directiva personalizada de iOS.

Tarea 4: Crear e implementar directivas de cumplimiento de dispositivos (opcional)

Las directivas de cumplimiento de dispositivos evalúan la configuración orientada a la seguridad y ofrecen informes que muestran si los dispositivos son compatibles con los estándares corporativos o no. Dicha configuración incluye:

- Longitud del PIN
- Estado de liberado
- Versión del sistema operativo

Vea otros recursos de configuración de cumplimiento de dispositivos:

- Más información sobre las directivas de cumplimiento de dispositivos.

Tarea 5: Publicar e implementar aplicaciones

Cuando use la MDM de Intune, puede proporcionar aplicaciones requiriendo su instalación automática o poniéndolas a disposición de los usuarios en el portal de empresa.

- Cómo agregar aplicaciones.
- Cómo implementar aplicaciones.

Tarea 6: Permitir la inscripción de dispositivos

La inscripción de dispositivos es necesaria para administrar el dispositivo. Aprenda a prepararse para inscribir dispositivos de propiedad corporativa y personales de usuario.

Pasos siguientes

Configuración de directivas de protección de aplicaciones (opcional).

Configuración de directivas de protección de aplicaciones (opcional)

14/05/2021 • 2 minutes to read

Las directivas de protección de aplicaciones le permiten:

- Cifrar aplicaciones
- Definir un PIN cuando se obtiene acceso a la aplicación
- Impedir que las aplicaciones se ejecuten en dispositivos desbloqueados o modificados, así como muchas otras protecciones

Si el teléfono del usuario se ha perdido o robado, puede aplicar selectivamente el borrado de los datos corporativos de forma remota, a la vez que deja intactos los datos personales.

Las directivas de protección de aplicaciones aplican seguridad en el nivel de aplicación y no requieren la inscripción de dispositivos. Se pueden usar con dispositivos inscritos en Intune o no. Además, se pueden aplicar a dispositivos inscritos en un proveedor de MDM externo.

Directivas de protección de aplicaciones con aplicaciones LOB

También puede ampliar las directivas de protección de aplicaciones móviles a las aplicaciones de línea de negocio (LOB) con el SDK para aplicaciones de Microsoft Intune o la herramienta de ajuste de aplicaciones de Microsoft Intune para las plataformas iOS/iPadOS y Android. Para más información, vea la herramienta de ajuste de aplicaciones para iOS o la herramienta de ajuste de aplicaciones para Android. Además, vea Preparar aplicaciones de línea de negocio para las directivas de protección de aplicaciones.

¿Cómo ayudan las directivas de protección de aplicaciones durante la migración?

En una migración, debe quitar los dispositivos del proveedor de MDM antiguo e inscribirlos en Intune. Debe planear esto y animar a los usuarios finales a dejar el proveedor de MDM antiguo e inscribirse inmediatamente en Intune. Pero durante la migración puede haber usuarios que retrasen la finalización del proceso de inscripción y cuyos dispositivos no estén administrados por ningún proveedor de MDM.

Este período puede dejar a su organización más vulnerable al robo de dispositivos y a la pérdida de datos corporativos si todavía se permite el acceso a los recursos corporativos. También puede dar lugar a una reducción de la productividad del usuario si se bloquea el acceso a los recursos corporativos.

Intune puede ofrecer protección de datos corporativos durante la migración con el fin de que todavía pueda tener cobertura de seguridad para los datos corporativos cuando no haya ninguna administración de nivel de dispositivo.

Cuando deshabilita el acceso condicional en el proveedor de MDM antiguo, los usuarios pueden seguir siendo productivos mientras los incorpora a Intune.

Lista de tareas para directivas de protección de aplicaciones

- Creación y asignación de directivas de protección de aplicaciones

Pasos siguientes

Cómo presentar Microsoft Intune a los usuarios finales

14/05/2021 • 4 minutes to read

Con Microsoft Intune, los empleados pueden usar dispositivos móviles a la vez que los datos de la empresa se mantienen protegidos. Para probar la implementación de Intune en la organización, puede probar una evaluación gratuita.

Cuando implemente Microsoft Intune, es importante que los empleados comprendan la necesidad de movilidad empresarial y administración de dispositivos. Si no explica este aspecto, algunos usuarios podrían pensar que se está vulnerando su privacidad. La preocupación de los usuarios por su privacidad es aún mayor cuando se implementa Intune como una solución BYOD.

> **IMPORTANT**
> Por eso, para que la implementación sea eficaz, es importante comprender las preocupaciones de los usuarios sobre por qué la empresa necesita administrar dispositivos, y resolverlas de forma proactiva.

Que la adopción se realice correctamente no depende solo de la distribución de una tecnología nueva y funcional para todos los empleados. También consiste en conseguir que los usuarios comprendan la nueva tecnología y la adopten de manera positiva. Por eso es importante que los usuarios comprendan en qué consiste la seguridad de datos que ofrece Intune y la acepten.

Aspectos sobre los usuarios que se han de tener en cuenta

¿Qué nivel de experiencia en tecnología tienen los usuarios? Los conocimientos y la experiencia relacionados con la tecnología pueden variar de un usuario a otro. Esta experiencia podría ser positiva, como por ejemplo, hacer fotos de las vacaciones familiares, o podría ser negativa, como por ejemplo, un dispositivo que cae sin querer dentro del fregadero. Las experiencias influyen en el modo en que los usuarios se aproximan a la tecnología para uso personal y laboral.

¿Qué significa la administración de la movilidad para los usuarios? Puede que los usuarios no comprendan del todo el acceso que se tiene (o no se tiene) a sus dispositivos y sus datos. Es muy probable que a los usuarios les preocupe que los técnicos de TI y los jefes puedan rastrear sus acciones. Aquellos usuarios con menos experiencia podrían creer que toda la actividad que realizan en sus dispositivos es privada.

¿En qué podría molestar Intune a los usuarios? Tenga en cuenta y respete el tiempo que tardarán los usuarios en instalar aplicaciones, inscribir dispositivos y mantener el cumplimiento. La principal prioridad de todas las implementaciones de Intune es proteger los datos corporativos. Pero tenga en cuenta que los usuarios podrían adoptar una actitud negativa hacia la administración de dispositivos si fuerza directivas como estas:

- Exigir el uso de códigos de acceso no razonables en dispositivos personales
- Enviar actualizaciones de aplicaciones necesarias en medio de llamadas de trabajo importantes

Estas directivas también podrían afectar negativamente a la productividad de los empleados.

Cosas que debe hacer

En esta lista ofrecemos algunas sugerencias para facilitar la implementación de Intune para los usuarios de los dispositivos de la organización.

- **Tenga recursos.** Con la documentación de Intune, los usuarios podrán completar tareas específicas de Intune de manera más sencilla, como inscribir dispositivos y solucionar problemas. Los usuarios pueden hacer clic en algunos artículos para acceder directamente a ellos desde el Portal de empresa. Estos artículos específicos explican algunas tareas relacionadas con la instalación de la aplicación Portal de empresa, la inscripción en Intune y tareas generales que los usuarios pueden hacer en sus dispositivos, además de solución de problemas. En el artículo Usar dispositivos administrados para realizar el trabajo se ofrece también una lista de esta documentación.
- **Sea accesible.** Indique a los usuarios dónde pueden buscar ayuda para los problemas que tengan con sus dispositivos. Cuando personalice el Portal de empresa, no olvide incluir la información de contacto del administrador de TI.
- **Sea personal.** Proporcione instrucciones que sean específicas para la implementación de la organización. De este modo, está mostrando a los usuarios que se preocupa por su experiencia. Use esta kit de adopción de Intune personalizable para crear sus propias instrucciones de inscripción dirigidas a los usuarios.
- **Busque formas distintas de comunicarse.** Los usuarios tienen diferentes estilos de aprendizaje y maneras preferidas de usar la información. Para los más visuales, Intune ofrece versiones en vídeo de cómo inscribir distintos tipos de dispositivo en Channel 9. Estos vídeos se pueden incluir directamente en su propio sitio de SharePoint. También puede descargar copias locales de la pista de vídeo o audio.
- **Sea consciente.** La experiencia de usuario de Intune también tiene un impacto en la productividad. Al comprender la experiencia de los usuarios, resulta más fácil solucionar los problemas de los usuarios y los dispositivos. Por ejemplo, puede conocer y entender el modo en que los usuarios adquieren sus aplicaciones. Al conocer esta información con antelación, le resultará más fácil y rápido diagnosticar y corregir problemas.
- **Android**
  - Uso de un dispositivo Android con Intune
  - Cómo obtienen sus aplicaciones los usuarios de Android
- **iOS**
  - Cómo obtienen sus aplicaciones los usuarios de iOS/iPadOS
- **Windows**
  - Uso de un dispositivo Windows con Intune
  - Cómo obtienen sus aplicaciones los usuarios de Windows
- **Sea claro.** Indique claramente qué va a administrar en los dispositivos de los usuarios. Diga a los usuarios qué tipo de datos se van a recopilar y por qué. Infórmeles de cómo piensa usar todos estos datos. Microsoft cree que usted tiene derecho a conocer tanta información como sea posible sobre cómo gestionamos los datos de clientes en la nube, y cree que esta filosofía puede mejorar considerablemente la satisfacción del usuario con Intune.

> **NOTE**
> La transparencia, siempre que sea posible, es fundamental para el éxito de la implementación.

Pasos siguientes

Cree una declaración con la ayuda del departamento jurídico y de recursos humanos para tratar mejor las preocupaciones de los empleados sobre su privacidad. Es importante combinar confianza con directivas de cumplimiento bien diseñadas. Los usuarios deberían saber que aunque usted *pueda* consultar ciertos tipos de

datos personales, no *quiere* hacerlo. Ayúdeles a comprender que podrían exigirle responsabilidad por invadir su privacidad.

Ayudar a que los usuarios finales comprendan los mensajes de la aplicación Portal de empresa

14/05/2021 • 6 minutes to read

> **NOTE**
> La siguiente información se aplica solo a dispositivos con Android 6.0 y versiones posteriores y iOS 10 y versiones posteriores.

Comprenda los distintos mensajes de la aplicación que los usuarios finales pueden ver en Portal de empresa. Normalmente, estos mensajes de la aplicación se muestran en distintos puntos del proceso de inscripción. Descubra dónde aparecen, cuál es su significado y qué ocurre si los usuarios deniegan el acceso. Además, aprenderá a explicar mejor los mensajes a los usuarios.

- **¿Permitir que el Portal de empresa realice y administre llamadas telefónicas?**
- **¿Permitir que Portal de empresa tenga acceso a fotos, elementos multimedia y archivos del dispositivo?**

> **NOTE**
> No vendemos ningún dato recogido por nuestro servicio a terceros por ningún motivo.

¿Permitir que Portal de empresa realice y administre llamadas telefónicas?

Dónde aparece

El mensaje **¿Permitir que Portal de empresa realice y administre llamadas telefónicas?** aparece cuando los usuarios pulsan **Inscribir** en la aplicación Portal de empresa mientras inscriben su dispositivo.

Significado

Al aceptar este aviso, los usuarios permiten que se envíen los números de teléfono y de IMEI del dispositivo al servicio Intune. Aparecerán en la consola de administración en la página **Hardware**.

> **NOTE**
> **La aplicación Portal de empresa nunca hace ni administra llamadas telefónicas.** Google controla el texto del mensaje y no se puede cambiar.

Para ver la página **Hardware**, debe ir a **Grupos** > **All mobile devices (Todos los dispositivos móviles)** > **Dispositivos**. Seleccione el dispositivo del usuario y vaya a **Ver propiedades** > **Hardware**.

Qué sucede si los usuarios deniegan el acceso

Si los usuarios deniegan el acceso, pueden seguir usando la aplicación de Portal de empresa e inscribir su dispositivo. Sin embargo, el número de teléfono y el IMEI del dispositivo estarán en blanco en la página de **hardware** de la consola de administración. La segunda vez que los usuarios inician sesión en la aplicación Portal de empresa después de denegar el acceso, el mensaje muestra una casilla de verificación **Never ask again** (No volver a preguntar) que los usuarios pueden marcar para detener el aviso.

Si los usuarios permiten el acceso, pero luego lo deniegan, el mensaje aparecerá la próxima vez que los usuarios inicien sesión en la aplicación Portal de empresa después de la inscripción.

Si los usuarios más adelante deciden permitir el acceso, pueden ir a **Configuración** > **Aplicaciones** > **Portal de empresa** > **Permisos** > **Teléfono** y activarlo.

Cómo explicar esto a los usuarios

Envíe a los usuarios a Inscribir el dispositivo Android en Intune para más información.

Allow Company Portal to access your contacts? (¿Permitir que el portal de empresa tenga acceso a los contactos?)

Dónde aparece

El mensaje **¿Permitir que el portal de empresa tenga acceso a los contactos?** aparece cuando los usuarios pulsan **Inscribir** en la aplicación Portal de empresa mientras inscriben el dispositivo.

Significado

Al aceptar este aviso, los usuarios permiten a Intune crear su cuenta de trabajo y administrar la identidad de Azure Active Directory registrada para el usuario en ese dispositivo.

> **NOTE**
> **Microsoft nunca accede a los contactos.** Google controla el texto del mensaje y no se puede cambiar.

Qué sucede si los usuarios deniegan el acceso

Si los usuarios deniegan el acceso, el dispositivo no se inscribirá en Intune ni se podrá administrar. La segunda vez que los usuarios inician sesión en la aplicación Portal de empresa después de denegar el acceso, el mensaje muestra una casilla **No volver a preguntar** que los usuarios pueden seleccionar para detener el aviso.

Si los usuarios permiten el acceso, pero luego lo deniegan, el mensaje aparece la próxima vez que los usuarios inicien sesión en la aplicación Portal de empresa después de la inscripción.

Si los usuarios más adelante deciden permitir el acceso, pueden ir a **Configuración** > **Aplicaciones** > **Portal de empresa** > **Permisos** > **Teléfono** y activarlo.

Cómo explicar esto a los usuarios

Envíe a los usuarios a Inscribir el dispositivo Android en Intune para más información.

¿Permitir que Portal de empresa tenga acceso a fotos, elementos multimedia y archivos del dispositivo?

Dónde aparece

El mensaje **¿Permitir que Portal de empresa tenga acceso a fotos, elementos multimedia y archivos del dispositivo?** aparece cuando los usuarios pulsan **Enviar datos** para enviar registros a su administrador de TI.

Significado

Al aceptar este aviso, los usuarios permiten que su dispositivo escriba registros de datos en la tarjeta SD de este. Esto también permite que esos registros se trasladen mediante un cable USB.

> **NOTE**
> **La aplicación Portal de empresa nunca tiene acceso a las fotos, elementos multimedia ni archivos de los usuarios.** Google controla el texto del mensaje y no se puede cambiar.

Qué sucede si los usuarios deniegan el acceso

Si los usuarios deniegan el acceso, podrán enviar registros de datos por correo electrónico, pero los registros no se copiarán en la tarjeta SD del dispositivo.

La segunda vez que los usuarios inician sesión en la aplicación Portal de empresa después de denegar el acceso, el mensaje muestra una casilla **No volver a preguntar** que los usuarios pueden seleccionar para que el mensaje no se vuelva a mostrar. Si los usuarios permiten el acceso, pero luego lo deniegan, el mensaje aparece la próxima vez que los usuarios intenten enviar registros. No obstante, si los usuarios más adelante deciden permitir el acceso, pueden ir a **Configuración** > **Aplicaciones** > **Portal de empresa** > **Permisos** > **Almacenamiento** y activar el permiso.

Cómo explicar esto a los usuarios

Envíe a sus usuarios a Enviar registros al administrador de TI mediante correo electrónico.

El servicio de soporte técnico de su empresa debe concederle acceso a sus recursos

Dónde aparece

Si no ha agregado la aplicación Portal de empresa a las listas **Aplicaciones permitidas** o **Aplicaciones exentas** y un usuario intenta iniciar sesión, se producirá un error en el inicio de sesión. Se mostrará el siguiente mensaje:

> **El servicio de soporte técnico de su empresa debe concederle acceso a sus recursos**
> Su empresa está usando directivas de Windows Information Protection para proteger su dispositivo. El servicio de soporte técnico de su empresa tendrá que asegurarse de que permite que Portal de empresa pueda acceder a esos recursos.

Significado

Agregue Portal de empresa a las listas **Aplicaciones permitidas** o **Aplicaciones exentas** en la directiva de protección de aplicaciones de Windows Information Protection (WIP). Para obtener más información, consulte Creación e implementación de una directiva de protección de aplicaciones de Windows Information Protection (WIP) con Intune.

Aprobación de una aplicación de empresa iOS/iPadOS (aplicación de línea de negocio) en un dispositivo iOS/iPadOS

Dónde aparece

De manera predeterminada, su dispositivo no confía en las aplicaciones iOS que desarrolla su organización que no están disponibles en App Store. Cuando instala ese tipo de aplicaciones con Portal de empresa de Intune e inicia la aplicación, se muestra este mensaje:

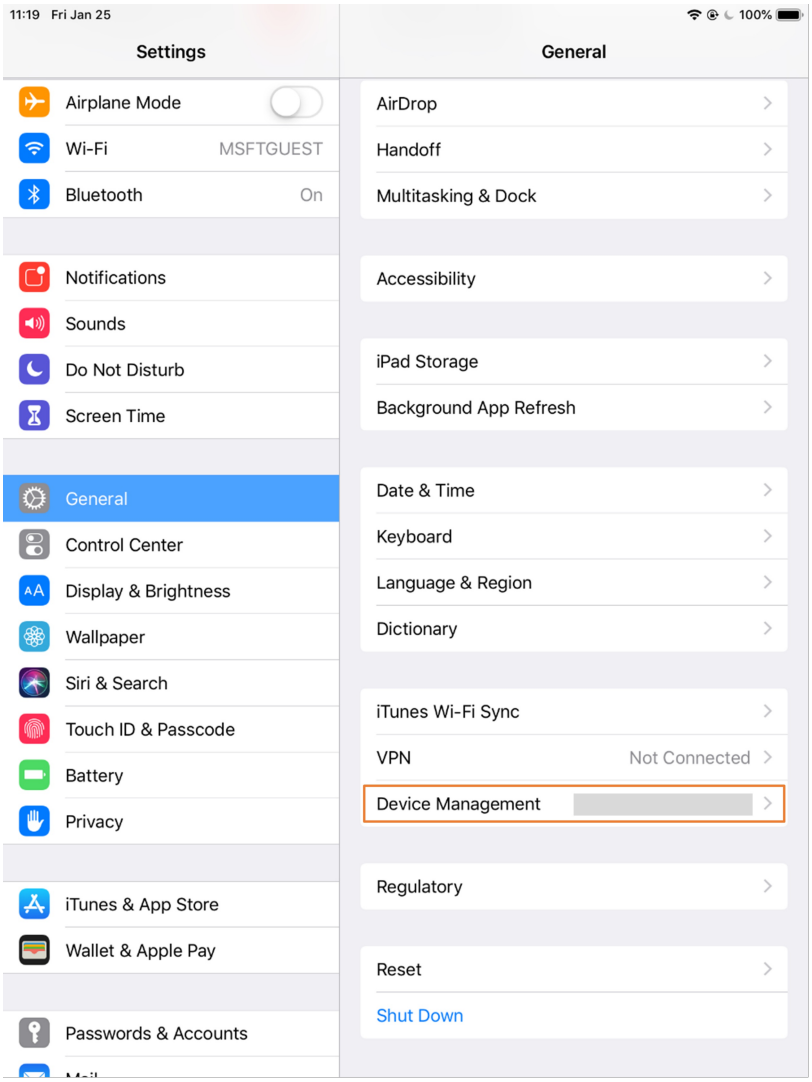
Significado

Este mensaje significa que tendrá que modificar la configuración del dispositivo iOS/iPadOS para aprobar e instalar una aplicación desarrollada por la empresa en el dispositivo iOS/iPadOS.

Cuando instala ese tipo de aplicaciones con Portal de empresa de Intune e inicia la aplicación, siga estos pasos para aprobar la aplicación después de descargarla:

1. Después de iniciar una aplicación de empresa instalada (aplicación de línea de negocio), verá el mensaje "Desarrollador empresarial no confiable".
   Presione **Cancelar**.

2. Vaya a **Configuración** > **General** > **Administración de dispositivos**.



3. Seleccione **Perfil de administración** > **Aplicación de empresa**.

4. Seleccione el nombre del desarrollador.

5. Presione **Confiar en** ***nombre del desarrollador*** .

6. Para confirmar la aplicación, seleccione **Confiar** en el mensaje emergente de instalación de la aplicación.

Debería ser capaz de iniciar y usar la aplicación de empresa.

Vea también

Qué decirles a los usuarios finales sobre el uso de Intune

Qué esperar cuando la aplicación Android está administrada por directivas de protección de aplicaciones

14/05/2021 • 3 minutes to read

En este artículo se describe la experiencia del usuario con aplicaciones con directivas de protección de aplicaciones. Las directivas de protección de aplicaciones solo se aplican cuando se usan aplicaciones en el contexto laboral, por ejemplo, cuando el usuario accede a las aplicaciones con una cuenta profesional o a archivos que están almacenados en una ubicación de OneDrive para la Empresa.

Acceso a las aplicaciones

La aplicación Portal de empresa se necesita en todas las aplicaciones que están asociadas a directivas de protección de aplicaciones en los dispositivos Android.

En el caso de los dispositivos que no están inscritos en Intune, la aplicación Portal de empresa debe instalarse en el dispositivo. En cambio, el usuario no tiene que iniciar la aplicación Portal de empresa ni iniciar sesión en ella para poder usar aplicaciones administradas por directivas de protección de aplicaciones.

La aplicación Portal de empresa es una manera de que Intune pueda compartir datos en una ubicación protegida. Por lo tanto, la aplicación Portal de empresa es un requisito para todas las aplicaciones asociadas con las directivas de protección de aplicaciones, incluso si el dispositivo no está inscrito en Intune.

Uso de aplicaciones con compatibilidad con varias identidades

Las directivas de protección de aplicaciones solo se aplican en el contexto laboral. Por lo tanto, la aplicación podría comportarse de manera distinta si el contexto es laboral o personal.

Por ejemplo, el usuario obtiene una solicitud de PIN al obtener acceso a los datos de trabajo. En la **aplicación Outlook**, al usuario se le pide un PIN al iniciar la aplicación. En la **aplicación OneDrive**, al usuario se le pide el PIN cuando escribe la cuenta profesional. En Microsoft **Word**, **PowerPoint** y **Excel**, al usuario se le pide el PIN cuando obtiene acceso a documentos que se encuentran almacenados en la ubicación OneDrive para la Empresa.

Administración de cuentas de usuario en el dispositivo

Las aplicaciones de varias identidades permiten a los usuarios agregar varias cuentas. Intune App solo admite una cuenta administrada. Intune App no limita el número de cuentas no administradas.

Cuando hay una cuenta administrada en una aplicación:

- Si un usuario intenta agregar una segunda cuenta administrada, se le pide que seleccione cuál quiere usar. La otra cuenta se quita.
- Si el administrador de TI agrega una directiva a una segunda cuenta existente, se pide al usuario que seleccione qué cuenta administrada quiere usar. La otra cuenta se quita.

Consulte el siguiente escenario de ejemplo para profundizar aún más en cómo se tratan varias cuentas de usuario.

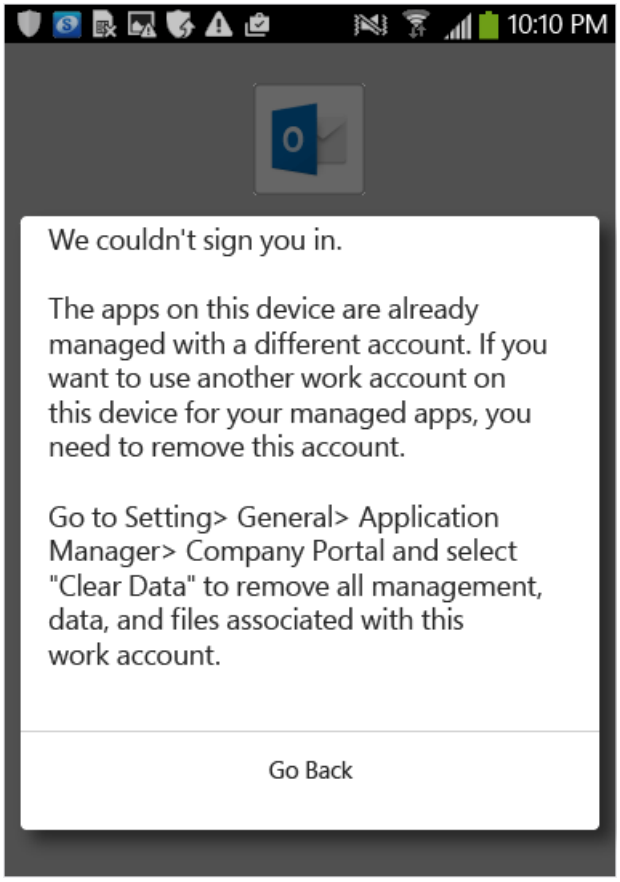
El usuario A trabaja para dos empresas: la **empresa X** y la **empresa Y**. El usuario A tiene una cuenta

profesional para cada empresa y en ambas se usa Intune para implementar directivas de protección de aplicaciones. La **Empresa X** implementa directivas de protección de aplicaciones **antes que** la **Empresa Y**. La cuenta que está asociada a la **empresa X** obtiene la directiva de protección de aplicaciones, pero no la cuenta asociada a la empresa Y. Si quiere que la cuenta de usuario asociada a la empresa Y se administre mediante las directivas de protección de aplicaciones, deberá quitar la cuenta de usuario asociada a la empresa X y agregar la cuenta de usuario que esté asociada a la empresa Y.

Incorporación de una segunda cuenta

Android

Si usa un dispositivo Android, podría aparecer un mensaje de bloqueo con instrucciones para quitar la cuenta existente y agregar una nueva. Para quitar la cuenta existente, vaya a **Configuración** > **General** > **Administrador de aplicaciones** > **Portal de empresa**. Luego, elija **Borrar datos**.



Visualización de archivos multimedia con la aplicación de Azure Information Protection

Para ver archivos de imagen, AV y PDF de la empresa en dispositivos Android, use la aplicación Azure Information Protection (conocida anteriormente como la aplicación Rights Management sharing).

Descargue esta aplicación de Google Play Store.

Se admiten los siguientes tipos de archivos:

- **Audio:** AAC LC, HE-AACv1 (AAC+), HE-AACv2 (AAC+ mejorado), AAC ELD (AAC retraso bajo mejorado), AMR-NB, AMR-WB, FLAC, MP3, MIDI, Ogg Vorbis
- **Vídeo:** H.263, H.264 AVC, MPEG-4 SP, VP8
- **Imagen:** .jpg, .pjpg, .png, .ppng, .bmp, .pbmp, .gif, .pgif, .jpeg, .pjpeg
- **Documentos:** PDF, PPDF

PFILE
Pfile es un formato "contenedor" genérico para archivos protegidos que encapsula el contenido cifrado y las licencias de Azure Information Protection. Puede usarse para proteger cualquier tipo de archivo.

Pasos siguientes

Qué esperar cuando la aplicación iOS/iPadOS se administra con directivas de protección de aplicaciones

Qué esperar cuando la aplicación iOS/iPadOS se administra con directivas de protección de aplicaciones

14/05/2021 • 3 minutes to read

Las directivas de protección de aplicaciones de Intune se aplican a las aplicaciones que se usan para el trabajo o la escuela. Esto significa que, cuando los empleados y los alumnos usan sus aplicaciones en un contexto personal, es posible que no noten ninguna diferencia en su experiencia. Sin embargo, en el contexto profesional o educativo, pueden recibir mensajes para tomar decisiones con respecto a la cuenta, actualizar su configuración o ponerse en contacto con usted para obtener ayuda. Use este artículo para obtener información sobre lo que experimentan los usuarios cuando intentan acceder a aplicaciones protegidas por Intune y usarlas.

Acceso a las aplicaciones

Si el dispositivo **no está inscrito en Intune**, al usuario final se le pide que reinicie la aplicación cuando la use por primera vez. Se requiere un reinicio para poder aplicar directivas de protección de aplicaciones a la aplicación.

En los dispositivos que **están inscritos para la administración en Intune**, el usuario ve un mensaje que indica que la aplicación ahora está administrada.

Uso de aplicaciones con compatibilidad con varias identidades

Las aplicaciones que admiten varias identidades permiten usar diferentes cuentas de trabajo y personales para tener acceso a las mismas aplicaciones. Las directivas de protección de aplicaciones, como escribir un PIN de dispositivo, se activan cuando los usuarios acceden a estas aplicaciones en un contexto profesional o educativo.

Los usuarios pueden experimentar la solicitud de PIN de manera diferente en todas sus aplicaciones, en función de cómo configure las directivas. Por ejemplo, puede configurar las directivas para que:

- Microsoft Outlook solicite al usuario un PIN cuando inicie la aplicación.
- OneDrive solicite al usuario un PIN cuando inicie sesión en su cuenta profesional.
- Microsoft Word, PowerPoint y Excel soliciten un PIN al usuario cuando acceda a documentos almacenados en la ubicación de OneDrive para la Empresa.

- Obtenga más información sobre las aplicaciones que admiten protección de aplicaciones y varias identidades con Intune.

Administración de cuentas de usuario en el dispositivo

Las directivas de protección de aplicaciones de Intune limitan a los usuarios a una cuenta profesional o educativa administrada por aplicación. Las directivas de protección de aplicaciones no limitan el número de cuentas no administradas que un usuario puede agregar.

- Si un usuario intenta agregar una segunda cuenta administrada, se le pide que seleccione cuál quiere usar. Si el usuario agrega la segunda cuenta, se quita la primera.
- Si agrega directivas de protección a otra de las cuentas del usuario, se le pedirá al usuario que seleccione la cuenta administrada que se va a usar. La otra cuenta se quita.

Algunos usuarios no tendrán la opción de cambiar o seleccionar entre cuentas administradas. La opción no está

disponible en los dispositivos que:

- Administra Intune
- Los administran soluciones de Enterprise Mobility Management y se configuran con el valor IntuneMAMUPN

En el escenario de ejemplo siguiente se describe cómo se tratan varias cuentas de usuario:

El usuario A trabaja para dos empresas: la **empresa X** y la **empresa Y**. El usuario A tiene una cuenta profesional para cada empresa y en ambas se usa Intune para implementar directivas de protección de aplicaciones. La **Empresa X** implementa directivas de protección de aplicaciones **antes que** la **Empresa Y**. La cuenta que está asociada a la **empresa X** obtiene la directiva de protección de aplicaciones en primer lugar. Si quiere que la cuenta de usuario asociada a la empresa Y se administre mediante las directivas de protección de aplicaciones, deberá quitar la cuenta de usuario asociada a la empresa X y agregar la cuenta de usuario que esté asociada a la empresa Y.

Pasos siguientes

What to expect when your Android app is managed by app protection policies (Qué esperar cuando la aplicación Android se administra con directivas de protección de aplicaciones)

Cómo obtienen sus aplicaciones los usuarios de Android

14/05/2021 • 3 minutes to read

Este artículo le ayuda a comprender cómo y dónde obtienen los usuarios finales y los administradores de dispositivos Android las aplicaciones que se distribuyen a través de Microsoft Intune. La información puede variar por tipo de dispositivo (dispositivos Android nativos o dispositivos Samsung Knox Standard).

Dispositivos Android nativos (distintos a Samsung KNOX Standard)

TIPO DE APLICACIÓN	APLICACIONES DE LÍNEA DE NEGOCIO (LOB)	APLICACIONES DE PLAY STORE
Aplicaciones disponibles	Los usuarios tocan **instalar** en el Portal de empresa. Aparece una notificación que los usuarios tocan para iniciar la instalación. Una vez realizada la instalación correctamente, la notificación desaparece.	Los usuarios tocan la aplicación del Portal de empresa y se les dirige a una página de la aplicación en la Play Store. Aquí es donde inician la instalación.
Required apps	Los usuarios ven una notificación, que no se puede descartar y que indica que deben instalar una aplicación. Los usuarios tocan la notificación para iniciar la instalación. Una vez realizada la instalación correctamente, la notificación desaparece.	Los usuarios ven una notificación, que no se puede descartar y que indica que deben instalar una aplicación. Los usuarios tocan la notificación y se les dirige a una página de la aplicación en la Play Store. Aquí es donde inician la instalación. Una vez realizada la instalación correctamente, la notificación desaparece.

Los usuarios finales necesitan permitir la instalación desde orígenes desconocidos para poder instalar aplicaciones de LOB. Esta configuración se encuentra normalmente en dos lugares diferentes, en función de la versión de Android:

- Android 7.1.2 y versiones anteriores: **Configuración** > **Seguridad** > **Orígenes desconocidos**
- Android 8.0 y versiones posteriores: **Configuración** > **Aplicaciones y notificaciones** > **Acceso especial a las aplicaciones** > **Instalar aplicaciones desconocidas** > **Portal de empresa** > **Permitir desde este origen**

Si ocurre esto, la aplicación Portal de empresa informará y guiará directamente al usuario final hasta la configuración adecuada.

Dispositivos Samsung Knox Standard con Android

TIPO DE APLICACIÓN	APLICACIONES DE LÍNEA DE NEGOCIO (LOB)	APLICACIONES DE PLAY STORE
Aplicaciones disponibles	Los usuarios tocan **instalar** en el Portal de empresa. La aplicación se instala sin la intervención del usuario.	Los usuarios tocan la aplicación del Portal de empresa y se les dirige a una página de la aplicación en la Play Store. Aquí es donde inician la instalación.

TIPO DE APLICACIÓN	APLICACIONES DE LÍNEA DE NEGOCIO (LOB)	APLICACIONES DE PLAY STORE
Required apps	La aplicación se instala sin la intervención del usuario.	Los usuarios ven una notificación, que no se puede descartar y que indica que deben instalar una aplicación. Los usuarios tocan la notificación y se les dirige a una página de la aplicación en la Play Store. Aquí es donde inician la instalación. Una vez realizada la instalación correctamente, la notificación desaparece.

Las aplicaciones pueden ser administradas o no administradas, tal como se describe a continuación. El proceso de crear aplicaciones administradas es el mismo para todos los tipos de dispositivos Android.

- Aplicaciones administradas: estas aplicaciones se administran a través de directivas. Intune las ha "encapsulado" o compilado mediante el SDK para aplicaciones de Intune. Estas aplicaciones pueden administrarse mediante Intune y las directivas de aplicación pueden aplicarse a estas.
- Aplicaciones no administradas: estas aplicaciones no se administran a través de directivas. Intune no las ha encapsulado o no incorporan el SDK para aplicaciones de Intune. Las directivas de aplicación no pueden aplicarse a estas aplicaciones.

Dispositivos Zebra con Zebra Mobility Extensions

Intune usa el kit de herramientas Zebra Mobility Extensions (MX) para instalar de forma silenciosa aplicaciones en dispositivos Zebra administrados por el administrador de dispositivos. Esta característica permite implementar y actualizar aplicaciones en dispositivos Zebra sin intervención del usuario. Si la versión MX del dispositivo es 4.2 o anterior, las aplicaciones no se instalan de forma silenciosa. Para obtener más información, vea la página sobre la matriz completa de características de MX en el sitio web de Zebra.

Las aplicaciones de LOB implementadas en dispositivos Zebra deben instalarse desde una ubicación pública en el dispositivo. El paquete de la aplicación. apk puede ser accesible para otras aplicaciones y servicios que también tienen acceso al almacenamiento público en el dispositivo. Normalmente, este acceso es una ventana pequeña entre la finalización de la descarga de la aplicación y el principio de la instalación. Esta ventana puede permitir un ataque de temporización. Por ejemplo, un paquete. apk se podría cambiar durante esta ventana. Intune reduce la cantidad de tiempo que el .apk pasa en el almacenamiento público y no permite la instalación de aplicaciones sin firmar. Para ayudar a minimizar el riesgo de seguridad, asegúrese de que los archivos. apk que cargue no contengan información confidencial.

Vea también

Agregar aplicaciones con Microsoft Intune

Cómo obtienen sus aplicaciones los usuarios de iOS/iPadOS

Cómo obtienen sus aplicaciones los usuarios de Windows

Cómo obtienen sus aplicaciones los usuarios de iOS/iPadOS

14/05/2021 • 2 minutes to read

Lea esta información para comprender cómo y dónde obtienen los usuarios finales las aplicaciones que se distribuyen a través de Microsoft Intune.

Aplicaciones obligatorias: son las aplicaciones que exige el administrador y que se instalan en el dispositivo con intervención mínima del usuario, según la plataforma.

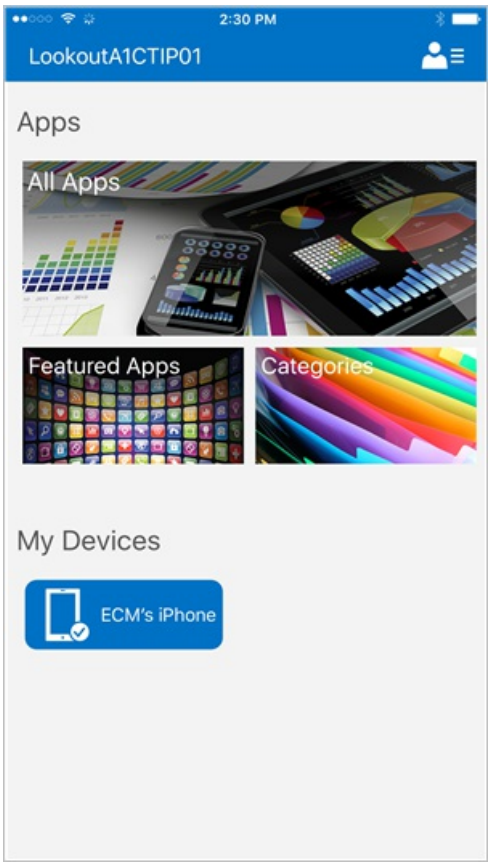
Aplicaciones disponibles: son las aplicaciones que se proporcionan en la lista de aplicaciones de portal de empresa y que un usuario puede instalar si quiere.

Aplicaciones administradas: son aplicaciones que se pueden administrar mediante directivas y que se han "encapsulado" con Intune o se han creado con el kit de desarrollo de software (SDK) para aplicaciones de Intune. Estas aplicaciones pueden administrarse mediante Intune y las directivas de protección de aplicaciones pueden aplicarse a estas.

Aplicaciones no administradas: las aplicaciones que los usuarios pueden descargar desde el App Store de iOS/iPadOS que no están integradas con el SDK para aplicaciones de Intune. Intune no tiene ningún control sobre la distribución, la administración o el borrado selectivo de estas aplicaciones.

Los usuarios inscritos obtienen sus aplicaciones tocando en los iconos siguientes de la pantalla de aplicaciones de la aplicación del Portal de empresa:

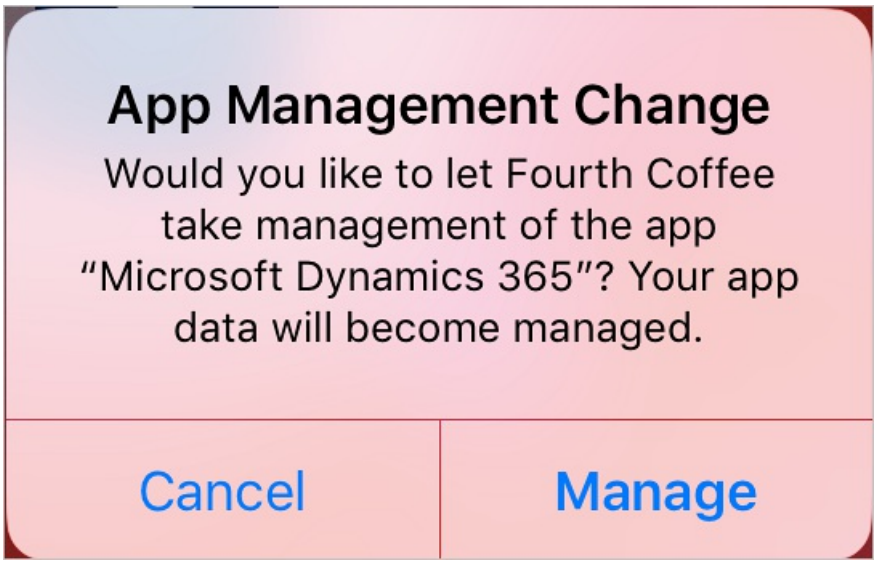
- **Todas las aplicaciones** apunta a una lista de todas las aplicaciones en la pestaña TODO del sitio web del Portal de empresa.
- **Las aplicaciones destacadas** llevarán a los usuarios a la pestaña DESTACADOS del sitio web del Portal de empresa.
- **Categorías** apunta a la pestaña CATEGORÍAS del sitio web del Portal de empresa.



Para más información sobre cómo agregar aplicaciones, vea Agregar una aplicación a Microsoft Intune.

Toma de control de la administración de aplicaciones

Si una aplicación ya está instalada en el dispositivo de un usuario final, el dispositivo iOS o iPadOS muestra una alerta para permitir la administración de la aplicación por parte de su organización. El usuario final debe permitir que la organización asuma la administración de la aplicación para de que se puedan aplicar las configuraciones de aplicaciones en un dispositivo administrado. Si el usuario cancela la alerta, la alerta aparecerá periódicamente mientras el dispositivo se administre y la aplicación se asigne.



Vea también

Cómo obtienen sus aplicaciones los usuarios de Android

Cómo obtienen sus aplicaciones los usuarios de Windows

Cómo obtienen sus aplicaciones los usuarios de Windows

14/05/2021 • 2 minutes to read

Lea esta información para comprender cómo y dónde obtienen los usuarios las aplicaciones que se distribuyen a través de Microsoft Intune.

Las **aplicaciones obligatorias** las exige el administrador y se instalan en el dispositivo con intervención mínima del usuario, según la plataforma.

Las **aplicaciones disponibles** se proporcionan en la lista de la aplicación Portal de empresa que un usuario puede elegir instalar.

Las **aplicaciones administradas** se pueden administrar mediante directivas y que se han "encapsulado" con Intune o se han creado con el kit de desarrollo de software (SDK) de aplicaciones de Intune. Estas aplicaciones pueden administrarse mediante Intune y las directivas de protección de aplicaciones pueden aplicarse a estas.

Las **aplicaciones no administradas** se pueden administrar mediante directivas y no se han encapsulado con Intune o no incorporan el SDK para aplicaciones de Intune. Las directivas de protección de aplicaciones no pueden aplicarse a estas aplicaciones.

Vea también

Cómo obtienen sus aplicaciones los usuarios de Android Cómo obtienen sus aplicaciones los usuarios de iOS/iPadOS

Datos que Intune manda a Apple

14/05/2021 • 2 minutes to read

Cuando se habilita cualquiera de los siguientes servicios de Apple en un dispositivo, Microsoft Intune establece una conexión con Apple y comparte información del usuario y el dispositivo con Apple:

- Programa de inscripción de dispositivos (DEP) de Apple
- Certificado push MDM de Apple (APNS)
- Apple School Manager (ASM)
- Programa de Compras por Volumen de Apple (VPP)

Para que Microsoft Intune pueda establecer una conexión, debe crear una cuenta de Apple para cada servicio de Apple.

En la tabla siguiente se muestran los datos que Microsoft Intune envía desde un dispositivo a los servicios habilitados de Apple.

SERVICIO	DATOS QUE SE ENVÍAN A APPLE	USADA PARA
APNS	Token, PushMagic	Si el servidor acepta el dispositivo, este proporciona su token de dispositivo de notificación push al servidor. El servidor debe usar este token para enviar mensajes push al dispositivo. Este mensaje de registro también contiene una cadena de PushMagic. El servidor debe recordar esta cadena e incluirla en cualquier mensaje push que envíe al dispositivo.
ASM/DEP	Token de servidor	Token de dispositivo de notificación push usado para autenticar el servicio de Apple.
ASM/DEP	server_name	Nombre de identificación del servidor MDM.
ASM/DEP	server_uuid	Identificador del servidor generado por el sistema.
ASM/DEP	admin_id	ID de Apple de la persona que ha generado los tokens actuales que están en uso.
ASM/DEP	org_name	Nombre de la organización.
ASM/DEP	org_email	Dirección de correo electrónico de la organización.
ASM/DEP	org_phone	Teléfono de la organización.
ASM/DEP	org_address	Dirección de la organización.

SERVICIO	DATOS QUE SE ENVÍAN A APPLE	USADA PARA
ASM/DEP	org_id	Id. de cliente de DEP. Esta clave solo está disponible en la versión 3 del protocolo y versiones posteriores.
ASM/DEP	serial_number	Número de serie del dispositivo (cadena).
ASM/DEP	modelo	Nombre del modelo (cadena).
ASM/DEP	description	Descripción del dispositivo (cadena).
ASM/DEP	asset_tag	Etiqueta de activo del dispositivo (cadena).
ASM/DEP	profile_status	Estado de instalación del perfil. Los valores posibles son **vacío**, **asignado**, **insertado** o **eliminado**.
ASM/DEP	profile_uuid	Identificador único del perfil asignado.
ASM/DEP	device_assigned_by	Dirección de correo electrónico de la persona que ha asignado el dispositivo.
ASM/DEP	os	Sistema operativo del dispositivo: iOS/iPadOS, OSX o tvOS. Esta clave es válida en X-Server-Protocol-Version 2 y versiones posteriores.
ASM/DEP	device_family	Familia de productos de Apple del dispositivo: iPad, iPhone, iPod, Mac o AppleTV. Esta clave es válida en X-Server-Protocol-Version 2 y versiones posteriores.
ASM/DEP	profile_name	Cadena. Nombre legible para el perfil.
ASM/DEP	support_phone_number	Opcional. Cadena. Número de teléfono de soporte técnico de la organización.
ASM/DEP	support_email_address	Opcional. Cadena. Dirección de correo electrónico de soporte técnico de la organización. Esta clave es válida en X-Server-Protocol-Version 2 y versiones posteriores.
ASM/DEP	department	Opcional. Cadena. Nombre de la ubicación o el departamento definido por el usuario.
ASM/DEP	dispositivos	Matriz de cadenas que contienen números de serie de dispositivos. (Puede estar vacía).
VPP	Intune UserId guid	GUID generado por Intune.

SERVICIO	DATOS QUE SE ENVÍAN A APPLE	USADA PARA
VPP	Managed AppleId UPN	ID de Apple especificado por el administrador al configurar la conexión de token de ubicación de Apple Business Manager (token de VPP) con Apple.
VPP	Número de serie	Número de serie del dispositivo administrado.

Para dejar de usar los servicios de Apple con Microsoft Intune y eliminar los datos, debe deshabilitar la administración de token de Apple de Microsoft Intune y también eliminar su cuenta de Apple. Consulte en la cuenta de Apple cómo realizar la administración de la cuenta.

Datos que Intune manda a Google

14/05/2021 • 2 minutes to read

Cuando se habilita la administración de dispositivos empresariales Android en un dispositivo, Microsoft Intune establece una conexión con Google y comparte información del usuario y el dispositivo con Google. Antes de que Microsoft Intune pueda establecer una conexión, debe crear una cuenta de Google.

En la tabla siguiente se enumeran los datos que Microsoft Intune envía a Google cuando está habilitada la administración de dispositivos en un dispositivo:

DATOS QUE SE ENVÍAN A GOOGLE	DETALLES	USADA PARA	EJEMPLO
EnterpriseId	Se originan en Google al enlazar la cuenta de Gmail con Intune.	Identificador principal que se usa para comunicarse entre Intune y Google. Esta comunicación incluye la configuración de directivas, la administración de dispositivos y el enlace o desenlace de la empresa Android con Intune.	Identificador único, formato de ejemplo: LC04eik8a6
Cuerpo de la directiva	Se origina en Intune cuando se guarda una nueva directiva de aplicación o configuración.	Aplicar directivas a los dispositivos.	Se trata de una colección de todos los valores configurados para una directiva de aplicación o configuración. Puede contener información del cliente si se proporciona como parte de una directiva, como nombres de red, nombres de aplicaciones y configuración específica de la aplicación.

DATOS QUE SE ENVÍAN A GOOGLE	DETALLES	USADA PARA	EJEMPLO
Datos del dispositivo	Los escenarios de perfil de trabajo de dispositivos Android Enterprise de propiedad personal y corporativa se inician con la inscripción en Intune. Los dispositivos de escenarios de dispositivo administrado comienzan con la inscripción en Google.	La información de los datos del dispositivo se envía entre Intune y Google para realizar varias acciones como la aplicación de directivas, la administración del dispositivo y la creación de informes generales.	**Identificador único para representar el nombre del dispositivo.** Ejemplo: enterprises/LC04ebru7b/devices/3592d971168f9ae4 **Identificador único para representar el nombre de usuario.** Ejemplo: Enterprises/LC04ebru7b/users/116838519924207449711 **Estado del dispositivo.** Ejemplos: activo, deshabilitado, aprovisionamiento. **Estados de cumplimiento.** Ejemplos: configuración no admitida, faltan aplicaciones necesarias **Información del software.** Ejemplos: versiones de software y nivel de revisión. **Información de red.** Ejemplos: IMEI, MEID, WifiMacAddress **Configuración del dispositivo.** Ejemplos: información sobre niveles de cifrado y si el dispositivo permite aplicaciones desconocidas. Vea a continuación un ejemplo de un mensaje JSON.
newPassword	Se origina en Intune.	Restablecer la contraseña del dispositivo.	Cadena que representa una nueva contraseña.
Usuario de Google	Google	Administración del perfil del trabajo para escenarios de perfil de trabajo de propiedad personal (BYOD).	Identificador único para representar la cuenta de Gmail vinculada. Ejemplo: 114223373813435875042
Datos de aplicaciones	Se origina en Intune al guardar la directiva de aplicación.		Cadena de nombre de aplicación. Ejemplo: app:com.microsoft.windowsintune.companyportal

DATOS QUE SE ENVÍAN A GOOGLE	DETALLES	USADA PARA	EJEMPLO
Cuenta de servicio de empresa	Se origina en Google tras la solicitud de Intune.	Se usa para la autenticación entre Intune y Google para transacciones relacionadas con este cliente.	Hay varias partes: **Id. de empresa**: documentado anteriormente. **UPN**: UPN generado usado en la autenticación en nombre del cliente. Ejemplo: w49d77900526190e26708c31c9e8a0@pfwp-commicrosoftonedfmdm2.google.com.iam.gserviceaccount.com **Clave**: blob codificado en Base64 usado en solicitudes de autenticación que se almacena cifrado en el servicio, pero este es el aspecto del blob: Identificador único para representar la clave del cliente Ejemplo: a70d4d53eefbd781ce7ad6a6495c65eb15e74f1f

Para dejar de usar la administración de dispositivos empresariales Android con Microsoft Intune y eliminar los datos, debe deshabilitar la administración de dispositivos empresariales Android de Microsoft Intune y también eliminar su cuenta de Google. Consulte en la cuenta de Google cómo realizar la administración de la cuenta.

Datos que Apple manda a Intune

14/05/2021 • 5 minutes to read

Cuando se habilita cualquiera de los siguientes servicios de Apple en un dispositivo, Microsoft Intune establece una conexión con Apple para compartir información del usuario y el dispositivo:

- Programa de inscripción de dispositivos (DEP) de Apple
- Certificado push MDM de Apple (APN)
- Apple School Manager (ASM)
- Programa de Compras por Volumen de Apple (VPP)

Para que Microsoft Intune pueda establecer una conexión, debe crear una cuenta de Apple para cada servicio de Apple.

> **NOTE**
> De acuerdo con la directiva de Microsoft y de Apple, no vendemos a terceros los datos recopilados por nuestro servicio por ningún motivo.

En la tabla siguiente se muestran los datos que un dispositivo Apple envía a Intune. Intune también envía datos a Apple.

SERVICIO	MENSAJE	DATOS QUE SE ENVÍAN A INTUNE	USADA PARA
APNs	Autenticar	MessageType	El tipo de mensaje: autenticar.
APNs	Autenticar	Tema	El tema que el dispositivo escuchará.
APNs	Autenticar	MesUDID	El UDID de los dispositivos.
APNs	Autenticar	OSVersion	La versión del SO del dispositivo.
APNs	Autenticar	BuildVersion	La versión de compilación del dispositivo.
APNs	Autenticar	ProductName	El nombre de producto del dispositivo.
APNs	Autenticar	SerialNumber	El número de serie del dispositivo.
APNs	Autenticar	IMEI	La identidad internacional de equipo móvil del dispositivo.
APNs	Autenticar	MEID	El identificador de equipo móvil del dispositivo.

SERVICIO	MENSAJE	DATOS QUE SE ENVÍAN A INTUNE	USADA PARA
APNs	TokenUpdate	Tema	El tema que el dispositivo escuchará.
APNs	TokenUpdate	UDID	El UDID del dispositivo.
APNs	TokenUpdate	Token	El token de inserción para el dispositivo. El servidor debe utilizar este token actualizado al enviar notificaciones de inserción al dispositivo.
APNs	TokenUpdate	PushMagic	La cadena mágica que debe incluirse en el mensaje de notificación de inserción.
APNs	TokenUpdate	UnlockToken	Un blob de datos que puede usarse para desbloquear el dispositivo.
APNs	TokenUpdate	AwaitingConfiguration	Si se establece en true, el dispositivo está esperando un comando MDM DeviceConfigured antes de iniciar el Asistente para configuración.
APNs	Restauración	MessageType	El tipo de mensaje: restauración.
APNs	Restauración	Tema	El tema que el dispositivo escuchará.
APNs	Restauración	UDID	El UDID del dispositivo.
APNs	Protocolo MDM	Estado	Estado.
APNS	Protocolo MDM	UDID	El UDID del dispositivo.
APNs	Protocolo MDM	CommandUUID	UUID del comando para el que es esta respuesta.
APNs	Protocolo MDM	ErrorChain	Matriz de diccionarios que representa la cadena de errores que se produjeron.
ASM/DEP	Token del programa de inscripción	Número de serie	El número de serie del dispositivo.
ASM/DEP	Token del programa de inscripción	modelo	El nombre de modelo del dispositivo.
ASM/DEP	Token del programa de inscripción	Descripción	Una descripción del dispositivo.

SERVICIO	MENSAJE	DATOS QUE SE ENVÍAN A INTUNE	USADA PARA
ASM/DEP	Token del programa de inscripción	Color	El color del dispositivo.
ASM/DEP	Token del programa de inscripción	Etiqueta de recurso	La etiqueta de recurso del dispositivo.
ASM/DEP	Token del programa de inscripción	Estado de perfil	El estado de instalación del perfil.
ASM/DEP	Token del programa de inscripción	UUID de perfil	El UUID del perfil asignado.
ASM/DEP	Token del programa de inscripción	Hora de asignación del perfil	Una marca de tiempo en formato ISO 8601 que indica cuándo se asignó un perfil al dispositivo.
ASM/DEP	Token del programa de inscripción	Hora de inserción de perfil	Una marca de tiempo en formato ISO 8601 que indica cuándo se insertó un perfil en el dispositivo.
ASM/DEP	Token del programa de inscripción	Fecha de asignación del dispositivo	Una marca de tiempo en formato ISO 8601 que indica cuándo se inscribió el dispositivo en el Programa de inscripción de dispositivos.
ASM/DEP	Token del programa de inscripción	Dispositivo asignado por	Dirección de correo electrónico de la persona que ha asignado el dispositivo.
ASM/DEP	Token del programa de inscripción	Sistema operativo	El sistema operativo del dispositivo.
ASM/DEP	Token del programa de inscripción	Familia de dispositivos	La familia de productos de Apple del dispositivo.
VPP	Token de ubicación de Apple Business Manager	Identificador de usuario de Apple	Un identificador de usuario generado por Apple.
VPP	Token de ubicación de Apple Business Manager	Descripción de la aplicación	Descripción de una aplicación VPP.
VPP	Token de ubicación de Apple Business Manager	Icono de aplicación	La dirección URL de un icono hospedado por Apple para una aplicación VPP.
VPP	Token de ubicación de Apple Business Manager	Identificador de aplicación	El identificador de aplicación de Apple, también conocido como adamsId.

SERVICIO	MENSAJE	DATOS QUE SE ENVÍAN A INTUNE	USADA PARA
VPP	Token de ubicación de Apple Business Manager	Nombre de aplicación	El nombre de una aplicación VPP.
VPP	Token de ubicación de Apple Business Manager	assignedCount	El número de licencias asignadas para una aplicación.
VPP	Token de ubicación de Apple Business Manager	availableCount	El número de licencias no asignadas para una aplicación.
VPP	Token de ubicación de Apple Business Manager	bundleId	BundleId de una aplicación.
VPP	Token de ubicación de Apple Business Manager	copyright	La información de derechos de autor de una aplicación.
VPP	Token de ubicación de Apple Business Manager	CountryCode	El código de país de un programa VPP.
VPP	Token de ubicación de Apple Business Manager	deviceAssignable	Apple devuelve true si el administrador puede asignar una licencia de dispositivo para una aplicación. De lo contrario, se devuelve false.
VPP	Token de ubicación de Apple Business Manager	facilitatorMemberId	El identificador de miembro de un facilitador de cuenta VPP.
VPP	Token de ubicación de Apple Business Manager	Géneros	Los géneros de una aplicación.
VPP	Token de ubicación de Apple Business Manager	Intune UserId guid	El GUID generado por Intune.
VPP	Token de ubicación de Apple Business Manager	isIrrevocable	Apple devuelve true si no se puede revocar la licencia. Si se puede revocar, se devuelve false.
VPP	Token de ubicación de Apple Business Manager	Identificador de licencia	El identificador generado por Apple para identificar una licencia específica.
VPP	Token de ubicación de Apple Business Manager	Ubicación	Ubicación almacenada en los datos de configuración VPP de Apple.
VPP	Token de ubicación de Apple Business Manager	Managed AppleId UPN	El correo electrónico de AppleID para el usuario, el administrador y el miembro facilitador.

SERVICIO	MENSAJE	DATOS QUE SE ENVÍAN A INTUNE	USADA PARA
VPP	Token de ubicación de Apple Business Manager	OrganizationId	El identificador de la organización asignado por Apple.
VPP	Token de ubicación de Apple Business Manager	pricingParam	El tipo de precio de Apple para una aplicación.
VPP	Token de ubicación de Apple Business Manager	productType	El tipo de producto de una aplicación VPP.
VPP	Token de ubicación de Apple Business Manager	retiredCount	El número de licencias retiradas para una aplicación.
VPP	Token de ubicación de Apple Business Manager	totalCount	El número total de licencias adquiridas para una aplicación.
VPP	Token de ubicación de Apple Business Manager	url	La dirección URL de la tienda iTunes de una aplicación.
VPP	Token de ubicación de Apple Business Manager	Estado de usuario	El estado de usuario en programas VPP de Apple.

Para dejar de usar los servicios de Apple con Microsoft Intune y eliminar los datos, debe deshabilitar la administración de token de Apple de Microsoft Intune y también eliminar su cuenta de Apple. Consulte en la cuenta de Apple cómo realizar la administración de la cuenta.

Datos que Google manda a Intune

14/05/2021 • 2 minutes to read

Cuando se habilita la administración de dispositivos empresariales Android en un dispositivo, Microsoft Intune establece una conexión con Google y la información del usuario y del dispositivo se comparte entre Intune y Google. Antes de que Microsoft Intune pueda establecer una conexión, debe crear una cuenta de Google.

En la tabla siguiente se enumeran los datos que Google envía a Intune cuando está habilitada la administración de dispositivos en un dispositivo:

DATOS QUE GOOGLE MANDA A INTUNE	DETALLES	USADA PARA	EJEMPLO
Datos empresariales	Identificadores empresariales del cliente en Google.	Vincular la información del cliente entre Intune y Google.	Ejemplo de **enterpriseId**: LC04eik8a6. **Nombre**. El nombre de administrador, tal y como se especificó al configurar Android Enterprise. Ejemplo: Joe Smith. **Correo electrónico del administrador**. YourAdmin@gmail.com que se usó al configurar Android Enterprise.
Datos de aplicaciones	Datos para las aplicaciones administradas de Play Store.	Dirigir la aplicación a los usuarios o dispositivos como disponible o requerida.	Ejemplo de **nombre de aplicación**: aplicación de inventario de almacén de Contoso. Ejemplo de **identificador único para representar la aplicación**: app:com.Contoso.Warehouse.InventoryTracking
Cuenta de servicio	Cuenta de servicio de Google interna y única para usarse con llamadas de clientes específicos.	Se usa para realizar llamadas en Google en el nombre del cliente (para ver las aplicaciones, los dispositivos, etc.)	Ejemplo de **nombre**: InternalAccount@InternalService.com. Ejemplo de **claves**: ServiceAccountPassword

Para dejar de usar la administración de dispositivos empresariales Android con Microsoft Intune y eliminar los datos, debe deshabilitar la administración de dispositivos empresariales Android de Microsoft Intune y también eliminar su cuenta de Google. Consulte en la cuenta de Google cómo realizar la administración de la cuenta.

Configurar Intune

14/05/2021 • 2 minutes to read

Estos pasos de configuración le ayudarán a habilitar la administración de dispositivos móviles (MDM) mediante Intune. Los dispositivos deben administrarse antes de conceder acceso a los recursos de la empresa a los usuarios o administrar su configuración.

Algunos pasos, como la configuración de una suscripción a Intune y de la entidad de MDM, son necesarios para la mayoría de los escenarios. Otros pasos, tales como configurar un dominio personalizado o agregar aplicaciones, son opcionales según cuáles sean las necesidades de su empresa.

Si actualmente usa Microsoft Endpoint Configuration Manager para administrar equipos y servidores, puede conectar Configuration Manager a la nube con administración conjunta.

> **TIP**
> Si adquiere un mínimo de 150 licencias de Intune en un plan válido, puede usar el *Beneficio del centro de FastTrack*. Con este servicio, los especialistas de Microsoft trabajan con usted para preparar su entorno para Intune. Consulte Beneficio del centro de FastTrack para Enterprise Mobility + Security (EMS).

PASOS	ESTADO
1	Configuraciones compatibles: información necesaria antes de empezar. Esto incluye las configuraciones admitidas y los requisitos de red.
2	Iniciar sesión en Intune: inicie sesión en la suscripción de prueba o cree una suscripción a Intune.
3	Configurar el nombre de dominio: establezca el registro DNS para conectar el nombre de dominio de la empresa con Intune. Esto proporciona a los usuarios un dominio conocido al conectarse a Intune y usar los recursos.
4	Agregar usuarios y grupos: agregue usuarios y grupos, o bien conecte Active Directory para la sincronización con Intune. Se requiere, a menos que los dispositivos sean de pantalla completa "sin usuarios". Los grupos se usan para asignar aplicaciones, configuraciones y otros recursos.
5	Asignar licencias: conceda permiso a los usuarios para que usen Intune. Cada usuario o dispositivo sin usuarios necesita una licencia de Intune para poder acceder al servicio.
6	Establecer la autoridad de MDM: use grupos de usuarios y dispositivos para simplificar las tareas de administración. Los grupos se usan para asignar aplicaciones, configuraciones y otros recursos.
7	Agregar aplicaciones: las aplicaciones se pueden asignar a grupos e instalarse de forma automática u opcional.

PASOS	ESTADO
8	Configurar dispositivos: configure los perfiles que administren la configuración de los dispositivos. Los perfiles de dispositivo pueden establecer con antelación la configuración del correo, la VPN, el Wi-Fi y las características del dispositivo. También pueden restringir dispositivos para ayudar a proteger tanto a los propios dispositivos como a los datos.
9	Personalizar el Portal de empresa: personalice el Portal de empresa de Intune que los usuarios emplean para inscribir dispositivos e instalar aplicaciones. Estos valores se muestran tanto en la aplicación Portal de empresa como en el sitio web del Portal de empresa de Intune.
10	Habilitar la inscripción de dispositivos: habilite la administración de Intune de dispositivos iOS/iPadOS, Windows, Android y Mac mediante el establecimiento de la entidad MDM y la habilitación de plataformas específicas.
11	Configurar directivas de aplicaciones: proporcione valores concretos en función de las directivas de protección de aplicaciones en Microsoft Intune.

Exploradores y sistemas operativos compatibles en Intune

14/05/2021 • 3 minutes to read

Antes de configurar Microsoft Intune, consulte los sistemas operativos y exploradores compatibles.

Para obtener ayuda para la instalación de Intune en su dispositivo, consulte el uso de dispositivos administrados para realizar el trabajo y Uso de ancho de banda de red de Intune.

Para más información sobre la compatibilidad con proveedores de servicios de configuración, consulte Configuration service provider reference (Referencia del proveedor de servicios de configuración).

> **NOTE**
> Intune requiere Android 6.x o superior para que las aplicaciones y los dispositivos accedan a los recursos de la empresa a través de la aplicación Portal de empresa para Android e Intune App SDK para Android. Este requisito no se aplica a los equipos Polycom basados en Android que ejecuten la versión 4.4. Estos dispositivos seguirán siendo compatibles.

Sistemas operativos admitidos por Intune

Puede administrar los dispositivos que ejecuten los siguientes sistemas operativos:

Apple

- Apple iOS 12.0 y versiones posteriores
- Apple iPadOS 13.0 y versiones posteriores
- Mac OS X 10.13 y versiones posteriores

Google

- Android 5.0 y versiones posteriores (incluido Samsung KNOX Standard 2.4 y versiones posteriores: requisitos)
- Android Enterprise: requisitos

Microsoft

- Surface Hub
- Windows 10 (versiones Home, S, Pro, Education y Enterprise)
- Windows 10 Enterprise 2019 LTSC

  Para obtener más información acerca de la administración de dispositivos que ejecutan Windows 10 Enterprise 2019 LTSC, consulte Novedades de Windows 10 Enterprise 2019 LTSC.
- Windows 10 IoT Enterprise (x86, x64)
- Windows Holographic for Business

  Para obtener más información sobre cómo administrar dispositivos que ejecutan Windows Holographic for Business, consulte la asistencia técnica de Windows Holographic for Business.
- Windows 10 Teams (Surface Hub)

  Para obtener más información sobre la administración de dispositivos que ejecutan Windows 10 Teams,

vea Administrar la configuración con un proveedor de MDM (Surface Hub).

- Windows 10 1709 (RS3) y versiones posteriores, Windows 8.1 RT, equipos que ejecutan Windows 8.1 (modo de mantenimiento)

> **NOTE**
> No todas las ediciones de Windows admiten todas las características de sistema operativo disponibles que se configuran mediante MDM. Vea los documentos de referencia de los proveedores de servicios de configuración (CSP) de Windows. Cada CSP destaca las ediciones de Windows que se admiten.

Los clientes que tengan Enterprise Mobility + Security (EMS) también pueden usar Azure Active Directory (Azure AD) para registrar dispositivos Windows 10.

Para instrucciones sobre el uso de máquinas virtuales Windows 10 con Intune, consulte Uso de máquinas virtuales Windows 10.

> **NOTE**
> Intune no admite actualmente la administración de dispositivos habilitados para UWF. Para obtener más información, consulte el artículo Característica Filtro de escritura unificado (UWF).

Dispositivos Samsung Knox Standard admitidos

Para evitar errores de activación de Knox que impidan la inscripción de MDM, la aplicación Portal de empresa solo intenta llevar a cabo la activación de Samsung Knox durante la inscripción de MDM si el dispositivo aparece en la lista de dispositivos Knox admitidos. Los dispositivos que no admiten la activación de Samsung Knox se inscriben como dispositivos Android estándares. Un dispositivo Samsung podría tener algunos números de modelo que admitan Knox, mientras que otros no. Compruebe la compatibilidad de KNOX con el distribuidor de su dispositivo antes de adquirir e implementar dispositivos Samsung.

> **NOTE**
> La inscripción de dispositivos Samsung Knox puede requerir que habilite el acceso a servidores de Samsung.

Los modelos de dispositivos Samsung siguientes no admiten Knox. Se inscriben como dispositivos Android nativos mediante la aplicación Portal de empresa para Android:

NOMBRE DEL DISPOSITIVO	NÚMEROS DE MODELO DE LOS DISPOSITIVOS
Galaxy Avant	SM-G386T
Galaxy Core 2/Core 2 Duos	SM-G355H SM-G355M
Galaxy Core Lite	SM-G3588V
Galaxy Core Prime	SM-G360H
Galaxy Core LTE	SM-G386F SM-G386W

NOMBRE DEL DISPOSITIVO	NÚMEROS DE MODELO DE LOS DISPOSITIVOS
Galaxy Grand	GT-I9082L GT-I9082 GT-I9080L
Galaxy Grand 3	SM-G7200
Galaxy Grand Neo	GT-I9060I
Galaxy Grand Prime Value Edition	SM-G531H
Galaxy J Max	SM-T285YD
Galaxy J1	SM-J100H SM-J100M SM-J100ML
Galaxy J1 Ace	SM-J110F SM-J110H
Galaxy J1 Mini	SM-J105M
Galaxy J2/J2 Pro	SM-J200H SM-J210F
Galaxy J3	SM-J320F SM-J320FN SM-J320H SM-J320M
Galaxy K Zoom	SM-C115
Galaxy Light	SGH-T399N
Galaxy Note 3	SM-N9002 SM-N9009
Galaxy Note 7/Note 7 Duos	SM-N930S SM-N9300 SM-N930F SM-N930T SM-N9300 SM-N930F SM-N930S SM-N930T
Galaxy Note 10.1 3G	SM-P602
Galaxy S2 Plus	GT-I9105P
Galaxy S3 Mini	SM-G730A SM-G730V
Galaxy S3 Neo	GT-I9300 GT-I9300I

NOMBRE DEL DISPOSITIVO	NÚMEROS DE MODELO DE LOS DISPOSITIVOS
Galaxy S4	SM-S975L
Galaxy S4 Neo	SM-G318ML
Galaxy S5	SM-G9006W
Galaxy S6 Edge	404SC
Galaxy Tab A 7.0"	SM-T280 SM-T285
Galaxy Tab 3 7"/Tab 3 Lite 7"	SM-T116 SM-T210 SM-T211
Galaxy Tab 3 8.0"	SM-T311
Galaxy Tab 3 10.1"	GT-P5200 GT-P5210 GT-P5220
Galaxy Trend 2 Lite	SM-G318H
Galaxy V Plus	SM-G318HZ
Galaxy Young 2 Duos	SM-G130BU

Exploradores web compatibles con Intune

Las diferentes tareas administrativas requieren que use uno de los siguientes sitios web de administración.

- Centro de administración de Microsoft 365
- Azure Portal

Estos portales son compatibles con los siguientes exploradores:

- Microsoft Edge (versión más recientes)
- Safari (versión más reciente, solo Mac)
- Chrome (versión más reciente)
- Firefox (versión más reciente)

Ancho de banda y requisitos de configuración de red de Intune

14/05/2021 • 5 minutes to read

Puede usar esta información para comprender los requisitos de ancho de banda de las implementaciones de Intune.

Tráfico de red medio

En la tabla siguiente se muestra el tamaño aproximado y la frecuencia de contenido común que pasa a través de la red de cada cliente.

> **NOTE**
> Para asegurarse de que los dispositivos reciban actualizaciones y contenido de Intune, se deben conectar a Internet de forma periódica. El tiempo que se requiere para recibir actualizaciones o contenido puede variar, pero los dispositivos deben permanecer conectados de forma continua a Internet como mínimo una hora al día.

TIPO DE CONTENIDO	TAMAÑO APROXIMADO	FRECUENCIA Y DETALLES
Instalación del cliente de Intune **Los requisitos siguientes son adicionales a la instalación del cliente de Intune**	125 MB	**Una vez** El tamaño de la descarga de cliente varía dependiendo del sistema operativo del equipo cliente.
Paquete de inscripción de cliente	15 MB	**Una vez** Las descargas adicionales son posibles cuando hay actualizaciones para este tipo de contenido.
Agente de Endpoint Protection	65 MB	**Una vez** Las descargas adicionales son posibles cuando hay actualizaciones para este tipo de contenido.
Agente de Operations Manager	11 MB	**Una vez** Las descargas adicionales son posibles cuando hay actualizaciones para este tipo de contenido.
Agente de directivas	3 MB	**Una vez** Las descargas adicionales son posibles cuando hay actualizaciones para este tipo de contenido.

TIPO DE CONTENIDO	TAMAÑO APROXIMADO	FRECUENCIA Y DETALLES
Asistencia remota a través de agente de Microsoft Easy Assist	6 MB	**Una vez** Las descargas adicionales son posibles cuando hay actualizaciones para este tipo de contenido.
Operaciones diarias de cliente	6 MB	**A diario** El cliente de Intune se comunica regularmente con el servicio de Intune para buscar actualizaciones y directivas, y para notificar el estado del cliente al servicio.
Actualizaciones de definiciones de malware de Endpoint Protection	Variable Normalmente, de 40 KB a 2 MB	**A diario** Hasta tres veces al día.
Actualización del motor de Endpoint Protection	5 MB	**Mensual**
Actualizaciones de software	Variable El tamaño depende de las actualizaciones que implementa.	**Mensual** Normalmente, las actualizaciones de software se publican el segundo martes de cada mes. Un equipo recién inscrito o implementado puede utilizar más ancho de banda de red mientras se descarga el conjunto completo de actualizaciones publicadas anteriormente.
Service Packs	Variable El tamaño varía para cada Service Pack implementado.	**Variable** Depende de cuándo se implementan los Service Packs.
Distribución de software	Variable El tamaño depende del software implementado.	**Varía** Depende de cuándo se implementa el software.

Formas de reducir el uso de ancho de banda de red

Puede usar uno o varios de los métodos siguientes para reducir el uso de ancho de banda de red de clientes de Intune.

Utilizar un servidor proxy para almacenar en caché solicitudes de contenido

Un servidor proxy puede almacenar en caché contenido para reducir las descargas duplicadas y disminuir el ancho de banda de red del contenido de Internet.

Un servidor proxy de almacenamiento en caché que recibe solicitudes de contenido de los clientes puede recuperar dicho contenido y almacenar en caché tanto las respuestas web como las descargas. El servidor usa los datos almacenados en caché para responder solicitudes subsiguientes de los clientes.

A continuación, se indica la configuración típica que se utiliza para un servidor proxy que almacena en caché contenido para clientes de Intune.

SETTING	VALOR RECOMENDADO	DETALLES
Tamaño de caché	De 5 a 30 GB	El valor varía según el número de equipos cliente en la red y las configuraciones que se utilizan. Para evitar que los archivos se eliminen demasiado pronto, ajuste el tamaño de la caché para su entorno.
Tamaño de archivo de caché individual	950 MB	Es posible que esta opción no esté disponible en todos los servidores proxy de almacenamiento en caché.
Tipos de objetos que se almacenarán en caché	HTTP HTTPS BITS	Los paquetes de Intune son archivos CAB recuperados mediante la descarga del Servicio de transferencia inteligente en segundo plano (BITS) a través de HTTP.

> **NOTE**
> Si usa un servidor proxy para almacenar en caché las solicitudes de contenido, la comunicación solo se cifra entre el cliente y el proxy y desde el proxy a Intune. La conexión desde el cliente a Intune no se cifrará de un extremo a otro.

Para obtener información sobre el uso de un servidor proxy para almacenar contenido en caché, consulte la documentación de la solución de servidor proxy.

Optimización de entrega

La optimización de entrega le permite usar Intune para reducir el consumo de ancho de banda cuando los dispositivos Windows 10 descargan aplicaciones y actualizaciones. Mediante el uso de una memoria caché distribuida de organización automática, las descargas pueden extraerse de servidores tradicionales y orígenes alternativos (como elementos del mismo nivel de red).

Para ver la lista completa de las versiones de Windows 10 y los tipos de contenido admitidos por la optimización de entrega, consulte el artículo sobre la optimización de entrega para actualizaciones de Windows 10.

Puede configurar la optimización de entrega como parte de los perfiles de configuración del dispositivo.

Servicio de transferencia inteligente en segundo plano (BITS) y BranchCache

Puede usar Microsoft Intune para administrar equipos con Windows como dispositivos móviles con la administración de dispositivos móviles (MDM) o como equipos con el software cliente de Intune. Microsoft recomienda que los clientes usen la solución de administración de MDM siempre que sea posible. Cuando se administra de esta manera, no se admiten BranchCache ni BITS. Para más información, consulte Comparación de la administración de equipos con Windows como dispositivos móviles o equipos.

Usar (BITS) en los equipos (requiere el cliente de software de Intune)

Durante las horas que configuró, puede usar BITS en un equipo con Windows para disminuir el ancho de banda de red. Puede configurar la directiva para BITS en la página **Ancho de banda de red** de la directiva de agente de Intune.

> **NOTE**
> Para la administración de MDM en Windows, solo la interfaz de administración del SO del tipo de aplicación MobileMSI usa BITS para la descarga. AppX/MsiX usan su propia pila de descarga no BITS y las aplicaciones Win32 a través del agente de Intune usan Optimización de distribución en lugar de BITS.

Para obtener más información sobre BITS y equipos Windows, consulte Servicio de transferencia inteligente en segundo plano en la biblioteca TechNet.

Usar BranchCache en los equipos (requiere el cliente de software de Intune)

Los clientes de Intune pueden utilizar BranchCache para reducir el tráfico de la red de área extensa (WAN). Los siguientes sistemas operativos admiten BranchCache:

- Windows 7
- Windows 8.0
- Windows 8.1
- Windows 10

Para utilizar BranchCache, el equipo cliente debe tener BranchCache habilitado y, a continuación, configurarse para el **modo de caché distribuida**.

Cuando el cliente Intune está instalado en los equipos, BranchCache y el modo de caché distribuida están habilitados de manera predeterminada. Sin embargo, si la directiva de grupo deshabilitó BranchCache, Intune no invalida dicha directiva y BranchCache sigue deshabilitado.

Si usa BranchCache, colabore con otros administradores de la organización para administrar la directiva de grupo y la directiva de firewall de Intune. Asegúrese de que no implementen ninguna directiva que deshabilite las excepciones de BranchCache o de firewall. Para obtener información sobre BranchCache, vea Información general sobre BranchCache.

Pasos siguientes

Revise los puntos de conexión de Intune.

Uso de máquinas virtuales Windows 10 con Intune

14/05/2021 • 2 minutes to read

Intune admite la administración de máquinas virtuales que ejecutan Windows 10 Enterprise con algunas limitaciones. La administración de Intune no depende de la administración de Windows Virtual Desktop de la misma máquina virtual ni interfiere con este proceso.

Inscripción

- No se recomienda administrar máquinas virtuales de host de sesión a petición con Intune. Cada máquina virtual creada debe inscribirse. Además, la eliminación periódica de máquinas virtuales dejará registros de dispositivos huérfanos en Intune hasta que se limpien.
- Los tipos de implementación de aprovisionamiento previo y de implementación automática de Windows Autopilot no se admiten porque requieren un Módulo de plataforma segura (TPM) físico.
- La inscripción en la experiencia rápida (OOBE) no se admite en máquinas virtuales a las que solo se pueda acceder mediante RDP (como es el caso de las máquinas virtuales hospedadas en Azure). Esta restricción significa lo siguiente:
  - Windows Autopilot y la OOBE comercial no se admiten.
  - No se admite la página Estado de la inscripción.

Configuración

Intune no admite ninguna configuración que use un Módulo de plataforma segura o administración de hardware, lo que incluye:

- Configuración de BitLocker
- Configuración de la interfaz de configuración de firmware del dispositivo

Generación de informes

Intune detecta automáticamente las máquinas virtuales y las notifica como "máquina virtual" en **Dispositivos** > **Todos los dispositivos** > elija un dispositivo > campo **Información general** > **Modelo**.

Las máquinas virtuales desasignadas pueden contribuir a los informes de dispositivos no conformes porque no pueden registrarse con el servicio Intune.

Retirada

Si solo tiene acceso RDP, no use la acción de borrado. La acción de borrado eliminará la configuración de RDP de la máquina virtual e impedirá que se vuelva a conectar.

Pasos siguientes

Obtenga información sobre el uso de Windows Virtual Desktop con Intune

Uso de Windows Virtual Desktop con Intune

14/05/2021 • 2 minutes to read

Windows Virtual Desktopes un servicio de virtualización de escritorio y aplicaciones que se ejecuta en Microsoft Azure.Permite que los usuarios finales se conecten de forma segura a un escritorio completo desde cualquier dispositivo. Con Microsoft Intune, puede proteger y administrar sus máquinas virtuales Windows Virtual Desktop con una directiva y aplicaciones a gran escala, una vez inscritas.

Prerequisites

Actualmente, Intune admite máquinas virtuales Windows Virtual Desktop que:

- Ejecutan Windows 10 Enterprise, versión 1809 o posterior.
- Están unidas a Azure AD híbrido.
- Configuradas como escritorios remotos personales en Azure.
- Inscritas en Intune con alguno de los métodos siguientes:
  - Configuración de una directiva de grupo de Active Directory para inscribir automáticamente dispositivos unidos a Azure AD híbrido
  - Administración conjunta de Configuration Manager
  - Inscripción automática de usuarios mediante la unión a Azure AD

Para más información sobre los requisitos de licencias de Windows Virtual Desktop, vea ¿Qué es Windows Virtual Desktop?

Intune trata las máquinas virtuales personales Windows Virtual Desktop igual que los escritorios físicos Windows 10 Enterprise. Este tratamiento le permite usar algunas de las configuraciones existentes y proteger las máquinas virtuales con la directiva de cumplimiento y el acceso condicional. La administración de Intune no depende de la administración de Windows Virtual Desktop de la misma máquina virtual ni interfiere con este proceso.

Limitaciones

Hay algunas limitaciones que se deben tener en cuenta al administrar escritorios remotos Windows 10 Enterprise:

Configuración

Todas las limitaciones de las máquinas virtuales que se enumeran en Uso de máquinas virtuales Windows 10 con Intune también se aplican a las máquinas virtuales Windows Virtual Desktop.

Además, actualmente no se admiten los siguientes perfiles:

- Unión a un dominio
- Wi-Fi

Asegúrese de que la directiva RemoteDesktopServices/AllowUsersToConnectRemotel no está deshabilitada.

Acciones remotas

Las siguientes acciones remotas de dispositivos de escritorio Windows 10 no se admiten ni se recomiendan para las máquinas virtuales Windows Virtual Desktop:

- Restablecimiento de Autopilot

- Rotación de clave de BitLocker
- Empezar de cero
- Bloqueo remoto
- Restablecimiento de contraseña
- Eliminación de datos

Retirada

La eliminación de máquinas virtuales de Azure deja registros de dispositivos huérfanos en Intune. Se limpiarán automáticamente de acuerdo con las reglas de limpieza configuradas para el inquilino.

Sesión múltiple de Windows 10 Enterprise

Actualmente, Intune no admite la administración de varias sesiones de Windows 10 Enterprise.

Pasos siguientes

Más información sobre Windows Virtual Desktop

Puntos de conexión de red de Microsoft Intune

14/05/2021 • 5 minutes to read

En esta página se enumeran las direcciones IP y los valores de puerto necesarios para la configuración del proxy en las implementaciones de Intune.

Como un servicio solo en la nube, Intune no requiere una infraestructura local como servidores o puertas de enlace.

Acceso para dispositivos administrados

Para administrar dispositivos que se encuentren detrás de firewalls y servidores proxy, debe habilitar la comunicación para Intune.

> **NOTE**
> La información de la sección también se aplica a Microsoft Intune Certificate Connector. El conector tiene los mismos requisitos de red que los dispositivos administrados.

- El servidor proxy debe ser compatible con **HTTP (80)** y **HTTPS (443)** , ya que los clientes de Intune usan ambos protocolos. Windows Information Protection utiliza el puerto 444.
- Para algunas tareas (como descargar actualizaciones de software para el agente de PC clásico), Intune necesita acceso de un servidor proxy no autenticado a manage.microsoft.com.

Puede modificar la configuración del servidor proxy en equipos cliente individuales. También puede usar la opción de directiva de grupo para cambiar la configuración de todos los equipos cliente que se encuentran detrás de un servidor proxy especificado.

Los dispositivos administrados requieren configuraciones que dejen acceder a **Todos los usuarios** a los servicios a través de firewalls.

En las siguientes tablas se enumeran los puertos y los servicios a los que accede el cliente de Intune:

DOMINIOS	DIRECCIÓN IP
login.microsoftonline.com *.officeconfig.msocdn.com config.office.com graph.windows.net enterpriseregistration.windows.net	Más información URL de Office 365 e intervalos de direcciones IP
portal.manage.microsoft.com m.manage.microsoft.com	52.175.12.209 20.188.107.228 52.138.193.149 51.144.161.187 52.160.70.20 52.168.54.64 13.72.226.202 52.189.220.232
fef.msuc03.manage.microsoft.com	23.101.0.100

DOMINIOS	DIRECCIÓN IP
wip.mam.manage.microsoft.com	52.187.76.84 13.76.5.121 52.165.160.237 40.86.82.163 52.233.168.142 168.63.101.57 52.187.196.98 52.237.196.51
mam.manage.microsoft.com	104.40.69.125 13.90.192.78 40.85.174.177 40.85.77.31 137.116.229.43 52.163.215.232 52.174.102.180 52.187.196.173 52.156.162.48

DOMINIOS	DIRECCIÓN IP
*.manage.microsoft.com	104.214.164.192/27 104.46.162.96/27 13.67.13.176/28 13.67.15.128/27 13.69.231.128/28 13.69.67.224/28 13.70.78.128/28 13.70.79.128/27 13.71.199.64/28 13.73.244.48/28 13.74.111.192/27 13.75.39.208/28 13.77.53.176/28 13.86.221.176/28 13.89.174.240/28 13.89.175.192/28 20.189.105.0/24 20.189.172.160/27 20.189.229.0/25 20.191.167.0/25 20.37.153.0/24 20.37.192.128/25 20.38.81.0/24 20.41.1.0/24 20.42.1.0/24 20.42.130.0/24 20.42.224.128/25 20.43.129.0/24 20.44.19.224/27 20.49.93.160/27 40.119.8.128/25 40.67.121.224/27 40.70.151.32/28 40.71.14.96/28 40.74.25.0/24 40.78.245.240/28 40.78.247.128/27 40.79.197.64/27 40.79.197.96/28 40.80.180.208/28 40.80.180.224/27 40.80.184.128/25 40.82.248.224/28 40.82.249.128/25 52.150.137.0/25 52.162.111.96/28 52.168.116.128/27 52.182.141.192/27 52.236.189.96/27 52.240.244.160/27

Requisitos de red para aplicaciones Win32 y scripts de PowerShell

Si usa Intune para implementar scripts de PowerShell o aplicaciones Win32, también deberá conceder acceso a los puntos de conexión en los que reside actualmente el inquilino.

Para buscar la ubicación del inquilino (o la unidad de escalado de Azure, también conocida como ASU), inicie sesión en el Centro de administración de Microsoft Endpoint Manager y elija **Administración de inquilinos** > **Detalles del inquilino**. La ubicación aparece en **Ubicación de inquilino** como algo semejante a Norteamérica 0501 o Europa 0202. Busque el número correspondiente en la siguiente tabla. Esa fila le indicará

a qué nombre de almacenamiento y puntos de conexión de CDN debe conceder acceso. Las filas se diferencian por región geográfica, como indican las dos primeras letras de los nombres (na = Norteamérica, eu = Europa, ap = Asia Pacífico). La ubicación del inquilino será una de estas tres regiones, aunque la ubicación geográfica real de la organización podría estar en otro lugar.

UNIDAD DE ESCALADO DE AZURE (ASU)	NOMBRE DE ALMACENAMIENTO	CDN
AMSUA0601 AMSUA0602 AMSUA0101 AMSUA0102 AMSUA0201 AMSUA0202 AMSUA0401 AMSUA0402 AMSUA0501 AMSUA0502 AMSUA0701 AMSUA0702 AMSUA0801	naprodimedatapri naprodimedatasec naprodimedatahotfix	naprodimedatapri.azureedge.net naprodimedatasec.azureedge.net naprodimedatahotfix.azureedge.net
AMSUB0101 AMSUB0102 AMSUB0201 AMSUB0202 AMSUB0301 AMSUB0302 AMSUB0501 AMSUB0502 AMSUB0601	euprodimedatapri euprodimedatasec euprodimedatahotfix	euprodimedatapri.azureedge.net euprodimedatasec.azureedge.net euprodimedatahotfix.azureedge.net
AMSUC0101 AMSUC0201 AMSUC0301 AMSUC0501 AMSUD0101	approdimedatapri approdimedatasec approdimedatahotifx	approdimedatapri.azureedge.net approdimedatasec.azureedge.net approdimedatahotfix.azureedge.net

Servicios de notificaciones de inserción de Windows (WNS)

En los dispositivos de Windows administrados por Intune que se administran mediante administración de dispositivos móviles (MDM), las acciones de dispositivos y otras actividades inmediatas requieren el uso de servicios de notificaciones de inserción de Windows (WNS). Para obtener más información, consulte Permitir el tráfico de notificaciones de Windows a través de firewalls empresariales.

Requisitos de puerto para la optimización de entrega

Requisitos de puerto

En el tráfico de punto a punto, la optimización de entrega usa 7680 para TCP/IP o 3544 para NAT transversal (si lo desea, Teredo). Para la comunicación entre servicio y cliente, utiliza HTTP o HTTPS a través del puerto 80/443.

Requisitos de proxy

Para usar la optimización de entrega, debe permitir las solicitudes de intervalo de bytes. Para más información, vea Requisitos de proxy para Windows Update.

Requisitos de firewall

Permita los nombres de host siguientes a través del firewall para admitir la optimización de entrega. Para la comunicación entre los clientes y el servicio en la nube de la optimización de entrega:

- *.do.dsp.mp.microsoft.com

Para los metadatos de optimización de entrega:

- *.dl.delivery.mp.microsoft.com
- *.emdl.ws.microsoft.com

Información de red de dispositivos de Apple

USADA PARA	NOMBRE DE HOST (DIRECCIÓN IP/SUBRED)	PROTOCOLO	PUERTO
Recuperación y visualización de contenido de los servidores de Apple	itunes.apple.com *.itunes.apple.com *.mzstatic.com *.phobos.apple.com *.phobos.itunes-apple.com.akadns.net	HTTP	80
Comunicaciones con servidores APNS	#-courier.push.apple.com "#" es un número aleatorio entre 0 y 50.	TCP	5223 y 443
Distintas funcionalidades, como acceso a la World Wide Web, iTunes Store, App Store de macOS, iCloud, mensajería, etc.	phobos.apple.com ocsp.apple.com ax.itunes.apple.com ax.itunes.apple.com.edgesuite.net	HTTP/HTTPS	80 o 443

Para obtener más información, vea los artículos de Apple Puertos TCP y UDP usados por los productos de software de Apple, Acerca de los procesos en segundo plano de iTunes y las conexiones del host para el servidor de iTunes, iOS/iPadOS y macOS y Si tus clientes macOS e iOS/iPadOS no reciben notificaciones push de Apple.

Información del puerto de Android

En función de cómo decida administrar los dispositivos Android, es posible que tenga que abrir los puertos de Google Android Enterprise o la notificación de inserción de Android. Para obtener más información sobre los métodos de administración de Android admitidos, vea la documentación de inscripción de Android.

> **NOTE**
> Como Google Mobile Services no está disponible en China, los clientes en China administrados por Intune no pueden usar características que requieran Google Mobile Services. Estas características incluyen: funciones de Google Play Protect como la atestación de dispositivos SafetyNet, la administración de aplicaciones desde Google Play Store, las funciones de Android Enterprise (consulte esta documentación de Google). Además, la aplicación Portal de empresa de Intune para Android usa Google Mobile Services para comunicarse con el servicio Microsoft Intune. Como los servicios de Google Play no están disponible en China, algunas tareas pueden tardar hasta ocho horas en completarse. Para más información, consulte este artículo.

Google Android Enterprise

Google proporciona documentación sobre los puertos de red y los nombres de host de destino obligatorios en la sección **Firewall** de su documento Android Enterprise Bluebook.

Notificación de inserción de Android

Intune aprovecha la Mensajería en la nube de Firebase (FCM) de Google para notificaciones de inserción a fin de

desencadenar acciones e inserciones de dispositivo. Esto es necesario para el Administrador de dispositivos Android y Android Enterprise. Para obtener información sobre los requisitos de red de FCM, vea Los puertos de FCM y el firewall de Google.

Análisis de puntos de conexión

Para obtener más información sobre los puntos de conexión necesarios para al análisis de puntos de conexión, vea Configuración de proxy para el análisis de puntos de conexión.

Puntos de conexión del Gobierno de EE. UU. de Microsoft Intune

14/05/2021 • 2 minutes to read

En esta página se enumeran los puntos de conexión US Government, US Government Community (GCC) High y Department of Defense (DoD) necesarios para la configuración del proxy de las implementaciones de Intune.

Para administrar dispositivos que se encuentren detrás de firewalls y servidores proxy, debe habilitar la comunicación para Intune.

- El servidor proxy debe ser compatible con **HTTP (80)** y **HTTPS (443)** , ya que los clientes de Intune usan ambos protocolos.
- Para algunas tareas (como descargar actualizaciones de software), Intune necesita acceso de un servidor proxy no autenticado a manage.microsoft.com.

Puede modificar la configuración del servidor proxy en equipos cliente individuales. También puede usar la opción de directiva de grupo para cambiar la configuración de todos los equipos cliente que se encuentran detrás de un servidor proxy especificado.

Los dispositivos administrados requieren configuraciones que dejen acceder a **Todos los usuarios** a los servicios a través de firewalls.

Para más información sobre la inscripción automática de Windows 10 y el registro de dispositivos para clientes de la administración pública de Estados Unidos, consulte Configuración de la inscripción para dispositivos Windows.

En las siguientes tablas se enumeran los puertos y los servicios a los que accede el cliente de Intune:

PUNTO DE CONEXIÓN	DIRECCIÓN IP
*.manage.microsoft.us	52.243.26.209 52.247.173.11 52.227.183.12 52.227.180.205 52.227.178.107 13.72.185.168 52.227.173.179 52.227.175.242 13.72.39.209 52.243.26.209 52.247.173.11
enterpriseregistration.microsoftonline.us	13.72.188.239 13.72.55.179

Puntos de conexión del Gobierno de EE. UU. designados por el cliente:

- Azure Portal: https://portal.azure.us/
- Microsoft 365: https://portal.office365.us/
- Portal de empresa de Intune: https://portal.manage.microsoft.us/
- Centro de administración de Microsoft Endpoint Manager://endpoint.microsoft.us/

Puntos de conexión de servicio asociados de los que depende Intune:

- Servicio Sincronización de Azure AD: https://syncservice.gov.us.microsoftonline.com/DirectoryService.svc
- Evo STS: https://login.microsoftonline.us
- Proxy de directorio: https://directoryproxy.microsoftazure.us/DirectoryProxy.svc
- Azure AD Graph: https://directory.microsoftazure.us y https://graph.microsoftazure.us
- MS Graph: https://graph.microsoft.us
- ADRS: https://enterpriseregistration.microsoftonline.us

Servicios de notificaciones de inserción de Windows

En los dispositivos Windows administrados por Intune que se administran mediante administración de dispositivos móviles (MDM), las acciones de dispositivos y otras actividades inmediatas requieren Servicios de notificaciones de inserción de Windows (WNS). Para más información, vea Configuraciones de firewall y proxy de empresa para admitir el tráfico de WNS.

Información de red de dispositivos de Apple

SE USA PARA	NOMBRE DE HOST (DIRECCIÓN IP/SUBRED)	PROTOCOLO	PUERTO
Recuperación y visualización de contenido de los servidores de Apple	itunes.apple.com *.itunes.apple.com *.mzstatic.com *.phobos.apple.com *.phobos.itunes-apple.com.akadns.net	HTTP	80
Comunicación con servidores APNS	#-courier.push.apple.com "#" es un número aleatorio entre 0 y 50.	TCP	5223 y 443
Distintas funciones, como acceso a Internet, iTunes Store, App Store de macOS, iCloud, mensajería, etc.	phobos.apple.com ocsp.apple.com ax.itunes.apple.com ax.itunes.apple.com.edgesuite.net	HTTP/HTTPS	80 o 443

Para obtener más información, vea:

- Puertos TCP y UDP usados por los productos de software de Apple
- Acerca de los procesos en segundo plano de iTunes y las conexiones del host para el servidor de iTunes, iOS/iPadOS y macOS
- Si tus clientes macOS e iOS/iPadOS no reciben notificaciones push de Apple

Pasos siguientes

Puntos de conexión de red de Microsoft Intune

Puntos de conexión de China para Microsoft Intune

14/05/2021 • 2 minutes to read

En esta página se enumeran los puntos de conexión de China necesarios para la configuración del proxy en las implementaciones de Intune.

Para administrar dispositivos que se encuentren detrás de firewalls y servidores proxy, debe habilitar la comunicación para Intune.

- El servidor proxy debe ser compatible con **HTTP (80)** y **HTTPS (443)** , ya que los clientes de Intune usan ambos protocolos.
- Para algunas tareas (como descargar actualizaciones de software), Intune necesita acceso de un servidor proxy no autenticado a manage.microsoft.com.

Puede modificar la configuración del servidor proxy en equipos cliente individuales. También puede usar la opción de directiva de grupo para cambiar la configuración de todos los equipos cliente que se encuentran detrás de un servidor proxy especificado.

Los dispositivos administrados requieren configuraciones que dejen acceder a **Todos los usuarios** a los servicios a través de firewalls.

Para más información sobre la inscripción automática de Windows 10 y el registro de dispositivos para clientes de la administración pública de China, consulte Configuración de la inscripción para dispositivos Windows.

En las siguientes tablas se enumeran los puertos y los servicios a los que accede el cliente de Intune:

PUNTO DE CONEXIÓN	DIRECCIÓN IP
*.manage.microsoftonline.cn	40.73.38.143 139.217.97.81 52.130.80.24 40.73.41.162 40.73.58.153 139.217.95.85

Puntos de conexión designados por el cliente de Intune en China

- Azure Portal: https://portal.azure.cn/
- Microsoft 365: https://portal.partner.microsoftonline.cn/
- Portal de empresa de Intune: https://portal.manage.microsoftonline.cn/
- Centro de administración de Microsoft Endpoint Manager: https://endpoint.microsoftonline.cn/

Puntos de conexión de partners

Intune ofrecido por 21Vianet depende de los siguientes puntos de conexión de servicio de partners:

- Servicio Sincronización de Azure AD: https://syncservice.partner.microsoftonline.cn/DirectoryService.svc
- Evo STS: https://login.chinacloudapi.cn/
- Azure AD Graph: https://graph.chinacloudapi.us
- MS Graph: https://microsoftgraph.chinacloudapi.cn
- ADRS: https://enterpriseregistration.partner.microsoftonline.cn

Servicios de notificaciones de inserción de Windows

En los dispositivos Windows administrados por Intune que se administran mediante administración de dispositivos móviles (MDM), las acciones de dispositivos y otras actividades inmediatas requieren Servicios de notificaciones de inserción de Windows (WNS). Para más información, vea Configuraciones de firewall y proxy de empresa para admitir el tráfico de WNS.

Información de red de dispositivos de Apple

SE USA PARA	NOMBRE DE HOST (DIRECCIÓN IP/SUBRED)	PROTOCOLO	PUERTO
Recuperación y visualización de contenido de los servidores de Apple	itunes.apple.com *.itunes.apple.com *.mzstatic.com *.phobos.apple.com *.phobos.itunes-apple.com.akadns.net	HTTP	80
Comunicación con servidores APNS	#-courier.push.apple.com "#" es un número aleatorio entre 0 y 50.	TCP	5223 y 443
Distintas funciones, como acceso a Internet, iTunes Store, App Store de macOS, iCloud, mensajería, etc.	phobos.apple.com ocsp.apple.com ax.itunes.apple.com ax.itunes.apple.com.edgesuite.net	HTTP/HTTPS	80 o 443

Para obtener más información, vea:

- Puertos TCP y UDP usados por los productos de software de Apple
- Acerca de los procesos en segundo plano de iTunes y las conexiones del host para el servidor de iTunes, iOS/iPadOS y macOS
- Si tus clientes macOS e iOS/iPadOS no reciben notificaciones push de Apple

Pasos siguientes

Más información sobre Intune ofrecido por 21Vianet en China

Intune ofrecido por 21Vianet en China

14/05/2021 • 3 minutes to read

Intune ofrecido por 21Vianet está diseñado para satisfacer las necesidades de servicios en la nube seguros, confiables y escalables en China. Intune como servicio se basa en Microsoft Azure. Microsoft Azure ofrecido por 21Vianet es una instancia físicamente separada los servicios en la nube ubicados en China. Se ofrece y se realiza de forma independiente con 21Vianet. Este servicio se basa en la tecnología que Microsoft ha autorizado a 21Vianet.

Microsoft no ofrece con el propio servicio. 21Vianet ofrece, proporciona y administra la entrega del servicio. 21Vianet es un proveedor de servicios de centro de datos de Internet en China. Proporciona servicios de hospedaje, servicios de red administrados e infraestructura de informática en la nube. Gracias a las tecnologías de licencias de Microsoft, 21Vianet funciona en los centros de datos locales para ofrecer la posibilidad de usar el servicio de Intune al tiempo que mantiene los datos en China. 21Vianet también proporciona servicios de suscripción, facturación y soporte técnico.

> **NOTE**
> Si está interesado en ver o eliminar datos personales, vea el artículo Solicitudes de interesados de Azure para el RGPD. Si busca información general sobre RPGD, consulte la sección del RGPD del Portal de confianza de servicios.

Diferencias de características en Intune ofrecido por 21Vianet

Dado que los servicios de China operan en un partner de dentro de China, hay algunas diferencias de características con Intune.

- Intune ofrecido por 21Vianet solo admite implementaciones independientes. Los clientes pueden usar la administración conjunta para asociar la implementación existente de Configuration Manager a la nube de Microsoft Intune.
- No se admiten migraciones de nubes públicas a nubes independientes. Los clientes interesados en pasar a Intune ofrecido por 21Vianet deben migrar manualmente.
- Actualmente no se admite la característica de asociación de inquilinos (la sincronización de dispositivos a Intune sin inscripción para admitir escenarios de la consola en la nube).
- Las credenciales derivadas no se admiten cuando Intune lo ofrece 21Vianet.
- Se admite la administración de Windows 10 mediante el canal de MDM moderno.
- Intune ofrecido por 21Vianet no admite el conector de Exchange local.
- Las características de Windows Autopilot y de la Tienda para empresas no están disponibles actualmente.
- Dado que Google Mobile Services no está disponible en China, los clientes de Intune ofrecidos por 21Vianet no pueden usar características que requieran los servicios de Google para móviles. Estas características incluyen:
  - Funcionalidades de Google Play Protect como certificación de dispositivo SafetyNet
  - Administración de aplicaciones desde Google Play Store
  - Funcionalidades de Android Enterprise Para más información, consulte la documentación de Google.
- La aplicación Portal de empresa de Intune para Android utiliza los servicios de Google para móviles para comunicarse con el servicio Microsoft Intune. Como los servicios de Google Play no están disponible en China, algunas tareas pueden tardar hasta ocho horas en completarse. Para más información, consulte este artículo.
- Para seguir las regulaciones locales y proporcionar una funcionalidad mejorada, la experiencia del cliente de

Intune (aplicación Portal de empresa) puede diferir en China.
- Las barreras no están disponibles.
- La disponibilidad de administración de aplicaciones móviles (MAM) depende de las aplicaciones que están disponibles en la República Popular China.

Control de los datos de los clientes

En Microsoft Azure, Intune, Microsoft 365 y Power BI ofrecido por 21Vianet, usted tiene el control total de los datos:

- Sabe dónde se encuentran los datos del cliente.
- Puede controlar el acceso a los datos del cliente.
- Puede controlar los datos de los clientes si deja el servicio.
- Tiene opciones para controlar la seguridad de los datos de los clientes.

Con Microsoft Azure, Intune, Microsoft 365 y Power BI ofrecido por 21Vianet, usted es el propietario de los datos:

- 21Vianet no utiliza los datos de clientes para publicidad.
- Usted controla quién tiene acceso a los datos del cliente.
- Usamos el aislamiento lógico para separar los datos de cada cliente.
- Proporcionamos directivas de uso de datos sencillas y transparentes y obtenemos auditorías independientes.
- Nuestros subcontratistas están bajo contrato para cumplir con nuestros requisitos de privacidad.

Solicitudes de los titulares de los datos

El rol Administrador de inquilinos para Intune ofrecido por 21Vianet puede solicitar datos para los titulares de las siguientes maneras:

- Mediante el centro de administración de Azure Active Directory, un administrador de inquilinos puede eliminar de forma permanente un titular de los datos de Azure Active Directory y servicios relacionados. Para más información, consulte la sección Paso 5: Eliminar de Solicitudes de titulares de los datos de Azure para el RGPD y la CCPA
- Los administradores de inquilinos pueden exportar los registros generados por el sistema para los servicios de Microsoft ofrecidos por 21Vianet mediante la exportación del registro de datos. Para más información, consulte la sección Paso 6: Exportar de Solicitudes de titulares de los datos de Azure para el RGPD y la CCPA.

Pasos siguientes

Más información sobre los dispositivos compatibles con Intune.

Suscribirse o iniciar sesión en Microsoft Intune

14/05/2021 • 2 minutes to read

En este tema se explica a los administradores del sistema cómo pueden registrarse para obtener una cuenta de Intune.

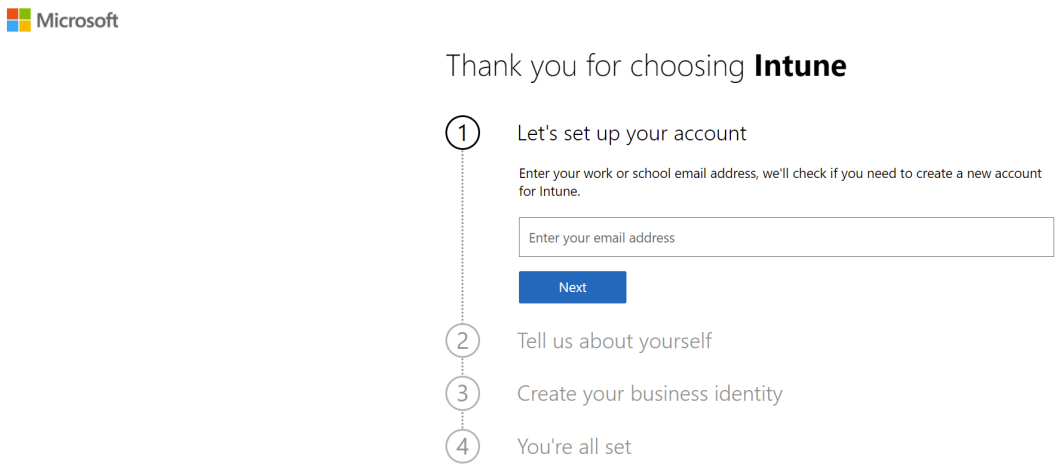
Antes de registrarse en Intune, determine si ya tiene una cuenta de Microsoft Online Services, Contrato Enterprise o un contrato de licencias por volumen equivalente. Un contrato de licencias por volumen de Microsoft u otras suscripciones a servicios en la nube de Microsoft, como Microsoft 365, suelen incluir una cuenta profesional o educativa.

Si ya dispone de una cuenta profesional o educativa, **inicie sesión** con dicha cuenta y agregue Intune a su suscripción. En caso contrario, puede **registrarse** para obtener una nueva cuenta y usar Intune para su organización.

> **WARNING**
> No puede combinar una cuenta profesional o educativa existente después de registrarse con una cuenta nueva.

Cómo registrarse en Intune

1. Visite la página de registro de Intune.



2. En la página de registro, inicie sesión o regístrese para administrar una nueva suscripción de Intune.

Consideraciones posteriores al registro

Cuando se haya registrado para obtener una nueva suscripción, recibirá un mensaje de correo electrónico con la información de la cuenta en la dirección de correo electrónico que haya proporcionado durante el proceso de registro. Este mensaje confirma que la suscripción está activa.

Una vez concluido el proceso de registro, se le dirigirá al Centro de administración de Microsoft 365, desde el que se pueden agregar usuarios y asignarles licencias. Si solo dispone de cuentas basadas en la nube con el nombre de dominio onmicrosoft.com predeterminado, puede continuar para agregar usuarios y asignar licencias. Pero si tiene pensado usar el nombre de dominio personalizado de su organización o sincronizar la información de la cuenta de usuario de Active Directory local, puede cerrar la ventana del explorador.

Inicio de sesión en Microsoft Intune

Una vez que se haya registrado en Intune, puede usar cualquier dispositivo con un explorador admitido para iniciar sesión en Intune a fin de administrar el servicio.

De manera predeterminada, la cuenta debe tener uno de los siguientes permisos en Azure AD:

- Administrador global
- Administrador del servicio Intune (también conocido como Administrador de Intune)

Para conceder acceso para administrar el servicio para los usuarios con otros permisos, vea Control de acceso basado en rol.

Dirección URL del portal de administración de Intune

Centro de administración de Microsoft Endpoint Manager: https://endpoint.microsoft.com

Intune para educación: https://intuneeducation.portal.azure.com

Direcciones URL para los servicios de Intune proporcionados por Microsoft 365

Microsoft 365 Empresa: https://portal.microsoft.com/adminportal

Administración de dispositivos móviles de Microsoft 365:
https://admin.microsoft.com/adminportal/home#/MifoDevices

Vea también

No puede iniciar sesión en Microsoft 365, Azure o Intune

Administradores sin licencia

14/05/2021 • 2 minutes to read

Puede conceder a los administradores acceso a Microsoft Endpoint Manager sin necesidad de una licencia de Intune. Esta característica se aplica a cualquier administrador, incluidos los administradores de Intune, los administradores globales, los administradores de Azure AD, etc. Es posible que para otras características o servicios, como Azure Active Directory (AD) Premium, se necesite una licencia para el administrador.

Permitir acceso

1. Inicie sesión en el Centro de administración de Microsoft Endpoint Manager > **Administración de inquilinos** > **Roles** > **Licencias de administrador**.
2. Seleccione **Permitir el acceso a administradores sin licencia** > **Sí**.

   > **WARNING**
   > No se puede deshacer esta configuración después de hacer clic en **Sí**.

3. A partir de ahora, los usuarios que inicien sesión en el centro de administración de Microsoft Endpoint Manager no necesitarán una licencia de Intune. Su ámbito de acceso se definirá mediante los roles que tengan asignados.

Intune admite hasta 350 administradores sin licencia por grupo de seguridad y solo se aplica a los miembros directos. Los administradores que superen este límite experimentarán un comportamiento imprevisible.

Los cambios en el acceso pueden tardar hasta 48 horas en aplicarse.

Pasos siguientes

Control de acceso basado en rol (RBAC) con Microsoft Intune

Licencias de Microsoft Intune

Configuración de un nombre de dominio personalizado

14/05/2021 • 2 minutes to read

En este tema se indica a los administradores cómo se puede crear un CNAME de DNS para simplificar y personalizar la experiencia de inicio de sesión con Microsoft Intune.

Cuando su organización se registra en un servicio en la nube de Microsoft como es Intune, se le asigna un nombre de dominio inicial hospedado en Azure Active Directory (AD) similar a **su-dominio.onmicrosoft.com**. En este ejemplo, **su-dominio** es el nombre del dominio que eligió al suscribirse. **onmicrosoft.com** es el sufijo asignado a las cuentas que agregue a su suscripción. Puede configurar el dominio personalizado de su organización para obtener acceso a Intune en lugar del nombre de dominio proporcionado con la suscripción.

Le recomendamos encarecidamente que, antes de crear nuevas cuentas de usuario o de sincronizar su instancia de Active Directory local, decida si va a usar únicamente el dominio .onmicrosoft.com o si va a agregar uno o más nombres de dominio personalizados. Configure un dominio personalizado antes de agregar usuarios para simplificar la administración de usuarios. La configuración de un dominio de cliente permite a los usuarios iniciar sesión con las credenciales que usan para obtener acceso a otros recursos del dominio.

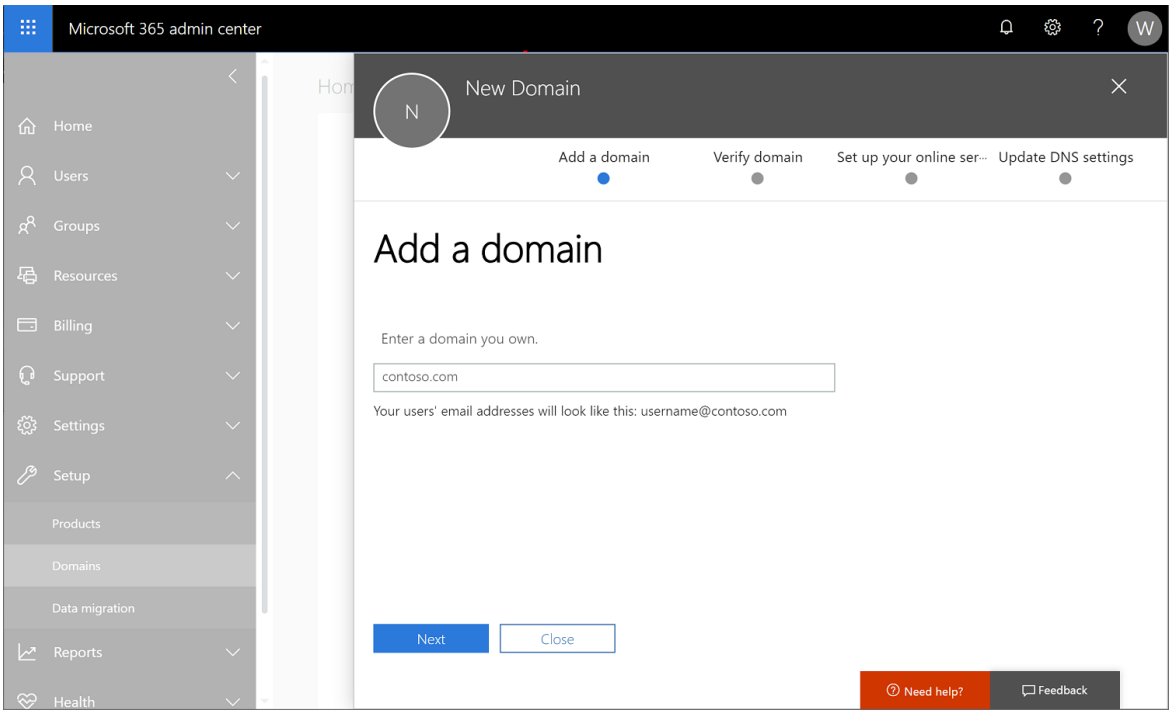
Al suscribirse a un servicio basado en la nube de Microsoft, la instancia de ese servicio se convierte en un inquilino de Microsoft Azure AD, que proporciona servicios de identidad y directorio al servicio basado en la nube. Además, como las tareas de configuración de Intune para que use el nombre de dominio personalizado de las organizaciones son las mismas que para otros inquilinos de Azure AD, puede usar la información y los procedimientos que se describen en Agregar el dominio.

> **TIP**
> Para obtener más información sobre los dominios personalizados, consulte Información general conceptual de nombres de dominio personalizado en Azure Active Directory.

No puede cambiar el nombre del dominio inicial onmicrosoft.com ni quitarlo. Puede agregar, comprobar o quitar los nombres de dominio personalizado usados en Intune para identificar claramente su negocio.

Para agregar y comprobar el dominio personalizado

1. Vaya al Centro de administración de Microsoft 365 e inicie sesión con su cuenta de administrador.
2. En el panel de navegación, elija **Configuración** > **Dominios**.
3. Elija **Agregar dominio** y escriba el nombre de su dominio personalizado. Seleccione **Siguiente**.



4. El cuadro de diálogo **Comprobar dominio** se abre proporcionándole los valores para crear el registro TXT en su proveedor de host DNS.

   - **Usuarios de GoDaddy**: el Centro de administración de Microsoft 365 lo lleva a la página de inicio de sesión de GoDaddy. El registro TXT se crea automáticamente después de escribir sus credenciales y de aceptar el acuerdo del permiso de cambio de dominio. También puede crear el registro TXT.
   - **Usuarios de Register.com**: siga las instrucciones paso a paso para crear el registro TXT.

5. Es posible que necesite crear registros DNS adicionales para las inscripciones de Intune.

Los pasos para agregar y comprobar un dominio personalizado también se pueden realizar en Azure Active Directory.

Puede obtener más información sobre su dominio inicial onmicrosoft.com en Microsoft 365.

Puede obtener más información sobre cómo simplificar la inscripción de Windows sin Azure AD Premium mediante la creación de un CNAME de DNS que redirija la inscripción a los servidores de Intune.

Adición de usuarios y concesión de permiso administrativo a Intune

14/05/2021 • 7 minutes to read

Como administrador, puede agregar usuarios directamente o sincronizarlos desde la instancia local de Active Directory. Una vez agregados, los usuarios pueden inscribir dispositivos y obtener acceso a los recursos de la empresa. También puede conceder a los usuarios permisos adicionales, incluidos permisos de *administrador global* y de *administrador de servicios*.

Agregar usuarios a Intune

Puede agregar usuarios manualmente a la suscripción de Intune mediante el Centro de administración de Microsoft 365 o el Centro de administración de Microsoft Endpoint Manager. Un administrador puede editar cuentas de usuario para asignar licencias de Intune. Puede asignar licencias en el centro de administración de Microsoft 365 o en el centro de administración de Microsoft Endpoint Manager. Para más información sobre cómo usar el Centro de administración de Microsoft 365, consulte el artículo sobre cómo agregar usuarios individuales o de manera masiva al Centro de administración de Microsoft 365.

Incorporación de usuarios de Intune en el Centro de administración de Microsoft 365

1. Inicie sesión en el Centro de administración de Microsoft 365 con una cuenta de administrador de administración de usuarios o administrador global.
2. En el menú de Microsoft 365, seleccione **Usuarios** > **Usuarios activos** > **Agregar un usuario**.
3. Especifique los siguientes detalles de usuario:
   - **Nombre**
   - **Apellido**
   - **Nombre para mostrar**
   - **Nombre de usuario**: nombre principal de usuario (UPN) almacenado en Azure Active Directory que se ha usado para tener acceso al servicio.
   - **Contraseña**: generar automáticamente o crear.
4. Elija **Siguiente**.
5. En la página **Asignar licencias de producto**, seleccione una **ubicación** y, a continuación, elija una licencia para este usuario. Se necesita una licencia que incluya Intune.
6. Elija **Siguiente**.
7. En la página **Configuración opcional**, tiene la opción de:
   - Asignar los nuevos roles de usuario (de forma predeterminada, al nuevo usuario se le asigna el rol de usuario).
   - Proporcionar información de perfil.
8. Elija **Siguiente**.
9. En la página **Revisar y finalizar**, seleccione **Terminar de agregar** para agregar el usuario. Elija **Cerrar** para cerrar la página **Agregar un usuario**.

Adición de usuarios de Intune en Azure Portal

1. En el Centro de administración de Microsoft Endpoint Manager, elija **Usuarios** > **Todos los usuarios** > **Nuevo usuario** > **Crear usuario**.
2. Especifique los siguientes detalles de usuario:
   - **Nombre de usuario**: el nuevo nombre que usará el usuario para iniciar sesión en Azure Active

Directory.

- **Nombre**: el nombre de pila del usuario.

3. Elija si desea crear la contraseña para el nuevo usuario o hacer que se genere automáticamente.
4. Para asignar el nuevo usuario a grupos (opcional), seleccione **0 groups selected** (0 grupos seleccionados) para abrir el panel **Grupos**. Aquí puede seleccionar los grupos que desea asignar al usuario. Cuando termine de seleccionar grupos, elija **Seleccionar**.
5. De forma predeterminada, al nuevo usuario se le asigna el rol **Usuario**. Si desea agregar roles al usuario, seleccione **Usuario** en **Grupos y roles**. En el panel **Roles del directorio**, seleccione los roles que desea asignar al usuario y, después, elija **Seleccionar**.
6. Si desea impedir que el usuario inicie sesión, puede seleccionar **Sí** en **Bloqueo de inicio de sesión**. Asegúrese de volver a cambiar esta opción a **No** cuando esté listo para permitir que el usuario inicie sesión.
7. Elija una **Ubicación de uso** para el nuevo usuario. Es necesario especificar la ubicación de uso para poder asignar una licencia de Intune al nuevo usuario.
8. Opcionalmente, puede proporcionar información para los campos **Puesto**, **Departamento**, **Nombre de compañía** y **Administrador**.
9. Seleccione **Crear** para agregar el nuevo usuario a Intune.

Conceder permisos de administrador

Tras agregar usuarios adicionales a la suscripción de Intune, le recomendamos que conceda permiso administrativo a algunos usuarios. Para conceder permisos administrativos, siga estos pasos:

Concesión de permisos administrativos en Microsoft 365

1. Inicie sesión en el Centro de administración de Microsoft 365 con una cuenta de administrador global > seleccione **Usuarios** > **Usuarios activos** > elija el usuario para conceder permisos de administrador.
2. En el panel de usuario, elija **Administrar roles** en **Roles**.
3. En el panel **Administrar roles**, seleccione el permiso de administración que se va a conceder de la lista de roles disponibles.
4. Elija **Guardar cambios**.

Concesión de permisos de administración en Azure Portal

1. Inicie sesión en el Centro de administración de Microsoft Endpoint Manager con una cuenta de administrador global > **Usuarios** > y, a continuación, elija el usuario al que desea conceder permisos de administrador.
2. Seleccione **Roles asignados** > **Agregar asignaciones**.
3. En el panel **Roles del directorio**, seleccione los roles que desea asignar al usuario > **Agregar**

Tipos de administradores

Asigne a los usuarios uno o varios permisos de administrador. Estos permisos definen el ámbito administrativo de los usuarios y las tareas que pueden administrar. Los permisos de administrador son comunes entre los diferentes servicios en la nube de Microsoft, y es posible que algunos servicios no sean compatibles con determinados permisos. Azure Portal y el Centro de administración de Microsoft 365 muestran roles de administrador limitados que no usa Intune. Los permisos de administrador de Intune incluyen las opciones siguientes:

- **Administrador global**: (Microsoft 365 e Intune) tiene acceso a todas las características administrativas de Intune. De manera predeterminada, la persona que se suscriba a Intune se convertirá en un administrador global. Los administradores globales son los únicos administradores que pueden asignar otros roles de administrador. Puede tener más de un administrador global en la organización. Como procedimiento recomendado, se recomienda que solo unas pocas personas de la empresa tengan este rol, a fin de disminuir el riesgo para la empresa.
- **Administrador de contraseñas**: (Microsoft 365 e Intune) restablece contraseñas, administra solicitudes

del servicio y supervisa el mantenimiento de dicho servicio. Los administradores de contraseñas están limitados a restablecer las contraseñas de los usuarios.

- **Administrador de soporte técnico del servicio**: (Microsoft 365 e Intune) abre solicitudes de soporte técnico con Microsoft y puede ver el panel de servicio y el centro de mensajes. Tienen permisos de "solo para visualización", excepto para abrir incidencias de soporte técnico y leerlas.
- **Administrador de facturación**: (Microsoft 365 e Intune) hace compras, administra suscripciones e incidencias de soporte técnico y supervisa el mantenimiento del servicio.
- **Administrador de usuarios**: (Microsoft 365 e Intune) restablece contraseñas, supervisa el mantenimiento del servicio, agrega y elimina cuentas de usuario y, además, administra solicitudes de servicio. El administrador de control de usuarios no puede eliminar a un administrador global, crear otros roles de administrador ni restablecer las contraseñas de otros administradores.
- **Administrador de Intune**: todos los permisos de Administrador global de Intune excepto el permiso para crear administradores con las opciones **Rol de directorio**.

La cuenta que se usa para crear la suscripción a Microsoft Intune es un administrador global. Como procedimiento recomendado, no use un administrador global para las tareas de administración cotidianas. Aunque los administradores no necesitan tener una licencia de Intune para acceder al portal de Intune en Azure, sí que necesitan tener una licencia de Intune para realizar ciertas tareas de administración, como configurar el Conector de servicio de Exchange.

Para acceso al Centro de administración de Microsoft 365, la cuenta debe tener establecido un **inicio de sesión permitido**. En Azure Portal, en **Perfil**, establezca **Bloquear inicio de sesión** en **No** para permitir el acceso. Este estado es distinto a tener una licencia para la suscripción. De manera predeterminada, todas las cuentas de usuario tienen el estado **Permitido**. Los usuarios que no tienen permisos de administrador pueden usar el Centro de administración de Microsoft 365 para restablecer las contraseñas de Intune.

Sincronizar Active Directory y agregar usuarios a Intune

Puede configurar la sincronización de directorios para importar las cuentas de usuario desde la instancia local de Active Directory a Microsoft Azure Active Directory (Azure AD), que incluye los usuarios de Intune. Tener el servicio local de Active Directory conectado con todos los servicios basados en Azure Active Directory facilita la administración de identidades de usuario en gran medida. También puede configurar características de inicio de sesión único para que la experiencia de autenticación resulte fácil y familiar a los usuarios. Al vincular el mismo inquilino de Azure AD con varios servicios, las cuentas de usuario que sincronizó previamente están disponibles para todos los servicios basados en la nube.

Sincronización de usuarios locales con Azure AD

La única herramienta que necesita para sincronizar las cuentas de usuario con Azure AD es el Asistente de Azure AD Connect. El Asistente de Azure AD Connect proporciona una experiencia guiada y simplificada que conectará su infraestructura de identidad local con la nube. Elija la topología y las necesidades (uno o varios directorios, sincronización de hash de contraseñas, autenticación de paso a través o federación). El asistente implementa y configura todos los componentes necesarios para preparar la conexión. Esto incluye los servicios de sincronización, los servicios de federación de Active Directory (AD FS) y el módulo de PowerShell de Azure AD.

> **TIP**
> Azure AD Connect abarca funciones que se publicaron anteriormente, como la Sincronización de directorios y la Sincronización de Azure AD. Obtenga más información sobre la integración de directorios. Para obtener información sobre la sincronización de cuentas de usuario desde un directorio local con Azure AD, consulte Similitudes entre Active Directory y Azure AD.

Agregar grupos para organizar usuarios y dispositivos

14/05/2021 • 4 minutes to read

Intune usa grupos de Azure Active Directory (AD) para administrar dispositivos y usuarios. Como administrador de Intune, puede configurar los grupos de modo que satisfagan sus necesidades organizativas. Cree grupos para organizar a los usuarios o dispositivos por ubicación geográfica, departamento o características de hardware. Use los grupos para administrar tareas a escala. Por ejemplo, puede establecer directivas para muchos usuarios o implementar aplicaciones para un conjunto de dispositivos.

Puede agregar los siguientes tipos de grupos:

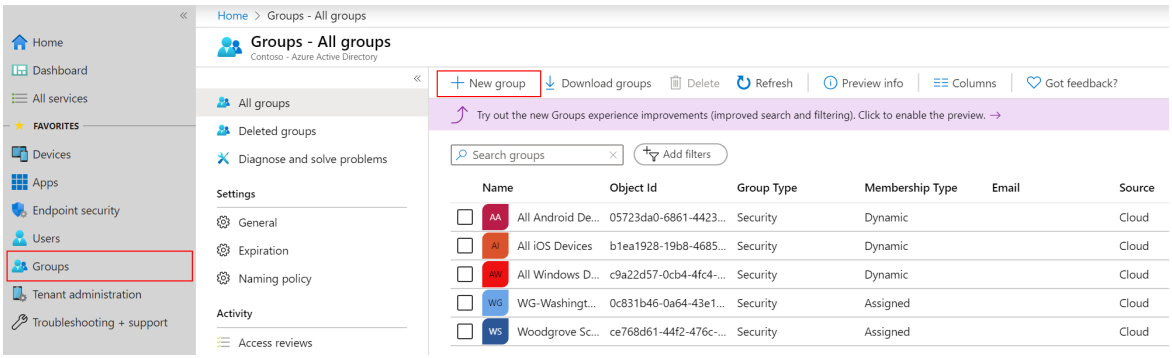
- **Grupos asignados**: agregue manualmente usuarios o dispositivos a un grupo estático.
- **Grupos dinámicos** (requiere Azure AD Premium): agregue automáticamente usuarios o dispositivos a grupos de usuarios o grupos de dispositivos en función de una expresión que cree.

  Por ejemplo, cuando se agrega un usuario con el título de administrador, el usuario se agrega automáticamente a un grupo de usuarios **Todos los administradores**. O bien, cuando un dispositivo tiene el tipo de sistema operativo para dispositivos iOS/iPadOS, se agrega de forma automática a un grupo de dispositivos **Todos los dispositivos iOS/iPadOS**.

Agregar un grupo nuevo

Use los siguientes pasos para crear un grupo.

1. Inicie sesión en el Centro de administración de Microsoft Endpoint Manager.
2. Seleccione **Grupos** > **Nuevo grupo**:



3. En **Tipo de grupo**, elija una de las opciones siguientes:
   - **Seguridad**: los grupos de seguridad definen quién puede acceder a los recursos, y se recomiendan para los grupos de Intune. Por ejemplo, puede crear grupos para usuarios, como **Todos los empleados de Charlotte** o **Trabajadores remotos**. O bien, puede crear grupos para dispositivos, como **Todos los dispositivos iOS/iPadOS** o **Todos los dispositivos Windows 10 de los alumnos**.

> **TIP**
>
> Los usuarios y los grupos creados también pueden verse en el Centro de administración de Microsoft 365, el centro de administración de Azure Active Directory y Microsoft Intune en Azure Portal. En el inquilino de la organización, puede crear y administrar grupos en todas estas áreas.
>
> Si su rol principal es la administración de dispositivos, se recomienda usar el Centro de administración de Microsoft Endpoint Manager.

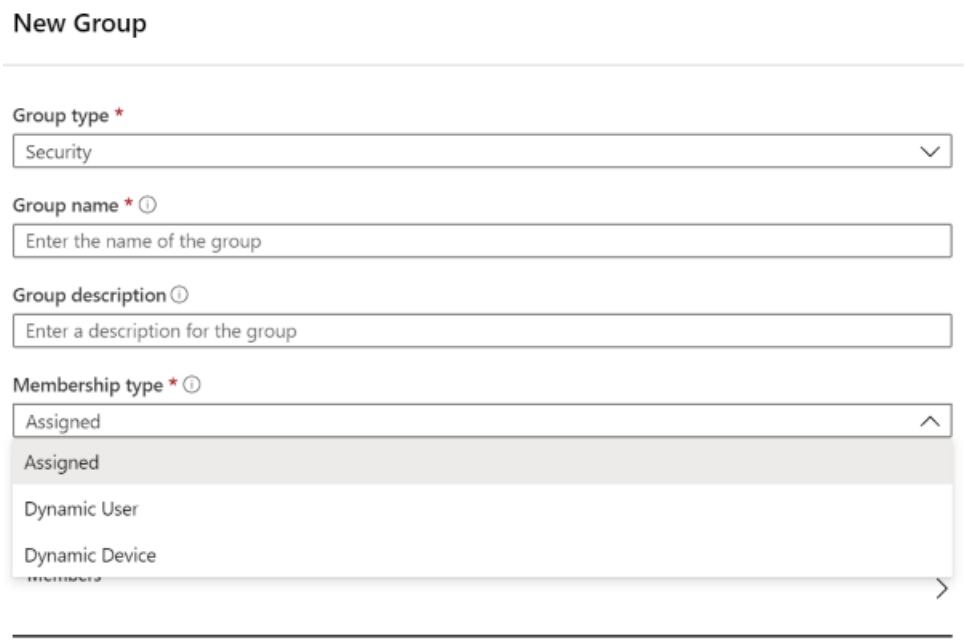
- **Microsoft 365**: Proporciona oportunidades de colaboración al otorgar a los miembros acceso compartido a un buzón, calendario, archivos, sitio de SharePoint, etc. Esta opción también le permite conceder acceso al grupo a personas ajenas a la organización. Para obtener más información, consulte Más información sobre los grupos de Microsoft 365.

4. Escriba los valores para **Nombre del grupo** y **Descripción del grupo** del nuevo grupo. Sea concreto e incluya información que permita a que otros usuarios saber para qué sirve el grupo.

   Por ejemplo, escriba **Todos los dispositivos de los alumnos de Windows 10** como nombre del grupo y **Todos los dispositivos de Windows 10 que usan los alumnos de secundaria de Contoso de los niveles 9-12** como descripción del grupo.

5. Especifique el valor de **Tipo de pertenencia**. Las opciones son:

   - **Asignados**: los administradores asignan manualmente usuarios o dispositivos a este grupo y quitan manualmente usuarios o dispositivos.
   - **Usuario dinámico**: los administradores crean reglas de pertenencia para agregar y quitar miembros automáticamente.
   - **Dispositivo dinámico**: los administradores crean reglas de grupo dinámicas para agregar y quitar dispositivos automáticamente.



Para más información sobre estos tipos de pertenencia y la creación de expresiones dinámicas, consulte:

- Creación de un grupo básico e incorporación de miembros con Azure Active Directory
- Reglas de pertenencia dinámica a grupos de Azure Active Directory

> **NOTE**
>
> En este centro de administración, al crear usuarios o grupos, es posible que no vea la personalización de marca de **Azure Active Directory**. Sin embargo, eso es lo que está usando.

6. Elija **Crear** para agregar el nuevo grupo. El grupo se muestra en la lista.

> **TIP**
>
> Tenga en cuenta algunos de los otros grupos de dispositivos y usuarios dinámicos que puede crear, por ejemplo:
>
> - Todos los estudiantes de secundaria de Contoso
> - Todos los dispositivos Android Enterprise
> - Todos los dispositivos iOS 11 y anteriores
> - Marketing
> - Recursos humanos
> - Todos los empleados de Charlotte
> - Todos los empleados de WA

Grupos y directivas

El acceso a los recursos de su organización está controlado por los usuarios y grupos que se creen.

Al crear grupos, tenga en cuenta cómo se aplicarán las directivas de cumplimiento y los perfiles de configuración. Por ejemplo, puede tener:

- Directivas que son específicas de un sistema operativo de dispositivo.
- Directivas que son específicas de los distintos roles de su organización.
- Directivas que son específicas de las unidades organizativas definidas en Active Directory.

Para crear los requisitos básicos de cumplimiento de la organización, puede crear una directiva predeterminada que se aplique a todos los grupos y dispositivos. Luego, puede crear directivas más específicas para las categorías más amplias de usuarios y dispositivos. Por ejemplo, puede crear directivas de correo electrónico para cada uno de los sistemas operativos de dispositivos.

Para instrucciones y recomendaciones sobre los perfiles de configuración, consulte Asignación de perfiles de dispositivo en Microsoft Intune y Recomendaciones de perfiles.

Vea también

- Control de acceso basado en rol (RBAC) con Microsoft Intune
- Administración del acceso a recursos y aplicaciones con grupos en Azure Active Directory
- Asignación de aplicaciones a grupos con Microsoft Intune

Asignar licencias a los usuarios para que puedan inscribir dispositivos en Intune

14/05/2021 • 4 minutes to read

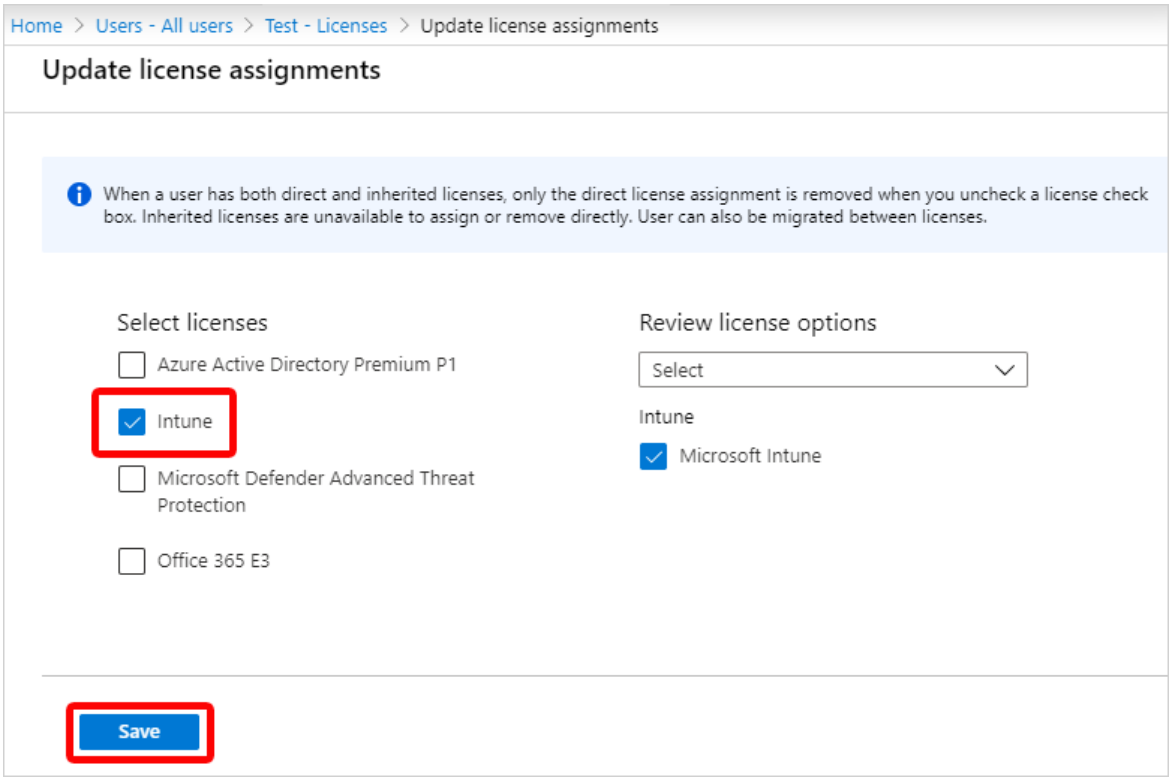
Tanto si quiere agregar usuarios manualmente como si quiere sincronizar desde Active Directory local, debe asignar primero a cada usuario una licencia de Intune para que los usuarios puedan inscribir sus dispositivos en Intune. Para obtener una lista de licencias, vea Licencias que incluyen Intune.

> **NOTE**
> Los usuarios que tienen asignada la directiva de protección de aplicaciones de Intune y no inscriben sus dispositivos en Microsoft Intune también necesitarán una licencia de Intune para recibir la directiva.

Asignación de una licencia de Intune en el Centro de administración de Microsoft Endpoint Manager

Puede usar el Centro de administración de Microsoft Endpoint Manager para agregar manualmente usuarios basados en la nube y asignar licencias a las cuentas de usuario basadas en la nube y a las cuentas sincronizadas desde Active Directory local con Azure AD.

1. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Usuarios** > **Todos los usuarios** > elija un usuario > **Licencias** > **Asignaciones**.
2. Elija el cuadro para **Intune** > **Guardar**. Si desea usar Enterprise Mobility + Security E5 u otra licencia, active ese cuadro en su lugar.



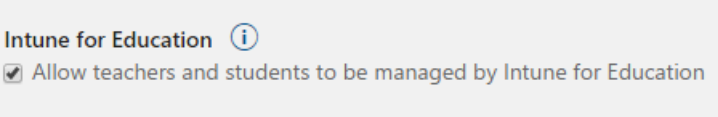
3. Ahora, la cuenta de usuario tiene los permisos necesarios para usar el servicio e inscribir dispositivos en la administración.

Asignación de una licencia de Intune con Azure Active Directory

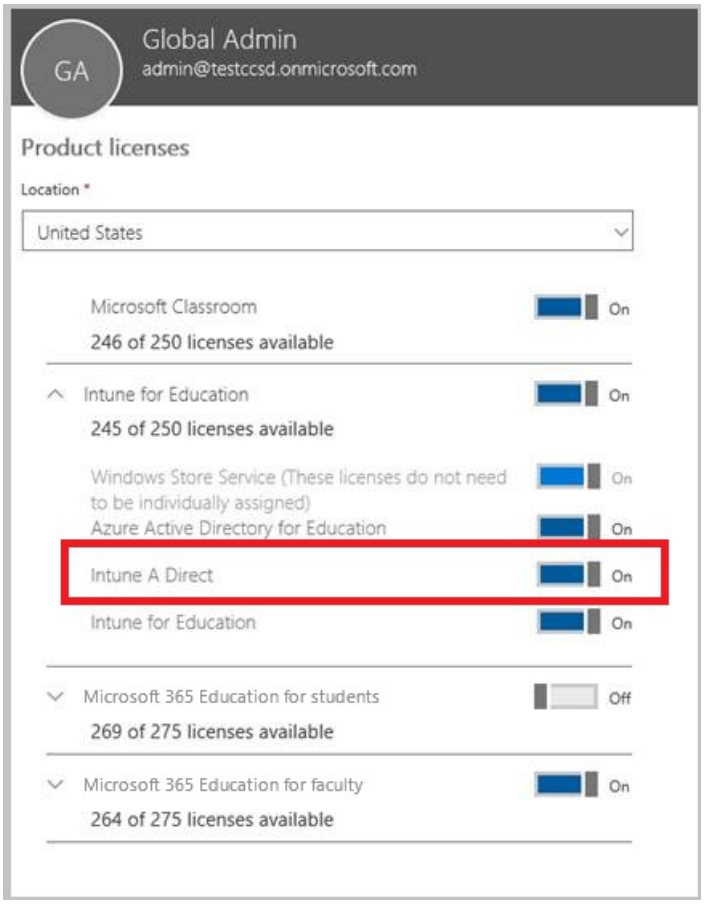
También puede asignar licencias de Intune a los usuarios a través de Azure Active Directory. Para más información, consulte el artículo Licencia de usuarios en Azure Active Directory.

Uso de School Data Sync para asignar licencias a los usuarios de Intune for Education

Si se trata de una organización educativa, puede utilizar School Data Sync (SDS) para asignar licencias de Intune for Education a los usuarios sincronizados. Active la casilla de Intune for Education al configurar el perfil de SDS.



Al asignar una licencia de Intune for Education, asegúrese de que también se asigne la licencia de Intune A Direct.



Vea la información general de School Data Sync para obtener más información sobre SDS.

Cómo las licencias de usuario y dispositivo afectan el acceso a los servicios

- Cada **usuario** al que asigna una licencia de software de usuario puede acceder a los servicios en línea y al software relacionado (incluido software de System Center) y usarlos para administrar las aplicaciones y hasta 15 dispositivos MDM.
- Puede comprar licencias para cualquier dispositivo por separado de las licencias de usuario. No es necesario que las licencias de dispositivo se asignen a los dispositivos. Cada dispositivo que accede y utiliza los servicios en línea y el software relacionado (incluido el software System Center) debe tener una licencia de

dispositivo.

- Si más de un usuario usa un dispositivo, cada uno de ellos debe tener una licencia de software de dispositivos, o bien todos los usuarios deben tener una licencia de software de usuario.

Descripción del tipo de licencias adquiridas

El modo en el que haya adquirido Intune determina la información de la suscripción:

- Si ha adquirido Intune a través de un Contrato Enterprise, encontrará la información de suscripción en el portal de licencias por volumen, en **Suscripciones**.
- Si ha adquirido Intune a través de un Proveedor de soluciones en la nube, acuda a su distribuidor.
- Si ha adquirido Intune con una tarjeta de crédito o con factura, las licencias se basarán en el usuario.

Usar PowerShell para administrar de forma selectiva las licencias de usuario de EMS

Las organizaciones que usan Microsoft Enterprise Mobility + Security (anteriormente denominado Enterprise Mobility Suite) pueden tener usuarios que solo necesiten Azure Active Directory Premium o los servicios de Intune en el paquete de EMS. Puede asignar un servicio o un subconjunto de servicios mediante los cmdlets de PowerShell de Azure Active Directory.

Para asignar licencias de usuario de forma selectiva a los servicios de EMS, abra PowerShell como administrador en un equipo que tenga instalado el módulo de Azure Active Directory para Windows PowerShell. Puede instalar PowerShell en un equipo local o en un servidor de ADFS.

Debe crear una nueva definición de SKU de licencia que solo se aplique a los planes de servicio deseados. Para ello, deshabilite los planes que no quiera aplicar. Por ejemplo, podría crear una definición de SKU de licencia que no asigne una licencia de Intune. Para ver una lista con los servicios disponibles, escriba:

```
(Get-MsolAccountSku | Where {$_.SkuPartNumber -eq "EMS"}).ServiceStatus
```

Puede ejecutar el comando siguiente para excluir el plan de servicio Intune. Puede usar el mismo método para realizar una expansión a todo un grupo de seguridad o puede usar filtros más pormenorizados.

Ejemplo 1
Cree un nuevo usuario en la línea de comandos y asigne una licencia de EMS sin habilitar la parte de Intune de la licencia:

```
Connect-MsolService

New-MsolUser -DisplayName "Test User" -FirstName FName -LastName LName -UserPrincipalName
user@<TenantName>.onmicrosoft.com –Department DName -UsageLocation US

$CustomEMS = New-MsolLicenseOptions -AccountSkuId "<TenantName>:EMS" -DisabledPlans INTUNE_A
Set-MsolUserLicense -UserPrincipalName user@<TenantName>.onmicrosoft.com -AddLicenses <TenantName>:EMS -
LicenseOptions $CustomEMS
```

Realice la comprobación con lo siguiente:

```
(Get-MsolUser -UserPrincipalName "user@<TenantName>.onmicrosoft.com").Licenses.ServiceStatus
```

Ejemplo 2
Deshabilite la parte de Intune de la licencia de EMS de un usuario que ya tenga asignada una licencia:

```
Connect-MsolService

$CustomEMS = New-MsolLicenseOptions -AccountSkuId "<TenantName>:EMS" -DisabledPlans INTUNE_A
Set-MsolUserLicense -UserPrincipalName user@<TenantName>.onmicrosoft.com -LicenseOptions $CustomEMS
```

Realice la comprobación con lo siguiente:

```
(Get-MsolUser -UserPrincipalName "user@<TenantName>.onmicrosoft.com").Licenses.ServiceStatus
```

Licencias de Microsoft Intune

14/05/2021 • 2 minutes to read

Microsoft Intune está disponible para las distintas necesidades de los clientes y los diversos tamaños de las organizaciones, desde una experiencia de administración fácil de usar para escuelas y pequeñas empresas a funcionalidades más avanzadas requeridas por los clientes empresariales. La mayoría de las licencias que incluyen Microsoft Intune también conceden los derechos a usar Microsoft Endpoint Configuration Manager, siempre y cuando la suscripción permanezca activa. Un administrador debe tener una licencia asignada para administrar Intune (a menos que permita a los administradores sin licencia).

Microsoft Intune

Intune se incluye en las licencias siguientes:

- Microsoft 365 E5
- Microsoft 365 E3
- Enterprise Mobility + Security E5
- Enterprise Mobility + Security E3
- Microsoft 365 Empresa Premium
- Microsoft 365 F1
- Microsoft 365 F3
- Microsoft 365 Administración Pública G5
- Microsoft 365 Administración Pública G3
- Intune para educación

Microsoft Intune for Education

Intune for Education se incluye en las licencias siguientes:

- Microsoft 365 Education A5
- Microsoft 365 Education A3

Licencias para dispositivos administrados por Configuration Manager en Intune

Para que los dispositivos administrados por Configuration Manager existentes se inscriban en Intune para la administración conjunta a escala sin interacción del usuario, la administración conjunta usa una característica de Azure Active Directory (Azure AD) denominada inscripción automática de Windows 10. La inscripción automática con administración conjunta requiere licencias tanto para Azure AD Premium (AADP1) como para Intune. A partir del 1 de diciembre de 2019, ya no es necesario asignar licencias de Intune individuales para este escenario. Microsoft Endpoint Manager ahora incluye licencias de Intune para la administración conjunta. El requisito de licencia de AADP1 independiente sigue siendo el mismo para que funcione este escenario. De todos modos tiene que asignar licencias de Intune para otros escenarios de inscripción.

Información adicional

- Una suscripción de dispositivos y del usuario de Microsoft Intune está disponible como independiente, además de las agrupaciones indicadas arriba.

- Una suscripción solo de dispositivos de Microsoft Intune está disponible para administrar quioscos, dispositivos dedicados, dispositivos de sala de teléfono, IoT y otros dispositivos de uso único que no requieren características de seguridad y administración basadas en el usuario. Para obtener más información, vea Introducción a las licencias de dispositivos en Microsoft Intune.
- La licencia de Microsoft Intune adecuada es necesaria si un usuario o dispositivo se beneficia de forma directa o indirecta del servicio de Microsoft Intune, incluido el acceso a dicho servicio a través de una API de Microsoft.
- Intune no se incluye en las licencias que no figuran en las tablas anteriores.

Administradores sin licencia

Para obtener más información sobre cómo conceder a los administradores acceso a Microsoft Endpoint Manager sin una licencia de Intune, consulte Administradores sin licencia.

Visite la página de licencias de Microsoft para obtener la información más reciente sobre ediciones de productos, actualizaciones de licencias de productos, planes de licencias de volumen y otra información relacionada con sus casos de uso específicos.

Para obtener información sobre cómo las licencias de usuario y dispositivo afectan el acceso a los servicios, y cómo se debe asignar una licencia a un usuario, consulte el artículo sobre cómo asignar licencias de Intune a las cuentas de usuario.

Establecer la entidad de administración de dispositivos móviles

14/05/2021 • 10 minutes to read

La configuración de la entidad de administración de dispositivos móviles (MDM) determina cómo se administran los dispositivos. Como administrador de TI, debe establecer una entidad de MDM antes de que los usuarios puedan inscribir dispositivos para la administración.

Las configuraciones posibles son:

- **Intune independiente**: administración solo en la nube, que se configura con Azure Portal. Incluye el conjunto completo de funcionalidades que ofrece Intune. Establecer la entidad de MDM en la consola de Intune.
- **Administración conjunta de Intune**: integración de la solución de nube de Intune con Configuration Manager para dispositivos Windows 10. Intune se configura mediante la consola de Configuration Manager. Configuración de la inscripción automática de dispositivos en Intune.
- **Basic Mobility and Security for Microsoft 365** (Movilidad y seguridad básicas para Microsoft 365): si tiene esta configuración activada, verá la entidad de MDM establecida en "Office 365". Si quiere empezar a usar Intune, deberá adquirir licencias de Intune.
- **Coexistencia de Basic Mobility and Security for Microsoft 365** (Movilidad y seguridad básicas para Microsoft 365): puede agregar Intune a su inquilino si ya usa Basic Mobility and Security for Microsoft 365 y establecer la entidad de administración en Intune o en Basic Mobility and Security for Microsoft 365 para que cada usuario indique qué servicio se usará para administrar sus dispositivos inscritos en MDM. La entidad de administración del usuario se define en función de la licencia asignada al usuario: Si el usuario tiene solo una licencia básica o estándar de Microsoft 365, los dispositivos se administrarán mediante Basic Mobility and Security for Microsoft 365. Si el usuario tiene una licencia de Intune, los dispositivos se administrarán mediante Intune. Si agrega una licencia de Intune a un usuario administrado previamente por Basic Mobility and Security for Microsoft 365, sus dispositivos se cambiarán a la administración de Intune. Asegúrese de tener las configuraciones de Intune asignadas a los usuarios para reemplazar Basic Mobility and Security for Microsoft 365 antes de cambiar los usuarios a Intune; de lo contrario, sus dispositivos perderán la configuración de Basic Mobility and Security for Microsoft 365 y no recibirán ningún reemplazo de Intune.

Establecimiento de la entidad de MDM en Intune

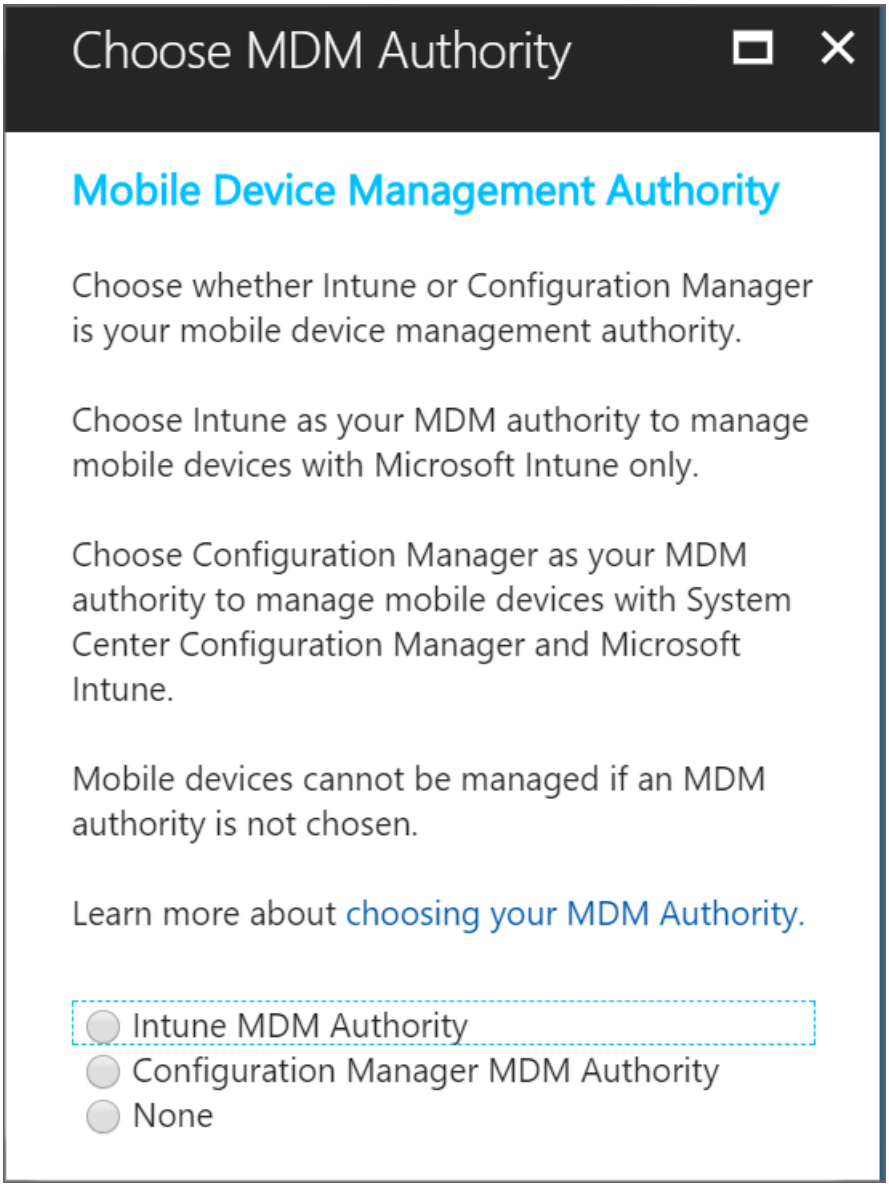
En el caso de los inquilinos que usan la versión de servicio 1911 y versiones posteriores, la entidad de MDM se establece automáticamente en Intune.

En el caso de los inquilinos de versión de servicio anterior a 1911, haga lo siguiente si aún no ha establecido la entidad de MDM.

1. En el Centro de administración de Microsoft Endpoint Manager, seleccione el banner naranja para abrir la configuración **Entidad de administración de dispositivos móviles**. El banner naranja aparece únicamente si aún no ha establecido la entidad de MDM.
2. En **Entidad de administración de dispositivos móviles**, elija la entidad de MDM entre las opciones siguientes:

- **Entidad de MDM de Intune**

- Ninguno



Un mensaje indica que ha configurado correctamente su entidad de MDM en Intune.

Flujo de trabajo de UI de administración de Intune

Cuando se habilita la administración de dispositivos Android o Apple, Intune envía información del usuario y dispositivo para integrar con estos servicios de terceros a fin de administrar sus dispositivos correspondientes.

Los escenarios que agregan un consentimiento para compartir datos se incluyen cuando:

- Se habilitan perfiles de trabajo de propiedad personal y corporativa de Android Enterprise.
- Se habilitan y cargan certificados push MDM de Apple.
- Se habilita cualquiera de los servicios de Apple, por ejemplo, el Programa de inscripción de dispositivos, School Manager o el Programa de Compras por Volumen.

En cada caso, el consentimiento está estrictamente relacionado con la ejecución de un servicio de administración de dispositivos móviles. Por ejemplo, confirmar que un administrador de TI ha autorizado a dispositivos Google o Apple para que se inscriban. La documentación para tratar qué información se comparte cuando los nuevos flujos de trabajo se publican está disponible en las siguientes ubicaciones:

- Datos que Intune manda a Google
- Data que Intune manda a Apple

Principales consideraciones

Después de cambiar a la nueva entidad de MDM, habrá probablemente un tiempo de transición (hasta ocho horas) antes de que el dispositivo se compruebe y se sincronice con el servicio. Es necesario que configure los valores de la nueva entidad de MDM para asegurarse de que los dispositivos inscritos seguirán administrados y protegidos después del cambio.

- Los dispositivos deben conectarse al servicio después del cambio para que la configuración de la nueva entidad de MDM (Intune independiente) reemplace la configuración existente en el dispositivo.
- Después de cambiar la entidad de MDM, algunas de las opciones básicas (como los perfiles) de la entidad de MDM anterior permanecerán en el dispositivo durante siete días o hasta que el dispositivo se conecte al servicio por primera vez. Se recomienda que configure aplicaciones y valores (directivas, perfiles, aplicaciones, etc.) en la nueva entidad de MDM tan pronto como sea posible y que implemente la configuración en los grupos de usuarios que contienen usuarios con dispositivos ya inscritos. En cuanto el dispositivo se conecte con el servicio tras el cambio en la entidad de MDM, recibirá la nueva configuración desde la nueva entidad de MDM, evitando así los tiempos de inactividad en administración y protección.
- Los dispositivos sin usuarios asociados (normalmente cuando se tiene el Programa de inscripción de dispositivos iOS/iPadOS o escenarios de inscripción masiva) no se migran a la nueva entidad de MDM. Para esos dispositivos, debe llamar al soporte técnico para solicitar ayuda para trasladarlos a la nueva entidad de MDM.

Coexistence

Habilitar la coexistencia le permite usar Intune en un nuevo conjunto de usuarios y, al mismo tiempo, seguir usando la movilidad y seguridad básicas de los usuarios existentes. Puede controlar qué dispositivos administra Intune a través del usuario. Si a un usuario se le asigna una licencia de Intune o este usa la administración conjunta de Intune con Configuration Manager, Intune administrará todos sus dispositivos inscritos. De lo contrario, el usuario se administra mediante la movilidad y seguridad básicas.

Para habilitar la coexistencia, se deben realizar principalmente tres pasos:

1. Preparación
2. Adición de la entidad de MDM de Intune
3. Migración de usuarios y dispositivos (opcional).

Preparación

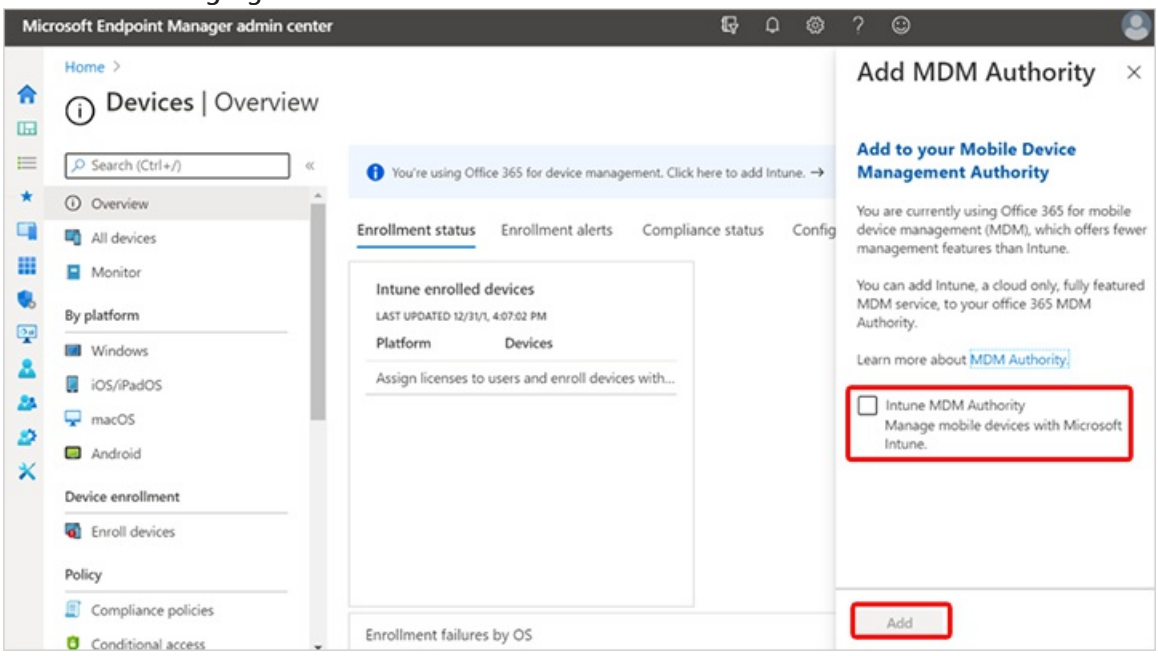
Antes de habilitar la coexistencia con la movilidad y seguridad básicas, tenga en cuenta los siguientes puntos:

- Asegúrese de que dispone de suficientes licencias de Intune para los usuarios que quiere administrar mediante Intune.
- Revise qué usuarios tienen asignadas licencias de Intune. Después de habilitar la coexistencia, todos los usuarios a los que ya se les haya asignado una licencia de Intune, tendrán sus dispositivos cambiados a Intune. Para evitar cambios de dispositivo inesperados, se recomienda no asignar ninguna licencia de Intune hasta que se haya habilitado la coexistencia.
- Cree e implemente directivas de Intune para reemplazar las directivas de seguridad de dispositivos que se implementaron originalmente mediante el Portal de seguridad y cumplimiento de Office 365. Este reemplazo debe realizarse para los usuarios que pasan de la movilidad y seguridad básicas a Intune. Si no hay ninguna directiva de Intune asignada a esos usuarios, la habilitación de la coexistencia podría hacer que se perdiera la configuración de la movilidad y seguridad básicas. Esta configuración se perderá sin que se reemplace, como es el caso de los perfiles de correo electrónico administrados. Incluso al reemplazar las directivas de seguridad de dispositivos por directivas de Intune, es posible que se pida a los usuarios que vuelvan a autenticar sus perfiles de correo electrónico después de que el dispositivo se mueva a la administración de Intune.

Adición de la entidad de MDM de Intune

Para habilitar la coexistencia, debe agregar Intune como entidad de MDM a su entorno:

1. Inicie sesión en el centro de administración de Microsoft Endpoint Manager con derechos de administrador global de Azure AD o de administrador del servicio Intune.
2. Vaya a **Dispositivos**.
3. Se muestra la hoja **Agregar entidad de MDM**.
4. Para cambiar la entidad de MDM de *Office 365* a *Intune* y habilitar la coexistencia, seleccione **Entidad de Intune MDM** > **Agregar**.



Migración de usuarios y dispositivos (opcional)

Una vez habilitada la entidad de MDM de Intune, la coexistencia se activa y puede empezar a administrar usuarios mediante Intune. También, si quiere mover los dispositivos administrados anteriormente mediante la movilidad y seguridad básicas para que los administre Intune, asigne a esos usuarios una licencia de Intune. Los dispositivos de los usuarios cambiarán a Intune en la siguiente sincronización de MDM. La configuración que se aplica a estos dispositivos mediante la movilidad y seguridad básicas dejará de aplicarse y se quitará de los dispositivos.

Limpieza de dispositivos móviles tras la expiración del certificado MDM

El certificado MDM se renueva automáticamente cuando los dispositivos móviles se comunican con el servicio de Intune. Si se borran los dispositivos móviles o estos no pueden comunicarse con el servicio de Intune durante un tiempo, el certificado de MDM no se renovará. El dispositivo se quita del portal de Azure 180 días después de que expire el certificado MDM.

Eliminación de la entidad de MDM

No se puede cambiar la entidad de MDM a Desconocido. El servicio usa la entidad de MDM para determinar a qué portal informan los dispositivos inscritos (Microsoft Intune o Basic Mobility and Security for Microsoft 365).

Qué esperar después de cambiar la entidad de MDM

- Cuando el servicio de Intune detecta que ha cambiado la entidad de MDM de un inquilino, envía un mensaje de notificación a todos los dispositivos inscritos para que inicien el proceso de comprobación y se sincronicen en el servicio (esta notificación no forma parte de la comprobación programada regularmente).

Por lo tanto, una vez que cambie la entidad de MDM para el inquilino de Intune independiente, todos los dispositivos que estén encendidos y en línea se conectarán en el servicio, recibirán la nueva entidad de MDM y serán administrados por esta. No hay ninguna interrupción en el proceso de administración y protección de estos dispositivos.

- Incluso para los dispositivos que están encendidos y en línea durante el cambio en la entidad de MDM (o poco tiempo después), pasarán hasta ocho horas (según el tiempo de la siguiente comprobación periódica programada) hasta que los dispositivos se registren en el servicio bajo la nueva entidad de MDM.

> **IMPORTANT**
> Entre el momento en que cambie la entidad MDM y se cargue el certificado de APNs renovado en la nueva entidad, se producirá un error en las inscripciones de nuevos dispositivos y las comprobaciones de dispositivos iOS/iPadOS. Por lo tanto, es importante revisar y cargar el certificado de Apple Push Notification Service en la nueva entidad tan pronto como sea posible después del cambio de entidad de MDM.

- Los usuarios pueden cambiar rápidamente a la nueva entidad de MDM iniciando manualmente una comprobación desde el dispositivo en el servicio. Los usuarios pueden realizar este cambio con facilidad mediante la aplicación del Portal de empresa y el inicio de una comprobación de cumplimiento del dispositivo.
- Para validar que todo funciona correctamente después de que los dispositivos se hayan comprobado y sincronizado con el servicio tras el cambio de entidad de MDM, busque los dispositivos en la entidad de MDM.
- Existe un período transitorio entre el momento en que un dispositivo está sin conexión durante el cambio de entidad de MDM y el momento en que se comprueba la idoneidad de ese dispositivo para su registro en el servicio. Para garantizar que el dispositivo permanece protegido y funcional durante este período transitorio, los siguientes perfiles permanecen en el dispositivo hasta siete días (o hasta que el dispositivo se conecte con la nueva entidad de MDM y reciba la nueva configuración que sobrescribirá la actual):
  - Perfil de correo electrónico
  - Perfil de VPN
  - Perfil de certificado
  - Perfil de Wi-Fi
  - Perfiles de configuración
- Después de cambiar a la nueva entidad de MDM, los datos de cumplimiento de la consola de administración de Microsoft Intune pueden tardar hasta una semana en informar con exactitud. Pero los estados de cumplimiento de Azure Active Directory y en el dispositivo serán precisos para que el dispositivo siga estando protegido.
- Compruebe que la nueva configuración destinada a sobrescribir la configuración actual tiene el mismo nombre que la anterior para asegurarse de que efectivamente se sobrescribe. En caso contrario, los dispositivos podrían terminar con directivas y perfiles redundantes.

> **TIP**
> Es recomendable que cree todas las configuraciones y parámetros de administración, así como las implementaciones, poco después de que se haya completado el cambio a la entidad de MDM. De esta manera se asegurará de que los dispositivos están protegidos y se administran de manera activa durante el período transitorio.

- Después de cambiar la entidad de MDM, siga estos pasos para validar que los nuevos dispositivos se inscriben correctamente en la nueva entidad:
  - Inscripción de un dispositivo nuevo
  - Asegúrese de que el dispositivo recién inscrito aparece en la entidad de MDM.

    - Realice una acción, como el bloqueo remoto, desde la consola de administración en el dispositivo. Si se completa correctamente, el dispositivo se está administrando mediante la nueva entidad de MDM.
- Si tiene problemas con dispositivos concretos, puede anular la inscripción de esos dispositivos y realizarla de nuevo para que se conecten a la nueva entidad y se administren lo antes posible.

Pasos siguientes

Con la entidad de MDM configurada, puede empezar a inscribir dispositivos.

Control de acceso basado en rol (RBAC) con Microsoft Intune

14/05/2021 • 4 minutes to read

El control de acceso basado en rol (RBAC) ayuda a administrar quién tiene acceso a los recursos de la organización y qué se puede hacer con dichos recursos. Mediante la asignación de roles a los usuarios de Intune, puede limitar lo que pueden ver y cambiar. Cada rol tiene un conjunto de permisos que determinan a qué pueden acceder y qué pueden cambiar dentro de la organización los usuarios con dicho rol.

Para crear, editar o asignar roles, la cuenta debe tener uno de los siguientes permisos en Azure AD:

- **Administrador global**
- **Administrador del servicio Intune** (también conocido como **Administrador de Intune**)

Para obtener consejos y sugerencias sobre la RBAC en Intune, puede ver esta serie de cinco vídeos en los que se muestran ejemplos y tutoriales: 1, 2, 3, 4, 5.

Roles

Un rol define el conjunto de permisos concedidos a los usuarios que están asignados a ese rol. Puede usar tanto los roles integrados como roles personalizados. Los roles integrados abarcan algunos escenarios comunes de Intune. También puede crear sus propios roles personalizados con el conjunto de permisos que exactamente necesita. Varios roles de Azure Active Directory tienen permisos para Intune. Para ver un rol, seleccione **Intune** > **Administración de inquilinos** > **Roles** > **Todos los roles** > elija un rol. Podrá administrar el rol en las siguientes páginas:

- **Propiedades**: el nombre, la descripción, los permisos y las etiquetas de ámbito para el rol.
- **Asignaciones**: lista de asignaciones de roles que definen qué usuarios tienen acceso a qué usuarios o dispositivos. Un rol puede tener varias asignaciones y un usuario puede tener varias asignaciones.

Roles integrados

Puede asignar roles integrados a los grupos sin ninguna configuración adicional. No se puede eliminar o editar el nombre, la descripción, el tipo o los permisos de un rol integrado.

- **Administrador de aplicaciones**: permite administrar las aplicaciones móviles y administradas, leer la información del dispositivo y ver los perfiles de configuración del dispositivo.
- **Administrador de seguridad de puntos de conexión**: administra las características de seguridad y cumplimiento, como las líneas de base de seguridad, el cumplimiento de dispositivos, el acceso condicional y Microsoft Defender para punto de conexión.
- **Operador del departamento de soporte técnico**: realiza tareas remotas relacionadas con usuarios y dispositivos y puede asignar aplicaciones o directivas a usuarios o dispositivos.
- **Administrador de roles de Intune**: permite administrar los roles de Intune personalizados y agregar las asignaciones de roles de Intune integrados. Esta es la única función de Intune que permite asignar permisos a los administradores.
- **Administrador de directivas y perfiles**: administra la directiva de cumplimiento, los perfiles de configuración, la inscripción de Apple, los identificadores de dispositivos corporativos y las líneas base de seguridad.
- **Operador de solo lectura**: ve información sobre usuarios, dispositivos, inscripciones, configuraciones y aplicaciones. No puede realizar cambios en Intune.

- **Administrador de la escuela**: administra dispositivos Windows 10 en Intune for Education.

Roles personalizados

Puede crear sus propios roles con permisos personalizados. Para obtener más información sobre los roles personalizados, vea Creación de un rol personalizado.

Roles de Azure Active Directory con acceso a Intune

ROL DE AZURE ACTIVE DIRECTORY	TODOS LOS DATOS DE INTUNE	DATOS DE AUDITORÍA DE INTUNE
Administrador global	Lectura/escritura	Lectura/escritura
Administrador de servicios de Intune	Lectura/escritura	Lectura/escritura
Administrador de acceso condicional	None	None
Administrador de seguridad	Solo lectura (permisos administrativos completos para el nodo Seguridad de puntos de conexión)	Solo lectura
Operador de seguridad	Solo lectura	Solo lectura
Lector de seguridad	Solo lectura	Solo lectura
Administrador de cumplimiento	Ninguno	Solo lectura
Administrador de datos de cumplimiento	Ninguno	Solo lectura
Lector global	Solo lectura	Solo lectura
Lector de informes	Solo lectura	None

TIP

Intune también muestra tres extensiones de Azure AD: **Usuarios**, **Grupos** y **Acceso condicional**, que se controlan mediante RBAC en Azure AD. Además, el **administrador de cuentas de usuario** solo realiza actividades de usuario o grupo de AAD y no tiene permisos completos para realizar todas las actividades en Intune. Para más información, vea RBAC con Azure AD.

Asignaciones de roles

Una asignación de roles define:

- Qué usuarios están asignados al rol.
- Qué recursos pueden ver.
- Qué recursos pueden cambiar.

Puede asignar a los usuarios tanto roles personalizados como integrados. Para asignar un rol de Intune a un usuario, este debe tener una licencia de Intune. Para ver una asignación de roles, elija **Intune** > **Administración de inquilinos** > **Roles** > **Todos los roles** > elija un rol > **Asignaciones** > elija una asignación. En la página **Propiedades**, puede editar:

- **Aspectos básicos**: el nombre y la descripción de las asignaciones.

- **Miembros**: todos los usuarios de los grupos de seguridad de Azure mostrados tienen permiso para administrar los usuarios o los dispositivos que aparecen en Ámbito (grupos).
- **Ámbito (grupos)** : los usuarios de Miembros pueden administrar todos los usuarios o dispositivos de estos grupos de seguridad de Azure.
- **Ámbito (etiquetas)** : los usuarios de Miembros pueden ver los recursos que tienen las mismas etiquetas de ámbito.

Asignaciones de varios roles

Si un usuario tiene varias asignaciones de roles, los permisos y las etiquetas de ámbito de estas asignaciones de roles se amplían a diferentes objetos, como se indica a continuación:

- Los permisos de asignación y las etiquetas de ámbito solo se aplican a los objetos (como directivas o aplicaciones) del Ámbito (grupos) de la asignación de ese rol. Los permisos de asignación y las etiquetas de ámbito no se aplican a los objetos de otras asignaciones de roles, a menos que la otra asignación los conceda específicamente.
- Otros permisos (por ejemplo, los de creación, lectura, actualización y eliminación) y las etiquetas de ámbito se aplican a todos los objetos del mismo tipo (como todas las directivas o aplicaciones) en cualquiera de las asignaciones del usuario.
- Los permisos y las etiquetas de ámbito para objetos de tipos diferentes (como directivas o aplicaciones) no se aplican entre sí. Por ejemplo, un permiso de lectura para una directiva no proporciona un permiso de lectura a las aplicaciones de las asignaciones del usuario.

Pasos siguientes

- Asignar de un rol a un usuario
- Crear un rol personalizado

Asignación de un rol a un usuario de Intune

14/05/2021 • 2 minutes to read

Puede asignar un rol integrado o personalizado a un usuario de Intune.

Para crear, editar o asignar roles, la cuenta debe tener uno de los siguientes permisos en Azure AD:

- **Administrador global**
- **Administrador del servicio de Intune**

1. En el Centro de administración de Microsoft Endpoint Manager, elija **Administración de inquilinos** > **Roles** > **Todos los roles**.
2. En la hoja **Roles de Intune: Todos los roles**, elija el rol integrado que quiera asignar > **Asignaciones** > **Asignar**.
3. En la página **Datos básicos**, escriba un **Nombre de asignación** y una **Descripción de la asignación** opcional y, luego, elija **Siguiente**.
4. En la página **Grupos de administradores**, seleccione el grupo que contenga el usuario al que quiera conceder los permisos. Elija **Siguiente**.
5. En la página **Ámbito (grupos)** , elija un grupo que contenga los usuarios o dispositivos que el miembro anterior tendrá permiso para administrar. Seleccione **Siguiente**.
6. En la página **Ámbito (etiquetas)** , elija las etiquetas donde se aplicará esta asignación de roles. Seleccione **Siguiente**.
7. Cuando haya terminado, elija **Crear** en la página **Revisar y crear**. La nueva asignación se muestra en la lista de asignaciones.

Pasos siguientes

- Más información sobre el control de acceso basado en rol en Intune
- Creación de un rol personalizado

Creación de un rol personalizado en Intune

14/05/2021 • 2 minutes to read

Puede crear un rol personalizado en Intune que incluya los permisos necesarios para una función de trabajo específica. Por ejemplo, si un grupo del departamento de TI administra las aplicaciones, las directivas y los perfiles de configuración, puede agregar todos los permisos juntos en un rol personalizado. Después de crear un rol personalizado, puede asignarlo a todos los usuarios que necesiten esos permisos.

Para crear, editar o asignar roles, la cuenta debe tener uno de los siguientes permisos en Azure AD:

- **Administrador global**
- **Administrador del servicio de Intune**

Para crear un rol personalizado

1. En el Centro de administración de Microsoft Endpoint Manager, elija **Administración de inquilinos** > **Roles** > **Todos los roles** > **Crear**.
2. En la página **Datos básicos**, escriba un nombre y una descripción para el nuevo rol y, después, elija **Siguiente**.
3. En la página **Permisos**, elija los permisos que quiera usar con este rol.
4. En la página **Ámbito (etiquetas)** , seleccione las etiquetas para este rol. Cuando este rol se asigna a un usuario, el usuario puede acceder a los recursos que también tienen estas etiquetas. Elija **Siguiente**.
5. Cuando haya terminado, elija **Crear** en la página **Revisar y crear**. El nuevo rol se muestra en la lista de la hoja **Roles de Intune: Todos los roles**.

Copia de un rol

También puede copiar un rol existente.

1. En el Centro de administración de Microsoft Endpoint Manager, elija **Administración de inquilinos** > **Roles** > **Todos los roles** > active la casilla de un rol de la lista > **Duplicar**.
2. En la página **Datos básicos**, escriba un nombre. Asegúrese de usar un nombre único.
3. Todos los permisos y etiquetas de ámbito del rol original estarán ya seleccionados. Posteriormente, puede cambiar los valores de **Nombre**, **Descripción**, **Permisos** y **Ámbito (etiquetas)** del rol duplicado.
4. Una vez realizados todos los cambios que quiere, elija **Siguiente** para ir a la página **Revisar y crear**. Seleccione **Crear**.

Pasos siguientes

- Asignación de un rol a un usuario
- Más información sobre el control de acceso basado en rol en Intune

Usar control de acceso basado en rol (RBAC) y etiquetas de ámbito para TI distribuida

14/05/2021 • 5 minutes to read

Puede usar control de acceso basado en rol y etiquetas de ámbito para asegurarse de que los administradores adecuados tengan el acceso y la visibilidad correctos para los objetos de Intune apropiados. Los roles determinan qué acceso tienen los administradores a qué objetos. Las etiquetas de ámbito determinan qué objetos pueden ver los administradores.

Por ejemplo, imagine que un administrador de la sucursal regional de Seattle tiene el rol Administrador de perfiles y directivas. Quiere que este administrador solo vea y administre los perfiles y las directivas que se aplican exclusivamente a los dispositivos de Seattle. Para configurar este acceso, debería hacer lo siguiente:

1. Crear una etiqueta de ámbito denominada Seattle.
2. Crear una asignación de roles para el rol Administrador de perfiles y directivas con:
   - Miembros (grupos) = un grupo de seguridad denominado Administradores de TI de Seattle. Todos los administradores de este grupo tienen permiso para administrar las directivas y los perfiles de los usuarios o los dispositivos de Ámbito (grupos).
   - Ámbito (grupos) = un grupo de seguridad denominado Usuarios de Seattle. Todos los usuarios o dispositivos de este grupo pueden tener sus perfiles y directivas administrados por los administradores de Miembros (grupos).
   - Ámbito (etiquetas) = Seattle. Los administradores de Miembros (grupos) pueden ver los objetos de Intune que tienen también la etiqueta de ámbito Seattle.
3. Agregue la etiqueta de ámbito Seattle a las directivas y los perfiles a los que quiera que puedan tener acceso los administradores de Miembros (grupos).
4. Agregar la etiqueta de ámbito Seattle a los dispositivos que quiere que sean visibles para los administradores de Miembros (grupos).

Etiquetas de ámbito predeterminadas

La etiqueta de ámbito predeterminada se agrega de forma automática a todos los objetos sin etiqueta que admiten etiquetas de ámbito.

Esta característica es similar a la característica de ámbitos de seguridad de Microsoft Endpoint Configuration Manager.

Para crear una etiqueta de ámbito

1. En el Centro de administración de Microsoft Endpoint Manager, elija **Administración de inquilinos** > **Roles** > **Ámbito (etiquetas)** > **Crear**.
2. En la página **Datos básicos**, proporcione un **Nombre** y una **Descripción** opcional. Elija **Siguiente**.
3. En la página **Asignaciones**, elija los grupos que contengan los dispositivos que quiera asignar a esta etiqueta de ámbito. Elija **Siguiente**.
4. En la página **Revisar y crear**, elija **Crear**.

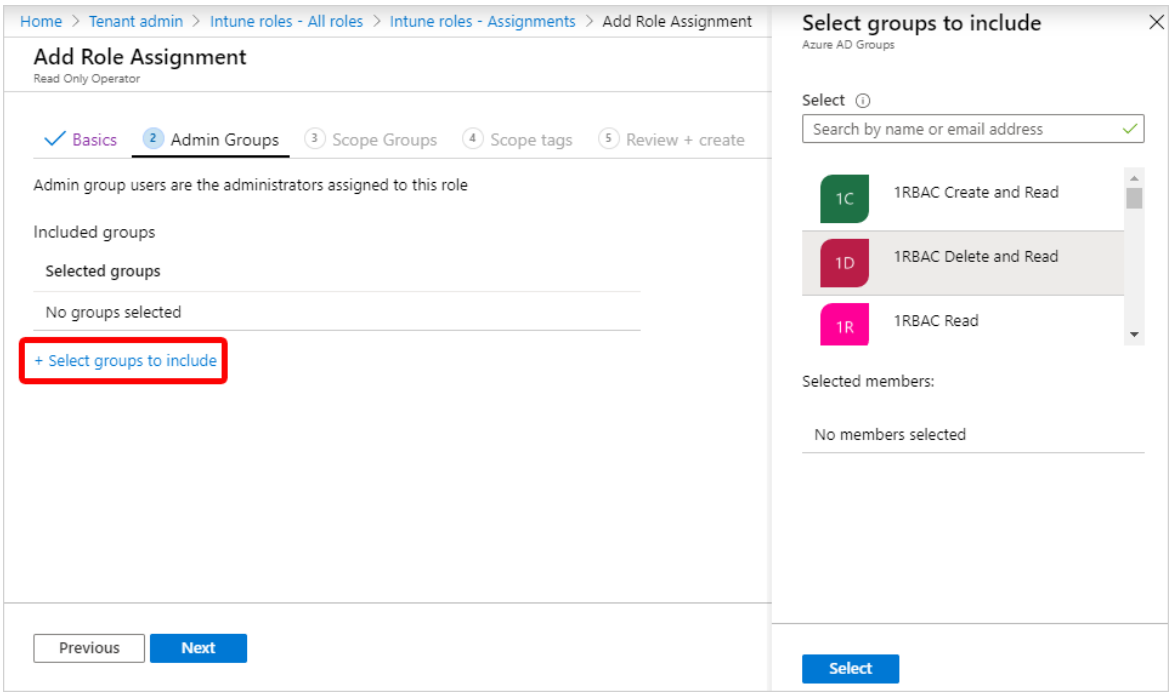
Para asignar una etiqueta de ámbito a un rol

1. En el Centro de administración de Microsoft Endpoint Manager, elija **Administración de inquilinos** >

Roles > **Todos los roles** > seleccione un rol > **Asignaciones** > **Asignar**.

2. En la página **Datos básicos**, proporcione un **Nombre de asignación** y una **Descripción**. Elija **Siguiente**.

3. En la página **Grupos de administración**, elija **Seleccionar grupos para incluir** y seleccione los grupos que quiere que formen parte de esta asignación. Los usuarios de este grupo tendrán permisos para administrar los usuarios o dispositivos de Ámbito (grupos). Elija **Siguiente**.



4. En la página **Grupos de ámbito**, seleccione una de las opciones siguientes para **Asignar a**

   - **Grupos seleccionados**: seleccione los grupos que contienen los usuarios o dispositivos que quiere administrar. Todos los usuarios o dispositivos de los grupos seleccionados serán administrados por los usuarios de los grupos de administración.
   - **Todos los usuarios**: todos los usuarios pueden ser administrados por los usuarios de los grupos de administración.
   - **Todos los dispositivos**: todos los dispositivos pueden ser administrados por los usuarios de los grupos de administración.
   - **Todos los usuarios y dispositivos**: todos los usuarios y todos los dispositivos pueden ser administrados por los usuarios de los grupos de administración.

5. Elija **Siguiente**.

6. En la página **Ámbito (etiquetas)** , seleccione las etiquetas que quiera agregar a este rol. Los usuarios de los grupos de administración tendrán acceso a los objetos de Intune que también tengan la misma etiqueta de ámbito. Puede asignar un máximo de 100 etiquetas de ámbito a un rol.

7. Elija **Siguiente** para ir a la página **Revisar y crear** y, después, seleccione **Crear**.

Asignación de etiquetas de ámbito a otros objetos

En el caso de los objetos que admiten etiquetas de ámbito, estas suelen aparecer en **Propiedades**. Por ejemplo, para asignar una etiqueta de ámbito a un perfil de configuración, siga estos pasos:

1. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Dispositivos** > **Perfiles de configuración** > elija un perfil.

2. Seleccione **Propiedades** > **Ámbito (etiquetas)** > **Editar** > **Seleccionar etiquetas de ámbito** > elija

las etiquetas que quiera agregar al perfil. Puede asignar un máximo de 100 etiquetas de ámbito a un objeto.

3. Elija **Seleccionar** > **Revisar + guardar**.

Detalles de las etiquetas de ámbito

Al trabajar con etiquetas de ámbito, recuerde estos detalles:

- Puede asignar etiquetas de ámbito a un tipo de objeto de Intune si el inquilino puede tener varias versiones de ese objeto (como asignaciones de roles o aplicaciones). Los objetos de Intune siguientes son excepciones a esta regla y actualmente no admiten etiquetas de ámbito:
  - Perfiles ESP de Windows
  - Identificadores de dispositivos corporativos
  - Dispositivos Autopilot
  - Ubicaciones de cumplimiento de dispositivos
  - Dispositivos Jamf
- Las aplicaciones de VPP y los libros electrónicos asociados al token de VPP heredan las etiquetas de ámbito asignadas al token de VPP asociado.
- Cuando un administrador crea un objeto en Intune, todas las etiquetas de ámbito asignadas a ese administrador se asignan automáticamente al nuevo objeto.
- El RBAC de Intune no se aplica a los roles de Azure Active Directory. Por lo tanto, los roles Administradores de servicios de Intune y Administradores globales tienen acceso de administrador completo a Intune independientemente de las etiquetas de ámbito que tengan.
- Si una asignación de roles no tiene etiqueta de ámbito, el administrador de TI puede ver todos los objetos en función de los permisos de los administradores de TI. Los administradores que no tienen etiquetas de ámbito esencialmente tienen todas las etiquetas de ámbito.
- Solo puede asignar una etiqueta de ámbito que tenga en las asignaciones de roles.
- Solo puede dirigirse a grupos que aparezcan en el Ámbito (grupos) de la asignación de roles.
- Si tiene una etiqueta de ámbito asignada a su rol, no puede eliminar todas las etiquetas de ámbito en un objeto de Intune. Se necesita al menos una etiqueta de ámbito.

Pasos siguientes

Obtenga información sobre cómo se comportan las etiquetas de ámbito cuando hay varias asignaciones de roles. Administre sus roles y perfiles.

Uso de filtros (vista previa) al asignar aplicaciones, directivas y perfiles en Microsoft Endpoint Manager

20/05/2021 • 7 minutes to read

Al crear una directiva, puede usar filtros para asignar una directiva basada en las reglas que cree. Por ejemplo, use filtros para dirigirse a dispositivos con una versión específica del sistema operativo o un fabricante específico, o bien para dirigirse solo a dispositivos personales o a dispositivos propiedad de la organización, etc.

Por ejemplo, puede usar filtros en los siguientes escenarios:

- Implementación de una directiva de restricción de dispositivos Windows 10 solo en los dispositivos corporativos del departamento de marketing, excluyendo los dispositivos personales.
- Implementación de una aplicación iOS/iPadOS solo en los dispositivos iPad del grupo Usuarios financieros.
- Implementación de una directiva de cumplimiento de teléfonos móviles Android para todos los usuarios de la empresa y exclusión de los dispositivos de la sala de reuniones Android que no admitan la configuración de la directiva de cumplimiento de teléfonos móviles.

Los filtros incluyen las siguientes características y ventajas:

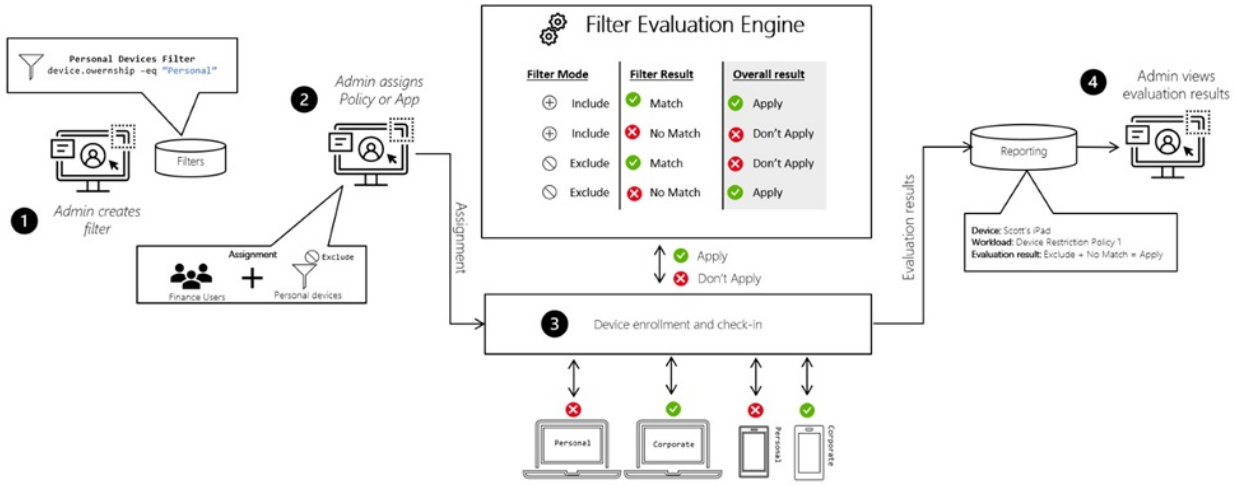
- Mejoran la flexibilidad y granularidad al asignar directivas y aplicaciones de Intune.
- Se usan al asignar aplicaciones, directivas y perfiles. Se dirigen dinámicamente a los dispositivos en función de las propiedades del dispositivo que especifique.
- Pueden incluir o excluir dispositivos de un grupo específico en función de los criterios especificados.
- Crean una consulta de las propiedades del dispositivo en función de la plataforma del dispositivo, incluidos Android, iOS/iPadOS, macOS y Windows 10.
- Se pueden usar y reutilizar en varios escenarios en el modo "Incluir" o "Excluir".

Esta característica se aplica a:

- Administrador de dispositivos Android
- Android Enterprise
- iOS/iPadOS
- macOS
- Windows 10 y versiones posteriores

En este artículo se describe la arquitectura de filtro y se muestra cómo crear, actualizar y eliminar un filtro.

Funcionamiento de los filtros



Antes de aplicar una directiva a un dispositivo, los filtros evalúan dinámicamente la aplicabilidad. A continuación, se proporciona una descripción general de la imagen anterior:

1. Cree un filtro reutilizable para cualquier plataforma en función de algunas propiedades del dispositivo. En el ejemplo, el filtro es para dispositivos personales.
2. Asigne una directiva o aplicación al grupo. En la asignación, agregue el filtro en el modo de incluir o excluir. Por ejemplo, "incluya" dispositivos personales o "excluya" dispositivos personales de la directiva.
3. El filtro se evalúa cuando el dispositivo se inscribe, se registra con el servicio de Intune o en cualquier otro momento en el que una directiva evalúa.
4. Verá los resultados del filtro en función de la evaluación. Por ejemplo, la aplicación o las directivas se aplican o no se aplican.

Requisitos previos

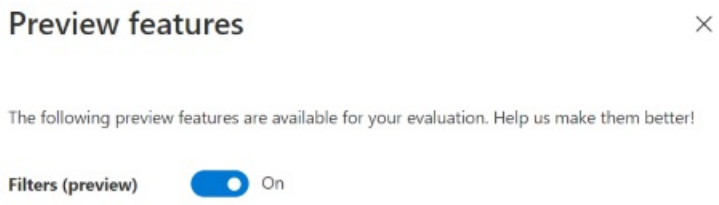
- Inicie sesión como un administrador de Intune. Para más información, vea Control de acceso basado en rol (RBAC) con Microsoft Intune.

Habilitación de filtros y adición de un filtro

Habilitación de la versión preliminar pública de filtros

Para usar filtros, debe habilitarlos en el inquilino de su organización.

1. Inicie sesión en el Centro de administración de Endpoint Manager.
2. Seleccione **Administración de inquilinos** > **Filtros (vista previa)** > **Pruebe la característica de filtros (versión preliminar)** .
3. Establezca **Filtros (vista previa)** en **Activado**:



TIP

- Las características de versión preliminar pública de Microsoft Endpoint Manager son totalmente compatibles con Microsoft. Para obtener más información, consulte Versión preliminar pública en Microsoft Intune.
- Para habilitar o deshabilitar filtros para el inquilino, la cuenta debe tener el permiso de administrador del servicio de Intune (también conocido como administrador de Intune).
- Puede deshabilitar la característica **Filtros (vista previa)** si la vuelve a establecer en **Desactivado**. Para desactivar esta característica, debe quitar las asignaciones de filtro y, a continuación, eliminar todos los filtros que ha creado.
- Microsoft quiere sus comentarios sobre esta característica. Para proporcionar comentarios, vaya a Tell us what you think about the Filters (preview) feature (Cuéntenos lo que piensa sobre la característica Filtros [vista previa]).

Crear un filtro

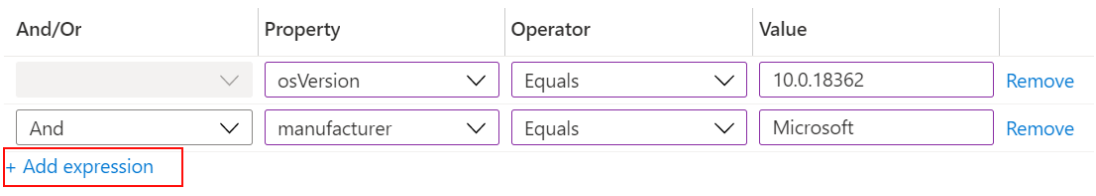
1. Inicie sesión en el Centro de administración de Endpoint Manager.
2. Seleccione **Administración de inquilinos** > **Filtros (vista previa)** > **Crear**.

   También puede crear filtros en **Dispositivos** > **Filtros (vista previa)** o en **Aplicaciones** > **Filtros (vista previa)** .
3. En **Básico**, escriba las propiedades siguientes:

   - **Nombre del filtro**: escriba un nombre descriptivo para el filtro. Asigne un nombre a los filtros para que pueda identificarlos de manera sencilla más adelante. Por ejemplo, un buen nombre de filtro es **filtro de versión del sistema operativo Windows**.
   - **Descripción**: escriba una descripción para el filtro. Esta configuración es opcional pero recomendada.
   - **Plataforma**: seleccione la plataforma. Las opciones son:
     - Administrador de dispositivos Android
     - Android Enterprise
     - iOS/iPadOS
     - macOS
     - Windows 10
4. Seleccione **Siguiente**.
5. En **Reglas**, hay dos maneras de crear una regla: usar el **generador de reglas** o la **sintaxis de regla**.

   Generador de reglas:

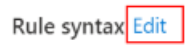
   - **And/Or**: después de agregar una expresión, puede añadirle contenido mediante las opciones `and` o `or`.
   - **Propiedad**: seleccione una propiedad para la regla, como la SKU del dispositivo o del sistema operativo.
   - **Operador**: seleccione el operador de la lista, como `equals` o `contains`.
   - **Valor**: escriba el valor en la expresión. Por ejemplo, escriba `10.0.18362` para la versión del sistema operativo o `Microsoft` para el fabricante.
   - **Agregar expresión**: después de agregar la propiedad, el operador y el valor, seleccione **Agregar expresión**:



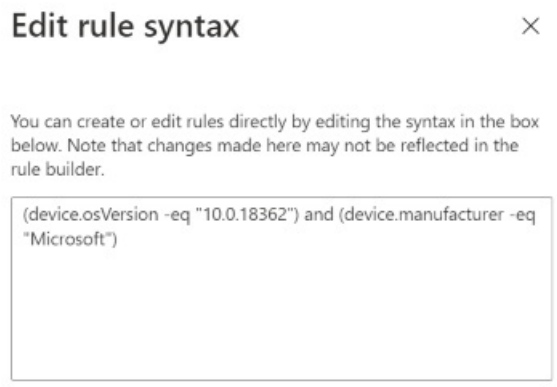
La expresión que creó se agrega automáticamente al editor de sintaxis de reglas.

Sintaxis de regla:

También puede escribir manualmente la expresión de regla y escribir sus propias reglas en el editor de sintaxis de reglas. En **Sintaxis de regla**, seleccione **Editar**:



Se abre el generador de expresiones. Escriba manualmente expresiones, como `(device.osVersion -eq "10.0.18362") and (device.manufacturer -eq "Microsoft")`:



Para obtener más información sobre cómo escribir sus propias expresiones, consulte Propiedades del dispositivo, operadores y edición de reglas al crear filtros.

Seleccione **Aceptar** para guardar la expresión.

> **TIP**
> - Al crear una regla, se valida para la sintaxis correcta y se muestran los errores.
> - Si escribe una sintaxis que no es compatible con el generador de reglas básico, el generador de reglas se deshabilita. Por ejemplo, el uso de paréntesis anidados deshabilita el generador de reglas básico.

6. Seleccione **Siguiente**.
7. En **Etiquetas de ámbito** (opcional), asigne una etiqueta para filtrar el perfil por grupos de TI específicos, como `US-NC IT Team` o `JohnGlenn_ITDepartment`. Para obtener más información sobre las etiquetas de ámbito, vea Usar control de acceso basado en rol (RBAC) y etiquetas de ámbito.

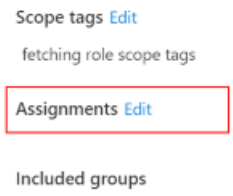
   Seleccione **Siguiente**.
8. En **Revisar y crear**, revise la configuración. Si selecciona **Crear**, se guardan los cambios. Se crea el filtro y está listo para usarse. El filtro también se muestra en la lista de filtros.

Uso de un filtro

Una vez creado el filtro, estará listo para usarse al asignar las aplicaciones o directivas.

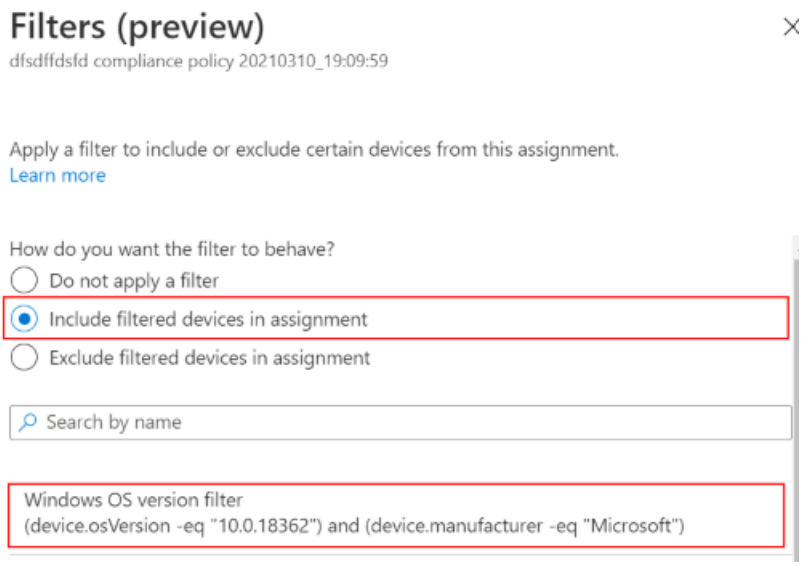
1. Inicie sesión en el Centro de administración de Endpoint Manager.
2. Vaya a las aplicaciones, las directivas de cumplimiento o los perfiles de configuración. Para obtener una lista de lo que se admite, consulte Cargas de trabajo admitidas al crear filtros. Seleccione una directiva existente o cree una nueva.

   Por ejemplo, seleccione **Dispositivos** > **Directivas de cumplimiento** y seleccione una directiva existente. Seleccione **Propiedades** > **Asignaciones** > **Editar**:



3. Asigne la directiva a un grupo de usuarios o a un grupo de dispositivos.
4. Seleccione **Editar filtro**. Puede elegir **incluir dispositivos filtrados** o **excluir dispositivos filtrados**. Se muestra una lista de filtros que coinciden con la plataforma de directivas.
5. Seleccione el filtro > **Seleccionar**.

   Por ejemplo, seleccione **Incluir los dispositivos filtrados en la asignación** y seleccione el filtro:



6. Para guardar los cambios, seleccione **Revisar y guardar** > **Guardar**.

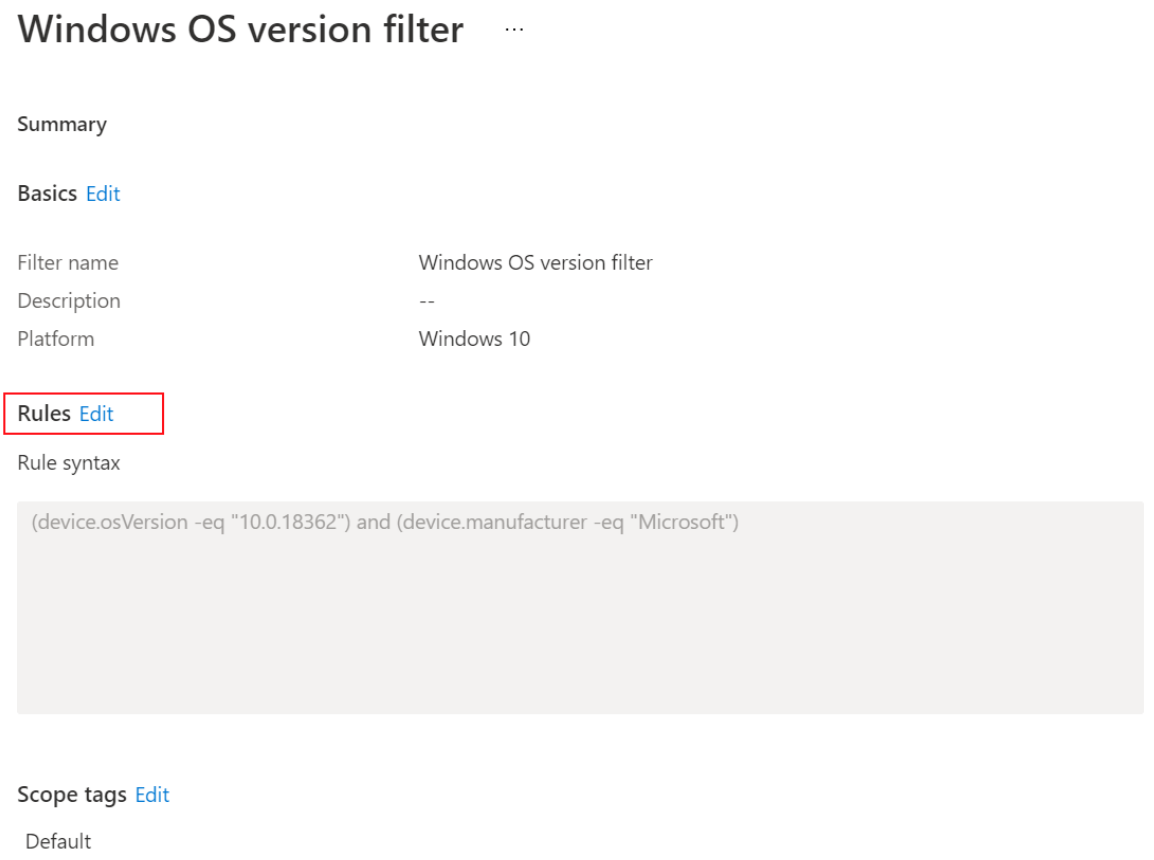
Cuando el dispositivo se registra con el servicio de Intune, se evalúan las propiedades definidas en el filtro y se determina si se debe aplicar la aplicación o la directiva.

Cambio de un filtro existente

Una vez creado un filtro, se podrá cambiar o actualizar.

1. Inicie sesión en el Centro de administración de Endpoint Manager.
2. Seleccione **Administración de inquilinos** > **Filtros (vista previa)** . Se muestra una lista de todos los filtros.

   También puede actualizar filtros en **Dispositivos** > **Filtros (vista previa)** o en **Aplicaciones** > **Filtros (vista previa)** .
3. Seleccione el filtro que quiera modificar. Seleccione **Reglas** > **Editar** y realice los cambios:



4. Para guardar los cambios, seleccione **Revisar y guardar** > **Guardar**.

Eliminación de un filtro

1. Inicie sesión en el Centro de administración de Endpoint Manager.
2. Seleccione **Administración de inquilinos** > **Filtros (vista previa)** . Se muestra una lista de todos los filtros.

   También puede eliminar filtros en **Dispositivos** > **Filtros (vista previa)** o en **Aplicaciones** > **Filtros (vista previa)** .
3. Junto al filtro, seleccione los puntos suspensivos (...) y, después, **Eliminar**:

Para eliminar un filtro, debe quitarlo de cualquier asignación de directiva. De lo contrario, al intentar eliminar el filtro, se producirá el siguiente error:

```
Unable to delete assignment filter – An assignment filter is associated with existing assignments. Delete all the assignments for the filter and try again.
```

Pasos siguientes

- Propiedades del dispositivo, operadores y edición de reglas al crear filtros
- Cargas de trabajo admitidas al crear filtros
- Informes de filtros y solución de problemas

Propiedades del dispositivo, operadores y edición de reglas al crear filtros en Microsoft Endpoint Manager

20/05/2021 • 6 minutes to read

Al crear una aplicación, una directiva de cumplimiento o un perfil de configuración, se asigna esa aplicación o directiva a grupos (usuarios o dispositivos). Al asignar la aplicación o la directiva, también se pueden usar filtros. Para obtener más información sobre esta característica, consulte Uso de filtros al asignar aplicaciones, directivas y perfiles.

Cuando se crea un filtro, se escriben las propiedades del dispositivo que se usarán en el filtro. Por ejemplo, en el filtro, escriba el fabricante del dispositivo para que la directiva solo se aplique a los dispositivos de Microsoft.

También está disponible la edición avanzada de reglas. Para crear expresiones, se pueden usar operadores comunes, como `and`, `contains` y `startsWith`. Estas expresiones se guardan y se usan en el filtro.

En este artículo se describen las distintas propiedades del dispositivo y los operadores que pueden usarse en los filtros y se proporcionan ejemplos.

Propiedades de dispositivo

- **Nombre del dispositivo**: cree una regla de filtro basada en la propiedad de nombre del dispositivo de Intune. Escriba un valor de cadena para el nombre completo del dispositivo (mediante los operadores `-eq`, `-ne`, `-in` y `-notIn`) o un valor parcial (mediante los operadores `-startswith`, `-contains` y `-notcontains`).

  Ejemplos:

  - `(device.deviceName -eq "Scott's Device")`
  - `(device.deviceName -in ["Scott's device", "Sara's device"])`
  - `(device.deviceName -startsWith "S")`

  Esta propiedad se aplica a:

  - Administrador de dispositivos Android
  - Android Enterprise
  - iOS/iPadOS
  - macOS
  - Windows 10 y versiones posteriores
- **Fabricante**: cree una regla de filtro basada en la propiedad de fabricante del dispositivo de Intune. Escriba el valor de cadena completo (mediante los operadores `-eq`, `-ne`, `-in` y `-notIn`) o un valor parcial (mediante los operadores `-startswith`, `-contains` y `-notcontains`).

  Ejemplos:

  - `(device.manufacturer -eq "Microsoft")`
  - `(device.manufacturer -startsWith "Micro")`

  Esta propiedad se aplica a:

  - Administrador de dispositivos Android

- Android Enterprise
- iOS/iPadOS
- macOS
- Windows 10 y versiones posteriores

- **Modelo**: cree una regla de filtro basada en la propiedad de modelo del dispositivo de Intune. Escriba el valor de cadena completo (mediante los operadores `-eq`, `-ne`, `-in` y `-notIn`) o un valor parcial (mediante los operadores `-startswith`, `-contains` y `-notcontains`).

  Ejemplos:

  - `(device.model -eq "Surface Book 3")`
  - `(device.model -in ["Surface Book 3", "Surface Book 2"])`
  - `(device.model -startsWith "Surface Book")`

  Esta propiedad se aplica a:

  - Administrador de dispositivos Android
  - Android Enterprise
  - iOS/iPadOS
  - macOS
  - Windows 10 y versiones posteriores
- **Categoría del dispositivo**: cree una regla de filtro basada en la propiedad de categoría del dispositivo de Intune. Escriba el valor de cadena completo (mediante los operadores `-eq`, `-ne`, `-in` y `-notIn`) o un valor parcial (mediante los operadores `-startswith`, `-contains` y `-notcontains`).

  Ejemplos:

  - `(device.deviceCategory -eq "Engineering devices")`
  - `(device.deviceCategory -contains ["Engineering devices", "EMEA devices"])`
  - `(device.model -startsWith "E")`

  Esta propiedad se aplica a:

  - Administrador de dispositivos Android
  - Android Enterprise
  - iOS/iPadOS
  - macOS
  - Windows 10 y versiones posteriores
- **Versión del sistema operativo**: cree una regla de filtro basada en la versión del sistema operativo (SO) del dispositivo de Intune. Escriba el valor de cadena completo (mediante los operadores `-eq`, `-ne`, `-in` y `-notIn`) o un valor parcial (mediante los operadores `-startswith`, `-contains` y `-notcontains`).

  Ejemplos:

  - `(device.osVersion -eq "14.2.1")`
  - `(device.osVersion -in ["10.15.3 (19D2064)","10.14.2 (18C54)"])`
  - `(device.osVersion -startsWith "10.0.18362")`

  Esta propiedad se aplica a:

  - Administrador de dispositivos Android
  - Android Enterprise
  - iOS/iPadOS
  - macOS
  - Windows 10 y versiones posteriores

- **IsRooted**: cree una regla de filtro basada en la propiedad de dispositivo con acceso "root" (Android) o con jailbreak (iOS/iPadOS). Seleccione `True`, `False` o valores desconocidos mediante los operadores `-eq` y `-ne`.

  Ejemplo:

  - `(device.isRooted -eq "True")`

  Esta propiedad se aplica a:

  - Administrador de dispositivos Android
  - Android Enterprise (solo perfil de trabajo)
  - iOS/iPadOS
- **Propiedad del dispositivo**: cree una regla de filtro basada en la propiedad del dispositivo en Intune. Seleccione `Personal`, `Corporate` o valores desconocidos mediante los operadores `-eq` y `-ne`.

  Ejemplo:

  - `(device.deviceOwnership -eq "Personal")`

  Esta propiedad se aplica a:

  - Administrador de dispositivos Android
  - Android Enterprise
  - iOS/iPadOS
  - macOS
  - Windows 10 y versiones posteriores
- **Nombre del perfil de inscripción**: cree una regla de filtro basada en el nombre del perfil de inscripción. Esta propiedad se aplica a un dispositivo cuando este se inscribe. Es un valor de cadena creado por el usuario y coincide con el Windows Autopilot, la inscripción automatizada de dispositivos (ADE) de Apple o el perfil de inscripción de Google aplicado al dispositivo. Para ver los nombres del perfil de inscripción, inicie sesión en el Centro de administración de Endpoint Manager y vaya a **Dispositivos** > **Inscribir dispositivos**.

  Escriba el valor de cadena completo (mediante los operadores `-eq`, `-ne`, `-in` y `-notIn`) o un valor parcial (mediante los operadores `-startswith`, `-contains` y `-notcontains`).

  Ejemplos:

  - `(device.enrollmentProfileName -eq "DEP iPhones")`
  - `(device.enrollmentProfileName -startsWith "AutoPilot Profile")`

  Esta propiedad se aplica a:

  - iOS/iPadOS
  - Windows 10 y versiones posteriores
- **SKU del sistema operativo**: cree una regla de filtro basada en la SKU del sistema operativo Windows 10 del dispositivo. Escriba el valor de cadena completo (mediante los operadores `-eq`, `-ne`, `-in` y `-notIn`) o un valor parcial (mediante los operadores `-startswith`, `-contains` y `-notcontains`).

  Ejemplos:

  - `(device.operatingSystemSKU -eq "Enterprise")`
  - `(device.operatingSystemSKU -in ["Enterprise", "EnterpriseS", "EnterpriseN", "EnterpriseEval"])`
  - `(device.operatingSystemSKU -startsWith "Enterprise")`

  Puede usar los siguientes valores admitidos para la propiedad **SKU del sistema operativo**. El Centro de administración de Endpoint Manager no muestra los nombres de SKU. Por lo tanto, asegúrese de usar

los valores admitidos en la tabla siguiente:

VALOR ADMITIDO	DEFINICIÓN DE SKU DEL SISTEMA OPERATIVO
Education	Windows 10 Education (SKU 121)
EducationN	Windows 10 Education (SKU 122)
Empresa	Windows 10 Enterprise (SKU 4)
EnterpriseEval	Windows 10 Enterprise Evaluation (SKU 72)
EnterpriseG	Windows 10 Enterprise G (SKU 171)
EnterpriseGN	Windows 10 Enterprise G N (SKU 172)
EnterpriseS	Windows 10 Enterprise LTSB (SKU 125)
EnterpriseSEval	Windows 10 Enterprise LTSB Evaluation (SKU 129)
EnterpriseSN	Windows 10 Enterprise LTSB N (SKU 162)
ServerRdsh	Windows 10 Enterprise Multi-session (SKU 175)
EnterpriseN	Windows 10 Enterprise N (SKU 27)
EnterpriseNEval	Windows 10 Enterprise N Evaluation (SKU 84)
Holographic	Windows 10 Holographic (SKU 136)
Principal	Windows 10 Home (SKU 101)
CoreCountrySpecific	Windows 10 Home China (SKU 99)
CoreN	Windows 10 Home N (SKU 98)
CoreSingleLanguage	Windows 10 Home Single Language (SKU 100)
IoTUAP	Windows 10 IoT Core (SKU 123)
IoTUAPCommercial	Windows 10 IoT Core Commercial (SKU 131)
IoTEnterprise	Windows 10 IoT Enterprise (SKU 188)
Profesional	Windows 10 Professional (SKU 48)
ProfessionalEducation	Windows 10 Professional Education (SKU 164)
ProfessionalEducationN	Windows 10 Professional Education N (SKU 165)
ProfessionalWorkstation	Windows 10 Professional for Workstation (SKU 161)
ProfessionalN	Windows 10 Professional for Workstation N (SKU 162)

VALOR ADMITIDO	DEFINICIÓN DE SKU DEL SISTEMA OPERATIVO
BusinessN	Windows 10 Professional N (SKU 49)
ProfessionalSingleLanguage	Windows 10 Professional Single Language (SKU 138)
PPIPro	Windows 10 TeamOS (SKU 119)

Esta propiedad se aplica a:

- Windows 10 y versiones posteriores

Edición avanzada de reglas

Al crear un filtro, puede crear manualmente reglas simples o complejas en el editor de sintaxis de reglas. También puede usar operadores comunes, como `or`, `contains`, etc. El formato es similar al de los grupos dinámicos de Azure AD: `([entity].[property name] [operation] [value])`.

Aspectos que debe saber

- Las propiedades, las operaciones y los valores no distinguen mayúsculas de minúsculas.
- Se admiten paréntesis y paréntesis anidados.
- Algunas opciones de sintaxis avanzadas, como paréntesis anidados, solo están disponibles en el editor de sintaxis de reglas. Si usa expresiones avanzadas en el editor de sintaxis de reglas, el generador de reglas se deshabilita.

  Para obtener más información sobre el editor de sintaxis de reglas y el generador de reglas, consulte Uso de filtros al asignar aplicaciones, directivas y perfiles.

Operadores admitidos

Puede usar los operadores siguientes en el editor de sintaxis de reglas:

- **Or**: se usa para todos los tipos de valor, especialmente al agrupar reglas simples.
  - **Valores permitidos**: `-or` | `or`
  - **Ejemplo**: `(device.manufacturer -eq "Samsung") or (device.model -contains "Galaxy Note")`
- **And**: se usa para todos los tipos de valor, especialmente al agrupar reglas simples.
  - **Valores permitidos**: `-and` | `and`
  - **Ejemplo**: `(device.manufacturer -eq "Samsung") and (device.model -contains "Galaxy Note")`
- **Equals**: se usa para todos los tipos de valor, incluidas reglas simples, cadenas, matrices, etc.
  - **Valores permitidos**: `-eq` | `eq`
  - **Ejemplo**: `(device.manufacturer -eq "Samsung") and (device.model -eq "Galaxy Note")`
- **NotEquals**: se usa para todos los tipos de valor, incluidas reglas simples, cadenas, matrices, etc.
  - **Valores permitidos**: `-ne` | `ne`
  - **Ejemplo**: `(device.manufacturer -ne "Samsung") or (device.model -ne "Galaxy Note")`
- **StartsWith**: se usa para tipos de valor de cadena.
  - **Valores permitidos**: `-startsWith` | `startsWith`
  - **Ejemplo**: `(device.manufacturer -startsWith "Sams")`
- **In**: se usa para tipos de valor de matriz, como `["1", "2"]`.

- **Valores permitidos**: `-in` | `in`
- **Ejemplo**: `(device.manufacturer -in ["Samsung","Lenovo","Microsoft"])`

- **NotIn**: se usa para tipos de valor de matriz, como `["1", "2"]`.
  - **Valores permitidos**: `-notIn` | `notIn`
  - **Ejemplo**: `(device.manufacturer -notIn ["Samsung","Lenovo","Microsoft"])`
- **Contains**: se usa para tipos de valor de cadena.
  - **Valores permitidos**: `-contains` | `contains`
  - **Ejemplo**: `(device.manufacturer -contains "Samsung")`
- **NotContains**: se usa para tipos de valor de cadena.
  - **Valores permitidos**: `-notContains` | `notContains`
  - **Ejemplo**: `(device.manufacturer -notContains "Samsung")`

Pasos siguientes

- Uso de filtros al asignar aplicaciones, directivas y perfiles
- Cargas de trabajo admitidas al crear filtros
- Informes de filtros y solución de problemas

Lista de plataformas, directivas y tipos de aplicaciones compatibles con los filtros en Microsoft Endpoint Manager

27/05/2021 • 6 minutes to read

Al crear una aplicación, una directiva de cumplimiento o un perfil de configuración, se asigna la directiva a grupos (usuarios o dispositivos). Al asignar la directiva, también puede usar filtros. Por ejemplo, puede asignar directivas a dispositivos Windows 10 que ejecutan una versión específica del sistema operativo. Para obtener más información, consulte Uso de filtros al asignar aplicaciones, directivas y perfiles.

Los filtros admiten algunas de las diferentes cargas de trabajo disponibles en Microsoft Intune. En este artículo se enumeran los tipos de aplicación, las directivas de cumplimiento y los perfiles de configuración de dispositivos que admiten filtros. También se enumeran las cargas de trabajo que no se admiten.

Antes de empezar

- En este artículo se presupone que está familiarizado con los filtros. Si no es así, puede obtener más información en Uso de filtros al asignar aplicaciones, directivas y perfiles.
- ✔: admite filtros.
- ✘: no admite filtros.
- N/D: no se aplica a la plataforma.

Tipos de aplicaciones

Puede usar filtros para algunas directivas comunes de aplicación en las siguientes plataformas. Para obtener una lista de lo que no se admite, consulte No compatible (en este artículo).

Administrador de dispositivos Android

TIPO DE APLICACIÓN	COMPATIBLE
Aplicación de la tienda	✔
Aplicaciones de Microsoft 365	N/D
Versión 77 de Microsoft Edge y versiones posteriores	N/D
Microsoft Defender para punto de conexión	N/D
Vínculo web	✘
Aplicaciones de línea de negocio	✔

Android Enterprise

TIPO DE APLICACIÓN	COMPATIBLE
Aplicación de la tienda	N/D

TIPO DE APLICACIÓN	COMPATIBLE
Aplicaciones de Microsoft 365	N/D
Versión 77 de Microsoft Edge y versiones posteriores	N/D
Microsoft Defender para punto de conexión	N/D
Vínculo web	N/D
Aplicaciones de línea de negocio	N/D
Aplicaciones del sistema de Android Enterprise	✔
Aplicación de Google Play Store administrado	✔
Vínculo web de Google Play administrado	✔
Aplicación de línea de negocio de Android administrada	✔

NOTE

Los filtros no se admiten en dispositivos de perfil de trabajo corporativo de Android Enterprise cuando se usan en asignaciones de aplicaciones "Disponibles". Si los usuarios tienen como destino una intención de aplicación "Disponible", la aplicación sigue mostrándose como disponible para su instalación desde Google Managed Play Store. Se omite cualquier filtrado de inclusión o exclusión.

iOS/iPadOS

TIPO DE APLICACIÓN	COMPATIBLE
Aplicación de la tienda	✔
Aplicaciones de Microsoft 365	N/D
Versión 77 de Microsoft Edge y versiones posteriores	N/D
Microsoft Defender para punto de conexión	N/D
Vínculo web	✘
Aplicaciones de línea de negocio	✔
Aplicación del programa de compras por volumen (VPP) de iOS/iPadOS	✔

macOS

TIPO DE APLICACIÓN	COMPATIBLE
Aplicación de la tienda	N/D

TIPO DE APLICACIÓN	COMPATIBLE
Aplicaciones de Microsoft 365	✔
Versión 77 de Microsoft Edge y versiones posteriores	✔
Microsoft Defender para punto de conexión	✔
Vínculo web	✖
Aplicaciones de línea de negocio	✔

Windows 10 y versiones posteriores

TIPO DE APLICACIÓN	COMPATIBLE
Aplicación de la tienda	✔
Aplicaciones de Microsoft 365	✔
Versión 77 de Microsoft Edge y versiones posteriores	✔
Microsoft Defender para punto de conexión	N/D
Vínculo web	✖
Aplicaciones de línea de negocio	✔
Aplicación Windows (Win32)	✔
Microsoft Store para Empresas	✔

Directivas de cumplimiento

Puede usar filtros para todas las directivas de cumplimiento en las siguientes plataformas:

- Administrador de dispositivos Android
- Android Enterprise
- iOS/iPadOS
- macOS
- Windows 10 y versiones posteriores

> **NOTE**
> Actualmente no se admite el uso de filtros con directivas de cumplimiento que requieran una señal de detección de amenazas móviles (MTD) o Microsoft Defender para punto de conexión (MDE). Por ejemplo, las siguientes directivas de cumplimiento requieren una señal:
>
> - Solicitar que el dispositivo tenga o esté por debajo de la puntuación de riesgo de la máquina
> - Requerir que el dispositivo tenga el nivel de amenaza del dispositivo

Perfiles de configuración de dispositivos y seguridad de puntos de

conexión

Puede usar filtros para algunas directivas comunes de configuración de dispositivos en las plataformas siguientes. Para obtener una lista de lo que no se admite, consulte No compatible (en este artículo).

> **NOTE**
>
> Algunos tipos de perfil solo están disponibles para plataformas específicas. Por ejemplo, el tipo de perfil **Características del dispositivo** incluye configuraciones que solo están disponibles para dispositivos iOS/iPadOS y macOS.
>
> Para obtener una lista de todos los perfiles de configuración de dispositivos y las plataformas a las que se aplican, consulte Aplicación de características y configuración en los dispositivos.

Administrador de dispositivos Android

TIPO DE PERFIL	COMPATIBLE
Personalizado	✔
Credencial derivada	N/D
Restricciones de dispositivos	✔
Restricciones de dispositivos (Windows 10 Team)	N/D
Características del dispositivo	N/D
Email	N/D
Correo electrónico (solo Samsung KNOX)	✔
Endpoint Protection	N/D
Perfil de MX (solo Zebra)	✔
Certificado PKCS	✔
Certificado PKCS importado	✔
Certificado SCEP	✔
Catálogo de configuración	N/D
Certificado de confianza	✔
VPN	✔
Wi-Fi	✔
Perfil de seguridad de puntos de conexión	
Protección de cuentas	N/D

TIPO DE PERFIL	COMPATIBLE
Antivirus	N/D
Reducción de la superficie expuesta a ataques	N/D
Cifrado de discos	N/D
Detección de puntos de conexión y respuesta	N/D
Firewall	N/D
Base de referencia de seguridad	N/D

Android Enterprise

TIPO DE PERFIL	COMPATIBLE
Personalizado	✔
Credencial derivada	✔
Restricciones de dispositivos	✔
Restricciones de dispositivos (Windows 10 Team)	N/D
Características del dispositivo	N/D
Correo electrónico	✔
Endpoint Protection	N/D
OEMConfig	✘
Certificado PKCS	✔
Certificado PKCS importado	✔
Certificado SCEP	✔
Catálogo de configuración	N/D
Certificado de confianza	✔
VPN	✔
Wi-Fi	✔
Perfil de seguridad de puntos de conexión	
Protección de cuentas	N/D

TIPO DE PERFIL	COMPATIBLE
Antivirus	N/D
Reducción de la superficie expuesta a ataques	N/D
Cifrado de discos	N/D
Detección de puntos de conexión y respuesta	N/D
Firewall	N/D
Base de referencia de seguridad	N/D

iOS/iPadOS

TIPO DE PERFIL	COMPATIBLE
Personalizado	✔
Credencial derivada	✔
Restricciones de dispositivos	✔
Restricciones de dispositivos (Windows 10 Team)	N/D
Características del dispositivo	✔
Correo electrónico	✔
Endpoint Protection	N/D
Certificado PKCS	✔
Certificado PKCS importado	✔
Certificado SCEP	✔
Catálogo de configuración	N/D
Certificado de confianza	✔
VPN	✔
Wi-Fi	✔
Perfil de seguridad de puntos de conexión	
Protección de cuentas	N/D
Antivirus	N/D

TIPO DE PERFIL	COMPATIBLE
Reducción de la superficie expuesta a ataques	N/D
Cifrado de discos	N/D
Detección de puntos de conexión y respuesta	N/D
Firewall	N/D
Base de referencia de seguridad	N/D

macOS

TIPO DE PERFIL	COMPATIBLE
Personalizado	✔
Credencial derivada	N/D
Restricciones de dispositivos	✔
Restricciones de dispositivos (Windows 10 Team)	N/D
Características del dispositivo	✔
Email	N/D
Endpoint Protection	✔
Extensiones	✔
Certificado PKCS	✔
Certificado PKCS importado	✔
Archivo de preferencia	✔
Certificado SCEP	✔
Catálogo de configuración	✘
Certificado de confianza	✔
VPN	✔
Wi-Fi	✔
Red cableada	✔
Perfil de seguridad de puntos de conexión	

TIPO DE PERFIL	COMPATIBLE
Protección de cuentas	N/D
Antivirus	✕
Reducción de la superficie expuesta a ataques	N/D
Cifrado de discos	✕
Detección de puntos de conexión y respuesta	N/D
Firewall	✕
Base de referencia de seguridad	N/D

Windows 10 y versiones posteriores

TIPO DE PERFIL	COMPATIBLE
Plantillas administrativas	✔
Personalizado	✔
Credencial derivada	N/D
Optimización de entrega	✔
Restricciones de dispositivos	✔
Restricciones de dispositivos (Windows 10 Team)	✔
Características del dispositivo	N/D
Interfaz de configuración de firmware de dispositivos	✕
Unión al dominio	✔
Actualización de edición y conmutador de modo S	✔
Correo electrónico	✔
Endpoint Protection	✔
Protección de identidad	✔
Pantalla completa	✔
Microsoft Defender para punto de conexión (Windows 10 Desktop)	✔
Límite de red	✔

TIPO DE PERFIL	COMPATIBLE
Certificado PKCS	✔
Certificado PKCS importado	✔
Certificado SCEP	✔
Evaluación segura (Education)	✔
Catálogo de configuración	✕
Dispositivos multiusuario compartidos	✔
Certificado de confianza	✔
VPN	✔
Wi-Fi	✔
Seguimiento de estado de Windows	✔
Perfil de seguridad de puntos de conexión	
Protección de cuentas	✕
Antivirus	✕
Reducción de la superficie expuesta a ataques	✕
Cifrado de discos	✕
Detección de puntos de conexión y respuesta	✕
Firewall	✕
Base de referencia de seguridad	✕

No compatible

Las siguientes características no admiten el uso de filtros:

- Catálogo de ajustes de perfiles de configuración
- Directivas de configuración de aplicaciones para Android e iOS/iPadOS
- Directivas de protección de aplicaciones para Android, iOS/iPadOS y Windows 10
- Directivas de personalización de experiencias de usuario final
- Restricciones de inscripción
- Perfiles de aprovisionamiento de aplicaciones de iOS/iPadOS
- Administración de dispositivos de socio
- Directivas para las aplicaciones de Office
- Conjuntos de directivas

- Scripts de PowerShell para Windows 10
- Directivas complementarias del modo S para Windows 10
- Scripts de shell para macOS
- Términos y condiciones
- Directivas de actualización para iOS/iPadOS
- Actualizaciones de características de Windows 10
- Anillos de actualización de Windows 10

Pasos siguientes

- Uso de filtros al asignar aplicaciones, directivas y perfiles
- Propiedades del dispositivo admitidas al crear filtros

Informes de filtros y solución de problemas en Microsoft Endpoint Manager

27/05/2021 • 8 minutes to read

Al crear una aplicación, una directiva de cumplimiento o un perfil de configuración, se asigna la directiva a grupos (usuarios o dispositivos). Al asignar la aplicación o la directiva, también se pueden usar filtros. Por ejemplo, puede asignar directivas a dispositivos Windows 10 que ejecutan una versión específica del sistema operativo. Para obtener más información, consulte Uso de filtros al asignar aplicaciones, directivas y perfiles.

Los dispositivos se evalúan con estos filtros para cumplir las reglas que configure. Los resultados de las evaluaciones de filtro se registran y se notifican en el Centro de administración de Microsoft Endpoint Manager.

Use este artículo para obtener más información sobre las características de informes y para ayudar a solucionar problemas de filtros y conflictos.

IMPORTANT

- A partir de la hora de evaluación, los resultados de la evaluación de filtros pueden tardar hasta 30 minutos en mostrarse en el Centro de administración de Endpoint Manager.
- Esta característica está en versión preliminar pública. El punto de entrada a los resultados de la evaluación de filtros cambiará y se integrará más en los informes de directivas y aplicaciones.

Informes

El Centro de administración de Endpoint Manager contiene datos de informes por dispositivo y por aplicación. Use esta información para solucionar problemas de evaluación de filtros y determinar por qué se aplicó o no se aplicó una directiva.

Puede usar los informes siguientes para obtener más información sobre los filtros:

- Informe de evaluación de filtros para dispositivos (en este artículo)
- Informe de evaluación de filtros de aplicaciones (en este artículo)

Informe de evaluación de filtros para dispositivos

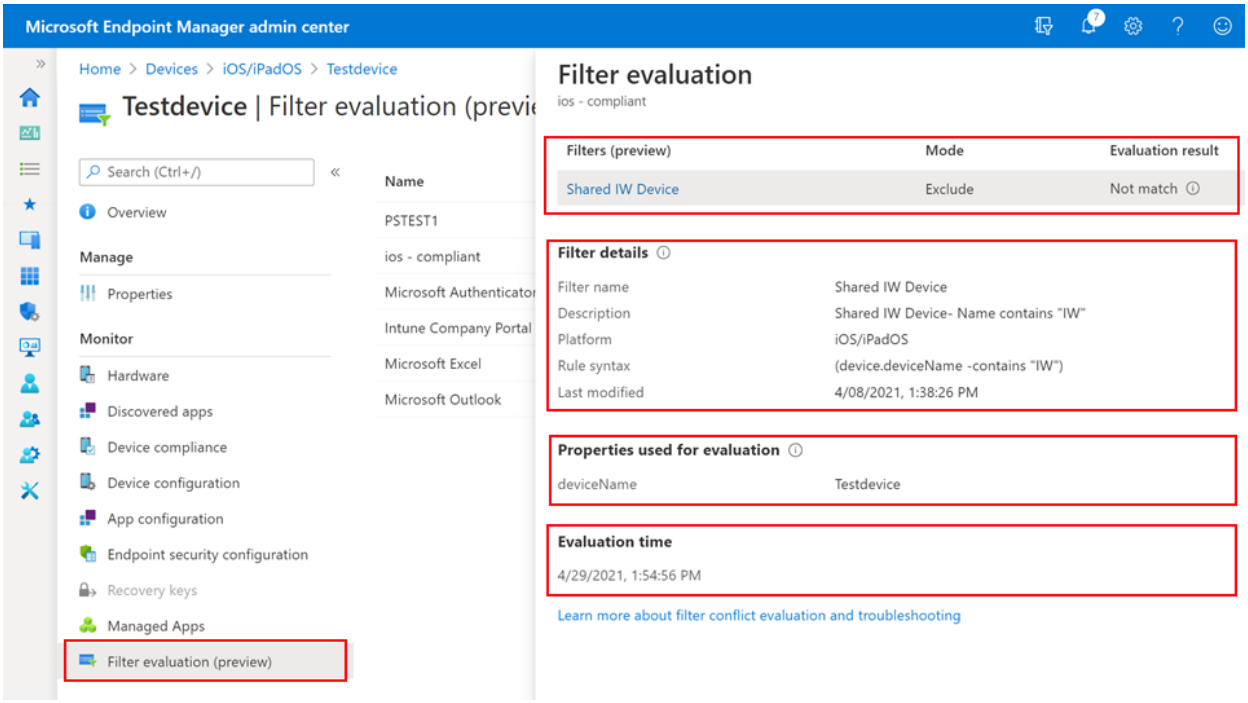
Este informe muestra todas las aplicaciones o directivas en las que se ha aplicado un filtro. Para cada aplicación o directiva evaluada, puede ver los filtros aplicados y obtener información más detallada.

1. Inicie sesión en el Centro de administración de Endpoint Manager.
2. Seleccione **Dispositivos** > **Todos los dispositivos** > seleccione un dispositivo > **Evaluación de filtros (vista previa)** . Se muestra la siguiente información:
   - Filtros que se evaluaron.
   - Fecha y hora en que se produjo la evaluación.
   - Resultados de la evaluación: **Coincidencia** o **Sin coincidencias**.
   - Si el filtro usaba el modo Incluir o Excluir.
   - Nombre, descripción y reglas del filtro.
   - Propiedades que se evaluaron, como `deviceName`.

   La sección **Información del filtro** se rellena con el nombre, la descripción y las reglas del filtro configurados actualmente. La información no se rellena a partir de los datos de registro. El nombre, la

sintaxis y cualquier otro metadato del filtro pueden haber cambiado desde la hora de la última evaluación. Al solucionar problemas, asegúrese de ver las marcas de tiempo **Hora de evaluación** y **Última modificación**.

En el ejemplo siguiente, puede ver esta información para **TestDevice**:

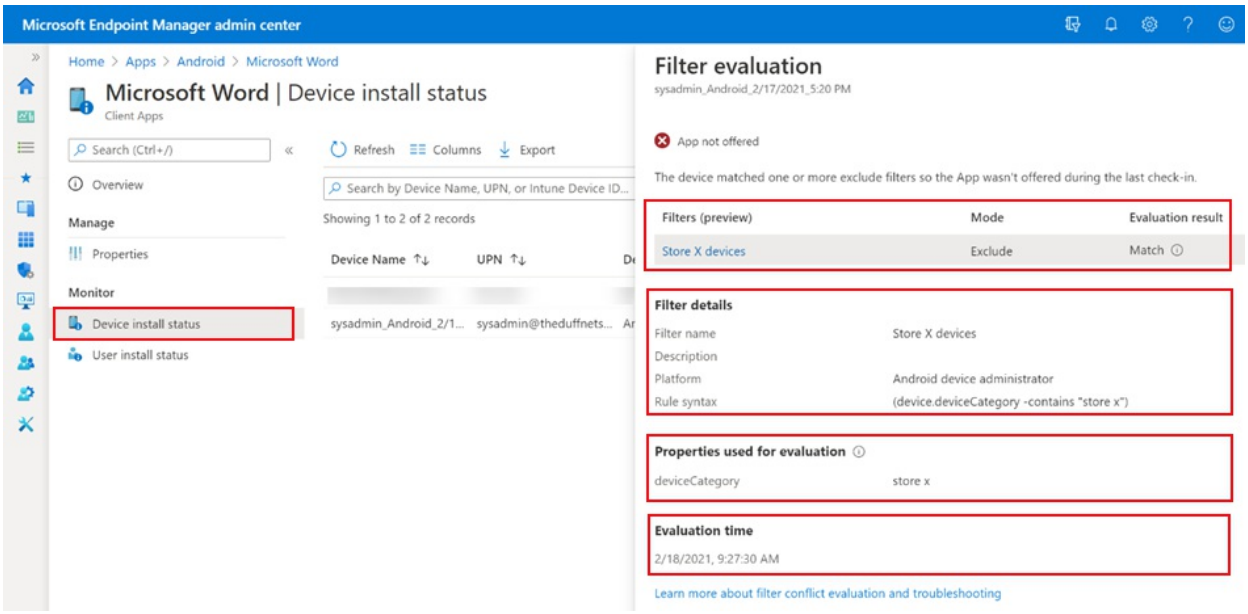


Informe de evaluación de filtros de aplicaciones

Este informe muestra información de filtro para cada dispositivo que se evaluó en una asignación de aplicación. Para cada dispositivo, puede ver la aplicabilidad general del dispositivo para una aplicación y obtener información más detallada sobre la evaluación del filtros.

1. Inicie sesión en el Centro de administración de Endpoint Manager.
2. Seleccione **Aplicaciones** > **Todas las aplicaciones** > seleccione una aplicación > **Estado de instalación del dispositivo**.
3. Seleccione **Filtro** columna > **Filtros evaluados**. Se muestra la siguiente información:
   - Filtros que se evaluaron.
   - Fecha y hora en que se produjo la evaluación.
   - Resultados de la evaluación: **Coincidencia** o **Sin coincidencias** y **App assignment applied** (Asignación de aplicaciones aplicada) o **App assignment not applied** (Asignación de aplicaciones no aplicada).
   - Si el filtro usaba el modo Incluir o Excluir.
   - Nombre, descripción y reglas del filtro.
   - Propiedades que se evaluaron, como `deviceCategory`.

En el ejemplo siguiente, puede ver esta información para la aplicación de la tienda **Microsoft Word**:



Incluir frente a excluir

Al crear un filtro, optará por incluir o excluir dispositivos en función de algunas propiedades, como `device.model -equals “Surface pro”` o `device.model -notEquals “Surface pro”`. Puede ser difícil comprender los resultados de la evaluación, especialmente al incluir o excluir dispositivos.

Use la tabla siguiente para ayudar a comprender cuándo se incluyen o excluyen dispositivos:

MODO DE FILTRO	RESULTADO DE FILTRO	RESULTADO GLOBAL
Incluir	Match	Aplicación de la asignación de directivas o aplicaciones
Incluir	Not Match	No aplicación de la asignación de directivas o aplicaciones
Exclude	Match	No aplicación de la asignación de directivas o aplicaciones
Exclude	Not Match	Aplicación de la asignación de directivas o aplicaciones

Aspectos que debe saber

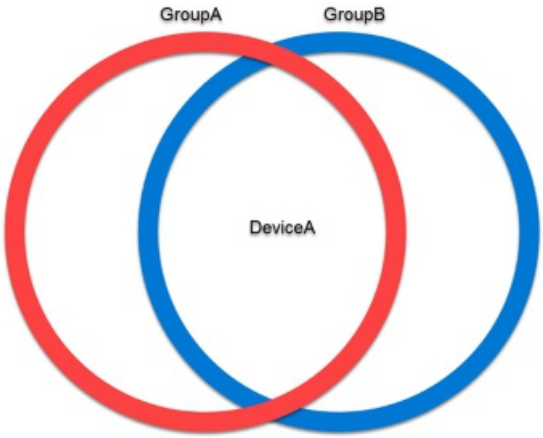
- Un resultado de filtro **Sin evaluar** puede mostrarse cuando una directiva tiene una asignación en conflicto en el dispositivo. Para obtener más información, consulte Resolución de conflictos de filtros y asignaciones (en este artículo).
- Los filtros se evalúan durante la inscripción y el registro del dispositivo. La evaluación también se puede ejecutar en otras ocasiones, como en una comprobación de cumplimiento.
- Los resultados de la evaluación de filtros más recientes se almacenan durante 30 días. Si los registros han expirado, es posible que vea el siguiente mensaje: **We were not able to retrieve any filter evaluation results** (No hemos podido recuperar ningún resultado de evaluación de filtros).

Resolución de conflictos de filtros y de asignación

Al asignar una directiva a un grupo (usuarios o dispositivos), es posible superponer asignaciones. No se recomienda, ya que la superposición puede provocar conflictos.

Intune ayuda a evitar conflictos. Impide que cree varias asignaciones en el mismo grupo de Azure AD. No se recomienda asignar aplicaciones o directivas al mismo usuario o dispositivo de destino con más de una intención. Por ejemplo, al implementar una aplicación, no puede seleccionar un grupo para una asignación **Disponible** y, a continuación, el mismo grupo para una asignación **Requerido**.

Puede producirse una superposición cuando un usuario o dispositivo está en varios grupos de destino. No se recomiendan asignaciones en conflicto. Para obtener más información, consulte conflictos entre las intenciones de aplicación.



Cuando se usan filtros, la resolución de conflictos se gestiona mediante los métodos siguientes:

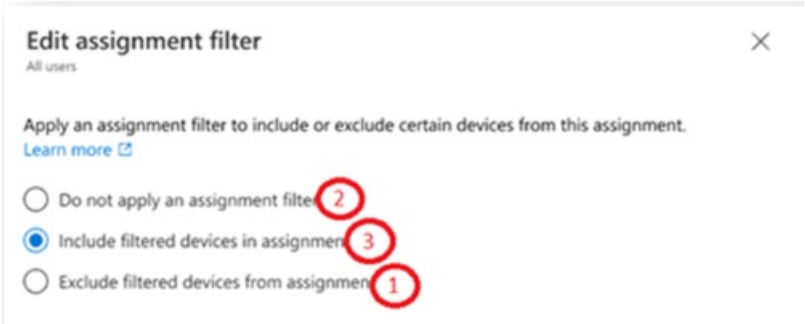
- Modo de filtro (en este artículo)
- Uso de la lógica "OR" cuando los modos de filtro son los mismos (en este artículo)
- Intención de aplicación (en este artículo)

Modo de filtro

Cuando hay un dispositivo con asignaciones en conflicto para la misma directiva, se aplica la siguiente prioridad:

1. Se aplica el modo **Excluir**. **Excluir** gana a **Sin filtro** y al modo **Incluir**.
2. Se aplica el modo **Sin filtro**. **Sin filtro** gana al modo **Incluir**.
3. Se aplica el modo **Incluir**.

Al asignar la aplicación o la directiva, elegirá aplicar un filtro:



Por ejemplo:

- PolicyA se asigna a tres grupos de dispositivos: GroupA, GroupB y GroupC.
- La asignación de GroupA usa FilterA. FilterA usa el modo Incluir.
- La asignación de GroupB usa FilterB. FilterB usa el modo Excluir.
- La asignación de GroupC no usa ningún filtro.
- DeviceA es miembro de los tres grupos: GroupA, GroupB y GroupC.

En este escenario, la asignación de exclusión gana debido a la prioridad del modo de filtro. DeviceA evalúa a

FilterB. Si DeviceA coincide con las reglas, se excluye de PolicyA. Si DeviceA no coincide con FilterB, se aplica PolicyA. DeviceA no hace más evaluaciones en las asignaciones y los filtros de GroupB y GroupC.

Uso de la lógica "OR" cuando los modos de filtro son los mismos

Si se aplican varios filtros que usan el mismo modo, como Incluir, se usa la lógica **OR**. El dispositivo solo debe coincidir con las reglas de uno de los filtros para incluirse (o excluirse) de la asignación de directiva.

Por ejemplo:

- PolicyA se asigna a dos grupos: GroupA y GroupB.
- La asignación de GroupA usa FilterA. FilterA usa el modo Incluir.
- La asignación de GroupB usa FilterB. FilterB usa el modo Incluir.
- DeviceA es miembro de ambos grupos: GroupA y GroupB.

En este escenario, ambos filtros usan el mismo modo. Por lo tanto, los filtros resuelven el conflicto con la lógica **OR**. DeviceA evalúa a FilterA y FilterB. Si DeviceA coincide con las reglas de cualquiera de los filtros, DeviceA recibe a PolicyA. Si DeviceA no coincide con ninguno de los filtros, no se aplica PolicyA.

Intención de aplicación

Las aplicaciones usan la resolución de conflictos basada en la "intención". La intención se evalúa antes de evaluar los filtros. Por ejemplo, las aplicaciones evalúan si un dispositivo tiene como destino la intención de asignación **Disponible**, **Requerido** o **Desinstalar**. A continuación, la intención ganadora se pasa al motor de filtrado para determinar la aplicabilidad.

Por ejemplo:

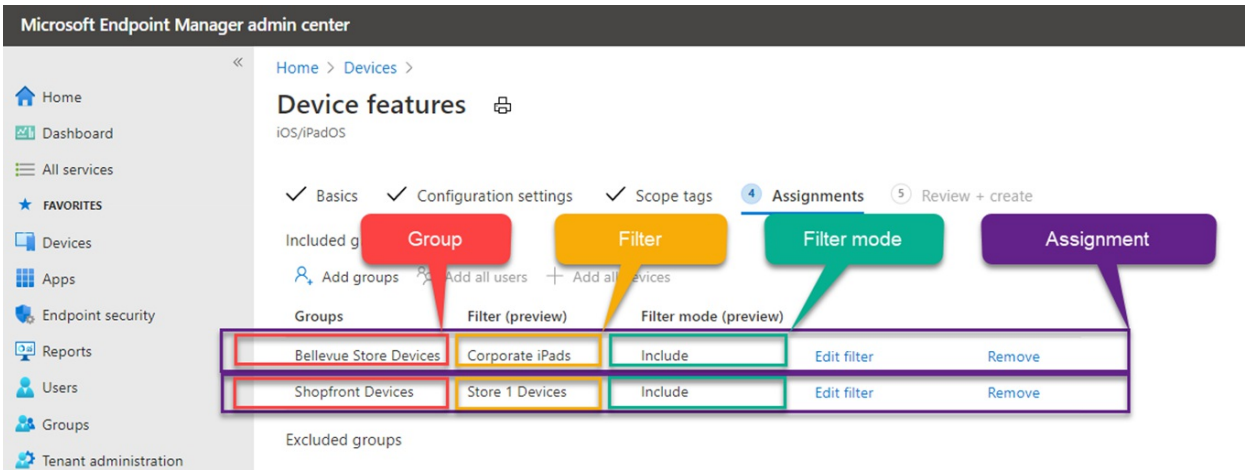
- AppA se asigna a dos grupos: GroupA y GroupB.
- La asignación de GroupA usa la intención **Requerido**. La asignación de GroupA usa FilterA, que a su vez usa el modo Incluir.
- La asignación de GroupB usa la intención **Desinstalar**. La asignación de GroupB usa FilterB, que a su vez usa el modo Incluir.
- DeviceA es miembro de ambos grupos: GroupA y GroupB.

En este escenario, la intención de aplicación que gana es **Requerido**. Para obtener más información, consulte conflictos entre las intenciones de aplicación. Por lo tanto, DeviceA solo debe evaluar a FilterA. Si DeviceA coincide con las reglas de FilterA, DeviceA recibe a AppA como una aplicación necesaria.

Las aplicaciones usan un comportamiento especial al resolver conflictos entre las asignaciones **Requerido** y **Disponible**. Si un usuario o dispositivo tiene como destino las asignaciones **Disponible** y **Requerido**, recibe una intención combinada denominada **Requerido y disponible**. El dispositivo debe evaluar los filtros usados en ambas asignaciones. Al evaluar ambos filtros, el dispositivo implementa la misma resolución de conflictos: Modo de filtro y Lógica "OR" cuando los modos de filtro son los mismos.

Matriz de resolución de conflictos

En el ejemplo siguiente, hay un conflicto entre las asignaciones porque el mismo usuario o dispositivo está en ambas asignaciones:



En la siguiente matriz se explica el impacto, en función del escenario de conflicto:

				Assignment 2		
				Group G2		
				Filter F2		None
			Filter mode	Include	Exclude	None
Assignment 1	Group G1	Filter F1	Include	Device in G1 must match F1 to have policy applied, otherwise device is excluded. Device in G2 must match F2 to have policy applied, otherwise device is excluded. Device in both G1 and G2 must match either F1 OR F2 to have policy applied, otherwise device is excluded.	Device in G1 must match F1 to be included in policy, otherwise device is excluded. Device in G2 must match F2 to be excluded from policy, otherwise policy is applied. Device in both G1 and G2 will only process F2 (Exclude). If match F2 device is excluded, If no-match, policy is applied.	Device in G1 must match F1 to have policy applied, otherwise device is excluded. Device in G2 has policy applied. Device in both G1 and G2 will have policy applied.
			Exclude	Device in G1 must match F1 to be excluded from policy, otherwise policy is applied. Device in G2 must match F2 to be included in policy, otherwise device is excluded. Device in both G1 and G2 will only process F1 (Exclude). If match F1 device is excluded, If no-match, policy is applied.	Device in G1 must match F1 to be excluded from policy, otherwise policy is applied. Device in G2 must match F2 to be excluded from policy, otherwise policy is applied. Device in both G1 and G2 must match either F1 OR F2 to be excluded from policy, otherwise the policy is applied. (Note: match any filter to be excluded)	Device in G1 must match F1 to be excluded from policy, otherwise policy is applied. Device in G2 has policy applied. Device in both G1 and G2 must match F1 (Exclude) to be excluded from policy, otherwise policy is applied.
		None	None	Device in G1 has policy applied Device in G2 must match F2 to have policy applied, otherwise device is excluded. Device in both G1 and G2 will have policy applied.	Device in G1 has policy applied. Device in G2 must match F2 to be excluded from policy, otherwise policy is applied. (Exclude wins). Device in both G1 and G2 must match F2 (Exclude) to be excluded from policy, otherwise the policy is applied.	Device in G1 has policy applied. Device in G2 has policy applied. Device in both G1 and G2 has policy applied.

Pasos siguientes

- Uso de filtros al asignar aplicaciones, directivas y perfiles
- Propiedades del dispositivo admitidas al crear filtros
- Cargas de trabajo admitidas al crear filtros

Uso de conjuntos de directivas para agrupar colecciones de objetos de administración

14/05/2021 • 6 minutes to read

Los conjuntos de directivas permiten crear una agrupación de referencias a entidades de administración ya existentes que se deben identificar, establecer como destino y supervisar como una sola unidad conceptual. Un conjunto de directivas es una colección asignable de aplicaciones, directivas y otros objetos de administración que se han creado. La creación de un conjunto de directivas permite seleccionar muchos objetos diferentes a la vez y asignarlos desde un único lugar. A medida que la organización va cambiando, se puede regresar a un conjunto de directivas para agregarle o quitarle objetos y asignaciones. Un conjunto de directivas puede servir para asociar y asignar objetos existentes (como aplicaciones, directivas y VPN) a un único paquete.

IMPORTANT

Para obtener una lista de los problemas conocidos relativos a los conjuntos de directivas, vea Problemas conocidos de los conjuntos de directivas.

Los conjuntos de directivas no reemplazan los conceptos ni los objetos existentes. Puede seguir asignando objetos individuales y, asimismo, hacer referencia a objetos individuales como parte de un conjunto de directivas. Por lo tanto, cualquier cambio que se realice en esos objetos individuales se verá reflejado en el conjunto de directivas.

Los conjuntos de directivas se pueden usar para lo siguiente:

- Agrupar objetos que se deben asignar juntos
- Asignar los requisitos mínimos de configuración de la organización en todos los dispositivos administrados
- Asignar aplicaciones relevantes o de uso frecuente a todos los usuarios

Se pueden incluir los siguientes objetos de administración en un conjunto de directivas:

- Aplicaciones
- Directivas de configuración de aplicaciones
- Directivas de protección de aplicaciones
- Perfiles de configuración de dispositivos
- Directivas de cumplimiento de dispositivos
- Restricciones de tipo de dispositivo
- Perfiles de Windows Autopilot Deployment
- Página de estado de inscripción

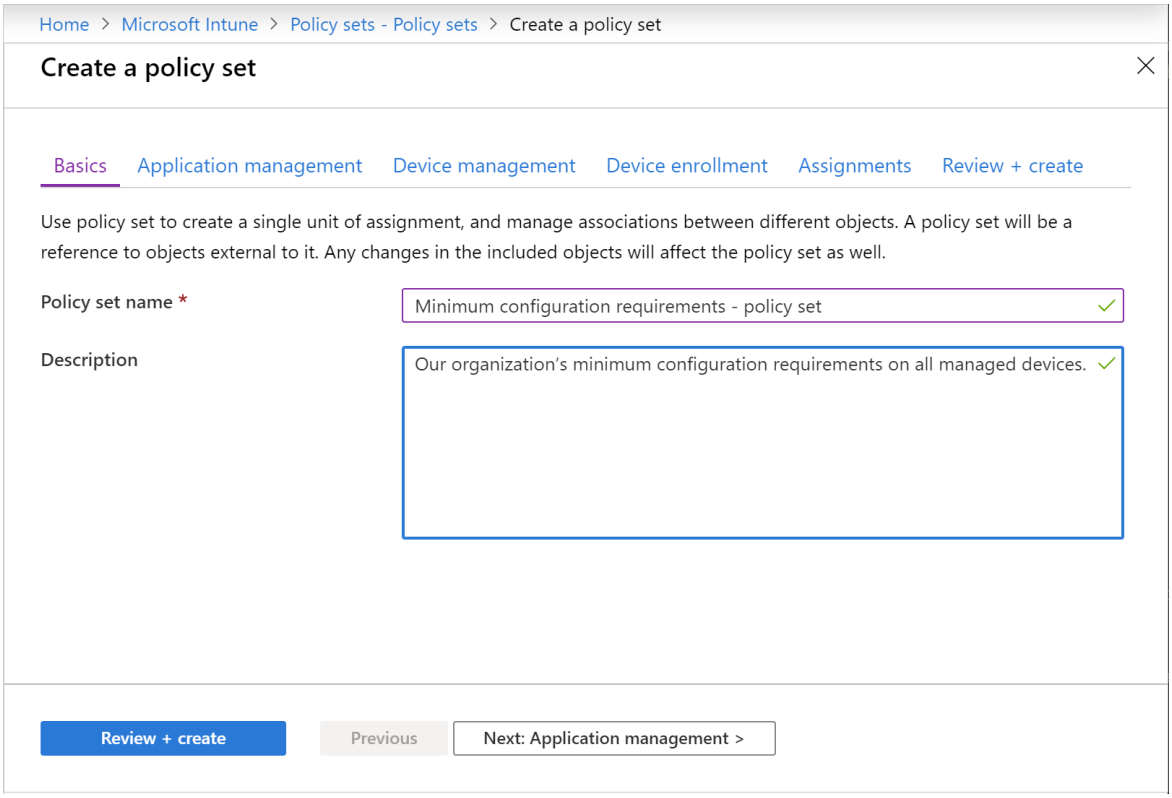
Cuando se crea un conjunto de directivas, se crea una única unidad de asignación y se administran las asociaciones entre los distintos objetos. Un conjunto de directivas será una referencia a los objetos que son externos a él. Cualquier cambio que se realice en los objetos incluidos también afectará al conjunto de directivas. Después de crear un conjunto de directivas, puede ver y editar repetidamente sus objetos y asignaciones.

NOTE

Los conjuntos de directivas admiten configuraciones de Windows, Android, macOS e iOS/iPadOS, y se pueden asignar entre plataformas.

Cómo crear un conjunto de directivas

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione **Dispositivos** > **Conjuntos de directivas** > **Conjuntos de directivas** > **Crear**.
3. En la página **Datos básicos**, agregue los siguientes valores:
   - **Nombre del conjunto de directivas**: indique un nombre para este conjunto de directivas.
   - **Descripción**: opcionalmente, especifique una descripción del conjunto de directivas.



4. Haga clic en **Siguiente: Administración de aplicaciones**.
   En la página **Administración de aplicaciones** puede decidir si quiere agregar aplicaciones, directivas de configuración de aplicaciones y directivas de protección de aplicaciones al conjunto de directivas. Para más información sobre cómo administrar aplicaciones, vea ¿Qué es la administración de aplicaciones de Microsoft Intune?
5. Haga clic en **Siguiente: Administración de dispositivos**.
   En la página **Administración de dispositivos** puede agregar objetos de administración de dispositivos al conjunto de directivas, como perfiles de configuración de dispositivos y directivas de cumplimiento de dispositivos. Asegúrese de incluir todos los objetos asociados, como otras directivas, certificados y perfiles de línea de base de seguridad.
6. Haga clic en **Siguiente: Inscripción de dispositivos**.
   En la página **Inscripción de dispositivos** puede agregar objetos de inscripción de dispositivos al conjunto de directivas, como restricciones de tipo de dispositivo, perfiles de Windows Autopilot Deployment y perfiles de página de estado de la inscripción.
7. Haga clic en **Siguiente: Asignaciones**.
   En la página **Asignaciones** puede asignar el conjunto de directivas a usuarios y dispositivos. Es importante saber que un conjunto de directivas se puede asignar a un dispositivo, independientemente de si dicho dispositivo está administrado o no por Intune.
8. Haga clic en **Siguiente: Revisar + crear** para revisar los valores especificados en el perfil.
9. Cuando haya terminado, haga clic en **Crear** para crear el conjunto de directivas en Intune.

Problemas conocidos de los conjuntos de directivas

Los conjuntos de directivas, novedad en la versión 1910, presentan los siguientes problemas conocidos.

- Al crear un conjunto de directivas, si un administrador con ámbito intenta crear un conjunto de directivas sin seleccionar ninguna etiqueta de ámbito, cuando llegue a la página **Revisar + crear**, se producirá un error de validación y se mostrará un error en la barra de estado. El administrador deberá cambiar a otra página en el proceso y, tras ello, regresar a la página **Revisar + crear**. Esto hará que la opción **Crear** se habilite.
- Actualmente, los conjuntos de directivas admiten los siguientes tipos de aplicaciones:
  - Aplicación de la Tienda iOS/iPadOS
  - Aplicación de línea de negocio iOS/iPadOS
  - Aplicación de línea de negocio iOS/iPadOS administrada
  - Aplicación de la tienda Android
  - Aplicación de línea de negocio de Android
  - Aplicación de línea de negocio de Android administrada
  - Aplicaciones de Microsoft 365 (Windows 10)
  - Vínculo web
  - Aplicación iOS/iPadOS integrada
  - Aplicación de Android integrada
- Una asignación de conjunto de directivas de tipo **Todos los usuarios** no se puede establecer en **Perfil de AutoPilot**.
- Los conjuntos de directivas presentan las siguientes restricciones de inscripción y problemas de página de estado de la inscripción:
  - Las restricciones y las páginas de estado de la inscripción no admiten asignaciones de grupos virtuales.
  - Las restricciones y las páginas de estado de la inscripción no admiten asignaciones de grupos de exclusión de manera estricta.
  - Las restricciones y las páginas de estado de la inscripción emplean una resolución de conflictos basada en prioridades. Las restricciones y las páginas de estado de la inscripción pueden no ser de aplicación en los mismos usuarios que el resto de cargas de un conjunto de directivas si esas restricciones y páginas de estado de la inscripción son el destino de una restricción y una página de estado de inscripción con una mayor prioridad.
  - Las restricciones y las páginas de estado de la inscripción predeterminadas no se pueden agregar a un conjunto de directivas.
- Los tipos de directivas MAM que admiten conjuntos de directivas son los siguientes:
  - Protección de aplicaciones administradas de destino de MDM de WIP (Windows) MAM
  - Protección de aplicaciones administradas de destino de iOS/iPadOS MAM
  - Protección de aplicaciones administradas de destino de Android MAM
  - Configuración de aplicaciones administradas de destino de iOS/iPadOS MAM
  - Configuración de aplicaciones administradas de destino de Android MAM
- Los tipos de directivas MAM que no admiten conjuntos de directivas son los siguientes:
  - Protección de aplicaciones administradas de destino de WIP (Windows) MAM
- MAM procesa las asignaciones de conjuntos de directivas como asignaciones directas en los siguientes tipos de directivas:
  - Protección de aplicaciones administradas de destino de iOS/iPadOS MAM

- Protección de aplicaciones administradas de destino de Android MAM
- Configuración de aplicaciones administradas de destino de iOS/iPadOS MAM
- Configuración de aplicaciones administradas de destino de Android MAM

  Si se agrega una directiva a un conjunto de directivas que está implementado en un grupo, dicho grupo se mostraría como directamente asignado en la carga de trabajo, y no "asignado mediante el conjunto de directivas". En consecuencia, MAM no procesa las eliminaciones de asignaciones de grupos procedentes de conjuntos de directivas.

- MAM no permite realizar implementaciones en grupos virtuales de tipo **Todos los usuarios** y **Todos los dispositivos** de ningún tipo de directiva.
- El perfil de configuración de dispositivo de tipo "Plantillas administrativas" no se puede seleccionar como parte de un conjunto de directivas.

Pasos siguientes

- Inscripción de dispositivos en Microsoft Intune

Uso de la página de estado del inquilino de Intune

14/05/2021 • 5 minutes to read

La página de estado del inquilino de Microsoft Intune es un centro donde puede ver detalles importantes y actuales sobre el inquilino. Entre estos detalles se incluyen la disponibilidad y el uso de la licencia, el estado del conector y comunicaciones importantes sobre el servicio Intune.

> **TIP**
> Un inquilino es una instancia de Azure Active Directory (Azure AD). La suscripción a Intune está hospedada en un inquilino de Azure AD. Para obtener más información, vea Configuración de un inquilino en la documentación de Azure AD.

Para ver el panel, inicie sesión en el centro de administración de Microsoft Endpoint Manager, vaya a **Administración de inquilinos** y, a continuación, seleccione **Estado del inquilino**.

La página se divide en tres pestañas:

Detalles del inquilino

Detalles del inquilino proporciona información de un vistazo sobre el inquilino. Vea detalles como el nombre y la ubicación del inquilino, la entidad de MDM y el número de versión del servicio de inquilinos. El número de versión del servicio es un vínculo que abre el artículo *Novedades en Intune* en Microsoft Docs. En *Novedades*, puede consultar información sobre las últimas características y actualizaciones del servicio Intune.

En esta pestaña, también encontrará información básica sobre las licencias disponibles y cuántas se han asignado a los usuarios. No se muestran las licencias de los dispositivos.

Estado del conector

Estado del conector es una ubicación única para revisar el estado de todos los conectores disponibles para Intune.

Los conectores son:

- **Conexiones que se configuran a servicios externos**. Por ejemplo, el servicio *Programa de Compras por Volumen de Apple* o el servicio *Windows Autopilot*. El estado de este tipo de conector se basa en la hora de la última sincronización correcta.
- **Certificados o credenciales necesarios para conectarse a un servicio externo no administrado**, como certificados de *Apple Push Notification Services* (APN). El estado de este tipo de conector se basa en la marca de tiempo de expiración del certificado o la credencial.

Al abrir la pestaña *Estado del conector*, los conectores incorrectos se muestran en la parte superior de la lista. Luego aparecen los conectores con advertencias y, después, la lista de conectores correctos. Los conectores que todavía no se han configurado aparecen al final como *No habilitado*.

Si hay más de un conector de cualquier tipo, el estado es un resumen de todos esos conectores. El estado mínimo de cualquier conector se usa como estado del grupo.

Estado del conector:

- **Incorrecto**:

    - El certificado o la credencial ha expirado
    - La última sincronización fue hace tres o más días
- **Advertencia**:
    - El certificado o la credencial expira en siete días
    - La última sincronización fue hace más de un día
- **Correcto**:
    - El certificado o la credencial no expira en los próximos siete días
    - La última sincronización fue hace menos de un día

Cuando se selecciona un conector de la lista, el portal presenta la página del portal que es relevante para ese conector. En la página Conectores, puede ver el estado de los conectores configurados previamente. También puede seleccionar opciones para agregar o crear un nuevo conector de ese tipo.

Por ejemplo, si selecciona el conector **Fecha de caducidad de VPP**, se abre la página **Tokens del programa de compras por volumen de iOS**. En esta página puede ver más detalles sobre ese conector, crear una nueva configuración o editar y corregir problemas con una existente.

Panel de Service Health

En el panel de Service Health puede ver detalles de los *incidentes en el servicio* que afectan a su inquilino y *noticias de Intune* que proporcionan información sobre actualizaciones y cambios planeados.

Service Health y centro de mensajes de Intune

Vea detalles de incidentes activos y avisos sin tener que ir al panel de Estado del servicio Microsoft 365 ni al Centro de mensajes, que se encuentran en el Centro de administración de Microsoft 365. Solo se muestran los incidentes que afectan a su inquilino.

Al seleccionar un incidente, los detalles de este se presentan directamente en la página Estado del inquilino. Para ver avisos e incidentes pasados, seleccione **See past Incidents/Advisories** (Ver incidentes y avisos pasados). Se abre el centro de administración de Microsoft 365, donde puede ver los avisos e incidentes del inquilino de los últimos 30 días.

Para ver información de *Service Health para Intune*, la cuenta debe tener el rol **Administrador global** o **Administrador de soporte técnico del servicio** en Azure Active Directory o el Centro de administración de Microsoft 365. Para asignar estos permisos, inicie sesión en el centro de administración de Microsoft 365 con permisos de Administrador global. Seleccione **Usuarios** > **Usuarios activos** y luego seleccione la cuenta que requiere acceso. Seleccione **Editar** en los roles, *Administrador de soporte técnico del servicio* o *Administrador global* y **Guardar** para asignar los permisos.

Las preferencias de comunicación de Estado del servicio Intune solo se pueden establecer a través del centro de administración de Microsoft 365.

Centro de mensajes de Intune

Vea comunicaciones informativas del equipo del servicio Intune sin tener que ir al centro de mensajes de Office. Las comunicaciones incluyen mensajes sobre los cambios que se han producido recientemente en el servicio Intune o que están en camino para el inquilino.

De forma predeterminada, se muestran los 10 mensajes más recientes y activos. Para ver mensajes más antiguos, seleccione **Ver mensajes anteriores** para abrir el *Centro de mensajes* en el Centro de administración de Microsoft 365.

Para ver información de Noticias de Intune, la cuenta debe tener el rol **Administrador global** o **Administrador de soporte técnico del servicio** en Azure Active Directory, o bien el rol **Lector del Centro de mensajes** en el Centro de administración de Microsoft 365. Para asignar este permiso, inicie sesión en el centro de administración de Microsoft 365 con permisos de administrador. Seleccione **Usuarios** > **Usuarios**

activos y luego seleccione la cuenta que requiere acceso. Seleccione **Editar** en *Roles*, seleccione *Administrador de comunicaciones de Teams* y luego seleccione **Guardar** para asignar los permisos.

Las preferencias de comunicación del centro de mensajes de Intune solo se pueden establecer a través del centro de administración de Microsoft 365.

Pasos siguientes

- Tutorial de Intune en Microsoft Endpoint Manager
- Obtener soporte para Intune

Uso del portal de solución de problemas para ayudar a los usuarios de su empresa

14/05/2021 • 6 minutes to read

El portal de solución de problemas permite que los operadores del departamento de soporte técnico y los administradores de Intune vean la información de usuario para solucionar las solicitudes de ayuda del usuario. Las organizaciones que disponen de un departamento de soporte técnico pueden asignar el **Operador del departamento de soporte técnico** a un grupo de usuarios. El rol de operador del departamento de soporte técnico puede usar el panel **Solución de problemas**.

En el panel **Solución de problemas** también se muestran los problemas de inscripción del usuario. Los detalles del problema y los pasos de corrección sugeridos pueden ayudar a los administradores y a los operadores del departamento de soporte técnico a solucionar los problemas. Ciertos problemas de inscripción no se capturan, y es posible que no se sugieran correcciones para algunos errores.

Para conocer los pasos sobre cómo agregar un rol de operador del departamento de soporte técnico, consulte Control de administración basada en roles (RBAC) con Intune

Cuando un usuario se pone en contacto con el soporte técnico por un problema técnico con Intune, el operador del departamento de soporte técnico introduce el nombre del usuario. Intune muestra datos útiles que pueden ayudar a resolver muchos problemas de nivel 1, incluidos los siguientes:

- Estado del usuario
- Assignments
- Problemas de cumplimiento
- El dispositivo no responde
- El dispositivo no obtiene una configuración Wi-Fi o VPN
- Error de instalación de la aplicación

Para ver los detalles de solución de problemas, siga estos pasos:

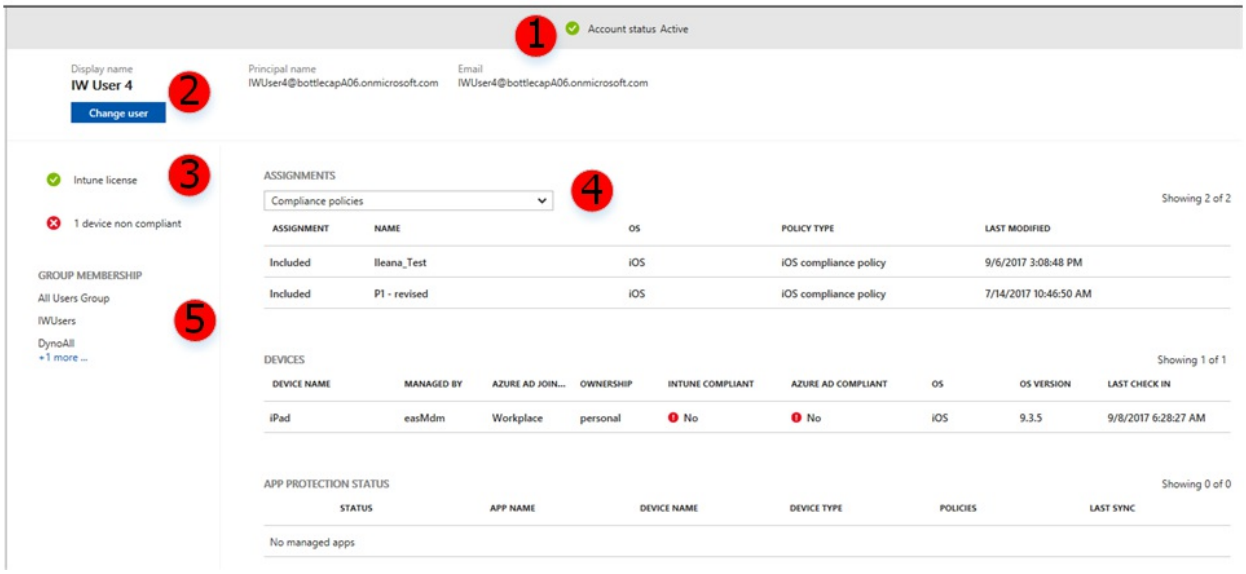
En el panel de solución de problemas, elija la opción **Seleccionar usuario** para ver la información del usuario. La información de usuario puede ayudarle a comprender el estado actual de los usuarios y sus dispositivos.

1. Inicie sesión en Intune.
2. En el panel **Intune**, elija **Solucionar problema**.
3. Haga clic en **Seleccionar** para seleccionar un usuario para solucionar problemas.
4. Seleccione un usuario escribiendo su nombre o dirección de correo electrónico. Haga clic en **Seleccionar**. La información de solución de problemas del usuario se muestra en el panel de solución de problemas. En la tabla siguiente se explica la información proporcionada.

> **NOTE**
> También puede acceder al panel de **solución de problemas** visitando la página https://aka.ms/intunetroubleshooting desde el explorador.

Áreas del panel de solución de problemas

Puede usar el panel **Solución de problemas** para consultar la información de usuario.



ÁREA	NOMBRE	DESCRIPCIÓN
1.	Estado de la cuenta	Muestra el estado del inquilino actual de Intune como **Activo** o **Inactivo**.
2.	Selección de usuarios	El nombre del usuario seleccionado actualmente. Haga clic en **Cambiar usuario** para elegir un usuario nuevo.
3.	Estado del usuario	Muestra el estado de la licencia de Intune del usuario, el número de dispositivos y el cumplimiento de cada uno.
4.	Información de usuario	Use la lista para seleccionar los detalles que vaya a consultar en el panel. Puede seleccionar: • Aplicaciones cliente • Directivas de cumplimiento • Directivas de configuración • Directivas de protección de aplicaciones • Restricciones de inscripción
5.	Pertenencia a grupos	Muestra los grupos actuales de los que es miembro el usuario seleccionado.

Referencia de errores de inscripción

La tabla Errores de inscripción enumera los intentos de inscripción que no han tenido éxito. Los dispositivo enumerados en la tabla siguiente pueden haberse inscrito correctamente en un intento posterior. Puede que no se muestren todos los intentos con error. La información de mitigación no está disponible para todos los errores.

COLUMNA DE TABLA	DESCRIPCIÓN
Inicio de inscripción	La hora en la que el usuario comenzó la inscripción.

COLUMNA DE TABLA	DESCRIPCIÓN
Sistema operativo	El sistema operativo del dispositivo.
Versión del SO	Versión del sistema operativo del dispositivo.
Error	El motivo del error.

Detalles del error

Cuando se elige una fila de error, se proporcionan más detalles.

SECCIÓN	DESCRIPCIÓN
Detalles del error	Una explicación más detallada del error.
Soluciones posibles	Pasos sugeridos para resolver el error. Puede que algunos errores no tengan solución.
Recursos (opcional)	Vínculos para obtener más información o áreas del portal en las que deben tomarse medidas.

Errores de inscripción

ERROR	DETALLES
Tiempo de espera o error de iOS/iPadOS	Tiempo de espera agotado entre el dispositivo e Intune debido a que el usuario tarda demasiado en realizar la inscripción.
Usuario no encontrado o sin licencia	El usuario no tiene una licencia o se ha quitado del servicio.
Dispositivo ya inscrito	Un usuario intentó inscribir un dispositivo mediante el Portal de empresa en un dispositivo que todavía está inscrito para otro usuario.
No incorporado a Intune	Se intentó una inscripción sin que la entidad de administración de dispositivos móviles (MDM) de Intune estuviese configurada.
Error de autorización de inscripción	Se intentó realizar la inscripción con una versión antigua del portal de empresa.
Dispositivo no compatible	El dispositivo no cumple los requisitos mínimos para la inscripción en Intune.
Las restricciones de inscripción no se cumplen	Esta inscripción se ha bloqueado debido a una restricción de inscripciones configurada por el administrador.
Versión de dispositivo demasiado baja	El administrador ha configurado una restricción de inscripción que exige una versión de dispositivo superior.
Versión de dispositivo demasiado alta	El administrador ha configurado una restricción de inscripción que exige una versión de dispositivo inferior.

ERROR	DETALLES
El dispositivo no se puede inscribir como personal	El administrador ha configurado una restricción de inscripción para bloquear las inscripciones personales y el dispositivo con el error no se ha predefinido como corporativo.
Plataforma de dispositivo bloqueada	El administrador ha configurado una restricción de inscripción que bloquea la plataforma de este dispositivo.
El token en masa ha expirado	El token en masa del paquete de aprovisionamiento ha expirado.
No se encontraron los detalles o el dispositivo Autopilot	No se ha encontrado el dispositivo Autopilot al intentar inscribir.
El perfil de Autopilot no se ha encontrado o no se ha asignado	El dispositivo no tiene un perfil de Autopilot activo.
Método de inscripción de Autopilot no esperado	El dispositivo ha intentado inscribirse mediante un método no permitido.
El dispositivo Autopilot se ha eliminado	Se ha quitado de Autopilot el dispositivo que intentaba inscribirse para esta cuenta.
Se alcanzó el límite de dispositivos	Esta inscripción se ha bloqueado debido a una restricción en el límite de dispositivos configurada por el administrador.
Incorporación de Apple	Se ha bloqueado la inscripción de todos los dispositivos iOS/iPadOS debido a que falta o ha expirado el certificado push MDM de Apple en Intune.
Dispositivo no registrado previamente	El dispositivo no se ha registrado previamente como corporativo y todas las inscripciones personales han sido bloqueadas por el administrador.
Característica no compatible	Es probable que el usuario intentase realizar la inscripción a través de un método que no es compatible con la configuración de Intune.

Recopilación de los datos disponibles desde un dispositivo móvil

Use los siguientes recursos para ayudarle a recopilar los datos de servicio al solucionar problemas del dispositivo del usuario:

- Enviar errores de inscripción de iOS/iPadOS al administrador de TI
- Ayudar al equipo de soporte técnico de su empresa a solucionar los problemas del dispositivo mediante el registro detallado
- Enviar registros de Android al equipo de soporte técnico de su empresa mediante un cable USB
- Enviar registros de datos de diagnóstico al administrador de TI mediante correo electrónico
- Enviar errores de inscripción de Android al administrador de TI

Pasos siguientes

Puede obtener más información sobre el control de administración basada en roles (RBAC) para definir los roles

en su dispositivo de empresa, en la administración de aplicaciones móviles y en las tareas de protección de datos en Control de administración basada en roles (RBAC) con Intune.

Obtenga información sobre los problemas conocidos de Microsoft Intune. Para obtener más información, consulte Problemas conocidos de Microsoft Intune.

Obtenga información sobre cómo crear una incidencia de soporte técnico y obtener ayuda cuando lo necesite. Obtención de soporte técnico.

Cómo usar los documentos

14/05/2021 • 9 minutes to read

En este artículo se ofrecen recursos y sugerencias para usar la biblioteca de documentación de Microsoft Endpoint Manager. El ámbito de aplicación es Configuration Manager, Microsoft Intune y Autopilot, y se tratan las siguientes áreas:

- Procedimiento para realizar búsquedas
- Envío de errores, mejoras, preguntas y nuevas ideas sobre la documentación
- Procedimiento para recibir notificaciones de los cambios
- Procedimiento para colaborar en documentación

Para obtener ayuda y soporte general, consulte:

- Buscar ayuda para Configuration Manager
- Obtener soporte en Microsoft Endpoint Manager

> **TIP**
> Visite también el nodo **Documentación** del área de trabajo **Comunidad** de la consola de Configuration Manager. Este nodo incluye información actualizada acerca de los artículos de soporte técnico y la documentación de Configuration Manager. Para obtener más información, vea Uso de la consola de Configuration Manager.

La información de este artículo también se aplica a la documentación de PowerShell de Configuration Manager del repositorio sccm-docs-powershell-ref.

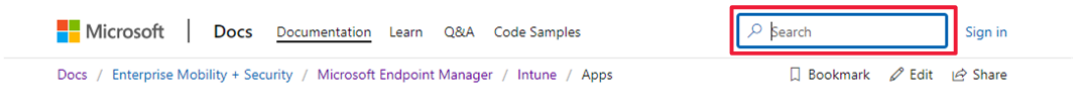
Buscar

Usa los consejos de búsqueda siguientes para tratar de encontrar la información que necesitas:

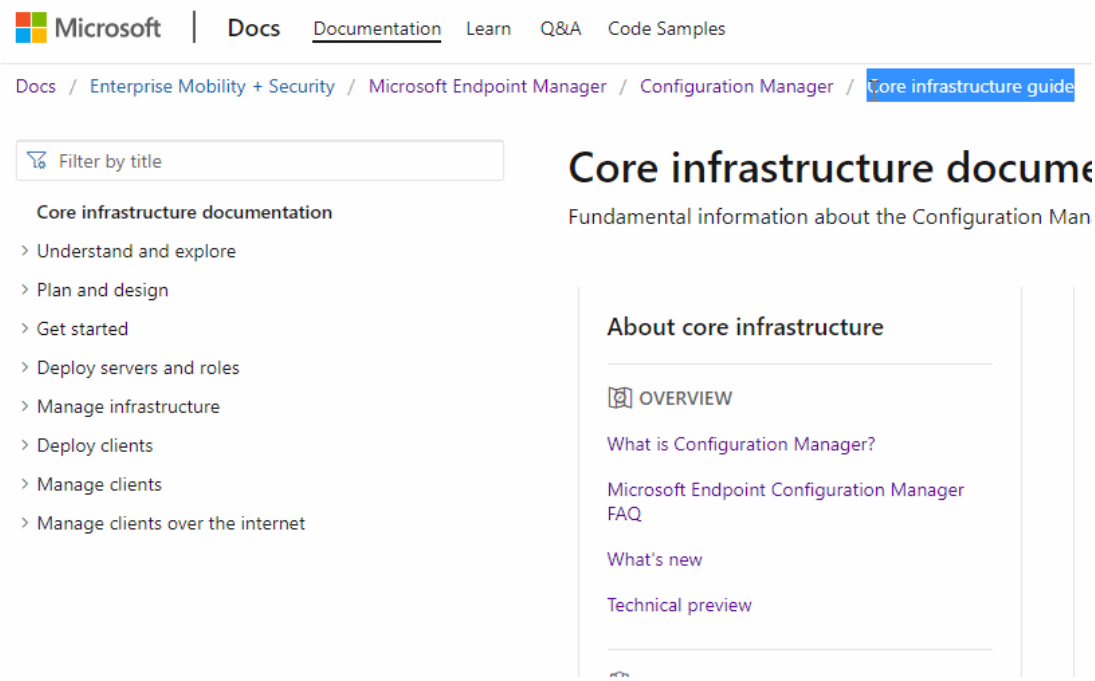
- Al usar su motor de búsqueda preferido para buscar contenido, incluya una palabra clave junto a las palabras clave de búsqueda. Por ejemplo, `ConfigMgr` para Configuration Manager y `Intune` para Intune.
  - Busque los resultados en `docs.microsoft.com/mem`. Los resultados de `docs.microsoft.com/previous-versions`, `technet.microsoft.com` o `msdn.microsoft.com` corresponden a versiones anteriores del producto.
  - Para centrar más los resultados de la búsqueda en la biblioteca de contenido actual, incluya `site:docs.microsoft.com` en la consulta para definir el ámbito del motor de búsqueda.
- Use los términos de búsqueda que coincidan con la terminología en la interfaz de usuario y la documentación en línea. Evite términos no oficiales o abreviaciones que es posible que vea en el contenido de la Comunidad. Por ejemplo, busque:
  - "punto de administración" en lugar de "MP"
  - "tipo de implementación" en lugar de "DT"
  - "extensión de administración de Intune" en lugar de "IME"
- Para buscar dentro del artículo actual, use la característica **Buscar** del explorador. Con los exploradores web más modernos, presione **Ctrl**+**F** y luego escriba los términos de búsqueda.
- En cada artículo de `docs.microsoft.com` se incluyen los siguientes campos para ayudar a buscar el

contenido:

- **Búsqueda** en la esquina superior derecha. Para buscar todos los artículos, escriba los términos en este campo. Los artículos de esta biblioteca de contenido incluyen automáticamente uno de los siguientes ámbitos de búsqueda: `ConfigMgr` o `Intune`.



- **Filtre por título** sobre la tabla de contenido de la izquierda. Para buscar en la tabla de contenido actual, escriba los términos en este campo. Este campo solo compara los términos que aparecen en los títulos de artículo del nodo actual. Por ejemplo, **Infraestructura central de Configuration Manager** (`docs.microsoft.com/mem/configmgr/core`) o **Aplicaciones de Intune** (`https://docs.microsoft.com/mem/intune/apps/`). El último elemento de los resultados de la búsqueda ofrece la opción de buscar los términos en toda la biblioteca de contenido.



¿Tiene problemas para encontrar algo? Rellene los comentarios Al registrar un problema con los resultados de la búsqueda, indique el motor de búsqueda que está usando, las palabras clave que ha intentado y el artículo de destino. Estos comentarios ayudan a Microsoft a optimizar el contenido para que la búsqueda sea mejor.

Adición de un motor de búsqueda personalizado

Con muchos exploradores web modernos, puede crear un motor de búsqueda personalizado. Use esta característica para buscar `docs.microsoft.com` de forma rápida y sencilla. Por ejemplo, con Microsoft Edge, versión 77 y posteriores, utilice el siguiente proceso:

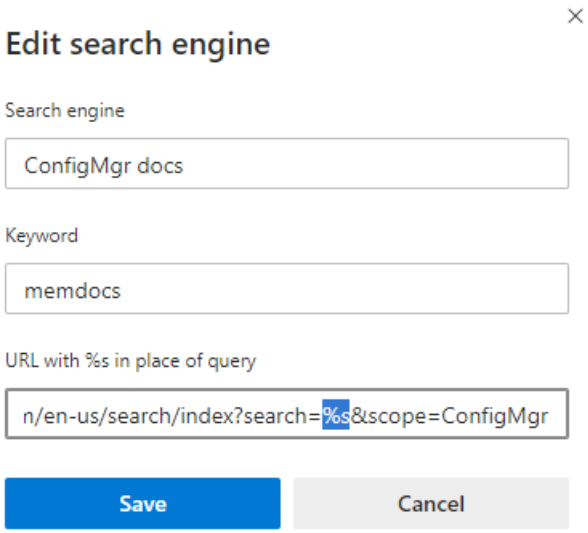
1. En Microsoft Edge, versión 77 y posteriores, abra **Configuración**.
2. En el menú de la izquierda, seleccione **Privacidad, búsqueda y servicios**.
3. Desplácese hasta la parte inferior del grupo **Servicios** y seleccione **Barra de direcciones y búsqueda**.
4. Seleccione **Administrar motores de búsqueda**.
5. Seleccione **Agregar** y especifique la siguiente información:

   - **Motor de búsqueda**: escriba un nombre descriptivo para identificarlo en la lista de motores de búsqueda. Por ejemplo, `Microsoft docs`.

- **Palabra clave**: especifique un término corto para usarlo en la barra de direcciones para activar este motor de búsqueda. Por ejemplo, `memdocs`.
- **Dirección URL con `%s` en lugar de la consulta**: Por ejemplo,

```
https://docs.microsoft.com/en-us/search/index?search=%s&scope=ConfigMgr
```

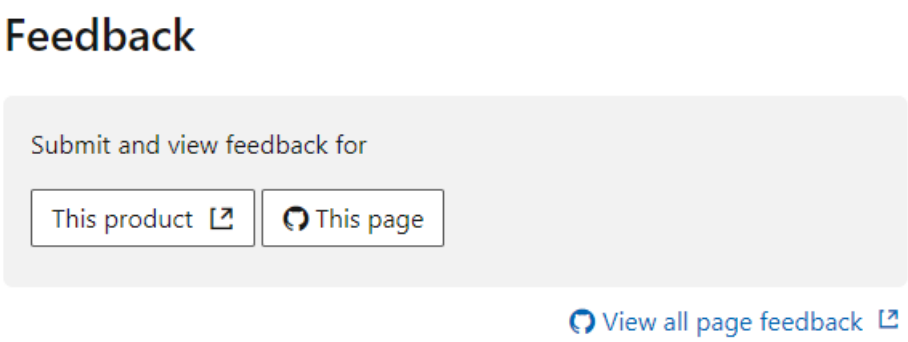
> **NOTE**
>
> Este ejemplo es específico del ámbito de `ConfigMgr`. Puede quitar la variable de ámbito para buscar en todos los `docs.microsoft.com` o usar un ámbito diferente.
>
> El motor de búsqueda de Microsoft Docs requiere una configuración regional en la dirección. Por ejemplo, `en-us`. Puede cambiar la entrada para usar una configuración regional diferente.



Después de agregar este motor de búsqueda, escriba la palabra clave en la barra de direcciones del explorador, presione `Tab`, escriba los términos de búsqueda y presione `Enter`. Buscará automáticamente los términos especificados en Microsoft Docs mediante el ámbito definido.

Acerca de Comentarios

Seleccione el vínculo **Comentarios** de la esquina superior derecha de cualquier artículo para ir a la sección Comentarios de la parte inferior. Los comentarios se integran con Problemas de GitHub. Para obtener más información sobre la integración con Problemas de GitHub, vea la entrada de blog de la plataforma de documentación.



Para compartir comentarios que sean sobre el propio producto y no sobre la documentación, seleccione **Este producto**. Esta acción abre el sitio web UserVoice del producto.

Para compartir comentarios sobre el artículo de documentación actual, seleccione **Esta página**. Una cuenta de GitHub es un requisito previo para proporcionar comentarios sobre la documentación. Una vez que inicie sesión, hay una autorización de una sola vez para la organización de MicrosoftDocs. A continuación, se abre el formulario de nuevo problema (New issue) de GitHub. Agregue un título descriptivo y comentarios detallados en el cuerpo, pero no modifique la sección de detalles del documento. A continuación, seleccione **Submit new issue** (Enviar nuevo problema) para registrar un nuevo problema sobre el artículo de destino en el repositorio MEMDocs de GitHub.

Para ver si ya hay comentarios sobre este artículo, seleccione **View all page feedback** (Ver todos los comentarios de la página). Esta acción abre una consulta de problemas de GitHub sobre este artículo. De forma predeterminada, se muestran los problemas abiertos y cerrados. Revise los comentarios que ya hay antes de enviar un nuevo problema. Si encuentra un problema relacionado, seleccione el icono de la cara para agregar una reacción, agregue un comentario a la conversación o seleccione **Subscribe** (Suscribirse) para recibir notificaciones.

Tipos de comentarios

Use Problemas de GitHub para enviar los siguientes tipos de comentarios:

- Error de documento: el contenido está obsoleto, es poco claro, confuso o se ha interrumpido.
- Mejora de documento: una sugerencia para mejorar el artículo.
- Pregunta de documento: necesita ayuda para encontrar documentación existente.
- Idea de documento: una sugerencia para un artículo nuevo. Use este método en lugar de UserVoice para los comentarios sobre la documentación.
- Enhorabuena: comentarios positivos sobre un artículo útil o informativo.
- Localización: comentarios sobre la traducción del contenido.
- Optimización del motor de búsqueda (SEO): comentarios sobre problemas de búsqueda de contenido. Incluya el motor de búsqueda, las palabras clave y el artículo de destino en los comentarios.

Si crea un problema sobre algo que no está relacionado con la documentación, Microsoft cerrará el problema y le redirigirá a un canal de comentarios más pertinente. Por ejemplo:

- Comentarios del producto para Configuration Manager o Intune
- Preguntas sobre el producto
- Solicitudes de soporte técnico para Configuration Manager o Microsoft Endpoint Manager

Para compartir comentarios sobre la plataforma docs.microsoft.com, consulte el artículo correspondiente a los comentarios sobre la documentación. La plataforma incluye todos los componentes contenedores, como el encabezado, la tabla de contenido y el menú de la derecha. También cómo se representan los artículos en el explorador, como la fuente, los cuadros de alerta y los delimitadores de página.

Notificaciones

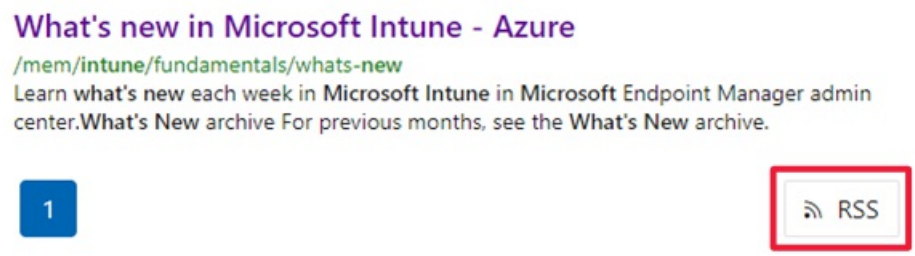
Para recibir notificaciones cuando cambie el contenido de la biblioteca de documentación, siga estos pasos:

1. Use la búsqueda de documentos para buscar un artículo o un conjunto de artículos. Por ejemplo:
   - Busque un solo artículo por título: Novedades de Microsoft Intune

     > **TIP**
     > Para refinar una búsqueda a un solo artículo, use el título completo que aparece en los resultados de la búsqueda de docs.microsoft.com. Este título es el que aparece en la pestaña del explorador.

   - Busque cualquier artículo de Configuration Manager sobre BitLocker.

2. En la parte inferior de la lista de resultados, seleccione el vínculo **RSS**.



3. Use esta fuente en cualquier aplicación RSS para recibir notificaciones cuando haya un cambio en cualquiera de los resultados de la búsqueda.

Hay varios artículos populares en esta biblioteca de contenido que tienen una sugerencia en la parte superior con un vínculo a la fuente RSS.

> **TIP**
> También puede **seguir el hilo** del repositorio MEMDocs en GitHub. Este método puede generar *muchas* notificaciones. Además, no incluye los cambios de un repositorio privado que usa Microsoft.

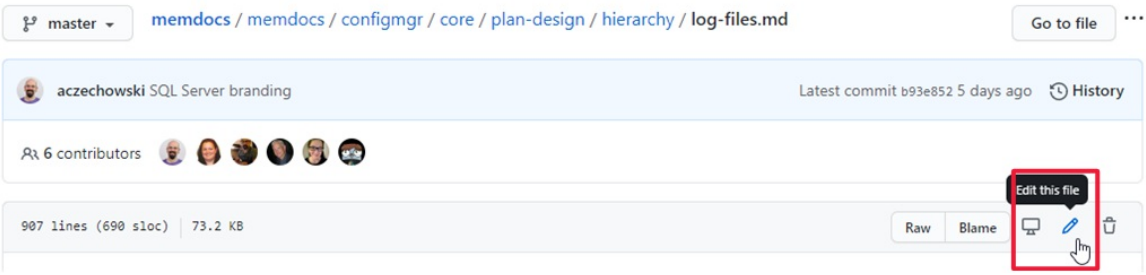
Contribuir

La biblioteca de documentación de Microsoft Endpoint Manager, al igual que la mayor parte del contenido de docs.microsoft.com, es de código abierto en GitHub. Esta biblioteca acepta y fomenta contribuciones de la comunidad. Para obtener más información sobre cómo empezar, vea la guía para colaboradores. El único requisito previo es crear una cuenta de GitHub.

Pasos básicos para contribuir

1. En el artículo de destino, seleccione el icono de **editar** en la esquina superior derecha. Esta acción abre el archivo de origen de GitHub.

2. Para editar el archivo de origen, seleccione el icono de lápiz.



3. Realice cambios en el origen Markdown. Para obtener más información, vea How to use Markdown for writing Docs (Cómo usar Markdown para escribir documentos).

4. En la sección Propose file change (Proponer cambio de archivo), escriba el comentario de confirmación público que describe *qué* ha modificado. Luego, seleccione **Propose file change** (Proponer cambio de archivo).

5. Desplácese hacia abajo y compruebe los cambios realizados. Seleccione **Crear solicitud de incorporación de cambios** para abrir el formulario. Describa *por qué* ha realizado este cambio. Seleccione **Crear solicitud de incorporación de cambios**.

El equipo de redacción recibe su solicitud de incorporación de cambios y la asigna al redactor adecuado. El autor revisa el texto y realiza un paso de edición rápida en él, y aprobará y combinará los cambios, o bien se pondrá en contacto con usted para obtener más información sobre la actualización.

Cómo contribuir

Si quiere contribuir, pero no sabe por dónde empezar, vea las siguientes sugerencias:

- Revise la precisión de un artículo. Luego actualice los metadatos **ms.date** mediante el formato `mm/dd/yyyy`. Esta contribución ayuda a mantener el contenido actualizado.
- Agregue aclaraciones, ejemplos o instrucciones en función de su experiencia. Esta contribución usa el poder de la comunidad para compartir conocimiento.
- Traducciones correctas a un idioma distinto del inglés. Esta contribución mejora la facilidad de uso del contenido localizado.
- Busque las etiquetas destinadas a la comunidad en la lista de problemas:
  - **good-first-issue**
  - **help-wanted**

    Los autores de Microsoft asignan estas etiquetas a problemas que son adecuados para la contribución de la comunidad. Se usan principalmente para la documentación de PowerShell de Configuration Manager.

> **NOTE**
> Las contribuciones grandes requieren la firma de un contrato de licencia de colaboración (CLA) si no es empleado de Microsoft. GitHub automáticamente requiere que firme este acuerdo cuando una contribución alcanza el umbral. Solo tiene que firmar este contrato una vez.

Sugerencias de contribución

Siga estas directrices generales cuando haga contribuciones:

- No nos sorprenda con grandes solicitudes de incorporación de cambios. En su lugar, notifique un problema e inicie una discusión. Así podremos acordar un rumbo antes de invertir una gran cantidad de tiempo.
- Lea la guía de estilo de Microsoft. Conozca los 10 principales consejos sobre el estilo y el tono de Microsoft.
- Siga el flujo de trabajo de GitHub Flow.
- Publique frecuentemente en blogs o en tweets (o donde sea) los contenidos con los que contribuya.

(Esta lista la hemos tomado de la guía del contribuidor de .NET).

Procedimientos para obtener soporte en el Centro de administración de Microsoft Endpoint Manager

14/05/2021 • 7 minutes to read

Microsoft proporciona, a escala global, soporte para suscripciones, facturación, preventa y asuntos técnicos en servicios basados en la nube de administración de dispositivos, como Intune, Configuration Manager y Escritorio administrado de Microsoft. Puede solicitar soporte para todos esos aspectos desde el Centro de administración de Microsoft Endpoint Manager.

El soporte técnico está disponible tanto en línea como por teléfono para las suscripciones de pago y de prueba. El soporte técnico en línea está disponible en inglés y japonés. El soporte técnico telefónico y para facturación en línea está disponible en otros idiomas.

Con el acceso administrativo al Centro de administración, puede usar la opción **Ayuda y soporte técnico** para registrar una incidencia de soporte técnico en línea sobre un servicio compatible. Para crear y administrar un incidente de soporte técnico, su cuenta debe tener un rol de Azure Active Directory (Azure AD) que incluya la *acción* **microsoft.office365.supportTickets/tickets/manage**. Para información sobre los permisos y roles de Azure AD que se necesitan para crear una incidencia de soporte técnico, consulte el artículo sobre los roles de administrador en Azure Active Directory.

> **IMPORTANT**
> Para obtener soporte técnico para productos de terceros que funcionan con Intune (por ejemplo, Saaswedo, Cisco o Lookout), póngase en contacto con el proveedor de ese producto en primer lugar. Asegúrese de que ha configurado el otro producto correctamente antes de abrir una solicitud con el soporte técnico de Intune.

Acceso a Ayuda y soporte técnico

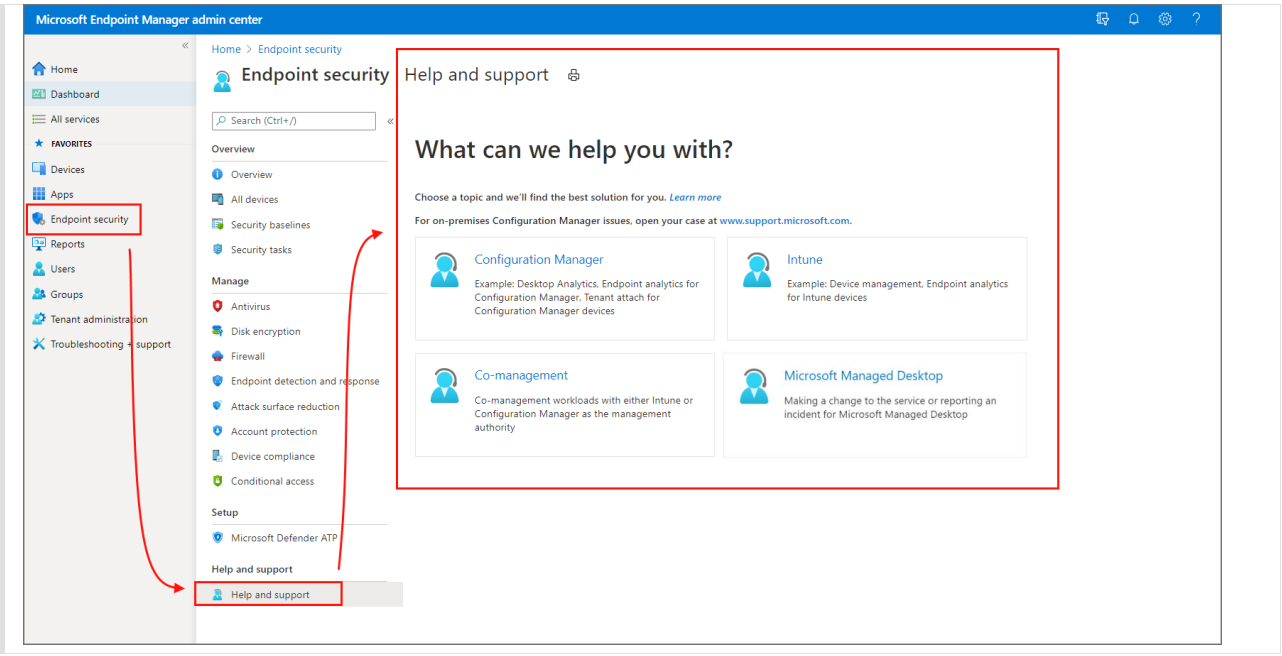
Use uno de los siguientes vínculos para abrir el Centro de administración de Microsoft Endpoint Manager. El que use dependerá de cómo esté hospedado el inquilino:

- **Nube pública**: use https://endpoint.microsoft.com.
- **Nube privada** para organismos públicos, también conocida como "nube soberana"; por ejemplo, Azure Government. Use https://endpoint.microsoft.us.

Desde el Centro de administración, use uno de los métodos siguientes para acceder a Ayuda y soporte técnico:

- Vaya a **Solución de problemas + soporte técnico** > **Ayuda y soporte técnico** para abrir el panel *Ayuda y soporte técnico*.
- En cualquier nodo del Centro de administración, seleccione **Ayuda y soporte técnico** para abrir el panel *Ayuda y soporte técnico*.
- En cualquier nodo del Centro de administración, seleccione el icono **?** de la esquina superior derecha para abrir el panel *Ayuda*. A continuación, seleccione **Ayuda y soporte técnico** para abrir el panel *Ayuda y soporte técnico*.

En la siguiente imagen se ilustra un ejemplo de cómo acceder a Ayuda y soporte técnico en Microsoft Intune desplazándonos hasta el nodo Seguridad de los puntos de conexión y seleccionando Ayuda y soporte técnico:



En el panel *Ayuda y soporte técnico*, seleccione un mosaico según el ámbito en el que necesite asistencia. La siguiente información puede ayudarlo a elegir el adecuado:

- **Intune**:
  - Administración de dispositivos con Intune
  - Análisis de puntos de conexión para dispositivos de Intune
- **Configuration Manager**:
  - Análisis de escritorio
  - Análisis de puntos de conexión para dispositivos de Configuration Manager
  - Asociación de inquilinos para dispositivos de Configuration Manager

  Si tiene problemas con su **instancia local de Configuration Manager**, abra el caso en www.support.microsoft.com.
- **Administración conjunta**:
  - Administración conjunta de cargas de trabajo con Intune o Configuration Manager como entidad de administración
- **Escritorio administrado de Microsoft**:

  Este mosaico solo está disponible para los clientes de Escritorio administrado de Microsoft.
  - Solicitudes de información para la configuración o el inquilino de Escritorio administrado de Microsoft
  - Solicitudes de cambios en la configuración de los dispositivos de Escritorio administrado de Microsoft
  - Notificación de un incidente o una interrupción

  Si es cliente de Escritorio administrado de Microsoft, al seleccionar ese icono para problemas relacionados con Escritorio administrado de Microsoft, se le redirigirá a la página Solicitudes de servicio. Para obtener más información sobre Solicitudes de servicio, consulte Soporte de administración para Escritorio administrado de Microsoft.

TIP

Es posible que Ayuda y soporte técnico no se abra con los inquilinos recién creados y que se muestre el siguiente mensaje:

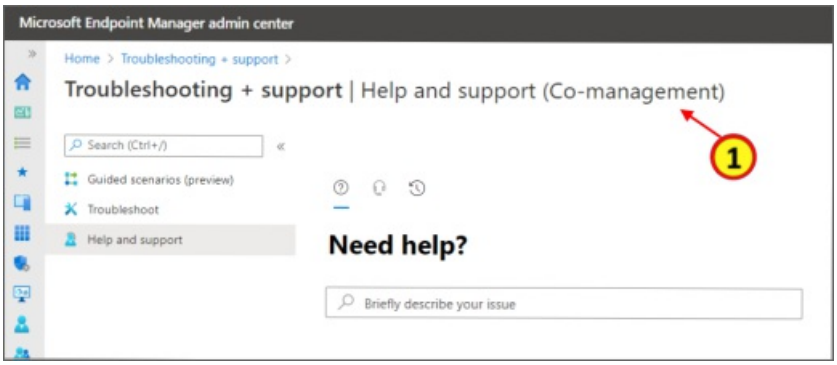
- *We encountered an unknown problem. Please refresh the page but if the problem persists, please create a case through M365 Admin Center and reference the session ID provided.* (Se encontró un problema desconocido. Actualice la página; si el problema persiste, cree un caso en el Centro de administración de M365 y haga referencia al identificador de sesión proporcionado).

Los detalles del error incluyen un *identificador de sesión*, la *extensión*, etc.

Este problema se produce cuando no ha autenticado y accedido a Necesito ayuda desde la nueva cuenta de inquilino a través del **Centro de administración de Microsoft 365**, en https://admin.microsoft.com, o el **portal de Office 365**, en https://portal.office.com. Para resolver este problema, seleccione el vínculo del *Centro de administración de Microsoft 365* en el mensaje, o bien visite https://portal.office.com e inicie sesión. Después de la autenticación en cualquiera de los sitios, vaya al área de administración y haga clic en el icono Necesito ayuda que hay en la parte inferior derecha. Después de completar estos pasos, *Ayuda y soporte técnico* para Intune se vuelve accesible.

Experiencia de soporte técnico

Después de seleccionar un ámbito de soporte, el Centro de administración mostrará la página Ayuda y soporte técnico, en la que aparece el ámbito de soporte que ha seleccionado en la parte superior **(1)** . Si se seleccionó un escenario de soporte incorrecto, deberá volver y seleccionar otro ámbito:



Encima del mosaico *¿Necesita ayuda?* hay tres iconos que puede seleccionar para abrir diferentes paneles de la ventana *¿Necesita ayuda?* . El panel que está viendo se identifica con el subrayado.

TIP

Los clientes con un contrato de soporte técnico **Premier** o **Unified** tienen opciones adicionales de soporte técnico y verán un banner en la ventana ¿Necesita ayuda? que recuerda a la siguiente imagen:

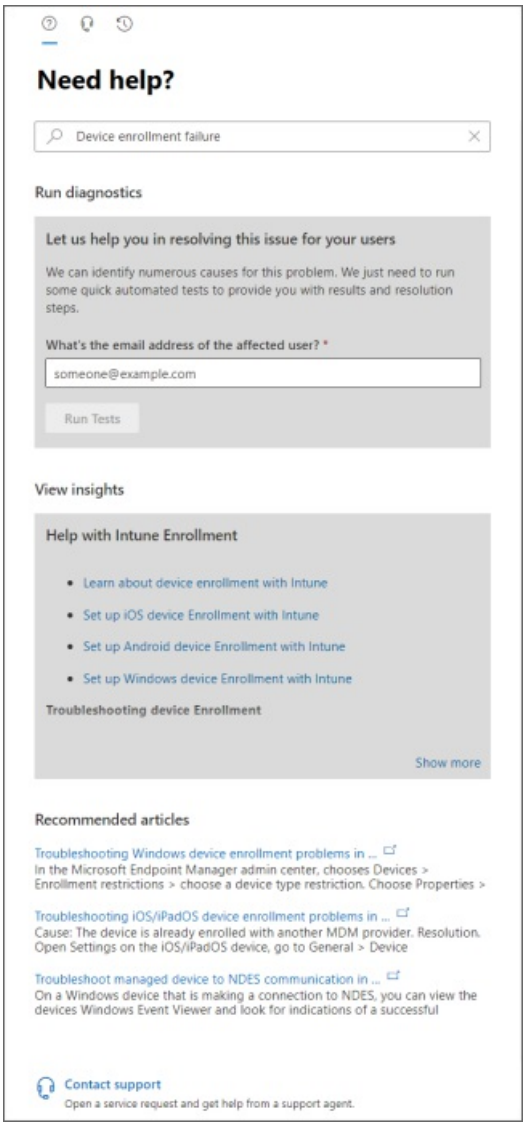
De forma predeterminada, se abre la página Ayuda y soporte técnico en el panel *Buscar soluciones*. Sin embargo, si tiene un caso de soporte activo, Ayuda y soporte técnico se abre en el panel *Solicitudes de servicio*, donde puede ver los detalles de los casos de soporte activos y cerrados.

Buscar soluciones

En el panel *Buscar soluciones*, especifique algunos detalles sobre una incidencia en el cuadro de texto proporcionado. El panel devuelve una o varias de las siguientes opciones en función de los detalles proporcionados:

- **Ejecutar diagnósticos**: desde la consola, puede iniciar investigaciones y pruebas automatizadas del inquilino que puedan revelar problemas conocidos. Al ejecutar un diagnóstico, es posible que reciba pasos de mitigación que puede seguir para resolver el problema.
- **Ver conclusiones**: busque vínculos a documentación que proporcione contexto del área de producto o las acciones que ha descrito.
- **Artículos recomendados**: siga los vínculos a la solución de problemas y al contenido relacionado que se centre en el problema que ha descrito.

Por ejemplo, para Microsoft Intune, podría escribir **error de inscripción de dispositivo**. Con estos criterios, entre los resultados estaría la opción de seleccionar Ejecutar diagnósticos en una cuenta de usuario:

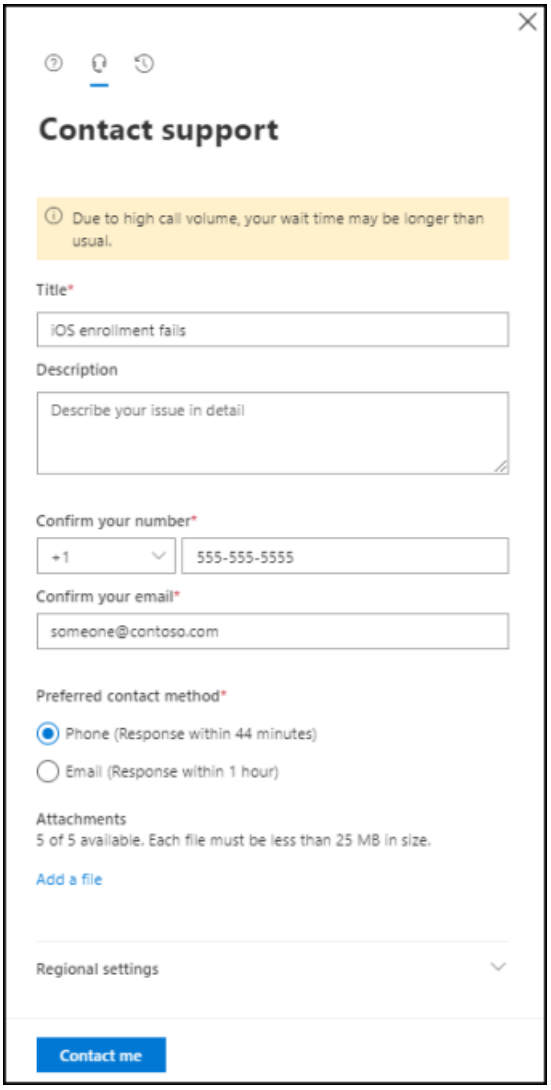


Ejecutar diagnósticos puede identificar problemas en esa cuenta de su instancia de Azure AD. En este ejemplo, el usuario no tiene asignada una licencia de Intune, lo que impide la inscripción del dispositivo, y se proporciona un vínculo al contenido pertinente:

Póngase en contacto con el soporte técnico.

En el panel *Contacto con soporte técnico*, puede enviar una solicitud de asistencia. Este panel está disponible después de proporcionar algunas palabras clave básicas en el panel *Buscar soluciones*.

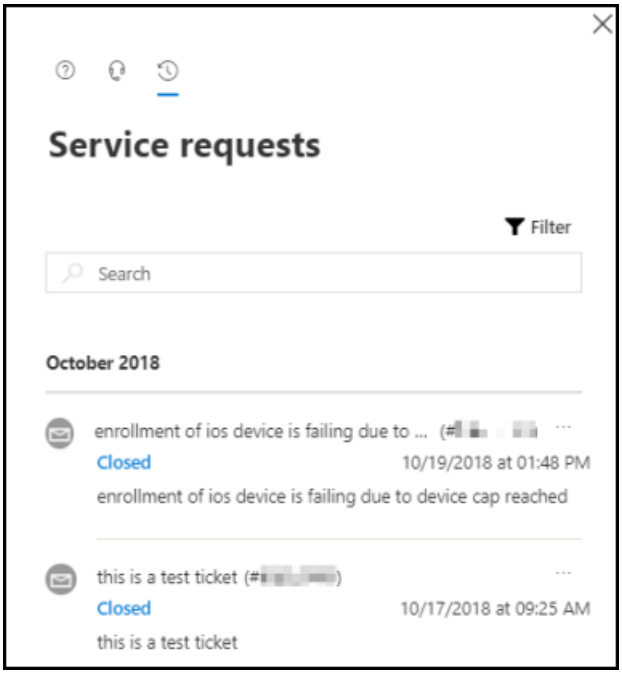
Al solicitar asistencia, proporcione una descripción del problema con tantos detalles como sea necesario. Después de confirmar la información de contacto de teléfono y correo electrónico, seleccione el método de contacto preferido. La ventana muestra un tiempo de respuesta para cada método de contacto, lo que le permite estimar cuándo se pondrán en contacto con usted. Antes de enviar la solicitud, adjunte archivos como registros o capturas de pantallas que puedan ayudar a rellenar los detalles del problema.



Después de rellenar la información necesaria, seleccione **Ponerse en contacto conmigo**.

Solicitudes de servicio

El panel *Solicitudes de servicio* muestra el historial de casos. Los casos activos se encuentran arriba de la lista, con las incidencias cerradas que también están disponibles para revisión.



Si tiene un número de caso de soporte técnico activo, puede escribirlo aquí para ir a ese problema o puede seleccionar un incidente de la lista de incidentes activos y cerrados para ver más información sobre él.

Cuando haya terminado de ver los detalles de un incidente, seleccione la flecha izquierda que aparece en la parte superior de la ventana de la solicitud de servicio, justo encima de los tres iconos del panel *¿Necesita ayuda?* La flecha atrás vuelve a la lista de incidentes de soporte técnico que ha abierto.

Clientes de soporte técnico Premier y Unified

Los clientes con un contrato de soporte técnico **Premier** o **Unified** pueden especificar la gravedad del problema y programar una devolución de llamada de soporte técnico a una hora y en un día concretos. Estas opciones están disponibles al abrir o enviar una nueva incidencia y al editar un caso de soporte activo.

Gravedad: las opciones para especificar la gravedad de una incidencia dependen del contrato de soporte técnico:

- *Premier*: gravedad de A, B o C.
- *Unified*: crítico o no crítico.

La selección de un problema con una gravedad **A** o **Crítica** le limita a un caso de soporte técnico por teléfono, que proporciona la opción más rápida para recibir asistencia.

Callback schedule (Programación de devolución de llamada): puede solicitar una devolución de llamada a una hora y en un día determinados.

Pasos siguientes

- Soporte de facturación y administración de suscripciones
- Licencias por volumen
- Solución de problemas de Intune

Informes de Intune

14/05/2021 • 20 minutes to read

Los informes de Microsoft Intune le permiten supervisar de forma más eficaz y proactiva el estado y la actividad de los puntos de conexión de toda la organización, además de proporcionar otros datos de informes en Intune. Por ejemplo, podrá ver informes sobre el cumplimiento, el estado y las tendencias de los dispositivos. Además, puede crear informes personalizados para obtener datos más específicos.

> **NOTE**
> Los cambios en los informes de Intune se implementarán gradualmente durante un período de tiempo para ayudarle a preparar la nueva estructura y adaptarse a ella.

Los tipos de informes se organizan en las siguientes áreas de enfoque:

- **Operativo**: proporciona datos dirigidos oportunamente que le ayudan a centrar la atención y tomar medidas. Los administradores, los expertos en la materia y el departamento de soporte técnico encontrarán estos informes particularmente útiles.
- **Organizativo**: proporciona un resumen más amplio de una vista general, como el estado de administración de los dispositivos. Los administradores encontrarán estos informes particularmente útiles.
- **Histórico**: proporciona patrones y tendencias a lo largo de un período de tiempo. Los administradores encontrarán estos informes particularmente útiles.
- **Especialista**: le permite usar datos sin procesar para crear sus propios informes personalizados. Los administradores encontrarán estos informes particularmente útiles.

La plataforma de informes proporciona una experiencia de informes coherente y más completa. Los informes disponibles proporcionan la siguiente funcionalidad:

- **Búsqueda y ordenación**: puede buscar y ordenar por columna, independientemente del tamaño del conjunto de datos.
- **Paginación de datos**: puede examinar los datos en función de la paginación (página a página o saltar a una página específica).
- **Rendimiento**: puede generar y ver rápidamente los informes creados a partir de inquilinos de gran tamaño.
- **Exportación**: puede exportar rápidamente los datos de informes generados a partir de inquilinos de gran tamaño.

¿Quién puede acceder a los datos?

Los usuarios con los siguientes permisos pueden revisar los registros:

- Administrador global
- Administrador de servicios de Intune
- Administradores asignados a un rol de Intune con los permisos de **Lectura**

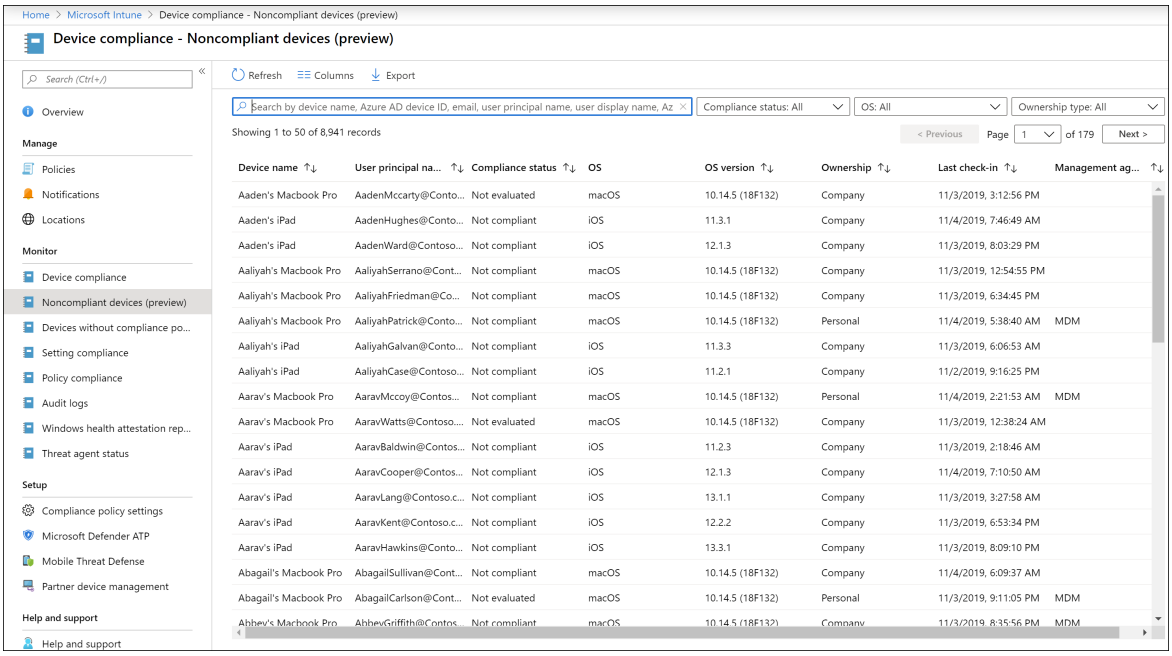
Informe Dispositivos no conformes (operativo)

En el informe **Dispositivos no conformes** se proporcionan los datos que suelen usar los roles del departamento de soporte técnico o de administrador para identificar problemas y ayudar a resolverlos. Los datos que se encuentran en este informe son oportunos, anuncian comportamientos inesperados y pretenden ser accionables. El informe está disponible junto con la carga de trabajo, lo que convierte a estos informes en

accesibles sin desplazarse lejos de los flujos de trabajo activos. Este informe proporciona funcionalidades de filtrado, búsqueda, paginación y ordenación. También puede explorar en profundizar para solucionar problemas.

Puede ver el informe **Dispositivos no conformes** mediante los pasos siguientes:

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione **Dispositivos** > **Monitor** > **Dispositivos no conformes**.



> **TIP**
>
> Si ya ha usado Intune en Azure Portal antes, encontraría los detalles anteriores en Azure Portal al iniciar sesión en Intune y seleccionar **Cumplimiento de dispositivos** > **Dispositivos no compatibles**.

Directivas no conformes (versión preliminar)

El informe **Directivas no conformes** puede ayudarle a solucionar problemas de directivas que tienen errores o conflictos de cumplimiento.

Al seleccionar el informe, se muestra una lista de directivas de cumplimiento que tienen uno o más dispositivos con un error o un estado no compatible. Los detalles incluyen el recuento de cada una de esas categorías y la plataforma del dispositivo. Use este informe para profundizar en entradas individuales con el fin de obtener más información y, en cada nivel, puede ordenar y filtrar los registros.

Mientras visualiza el informe:

- Seleccione una directiva para ver las directivas de cumplimiento de dispositivos con dispositivos en un estado de error o no compatible. La información incluye el estado de implementación y la última vez que se ha actualizado el estado.
- Seleccione un dispositivo de la lista para profundizar y ver una lista de configuraciones de la directiva. La lista de configuraciones incluye el estado de la configuración, como *Compatible*, *No compatible* o *No aplicable*. Si se ha producido un error, se muestra el código de error correspondiente.
- Si después selecciona una configuración específica, verá más detalles sobre el estado o el código de error. Esta información también incluye los perfiles que se han usado para implementar la configuración en el dispositivo.

Para ver el informe de directivas no conformes:

1. Inicie sesión en el Centro de administración de Microsoft Endpoint Manager.
2. Seleccione **Dispositivos** > **Monitor** > **Directivas no conformes**.

> **NOTE**
>
> *Este informe se encuentra en versión preliminar.*

Informe Puntos de conexión incorrectos de Windows 10 (operativo)

El informe **Puntos de conexión incorrectos de Windows 10** muestra los datos que suelen usar los roles del departamento de soporte técnico o de administrador para identificar problemas y ayudar a resolverlos. Los datos que se encuentran en este informe son oportunos y anuncian el dispositivo incorrecto, el nombre principal de usuario primario y el estado de algunos valores. El informe está disponible como una pestaña dentro de la carga de trabajo principal **Antivirus**. Este informe proporciona funcionalidades de filtrado, búsqueda, paginación y ordenación.

Puede ver el informe **Puntos de conexión incorrectos de Windows 10** mediante los pasos siguientes:

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione la pestaña **Seguridad de los puntos de conexión** > **Antivirus** > **Puntos de conexión incorrectos de Windows 10**.

Para obtener información sobre las acciones que puede llevar a cabo con este informe, vea el informe Acciones en masa para dispositivos.

Informe Malware activo de Windows 10 (operativo)

El informe **Malware activo de Windows 10** proporciona datos para identificar los dispositivos con problemas de malware y ayudar a solucionar los problemas. Los datos que se encuentran en este informe son oportunos y anuncian el dispositivo incorrecto, el nombre de usuario y la gravedad. El informe está disponible como una pestaña dentro de la carga de trabajo principal **Antivirus**. Este informe proporciona funcionalidades de filtrado, búsqueda, paginación y ordenación.

Puede ver el informe **Malware activo de Windows 10** mediante los pasos siguientes:

1. Inicie sesión en el Centro de administración de Microsoft Endpoint Manager.
2. Seleccione la pestaña **Seguridad de los puntos de conexión** > **Antivirus** > **Malware activo de Windows 10**.

Para obtener información sobre las acciones que puede llevar a cabo con este informe, vea el informe Acciones en masa para dispositivos.

Informe Errores de actualización de características (operativo)

El informe operativo **Errores de actualización de características**, un informe de actualización de Windows, proporciona detalles sobre los errores de los dispositivos que se establecen como destino mediante una directiva de **actualizaciones de características de Windows 10** y que han intentado llevar a cabo una actualización. Los datos que se encuentran en este informe son oportunos e indican un número de dispositivos con errores. Puede explorar en profundidad para solucionar problemas. Este informe proporciona funcionalidades de filtrado, búsqueda, paginación y ordenación.

Para que este informe pueda mostrar datos, debe configurar la *recopilación de datos* para los informes de actualizaciones de características de Windows 10. Para obtener información sobre cómo configurar la recopilación de datos y utilizar este informe para resolver los errores de actualización, consulte Informes de la

directiva de actualizaciones de características de Windows 10.

Para ver el informe **Errores de actualización de características**, siga estos pasos:

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione **Dispositivos** > **Supervisar** > **Errores de actualización de características**.

> **NOTE**
> *Este informe se encuentra en versión preliminar.*

> **IMPORTANT**
> Para obtener una imagen completa del estado de las actualizaciones de características de Windows, use los siguientes informes de actualizaciones de características:
>
> - **Actualizaciones de características de Windows 10 (organizativo)**
> - **Informe Errores de actualización de características (operativo)** *(este informe)*
>
> Juntos, estos informes proporcionan información sobre el estado de actualización y el cumplimiento de los dispositivos Windows en su organización y pueden ayudarle a solucionar problemas con la implementación de la actualización de características.

Informe Errores de asignación (operativo)

El informe operativo **Errores de asignación** ayuda a solucionar errores y conflictos de los perfiles de configuración que se han destinado a los dispositivos. En este informe se mostrará una lista de perfiles de configuración para el inquilino y el número de dispositivos en un estado de error o conflicto. Con esta información, puede explorar en profundidad un perfil para ver una lista de los dispositivos y usuarios en un estado de error relacionados con el perfil. Además, puede explorar todavía más para ver una lista de opciones y detalles de configuración relacionados con la causa del error. Tiene la capacidad de filtrar por tipo y plataforma, ordenar según la columna y buscar por nombre de perfil.

Puede ver el informe **Errores de asignación** mediante los pasos siguientes:

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione **Dispositivos** > **Monitor** > **Errores de asignación**.

> **NOTE**
> *Este informe se encuentra en versión preliminar.*

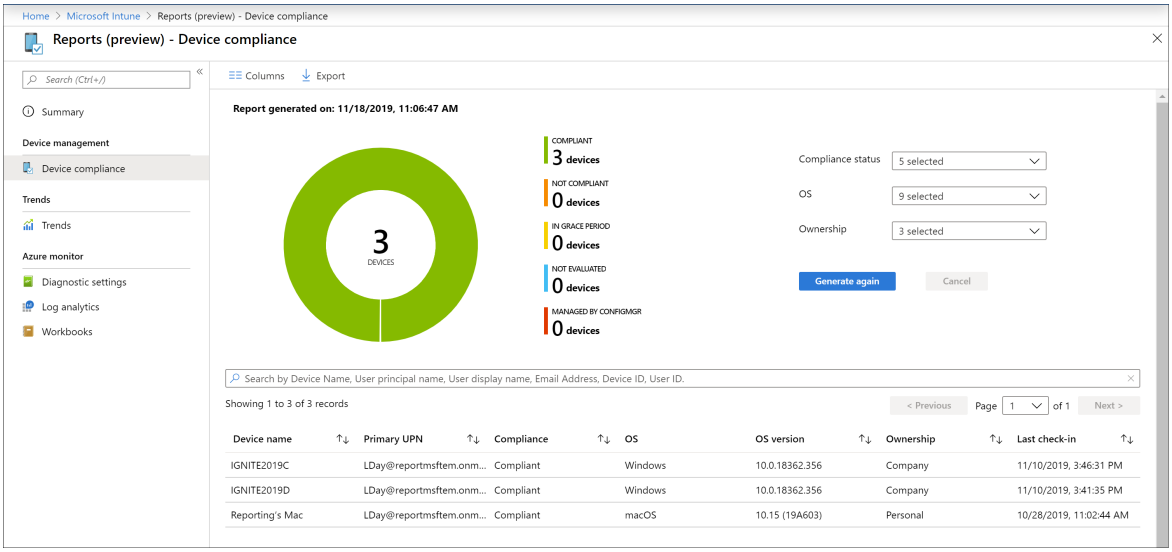
Informe de cumplimiento de dispositivos (organizativo)

Los informes de cumplimiento de dispositivos son generales por naturaleza y proporcionan una vista más tradicional de los datos de informes para identificar las métricas agregadas. Este informe está diseñado para trabajar con grandes conjuntos de datos a fin de obtener una imagen completa del cumplimiento de los dispositivos. Por ejemplo, el informe de cumplimiento de dispositivos muestra todos los estados de cumplimiento de los dispositivos, de modo que se proporciona una vista más amplia de los datos, con independencia del tamaño del conjunto de datos. Este informe muestra el desglose completo de los registros, además de una visualización adecuada de las métricas agregadas. Para generarlo, se le pueden aplicar filtros y seleccionar el botón "Generar informe". Los datos se actualizan para mostrar el estado más reciente con la posibilidad de ver los registros individuales que componen los datos agregados. Al igual que la mayoría de los informes de la nueva plataforma, estos registros son susceptibles de ordenación y búsqueda para centrarse en

la información que necesita.

Para ver un informe generado del estado de un dispositivo, puede seguir estos pasos:

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione la pestaña **Informes** > **Cumplimiento de dispositivos** > **Informes** > **Cumplimiento de dispositivos**.
3. Seleccione los filtros **Estado de cumplimiento**, **OS** y **Propiedad** para refinar el informe.
4. Haga clic en **Generar informe** (o **Generar de nuevo**) para recuperar los datos actuales.



> **NOTE**
>
> Este informe de **Cumplimiento de dispositivos** proporciona una marca de tiempo de la última vez que se generó el informe.

Para ver información relacionada, consulte Exigencia del cumplimiento de Microsoft Defender para punto de conexión con acceso condicional en Intune.

Informe de idoneidad para la administración conjunta (organizativo)

El informe **Idoneidad para la administración conjunta** proporciona una evaluación de idoneidad para los dispositivos que se pueden administrar de manera conjunta. Los dispositivos deben actualizarse a Windows 10 e inscribirse en Azure Active Directory para ser válidos. Algunos dispositivos (como los dispositivos con el sistema operativo Windows Server) no son válidos para la administración conjunta. La administración conjunta permite administrar simultáneamente dispositivos Windows 10 mediante Configuration Manager y Microsoft Intune.

Para ver un informe generado del estado de un dispositivo, puede seguir estos pasos:

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione la pestaña **Informes** > **Cloud attached devices**(Dispositivos conectados a la nube) > **Informes** > **Co-management eligibility** (Idoneidad para la administración conjunta).
3. Haga clic en **Generar informe** (o **Generar de nuevo**) para recuperar los datos actuales.

Para más información, vea ¿Qué es la administración conjunta?

Informe Estado del agente de antivirus (organizativo)

El informe **Estado del agente de antivirus** proporciona el estado del agente de los dispositivos de la organización.

El informe está disponible en la carga de trabajo principal **Antivirus de Microsoft Defender** y proporciona funciones de filtrado, búsqueda, paginación y ordenación. Los datos de este informe son puntuales y muestran los detalles siguientes:

- Si un dispositivo tiene protección en tiempo real o de red, así como el estado
- El estado de Windows Defender
- Si está habilitada la protección contra alteraciones
- Si el dispositivo es una máquina virtual o un dispositivo físico.
- Se destacan el dispositivo incorrecto, el nombre de usuario y la gravedad.

En este informe, las visualizaciones de datos se muestran en forma de gráfico circular con un desglose del recuento de estados de agente en todos los dispositivos y se incluyen las acciones remotas.

Puede ver el informe **Estado del agente de antivirus** mediante los pasos siguientes:

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione **Informes** > **Antivirus de Microsoft Defender** para abrir la vista de informes predeterminada, que es la página **Resumen**. La página Resumen muestra los detalles agregados de los informes del antivirus, admite una *actualización* y refleja los datos encontrados en el informe Estado del agente de antivirus.
3. Seleccione la pestaña **Informes** > **Estado del agente de antivirus** para abrir el informe.
4. Haga clic en **Generar informe** (o **Generar de nuevo**) para recuperar los datos actuales.

La información de este informe se basa en los detalles disponibles en el CSP de Defender, que se documenta en la documentación de administración de cliente de Windows.

Los informes adicionales del Antivirus de Microsoft Defender incluyen:

- Informe de malware detectado, un informe de la organización que se detalla en este artículo.
- Informes de directivas antivirus, que están disponibles en el nodo Antivirus en Seguridad de los puntos de conexión del Centro de administración de Microsoft Endpoint Manager.

Informe de malware detectado (organizativo)

El informe **Malware detectado** proporciona el estado de malware de los dispositivos de la organización. Este informe muestra el número de dispositivos con malware detectado, así como detalles de malware. Los datos que se encuentran en este informe son oportunos e indican el nombre del dispositivo y la gravedad, así como otros detalles relacionados con el malware. En este informe se muestra un gráfico circular para el recuento de dispositivos en cada estado de malware. El informe está disponible en la carga de trabajo principal **Antivirus de Microsoft Defender**. Este informe proporciona también funcionalidades de filtrado, búsqueda, paginación y ordenación.

Puede ver el informe **Malware detectado** mediante los pasos siguientes:

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione **Informes** > **Antivirus de Microsoft Defender** para abrir la vista de informes predeterminada, que es la página Resumen. La página Resumen muestra los detalles agregados de los informes del antivirus, admite una *actualización* y refleja los datos encontrados en el informe Estado del agente de antivirus.
3. Seleccione la pestaña **Informes** > **Malware detectado** para abrir el informe.
4. Haga clic en **Generar informe** (o **Generar de nuevo**) para recuperar los datos actuales.

La información de este informe se basa en los detalles disponibles en el CSP de Defender, que se documenta en la documentación de administración de cliente de Windows.

Los informes adicionales del Antivirus de Microsoft Defender incluyen:

- Informe Estado del agente de antivirus, un informe organizativo que se detalla en este artículo.
- Informes de directivas antivirus, que están disponibles en el nodo Antivirus en Seguridad de los puntos de conexión del Centro de administración de Microsoft Endpoint Manager.

Actualizaciones de características de Windows 10 (organizativo)

El informe **Actualizaciones de características de Windows 10**, un informe de actualización de Windows, proporciona una visión general del cumplimiento de los dispositivos que se establecen como destino mediante una directiva de **actualizaciones de características de Windows 10**. Este informe proporciona la situación de actualización basada en el estado de actualización. También puede ver detalles específicos de la actualización del dispositivo. Los datos que se encuentran en estos informes son oportunos e indican el nombre del dispositivo y el estado, así como otros detalles relacionados con la actualización. Hay disponible un informe de resumen en la carga de trabajo **Actualizaciones de Windows**. Este informe proporciona también funcionalidades de filtrado, búsqueda, paginación y ordenación.

Para obtener información sobre cómo utilizar este informe para resolver los errores de actualización, consulte Informes de la directiva de actualizaciones de características de Windows 10.

Puede ver el informe **Actualizaciones de características de Windows 10** mediante los pasos siguientes:

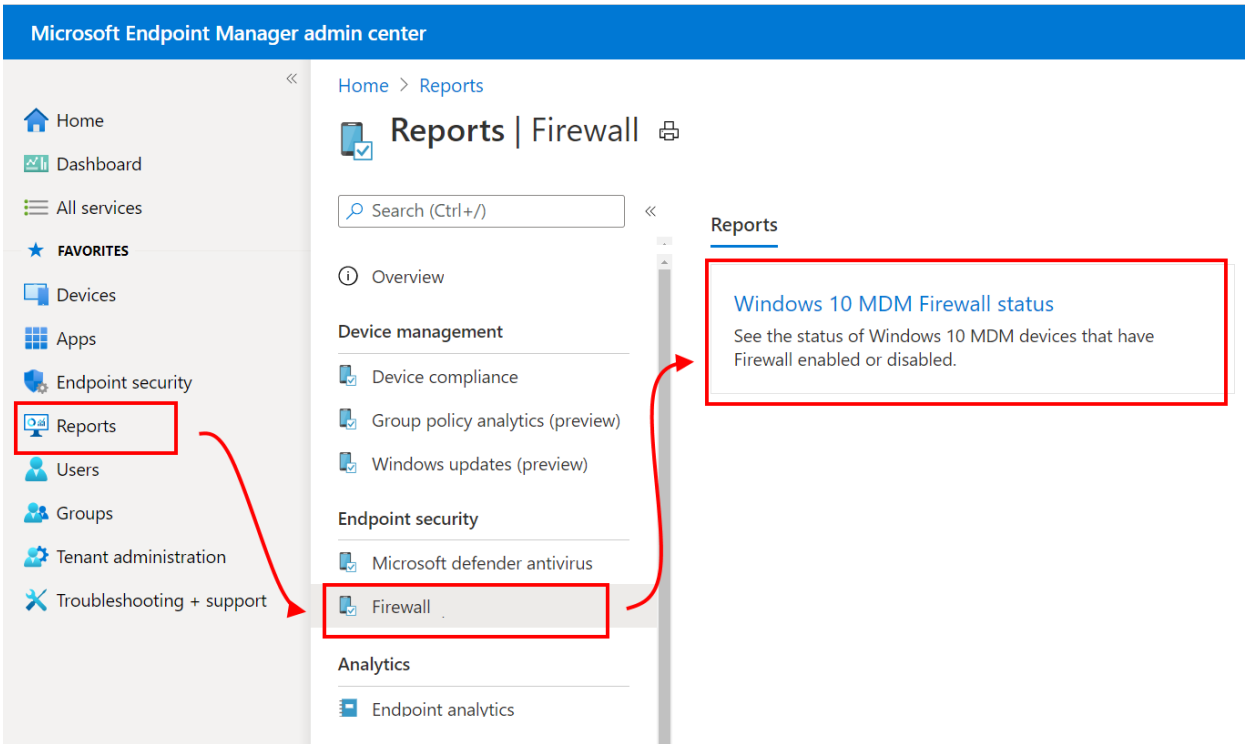
1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione **Informes** > **Actualizaciones de Windows** para ver el informe de resumen.
3. Seleccione la pestaña **Informes** y haga clic en **informe de actualización de características de Windows** para ver el informe **Actualizaciones de características de Windows 10**.
4. Seleccione los filtros **Update aggregated status** (Actualizar estado agregado) y **Ownership** (Propiedad) para restringir el informe.
5. Haga clic en **Generar informe** (o **Generar de nuevo**) para recuperar los datos actuales.

> **IMPORTANT**
>
> Para obtener una imagen completa del estado de las actualizaciones de características de Windows, use los siguientes informes de actualizaciones de características:
>
> - Actualizaciones de características de Windows 10 (organizativo) *(este informe)*
> - Informe Errores de actualización de características (operativo)
>
> Juntos, estos informes proporcionan información sobre el estado de actualización y el cumplimiento de los dispositivos Windows en su organización y pueden ayudarle a solucionar problemas con la implementación de la actualización de características.

Estado del firewall de los dispositivos MDM para Windows 10 (organizativo)

En versión preliminar pública. Este informe también se describe en la directiva de firewall de seguridad de los puntos de conexión junto con el informe Dispositivos MDM para Windows 10 con el firewall desactivado, que solo está disponible en el nodo de seguridad de los puntos de conexión.

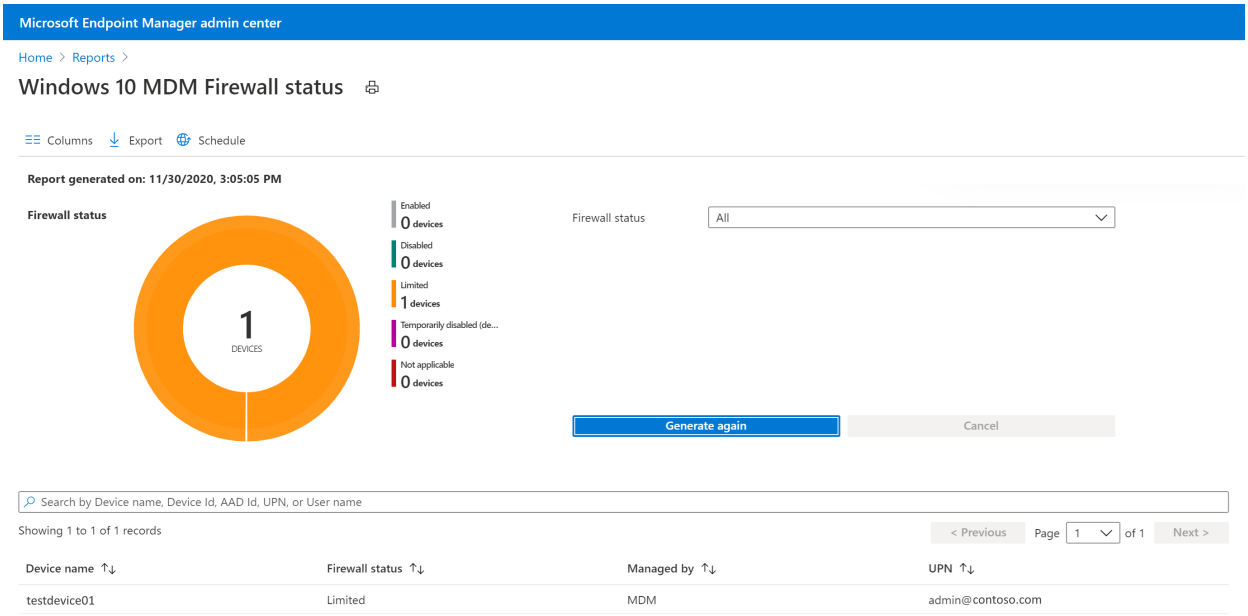
El informe **Estado del firewall de los dispositivos MDM para Windows 10** proporciona una vista de alto nivel del estado de firewall para los dispositivos administrados. Para ver este informe, abra el Centro de administración de Microsoft Endpoint Manager y, luego, vaya a **Informes** > **Firewall** > **Estado del firewall de los dispositivos MDM para Windows 10**.



Los datos se notifican a través del CSP de DeviceStatus de Windows e informan sobre el estado del firewall de los dispositivos administrados. Puede filtrar las devoluciones de este informe mediante una o varias de las categorías de detalles de estado.

Los detalles de estado incluyen:

- **Habilitado**: el firewall está habilitado y genera informes correctamente.
- **Deshabilitado**: el firewall está deshabilitado.
- **Limitado**: el firewall no supervisa todas las redes o algunas reglas están desactivadas.
- **Temporalmente deshabilitado**: de manera temporal, el firewall no supervisa todas las redes.
- **No aplicable**: el dispositivo no permite generar informes del firewall.



Informe de cargas de trabajo de administración conjunta (organizativo)

El informe de **cargas de trabajo de administración conjunta** proporciona un informe de los dispositivos que se administran de forma conjunta en la actualidad. Para cada dispositivo, el informe muestra la entidad de administración para las cargas de trabajo de cumplimiento, acceso a los recursos, configuración de dispositivos, Windows Update para empresas, Endpoint Protection, aplicaciones modernas y aplicaciones de Office. El informe también agrega todas las cargas de trabajo del dispositivo para mostrar un resumen de la administración total de la carga de trabajo. La administración conjunta permite administrar simultáneamente dispositivos Windows 10 mediante Configuration Manager y Microsoft Intune.

Para ver un informe generado del estado de un dispositivo, puede seguir estos pasos:

1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione la pestaña **Informes** > **Cloud attached devices** (Dispositivos conectados a la nube) > **Informes** > **Co-Managed Workloads** (Cargas de trabajo de administración conjunta).
3. Haga clic en **Generar informe** (o **Generar de nuevo**) para recuperar los datos actuales.

Para más información, vea ¿Qué es la administración conjunta?

Informe de tendencias de cumplimiento de dispositivos (histórico)

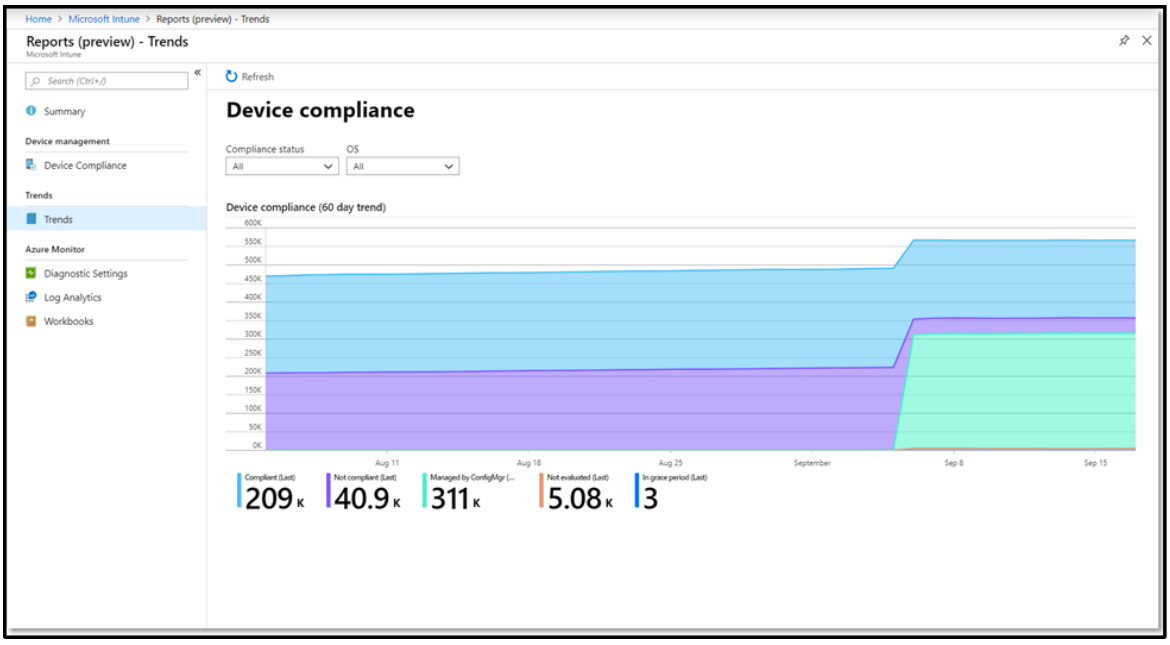
Los administradores y los arquitectos usarán probablemente los informes de tendencias de cumplimiento de dispositivos para identificar las tendencias a largo plazo en el cumplimiento de los dispositivos. Los datos agregados se muestran durante un período de tiempo y resultan útiles para tomar decisiones de inversión futuras, impulsar la mejora de los procesos o promover la investigación de posibles anomalías. También se pueden aplicar filtros para ver tendencias específicas. Los datos proporcionados por este informe son una instantánea del estado actual del inquilino (casi en tiempo real).

Un informe de tendencias de cumplimiento puede mostrar la tendencia de los estados de cumplimiento de los dispositivos durante un período de tiempo. Puede identificar dónde se han producido los picos de cumplimiento y centrar su tiempo y esfuerzo en consecuencia.

Para ver el informe de **Tendencias de cumplimiento de dispositivos**, siga estos pasos:

1. Inicie sesión en el Centro de administración de Microsoft Endpoint Manager.

2. Seleccione la pestaña **Informes** > **Cumplimiento de dispositivos** > **Informes** > **Tendencias de cumplimiento de dispositivos** para ver el cumplimiento de los dispositivos durante una tendencia de 60 días.



Informes de integración de Azure Monitor (especialista)

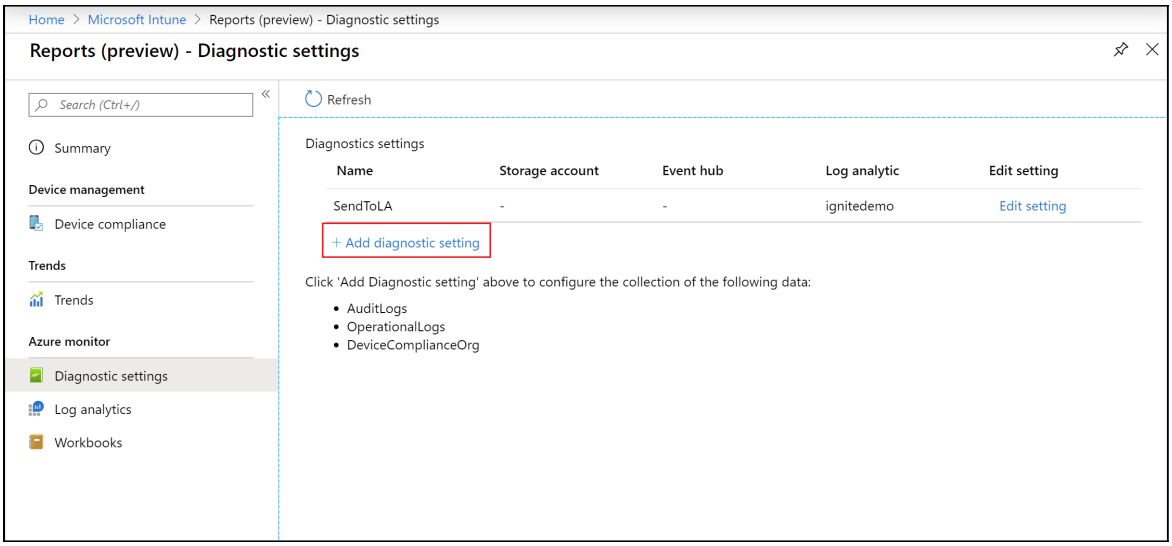
Puede personalizar sus propios informes para obtener los datos que desee. Los datos de los informes estarán disponibles opcionalmente a través de Azure Monitor mediante Log Analytics y los libros de Azure Monitor. Estas soluciones le permiten crear consultas personalizadas, configurar alertas y hacer que los paneles muestren los datos de cumplimiento de dispositivos de la manera deseada. Además, puede conservar los registros de actividad en su cuenta de almacenamiento de Azure, integrarlos con los informes mediante herramientas de administración de eventos e información de seguridad (SIEM) y correlacionar los informes con los registros de actividad de Azure AD. Además de para importar paneles, los libros de Azure Monitor se pueden usar cuando es necesario generar informes personalizados.

> **NOTE**
> La funcionalidad de informes complejos requiere una suscripción a Azure.

Un ejemplo de informe especializado podría correlacionar un conjunto de detalles del dispositivo, incluidos los datos de propiedad, con los datos de cumplimiento en un informe personalizado. Luego, este informe personalizado podría mostrarse en un panel existente en el portal de Azure Active Directory.

Para crear y ver informes personalizados, siga estos pasos:

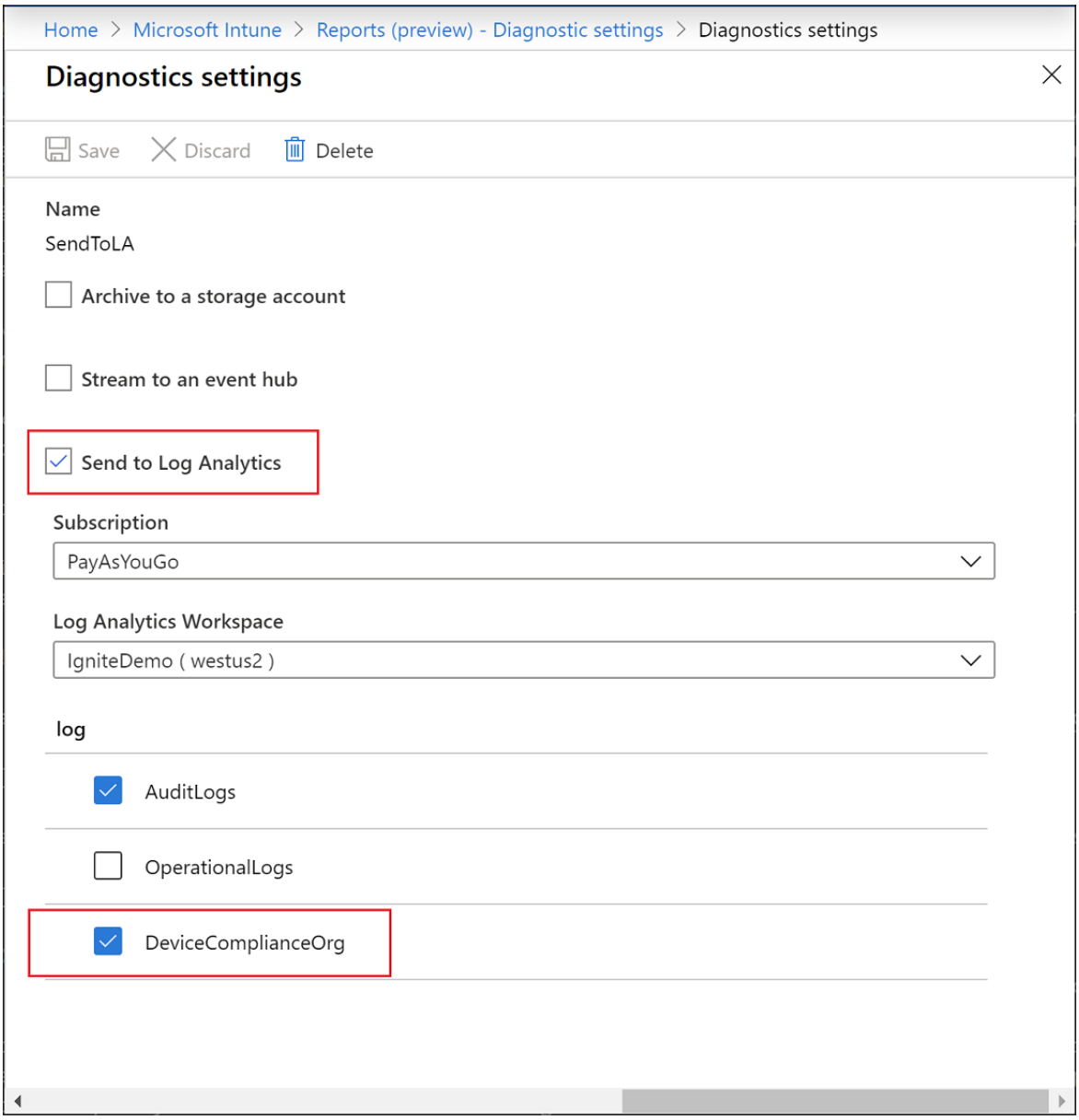
1. Inicie sesión en el Centro de administración del Administrador de puntos de conexión de Microsoft.
2. Seleccione **Informes** > **Configuración de diagnóstico** y agregue una configuración de diagnóstico.



3. Haga clic en **Agregar configuración de diagnóstico** para mostrar el panel **Configuración de diagnóstico**.

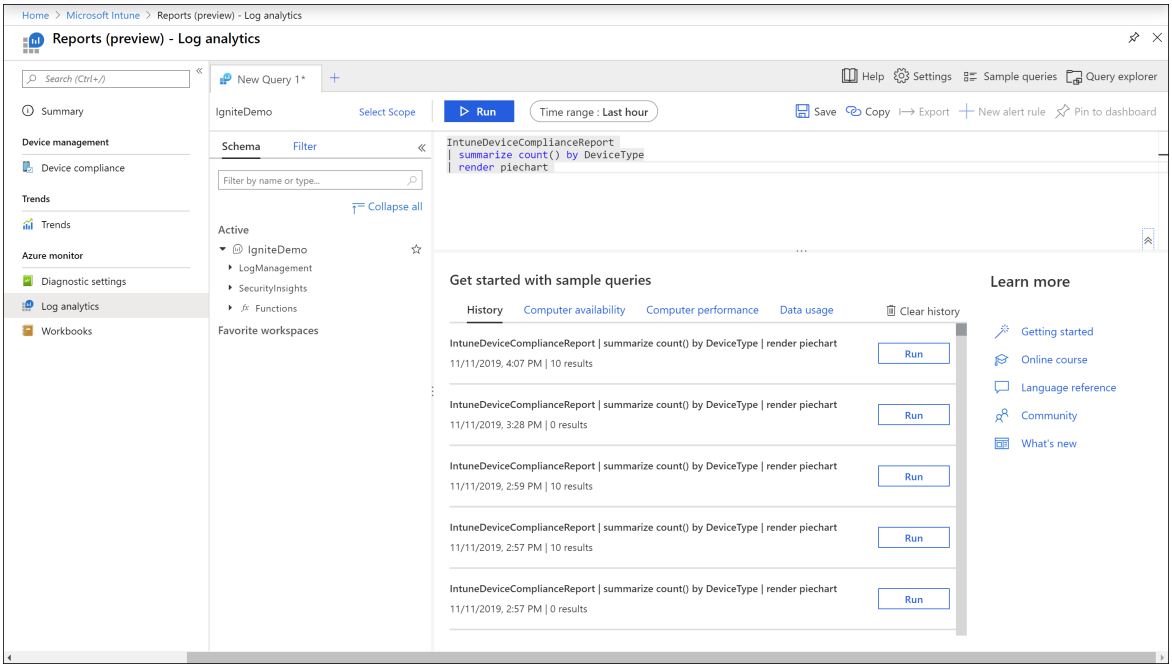
> **NOTE**
> Se requiere una suscripción de Azure para usar esta funcionalidad.

4. Rellene el campo **Nombre** de la configuración de diagnóstico.
5. Seleccione los valores **Enviar a Log Analytics** y **DeviceComplianceOrg**.



6. Haga clic en **Save**(Guardar).

7. Luego, seleccione **Log Analytics** para crear y ejecutar una nueva consulta mediante Log Analytics.



8. Seleccione **Libros** para crear o abrir un informe interactivo mediante libros de Azure Monitor.

Configuración de diagnóstico

Cada recurso de Azure requiere su propia configuración de diagnóstico. La configuración de diagnóstico define lo siguiente para un recurso:

- Categorías de los datos de los registros y las métricas que se envían a los destinos definidos en la configuración. Las categorías disponibles varían para los distintos tipos de recursos.
- Uno o más destinos para enviar los registros. Los destinos actuales incluyen el área de trabajo de Log Analytics, Event Hubs y Azure Storage.
- Directiva de retención para los datos almacenados en Azure Storage.

Una sola configuración de diagnóstico puede definir uno de los destinos. Si desea enviar datos a más de un tipo de destino determinado (por ejemplo, dos áreas de trabajo de Log Analytics diferentes), cree varias configuraciones. Cada recurso puede tener hasta 5 configuraciones de diagnóstico.

Para más información sobre la configuración de diagnóstico, consulte Creación de una configuración de diagnóstico para recopilar registros de plataforma y métricas en Azure.

Log Analytics

Log Analytics es la herramienta principal de Azure Portal para escribir consultas de registro y analizar de forma interactiva los resultados de las consultas. Incluso si una consulta de registro se usa en otro lugar en Azure Monitor, normalmente deberá escribir y probar la consulta primero mediante Log Analytics. Para más información sobre el uso de Log Analytics y la creación de consultas de registro, consulte Introducción a las consultas de registro en Azure Monitor.

Workbooks

Los libros combinan texto, consultas de análisis, métricas de Azure y parámetros en informes interactivos enriquecidos. Otros miembros del equipo con acceso a los mismos recursos de Azure pueden editar los libros. Para más información sobre los libros, consulte Libros de Azure Monitor. Además, puede trabajar con las plantillas de libro y contribuir a ellas. Para más información, consulte Plantillas de libro de Azure Monitor.

Informes de acciones en masa para dispositivos

Los informes **Puntos de conexión incorrectos de Windows 10** y **Malware activo de Windows 10** ofrecen acciones en masa aplicables a los dispositivos seleccionados en cada informe. Para usar una acción en

masa, seleccione una fila que corresponda a cada dispositivo (hasta 100 dispositivos a la vez) y seleccione la acción. Las acciones disponibles son las siguientes:

- **Reiniciar**: esta acción realiza un reinicio de los dispositivos seleccionados.
- **Examen rápido**: esta acción realiza un examen rápido de Windows Defender de los dispositivos seleccionados.
- **Examen completo**: esta acción realiza un examen completo de Windows Defender de los dispositivos seleccionados.

Para obtener más información acerca de la diferencia entre un *examen rápido* y un *análisis completo*, vea Configuración de un análisis rápido o completo programado del Antivirus de Microsoft Defender.

Pasos siguientes

Conozca más sobre las siguientes tecnologías:

- Blog: Plataforma de informes de Microsoft Intune
- Azure Monitor
- ¿Qué es Log Analytics?
- Consultas de registros
- Introducción a los análisis de registros de Azure Monitor
- Libros de Azure Monitor
- Herramientas de administración de eventos e información de seguridad (SIEM)

Exportación de informes de Intune mediante Graph API

14/05/2021 • 3 minutes to read

Todos los informes que se han migrado a la infraestructura de informes de Intune estarán disponibles para la exportación desde una sola API de exportación de nivel superior. Debe usar Microsoft Graph API para hacer la llamada HTTP. Microsoft Graph es una API web de RESTful que le permite acceder a los recursos del servicio Microsoft Cloud.

> **NOTE**
> Para obtener información sobre cómo realizar llamadas API de REST, incluidas las herramientas para interactuar con Microsoft Graph, vea Uso de Microsoft Graph API.

Microsoft Endpoint Manager exportará informes con el siguiente punto de conexión de Microsoft Graph API:

```
https://graph.microsoft.com/beta/deviceManagement/reports/exportJobs
```

Solicitud y respuesta de informes de dispositivos de ejemplo

Al realizar la solicitud, debe proporcionar un parámetro `reportName` como parte del cuerpo de la solicitud basándose en el informe que desea exportar. A continuación, se muestra un ejemplo de una solicitud de exportación del informe **Dispositivos**. Debe usar el método HTTP POST en la solicitud. El método POST se usa para crear un recurso o realizar una acción.

Ejemplo de solicitud

La solicitud siguiente contiene el método HTTP usado en la solicitud a Microsoft Graph.

```
{
    "reportName": "Devices",
    "filter":"(OwnerType eq '1')",
    "localizationType": "LocalizedValuesAsAdditionalColumn",
    "select": [
        "DeviceName",
        "managementAgent",
        "ownerType",
        "complianceState",
        "OS",
        "OSVersion",
        "LastContact",
        "UPN",
        "DeviceId"
    ]
}
```

> **NOTE**
>
> Para recuperar datos, seleccione columnas específicas, como las especificadas en el ejemplo anterior. No cree automatización basada en las columnas predeterminadas de cualquier exportación de informes. Debe crear la automatización para seleccionar explícitamente las columnas pertinentes.

Ejemplo de respuesta

En función de la solicitud POST anterior, Graph devuelve un mensaje de respuesta. El mensaje de respuesta son los datos que solicitó o el resultado de la operación.


```
{
    "@odata.context":
"https://graph.microsoft.com/beta/$metadata#deviceManagement/reports/exportJobs/$entity",
    "id": "Devices_05e62361-783b-4cec-b635-0aed0ecf14a3",
    "reportName": "Devices",
    "filter":"(OwnerType eq '1')",
    "localizationType": "LocalizedValuesAsAdditionalColumn",
    "select": [
        "DeviceName",
        "managementAgent",
        "ownerType",
        "complianceState",
        "OS",
        "OSVersion",
        "LastContact",
        "UPN",
        "DeviceId"
    ],
    "format": "csv",
    "snapshotId": null,
    "status": "notStarted",
    "url": null,
    "requestDateTime": "2020-08-19T03:43:32.1405758Z",
    "expirationDateTime": "0001-01-01T00:00:00Z"
}
```


Después, puede usar el campo `id` para consultar el estado de la exportación con una solicitud GET:

Por ejemplo:

```
https://graph.microsoft.com/beta/deviceManagement/reports/exportJobs('Devices_05e62361-783b-4cec-b635-0aed0ecf14a3')
```

Tendrá que seguir llamando a esta dirección URL hasta que reciba una respuesta con un atributo `status: completed`. Tendrá un aspecto similar al ejemplo siguiente:

```
{
    "@odata.context":
"https://graph.microsoft.com/beta/$metadata#deviceManagement/reports/exportJobs/$entity",
    "id": "Devices_05e62361-783b-4cec-b635-0aed0ecf14a3",
    "reportName": "Devices",
    "filter":"(OwnerType eq '1')",
    "localizationType": "LocalizedValuesAsAdditionalColumn",
    "select": [
        "DeviceName",
        "managementAgent",
        "ownerType",
        "complianceState",
        "OS",
        "OSVersion",
        "LastContact",
        "UPN",
        "DeviceId"
    ],
    "format": "csv",
    "snapshotId": null,
    "status": "completed",
    "url": "https://amsua0702repexpstorage.blob.core.windows.net/cec055a4-97f0-4889-b790-
dc7ad0d12c29/Devices_05e62361-783b-4cec-b635-0aed0ecf14a3.zip?sv=2019-02-
02&sr=b&sig=%2BP%2B4gGiZf0YzlQRuAV5Ji9Beorg4nnOtP%2F7bbFGH7GY%3D&skoid=1db6df02-4c8b-4cb3-8394-
7ac2390642f8&sktid=72f988bf-86f1-41af-91ab-2d7cd011db47&skt=2020-08-19T03%3A48%3A32Z&ske=2020-08-
19T09%3A44%3A23Z&sks=b&skv=2019-02-02&se=2020-08-19T09%3A44%3A23Z&sp=r",
    "requestDateTime": "2020-08-19T03:43:32.1405758Z",
    "expirationDateTime": "2020-08-19T09:44:23.8540289Z"
}
```


Después, puede descargar directamente el archivo CSV comprimido desde el campo `url`.

Parámetros de informe

Hay cuatro parámetros principales que puede enviar en el cuerpo de la solicitud para definir la solicitud de exportación:

- `reportName`: Necesario. Este parámetro es el nombre del informe que desea especificar.
- `filter`: no es necesario para la mayoría de los informes. Tenga en cuenta que el parámetro filter es una cadena.
- `select`: No es necesario. Especifique las columnas del informe que desee. Solo se aceptarán los nombres de columna válidos pertinentes para el informe al que se realiza la llamada.
- `localizationType`: este parámetro controla el comportamiento de localización del informe. Los valores posibles son `LocalizedValuesAsAdditionalColumn` y `ReplaceLocalizableValues`.

Comportamiento de localización

El parámetro `localizationType` controla el comportamiento de localización del informe. Los valores posibles para este parámetro son `LocalizedValuesAsAdditionalColumn` y `ReplaceLocalizableValues`.

Valor de informe LocalizedValuesAsAdditionalColumn

Este valor del parámetro `localizationType` es el predeterminado. Se insertará automáticamente si no se especifica el parámetro `localizationType`. Este valor especifica que Intune proporciona dos columnas para cada columna localizable.

- *valor de enumeración*: la columna *valor de enumeración* contiene una cadena sin formato o un conjunto de números que no cambian, independientemente de la configuración regional. Esta columna estará debajo del nombre de la columna original (vea el ejemplo).

- *valor de cadena localizada*: esta columna será el nombre de la columna original con _loc anexado. Contendrá valores de cadena de lenguaje natural y condicional en función de la configuración regional (vea el ejemplo).

Ejemplo

SO	OS_LOC
1	Windows
1	Windows
1	Windows
2	iOS
3	Android
4	Mac

Valor de informe ReplaceLocalizableValues

El valor de informe ReplaceLocalizableValues solo devolverá una columna por atributo localizado. Esta columna contendrá el nombre de la columna original con los valores localizados.

Ejemplo

SO
Windows
Windows
Windows
iOS
Android
Mac

En el caso de las columnas sin valores localizados, solo se devuelven una columna con el nombre de columna true y los valores de columna true.

> **IMPORTANT**
> El parámetro `localizationType` es relevante para cualquier experiencia de exportación hospedada en la infraestructura de informes de Intune con algunas excepciones. Los tipos de informe `Devices` y `DevicesWithInventory` no respetarán el parámetro `localizationType` debido a los requisitos de compatibilidad heredados.

Pasos siguientes

- Documentación de Microsoft Graph
- Informes de Intune

Informes y propiedades de Intune disponibles mediante Graph API

14/05/2021 • 5 minutes to read

Microsoft Intune proporciona muchos informes en la consola que se pueden exportar mediante Graph API. Microsoft Graph es una API web de RESTful que le permite acceder a los recursos del servicio Microsoft Cloud. Para exportar informes de Intune, debe usar la API Microsoft Graph para realizar un conjunto de llamadas HTTP. Para obtener más información sobre , vea Exportación de informes de Intune mediante Graph API.

> **NOTE**
>
> Los informes de Intune que se han migrado a una nueva infraestructura de informes de Intuneestarán disponibles para exportarse desde una única exportación de nivel superior Graph API.
>
> Para obtener más información sobre cómo realizar llamadas a la API REST, incluidas las herramientas para interactuar con Microsoft Graph, consulte Uso de la API Microsoft Graph REST.

Microsoft Endpoint Manager exportará informes con el siguiente punto de conexión de Microsoft Graph API:

```
https://graph.microsoft.com/beta/deviceManagement/reports/exportJobs
```

La siguiente tabla contiene los posibles valores del parámetro `reportName`. Estos son los informes que están disponibles actualmente para la exportación.

REPORTNAME (PARÁMETRO DE EXPORTACIÓN)	INFORME ASOCIADO EN MICROSOFT ENDPOINT MANAGER
DeviceCompliance	Organización de cumplimiento de dispositivos
DeviceNonCompliance	Dispositivos no compatibles
Dispositivos	Lista de todos los dispositivos
DetectedAppsAggregate	Informe de aplicaciones detectadas
FeatureUpdatePolicyFailuresAggregate	En **Dispositivos** > **Supervisar** > **Failure for feature updates** (Error en las actualizaciones de características)
DeviceFailuresByFeatureUpdatePolicy	En **Dispositivos** > **Supervisar** > **Failure for feature updates** > *(Error en las actualizaciones de características), haga clic en el error*
FeatureUpdateDeviceState	En **Informes** > **Actualizciones de Windows** > **Informes** > **Informe de actualización de características de Windows**
UnhealthyDefenderAgents	En **Seguridad de los puntos de conexión** > **Antivirus** > **Puntos de conexión incorrectos de Windows 10**

REPORTNAME (PARÁMETRO DE EXPORTACIÓN)	INFORME ASOCIADO EN MICROSOFT ENDPOINT MANAGER
DefenderAgents	En **Informes** > **MicrosoftDefender** > **Informes** > **Estado del agente**
ActiveMalware	En **Seguridad de los puntos de conexión** > **Antivirus** > **Malware detectado de Windows 10**
Malware	En **Informes** > **MicrosoftDefender** > **Informes** > **Malware detectado**
AllAppsList	En **Aplicaciones Todas** las > **aplicaciones**
AppInstallStatusAggregate	En **Estado de instalación de** la aplicación > **monitor** de > **aplicaciones**
DeviceInstallStatusByApp	En **Aplicaciones** > **Todas las aplicaciones** Seleccione una aplicación > *individual.*
UserInstallStatusAggregateByApp	En **Aplicaciones** > **Todas las aplicaciones** Seleccione una aplicación > *individual.*

A continuación, se describe cada uno de los informes enumerados.

AllAppsList

La tabla siguiente contiene la salida posible al llamar al informe `AllAppsList`:

PROPIEDADES DISPONIBLES
AppIdentifier
Nombre
Publisher
Plataforma
Status
Tipo
Versión
Descripción
Desarrollador
FeaturedApp
Notas
Propietario

PROPIEDADES DISPONIBLES
DateCreated
LastModified
ExpirationDate
MoreInformationURL
PrivacyInformationURL
StoreURL
asignados

No hay ningún filtro para este informe.

AppInstallStatusAggregate

La tabla siguiente contiene la salida posible al llamar al informe `AppInstallStatusAggregate`:

PROPIEDADES DISPONIBLES
ApplicationId
DisplayName
Publisher
Plataforma
Platform_loc
AppVersion
InstalledDeviceCount
InstalledUserCount
FailedDeviceCount
FailedUserCount
PendingInstallDeviceCount
PendingInstallUserCount
NotApplicableDeviceCount
NotApplicableUserCount

PROPIEDADES DISPONIBLES
NotInstalledDeviceCount
NotInstalledUserCount
FailedDevicePercentage

Puede elegir filtrar la salida del informe `AppInstallStatusAggregate` en función de las columnas siguientes:

- `Platform`
- `FailedDevicePercentage`

DeviceInstallStatusByApp

La tabla siguiente contiene la salida posible al llamar al informe `DeviceInstallStatusByApp`:

PROPIEDADES DISPONIBLES
DeviceName
UserPrincipalName
Plataforma
AppVersion
deviceId
AssignmentFilterIdsExist
LastModifiedDateTime
AppInstallState
AppInstallState_loc
AppInstallStateDetails
AppInstallStateDetails_loc
HexErrorCode

Puede elegir filtrar la salida del informe `AppInstallStatusAggregate` en función de las columnas siguientes:

- `ApplicationId`
- `AppInstallState`
- `HexErrorCode` (Se usa como Código de error)

UserInstallStatusAggregateByApp

La tabla siguiente contiene la salida posible al llamar al informe `UserInstallStatusAggregateByApp`:

PROPIEDADES DISPONIBLES
UserName
UserPrincipalName
FailedCount
InstalledCount
PendingInstallCount
NotInstalledCount
NotApplicableCount

No hay ningún filtro para este informe.

Informe DeviceCompliance

La tabla siguiente contiene la salida posible al llamar al informe `DeviceCompliance`:

PROPIEDADES DISPONIBLES
DeviceId
IntuneDeviceId
AadDeviceId
DeviceName
DeviceType
OSDescription
OSVersion
OwnerType
LastContact
InGracePeriodUntil
IMEI
SerialNumber
ManagementAgents
PrimaryUser

PROPIEDADES DISPONIBLES
UserId
UPN (Nombre principal de usuario)
UserEmail
UserName
DeviceHealthThreatLevel
RetireAfterDatetime
PartnerDeviceId
ComplianceState
SO

Puede elegir filtrar la salida del informe `DeviceCompliance` en función de las columnas siguientes:

- `ComplianceState`
- `OS`
- `OwnerType`
- `DeviceType`

DeviceNonCompliance report

La tabla siguiente contiene la salida posible al llamar al informe `DeviceNonCompliance`:

PROPIEDADES DISPONIBLES
DeviceId
IntuneDeviceId
AadDeviceId
DeviceName
DeviceType
OSDescription
OSVersion
OwnerType
LastContact
InGracePeriodUntil

PROPIEDADES DISPONIBLES
IMEI
SerialNumber
ManagementAgents
PrimaryUser
UserId
UPN (Nombre principal de usuario)
UserEmail
UserName
DeviceHealthThreatLevel
RetireAfterDatetime
PartnerDeviceId
ComplianceState
SO

Puede elegir filtrar la salida del informe `DeviceNonCompliance` en función de las columnas siguientes:

- `OS`
- `OwnerType`
- `DeviceType`
- `UserId`
- `ComplianceState`

Informe de dispositivos

La tabla siguiente contiene la salida posible al llamar al informe `Devices`:

PROPIEDADES DISPONIBLES
DeviceId
DeviceName
DeviceType
ClientRegistrationStatus
OwnerType

PROPIEDADES DISPONIBLES
CreatedDate
LastContact
ManagementAgents
ManagementState
ReferenceId
CategoryId
EnrollmentType
CertExpirationDate
MDMStatus
OSVersion
GraphDeviceIsManaged
EasID
SerialNumber
EnrolledByUser
Fabricante
Modelado
OSDescription
IsManaged
EasActivationStatus
IMEI
EasLastSyncSuccessUtc
EasStateReason
EasAccessState
EncryptionStatus
SupervisedStatus

PROPIEDADES DISPONIBLES
PhoneNumberE164Format
InGracePeriodUntil
AndroidPatchLevel
WifiMacAddress
SCCMCoManagementFeatures
MEID
SubscriberCarrierNetwork
StorageTotal
StorageFree
ManagedDeviceName
LastLoggedOnUserUPN
MDMWinsOverGPStartTime
StagedDeviceType
UserApprovedEnrollment
ExtendedProperties
EntitySource
PrimaryUser
nombreDeCategoría
UserId
UPN (Nombre principal de usuario)
UserEmail
UserName
RetireAfterDatetime
PartnerDeviceId
HasUnlockToken

PROPIEDADES DISPONIBLES
CompliantState
ManagedBy
Propiedad
DeviceState
DeviceRegistrationState
SupervisedStatusString
EncryptionStatusString
SO
SkuFamily
JoinType
PhoneNumber
JailBroken
EasActivationStatusString

Puede elegir filtrar la salida del informe `Devices` en función de las columnas siguientes:

- `OwnerType`
- `DeviceType`
- `ManagementAgents`
- `CategoryName`
- `ManagementState`
- `CompliantState`
- `JailBroken`
- `LastContact`
- `CreatedDate`
- `EnrollmentType`

Informe DetectedAppsAggregate

La tabla siguiente contiene la salida posible al llamar al informe `DetectedAppsAggregate`:

PROPIEDADES DISPONIBLES
ApplicationKey
ApplicationName

PROPIEDADES DISPONIBLES
ApplicationVersion
DeviceCount
BundleSize

Puede elegir filtrar la salida del informe `DetectedAppsAggregate` en función de la columna siguiente:

- `ApplicationName`

Informe FeatureUpdatePolicyFailuresAggregate

La tabla siguiente contiene la salida posible al llamar al informe `FeatureUpdatePolicyFailuresAggregate`:

PROPIEDADES DISPONIBLES
PolicyId
PolicyName
FeatureUpdateVersion
NumberOfDevicesWithErrors

No puede filtrar este informe.

Informe DeviceFailuresByFeatureUpdatePolicy

La tabla siguiente contiene la salida posible al llamar al informe `DeviceFailuresByFeatureUpdatePolicy`:

PROPIEDADES DISPONIBLES
PolicyId
PolicyName
FeatureUpdateVersion
DeviceId
AADDeviceId
AlertId
EventDateTimeUTC
LastUpdatedAlertStatusDateTimeUTC
AlertType
AlertStatus

PROPIEDADES DISPONIBLES
AlertClassification
WindowsUpdateVersion
Compilar
AlertMessage
AlertMessageDescription
AlertMessageData
Win32ErrorCode
RecommendedAction
ExtendedRecommendedAction
StartDateTimeUTC
ResolvedDateTimeUTC
DeviceName
UPN (Nombre principal de usuario)

Puede elegir filtrar la salida del informe `DeviceFailuresByFeatureUpdatePolicy` en función de las columnas siguientes:

- `PolicyId` **(Obligatorio)**
- `AlertMessage`
- `RecommendedAction`
- `WindowsUpdateVersion`

Informe FeatureUpdateDeviceState

La tabla siguiente contiene la salida posible al llamar al informe `FeatureUpdateDeviceState`:

PROPIEDADES DISPONIBLES
PolicyId
PolicyName
FeatureUpdateVersion
DeviceId
AADDeviceId

PROPIEDADES DISPONIBLES
PartnerPolicyId
EventDateTimeUTC
LastSuccessfulDeviceUpdateStatus
LastSuccessfulDeviceUpdateSubstatus
LastSuccessfulDeviceUpdateStatusEventDateTimeUTC
CurrentDeviceUpdateStatus
CurrentDeviceUpdateSubstatus
CurrentDeviceUpdateStatusEventDateTimeUTC
LatestAlertMessage
LatestAlertMessageDescription
LatestAlertRecommendedAction
LatestAlertExtendedRecommendedAction
UpdateCategory
WindowsUpdateVersion
LastWUScanTimeUTC
Compilar
DeviceName
OwnerType
UPN (Nombre principal de usuario)
AggregateState

Puede elegir filtrar la salida del informe `FeatureUpdateDeviceState` en función de las columnas siguientes:

- `PolicyId` **(Obligatorio)**
- `AggregateState`
- `LatestAlertMessage`
- `OwnerType`

Informes UnhealthyDefenderAgents y DefenderAgents

Los informes `UnhealthyDefenderAgents` y `DefenderAgents` son dos informes distintos que tienen el mismo conjunto de propiedades y filtros. La tabla siguiente contiene la salida posible al llamar a los informes

`UnhealthyDefenderAgents` o `DefenderAgents`:

COLUMNAS DISPONIBLES
DeviceId
DeviceName
DeviceState
PendingFullScan
PendingReboot
PendingManualSteps
PendingOfflineScan
CriticalFailure
MalwareProtectionEnabled
RealTimeProtectionEnabled
NetworkInspectionSystemEnabled
SignatureUpdateOverdue
QuickScanOverdue
FullScanOverdue
RebootRequired
FullScanRequired
EngineVersion
SignatureVersion
AntiMalwareVersion
LastQuickScanDateTime
LastFullScanDateTime
LastQuickScanSignatureVersion
LastFullScanSignatureVersion
LastReportedDateTime

COLUMNAS DISPONIBLES
UPN (Nombre principal de usuario)
UserEmail
UserName

Puede elegir filtrar la salida de los informes `UnhealthyDefenderAgents` y `DefenderAgents` en función de las columnas siguientes:

- `DeviceState`
- `SignatureUpdateOverdue`
- `MalwareProtectionEnabled`
- `RealTimeProtectionEnabled`
- `NetworkInspectionSystemEnabled`

Informes ActiveMalware y Malware

Los informes `ActiveMalware` y `Malware` son dos informes distintos que tienen el mismo conjunto de propiedades y filtros. La tabla siguiente contiene la salida posible al llamar a los informes `ActiveMalware` o `Malware`:

COLUMNAS DISPONIBLES
DeviceId
DeviceName
MalwareId
MalwareName
AdditionalInformationUrl
Gravedad
MalwareCategory
ExecutionState
Estado
InitialDetectionDateTime
LastStateChangeDateTime
DetectionCount
UPN (Nombre principal de usuario)
UserEmail

COLUMNAS DISPONIBLES
UserName

Puede elegir filtrar la salida de los informes `ActiveMalware` y `Malware` en función de las columnas siguientes:

- `Severity`
- `ExecutionState`
- `State`

Pasos siguientes

- Documentación de Microsoft Graph
- Informes de Intune

Uso de registros de auditoría para realizar un seguimiento y supervisar eventos en Microsoft Intune

14/05/2021 • 2 minutes to read

Los registros de auditoría incluyen un registro de las actividades que generan un cambio en Microsoft Intune. Las acciones de creación, actualización (edición), eliminación, asignación y remotas crean eventos de auditoría que los administradores pueden revisar para la mayoría de las cargas de trabajo de Intune. La auditoría está habilitada de forma predeterminada para todos los clientes. No se puede deshabilitar.

> **NOTE**
> Los eventos de auditoría comenzaron a registrarse en la versión de características de diciembre de 2017. Los eventos anteriores no están disponibles.

¿Quién puede tener acceso a los datos?

Los usuarios con los siguientes permisos pueden revisar los registros de auditoría:

- Administrador global
- Administrador del servicio de Intune
- Administradores asignados a un rol de Intune con los permisos **Datos de auditoría** - **Lectura**

Registros de auditoría para cargas de trabajo de Intune

Puede revisar los registros de auditoría en el grupo de supervisión para cada carga de trabajo de Intune:

1. Inicie sesión en el Centro de administración de Microsoft Endpoint Manager.
2. Seleccione **Administración de inquilinos** > **Registros de auditoría**.
3. Para filtrar los resultados, seleccione **Filtro** y restrinja los resultados con las opciones siguientes.
   - **Categoría**: como, por ejemplo, **Cumplimiento**, **Dispositivo** y **Rol**.
   - **Actividad**: las opciones que se muestran aquí están restringidas por la opción elegida en **Categoría**.
   - **Intervalo de fechas**: puede elegir registros para el mes, semana o día anteriores.
4. Seleccione **Aplicar**.
5. Seleccione un elemento de la lista para ver los detalles de la actividad.

Enrutamiento de registros a Azure Monitor

También se pueden enrutar registros de auditoría y registros operativos a Azure Monitor. En **Administración de inquilinos** > **Registros de auditoría**, seleccione **Exportar**:

NOTE

- Para obtener más información sobre esta característica y revisar los requisitos previos para usarla, vea Envío de datos de registro a almacenamiento, centro de eventos o análisis de registros.
- **Iniciado por (actor)** incluye información sobre quién ejecutó la tarea y sobre dónde se ejecutó.

  Por ejemplo, si ejecuta la actividad en Intune en Azure Portal, como **Aplicación** siempre figura **Extensión del portal de Microsoft Intune** y como **Id. de aplicación** siempre se usa el mismo GUID.
- La sección **Destinos** muestra varios destinos y las propiedades que cambiaron.

Uso de API Graph para recuperar eventos de auditoría

Para más información sobre el uso de Graph API para recuperar hasta un año de eventos de auditoría, vea Enumerar auditEvents.

Pasos siguientes

Envío de datos de registro a Storage, Event Hubs o Log Analytics.

Revisión de los registros de protección de aplicaciones cliente.

Envío de datos de registro al almacenamiento, a Event Hubs o a Log Analytics en Intune

27/05/2021 • 11 minutes to read

Microsoft Intune incluye registros integrados que proporcionan información sobre el entorno:

- Los **registros de auditoría** muestran un registro de las actividades que generan un cambio en Intune, incluidas las acciones de creación, actualización (edición), eliminación, asignación y remotas.
- Los **registros operativos** muestran detalles sobre los usuarios y los dispositivos que se han inscrito correctamente o que no se pudieron inscribir, y detalles sobre los dispositivos no compatibles.
- **Los registros organizativos de conformidad de dispositivos** muestran un informe organizativo de la conformidad de dispositivos en Intune y detalles sobre los dispositivos no compatibles.

Estos registros también se pueden enviar a los servicios de Azure Monitor, incluidas las cuentas de almacenamiento, Event Hubs y Log Analytics. En concreto, puede:

- Archivar registros de Intune en una cuenta de almacenamiento de Azure para mantener los datos, o archivarlos durante un tiempo establecido.
- Transmitir registros de Intune a un centro de eventos de Azure para su análisis con herramientas de Administración de eventos e información de seguridad (SIEM) populares, como Splunk y QRadar.
- Integrar los registros de Intune con sus propias soluciones de registro personalizadas transmitiéndolos a un centro de eventos.
- Enviar registros de Intune a Log Analytics para habilitar las visualizaciones enriquecidas, la supervisión y las alertas de los datos conectados.

Estas características forman parte de la característica **Configuración de diagnóstico** en Intune.

En este artículo se muestra cómo usar la característica **Configuración de diagnóstico** para enviar datos de registro a distintos servicios, ofrece ejemplos y estimaciones de costos y responde a algunas preguntas comunes. Una vez que haya habilitado esta característica, los registros se enrutan al servicio Azure Monitor que elija.

> **NOTE**
> Estos registros usan esquemas que pueden cambiar. Para proporcionar comentarios, incluida la información de los informes, vaya a UserVoice.

Requisitos previos

Para usar esta característica, necesita:

- Una suscripción de Azure en la que pueda iniciar sesión. Si no tiene ninguna suscripción de Azure, puede registrarse para obtener una evaluación gratuita.
- Un entorno de Microsoft Intune (inquilino) en Azure
- Un usuario que sea un **administrador global** o **administrador de servicios de Intune** para el inquilino de Intune.

Dependiendo de dónde desea enrutar los datos de registro de auditoría, necesita uno de los siguientes servicios:

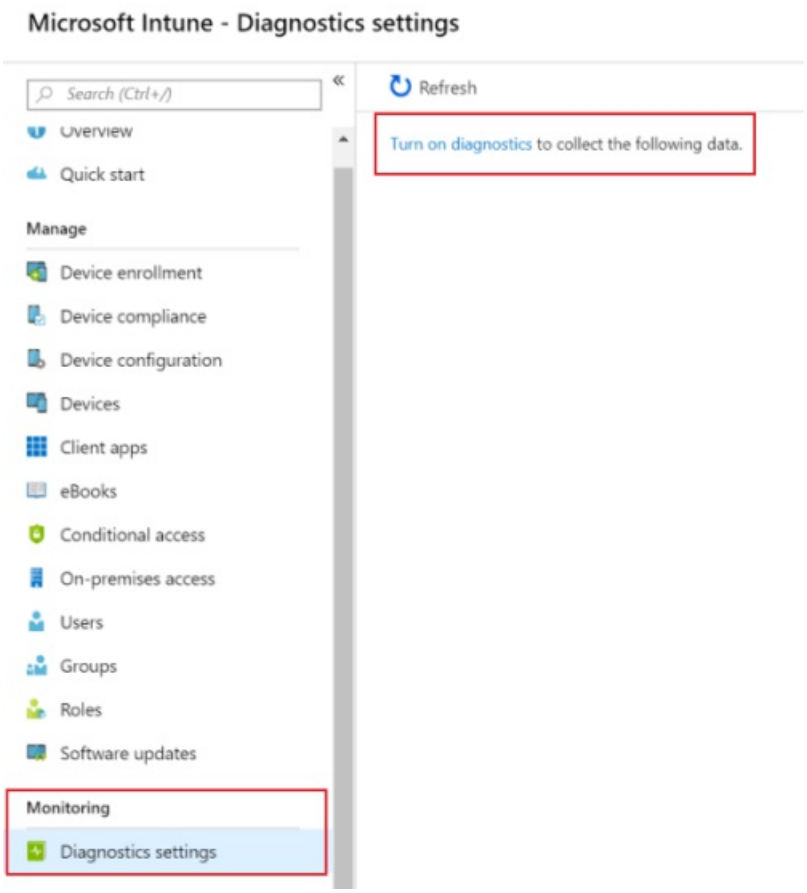
- Una cuenta de almacenamiento de Azure con permisos *ListKeys*. Se recomienda que use una cuenta de

almacenamiento general y no una cuenta de almacenamiento de blobs. Para información sobre los precios de almacenamiento, consulte la calculadora de precios de Azure Storage.

- Un espacio de nombres de Azure Event Hubs para integrar con soluciones de terceros.
- Un espacio de nombres de Azure Log Analytics para enviar registros a Log Analytics.

Envío de registros a Azure Monitor

1. Inicie sesión en el Centro de administración de Microsoft Endpoint Manager.
2. Seleccione **Informes** > **Configuración de diagnóstico**. La primera vez que lo abra, actívelo. De lo contrario, agregue un valor de configuración.



Si no se muestra la suscripción de Azure, vaya a la esquina superior derecha y seleccione la cuenta con sesión > **Cambiar directorio**. Es posible que tenga que escribir la cuenta de suscripción de Azure.

3. Escriba las propiedades siguientes:

   - **Nombre**: escriba un nombre para la configuración de diagnóstico. Esta configuración incluye todas las propiedades que especifique. Por ejemplo, escriba `Route audit logs to storage account`.
   - **Archivar en una cuenta de almacenamiento**: guarda los datos de registro en una cuenta de almacenamiento de Azure. Use esta opción si desea guardar o archivar los datos.
     a. Seleccione esta opción > **Configurar**.
     b. Elija una cuenta de almacenamiento existente en la lista > **Aceptar**.
   - **Transmitir a un centro de eventos**: transmite los registros a un centro de eventos de Azure. Si desea análisis en los datos de registro mediante las herramientas SIEM, como Splunk y QRadar, elija esta opción.
     a. Seleccione esta opción > **Configurar**.
     b. Elija un espacio de nombres de centro de eventos existente y la directiva en la lista > **Aceptar**.
   - **Enviar a Log Analytics**: envía los datos a Azure Log Analytics. Si desea usar las visualizaciones,

supervisión y alertas para los registros, elija esta opción.

a. Seleccione esta opción > **Configurar**.

b. Cree una nueva área de trabajo y escriba los detalles de la misma. O bien, elija un área de trabajo existente en la lista > **Aceptar**.

   El área de trabajo de Azure Log Analytics proporciona más detalles sobre estas configuraciones.

- **LOG** > **AuditLogs**: elija esta opción para enviar los registros de auditoría de Intune a su cuenta de almacenamiento, al centro de eventos o a Log Analytics. Los registros de auditoría muestran el historial de todas las tareas que genera un cambio en Intune, incluido quién lo hizo y cuándo.

  Si decide usar una cuenta de almacenamiento, especifique también cuántos días desea conservar los datos (retención). Para conservar los datos indefinidamente, establezca **Retención (días)** en `0` (cero).

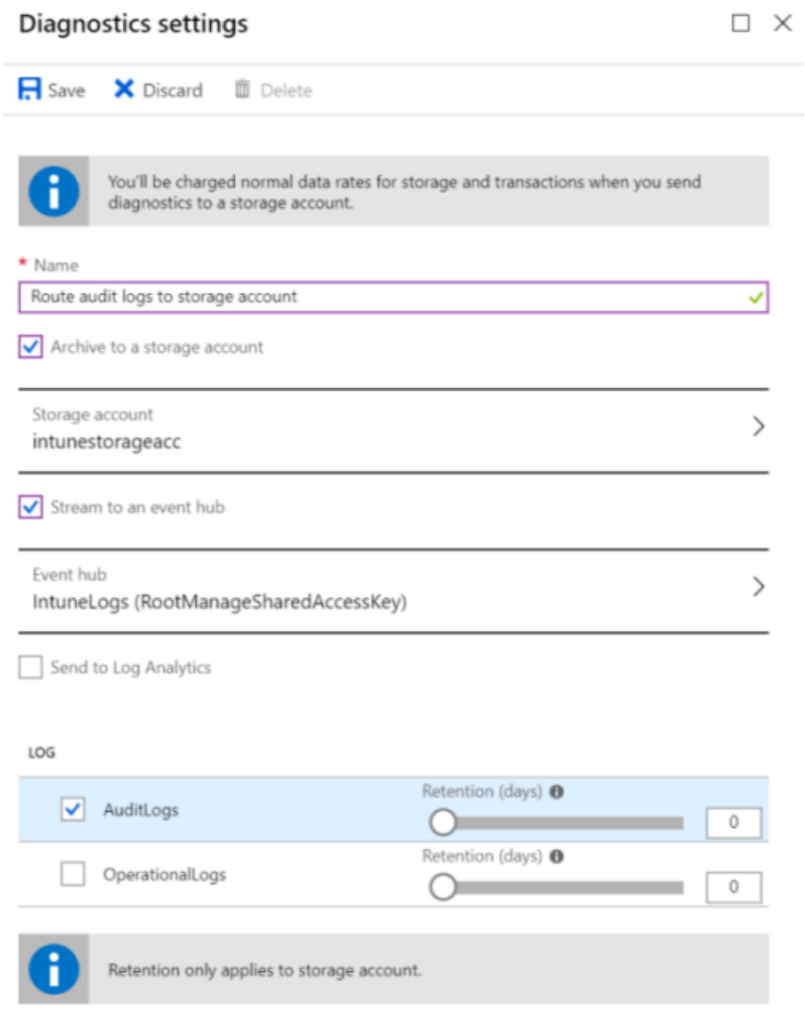
- **LOG** > **OperationalLogs**: los registros operativos muestran el éxito o el error de los usuarios y los dispositivos que se inscriben en Intune, así como detalles sobre los dispositivos no compatibles. Elija esta opción para enviar los registros de inscripción a su cuenta de almacenamiento, al centro de eventos o a Log Analytics.

  Si decide usar una cuenta de almacenamiento, especifique también cuántos días desea conservar los datos (retención). Para conservar los datos indefinidamente, establezca **Retención (días)** en `0` (cero).

- **LOG** > **DeviceComplianceOrg**: Los registros organizativos de conformidad de dispositivos muestran el informe organizativo de la conformidad de dispositivos en Intune y los detalles de los dispositivos no compatibles. Elija esta opción para enviar los registros de cumplimiento a la cuenta de almacenamiento, al centro de eventos o a Log Analytics.

  Si decide usar una cuenta de almacenamiento, especifique también cuántos días desea conservar los datos (retención). Para conservar los datos indefinidamente, establezca **Retención (días)** en `0` (cero).

Cuando termine, la configuración tendrá un aspecto similar a la siguiente configuración:



4. Guarde los cambios mediante **Guardar**. La configuración se mostrará en la lista. Cuando se haya creado, puede cambiar la configuración seleccionando **Editar configuración** > **Guardar**.

Uso de registros de auditoría en Intune

También puede exportar los registros de auditoría en otras partes de Intune, incluida la inscripción, el cumplimiento, la configuración, los dispositivos, las aplicaciones cliente y mucho más.

Para más información, vea Uso de registros de auditoría para realizar el seguimiento de los eventos y supervisarlos. Puede elegir dónde enviar los registros de auditoría, como se describe en Envío de registros a Azure Monitor (en este artículo).

Propiedades del registro de auditoría

En el registro de auditoría, puede encontrar propiedades que tengan valores específicos. En la siguiente tabla se proporciona esta información detallada.

PROPIEDAD	DESCRIPCIÓN DE LA PROPIEDAD	VALORES
ActivityType	La acción que realiza el administrador.	Create, Delete, Patch, Action, SetReference, RemoveReference, Get, Search
ActorType	Persona que realiza la acción.	Unknown = 0, ItPro, IW, System, Partner, Application, GuestUser

PROPIEDAD	DESCRIPCIÓN DE LA PROPIEDAD	VALORES
Categoría	Panel en el que ha tenido lugar la acción.	Other = 0, Enrollment = 1, Compliance = 2, DeviceConfiguration = 3, Device = 4, Application = 5, EBookManagement = 6, ConditionalAccess= 7, OnPremiseAccess= 8, Role = 9, SoftwareUpdates =10, DeviceSetupConfiguration = 11, DeviceIntent = 12, DeviceIntentSetting = 13, DeviceSecurity = 14, GroupPolicyAnalytics = 15
ActivityResult	Indica si la acción se ha realizado correctamente o no.	Success = 1

Consideraciones sobre el costo

Si ya tiene una licencia de Microsoft Intune, necesita una suscripción de Azure para configurar la cuenta de almacenamiento y el centro de eventos. La suscripción de Azure normalmente es gratuita. Sin embargo, tiene que pagar por usar recursos de Azure, incluida la cuenta de almacenamiento para archivado y el centro de eventos para la transmisión. La cantidad de datos y los costos varían según el tamaño del inquilino.

Tamaño de almacenamiento para los registros de actividad

Cada evento del registro de auditoría usa 2 KB de almacenamiento de datos aproximadamente. Para un inquilino con 100 000 usuarios, puede que tenga aproximadamente 1,5 millones de eventos al día. Puede necesitar unos 3 GB de almacenamiento de datos por día. Dado que suelen realizarse operaciones de escritura en lotes de cinco minutos, puede esperar aproximadamente 9000 operaciones de este tipo al mes.

En las siguientes tablas se muestra una estimación de costos según el tamaño del inquilino. También incluye una cuenta de almacenamiento de uso general v2 en la región Oeste de EE. UU. durante al menos un año de retención de datos. Para obtener una estimación para el volumen de datos que espera para sus registros, use la calculadora de precios de Azure Storage.

Registro de auditoría con 100 000 usuarios

CATEGORY	VALUE
Eventos por día	1,5 millones
Volumen estimado de datos al mes	90 GB
Costo estimado al mes (USD)	1,93 USD
Costo estimado al año (USD)	23,12 USD

Registro de auditoría con 1000 usuarios

CATEGORY	VALUE
Eventos por día	15,000
Volumen estimado de datos al mes	900 MB

CATEGORY	VALUE
Costo estimado al mes (USD)	0,02 USD
Costo estimado al año (USD)	0,24 USD

Mensajes del centro de eventos para los registros de actividad

Los eventos normalmente se realizan por lotes en intervalos de cinco minutos y se envían como un solo mensaje con todos los eventos dentro de ese período de tiempo. Un mensaje del centro de eventos tiene un tamaño máximo de 256 KB. Si el tamaño total de todos los mensajes dentro del período de tiempo superó ese volumen, se envían varios mensajes.

Por ejemplo, normalmente tienen lugar unos 18 eventos por segundo para un inquilino de gran tamaño de más de 100 000 usuarios. Esto equivale a 5400 eventos cada cinco minutos (300 segundos x 18 eventos). Los registros de auditoría tienen un tamaño aproximado de 2 KB por evento. Esto equivale a 10,8 MB de datos. Por lo tanto, se envían 43 mensajes al centro de eventos en ese intervalo de cinco minutos.

La siguiente tabla contiene los costos aproximados al mes para un centro de eventos básico en la región Oeste de EE. UU., en función del volumen de datos de eventos. Para obtener una estimación del volumen de datos que espera para sus registros, use la calculadora de precios de Event Hubs.

Registro de auditoría con 100 000 usuarios

CATEGORY	VALUE
Eventos por segundo	18
Eventos por intervalo de cinco minutos	5 400
Volumen por intervalo	10,8 MB
Mensajes por intervalo	43
Mensajes al mes	371,520
Costo estimado al mes (USD)	10,83 USD

Registro de auditoría con 1000 usuarios

CATEGORY	VALUE
Eventos por segundo	0,1
Eventos por intervalo de cinco minutos	52
Volumen por intervalo	104 KB
Mensajes por intervalo	1
Mensajes al mes	8 640
Costo estimado al mes (USD)	10,80 USD

Consideraciones sobre el costo de Log Analytics

Para revisar los costos relacionados con la administración del área de trabajo de Log Analytics, consulte Administración de los costos mediante el control del volumen de datos y la retención en Log Analytics.

Preguntas más frecuentes

Obtenga respuestas a las preguntas más frecuentes así como información sobre los problemas conocidos con los registros de Intune en Azure Monitor.

¿Qué registros se incluyen?

Los registros de auditoría y los registros operativos están disponibles para el enrutamiento mediante esta característica.

Después de una acción, ¿cuándo se muestran los registros correspondientes en el centro de eventos?

Los registros normalmente se muestran en el centro de eventos unos minutos después de realizar la acción. Documentación de Azure Event Hubs proporciona más información.

Después de una acción, ¿cuándo se muestran los registros correspondientes en la cuenta de almacenamiento?

Para las cuentas de almacenamiento de Azure, la latencia es en cualquier lugar de 5 a 15 minutos después de que se ejecuta la acción.

¿Qué ocurre si un administrador cambia el período de retención de una configuración de diagnóstico?

La nueva directiva de retención se aplica a los registros recopilados después del cambio. Los registros recopilados antes del cambio de directiva no se ven afectados.

¿Cuánto cuesta almacenar mis datos?

Los costos de almacenamiento dependen del tamaño de los registros y del período de retención que elija. Para una lista de los costos estimados para los inquilinos, que dependen del volumen de los registros generado, vea Tamaño de almacenamiento para los registros de actividad (en este artículo).

¿Cuánto cuesta transmitir mis datos a un centro de eventos?

El costo del streaming depende del número de mensajes que reciba por minuto. Para detalles sobre cómo se calculan los costos y las estimaciones de costos en función del número de mensajes, consulte Mensajes del centro de eventos para los registros de actividad (en este artículo).

¿Cómo integro los registros de auditoría de Intune con mi sistema SIEM?

Use Azure Monitor con Event Hubs para hacer streaming de los registros en el sistema SIEM. En primer lugar, transmita los registros a un centro de eventos. A continuación, configure la herramienta SIEM con el centro de eventos configurado.

¿Qué herramientas SIEM se admiten actualmente?

Actualmente, Splunk, QRadar y Sumo Logic (abre un nuevo sitio Web) admiten Azure Monitor. Para más información sobre cómo funcionan los conectores, consulte Flujo de datos de supervisión de Azure a un centro de eventos para que lo consuma una herramienta externa.

¿Puedo acceder a los datos desde un centro de eventos sin usar una herramienta SIEM externa?

Sí. Para acceder a los registros desde la aplicación personalizada, puede usar la API de Event Hubs.

¿Dónde se almacenan los datos?

Intune no almacena los datos enviados a través de la canalización. Intune enruta los datos a la canalización de Azure Monitor, con la autorización del inquilino. Para más información, consulte Introducción a Azure Monitor.

Pasos siguientes

- Archivado de registros de actividad en una cuenta de almacenamiento
- Enrutamiento de registros de actividad a un centro de eventos

- Integración de registros de actividad en Log Analytics

Asignación de directivas entre Mobility + Security básico e Intune

14/05/2021 • 2 minutes to read

Tanto Basic Mobility and Security, anteriormente Administración de dispositivos móviles de Microsoft 365 (MDM), como Intune se usan para administrar los dispositivos móviles. Parte de esta administración incluye la aplicación de diversas directivas que determinan cómo interactúan los dispositivos móviles con la seguridad y los datos de la empresa.

Si decide migrar su MDM de Basic Mobility and Security a Intune, deberá duplicar las directivas en Intune. Puede usar la herramienta de evaluación de la migración para administrar la migración. También puede usar los artículos de esta sección para entender las directivas de los dos sistemas y cómo se asignan entre sí.

En función de la configuración de directivas de Basic Mobility and Security, puede que se necesiten diferentes directivas de Intune y Azure AD para duplicar el comportamiento. Dado que Intune ofrece una mayor flexibilidad, cada directiva de origen puede traducirse en varias directivas de Intune y Azure Active Directory (Azure AD) para lograr el mismo efecto. Cada directiva de seguridad de dispositivos puede requerir hasta tres directivas de cumplimiento, seis perfiles de configuración y cinco directivas globales de acceso condicional.

Directivas de Basic Mobility and Security en el portal de Seguridad y cumplimiento de Office 365

Basic Mobility and Security emplea el portal de Seguridad y cumplimiento de Office 365 para administrar las directivas de seguridad de dispositivos.

Directivas de Intune en el centro de administración de Microsoft Endpoint Manager

Intune usa el centro de administración de Microsoft Endpoint Manager para administrar las siguientes directivas con el fin de obtener resultados similares a los de las directivas de seguridad de dispositivos de Office:

TIPO DE DIRECTIVA DE INTUNE	PROPÓSITO	UBICACIÓN DE INTUNE
Directivas de cumplimiento	Especifique la configuración del dispositivo como requisito de acceso.	Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **Directivas de cumplimiento**
Perfiles de configuración	Especifique otras opciones que no formen parte de los requisitos de acceso, como los perfiles de correo electrónico.	Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **Perfiles de configuración**
Directivas de acceso condicional	El acceso condicional de Azure AD bloquea el acceso si la configuración no es compatible.	Centro de administración de Microsoft Endpoint Manager > **Seguridad de los puntos de conexión** > **Acceso condicional** > **Directivas clásicas**

Las directivas de Intune y Azure AD son más eficaces que las directivas de MDM de Office y tienen muchas más configuraciones para lograr escenarios más avanzados. Antes de cambiar las directivas de Intune o Azure AD no mencionadas en estos artículos, primero debe leer la documentación pertinente de Intune o Azure AD.

Pasos siguientes

- Asignación de directivas de requisito de acceso de Basic Mobility and Security a Intune
- Asignación de directivas de configuración de Basic Mobility and Security a Intune
- Asignación de directivas varias de Basic Mobility and Security a Intune

Asignación de directivas de requisito de acceso de Basic Mobility and Security a Intune

14/05/2021 • 16 minutes to read

En este artículo se proporcionan los detalles de asignación entre Basic Mobility and Security e Intune. En concreto, en esta página se asignan directivas de requisito de acceso del portal de Seguridad y cumplimiento de Office 365 a las directivas equivalentes del centro de administración de Microsoft Endpoint Manager. Dado que Intune ofrece más flexibilidad, cada directiva de Office se traducirá en varias directivas de Intune y Azure Active Directory (Azure AD) para lograr el mismo resultado.

Si va a migrar desde Basic Mobility and Security a Intune, puede usar la herramienta de evaluación de la migración para automatizar gran parte de esta asignación.

Para ver estas configuraciones en el portal de Seguridad y cumplimiento de Office 365, inicie sesión en el portal en https://protection.office.com/devicev2 y, en la lista de **Directivas de seguridad de dispositivos**, seleccione el nombre de la directiva > **Editar directiva** > **Requisitos de acceso**.

> **IMPORTANT**
> La opción **If a device doesn't meet the requirements above...** (Si un dispositivo no cumple los requisitos anteriores,...) determina si debe usar directivas de cumplimiento o perfiles de configuración de Intune en todas las configuraciones de requisitos de acceso. Asegúrese de revisar primero los detalles de esta configuración.

If a device doesn't meet the requirements above, then... (Si un dispositivo no cumple los requisitos anteriores,...)

Esta configuración determina si debe usar directivas de cumplimiento o perfiles de configuración en Intune en todas las configuraciones de requisitos de acceso.

> **NOTE**
> Basic Mobility and Security nunca ha admitido la aplicación de acceso condicional en Windows.

Permitir infracción de informes y acceso (la inscripción única se ejecutará igualmente)

Todos los requisitos de acceso se implementarán en un perfil de configuración de dispositivos de Intune.

Bloquear el acceso e informar de la infracción

Todos los requisitos de acceso se implementarán en una directiva de cumplimiento de Intune y los grupos asignados también se asignarán a las directivas de acceso condicional clásicas:

- Directiva de dispositivo [GraphAggregatorService]
- Directiva de dispositivo [Office 365 Exchange Online]
- Directiva de dispositivo [Servicio Outlook para Exchange]
- Directiva de dispositivo [Office 365 SharePoint Online]
- Directiva de dispositivo [Servicio Outlook para OneDrive]

Requerir una contraseña

> **NOTE**
> Toda la configuración relacionada con la contraseña solo afecta a las cuentas locales de Windows. Las cuentas de usuario que proceden de Azure Active Directory no se administran con estas directivas.

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Tres directivas de cumplimiento:

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Requerir una contraseña para desbloquear dispositivos móviles**
- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Requerir una contraseña para desbloquear dispositivos móviles**
- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Requerir una contraseña para desbloquear dispositivos móviles**

Evitar contraseñas sencillas

En los dispositivos Android, esta opción y varias otras opciones de configuración de Office se incluyen en una configuración de cumplimiento de Android. Por lo tanto, esta configuración por sí sola no determina un valor de cumplimiento específico de Android.

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Tres directivas de cumplimiento:

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Contraseñas sencillas**
- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Contraseñas sencillas**
- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Tipo de contraseña requerida**.
  - Si se selecciona **Evitar contraseñas sencillas**, elija **Numérica compleja**, **Alfabética**, **Alfanumérica** o **Alfanumérica con símbolos** (según otras configuraciones de Office).
  - Si **Evitar contraseñas sencillas** no está seleccionada, elija **Numérica** o un tipo superior en la lista (según otras configuraciones de Office).

Requerir una contraseña alfanumérica

En los dispositivos Android, esta opción y varias otras opciones de configuración de Office se incluyen en una configuración de cumplimiento de Android. Por lo tanto, esta configuración por sí sola no determina un valor de

cumplimiento específico de Android.

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Tres directivas de cumplimiento:

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Tipo de contraseña requerida**
- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Tipo de contraseña requerida**
- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Tipo de contraseña requerida**.
  - Si se selecciona **Evitar contraseñas sencillas**, elija **Numérica compleja**, **Alfabética**, **Alfanumérica** o **Alfanumérica con símbolos** (según otras configuraciones de Office).
  - Si **Evitar contraseñas sencillas** no está seleccionada, elija **Numérica** o un tipo superior en la lista (según otras configuraciones de Office).

La contraseña debe incluir al menos entre 1 y 4 conjuntos de caracteres

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Cuatro directivas de cumplimiento:

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Complejidad de la contraseña**.

VALOR DE OFFICE	VALOR DE INTUNE
1	**Requerir el uso de dígitos y letras minúsculas**. La directiva de cumplimiento de Windows no permite un solo conjunto de caracteres, por lo que una configuración de Office de **1** se traduce en **Requerir el uso de dígitos y letras minúsculas**.
2	**Requerir el uso de dígitos y letras minúsculas**
3	**Requerir el uso de dígitos, letras minúsculas y mayúsculas**
4	**Requerir el uso de dígitos, letras minúsculas y mayúsculas y caracteres especiales**

- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del**

sistema > **Número de caracteres no alfanuméricos en la contraseña**. La directiva de cumplimiento de iOS no exige el número de conjuntos de caracteres, sino solo el número de caracteres no alfanuméricos que se deben usar. Por tanto, los valores de Office se traducen en el mismo número de caracteres no alfanuméricos necesarios.

VALOR DE OFFICE	VALOR DE INTUNE
Deshabilitada (0)	No configurado
1	1
2	2
3	3
4	4

- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Tipo de contraseña requerida**. Android no admite la distinción entre mayúsculas y minúsculas como conjuntos de caracteres diferentes, por lo que no se puede aplicar el valor de Office de 4. En su lugar, se traduce en al menos **Alfanumérica con símbolos**.

VALOR DE OFFICE	VALOR DE INTUNE
1	Al menos **Numérica** o **Numérica compleja** (según otras configuraciones de Office)
2	Al menos **Alfanumérica**
3	Al menos **Alfanumérica con símbolos**
4	Al menos **Alfanumérica con símbolos**

- nombre de la directiva_OfficeMDM > **Controles de acceso** > **Conceder** > **Requerir que el dispositivo esté marcado como compatible**

Longitud mínima de la contraseña

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Tres directivas de cumplimiento:

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Longitud mínima de la contraseña**
- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Longitud mínima de la contraseña**
- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A >

Propiedades > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Tipo de contraseña requerida** y **Longitud mínima de la contraseña**.

EL VALOR DE OFFICE DE REQUERIR UNA CONTRASEÑA ALFANUMÉRICA	EL VALOR DE INTUNE DE TIPO DE CONTRASEÑA REQUERIDA
Seleccionado	Al menos **Numérica** (según otras configuraciones de Office)
No seleccionado	Al menos **Numérica** (según otras configuraciones de Office)

Número de errores de inicio de sesión antes de borrar el dispositivo

Aunque esta opción se muestra en **Requisitos de acceso** en Basic Mobility and Security, el acceso se sigue permitiendo incluso si esta configuración todavía no se ha habilitado en el dispositivo; además, esta configuración no es un criterio de cumplimiento de dispositivos.

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Tres perfiles de configuración:

- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Contraseña** > **Número de errores de inicio de sesión antes de borrar el dispositivo**
- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre de la directiva_O365_i > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Contraseña** > **Número de errores de inicio de sesión antes de borrar el dispositivo**
- **Dispositivos** > **Android** > **Perfiles de configuración** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Contraseña** > **Número de errores de inicio de sesión antes de borrar el dispositivo**

Bloquear dispositivos si están inactivos durante muchos minutos

Las directivas de cumplimiento de Windows, iOS/iPad y Android no ofrecen la misma granularidad de valores, por lo que el intervalo de configuración de Office se asigna a menos valores de Intune.

Tres directivas de cumplimiento:

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Número máximo de minutos de inactividad antes de que se requiera la contraseña**

VALOR DE OFFICE	VALOR DE INTUNE
De 1 a 4	1 minuto
De 5 a 14	5 minutos
15 o más	15 minutos

- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i >

Propiedades > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Número máximo de minutos de inactividad antes de que se requiera la contraseña**

VALOR DE OFFICE	VALOR DE INTUNE
1	1 minuto
2	2 minutes
3	3 minutos
4	4 minutos
De 5 a 9	5 minutos (máximo para iOS)
De 10 a 14	10 minutos (solo iPadOS)
15 o más	15 minutos (solo iPadOS)

- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Tipo de contraseña requerida**.

VALOR DE OFFICE	VALOR DE INTUNE
De 1 a 4	1 minuto
De 5 a 14	5 minutos
De 15 a 29	15 minutos
De 30 a 59	30 minutos
60	60 minutos

Caducidad de contraseña

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Tres directivas de cumplimiento:

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Expiración de contraseña (días)**
- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Expiración de contraseña (días)**
- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Número de días hasta que expire la contraseña**.

Recordar el historial de contraseñas y evitar la reutilización

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Tres directivas de cumplimiento:

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Número de contraseñas anteriores para evitar que se reutilicen**
- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Número de contraseñas anteriores para evitar que se reutilicen**
- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Número de contraseñas anteriores para evitar que se reutilicen** y **Tipo de contraseña requerida**

EL VALOR DE OFFICE DE REQUERIR UNA CONTRASEÑA ALFANUMÉRICA	EL VALOR DE INTUNE DE TIPO DE CONTRASEÑA REQUERIDA
Seleccionado	Al menos **Numérica** (según otras configuraciones de Office)
No seleccionado	Al menos **Numérica** (según otras configuraciones de Office)

Requerir cifrado de datos en los dispositivos

Esta opción nunca ha sido configurable en Windows o iOS/iPadOS en Basic Mobility and Security.

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Una directiva de cumplimiento:

- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Seguridad del sistema** > **Cifrado de almacenamiento de datos en el dispositivo**

Evitar que los dispositivos liberados o acceso root se conecten

Esta opción nunca ha sido configurable en Windows en Basic Mobility and Security.

En dispositivos Android, Intune solo admite esta opción en los dispositivos de administrador de dispositivos Android.

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Dos directivas de cumplimiento:

- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Estado de dispositivos** > **Dispositivos con Jailbreak**
- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Estado de dispositivos** > **Dispositivos raíz**

Requerir administración del perfil de correo electrónico (necesario para el borrado selectivo en iOS)

La exigencia de esta opción nunca se ha admitido para el cumplimiento de Windows o Android en Basic Mobility and Security. El correo electrónico de Windows nunca se ha admitido en Windows 10 en Basic Mobility and Security.

En Android, esta opción solo se admitía en dispositivos Samsung Knox en Basic Mobility and Security.

Intune requiere que, al implementar el correo electrónico, se configuren opciones adicionales que no estaban disponibles en las directivas de seguridad de los dispositivos. Para más información, consulte Configuración adicional necesaria en Intune para los perfiles de correo electrónico.

Cuando **If a device doesn't meet the requirements above, then...** (Si un dispositivo no cumple los requisitos anteriores,...) esté establecido en **Bloquear el acceso e informar de la infracción**, use las directivas de cumplimiento de Intune como se muestra a continuación. Si el valor se establece en **Permitir...** , use en su lugar perfiles de configuración.

Tres perfiles de configuración y una directiva de cumplimiento

- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre de la directiva_O365_W_Correo electrónico > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración)

SETTING	VALUE
Servidor de correo electrónico	outlook.office365.com
Nombre de la cuenta	Correo electrónico de Office 365
Atributo de nombre de usuario de AAD	Nombre principal del usuario
Atributo de dirección de correo electrónico de AAD	Nombre principal del usuario
SSL	Habilitar

- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre de la directiva_O365_i_Correo electrónico > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración)

SETTING	VALUE
Servidor de correo electrónico	outlook.office365.com
Nombre de la cuenta	Correo electrónico de Office 365
Atributo de nombre de usuario de AAD	Nombre principal del usuario

SETTING	VALUE
Atributo de dirección de correo electrónico de AAD	Nombre principal del usuario
Nombre de autenticación	Nombre de usuario y contraseña
SSL	Habilitar

- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Correo electrónico** > **Unable to set up email on the device** (No se puede configurar el correo electrónico en el dispositivo) > **Require** (Requerir)
- **Dispositivos** > **Android ** > Perfiles de configuración > nombre de la directiva_O365_A_Correo electrónico > Propiedades > ** Configuration settings Edit** (Editar valores de configuración)

SETTING	VALUE
Servidor de correo electrónico	outlook.office365.com
Nombre de la cuenta	Correo electrónico de Office 365
Atributo de nombre de usuario de AAD	Nombre principal del usuario
Atributo de dirección de correo electrónico de AAD	Nombre principal del usuario
Nombre de autenticación	Nombre de usuario y contraseña
SSL	Habilitar

Configuración adicional necesaria en Intune para los perfiles de correo electrónico

Las directivas de seguridad de dispositivos no implementan las siguientes configuraciones, pero Intune exige que tengan un valor al implementar los perfiles de correo electrónico.

PLATAFORMA	SETTING	VALOR EN LA MIGRACIÓN
Android	Requerir S/MIME	false
Android	Sincronizar los contactos	true
Android	Sincronizar el calendario	true
Android	Sincronizar las tareas	true
Android	Sincronizar las notas	false
iOS	Bloquear el movimiento de mensajes a otras cuentas de correo electrónico	false
iOS	Bloquear el envío de correo electrónico desde direcciones de terceros	false

PLATAFORMA	SETTING	VALOR EN LA MIGRACIÓN
iOS	Bloquear la sincronización de las direcciones de correo electrónico usadas recientemente	false
iOS	Requerir S/MIME	false
Windows 10	Sincronizar los contactos	true
Windows 10	Sincronizar el calendario	true
Windows 10	Sincronizar las tareas	true

Asignación de directivas de configuración de Basic Mobility and Security a Intune

14/05/2021 • 5 minutes to read

En este artículo se proporcionan los detalles de asignación entre Basic Mobility and Security e Intune. En concreto, en esta página se asignan las directivas de configuración del portal de Seguridad y cumplimiento de Office 365 a las directivas equivalentes del centro de administración de Microsoft Endpoint Manager. Dado que Intune ofrece más flexibilidad, cada directiva de Office se traducirá en varias directivas de Intune y Azure Active Directory (Azure AD) para lograr el mismo resultado.

Si va a migrar desde Basic Mobility and Security a Intune, puede usar la herramienta de evaluación de la migración para automatizar gran parte de esta asignación.

Para ver esta configuración en el portal de Seguridad y cumplimiento de Office 365, inicie sesión en el portal y, luego, seleccione **Directivas de seguridad de dispositivos** > nombre de la directiva > **Editar directiva** > **Configuraciones**.

Requerir copia de seguridad cifrada

Esta opción nunca se ha admitido en Windows o Android en Basic Mobility and Security.

Un perfil de configuración:

- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Nube y almacenamiento** > **Forzar la copia de seguridad cifrada**

Bloquear copia de seguridad de la nube

Esta opción nunca se ha admitido en Windows o Android en Basic Mobility and Security.

Esta configuración solo se admite en dispositivos iOS supervisados.

Un perfil de configuración:

- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Nube y almacenamiento** > varias configuraciones de **Bloquear iCloud**

Bloquear sincronización de documentos

Esta opción nunca se ha admitido en Windows o Android en Basic Mobility and Security.

Esta configuración solo se admite en dispositivos iOS supervisados.

Un perfil de configuración:

- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Nube y almacenamiento** > **Bloquear la sincronización de datos y documentos de iCloud**

Bloquear sincronización de fotos

Esta opción nunca se ha admitido en Windows o Android en Basic Mobility and Security.

Un perfil de configuración:

- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Nube y almacenamiento** > **Bloquear Mis Fotos en streaming**

Bloquear captura de pantalla

En dispositivos Android, esta opción solo se admitía en dispositivos Samsung Knox en Basic Mobility and Security.

Tres perfiles de configuración:

- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **General** > **Captura de pantalla (solo móvil)**
- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **General** > **Bloquear capturas de pantalla y grabación de pantalla**
- **Dispositivos** > **Android** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **General** > **Captura de pantalla (solo Samsung KNOX)**

Bloquear las videoconferencias en el dispositivo

Esta opción nunca se ha admitido en Windows o Android en Basic Mobility and Security.

Esta configuración solo se admite en dispositivos iOS supervisados.

Un perfil de configuración:

- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **Aplicaciones integradas** > **Bloquear FaceTime**

Bloquear el envío de datos de diagnóstico desde el dispositivo

En dispositivos Android, esta opción solo se admitía en dispositivos Samsung Knox en Basic Mobility and Security.

En dispositivos Windows 10, el valor más restrictivo impide el envío de datos relacionados con la seguridad.

Tres perfiles de configuración:

- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **Informes y telemetría** > **Compartir datos de uso**

BLOQUEAR EL ENVÍO DE DATOS DE DIAGNÓSTICO DESDE EL VALOR DEL DISPOSITIVO	COMPARTIR VALOR DE DATOS DE USO
Seleccionado	Seguridad
No seleccionado	No configurado

- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Compliance settings Edit** (Editar configuración de cumplimiento) > **General** > **Block sending diagnostic and usage data to Apple** (Bloquear el envío de datos de diagnóstico y uso a Apple)
- **Dispositivos** > **Android** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **General** > **Diagnostic data (Samsung Knox only)** (Datos de diagnóstico [solo Samsung Knox])

Bloquear el acceso al almacén de aplicaciones

En dispositivos Android, esta opción solo se admitía en dispositivos Samsung Knox en Basic Mobility and Security.

En iOS, esta configuración solo se admite en dispositivos iOS supervisados.

Tres perfiles de configuración:

- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **Tienda de aplicaciones** > **Tienda de aplicaciones (solo móvil)**
- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **App Store, presentación de documentos, juegos** > **Bloquear tienda de aplicaciones**
- **Dispositivos** > **Android** > **Perfiles de configuración** > elegir un perfil con el tipo **Administrador de dispositivos** > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **Google Play Store** > **Google Play Store (solo Samsung Knox)**

Solicitar contraseña al obtener acceso a la tienda de aplicaciones

Esta opción nunca se ha admitido en Windows o Android en Basic Mobility and Security.

Apple no bloquea el acceso a la tienda de aplicaciones sin contraseña, pero bloquea las compras sin contraseña.

Un perfil de configuración:

- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **App Store, presentación de documentos, juegos** > **Requerir contraseña de iTunes Store para todas las compras**

Bloquear conexión con almacenamiento extraíble

Esta configuración nunca se ha admitido en iOS/iPad en Basic Mobility and Security.

En dispositivos Android, esta opción solo se admitía en dispositivos Samsung Knox en Basic Mobility and Security.

Dos perfiles de configuración:

- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **General** > **Almacenamiento extraíble**
- **Dispositivos** > **Android** > **Perfiles de configuración** > elegir un perfil con el tipo **Administrador de dispositivos** > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **Nube y almacenamiento** > **Almacenamiento extraíble (solo Samsung Knox)**

Bloquear conexión Bluetooth

Esta configuración nunca se ha admitido en iOS/iPad en Basic Mobility and Security.

En dispositivos Android, esta opción solo se admitía en dispositivos Samsung Knox en Basic Mobility and Security.

Dos perfiles de configuración:

- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre del perfil > **Propiedades** > **Configuration settings Edit** > > (Editar valores de configuración) **Red de telefonía móvil y conectividad** > **Bluethooth**
- **Dispositivos** > **Android** > **Perfiles de configuración** > elegir un perfil con el tipo **Administrador de dispositivos** > **Propiedades** > **Configuration settings Edit** (Editar valores de configuración) > **Google Play Store** > **Bluetooth (solo Samsung Knox)**

Pasos siguientes

Para migrar estas directivas, puede usar la herramienta de evaluación de la migración.

Asignación de directivas varias de Basic Mobility and Security a Intune

14/05/2021 • 5 minutes to read

En este artículo se proporcionan los detalles de asignación entre Basic Mobility and Security e Intune. En concreto, en esta página se asignan las siguientes directivas y propiedades de dispositivos del portal de Seguridad y cumplimiento de Office 365 a las directivas y propiedades equivalentes del centro de administración de Microsoft Endpoint Manager:

- Propiedades y acciones de dispositivos
- Configuración de acceso a dispositivos para toda la organización
- Nombre y descripción de las directivas de seguridad de dispositivos

Dado que Intune ofrece más flexibilidad, cada directiva de Office se traducirá en varias directivas de Intune y Azure Active Directory (Azure AD) para lograr el mismo resultado.

Si va a migrar desde Basic Mobility and Security a Intune, puede usar la herramienta de evaluación de la migración para automatizar gran parte de esta asignación.

Propiedades y acciones de dispositivos

Para ver esta configuración, inicie sesión en el centro de administración de Microsoft 365 y, luego, seleccione un dispositivo.

Usuario

- **Dispositivos** > **Todos los dispositivos** > nombre del dispositivo > **Información general** > **Inscrito por**

Tipo de dispositivo

- **Dispositivos** > **Todos los dispositivos** > nombre del dispositivo > **Información general** > **Sistema operativo**

Estado

No es una columna predeterminada en la lista de dispositivos del portal de Intune. Puede mostrarla mediante el selector **Columnas**.

- **Dispositivos** > **Todos los dispositivos** > columna **Estado del dispositivo**

Versión del SO

- **Dispositivos** > **Todos los dispositivos** > nombre del dispositivo > **Hardware** > **Versión del sistema operativo**

Restablecimiento de fábrica

- **Dispositivos** > **Todos los dispositivos** > nombre del dispositivo > **Información general** > **Borrar**

Eliminar datos de la compañía

- **Dispositivos** > **Todos los dispositivos** > nombre del dispositivo > **Información general** > **Retirar**

Configuración de acceso a dispositivos para toda la organización

Para ver esta configuración en el portal de Seguridad y cumplimiento de Office 365, inicie sesión en el portal y, luego, seleccione **Directivas de seguridad de dispositivos** > **Administrar la configuración de acceso**

de dispositivos en toda la organización.

Esta configuración está respaldada por la directiva Directiva de dispositivo [GraphAggregatorService] de acceso condicional. Incluye:

- Plataformas de dispositivo: iOS, Android
- Aplicaciones cliente de destino: clientes de escritorio de aplicación móvil
- Controles de acceso: se requiere un dispositivo compatible

Si un dispositivo no es compatible con MDM para Office 365, ¿desea permitir o bloquear el acceso a una cuenta de Exchange para que pueda usar el correo electrónico de su organización?

Esta configuración modifica una directiva de acceso condicional clásica:

- **Seguridad de los puntos de conexión** > **Acceso condicional** > **Directivas clásicas** > **Directiva de dispositivo [GraphAggregatorService]** > **Condiciones** > **Aplicaciones cliente (versión preliminar)** > **Aplicaciones móviles y aplicaciones de escritorio** > **Clientes de Exchange ActiveSync** > **Apply policy only to supported platform** (Aplicar directiva solo a la plataforma admitida)

¿Hay algún grupo de seguridad que desee excluir del control de acceso?

Esta configuración modifica cinco directivas de acceso condicional clásicas:

- Directiva de dispositivo [GraphAggregatorService]
- Directiva de dispositivo [Office 365 Exchange Online]
- Directiva de dispositivo [Servicio Outlook para Exchange]
- Directiva de dispositivo [Office 365 SharePoint Online]
- Directiva de dispositivo [Servicio Outlook para OneDrive]
- **Seguridad de los puntos de conexión** > **Acceso condicional** > nombre de la directiva > **Usuarios y grupos** > **Excluir**

Nombre y descripción de la directiva de seguridad de dispositivos

Para ver esta configuración en el portal de Seguridad y cumplimiento de Office 365, inicie sesión en el portal y, luego, seleccione **Directivas de seguridad de dispositivos** > nombre de la directiva > **Editar directiva** > **Nombre**.

Nombre

Hasta tres directivas de cumplimiento y hasta seis perfiles de configuración (tres para restricciones y tres para correo electrónico):

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Nombre**
- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Nombre**
- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Nombre**
- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre de la directiva_O365_W > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Nombre**
- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre de la directiva_O365_i > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Nombre**
- **Dispositivos** > **Android** > **Perfiles de configuración** > nombre de la directiva_O365_A > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Nombre**
- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre de la directiva_O365_W_Correo

electrónico > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Nombre**

- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre de la directiva_O365_i_Correo electrónico > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Nombre**
- **Dispositivos** > **Android** > **Perfiles de configuración** > nombre de la directiva_O365_A_Correo electrónico > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Nombre**

Descripción

Hasta tres directivas de cumplimiento y hasta seis perfiles de configuración (tres para restricciones y tres para correo electrónico):

- **Dispositivos** > **Windows** > **Directivas de cumplimiento** > nombre de la directiva_O365_W > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Descripción**
- **Dispositivos** > **iOS/iPadOS** > **Directivas de cumplimiento** > nombre de la directiva_O365_i > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Descripción**
- **Dispositivos** > **Android** > **Directivas de cumplimiento** > nombre de la directiva_O365_A > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Descripción**
- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre de la directiva_O365_W > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Descripción**
- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre de la directiva_O365_W > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Descripción**
- **Dispositivos** > **Android** > **Perfiles de configuración** > nombre de la directiva_O365_W > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Descripción**
- **Dispositivos** > **Windows** > **Perfiles de configuración** > nombre de la directiva_O365_W_Correo electrónico > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Descripción**
- **Dispositivos** > **iOS/iPadOS** > **Perfiles de configuración** > nombre de la directiva_O365_i_Correo electrónico > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Descripción**
- **Dispositivos** > **Android** > **Perfiles de configuración** > nombre de la directiva_O365_A_Correo electrónico > **Propiedades** > **Basics Edit** > (Editar aspectos básicos) **Descripción**

Pasos siguientes

Para migrar estas directivas, puede usar la herramienta de evaluación de la migración.

Novedades de Microsoft Intune: meses anteriores

14/05/2021 • 521 minutes to read

Noviembre de 2020

Administración de aplicaciones

Mejoras en la mensajería del perfil de trabajo en el Portal de empresa para Android

Hemos actualizado la mensajería en el Portal de empresa para Android para presentar y explicar mejor cómo funciona el perfil de trabajo. La nueva mensajería aparece:

- Después del flujo de configuración del perfil de trabajo. Los usuarios ven una nueva pantalla informativa en la que se explica dónde encontrar las aplicaciones de trabajo, con vínculos a la documentación de ayuda.
- Cuando un usuario vuelve a habilitar por error la aplicación Portal de empresa en el perfil personal. Hemos rediseñado una pantalla (**el dispositivo tiene ahora un perfil solo para trabajo**) con explicaciones más claras y nuevas ilustraciones para guiar a los usuarios a sus aplicaciones de trabajo, con vínculos a la documentación de ayuda.
- En la página **Ayuda**. En la sección **Preguntas más frecuentes**, hay un nuevo vínculo a la documentación de ayuda sobre cómo configurar el perfil de trabajo y buscar aplicaciones.

Los scripts de PowerShell se ejecutan antes que las aplicaciones y se reduce el tiempo de espera

Se han realizado algunas actualizaciones en los scripts de PowerShell:

- El flujo de ejecución de extensión de administración de Microsoft Intune vuelve a procesar primero los scripts de PowerShell y, después, ejecuta las aplicaciones Win32.
- Para resolver un problema de tiempo de espera de la página de estado de la inscripción (ESP), los scripts de PowerShell agotan el tiempo de espera pasados 30 minutos. Anteriormente, se agotaba el tiempo de espera al cabo de 60 minutos.

Para más información, consulte Uso de scripts de PowerShell para dispositivos Windows 10 en Intune.

Configuración del dispositivo

Menú de encendido, notificaciones de la barra de estado y configuraciones más restrictivas disponibles para dispositivos Android Enterprise dedicados

En dispositivos Android Enterprise dedicados inscritos en Intune que se ejecutan en modo de pantalla completa con una o varias aplicaciones, puede hacer lo siguiente:

- Restringir el menú de encendido, las advertencias de errores del sistema y el acceso a la aplicación Configuración.
- Elegir si los usuarios pueden ver los botones Inicio e Información general, y las notificaciones.

Para configurar estas opciones, cree un perfil de configuración de restricciones de dispositivos: **Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Android Enterprise** para la plataforma > **Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado** > **Restricciones de dispositivos** > **General**.

Para obtener más información sobre estos y otros valores que puede configurar, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

Se aplica a:

- Dispositivos Android Enterprise dedicados

Nueva opción para mostrar vistas previas para las notificaciones de aplicaciones en dispositivos iOS/iPadOS

En los dispositivos iOS/iPadOS, está la opción **Show Previews** (Mostrar vistas previas) (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** para la plataforma > **Características del dispositivo** para perfil > **Notificaciones de la aplicación**). Utilice esta opción para elegir cuándo se muestran las vistas previas recientes de notificaciones de la aplicación en los dispositivos.

Para obtener más información sobre la configuración de las notificaciones de la aplicación y otras opciones que puede configurar, consulte Configuración de dispositivos para usar las características comunes de iOS/iPadOS.

Reglas a petición con Microsoft Tunnel para iOS

Microsoft Tunnel ahora admite reglas a petición para dispositivos iOS/iPad. Con las reglas a petición, puede especificar el uso de la VPN cuando se cumplan las condiciones para nombres de dominio completo o direcciones IP específicos.

Para configurar reglas a petición para iOS/iPadOS con Microsoft Tunnel, configure un perfil de VPN para iOS/iPadOS como parte de la directiva de configuración de dispositivos. En la página *Opciones de configuración* del perfil, seleccione *Microsoft Tunnel* como *Tipo de conexión* y, después, tendrá acceso para configurar **Reglas de VPN a petición**.

Para obtener información sobre las reglas de VPN a petición que puede configurar, vea Configuración de VPN automática.

Se aplica a:

- iOS/iPadOS

Más opciones de autenticación para perfiles de Wi-Fi en dispositivos Windows 10 y más recientes

Nuevas opciones y características para perfiles de Wi-Fi en dispositivos que ejecutan Windows 10 y versiones más recientes (**Dispositivos** > **Configuración de dispositivo** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Wi-Fi** para el perfil > **Enterprise**):

- **Modo de autenticación**: autentique al usuario, al dispositivo, o bien use la autenticación de invitado.
- **Recordar credenciales en cada inicio de sesión**: obligue a los usuarios a escribir las credenciales cada vez que se conecten a la VPN. O bien, almacene en caché las credenciales para que los usuarios solo tengan que escribirlas una vez.
- Control más pormenorizado sobre el comportamiento de la autenticación, incluido lo siguiente:
  - Período de autenticación
  - Periodo de intervalo entre reintentos de autenticación
  - Período de inicio
  - Número máximo de mensajes EAPOL-Start
  - Número máximo de errores de autenticación
- **Use VLAN independientes para la autenticación de usuarios y dispositivos**: cuando se usa el inicio de sesión único, el perfil de Wi-Fi puede usar otra LAN virtual en función de las credenciales del usuario. El servidor Wi-Fi debe admitir esta característica.

Para ver estos valores y todos los que puede configurar, vaya a Agregar Wi-Fi para dispositivos Windows 10 y versiones posteriores en Intune.

Se aplica a:

- Windows 10 y versiones posteriores

Administración de dispositivos

Terminología de perfil de trabajo de propiedad personal

Para evitar confusiones, el término para el escenario de administración de Android Enterprise *perfil de trabajo* se cambiará a "dispositivos de propiedad personal con un perfil de trabajo" o *perfil de trabajo de propiedad*

personal en toda la documentación e interfaz de usuario de Intune. La finalidad es diferenciarlo del escenario de administración de "perfil de trabajo de propiedad corporativa".

Windows Autopilot para HoloLens 2 (versión preliminar)

Ahora Windows Autopilot para dispositivos HoloLens 2 está en versión preliminar pública. Los administradores ya no tienen que registrar a los inquilinos para la distribución de paquetes piloto. Para más información sobre el uso de Autopilot para HoloLens, consulte Windows Autopilot para HoloLens 2.

Fin de la compatibilidad con iOS 11

La inscripción en Intune y el Portal de empresa ahora admiten las versiones de iOS 12 y posteriores. No se admiten las versiones anteriores, pero seguirán recibiendo directivas.

Fin de la compatibilidad con macOS 10.12

Desde la publicación de macOS Big Sur, la inscripción de Intune y Portal de empresa ahora admiten macOS 10.13 y versiones posteriores. No se admiten versiones anteriores.

Seguridad de dispositivos

Nuevo parámetro para el perfil de control de dispositivos para la seguridad de puntos de conexión

Se ha agregado una opción nueva **Bloquear el acceso de escritura a almacenamiento extraíble** al perfil Control de dispositivos para la directiva Reducción de la superficie expuesta a ataques en la seguridad de los puntos de conexión. Cuando se establece en *Sí*, se bloquea el acceso de escritura al almacenamiento extraíble.

Mejoras en la configuración de los perfiles de la regla Reducción de la superficie expuesta a ataques

Se han actualizado las opciones para los valores aplicables del perfil de la regla Reducción de la superficie expuesta a ataques, que forma parte de la directiva Reducción de la superficie expuesta a ataques de las seguridades del punto de conexión.

Se ha aplicado la coherencia de los valores a las opciones existentes, como *Deshabilitar* y *Habilitar*, y se ha agregado una opción nueva, *Advertir*:

- **Advertir**: en dispositivos que ejecutan Windows 10, versión 1809 o posterior, el usuario del dispositivo recibe un mensaje de que puede omitir el valor. Por ejemplo, en *Impedir que Adobe Reader cree procesos secundarios*, la opción *Advertir* presenta a los usuarios la posibilidad de omitir ese bloqueo y permitir que Adobe Reader cree un proceso secundario. En los dispositivos que ejecutan versiones anteriores de Windows 10, la regla aplica el comportamiento sin la opción para omitirlo.

Compatibilidad con la combinación de directivas para los identificadores de dispositivos USB en los perfiles de control de dispositivos de la directiva de reducción de la superficie expuesta a ataques de seguridad de los puntos de conexión

Se ha agregado compatibilidad para la *combinación de directivas* de id. de dispositivo USB al perfil Control de dispositivos para la directiva Reducción de la superficie expuesta a ataques de seguridad de los puntos de conexión. La siguiente configuración de perfiles de *control de dispositivos* se evalúan con miras a la combinación de directivas:

- Allow hardware device installation by device identifiers (Permitir instalación de dispositivos de hardware mediante identificadores de dispositivo)
- Block hardware device installation by device identifiers (Bloquear instalación de dispositivos de hardware mediante identificadores de dispositivo)
- Permitir la instalación de dispositivos de hardware por clases de instalación
- Bloquear la instalación de dispositivos de hardware por clase de instalación
- Allow hardware device installation by device instance identifiers (Permitir instalación de dispositivos de hardware mediante identificadores de dispositivo)
- Block hardware device installation by device instance identifiers (Bloquear instalación de dispositivos de hardware mediante identificadores de dispositivo)

La combinación de directivas se aplica a la configuración de cada parámetro en los distintos perfiles que se aplican a un dispositivo. No incluye la evaluación entre diferentes configuraciones, incluso cuando dos parámetros están estrechamente relacionados.

Para obtener un ejemplo más detallado de lo que se combina y el modo en que las listas de permitidos y bloqueados para cada configuración admitida se combinan y aplican en un dispositivo, vea Combinación de directivas para configuraciones para perfiles de control de dispositivos.

Informe de operaciones de estado del antivirus mejorado para la seguridad del punto de conexión

Se han agregado detalles nuevos al informe de operaciones de estado del antivirus para el antivirus de Windows Defender, que es un informe de directiva de seguridad de punto de conexión.

Las siguientes nuevas columnas de información estarán disponibles para cada dispositivo:

- **Estado del producto**: el estado de Windows Defender en el dispositivo.
- **Protección contra manipulaciones**: habilitada o deshabilitada.
- **Máquina virtual**: si el dispositivo es una máquina virtual o un dispositivo físico.

Mejora en la combinación de reglas para las reglas de reducción de la superficie expuesta a ataques

Ahora las reglas de reducción de la superficie expuesta a ataques admiten un comportamiento nuevo para la combinación de configuraciones de distintas directivas, a fin de crear un superconjunto de directivas para cada dispositivo. Solo se combinan los valores que no están en conflicto, mientras que los que sí lo están no se agregan al superconjunto de reglas. Anteriormente, si dos directivas incluían conflictos para una sola configuración, se marcaban como en conflicto y no se implementaba ninguna configuración de ninguno de los perfiles.

El comportamiento de la combinación de reglas de reducción de la superficie expuesta a ataques es el siguiente:

- Se evalúan las reglas de reducción de la superficie expuesta a ataques de los siguientes perfiles para cada dispositivo al que se aplican las reglas:
  - Dispositivos > Directiva de configuración > Perfil de Endpoint Protection > Protección contra vulnerabilidades de seguridad de Microsoft Defender > Reducción de la superficie expuesta a ataques.
  - Seguridad de los puntos de conexión > Directiva de reducción de la superficie expuesta a ataques > Reglas de reducción de la superficie expuesta a ataques.
  - Seguridad de los puntos de conexión > Líneas de base de seguridad > Línea de base de Microsoft Defender for Endpoint > Reglas de reducción de la superficie expuesta a ataques.
- La configuración que no tiene conflictos se agrega a un superconjunto de directivas para el dispositivo.
- Cuando dos o más directivas tienen una configuración en conflicto, no se agrega a la directiva combinada, mientras que la configuración que no está en conflicto se agrega a la directiva de superconjunto que se aplica a un dispositivo.
- Solo se retienen las configuraciones de los valores en conflicto.

MVISION Mobile: nuevo asociado de Mobile Threat Defense

Puede controlar el acceso desde dispositivos móviles a recursos corporativos mediante el acceso condicional en función de la evaluación de riesgos realizada por MVISION Mobile, una solución de Mobile Threat Defense de McAfee que se integra con Microsoft Intune.

Supervisión y solución de problemas

Nuevo informe operativo de Intune para ayudar a solucionar problemas de perfil de configuración

Un nuevo informe operativo **Errores de asignación** está disponible en versión preliminar pública para ayudar a solucionar errores y conflictos de los perfiles de configuración que se han destinado a los dispositivos. En este informe se mostrará una lista de perfiles de configuración para el inquilino y el número de dispositivos en un estado de error o conflicto. Con esta información, puede explorar en profundidad un perfil para ver una lista de los dispositivos y usuarios en un estado de error relacionados con el perfil. Además, puede explorar todavía más para ver una lista de opciones y detalles de configuración relacionados con la causa del error. Puede filtrar, ordenar y buscar en todos los registros del informe. Puede encontrar este informe en el Centro de administración de Microsoft Endpoint Manager si selecciona **Dispositivos** > **Monitor** > **Errores de asignación (versión preliminar)** . Para obtener más información sobre los informes en Intune, vea Informes

de Intune.

Informe de actualizaciones para máquinas virtuales de Windows Virtual Desktop

La configuración siguiente se marca como **No aplicable** en los informes de directivas:

- Configuración de BitLocker
- Cifrado de dispositivos
- Configuración de Protección de aplicaciones de Defender
- Protección contra alteraciones de Defender
- Perfiles de Wi-Fi

Informe de directivas no conformes para solucionar problemas de dispositivos con errores o no conformes

En versión preliminar, el nuevo informe **Directivas no conformes** es un informe operativo que puede utilizar para ayudar a solucionar los errores y conflictos de las directivas de cumplimiento destinadas a los dispositivos. En el informe Directivas no conformes se muestra una lista de directivas de cumplimiento que tienen uno o más dispositivos con errores, o bien que se encuentran en un estado de no conformidad con la directiva.

Use este informe para:

- Ver las directivas de cumplimiento de dispositivos con dispositivos en un estado de error o no compatible, y después profundizar para ver la lista de dispositivos y usuarios en un estado de error.
- Explorar en profundidad para ver la lista de configuraciones y la información de configuración que produce un error.
- Filtrar, ordenar y buscar en todos los registros del informe. Se han agregado controles de paginación y la capacidad de exportación mejorada a un archivo CSV.
- Identificar cuándo se producen los problemas y optimizar su solución.

Para obtener más información sobre la supervisión de cumplimiento de dispositivos, vea Supervisión de las directivas de cumplimiento de dispositivos Intune.

Octubre de 2020

Administración de la aplicación

Las aplicaciones que requieren inscripción están ocultas cuando la inscripción está establecida en no disponible

Las aplicaciones asignadas con las intenciones **Disponible para dispositivos inscritos** y **Obligatoria** no se mostrarán en el Portal de empresa para los usuarios cuya opción de inscripción de dispositivos esté establecida en **No disponible**. Este cambio solo es aplicable cuando se ve la aplicación o el sitio web de Portal de empresa desde un dispositivo que no está inscrito, incluidos los dispositivos no inscritos que usan directivas de protección de aplicaciones (MAM-WE). Las aplicaciones seguirán siendo visibles para los usuarios que vean el Portal de empresa desde un dispositivo inscrito, independientemente del valor de la opción **Inscripción de dispositivos**. Para obtener más información, vea Opciones de configuración de inscripción de dispositivos.

Mejoras en la personalización de mensajes de privacidad de Portal de empresa para iOS

Ahora tiene mayor capacidad de personalizar la mensajería de privacidad en Portal de empresa para iOS. Además de la compatibilidad anterior con la posibilidad de personalizar lo que la organización *no puede ver*, ahora también podrá personalizar lo que *sí puede ver* en el mensaje de privacidad que se muestra a los usuarios finales en Portal de empresa para iOS. Para admitir esta característica, los dispositivos tendrán que ejecutar al menos la versión 4.11 de Portal de empresa para ver la mensajería personalizada sobre lo que se puede ver. Esta característica estará disponible en el Centro de administración de Microsoft Endpoint Manager si selecciona **Administración de inquilinos** > **Personalización**. Para obtener información relacionada, vea el mensaje Privacidad del Portal de empresa.

Directivas de protección de aplicaciones (MAM) de Android en dispositivos COPE

La compatibilidad con la administración de aplicaciones móviles (MAM) recién agregada habilita las directivas de protección de aplicaciones de Android en dispositivos Android Enterprise de propiedad corporativa con perfil

de trabajo (COPE). Para más información sobre las directivas de protección de aplicaciones, consulte Introducción general a las directivas de protección de aplicaciones.

Antigüedad máxima de la versión de Portal de empresa en el caso de dispositivos Android

Puede establecer un límite de antigüedad como el número máximo de días para la versión de Portal de empresa (CP) en dispositivos Android. Esta configuración garantiza que los usuarios finales estén comprendidos en un intervalo determinado de versiones de CP (en días). Cuando no se cumple la configuración de los dispositivos, se desencadena la acción seleccionada para esta configuración. Entre las acciones se incluyen **Bloquear acceso**, **Borrar datos** o **Advertir**. Puede encontrar esta opción en el Centro de administración de Microsoft Endpoint Manager si selecciona **Aplicaciones** > **Directivas de protección de aplicaciones** > **Crear directiva**. La opción **Antigüedad máxima de la versión de Portal de empresa (días)** estará disponible en la sección **Condiciones de dispositivo** del paso **Inicio condicional**. Para más información, consulte Configuración de directivas de protección de aplicaciones de Android: inicio condicional.

Compatibilidad de aplicaciones de línea de negocio de Mac como aplicaciones administradas en macOS 11 y versiones posteriores

Intune admite la propiedad de aplicación **Instalar como administrada** que se puede configurar para las aplicaciones de línea de negocio (LOB) de Mac implementadas en macOS 11 y versiones posteriores. Cuando esta opción está activada, la aplicación de línea de negocio de Mac se instalará como una aplicación administrada en los dispositivos compatibles (macOS 11 y versiones posteriores). Las aplicaciones de línea de negocio administradas se podrán quitar con el tipo de asignación **desinstalar** en los dispositivos compatibles (macOS 11 y versiones posteriores). Además, al quitar el perfil de MDM, se quitan todas las aplicaciones administradas del dispositivo. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **macOS** > **Agregar**. Para más información sobre cómo agregar aplicaciones, consulteIncorporación de aplicaciones a Microsoft Intune.

Habilitación de correos electrónicos S/MIME de Outlook siempre firmados o cifrados

Puede habilitar los correos electrónicos S/MIME de Outlook para que siempre se firmen o se cifren al crear un perfil de correo electrónico de Outlook en la configuración de aplicaciones para dispositivos iOS/iPadOS y Android Enterprise. Esta opción está disponible cuando se elige **Dispositivos administrados** al crear una directiva de configuración de aplicaciones de Outlook. Puede encontrar esta opción en el Centro de administración de Microsoft Endpoint Manager si selecciona **Aplicaciones** > **Directivas de configuración de aplicaciones** > **Agregar** > **Dispositivos administrados**. Para obtener información relacionada, vea Directivas de configuración de aplicaciones para Microsoft Intune.

Compatibilidad de aplicaciones Win32 con dispositivos de unión al área de trabajo (WPJ)

Las aplicaciones Win32 existentes son compatibles con dispositivos de unión al área de trabajo (WPJ). Los scripts de PowerShell, que anteriormente no se admitían en dispositivos WPJ, ahora pueden implementarse en dichos dispositivos. En concreto, los scripts de PowerShell de contexto de dispositivo funcionan en los dispositivos WPJ, pero el diseño no tiene en cuenta los scripts de PowerShell de contexto de usuario. Los scripts de contexto de usuario se omitirán en los dispositivos WPJ y no se notificarán a la consola de Microsoft Endpoint Manager. Para más información sobre PowerShell, vea Uso de scripts de PowerShell para dispositivos Windows 10 en Intune.

Configuración del dispositivo

Disponibilidad general de Device Firmware Configuration Interface (DFCI)

DFCI es un marco de trabajo de Unified Extensible Firmware Interface (UEFI) de código abierto. Permite administrar de forma segura la configuración de UEFI (BIOS) de los dispositivos de Windows Autopilot mediante Microsoft Endpoint Manager. También limita el control del usuario final sobre las configuraciones del firmware.

A diferencia de la administración de UEFI tradicional, DFCI elimina la necesidad de administrar soluciones de terceros. También proporciona administración del firmware sin interacción mediante Microsoft Endpoint Manager para la administración en la nube. DFCI también accede a la información de los dispositivos de Windows Autopilot existente para la autorización.

Para más información sobre esta característica, vea Uso de perfiles de DFCI en dispositivos Windows en Intune.

> **IMPORTANT**
> Los informes de directivas de DFCI en el centro de administración de Endpoint Manager no funcionaban según lo previsto. Todas las directivas notificaron un estado "pendiente". Este comportamiento se ha corregido.

Uso del valor Conectar automáticamente en perfiles de Wi-Fi básicos de Android Enterprise

En los dispositivos Android Enterprise, puede crear perfiles de Wi-Fi básicos que incluyen opciones de Wi-Fi comunes, como el nombre de la conexión. Puede configurar la opción **Conectar automáticamente** que se conecta de forma automática a la red Wi-Fi cuando los dispositivos se encuentran dentro del alcance.

Para ver estas opciones, vaya a Incorporación de configuración de Wi-Fi para dispositivos Android Enterprise dedicados y totalmente administrados en Microsoft Intune.

Se aplica a:

- Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado de Android Enterprise

Nueva experiencia del usuario y nueva opción Habilitación de descarga directa en dispositivos macOS mediante dominios asociados

Al crear un perfil de configuración de dominio asociado en dispositivos macOS, se actualiza la experiencia del usuario (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** para la plataforma > **Características del dispositivo** para el perfil > **Dominios asociados**). Todavía tendrá que escribir el identificador y los dominios de la aplicación.

En dispositivos macOS 11, o versiones posteriores, supervisados inscritos con la inscripción de dispositivos aprobados por el usuario o con la inscripción de dispositivos automatizada, puede usar la opción **Habilitar descarga directa**. La habilitación de las descargas directas permite que los datos del dominio se descarguen directamente de los dispositivos, en lugar de hacerlo mediante una red de entrega de contenido (CDN).

Para obtener más información, vea Dominios asociados en dispositivos macOS.

Se aplica a:

- macOS 11, o versiones superiores, (supervisado)

Nueva configuración de contraseñas de bloqueo en dispositivos macOS

Al crear un perfil de contraseña para macOS, hay nuevas configuraciones disponibles (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** para la plataforma > **Restricciones de dispositivos** para el perfil > **Contraseña**):

- **Número máximo de intentos de inicio de sesión permitidos**: número máximo de veces consecutivas (entre 2 y 11) que los usuarios pueden intentar iniciar sesión antes de que el dispositivo los bloquee. Establezca este valor en un número mayor. No se recomienda establecer este valor en 2 o 3, ya que los errores son habituales.

  Se aplica a todos los tipos de inscripción.

- **Duración del bloqueo**: elija cuánto tiempo dura el bloqueo, en minutos. Durante el bloqueo de un dispositivo, la pantalla de inicio de sesión está inactiva y los usuarios no pueden iniciar sesión. Cuando finaliza la duración del bloqueo, el usuario puede volver a iniciar sesión. Para usar esta opción, configure el valor **Número máximo de intentos de inicio de sesión permitidos**.

  Se aplica a macOS 10.10 y versiones más recientes, y a todos los tipos de inscripción.

Para ver estas opciones de configuración, vaya a Restricciones de dispositivos de contraseña de macOS.

Se aplica a:

- macOS

La configuración predeterminada "Tipo de contraseña requerida" cambia en los dispositivos Android Enterprise

En los dispositivos Android Enterprise, puede crear un perfil de contraseña de dispositivo que establezca el **Tipo de contraseña requerida** (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Android Enterprise** para la plataforma > **Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado** > **Restricciones de dispositivos** > **Contraseña del dispositivo**).

El valor predeterminado **Tipo de contraseña requerida** va a cambiar de **Numérico** a **Predeterminado del dispositivo**.

Los perfiles existentes no se ven afectados. Los nuevos perfiles usarán **Predeterminado del dispositivo** de forma automática.

Cuando se selecciona **Predeterminado del dispositivo**, la mayoría de los dispositivos no necesitan una contraseña. Si quiere solicitar a los usuarios que configuren un código de acceso en sus dispositivos, establezca la opción **Tipo de contraseña requerida** en algo más seguro que **Predeterminado del dispositivo**.

Para ver todos los valores que puede restringir, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características.

Se aplica a:

- Android Enterprise

Configuración del complemento Microsoft Enterprise SSO de macOS

> **IMPORTANT**
> En macOS, la extensión de SSO de Microsoft Azure AD aparecía en la interfaz de usuario de Intune, pero no funcionaba como se esperaba. Esta característica ya funciona y está disponible para su uso en la versión preliminar pública.

El equipo de Microsoft Azure AD creó una extensión de aplicación de inicio de sesión único (SSO) de redireccionamiento. Esta extensión de aplicación permite a los usuarios de macOS 10.15+ acceder a aplicaciones de Microsoft, aplicaciones de la organización y sitios web que admiten la característica SSO de Apple. Realiza la autenticación mediante Azure AD, con un inicio de sesión.

Con la versión del complemento Microsoft Enterprise SSO, puede configurar la extensión de SSO con el nuevo tipo de extensión de aplicación de Microsoft Azure AD en Intune (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** para plataforma > **Características del dispositivo** para perfil > **Extensión de aplicación de inicio de sesión único** > tipo de extensión de aplicación de SSO > **Microsoft Azure AD**).

Para obtener el SSO con el tipo de extensión de aplicación de SSO de Microsoft Azure AD, los usuarios deben instalar la aplicación de Portal de empresa en sus dispositivos macOS e iniciar sesión en ella.

Para obtener más información sobre las extensiones de aplicación de SSO de macOS, consulte Extensión de aplicación de inicio de sesión único.

Se aplica a:

- macOS 10.15 y versiones más recientes

Cambios en la configuración de contraseñas en los perfiles de restricción de dispositivos para el administrador de dispositivos Android

Recientemente hemos agregado *Complejidad de la contraseña* como nuevo valor de configuración para la directiva Conformidad de dispositivos y la restricción de dispositivos para el *Administrador de dispositivos Android*. Ahora hemos agregado más cambios a la interfaz de usuario para los valores de configuración de ambos tipos de directiva, con el fin de ayudar a Intune a integrar los cambios de las contraseñas en Android versión 10 y posteriores. Estos cambios ayudan a garantizar que la configuración de contraseñas siga aplicándose a los dispositivos según lo previsto.

Encontrará los siguientes cambios en la interfaz de usuario de Intune para la configuración de contraseñas para los dos tipos de directivas, que no afectarán a los perfiles existentes:

- Los valores de configuración se reorganizan en secciones que se basan en las versiones de dispositivo a las que se aplican los valores, como Android 9 y versiones anteriores o Android 10 y versiones posteriores.
- Actualizaciones en etiquetas y texto de ejemplo en la interfaz de usuario.
- Aclaraciones en las referencias a los PIN como *numéricos*, *alfabéticos* o *alfanuméricos*.

Se aplica a:

- Administrador de dispositivos Android

Versión nueva del conector de certificados PFX

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2008.60.612**. Esta nueva versión del conector:

- Se conrrige un problema con la entrega de certificados PKCS a dispositivos Android Enterprise totalmente administrados. El problema requiere que el proveedor de almacenamiento de claves (KSP) de cifrado sea un proveedor heredado. Ahora también puede usar un proveedor de almacenamiento de claves de cifrado de nueva generación (CNG).
- Cambios en la pestaña *Cuenta de CA* del conector de certificados PFX: El nombre de usuario y la contraseña (credenciales) que especifique se usarán para emitir y revocar certificados. Anteriormente, estas credenciales solo se usaban para la revocación de certificados.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, consulte Conectores de certificados.

Inscripción de dispositivos

Compatibilidad de Intune con el aprovisionamiento de dispositivos compartidos de Azure Active Directory

Con Intune, ahora puede aprovisionar dispositivos de Android Enterprise dedicados con Microsoft Authenticator configurado automáticamente en el modo de dispositivo compartido de Azure AD. Para más información sobre cómo usar este tipo de inscripción, consulte Configuración de la inscripción en Intune de dispositivos dedicados de Android Enterprise.

Guías de implementación de planeamiento, configuración e inscripción nuevas y actualizadas

Las guías de planeamiento y migración existentes se reescriben y se actualizan con nuevas instrucciones. También hay algunas guías de implementación nuevas que se centran en la configuración de Intune y la inscripción de dispositivos Android, iOS/iPadOS, macOS y Windows.

Para obtener más información, vaya a Información general.

Seguridad de dispositivos

Actualización de Microsoft Tunnel

Hemos publicado una nueva versión de Puerta de enlace de Microsoft Tunnel, que incluye los siguientes cambios:

- Correcciones en el registro. Puede ver los registros del sistema de Microsoft Tunnel al ejecutar la línea de comandos *journalctl -t mstunnel_monitor* en el servidor de túnel.
- Corrección de errores adicionales.

El servidor de Puerta de enlace de Microsoft Tunnel se actualizará automáticamente a la nueva versión.

Compatibilidad con directivas de protección de aplicaciones en Android y iOS/iPadOS para asociados adicionales

En octubre de 2019, la directiva de protección de aplicaciones de Intune agregó la capacidad de usar datos de nuestros asociados de Microsoft Threat Defense.

Con esta actualización, ampliamos esta compatibilidad a los dos asociados siguientes para usar una directiva de

protección de aplicaciones a fin de bloquear o borrar de forma selectiva los datos corporativos de un usuario en función del estado del dispositivo:

- **Check Point Sandblast** en Android, iOS y iPadOS
- **Symantec Endpoint Security** en Android, iOS y iPadOS

Para más información, consulte Creación de una directiva de protección de aplicaciones de Mobile Threat Defense con Intune.

Las tareas de seguridad de Microsoft Endpoint Manager incluyen información detallada sobre la configuración incorrecta de TVM en Microsoft Defender para punto de conexión.

Las tareas de seguridad de Microsoft Endpoint Manager ahora informan sobre las configuraciones incorrectas detectadas por Threat Vulnerability Management (TVM) y proporcionan detalles para su corrección. Los errores de configuración que se comunican a Intune se limitan a los problemas para cuya corrección se pueden ofrecer instrucciones.

TVM forma parte de Microsoft Defender para punto de conexión. Antes de esta actualización, los detalles de TVM solo incluían los detalles y los pasos de corrección para las aplicaciones.

Al ver las tareas de seguridad, encontrará una nueva columna denominada *Remediation Type* (Tipo de corrección) que identifica el tipo de problema:

- Aplicación: aplicaciones vulnerables y pasos de corrección. Ha estado disponible en tareas de seguridad antes de esta actualización.
- Configuración: nueva categoría de detalles de TVM que identifica errores de configuración y ofrece pasos de ayuda para solucionarlos.

Para más información sobre las tareas de seguridad, vea Uso de Intune para corregir las vulnerabilidades que identifica Microsoft Defender para punto de conexión.

Directivas de firewall de seguridad de los puntos de conexión para dispositivos asociados al inquilino

Como versión preliminar pública, puede implementar la directiva de firewalls de seguridad de los puntos de conexión en los dispositivos que se administran con Configuration Manager. Para hacer posible este escenario, es necesario configurar una asociación de inquilinos entre una versión admitida de Configuration Manager y la suscripción de Intune.

La directiva de firewalls sobre dispositivos asociados de inquilino es compatible con dispositivos que ejecutan *Windows 10 y versiones posteriores* y requiere que en el entorno se ejecute la *versión 2006 de la rama actual de Configuration Manager* con la revisión *KB4578605* en la consola.

Para más información, consulte los requisitos de las directivas de seguridad de punto de conexión de Intune para admitir la asociación de inquilinos.

Configuración expandida para administrar la instalación de dispositivos de hardware a través de listas de bloqueados y de permitidos

En los perfiles de **control de dispositivos**, que forman parte de la directiva de reducción de la superficie expuesta a ataques para la seguridad de puntos de conexión, hemos revisado y ampliado nuestra configuración para administrar la instalación de dispositivos de hardware. Ahora encontrará opciones de configuración que permiten definir listas de *bloqueados* y listas independientes de *permitidos* con *identificadores de dispositivo*, *clases de instalación* e *identificadores de instancia*. Ahora están disponibles las seis opciones siguientes:

- Allow hardware device installation by device identifiers (Permitir instalación de dispositivos de hardware mediante identificadores de dispositivo)
- Block hardware device installation by device identifiers (Bloquear instalación de dispositivos de hardware mediante identificadores de dispositivo)
- Allow hardware device installation by setup class (Permitir instalación de dispositivos de hardware mediante clases de instalación)
- Block hardware device installation by setup class (Bloquear instalación de dispositivos de hardware mediante

clases de instalación)

- Allow hardware device installation by device instance identifiers (Permitir instalación de dispositivos de hardware mediante identificadores de dispositivo)
- Block hardware device installation by device instance identifiers (Bloquear instalación de dispositivos de hardware mediante identificadores de dispositivo)

Cada uno de estos valores admite las opciones *Sí*, *No* y *Sin configurar*. Si se configura en *Sí*, se puede definir la lista de bloqueados o de permitidos para esa opción. En un dispositivo, se puede instalar o actualizar el hardware que se especifica en una lista de permitidos. Sin embargo, si se especifica el mismo hardware en una lista de bloqueados, dicha lista invalida la de permitidos y se impide la instalación o actualización del hardware.

Mejoras en las reglas de firewall de la seguridad de los puntos de conexión

Hemos realizado varios cambios para mejorar la experiencia de configuración de reglas de firewall en el perfil de reglas de firewall de Microsoft Defender de la directiva de firewall de seguridad de los puntos de conexión.

Estas mejoras incluyen:

- Diseño mejorado en la interfaz de usuario, incluidos los encabezados de sección para organizar la vista.
- Aumento del límite de caracteres para el campo de descripción.
- Validación de las entradas de direcciones IP.
- Ordenación de listas de direcciones IP.
- Opción para *seleccionar todas* las direcciones cuando se borran entradas de una lista de direcciones IP.

Uso de Microsoft Defender para punto de conexión en directivas de cumplimiento para iOS

Como versión preliminar pública, ahora puede usar la directiva de cumplimiento de dispositivos de Intune para incorporar dispositivos iOS a Microsoft Defender para punto de conexión.

Una vez que haya incorporado los dispositivos iOS/iPadOS inscritos, las directivas de cumplimiento para iOS pueden usar las señales de *nivel de amenaza* de Microsoft Defender. Son las mismas señales que se pueden usar para dispositivos Android y Windows 10.

Al final del año, la aplicación Defender para iOS debe pasar de versión preliminar pública a disponibilidad general.

Los perfiles de experiencia de seguridad de la directiva de antivirus para la seguridad de los puntos de conexión ahora tienen opciones de tres estados.

Hemos agregado un tercer estado de configuración en las opciones del perfil *Experiencia de Seguridad de Windows* para las directivas de antivirus de seguridad de los puntos de conexión. Esta actualización se aplica a la experiencia de Seguridad de Windows para Windows 10 y versiones posteriores).

Por ejemplo, si una opción ofrecía anteriormente **Sin configurar** y **Sí**, ahora, si la plataforma lo admite, tiene la opción adicional **No**.

Versión actualizada de la línea de base de seguridad de Edge

Hemos agregado una nueva línea de base de seguridad de Edge en Intune: Septiembre de 2020 (Edge versión 85 y posteriores).

Las versiones de línea base actualizadas proporcionan compatibilidad con los valores de configuración recientes para ayudarle a mantener las configuraciones que recomiendan los equipos de producto respectivos.

Para saber qué ha cambiado entre las versiones, en Comparación de versiones de línea de base aprenderá a exportar un archivo .CSV que muestre los cambios.

Nueva versión de Microsoft Tunnel

Hemos publicado una nueva versión de Puerta de enlace de Microsoft Tunnel. En la nueva versión se incluyen los cambios siguientes:

- Microsoft Tunnel ahora registra los detalles operativos y de supervisión en los registros del servidor Linux en

el formato *syslog*. Puede ver los registros del sistema de Microsoft Tunnel al ejecutar la línea de comandos `journalctl -t` en el servidor de túnel.

- Se corrigieron varios errores.

Supervisión y solución de problemas

Nuevo informe de errores de actualización de características de Windows 10

El informe operativo de **errores de actualización de características** proporciona detalles sobre los errores de los dispositivos que se establecen como destino mediante una directiva de **actualizaciones de características de Windows 10** y que han intentado llevar a cabo una actualización. En el centro de administración de Microsoft Endpoint Manager, seleccione **Dispositivos** > **Monitor** > **Feature update failures** (Errores de actualización de características) para ver este informe. Para obtener más información, vea el apartado sobre el informe de errores de actualización de características.

Actualizaciones de informes de antivirus

Se han actualizado los informes **Estado del agente de antivirus** y **Malware detectado**. Estos informes ahora muestran visualizaciones de datos y proporcionan columnas adicionales de información (**SignatureUpdateOverdue**, **MalwareID**, **displayName** e **InitialDetectionDateTime**). Además, se incluyen acciones remotas en el informe Estado del agente de antivirus. Para más información, consulte los informes Estado del agente de antivirus y Malware detectado.

Ayuda y soporte técnico actualizados para Microsoft Endpoint Manager

La experiencia de ayuda y soporte técnico utiliza aprendizaje automático para mostrar soluciones, diagnósticos y conclusiones que le ayudarán a resolver los problemas. Hemos actualizado la página de ayuda y soporte técnico del Centro de administración de Microsoft Endpoint Manager con una experiencia de usuario nueva y coherente que facilita la navegación. La nueva experiencia de usuario se ha implementado en todas las hojas de la consola y nos ayudará a obtener ayuda más pertinente.

Ahora encontrará una experiencia de soporte técnico actualizada y consolidada para las siguientes ofertas basadas en la nube desde el Centro de administración:

- **Intune**
- **Administrador de configuración**
- **Administración conjunta**
- **Escritorio administrado de Microsoft**

Scripts

Vista de scripts de PowerShell en el panel de solución de problemas de Intune

Ahora puede ver los scripts de PowerShell asignados en el panel de solución de problemas. Los scripts de PowerShell proporcionan comunicación de cliente de Windows 10 con Intune para ejecutar tareas de administración empresarial, como la configuración avanzada de dispositivos y la solución de problemas. Para más información, consulte Uso de scripts de PowerShell para dispositivos Windows 10 en Intune.

Recopilación de propiedades de dispositivo o de usuario personalizadas mediante scripts de shell en equipos Mac administrados

Puede crear un perfil de atributo personalizado que le permita recopilar propiedades personalizadas de un dispositivo macOS administrado mediante scripts de shell. Puede encontrar esta característica en el Centro de administración de Microsoft Endpoint Manager si selecciona **Dispositivos** > **macOS** > **Atributos personalizados**. Para obtener información relacionada, vea Uso de scripts de shell para dispositivos macOS en Intune.

Septiembre de 2020

Administración de aplicaciones

Mejora en la mensajería del perfil de trabajo en el Portal de empresa para Android

La pantalla del Portal de empresa que antes se titulaba "Ya va por la mitad" se ha actualizado para que explique mejor cómo funciona la administración de perfiles de trabajo. Los usuarios verán esta pantalla si vuelven a

habilitar el Portal de empresa en el perfil personal una vez que hayan realizado la inscripción del perfil de trabajo. También pueden ver esta pantalla durante la inscripción del perfil de trabajo en algunas versiones del sistema operativo Android, tal como se muestra en el documento de ayuda titulado Inscribir dispositivos con perfil profesional Android.

Entrega unificada de aplicaciones de Azure AD Enterprise y Office Online en el Portal de empresa de Windows

En la versión de 2006, anunciamos la entrega unificada de aplicaciones de Azure AD Enterprise y Office Online en el sitio web del Portal de empresa. Esta característica se admite en el Portal de empresa de Windows. En el panel **Personalización** de Intune, seleccione **Ocultar** o **Mostrar aplicaciones de Azure AD Enterprise** y **aplicaciones de Office Online** en el Portal de empresa de Windows. Cada usuario final verá todo el catálogo de aplicaciones desde el servicio de Microsoft elegido. De forma predeterminada, cada origen de aplicación adicional se establecerá en **Ocultar**. Para encontrar esta opción de configuración, seleccione **Administración de inquilinos** > **Personalización** en el Centro de administración de Microsoft Endpoint Manager. Para obtener información relacionada, vea Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune.

Descripciones de la aplicación Portal de empresa de Windows con texto enriquecido

Con Markdown, ahora puede mostrar descripciones de aplicaciones con texto enriquecido en el Portal de empresa de Windows. Para más información sobre el Portal de empresa de Intune, consulte Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune.

Permiso de directivas de protección de aplicaciones para que los administradores configuren las ubicaciones de datos entrantes de la organización

Ahora puede controlar qué orígenes de datos de confianza pueden abrirse en los documentos de la organización. De forma similar a la opción existente **Guardar copias de los datos de la organización** de la directiva de protección de aplicaciones, puede definir qué ubicaciones de datos entrantes son de confianza. Esta funcionalidad se relaciona con la siguiente configuración de la directiva de protección de aplicaciones:

- **Guardar copias de los datos de la organización**
- **Abrir datos en documentos de la organización**
- **Permitir a los usuarios abrir datos de servicios seleccionados**

En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Directivas de protección de aplicaciones** > **Crear directiva**. Para usar esta funcionalidad, las aplicaciones administradas por directivas de Intune deben implementar la compatibilidad con este control. Para más información, consulte Configuración de directivas de protección de aplicaciones de iOS y Configuración de directivas de protección de aplicaciones de Android.

Configuración del dispositivo

Actualización de la versión preliminar COPE: nuevas opciones de configuración para crear requisitos para la contraseña del perfil de trabajo de dispositivos de propiedad corporativa de Android Enterprise con un perfil de trabajo

Las nuevas opciones de configuración permiten a los administradores establecer requisitos para la contraseña del perfil de trabajo de dispositivos de propiedad corporativa de Android Enterprise con un perfil de trabajo:

- Tipo de contraseña obligatoria
- Longitud mínima de la contraseña
- Número de días hasta que expire la contraseña
- Número de contraseñas requeridas antes de que el usuario pueda reusar una
- Número de errores de inicio de sesión antes de borrar el dispositivo

Para más información, consulte Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

Actualización de la versión preliminar COPE: nuevas opciones para configurar el perfil personal de dispositivos de propiedad corporativa de Android Enterprise con un perfil de trabajo

En el caso de los dispositivos de propiedad corporativa de Android Enterprise con un perfil de trabajo, hay nuevas opciones de configuración que solo se aplican al perfil personal (**Dispositivos** > **Perfiles de**

configuración > **Crear perfil** > **Android Enterprise** > para la plataforma **Perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado** > **Restricciones de dispositivos** para el perfil > **Perfil personal**):

- **Cámara**: use esta opción para bloquear el acceso a la cámara durante el uso personal.
- **Captura de pantalla**: use esta opción para bloquear las capturas de pantalla durante el uso personal.
- **Permitir que los usuarios habiliten la instalación de aplicaciones de orígenes desconocidos en el perfil personal**: use esta opción para permitir que los usuarios instalen aplicaciones de orígenes desconocidos en el perfil personal.

Se aplica a:

- dispositivos de propiedad corporativa de Android Enterprise con un perfil de trabajo y dispositivos con habilitación personal.

Para ver todos los valores que puede configurar, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características.

Análisis de GPO locales mediante el análisis de directivas de grupo

En **Dispositivos** > **Análisis de directivas de grupo (versión preliminar)** , puede importar objetos de directiva de grupo (GPO) en el centro de administración de Endpoint Manager. Al realizar la importación, Intune analiza automáticamente el GPO y muestra las directivas que tienen una configuración equivalente en Intune. También se muestran los GPO que están en desuso o que ya no son compatibles. Para obtener más información, vaya a **Informes** > **Análisis de directivas de grupo (vista previa)** > Migration readiness report (Informe de preparación para la migración).

Para obtener más información sobre esta característica, consulte Análisis de directivas de grupo.

Se aplica a:

- Windows 10 y versiones posteriores

Bloqueo de clips de aplicación en iOS/iPadOS y aplazamiento de las actualizaciones de software que no sean del sistema operativo en dispositivos macOS

Cuando se crea un perfil de restricciones de dispositivos en dispositivos iOS/iPadOS y macOS, hay algunos valores de configuración nuevos:

iOS/iPadOS 14.0 y versiones posteriores: bloqueo de clips de aplicación

- Se aplica a iOS/iPadOS 14.0 y versiones posteriores.
- Los dispositivos deben haberse inscrito con la inscripción de dispositivos o con la inscripción de dispositivos automatizada (dispositivos supervisados).
- La opción **Bloquear clips de aplicación** bloquea los clips de aplicación en los dispositivos administrados (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** para la plataforma > **Restricciones de dispositivos** para el perfil > **General**). Cuando se bloquean, los usuarios no pueden agregar ningún clip de aplicación y se quitan los clips existentes.

macOS 11 y versiones posteriores: aplazamiento de las actualizaciones de software

- Se aplica a macOS 11 y versiones posteriores. En dispositivos macOS supervisados, el dispositivo debe tener la inscripción de dispositivos aprobada por el usuario o haberse inscrito a través de la inscripción de dispositivos automatizada.
- La opción existente **Aplazar las actualizaciones de software** ahora puede retrasar las actualizaciones tanto del sistema operativo como las que no son del sistema operativo (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** para la plataforma > **Restricciones de dispositivos** para el perfil > **General**). La opción existente **Retrasar la visibilidad de las actualizaciones de software** se aplica a las actualizaciones tanto del sistema operativo como las que no son del sistema operativo. El

aplazamiento de las actualizaciones de software que no sean del sistema operativo no afectará a las actualizaciones programadas.
- El comportamiento de las directivas existentes no cambia ni se elimina, y tampoco se ve afectado. Las directivas existentes se migrarán automáticamente a la nueva opción con la misma configuración.

Para ver las opciones de restricciones de dispositivos que se pueden configurar, consulte iOS/iPadOS y macOS.

Nuevas opciones de configuración con VPN por aplicación o VPN a petición en dispositivos iOS/iPad y macOS

Puede configurar perfiles de VPN automática en **Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPados** o **macOS** para la plataforma > **VPN** para el perfil > **VPN automática**. Hay nuevas opciones de VPN por aplicación que se pueden configurar:

- **Impedir que los usuarios deshabiliten la VPN automática**: al crear una conexión **VPN por aplicación** automática o **VPN a petición**, puede obligar a los usuarios a conservar la VPN automática habilitada y en ejecución.
- **Dominios asociados**: al crear una conexión **VPN por aplicación** automática, se pueden agregar dominios asociados en el perfil de VPN que inicien automáticamente la conexión VPN. Para obtener más información sobre los dominios asociados, vea Dominios asociados.
- **Dominios excluidos**: al crear una conexión **VPN por aplicación** automática, se pueden agregar dominios que puedan omitir la conexión VPN cuando se conecte la VPN por aplicación.

Para ver estas opciones y otras que se pueden configurar, vaya a Configuración de VPN en iOS/iPadOS y Configuración de VPN en macOS.

Configure la red privada virtual (VPN) por aplicación para dispositivos iOS/iPadOS.

Se aplica a:

- iOS/iPadOS 14 y versiones más recientes
- macOS Big Sur (macOS 11)

Establecimiento de la unidad de transmisión máxima para las conexiones VPN de IKEv2 en dispositivos iOS/iPadOS

A partir de iOS/iPadOS 14 y dispositivos más recientes, se puede configurar una unidad de transmisión máxima (MTU) personalizada al usar conexiones VPN de IKEv2 (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** para la plataforma > **VPN** para el perfil > **IKEv2** para el tipo de conexión).

Para obtener más información sobre esta opción y otras que se pueden configurar, vea Configuración de IKEv2.

Se aplica a:

- iOS/iPadOS 14 y versiones más recientes

Conexión VPN según la cuenta para perfiles de correo electrónico en dispositivos iOS/iPadOS

A partir de iOS/iPadOS 14, el tráfico de correo electrónico de la aplicación de correo nativa se puede enrutar a través de una VPN en función de la cuenta que emplea el usuario. En Intune, puede establecer la configuración del **perfil de VPN para la VPN según la cuenta** (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** > para la plataforma **Correo electrónico** > para el perfil **Configuración del correo electrónico de Exchange ActiveSync**).

Esta característica permite seleccionar un perfil de VPN según la aplicación para usarlo con una conexión VPN en función de la cuenta. La conexión VPN según la aplicación se activa automáticamente cuando los usuarios emplean la cuenta de la organización en la aplicación de correo.

Para ver esta opción y las demás que se pueden configurar, vaya a Incorporación de la configuración de correo electrónico para dispositivos iOS e iPadOS.

Se aplica a:

- iOS/iPadOS 14 y versiones más recientes

Deshabilitación de la selección aleatoria de direcciones MAC en redes Wi-Fi en dispositivos iOS/iPadOS

A partir de iOS/iPadOS 14, de forma predeterminada, los dispositivos presentan una dirección MAC aleatoria, en lugar de la dirección MAC física, al conectarse a una red. Este comportamiento se recomienda por cuestiones de privacidad, ya que es más difícil realizar un seguimiento de un dispositivo mediante su dirección MAC. Esta característica también interrumpe las funciones que se basan en una dirección MAC estática, incluido el control de acceso a la red (NAC).

Puede deshabilitar la selección aleatoria de direcciones MAC en función de la red en los perfiles de Wi-Fi (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** > para la plataforma > **Wi-Fi** para el perfil > **Básico** o **Empresa** para el tipo de Wi-Fi).

Para ver esta opción y las demás que se pueden configurar, vaya a Adición de configuración de Wi-Fi para dispositivos iOS/iPadOS.

Se aplica a:

- iOS/iPadOS 14 y versiones más recientes

Nueva configuración para perfiles de control de dispositivos

Hemos agregado un par de opciones en el perfil de *control de dispositivos* para la directiva de *reducción de la superficie expuesta a ataques* para los dispositivos que ejecutan Windows 10 o versiones posteriores:

- **Almacenamiento extraíble**
- **Conexiones USB (solo HoloLens)**

La directiva de *reducción de la superficie expuesta a ataques* forma parte de la seguridad de puntos de conexión en Intune.

Inscripción de dispositivos

En la página Estado de inscripción se muestran directivas de pantalla completa críticas

Ahora podrá ver el seguimiento de las siguientes directivas en la página Estado de inscripción:

- Acceso asignado
- Configuración del explorador en pantalla completa
- Configuración del explorador Edge

Actualmente no se realiza un seguimiento de las demás directivas de pantalla completa.

Administración de dispositivos

Compatibilidad con baterías PowerPrecision y PowerPrecision+ para dispositivos Zebra

En la página de detalles del hardware de un dispositivo, ahora se puede ver la siguiente información sobre los dispositivos Zebra que usan baterías PowerPrecision y PowerPrecision+:

- Valoración del estado de mantenimiento según Zebra (solo en baterías PowerPrecision+)
- Número de ciclos de carga completos consumidos
- Fecha de la última sincronización de la última batería que se encontró en el dispositivo
- Número de serie de la última batería que se encontró en el dispositivo

Actualización de la versión preliminar COPE: restablecimiento de la contraseña del perfil para dispositivos de propiedad corporativa de Android Enterprise con un perfil de trabajo

Ahora se puede restablecer la contraseña del perfil de trabajo en dispositivos de propiedad corporativa de Android Enterprise con un perfil de trabajo. Para obtener más información, vea Restablecimiento de un código de acceso.

Cambio del nombre de un dispositivo administrado de forma conjunta unido a Azure Active Directory

Ahora se puede cambiar el nombre de un dispositivo administrado de forma conjunta que esté unido a Azure AD. Para más información, vea Cambio de nombre de un dispositivo en Intune.

Asociación de inquilinos: escala de tiempo del dispositivo en el centro de administración

Cuando Configuration Manager sincroniza un dispositivo con Microsoft Endpoint Manager de Microsoft a través de una asociación de inquilinos, podrá ver una escala de tiempo de eventos. Esta escala de tiempo muestra la actividad pasada en el dispositivo que puede ayudarle a solucionar problemas. Para más información, consulte Asociación de inquilinos: escala de tiempo del dispositivo en el centro de administración.

Asociación de inquilinos: explorador de recursos en el centro de administración

Desde el centro de administración del punto de conexión de Microsoft, puede ver el inventario de hardware para los dispositivos Configuration Manager cargados mediante el explorador de recursos. Para más información, consulte Asociación de inquilinos: explorador de recursos en el centro de administración.

Asociación de inquilinos: CMPivot desde el centro de administración

Incorpore la eficacia de CMPivot al centro de administración de Microsoft Endpoint Manager. Permita que otros roles, como el de Departamento de soporte técnico, puedan iniciar consultas en tiempo real desde la nube en un dispositivo individual administrado por ConfigMgr y devolver los resultados al centro de administración. Esto proporciona todas las ventajas tradicionales de CMPivot, permitiendo a los administradores de TI y a otros roles designados evaluar rápidamente el estado de los dispositivos en su entorno y tomar medidas.

Para obtener más información sobre CMPivot desde el centro de administración, vea Requisitos previos de CMPivot, Información general de CMPivot y Scripts de ejemplo CMPivot.

Asociación de inquilinos: ejecución de scripts desde el centro de administración

Incorpore la eficacia de la característica Ejecutar scripts local de Configuration Manager al centro de administración de Microsoft Endpoint Manager. Permita que otros roles, como el de Departamento de soporte técnico, ejecuten scripts de PowerShell desde la nube en un dispositivo administrado de Configuration Manager individual en tiempo real. Esta característica proporciona todas las ventajas tradicionales de los scripts de PowerShell que ya ha definido y aprobado el administrador de Configuration Manager en este nuevo entorno. Para más información, consulte Asociación de inquilinos: ejecución de scripts desde el centro de administración.

Directiva de protección contra alteraciones para dispositivos con asociación de inquilinos en versión preliminar

En la versión preliminar, hemos agregado un nuevo perfil a la directiva de antivirus de seguridad de puntos de conexión de Intune que se puede usar para administrar la protección contra alteraciones en dispositivos con asociación de inquilinos: **Experiencia de Seguridad de Windows (versión preliminar)** .

El nuevo perfil se encuentra en la plataforma *Windows 10 y Windows Server (ConfigMgr)* cuando se crea una directiva antivirus.

Para poder usar las directivas de seguridad de puntos de conexión de Intune con los dispositivos con asociación de inquilinos, tiene que configurar la asociación de inquilinos en Configuration Manager y sincronizar los dispositivos con Intune.

También debe tener en cuenta los requisitos previos específicos que son necesarios para usar y admitir la protección contra alteraciones con la directiva de Intune.

Seguridad de dispositivos

Solución VPN de puerta de enlace de Microsoft Tunnel en versión preliminar

Ahora puede implementar la puerta de enlace de Microsoft Tunnel para proporcionar acceso remoto a recursos locales en dispositivos iOS y Android Enterprise (totalmente administrados, perfil de trabajo de propiedad corporativa, perfil de trabajo).

Microsoft Tunnel es compatible con VPN por aplicación y de dispositivo completo, tunelización dividida y funcionalidades de acceso condicional mediante la autenticación moderna. Tunnel puede admitir varios servidores de puerta de enlace para lograr una alta disponibilidad para la preparación de la producción.

Compatibilidad de autenticación biométrica adicional para dispositivos Android

Los nuevos dispositivos Android usan un conjunto más diverso de opciones biométricas, más allá de las huellas digitales. Cuando los OEM implementan la compatibilidad con opciones biométricas diferentes de las huellas

digitales, los usuarios finales pueden usar esta funcionalidad para disfrutar de un acceso seguro y una mejor experiencia. Con la versión de 2009 de Intune, puede permitir que los usuarios finales usen la huella digital o el desbloqueo facial, en función de lo que admita el dispositivo Android. Puede configurar si se pueden usar todos los tipos biométricos, además de la huella digital, para realizar la autenticación. Para obtener más información, consulte Experiencia de protección de aplicaciones para dispositivos Android.

Nuevos detalles de la configuración de seguridad de los puntos de conexión para un dispositivo

Ahora se pueden visualizar más detalles de los dispositivos como parte de la *configuración de seguridad de los puntos de conexión* de un dispositivo. Cuando profundice en los detalles del estado de las directivas que ha implementado en los dispositivos, ahora encontrará el siguiente valor de configuración:

- **UPN** (Nombre principal del usuario): el UPN identifica el perfil de seguridad de los puntos de conexión que se ha asignado a un usuario determinado del dispositivo. Esta información es útil para diferenciar entre varios usuarios de un dispositivo y varias entradas de un perfil o línea base que se han asignado al dispositivo.

Para obtener más información, vea Resolución de conflictos para las líneas de base de seguridad.

Permisos de RBAC expandidos para el rol de seguridad de los puntos de conexión

El rol **Administrador de seguridad de los puntos de conexión** para Intune tiene permisos adicionales de control de acceso basado en rol (RBAC) para **tareas remotas**.

Este rol concede acceso al centro de administración de Microsoft Endpoint Manager y lo pueden usar las personas que administran las características de seguridad y cumplimiento, incluidas las líneas de base de seguridad, el cumplimiento de dispositivos, el acceso condicional y Microsoft Defender para punto de conexión.

Entre los nuevos permisos para *tareas remotas* se incluyen los siguientes:

- Reiniciar ahora
- Bloqueo remoto
- Rotar las claves de BitLocker (versión preliminar)
- Rotar la clave de FileVault
- Sincronizar dispositivos
- Microsoft Defender
- Iniciar una acción de Configuration Manager

Para ver el conjunto completo de permisos de un rol de RBAC de Intune, vaya a (**Administración de inquilinos** > **Roles de Intune** > *seleccione un rol* > **Permisos**).

Actualizaciones para líneas base de seguridad

Hay nuevas versiones disponibles para las siguientes líneas de base de seguridad:

- **Línea base de seguridad de MDM (Seguridad de Windows 10)**
- **Línea base de Microsoft Defender para punto de conexión**

Las versiones de línea base actualizadas proporcionan compatibilidad con los valores de configuración recientes para ayudarle a mantener las configuraciones que recomiendan los equipos de producto respectivos.

Para saber qué ha cambiado entre las versiones, en Comparación de versiones de línea de base aprenderá a exportar un archivo .CSV que muestre los cambios.

Uso de los detalles de configuración de la seguridad de los puntos de conexión para identificar el origen de conflictos de directivas en los dispositivos.

Para contribuir a la resolución de conflictos, ya puede explorar los perfiles de línea base de seguridad para ver la *configuración de seguridad de los puntos de conexión* de un dispositivo seleccionado. A partir de ahí, podrá seleccionar las opciones de configuración que muestren *Conflicto* o *Error* y seguir profundizando para ver una lista de detalles, con los perfiles y las directivas que forman parte del conflicto.

Si después selecciona una directiva que es el origen de un conflicto, Intune abrirá el panel de información general de la directiva, desde donde podrá revisar o modificar la configuración de la directiva.

Los siguientes tipos de directivas pueden identificarse como orígenes de conflicto cuando se explora una línea base de seguridad:

- Directiva de configuración de dispositivos
- Directivas de seguridad de puntos de conexión

Para obtener más información, vea Resolución de conflictos para las líneas de base de seguridad.

Compatibilidad con certificados con un tamaño de clave de 4096 bits en dispositivos iOS y macOS

Al configurar un perfil de *certificado SCEP* para dispositivos iOS/iPadOS o macOS, ahora puede especificar un **tamaño de la clave (bits)** de **4096** bits.

Intune admite las claves de 4096 bits para las siguientes plataformas:

- iOS 14 y versiones posteriores
- macOS 11 y versiones posteriores

Para configurar perfiles de certificado SCEP, consulte Creación de un perfil de certificado SCEP.

Android 11 ha dejado de usar la implementación de certificados raíz de confianza en dispositivos inscritos por el administrador de dispositivos

A partir de Android 11, los certificados raíz de confianza ya no pueden instalar el certificado raíz de confianza en un dispositivo que esté inscrito como *administrador de dispositivos Android*. Esta limitación no afecta a dispositivos Samsung Knox. En el caso de dispositivos que no son Samsung, los usuarios deben instalar manualmente el certificado raíz de confianza en el dispositivo.

Después de instalar manualmente el certificado raíz de confianza en un dispositivo, puede usar SCEP para aprovisionar certificados en el dispositivo. Sigue teniendo que crear e implementar una directiva de *certificado de confianza* en el dispositivo y vincularla al perfil del *certificado SCEP*.

- Si el certificado raíz de confianza está en el dispositivo, el perfil de certificado SCEP se puede instalar correctamente.
- Si no se encuentra el certificado de confianza en el dispositivo, se producirá un error en el perfil de certificado SCEP.

Para obtener más información, vea Perfiles de certificado de confianza para el administrador de dispositivos Android.

Opciones de tres estados para más valores de configuración en la directiva de firewall de seguridad de los puntos de conexión

Hemos agregado un tercer estado de configuración a unos cuantos valores en directivas de firewall de seguridad de los puntos de conexión para Windows 10.

Se han actualizado los valores siguientes:

- El **protocolo de transferencia de archivos (FTP) con estado** ahora admite *No configurado*, *Permitir* y *Deshabilitado*.
- **Requerir que los módulos de generación de claves solo ignoren los conjuntos de autenticación que no admiten** ahora admite *No configurado*, *Habilitado* y *Deshabilitado*.

Implementación de certificados mejorada para Android Enterprise

Hemos mejorado la compatibilidad con el uso de certificados S/MIME para Outlook para el cifrado y la firma en dispositivos Android Enterprise que se inscriben como perfiles de trabajo de propiedad corporativa, dedicados y totalmente administrados. Antes, el uso de S/MIME requería que el usuario del dispositivo permitiera el acceso. Ahora, los certificados S/MIME se pueden usar sin interacción del usuario.

Para implementar certificados S/MIME en dispositivos Android compatibles, use un perfil de certificado PKCS

importado o un perfil de certificado SCEP para la configuración del dispositivo. Cree un perfil para **Android Enterprise** y seleccione **Certificado PKCS importado** en la categoría para el *perfil de trabajo de propiedad corporativa, dedicado y totalmente administrado*.

Detalles de estado mejorados en los informes de línea base de seguridad

Hemos empezado a mejorar muchos de los detalles de estado de la línea de base de seguridad. Ahora verá el estado más significativo y detallado al consultar la información sobre las versiones de línea de base que ha implementado.

En concreto, al seleccionar una línea base, una *Versión* y una instancia de esa línea base, en la información general inicial se mostrarán los detalles siguientes:

- Gráfico **Posición de línea de base de seguridad**: en este gráfico ahora se muestran los siguientes detalles de estado:
  - **Coincide con la línea de base predeterminada**: este estado reemplaza a *Coincide con la línea de base* e identifica cuándo la configuración de un dispositivo coincide con la configuración de línea de base predeterminada (sin modificar).
  - **Matches custom settings** (Coincide con la configuración personalizada): este estado identifica cuándo la configuración de un dispositivo coincide con la línea base que ha configurado (personalizado) e implementado.
  - **Configuración errónea**: este estado es una acumulación que representa tres condiciones de estado de un dispositivo: *Error*, *Pendiente* o *Conflicto*. Estos estados independientes están disponibles en otras vistas, tal como se indica a continuación.
  - **No aplicable**: este estado representa un dispositivo que no puede recibir la directiva. Por ejemplo, la directiva actualiza una configuración específica de la versión más reciente de Windows, pero el dispositivo ejecuta una versión anterior que no es compatible con esa configuración.
- **Posición de línea de base de seguridad por categoría**: se trata de una vista de lista en la que se muestra el estado del dispositivo por categoría. Las columnas disponibles reflejan en gran medida el gráfico *Posición de línea de base de seguridad*, pero en lugar de *Configuración errónea* verá tres columnas para el estado que componen la configuración errónea:
  - **Error**: no se ha podido aplicar la directiva. El mensaje se suele mostrar con un código de error vinculado a una explicación.
  - **Conflicto**: se aplican dos configuraciones al mismo dispositivo, e Intune no puede solucionar el conflicto. Un administrador debe encargarse de revisar.
  - **Pendiente**: el dispositivo no se ha registrado aún con Intune para recibir la directiva.

Nuevo valor para configurar la complejidad de la contraseña para Android 10 y versiones posteriores para dispositivos inscritos por el administrador de dispositivos

Con el fin de admitir nuevas opciones para Android 10 y versiones posteriores en dispositivos inscritos por el administrador de dispositivos Android, hemos agregado un nuevo valor de configuración denominado **Complejidad de la contraseña** a las directivas *Conformidad de dispositivos* y *Restricciones de dispositivos*. Este nuevo valor de configuración se usa para administrar el *grado* de seguridad de la contraseña según el tipo, la longitud y la calidad de la contraseña.

La complejidad de la contraseña no se aplica a los dispositivos Samsung Knox. En estos dispositivos, los valores de configuración de longitud y tipo de contraseña invalidan el de complejidad de la contraseña.

La complejidad de la contraseña admite las siguientes opciones:

- **Ninguno**: sin contraseña.
- **Bajo**: la contraseña cumple uno de los siguientes requisitos:
  - Patrón
  - PIN con secuencias repetidas (4444) u ordenadas (1234, 4321, 2468).
- **Medio**: la contraseña cumple uno de los siguientes requisitos:

    - PIN sin secuencias repetidas (4444) u ordenadas (1234, 4321, 2468), con una longitud de al menos 4.
    - Alfabético, con una longitud de al menos 4.
    - Alfanumérico, con una longitud de al menos 4.
- **Alto**: la contraseña cumple uno de los siguientes requisitos:
    - PIN sin secuencias repetidas (4444) u ordenadas (1234, 4321, 2468), con una longitud de al menos 8.
    - Alfabético, con una longitud de al menos 6.
    - Alfanumérico, con una longitud de al menos 6.

Este nuevo valor de configuración sigue siendo un trabajo en curso. A finales de octubre de 2020, Complejidad de la contraseña surtirá efecto en los dispositivos.

Si establece *Complejidad de la contraseña* en un valor que no sea *Ninguno*, también debe configurar un valor adicional a fin de asegurarse de que los usuarios finales que empleen una contraseña que no cumpla los requisitos de complejidad reciban una advertencia para actualizarla.

- Cumplimiento de dispositivos: Establezca **Requerir una contraseña para desbloquear dispositivos móviles** en **Requerir**.
- Restricciones de dispositivo: establezca **Contraseña** en **Requerir**.

Si no establece el valor de configuración adicional en Requerir, los usuarios con contraseñas no seguras no recibirán la advertencia.

Supervisión y solución de problemas

El análisis de puntos de conexión está disponible con carácter general

Análisis de puntos de conexión pretende mejorar la productividad de los usuarios y disminuir los costos de soporte técnico de TI al proporcionar información sobre la experiencia del usuario. Esta información permite que el departamento de TI optimice la experiencia del usuario final con soporte técnico proactivo y detecte regresiones a la experiencia del usuario mediante la evaluación del impacto de los cambios de configuración en el usuario. Para obtener más información, consulte Análisis de puntos de conexión.

Acciones masivas para dispositivos incluidos en el informe operativo

Como parte de los nuevos informes de antivirus que se incluyen en la seguridad de Microsoft Endpoint Manager, el informe operativo del **malware detectado de Windows 10** ofrece acciones masivas que se aplican a los dispositivos seleccionados en el informe. Entre las acciones se incluyen **Reiniciar**, **Examen rápido** y **Examen completo**. Para obtener más información, vea Informe de malware detectado de Windows 10.

Exportación de informes de Intune mediante Graph API

Todos los informes que se han migrado a la infraestructura de informes de Intune estarán disponibles para la exportación desde una sola API de exportación de nivel superior. Para obtener más información, vea Exportación de informes de Intune mediante Graph API.

Informes nuevos y mejorados del Antivirus de Microsoft Defender para Windows 10 y versiones más recientes

Vamos a agregar cuatro nuevos informes para el Antivirus de Microsoft Defender en Windows 10 en Microsoft Endpoint Manager. Entre estos informes se incluyen:

- Dos informes operativos: *puntos de conexión incorrectos de Windows 10* y *malware detectado de Windows 10*. En Microsoft Endpoint Manager, seleccione **Seguridad de los puntos de conexión** > **Antivirus**.
- Dos informes organizativos: *Estado del agente de antivirus* y *Malware detectado*. En Microsoft Endpoint Manager, seleccione **Informes** > **Antivirus de Microsoft Defender**.

Para obtener más información, vea Informes de Intune y Administración de la seguridad de puntos de conexión en Microsoft Intune.

Nuevo informe de actualizaciones de características de Windows 10

El informe de **actualizaciones de características de Windows 10** proporciona una vista general del

cumplimiento de los dispositivos que se establecen como destino mediante una directiva de **actualizaciones de características de Windows 10**. En el centro de administración de Microsoft Endpoint Manager, seleccione **Informes** > **Actualizaciones de Windows** para ver el resumen de este informe. Para ver los informes de directivas específicas, en la carga de trabajo **Actualizaciones de Windows**, seleccione la pestaña **Informes** y abra el **informe de actualización de características de Windows**. Para obtener más información, consulte Actualizaciones de características de Windows 10.

Agosto de 2020

Administración de aplicaciones

Revocación de licencias asociadas revocadas antes de eliminar el token de VPP de Apple

Cuando se elimina un token de VPP de Apple en Microsoft Endpoint Manager, todas las licencias asignadas por Intune asociadas a ese token se revocarán automáticamente antes de la eliminación.

Mejora en la página Actualizar configuración del dispositivo de la aplicación Portal de empresa para Android para mostrar descripciones

En la aplicación Portal de empresa de dispositivos Android, en la página **Actualizar configuración del dispositivo** se muestra la configuración que debe actualizar un usuario para que sea compatible. Los usuarios expanden el problema para ver más información y verán el botón **Resolver**.

Esta experiencia del usuario se ha mejorado. Las opciones enumeradas se expanden de forma predeterminada para mostrar la descripción y el botón **Resolver**, cuando proceda. Anteriormente, los problemas estaban contraídos de forma predeterminada. Este nuevo comportamiento predeterminado reduce el número de clics, por lo que los usuarios pueden resolver los problemas más rápidamente.

El Portal de empresa agrega compatibilidad con las aplicaciones de Configuration Manager

El Portal de empresa ahora admite aplicaciones de Configuration Manager. Esta característica permite a los usuarios finales ver las aplicaciones implementadas de Configuration Manager y de Intune en el Portal de empresa de los clientes administrados conjuntamente. Esta nueva versión del Portal de empresa mostrará las aplicaciones implementadas por Configuration Manager para todos los clientes administrados conjuntamente. Esta compatibilidad ayuda a los administradores a consolidar sus diferentes experiencias del portal de usuario final. Para más información, consulte Uso de la aplicación Portal de empresa en dispositivos administrados conjuntamente.

Configuración del dispositivo

Uso de NetMotion como un tipo de conexión de VPN para dispositivos iOS/iPadOS y macOS

Al crear un perfil de VPN, NetMotion está disponible como tipo de conexión VPN (**Dispositivos** > **Configuración de dispositivos** > **Crear perfil** > **iOS/iPadOS** o **macOS** para plataforma > **VPN** para perfil > **NetMotion** para tipo de conexión).

Para obtener más información sobre los perfiles de VPN en Intune, consulte Creación de perfiles de VPN para conectarse a servidores VPN.

Se aplica a:

- iOS/iPadOS
- macOS

Más opciones del protocolo de autenticación extensible protegido (PEAP) para perfiles Wi-Fi de Windows 10

En los dispositivos Windows 10, puede crear perfiles de Wi-Fi con el protocolo de autenticación extensible (EAP) para autenticar las conexiones Wi-Fi (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Windows 10 y posteriores** para plataforma > **Wi-Fi** para perfil > **Empresa**).

Al seleccionar EAP protegido (PEAP), hay nuevas opciones de configuración disponibles:

- **Realizar validación del servidor en PEAP fase 1**: En la fase 1 de negociación PEAP, el servidor se comprueba mediante la validación del certificado.

    - **Deshabilitar los mensajes de usuario para la validación del servidor en PEAP fase 1**: en la fase 1 de la negociación de PEAP, no se muestran los mensajes de usuario que soliciten autorizar nuevos servidores PEAP para entidades de certificación de confianza.
- **Requerir enlace criptográfico**: impide las conexiones a servidores PEAP que no utilizan el enlace criptográfico durante la negociación PEAP.

Para ver la configuración que puede realizar, vaya a Agregar Wi-Fi para dispositivos Windows 10 y versiones posteriores en Intune.

Se aplica a:

- Windows 10 y versiones posteriores

Impedir que los usuarios desbloqueen dispositivos de perfil de trabajo de Android Enterprise mediante examen facial y del iris

Ahora puede evitar que los usuarios utilicen el examen facial o del iris para desbloquear sus dispositivos administrados de perfil de trabajo, ya sea en el nivel de dispositivo o en el nivel de perfil de trabajo. Esta opción se puede establecer en las secciones **Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Android Enterprise** para la plataforma > **Perfil de trabajo** > **Restricciones de dispositivos** para el perfil > **Configuración del perfil profesional** y **Contraseña**.

Para más información, consulte Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

Se aplica a:

- Perfil de trabajo de Android Enterprise

Uso de extensiones de aplicación de SSO en más aplicaciones iOS/iPadOS con el complemento de Microsoft Enterprise SSO

El complemento Microsoft Enterprise SSO para dispositivos Apple se puede usar con todas las aplicaciones que admiten las extensiones de aplicación SSO. En Intune, esta característica significa que el complemento funciona con aplicaciones móviles iOS/iPadOS que no usan la biblioteca de autenticación de Microsoft (MSAL) para dispositivos Apple. Las aplicaciones no necesitan usar MSAL, pero tienen que autenticarse con puntos de conexión de Azure AD.

Para configurar las aplicaciones de iOS/iPadOS para usar SSO con el complemento, agregue los identificadores de lote de aplicaciones en un perfil de configuración de iOS/iPadOS (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** para plataforma > **Características del dispositivo** para perfil > **Extensión de aplicación de inicio de sesión único** > **Microsoft Azure AD** > para tipo de extensión de aplicación de SSO > **Identificadores de lote de las aplicaciones**).

Para ver la configuración actual de la extensión de la aplicación de SSO que puede configurar, vaya a Extensión de aplicación de inicio de sesión único.

Se aplica a:

- iOS/iPadOS

Nueva versión del conector de certificados PFX y cambios para la compatibilidad con el perfil de certificado PKCS

Hemos publicado una nueva versión del conector de certificados PFX, versión **6.2008.60.607**. Esta nueva versión del conector:

- Admite perfiles del certificado PKCS en todas las plataformas admitidas excepto Windows 8.1.

  Hemos consolidado toda la compatibilidad con PCKS en el conector de certificados PFX. Esto significa que si no usa SCEP en su entorno ni NDES con otras intenciones, puede quitar el conector del certificado de Microsoft y desinstalar NDES de su entorno.

- Dado que no se ha eliminado ninguna funcionalidad del conector del certificado de Microsoft, puede seguir utilizándolos para admitir los perfiles de certificado PKCS.

- Admite la revocación de certificados para Outlook S/MIME.
- Requiere .NET Framework 4.7.2.

Para más información sobre los conectores de certificados, incluida una lista de versiones de conector para los conectores de ambos certificados, vea Conectores de certificados.

Administración de dispositivos

Asociación de inquilinos: instalación de una aplicación desde el centro de administración

Ahora puede iniciar la instalación de una aplicación en tiempo real para un dispositivo asociado al inquilino desde el centro de administración de Microsoft Endpoint Manager. Para más información, consulte Asociación de inquilinos: instalación de una aplicación desde el centro de administración.

Seguridad de dispositivos

Implementación de la directiva de antivirus de seguridad de punto de conexión en dispositivos con asociación de inquilinos (versión preliminar)

Como versión preliminar, puede implementar la directiva de antivirus de seguridad de punto de conexión en los dispositivos que se administran con Configuration Manager. Para hacer posible este escenario, es necesario configurar una asociación de inquilinos entre una versión admitida de Configuration Manager y la suscripción de Intune. Se admiten las siguientes versiones de Configuration Manager:

- Versión 2006 de la rama actual de Configuration Manager

Para más información, consulte los [requisitos de las directivas de seguridad de punto de conexión de Intune] (../protect/tenant-attach-intune.md# requirements-for-intune-endpoint-security-policies) para admitir asociación de inquilinos.

Cambios para las exclusiones de la directiva de antivirus para la seguridad de los puntos de conexión

Se han introducido dos cambios en la administración de las listas de exclusión de Antivirus de Microsoft Defender que se configuran como parte de una directiva de antivirus de seguridad de punto de conexión. Los cambios le ayudan a evitar conflictos entre las distintas directivas y a resolver aquellos relacionados con las listas de exclusión que podrían existir en las directivas previamente implementadas.

Ambos cambios se aplican a la configuración de directiva de los siguientes proveedores de servicios de configuración de Antivirus de Microsoft Defender (CSP):

- Defender/ExcludedPaths
- Defender/ExcludedExtensions
- Defender/ExcludedProcesses

Los cambios son:

- Nuevo tipo de perfil: **Exclusiones del Antivirus de Microsoft Defender**: use este nuevo tipo de perfil para Windows 10 y versiones posteriores para definir una directiva que se centre únicamente en las exclusiones del antivirus. Este perfil puede ayudarle a simplificar la administración de las listas de exclusión separándolas de otras configuraciones de directiva.

  Entre las exclusiones que se pueden configurar se incluyen los *procesos*, las *extensiones de archivos* y los *archivos* y *carpetas* de Defender que no quiere que examine Microsoft Defender.

- **Combinación de directivas**: Intune ahora combina la lista de exclusiones que ha definido en perfiles independientes en una única lista de exclusiones que se aplicarán a cada dispositivo o usuario. Por ejemplo, en el caso de un usuario con tres directivas independientes, las listas de exclusión de esas tres directivas se combinan en un único superconjunto de *exclusiones de antivirus de Microsoft Defender*, que se aplican de este modo al usuario.

Importación y exportación de listas de intervalos de direcciones para reglas de firewall de Windows

Hemos agregado compatibilidad con la **importación** o la **exportación** de una lista de intervalos de

direcciones mediante archivos .csv en el perfil de reglas de firewall de Microsoft Defender en la directiva de firewall para la seguridad de los puntos de conexión. Los siguientes valores de configuración de reglas de firewall de Windows admiten ahora la importación y la exportación:

- **Intervalos de direcciones locales**
- **Intervalos de direcciones remotas**

También hemos mejorado la validación de la entrada de intervalos de direcciones locales y remotas para ayudar a evitar entradas duplicadas o no válidas.

Para obtener más información sobre estas opciones, consulte la configuración de las reglas del firewall de Microsoft Defender.

Establecimiento del estado de cumplimiento del dispositivo desde proveedores de MDM de terceros

Intune admite ahora soluciones MDM de terceros como origen de detalles de cumplimiento de dispositivos. Estos datos de cumplimiento de terceros se pueden usar para aplicar directivas de acceso condicional a aplicaciones de Microsoft 365 en iOS y Android gracias a la integración con Microsoft Intune. Intune evalúa los detalles de cumplimiento del proveedor de terceros para determinar si un dispositivo es de confianza y, luego, establece los atributos de acceso condicional en Azure AD. Para continuar, se crearán las directivas de acceso condicional de Azure AD desde el centro de administración de Microsoft Endpoint Manager o el portal de Azure AD.

En esta versión, se admiten los siguientes proveedores de MDM de terceros, como una versión preliminar pública:

- VMware Workspace ONE UEM (antes conocido como AirWatch)

Esta actualización se va a implementar en los clientes globalmente. Esta funcionalidad aparecerá la próxima semana.

Aplicaciones de Intune

La imagen de marca personalizada se muestra ahora en la página del perfil del Portal de empresa de Windows

Como administrador de Microsoft Intune, puede cargar una imagen de marca personalizada en Intune que se mostrará como imagen de fondo en la página de perfil del usuario en la aplicación del Portal de empresa de Windows. Para más información, consulte Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune.

Julio de 2020

Administración de aplicaciones

Actualización de iconos de dispositivos en aplicaciones del Portal de empresa y de Intune en Android

Hemos actualizado los iconos de dispositivos de las aplicaciones del Portal de empresa y de Intune de los dispositivos Android para crear una apariencia más moderna y en consonancia con el sistema de diseño de Microsoft Fluent. Puede encontrar información relacionada en Actualizaciones de los iconos de la aplicación del Portal de empresa para iOS o iPadOS y macOS.

Compatibilidad con Exchange On-Premises Connector

Intune está retirando la compatibilidad con la característica Exchange On-Premises Connector del servicio Intune a partir de la versión 2007 (julio). En este momento, los clientes existentes con un conector activo podrán continuar con la función actual. Los clientes nuevos y los existentes que no tengan un conector activo ya no podrán crear otros conectores ni administrar dispositivos de Exchange ActiveSync (EAS) desde Intune. En el caso de esos clientes, Microsoft recomienda el uso de la autenticación moderna híbrida (HMA) de Exchange para proteger el acceso a Exchange local. HMA habilita las dos directivas de Intune App Protection (también conocidas como MAM) y el acceso condicional a través de Outlook Mobile para Exchange local.

S/MIME para Outlook en dispositivos iOS y Android sin inscripción

Ahora se puede habilitar S/MIME para Outlook en dispositivos iOS y Android mediante la directiva de configuración de aplicaciones para aplicaciones administradas. Esto permite la entrega de directivas independientemente del estado de inscripción de los dispositivos. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Directivas de configuración de aplicaciones** > **Agregar** > **Aplicaciones administrados**. Además, puede elegir si quiere permitir que los usuarios cambien esta configuración en Outlook. Sin embargo, para implementar automáticamente certificados de S/MIME en Outlook para iOS y Android, el dispositivo debe estar inscrito. Para obtener información general sobre S/MIME, vea Información general sobre S/MIME para firmar y cifrar el correo electrónico en Intune. Para obtener más información sobre las opciones de configuración de Outlook, vea Opciones de configuración de Microsoft Outlook y Agregar directivas de configuración para aplicaciones administradas sin inscripción de dispositivos. Para obtener información sobre S/MIME en Outlook para iOS y Android, vea Escenarios de S/MIME y Claves de configuración: opciones de S/MIME.

Configuración del dispositivo

Nueva configuración de VPN para dispositivos Windows 10 y versiones más recientes

Cuando se crea un perfil de VPN mediante el tipo de conexión de IKEv2, hay nuevas opciones que puede configurar(**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Windows 10 y posteriores** como plataforma > **VPN** para el perfil > **VPN base**):

- **Túnel de dispositivos**: permite que los dispositivos se conecten de forma automática a la VPN sin necesidad de interacción del usuario, incluido su inicio de sesión. Esta característica requiere que se habilite **Always On** y que se usen **certificados de máquina** como método de autenticación.
- Configuración de Cryptography Suite: Configure los algoritmos que se usan para proteger las asociaciones de seguridad IKE y secundarias, que permiten hacer coincidir la configuración de cliente y servidor.

Para ver las opciones que puede configurar, vaya a Configuración de dispositivos con Windows 10 y Windows Holographic para agregar conexiones VPN mediante Intune.

Se aplica a:

- Windows 10 y versiones posteriores

Configuración de más opciones de Microsoft Launcher en un perfil de restricciones de dispositivos en dispositivos empresariales Android (COBO)

En los dispositivos totalmente administrados de Android Enterprise, se pueden configurar las opciones de Microsoft Launcher mediante el perfil de restricciones de dispositivos (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Android Enterprise** como plataforma > **Solo el propietario del dispositivo** > **Restricciones de dispositivos** > **Experiencia de dispositivo** > **Totalmente administrado**).

Para ver estas opciones, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

También puede establecer la configuración de Microsoft Launcher mediante un perfil de configuración de aplicaciones.

Se aplica a:

- Dispositivos totalmente administrados del propietario del dispositivo Android Enterprise (COBO)

Nuevas características de Managed Home Screen en los dispositivos dedicados del propietario del dispositivo de Android Enterprise (COSU)

En los dispositivos Android Enterprise, los administradores pueden usar perfiles de configuración de dispositivos para personalizar Managed Home Screen en dispositivos dedicados mediante el modo de pantalla completa de varias aplicaciones (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Android Enterprise** para la plataforma > **Solo el propietario del dispositivo** > **Restricciones de dispositivo** para el perfil > **Experiencia de dispositivo** > **Dispositivo dedicado** > **Varias aplicaciones**).

En concreto, puede:

- Personalizar iconos, cambiar la orientación de la pantalla y mostrar notificaciones de aplicaciones en los iconos de distintivos
- Ocultar el acceso directo a la configuración administrada
- Acceder de forma más sencilla al menú de depuración
- Crear una lista permitida de redes Wi-Fi
- Acceso más sencillo a la información del dispositivo

Para obtener más información, vea Configuración de dispositivos Android Enterprise para permitir o restringir características y este blog.

Se aplica a:

- Dispositivos dedicados administrados del propietario del dispositivo Android Enterprise (COSU)

Plantillas administrativas actualizadas para Microsoft Edge 84

Se ha actualizado la configuración de ADMX disponible para Microsoft Edge. Los usuarios finales ahora pueden configurar e implementar la configuración de ADMX nueva agregada en Edge 84. Para obtener más información, vea las Notas de la versión de Edge 84.

Inscripción de dispositivos

El Portal de empresa de iOS admitirá la Inscripción de dispositivos automatizada de Apple sin afinidad de usuario

El Portal de empresa de iOS ahora se admite en los dispositivos inscritos con la Inscripción de dispositivos automatizada de Apple sin necesidad de un usuario asignado. Un usuario final puede iniciar sesión en el Portal de empresa de iOS para establecerse como usuario primario de un dispositivo iOS o iPad inscrito sin afinidad de dispositivo. Para más información sobre la Inscripción de dispositivos automatizada, consulte Inscripción automática de dispositivos iOS/iPadOS con Inscripción de dispositivos automatizada de Apple.

Dispositivos corporativos con habilitación personal (versión preliminar)

Intune ahora admite dispositivos corporativos de Android Enterprise con un perfil de trabajo para versiones de sistema operativo Android 8 y posteriores. Los dispositivos corporativos con un perfil de trabajo son uno de los escenarios de administración corporativa del conjunto de soluciones de Android Enterprise. Este escenario va destinado a dispositivos de usuario únicos para uso personal y corporativo. Este escenario de propiedad corporativa y con habilitación personal (COPE) ofrece lo siguiente:

- creación de contenedores de perfiles de trabajo y personales
- control de nivel de dispositivo para los administradores
- garantía para los usuarios finales de que sus datos y aplicaciones personales seguirán siendo privados

La primera versión preliminar pública incluirá un subconjunto de las características que se incluirán en la versión disponible con carácter general. De manera gradual se agregarán características adicionales. Las características que estarán disponibles en la primera versión preliminar incluyen las siguientes:

- Inscripción: los administradores pueden crear varios perfiles de inscripción con tokens únicos que no expiren. La inscripción de dispositivos se puede realizar mediante NFC, la entrada de tokens, el código QR, Zero Touch o Knox Mobile Enrollment.
- Configuración de dispositivos: un subconjunto de los valores de configuración existentes de dispositivos dedicados y totalmente administrados.
- Cumplimiento de dispositivos: las directivas de cumplimiento que están disponibles actualmente para los dispositivos totalmente administrados.
- Acciones de dispositivo: elimine el dispositivo (restablecimiento de fábrica), reinícielo y bloquéelo.
- Administración de aplicaciones: asignaciones de aplicaciones, configuración de aplicaciones y funcionalidades de informes asociadas
- Acceso condicional

Para obtener más información sobre la versión preliminar de la propiedad corporativa con perfil de trabajo, vea el blog de soporte técnico.

Administración de dispositivos

Asociación de inquilinos: detalles de cliente de ConfigMgr en el centro de administración (versión preliminar)

Ahora puede ver los detalles del cliente ConfigMgr, incluidas las recopilaciones, la pertenencia a grupos de límites y la información de cliente en tiempo real para un dispositivo específico en el centro de administración de Microsoft Endpoint Manager. Para más información, consulte Asociación de inquilinos: detalles de cliente de ConfigMgr en el centro de administración (versión preliminar)

Actualizaciones de la acción de bloqueo remoto para dispositivos macOS

Los cambios de la acción de bloqueo remoto para dispositivos macOS incluyen lo siguiente:

- El PIN de recuperación se muestra durante 30 días (en lugar de 7) antes de la eliminación.
- Si un administrador tiene abierto un segundo explorador e intenta volver a desencadenar el comando desde otra pestaña o explorador, Intune permite que el comando pase. Sin embargo, el estado de los informes se establece como erróneo en lugar de generar un nuevo PIN.
- Al administrador no se le permite emitir otro comando de bloqueo remoto si el anterior todavía está pendiente o si el dispositivo no se ha vuelto a sincronizar. Estos cambios están diseñados para impedir que se sobrescriba el PIN correcto después de varios comandos de bloqueo remoto.

Distinción entre el borrado y el borrado protegido en el informe de acciones de dispositivo

El informe **Acciones de dispositivo** ahora distingue entre las acciones de borrado y de borrado protegido. Para ver el informe, vaya al centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **Supervisar** > **Acciones de dispositivo** (en **Otros**).

Seguridad de dispositivos

Versión preliminar de la herramienta de migración de reglas de firewall de Microsoft Defender

Estamos trabajando en la versión preliminar pública de una herramienta basada en PowerShell que migrará las reglas de firewall de Microsoft Defender. Al instalar y ejecutar la herramienta, se crean automáticamente directivas de reglas de firewall de seguridad de los puntos de conexión para Intune basadas en la configuración actual de un cliente de Windows 10. Para obtener más información, vea Información general sobre la herramienta de migración de reglas de firewall de seguridad de los puntos de conexión.

Directiva de detección de puntos de conexión y respuesta para la incorporación de dispositivos de asociación de inquilinos a Microsoft Defender para punto de conexión disponible de manera general

Como parte de la seguridad del punto de conexión en Intune, las directivas de detección y de puntos de conexión y respuesta (EDR) para su uso con dispositivos que administra Configuration Manager ya no se encuentran en *versión preliminar* y ahora están *disponibles de manera general*.

Para usar la directiva de EDR con dispositivos de una versión compatible de Configuration Manager, configure Asociación de inquilinos para Configuration Manager. Después de completar la configuración de asociación de inquilinos, puede implementar las directivas de EDR para incorporar dispositivos que administra Configuration Manager a Microsoft Defender para punto de conexión.

La configuración de Bluetooth está disponible en los perfiles de control de dispositivos de la directiva de reducción de la superficie expuesta a ataques de seguridad de los puntos de conexión

Hemos agregado opciones de configuración para administrar Bluetooth en dispositivos Windows 10 en el perfil de control de dispositivos para la *directiva de reducción de la superficie expuesta a ataques de seguridad de los puntos de conexión*. Estas son las mismas opciones de configuración que las que han estado disponibles en los perfiles de restricción de dispositivos para *Configuración del dispositivo*.

Administración de las ubicaciones de origen de las actualizaciones de definiciones con la directiva antivirus de seguridad de puntos de conexión para dispositivos Windows 10

Hemos agregado dos nuevas opciones de configuración a la categoría *Actualizaciones* de la directiva antivirus de seguridad del punto de conexión para dispositivos Windows 10 que pueden ayudar a administrar la forma en la que los dispositivos obtienen definiciones de actualización:

- *Definir recursos compartidos de archivos para descargar actualizaciones de definiciones*
- *Definir orden de los orígenes para descargar actualizaciones de definiciones*

Gracias a las nuevas opciones de configuración, se pueden agregar recursos compartidos de archivos UNC como ubicaciones de origen de descarga para las actualizaciones de definiciones y definir el orden en el que se establece la comunicación con las distintas ubicaciones de origen.

Nodo mejorado de líneas base de seguridad

Hemos realizado algunos cambios para mejorar la facilidad de uso del nodo de línea base de seguridad en el centro de administración de Microsoft Endpoint Manager. Ahora, al acceder a **Seguridad de los puntos de conexión** > **Líneas base de seguridad** y seleccionar un tipo de línea base de seguridad, como la de MDM, aparecerá un panel **Perfiles**. En el panel Perfiles, se pueden ver los perfiles que se han creado para ese tipo de línea base. Anteriormente, la consola presentaba un panel Información general que incluía una acumulación de datos agregados que no siempre coincidía con los detalles que se encontraban en los informes de perfiles individuales.

Sin cambiar, en el panel Perfiles, se puede seleccionar un perfil y explorarlo para ver las propiedades de los perfiles, así como varios informes que están disponibles en *Supervisión*. Del mismo modo, en el mismo nivel que Perfiles, todavía se puede seleccionar la opción **Versiones** para ver las distintas versiones de ese tipo de perfil que se ha implementado. Al explorar una versión, también obtiene acceso a los informes, de forma similar a los informes de perfil.

Compatibilidad con credenciales derivadas para Windows

Ahora se pueden usar credenciales derivadas con sus dispositivos Windows. Esto expandirá la compatibilidad existente para iOS/iPadOS y Android, y estará disponible para los mismos proveedores de credenciales derivados:

- Entrust
- Intercede
- DISA Purebred

La compatibilidad con Windows incluye el uso de una credencial derivada para la autenticación en perfiles de Wi-Fi o VPN. En el caso de los dispositivos Windows, la credencial derivada se emite desde la aplicación cliente que proporciona el proveedor de credenciales derivadas que se usa.

Administración del cifrado de FileVault para dispositivos que ha cifrado el usuario del dispositivo en lugar de Intune

Intune ahora puede asumir la administración del cifrado de disco de FileVault en un dispositivo macOS que ha cifrado el usuario del dispositivo en lugar de la directiva de Intune. En este escenario se requiere lo siguiente:

- El dispositivo debe recibir la directiva de cifrado de disco de Intune que habilita FileVault.
- El usuario del dispositivo debe usar el sitio web del Portal de empresa a fin de cargar la clave de recuperación personal para el dispositivo cifrado en Intune. Para cargar la clave, es necesario selecciona la opción *Almacenar clave de recuperación* para su dispositivo macOS cifrado.

Una vez que el usuario cargue su clave de recuperación, Intune la rotará para confirmar que sea válida. Intune ahora puede administrar la clave y el cifrado como si usara la directiva para cifrar el dispositivo directamente. Si un usuario necesita recuperar su dispositivo, puede acceder a la clave de recuperación mediante cualquier dispositivo desde las ubicaciones siguientes:

- sitio web del Portal de empresa
- Aplicación Portal de empresa para iOS/iPadOS
- Aplicación Portal de empresa para Android
- Aplicación de Intune

Ocultación de la clave de recuperación personal de un usuario de dispositivo durante el cifrado de disco de FileVault de macOS

Al usar la directiva de seguridad del punto de conexión para configurar el cifrado de disco de FileVault para

macOS, use el valor **Ocultar clave de recuperación** para impedir la visualización de la *clave de recuperación personal* para el usuario del dispositivo, mientras se cifra el dispositivo. Al ocultar la clave durante el cifrado, puede ayudar a protegerla, ya que los usuarios no podrán anotarla mientras esperan a que el dispositivo se cifre.

Más adelante, si se necesita la recuperación, un usuario siempre puede usar cualquier dispositivo para ver su clave de recuperación personal mediante el sitio web del Portal de empresa de Intune, el Portal de empresa de iOS/iPadOS, el Portal de empresa de Android o la aplicación de Intune.

Vista mejorada de los detalles de base de referencia de seguridad de los dispositivos

Ahora puede explorar los detalles de un dispositivo para ver la información detallada de configuración de las líneas base de seguridad que se aplican al dispositivo. La configuración aparece en una lista sencilla y plana, que incluye la categoría de configuración, el nombre de la configuración y el estado. Para obtener más información, vea Visualización de configuraciones de seguridad de los puntos de conexión por dispositivo.

Supervisión y solución de problemas

Registros de cumplimiento de dispositivos ahora en inglés

Anteriormente, los registros de DeviceComplianceOrg de Intune solo tenían enumeraciones para ComplianceState, OwnerType y DeviceHealthThreatLevel. Ahora estos registros tienen información en inglés en las columnas.

Plantilla de informe de cumplimiento de Power BI V2.0

Las aplicaciones de plantilla de Power BI permiten a los asociados de Power BI compilar aplicaciones de Power BI con poca o ninguna programación e implementarlas en cualquier cliente de Power BI. Los administradores pueden actualizar la versión de la plantilla de informe de cumplimiento de Power BI de V1.0 a V2.0. En V2.0 se incluye un diseño mejorado, así como cambios en los cálculos y datos que se muestran como parte de la plantilla. Para obtener más información, vea Conexión a Data Warehouse con Power BI y Actualización de una aplicación de plantilla. Además, vea la entrada de blog Anuncio de una nueva versión del informe de cumplimiento de Power BI con Data Warehouse de Intune.

Control de acceso basado en roles.

Cambios de los permisos Asignar perfil y Actualizar perfil

Los permisos de control de acceso basado en rol se han cambiado por Asignar perfil y Actualizar perfil para el flujo de inscripción de dispositivo automatizada:

Asignar perfil: los administradores con este permiso también pueden asignar los perfiles a los tokens y asignar un perfil predeterminado a un token para la inscripción de dispositivo automatizada.

Actualizar perfil: los administradores con este permiso pueden actualizar los perfiles existentes solo para la inscripción de dispositivo automatizada.

Para ver estos roles, vaya al centro de administración de Microsoft Endpoint Manager > **Administración de inquilinos** > **Roles** > **Todos los roles** > **Crear** > **Permisos** > **Roles**.

Scripting

Propiedades adicionales de Data Warehouse v1.0

Hay otras propiedades disponibles mediante Intune Data Warehouse v1.0. Las propiedades siguientes se exponen ahora por medio de la entidad dispositivos:

- `ethernetMacAddress`: identificador de red único de este dispositivo.
- `office365Version`: versión de Microsoft 365 instalada en el dispositivo.

Las propiedades siguientes ahora se exponen por medio de la entidad devicePropertyHistory:

- `physicalMemoryInBytes`: memoria física en bytes.
- `totalStorageSpaceInBytes`: capacidad total de almacenamiento en bytes.

Para obtener más información, vea API de Data Warehouse de Microsoft Intune.

Junio de 2020

Administración de aplicaciones

Protección de la transferencia de datos de telecomunicaciones para aplicaciones administradas

Cuando se detecta un número de teléfono hipervinculado en una aplicación protegida, Intune comprueba si se ha aplicado una directiva de protección que permita transferir el número a una aplicación de marcador. Puede elegir cómo administrar este tipo de transferencia de contenido cuando se inicia desde una aplicación administrada por directiva. Al crear una directiva de protección de aplicaciones en Microsoft Endpoint Manager, seleccione una opción de aplicación administrada en **Enviar datos de la organización a otras aplicaciones** y, luego, elija una opción en **Transferir datos de telecomunicaciones a**. Para obtener más información sobre esta configuración de protección de datos, vea Configuración de directivas de protección de aplicaciones Android en Microsoft Intune y Configuración de directivas de protección de aplicaciones de iOS.

Entrega unificada de aplicaciones de Azure Active Directory Enterprise y Office Online en el Portal de empresa de Windows

En el panel **Personalización** de Intune, puede seleccionar **Ocultar** o **Mostrar Aplicaciones de Azure AD Enterprise** y **Aplicaciones de Office Online** en el Portal de empresa. Cada usuario final ve todo el catálogo de aplicaciones desde el servicio de Microsoft elegido. De forma predeterminada, cada origen de aplicación adicional se establecerá en **Ocultar**. Esta característica se va a aplicar en primer lugar en el sitio web del Portal de empresa y, luego, en el Portal de empresa de Windows. Para encontrar esta opción de configuración, seleccione **Administración de inquilinos** > **Personalización** en el Centro de administración de Microsoft Endpoint Manager. Para obtener información relacionada, vea Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune.

Mejoras en el Portal de empresa para la experiencia de inscripción de macOS

La experiencia de inscripción del Portal de empresa para macOS cuenta con un proceso de inscripción más sencillo que es más coherente con la experiencia de inscripción en el Portal de empresa para iOS. Los usuarios del dispositivo verán:

- Una interfaz de usuario más elegante.
- Una lista de comprobación de inscripción mejorada.
- Instrucciones más claras sobre cómo inscribir sus dispositivos.
- Mejores opciones de solución de problemas.

Para más información sobre el Portal de empresa de Intune, consulte Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune.

Mejoras en la página Dispositivos de iOS/iPadOS y los portales de empresa de macOS

Hemos realizado cambios en la página **Dispositivos** del Portal de empresa para mejorar la experiencia de la aplicación para usuarios de iOS/iPadOS y Mac. Además de crear una apariencia más moderna, hemos reorganizado los detalles del dispositivo en una sola columna con encabezados de sección definidos para que a los usuarios les resulte más fácil ver el estado de los dispositivos. También hemos agregado una mensajería más clara y pasos de solución de problemas para los usuarios cuyos dispositivos no cumplen los requisitos. Para obtener más información sobre el Portal de empresa, vea Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune. Para sincronizar manualmente un dispositivo, vea Sincronización manual del dispositivo iOS.

Configuración de la nube para la aplicación Portal de empresa de iOS o iPadOS

La nueva configuración de la **nube** para el Portal de empresa de iOS o iPadOS permite a los usuarios redirigir la autenticación hacia la nube adecuada para la organización. De forma predeterminada, la opción está configurada en **Automático**, que dirige la autenticación a la nube que el dispositivo del usuario detecta automáticamente. Si la autenticación de la organización debe redirigirse a una nube distinta de la que se detecta automáticamente (como una pública o de administración pública), los usuarios pueden seleccionar manualmente la nube adecuada si eligen **Configuración** de la aplicación > **Portal de empresa** > **Nube**. Los

usuarios solo deben cambiar el valor **Automático** de **Nube** si inician sesión desde otro dispositivo y este no detecta automáticamente la nube adecuada.

Tokens duplicados de VPP de Apple

Los tokens de VPP de Apple con la misma **Ubicación del token** ahora están marcados como **Duplicados** y se pueden sincronizar de nuevo cuando se ha quitado el token duplicado. Todavía puede asignar y revocar licencias para los tokens marcados como duplicados. Pero es posible que las licencias de las nuevas aplicaciones y los libros comprados no se reflejen una vez que un token se marca como duplicado. Para buscar los tokens de VPP de Apple del inquilino, en el Centro de administración de Microsoft Endpoint Manager, seleccione **Administración de inquilinos** > **Conectores y tokens** > **Tokens de VPP de Apple**. Para obtener más información relacionada con los tokens VPP, vea Administración de aplicaciones de iOS y macOS compradas a través del Programa de Compras por Volumen de Apple con Microsoft Intune.

Actualizaciones de la pantalla informativa en Portal de empresa para iOS/iPadOS

Se ha actualizado una pantalla informativa en Portal de empresa para iOS/iPadOS a fin de explicar mejor lo que un administrador puede ver y hacer en los dispositivos. Estas aclaraciones solo se aplican a los dispositivos corporativos. Solo se ha actualizado el texto; no se han realizado modificaciones reales de lo que el administrador puede ver o hacer en los dispositivos de usuario. Para ver las pantallas actualizadas, vaya a Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune.

Actualización de la experiencia del usuario final de inicio condicional de la aplicación Android

La versión 2006 del Portal de empresa de Android incluye cambios basados en las actualizaciones de la versión 2005. En 2005, implementamos una actualización en la que los usuarios finales de dispositivos Android que son objeto de una advertencia, un bloqueo o un borrado por parte de una directiva de protección de aplicaciones ven un mensaje de página completa en el que se describe el motivo de dicha advertencia, bloqueo o borrado y los pasos para corregir los problemas. En 2006, los nuevos usuarios de aplicaciones Android a los que se asignó a una directiva de protección de aplicaciones seguirán un flujo guiado para corregir los problemas que hacen que el acceso a su aplicación se bloquee.

Nuevas aplicaciones protegidas disponibles para Intune

Ya están disponibles las siguientes aplicaciones protegidas:

- BlueJeans Video Conferencing
- Cisco Jabber para Intune
- Tableau Mobile para Intune
- ZERO para Intune

Para obtener más información sobre las aplicaciones protegidas, vea Aplicaciones protegidas de Microsoft Intune.

Configuración del dispositivo

Adición de varios certificados raíz para la autenticación EAP-TLS en perfiles de Wi-Fi en dispositivos macOS

En los dispositivos macOS, puede crear un perfil de Wi-Fi y seleccionar el tipo de autenticación Protocolo de autenticación extensible (EAP) (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** para la plataforma > **Wi-Fi** para el perfil > **Tipo de Wi-Fi** establecido en Empresa).

Al establecer el **Tipo de EAP** en la autenticación **EAP-TLS**, **EAP-TTLS** o **PEAP**, puede agregar varios certificados raíz. Antes solo se podía agregar un certificado raíz.

Para obtener más información sobre las opciones que se pueden configurar, vea Incorporación de la configuración de Wi-Fi para dispositivos macOS en Microsoft Intune.

Se aplica a:

- macOS

Uso de certificados PKCS con perfiles de Wi-Fi en dispositivos Windows 10 y más recientes

Puede autenticar los perfiles de Wi-Fi de Windows con certificados SCEP (**Configuración de dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Wi-Fi** para el tipo de perfil > **Empresa** > **Tipo de EAP**). Ahora puede usar certificados PKCS con los perfiles de Wi-Fi de Windows. Esta característica permite a los usuarios autenticar perfiles de Wi-Fi mediante perfiles de certificado PKCS nuevos o existentes en el inquilino.

Para obtener más información sobre las opciones de Wi-Fi que se pueden configurar, vea Agregar Wi-Fi para dispositivos Windows 10 y versiones posteriores en Intune.

Se aplica a:

- Windows 10 y versiones posteriores

Perfiles de configuración de dispositivos de red cableada para dispositivos macOS

Hay disponible un nuevo perfil de configuración de dispositivos macOS que configura redes cableadas (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** para la plataforma > **Red cableada** para el perfil). Use esta característica para crear perfiles de 802.1x con el fin de administrar redes cableadas e implementarlas en los dispositivos macOS.

Para obtener más información sobre esta característica, vea Redes cableadas en dispositivos macOS.

Se aplica a:

- macOS

Uso de Microsoft Launcher como iniciador predeterminado para dispositivos empresariales Android totalmente administrados

En los dispositivos del propietario de dispositivos de Android Enterprise, puede configurar Microsoft Launcher como el iniciador predeterminado para dispositivos totalmente administrados (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Android Enterprise** como plataforma > **Propietario del dispositivo** > **restricciones de dispositivos** para el perfil > **Experiencia de dispositivo**). Para configurar el resto de la configuración de Microsoft Launcher, use directivas de configuración de aplicaciones.

Además, hay otras actualizaciones de la interfaz de usuario, entre las que se incluyen **Dispositivos dedicados**, cuyo nombre cambia a **Experiencia de dispositivo**.

Para ver los valores que puede restringir, consulte Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

Se aplica a:

- Dispositivos totalmente administrados del propietario del dispositivo Android Enterprise (COBO)

Uso de la configuración de modo de aplicación única autónoma para configurar la aplicación de Portal de empresa de iOS con el fin de que sea una aplicación de inicio y cierre de sesión

En los dispositivos iOS o iPadOS, puede configurar las aplicaciones para que se ejecuten en el modo de aplicación única autónoma (ASAM). Ahora, la aplicación Portal de empresa admite ASAM y se puede configurar para que sea una aplicación de inicio y cierre de sesión. En este modo, los usuarios deben iniciar sesión en la aplicación Portal de empresa para usar otras aplicaciones y el botón Pantalla principal del dispositivo. Cuando cierran sesión en la aplicación Portal de empresa, el dispositivo vuelve al modo de aplicación única y se bloquea en la aplicación Portal de empresa.

Para configurar el Portal de empresa de modo que esté en ASAM, vaya a **Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** para plataforma > **Restricciones de dispositivos** para perfil > **Modo de aplicación única autónoma**.

Para obtener más información, vea Modo de aplicación única autónoma (ASAM) y Modo de aplicación única (se abre el sitio web de Apple).

Se aplica a:

- iOS/iPadOS

Configuración del almacenamiento en caché de contenido en dispositivos macOS

En los dispositivos macOS, puede crear un perfil de configuración que configure el almacenamiento en caché de contenido (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** como plataforma > **Características del dispositivo** para tipo de perfil). Use esta configuración para eliminar la caché, permitir la caché compartida, establecer un límite de caché en el disco y mucho más.

Para más información sobre el almacenamiento en caché de contenido, consulte ContentCaching (abre el sitio web de Apple).

Para ver los valores que se pueden configurar, vea Configuración de características de dispositivos macOS en Intune.

Se aplica a:

- macOS

Agregue una nueva configuración de esquema y busque la configuración de esquema existente con OEMConfig en Android Enterprise.

En Intune, puede usar OEMConfig para administrar la configuración de los dispositivos Android Enterprise (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Android Enterprise** para plataforma > **OEMConfig** para el perfil). Al usar **Diseñador de configuraciones**, se muestran las propiedades del esquema de la aplicación. Ahora, en **Diseñador de configuraciones**, puede:

- Agregar una nueva configuración al esquema de la aplicación.
- Buscar valores nuevos y existentes en el esquema de la aplicación.

Para más información sobre los perfiles OEMConfig en Intune, consulte Uso y administración de dispositivos Android Enterprise con OEMConfig en Microsoft Intune.

Se aplica a:

- Android Enterprise

Bloqueo de sesiones temporales de iPad compartidas en dispositivos iPad compartidos

En Intune, hay una nueva opción para **bloquear sesiones temporales de iPad compartidas en dispositivos iPad compartidos** (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** como plataforma > **Restricciones de dispositivos** para tipo de perfil > **iPad compartido**). Cuando está habilitada, los usuarios finales no pueden usar la cuenta de invitado. Deben iniciar sesión en el dispositivo con el identificador y la contraseña de Apple administrados.

Para obtener más información, vea Configuración de dispositivos iOS e iPadOS para permitir o restringir características.

Se aplica a:

- Dispositivos iPad compartidos que ejecutan iOS/iPadOS 13.4 y versiones más recientes

Inscripción de dispositivos

Los dispositivos de tipo Bring Your Own Device pueden usar la VPN para la implementación

El nuevo botón de alternancia **Omitir comprobación de conectividad del dominio** del perfil de Autopilot le permite implementar dispositivos de Unión a Azure AD híbrido sin acceso a la red corporativa mediante su propio cliente VPN Win32 de terceros. Para ver el nuevo botón de alternancia, vaya al Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **Windows** > **Inscripción de Windows** > **Perfiles de implementación** > **Crear perfil** > **Configuración rápida (OOBE)** .

Los perfiles de la página de estado de inscripción pueden establecerse en grupos de dispositivos

Antes, los perfiles de la página de estado de inscripción (ESP) solo podían destinarse a grupos de usuarios.

Ahora también pueden establecerse en grupos de dispositivos. Para obtener más información, vea Configuración de una página de estado de inscripción.

Errores de sincronización de inscripción de dispositivos automatizada

Se notificarán nuevos errores para iOS/iPadOS y para dispositivos macOS, incluido lo siguiente:

- Caracteres no válidos en el número de teléfono o si el campo está vacío.
- Nombre de configuración no válido o vacío en el perfil.
- Valor de cursor no válido o expirado, o si no se encuentra ningún cursor.
- Token rechazado o expirado.
- El campo Departamento está vacío o la longitud es demasiado larga.
- Apple no encuentra el perfil y se debe crear uno nuevo.
- Se agregará un recuento de los dispositivos de Apple Business Manager eliminados a la página de información general en la que verá el estado de los dispositivos.

iPad compartidos para la empresa

Puede usar Intune y Apple Business Manager para configurar de forma fácil y segura un iPad compartido de modo que varios empleados puedan compartir dispositivos. iPad compartido de Apple proporciona una experiencia personalizada para varios usuarios a la vez que conserva los datos de usuario. Con un identificador de Apple administrado, los usuarios pueden acceder a sus aplicaciones, datos y configuraciones después de iniciar sesión en cualquier iPad compartido de su organización. iPad compartido funciona con identidades federadas.

Para ver esta característica, vaya al Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **iOS** > **Inscripción de iOS** > **Tokens del programa de inscripción** > **elija un token** > **Perfiles** > **Crear perfil** > **iOS**. En la página **Configuración de administración**, seleccione **Inscribir sin afinidad de usuario** y verá la opción **iPad compartido**.

Requiere iPadOS 13.4 y versiones posteriores. En esta versión se ha agregado compatibilidad con sesiones temporales con iPad compartido para que los usuarios puedan acceder a un dispositivo sin un identificador de Apple administrado. Al cerrar sesión, el dispositivo borra todos los datos de usuario para que esté listo para su uso de forma inmediata, lo que elimina la necesidad de borrarlo.

Interfaz de usuario actualizada para la inscripción de dispositivos automatizada de Apple

La interfaz de usuario se ha actualizado para reemplazar el Programa de inscripción de dispositivos de Apple por la inscripción de dispositivos automatizada, con el fin de reflejar la terminología de Apple.

Administración de dispositivos

Disponibilidad del PIN de bloqueo remoto de dispositivo para macOS

La disponibilidad de los PIN de bloqueo remoto para dispositivos macOS ha aumentado de 7 a 30 días.

Cambio del usuario primario en los dispositivos administrados conjuntamente

Puede cambiar el usuario primario de un dispositivo para dispositivos Windows administrados conjuntamente. Para más información sobre cómo buscarlo y cambiarlo, consulte Búsqueda del usuario primario de un dispositivo de Intune. Esta característica se implementará gradualmente a lo largo de las próximas semanas.

Al establecer el usuario primario de Intune, también se establece la propiedad del propietario de Azure AD.

Esta nueva característica establece automáticamente la propiedad del propietario en los dispositivos unidos a Azure AD híbrido recién inscritos al mismo tiempo que se establece el usuario primario de Intune. Para más información sobre el usuario primario, consulte Búsqueda del usuario primario de un dispositivo de Intune.

Se trata de un cambio en el proceso de inscripción y solo se aplica a los dispositivos recién inscritos. En el caso de los dispositivos unidos a Azure AD híbrido existentes, debe actualizar manualmente la propiedad del propietario de Azure AD. Para ello, puede usar la característica Cambiar el usuario primario o un script.

Cuando los dispositivos Windows 10 se unen a un directorio de Azure Active Directory híbrido, el primer usuario del dispositivo se convierte en el usuario primario de Endpoint Manager. Actualmente, el usuario no está

establecido en el objeto de dispositivo de Azure AD correspondiente. Esto produce una incoherencia al comparar la propiedad de *propietario* de un portal de Azure AD con la propiedad de *usuario primario* en el centro de administración de Microsoft Endpoint Manager. La propiedad de propietario de Azure AD se usa para proteger el acceso a las claves de recuperación de BitLocker. La propiedad no se rellena en los dispositivos unidos a Azure AD híbrido. Esta limitación evita la configuración del autoservicio de recuperación de BitLocker desde Azure AD. Esta próxima característica resuelve esta limitación.

Seguridad de dispositivos

Ocultación de la clave de recuperación de los usuarios durante el cifrado de FileVault 2 para dispositivos macOS

Se ha agregado una opción nueva a la categoría *FileVault* dentro de la plantilla Endpoint Protection de macOS: **Ocultar clave de recuperación**. Esta opción oculta la clave personal del usuario final durante el cifrado de FileVault 2.

Para ver la clave de recuperación personal de un dispositivo macOS cifrado, el usuario del dispositivo puede ir a cualquiera de las siguientes ubicaciones y hacer clic en *Obtener clave de recuperación* para el dispositivo macOS:

- Aplicación Portal de empresa de iOS/iPadOS
- Aplicación de Intune
- Sitio web del portal de empresa
- Aplicación Portal de empresa de Android

Compatibilidad con certificados de firma S/MIME y cifrado con Outlook en Android totalmente administrado

Ahora puede usar certificados de firma S/MIME y cifrado con Outlook en dispositivos que ejecutan Android Enterprise totalmente administrado.

Esto amplía la compatibilidad agregada el mes pasado para otras versiones de Android (compatibilidad con certificados de firma S/MIME y cifrado con Outlook en Android). Puede aprovisionar estos certificados mediante perfiles de certificado SCEP y PKCS importados.

Para obtener más información, vea Etiquetado de sensibilidad y protección en Outlook para iOS y Android en la documentación de Exchange.

Adición de un vínculo al sitio web de soporte técnico de Portal de empresa en correos electrónicos por incumplimiento

Cuando configure una plantilla de mensaje de notificación para enviar notificaciones por correo electrónico en caso de incumplimiento, use la nueva opción **Vínculo al sitio web de Portal de empresa** para incluir automáticamente un vínculo a dicho sitio web. Si establece esta opción en *Habilitar*, los usuarios con dispositivos no compatibles que reciban un correo electrónico basado en esta plantilla pueden usar el vínculo para abrir un sitio web y obtener más información sobre por qué su dispositivo no es compatible.

Uso de Microsoft Defender para punto de conexión en directivas de cumplimiento para Android

Ahora puede usar Intune para incorporar dispositivos Android a Microsoft Defender para punto de conexión. Una vez que haya incorporado los dispositivos inscritos, las directivas de cumplimiento para Android podrán usar las señales de *nivel de amenaza* de Microsoft Defender para punto de conexión. Estas son las mismas señales que se podían usar previamente para dispositivos Windows 10.

Configuración de la protección web de Defender para punto de conexión para dispositivos Android

Al usar Microsoft Defender para punto de conexión para dispositivos Android, puede configurar la protección web de Microsoft Defender para punto de conexión para deshabilitar la característica de examen de suplantación de identidad (phishing) o impedir que el examen use la VPN.

En función de cómo se inscriba el dispositivo Android con Intune, estarán disponibles las siguientes opciones:

- Administrador de dispositivos Android: use la configuración de OMA-URI personalizada para deshabilitar la característica de protección web o para deshabilitar el uso de VPN solo durante los exámenes.
- Perfil de trabajo de Android Enterprise: use un perfil de configuración de aplicaciones y el diseñador de configuraciones para deshabilitar todas las funciones de protección web.

Licencias

Los administradores ya no necesitan una licencia de Intune para acceder a la consola de administración de Microsoft Endpoint Manager.

Ahora puede establecer una alternancia en todo el inquilino que elimine el requisito de licencia de Intune para que los administradores accedan a la consola de administración de MEM y a las API de grafos de consulta. Una vez que se elimine el requisito de licencia, nunca se puede volver a restablecer.

> **NOTE**
> Algunas acciones, incluido el flujo del conector de TeamViewer, aún requieren una licencia de Intune para completarse.

Supervisión y solución de problemas

Uso del análisis de puntos de conexión para mejorar la productividad del usuario y reducir los costos de soporte técnico de TI

Durante la semana siguiente se implementará esta característica. El análisis de puntos de conexión tiene como objetivo mejorar la productividad del usuario y reducir los costos de soporte técnico de TI, gracias a la información detallada que se proporciona sobre la experiencia del usuario. La información permite que TI optimice la experiencia del usuario final con soporte técnico proactivo y detecte regresiones a la experiencia del usuario mediante la evaluación del impacto de los cambios de configuración en el usuario. Para más información, consulte Análisis de puntos de conexión (versión preliminar).

Corrección proactiva de los problemas del dispositivo del usuario final mediante paquetes de scripts

Puede crear y ejecutar paquetes de scripts en dispositivos de usuario final para buscar y corregir de forma proactiva los principales problemas de soporte técnico de la organización. La implementación de paquetes de scripts le ayudará a reducir las llamadas de soporte técnico. Cree su propio paquete de scripts o implemente uno de los que hemos escrito y usado en nuestro entorno para disminuir las incidencias de soporte técnico. Intune permite ver el estado de los paquetes de scripts implementados y supervisar los resultados de detección y corrección. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Informes** > **Análisis de puntos de conexión** > **Correcciones proactivas**. Para obtener más información, vea Correcciones proactivas.

Scripts

Disponibilidad de scripts de shell en dispositivos macOS

Los scripts de shell para dispositivos macOS ya están disponibles para los clientes de China y de la nube de administración pública. Para obtener más información sobre los scripts de shell, vea Uso de scripts de shell en dispositivos macOS en Intune.

Mayo de 2020

Administración de aplicaciones

Aplicaciones Windows de 32 bits (x86) en dispositivos ARM64

Las aplicaciones Windows de 32 bits (x86) implementadas como disponibles en dispositivos ARM64 ahora se mostrarán en el Portal de empresa. Para más información sobre las aplicaciones Windows de 32 bits, consulte Administración de aplicaciones Win32.

Icono de la aplicación Portal de empresa de Windows

Se actualizó el icono de la aplicación Portal de empresa de Windows. Para más información sobre el Portal de empresa de Intune, consulte Personalización de las aplicaciones del Portal de empresa de Intune, el sitio web del Portal de empresa y la aplicación de Intune.

Actualización de iconos de la aplicación Portal de empresa para iOS/iPados y macOS

Actualizamos los iconos en Portal de empresa para crear una apariencia más moderna que sea compatible en dispositivos de pantalla doble y se alinee con Microsoft Fluent Design System. Para ver los iconos actualizados, vaya a Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune.

Personalización de acciones de dispositivo de autoservicio en el Portal de empresa

Puede personalizar las acciones de dispositivo de autoservicio disponibles que se muestran a los usuarios finales en la aplicación Portal de empresa y el sitio web. Para ayudar a evitar acciones de dispositivo no deseadas, puede configurar estas opciones para la aplicación Portal de empresa si selecciona **Administración de inquilinos** > **Personalización**. Están disponibles las siguientes acciones:

- Ocultar el botón **Quitar** en los dispositivos corporativos de Windows.
- Ocultar el botón **Restablecer** en los dispositivos corporativos de Windows.
- Ocultar el botón **Restablecer** en los dispositivos corporativos de iOS.
- Ocultar el botón **Quitar** en los dispositivos corporativos de iOS. Para obtener más información, vea Acciones de dispositivo de autoservicio de usuario desde el Portal de empresa.

Actualización automática de aplicaciones disponibles para VPP

Las aplicaciones que se publican como aplicaciones disponibles para el Programa de compras por volumen (PCV) se actualizarán de forma automática cuando se habilita **Actualizaciones automáticas de la aplicación** para el token de PCV. Anteriormente, las aplicaciones disponibles para VPP no se actualizaban de forma automática, sino que los usuarios finales debían ir al Portal de empresa y volver a instalar la aplicación si había disponible una versión más reciente. Las aplicaciones necesarias siguen admitiendo las actualizaciones automáticas.

Experiencia del usuario del Portal de empresa de Android

En la versión 2005 de Portal de empresa de Android, los usuarios finales de dispositivos Android a los que una directiva de protección de aplicaciones emite una advertencia, un bloqueo o un borrado, verán una nueva experiencia de usuario. En lugar de la experiencia de cuadros de diálogo actual, los usuarios finales verán un mensaje de página completa en el que se describe el motivo de la advertencia, el bloqueo o el borrado, y los pasos para corregir el problema. Para obtener más información, vea Experiencia de protección de aplicaciones para dispositivos Android y Configuración de directivas de protección de aplicaciones Android en Microsoft Intune.

Compatibilidad con varias cuentas en el Portal de empresa para macOS

En los dispositivos macOS, ahora Portal de empresa almacena en caché las cuentas de usuario, lo que facilita el inicio de sesión. Los usuarios ya no tienen que iniciar sesión en el Portal de empresa cada vez que inician la aplicación. Además, en el Portal de empresa se mostrará un selector de cuenta si hay varias cuentas de usuario en caché, de modo que los usuarios no tengan que escribir su nombre de usuario.

Nuevas aplicaciones protegidas disponibles

Ya están disponibles las siguientes aplicaciones protegidas:

- Board Papers
- Breezy for Intune
- Hearsay Relate for Intune
- ISEC7 Mobile Exchange Delegate for Intune
- Lexmark for Intune
- Meetio Enterprise
- Microsoft Whiteboard
- Now® Mobile - Intune
- Qlik Sense Mobile
- ServiceNow® Agent - Intune
- ServiceNow® Onboarding - Intune
- Smartcrypt for Intune
- Tact for Intune
- Zero - email for attorneys

Para obtener más información sobre las aplicaciones protegidas, vea Aplicaciones protegidas de Microsoft Intune.

Búsqueda en la documentación de Intune desde el Portal de empresa

Ahora puede buscar en la documentación de Intune directamente desde la aplicación Portal de empresa para macOS. En la barra de menús, seleccione **Ayuda** > **Buscar** y escriba las palabras clave de la búsqueda para encontrar rápidamente las respuestas a las preguntas.

Portal de empresa para Android guía a los usuarios para obtener aplicaciones después de la inscripción del perfil de trabajo

Hemos mejorado las instrucciones en la aplicación del Portal de empresa para facilitar a los usuarios la búsqueda e instalación de aplicaciones. Después de la inscripción en la administración del perfil de trabajo, los usuarios recibirán un mensaje que explica cómo encontrar aplicaciones sugeridas en la versión con distintivo de Google Play. El último paso de Inscribir dispositivos con perfil Android se ha actualizado para mostrar el mensaje nuevo. Los usuarios también verán un nuevo vínculo **Obtener aplicaciones** en el cajón de Portal de empresa de la izquierda. Para dejar espacio a estas experiencias nuevas y mejoradas, se quitó la pestaña **APLICACIONES**. Para ver las pantallas actualizadas, vaya a Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune.

Configuración del dispositivo

Mejoras en la compatibilidad de OEMConfig con dispositivos Zebra Technologies

Intune es totalmente compatible con todas las características proporcionadas por OEMConfig de Zebra. Los clientes que administran dispositivos Zebra Technologies con Android Enterprise y OEMConfig pueden implementar varios perfiles de OEMConfig en un dispositivo. Los clientes también pueden ver informes completos sobre el estado de los perfiles de OEMConfig de Zebra.

Para obtener más información, vea Implementación de varios perfiles de OEMConfig en dispositivos Zebra en Microsoft Intune.

No hay ningún cambio en el comportamiento de OEMConfig para otros OEM.

Se aplica a:

- Android Enterprise
- Dispositivos Zebra Technologies que admiten OEMConfig. Para obtener detalles específicos sobre compatibilidad, póngase en contacto con Zebra.

Configuración de extensiones del sistema en dispositivos macOS

En los dispositivos macOS, puede crear un perfil de extensiones de kernel para configurar opciones en el nivel de kernel (**Dispositivos** > **Perfiles de configuración** > **macOS** para la plataforma > **Extensiones de kernel** para el perfil). Apple va a dejar en desuso las extensiones de kernel y las va a reemplazar por extensiones del sistema en una versión futura.

Las extensiones del sistema se ejecutan en el espacio del usuario y no tienen acceso al kernel. El objetivo es aumentar la seguridad y proporcionar un mayor control al usuario final, a la vez que se limitan los ataques en el nivel de kernel. Tanto las extensiones de kernel como las del sistema permiten a los usuarios instalar extensiones de aplicaciones que amplían las funciones nativas del sistema operativo.

En Intune, puede configurar tanto extensiones de kernel como del sistema (**Dispositivos** > **Perfiles de configuración** > **macOS** para la plataforma > **Extensiones del sistema** para el perfil). Las extensiones de kernel se aplican a la versión 10.13.2 y más recientes. Las extensiones del sistema se aplican a la versión 10.15 y más recientes. Desde macOS 10.15 a macOS 10.15.4, las extensiones de kernel y del sistema se pueden ejecutar en paralelo.

Para obtener información sobre estas extensiones en dispositivos macOS, vea Incorporación de extensiones de macOS.

Se aplica a:

- macOS 10.15 y versiones más recientes

Configuración de preferencias de privacidad de aplicaciones y procesos en dispositivos macOS

Con el lanzamiento de macOS Catalina 10.15, Apple ha agregado nuevas mejoras de seguridad y privacidad. De forma predeterminada, las aplicaciones y los procesos no pueden acceder a datos específicos sin el consentimiento del usuario. Si los usuarios no proporcionan su consentimiento, es posible que las aplicaciones y los procesos no funcionen. Intune va a agregar compatibilidad con opciones que permiten a los administradores de TI permitir o impedir el consentimiento del acceso a datos en nombre de los usuarios finales en dispositivos que ejecuten macOS 10.14 y versiones posteriores. Estas opciones garantizan que las aplicaciones y los procesos sigan funcionando correctamente y reducen el número de mensajes.

Para obtener más información sobre las opciones que se pueden administrar, vea Preferencias de privacidad de macOS.

Se aplica a:

- macOS 10.14 y versiones posteriores

Inscripción de dispositivos

Las restricciones de inscripción admiten etiquetas de ámbito

Ya se pueden asignar etiquetas de ámbito a las restricciones de inscripción. Para ello, vaya al Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **Restricciones de inscripción** > **Crear restricción**. Cree cualquier tipo de restricción y verá la página **Etiquetas de ámbito**. Para obtener más información, consulte Establecer restricciones de inscripción.

Compatibilidad con Autopilot para dispositivos HoloLens 2

Windows Autopilot ya es compatible con dispositivos HoloLens 2. Para más información sobre el uso de Autopilot para HoloLens, consulte Windows Autopilot para HoloLens 2.

Administración de dispositivos

Uso de la acción de sincronización remota de forma masiva para iOS

Ya se puede usar la acción de sincronización remota en hasta 100 dispositivos iOS a la vez. Para ver esta característica, vaya al Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **Todos los dispositivos** > **Acciones masivas del dispositivo**.

Reducción del intervalo de sincronización automatizada de dispositivos a 12 horas

En la Inscripción de dispositivos automatizada de Apple, el intervalo de sincronización automatizada de dispositivos entre Intune y Apple Business Manager se ha reducido de 24 a 12 horas. Para obtener más información sobre la sincronización, vea Sincronización de dispositivos administrados.

Seguridad de dispositivos

Compatibilidad con credenciales derivadas para DISA Purebred en dispositivos Android

Ahora puede usar *DISA Purebred* como proveedor de credenciales derivadas en dispositivos Android Enterprise totalmente administrados. La compatibilidad incluye la recuperación de una credencial derivada de DISA Purebred. Puede usar una credencial derivada para la autenticación de aplicaciones, Wi-Fi, VPN o la firma S/MIME o el cifrado con las aplicaciones que lo admitan.

Envío de notificaciones de inserción como acción en caso de no cumplimiento

Ahora puede configurar una acción en caso de no cumplimiento que envíe una notificación de inserción a un usuario cuando su dispositivo no cumpla las condiciones de una directiva de cumplimiento. La nueva acción es **Enviar notificación push al usuario final** y se admite en dispositivos iOS y Android.

Cuando los usuarios seleccionan la notificación de inserción en su dispositivo, se abre la aplicación Portal de empresa o Intune para mostrar detalles sobre el motivo del no cumplimiento.

Contenido de Seguridad de los puntos de conexión y nuevas características

La documentación de Seguridad de los puntos de conexión de Intune ya está disponible. En el nodo Seguridad

de los puntos de conexión del Centro de administración de Microsoft Endpoint Manager, es posible:

- Crear e implementar directivas de seguridad prioritarias para los dispositivos administrados
- Configurar la integración con Microsoft Defender for Endpoint y administrar las tareas de seguridad para ayudar a corregir los riesgos de los dispositivos en riesgo según la identificación del equipo de Defender for Endpoint
- Configurar líneas base de seguridad
- Supervisar el cumplimiento y las directivas de acceso condicional de un dispositivo
- Ver el estado de cumplimiento de todos los dispositivos desde Intune y Configuration Manager cuando Configuration Manager está configurado para la asociación de clientes.

Además de la disponibilidad de contenido, estas son las novedades de Seguridad de los puntos de conexión este mes:

- **Las directivas de seguridad de los puntos de conexión no están en la** *versión preliminar* _ y ya están listas para usarse en entornos de producción, como _disponibles con carácter general, con dos excepciones:
  - En una nueva *versión preliminar pública*, puede usar el perfil de **reglas de firewall de Microsoft Defender** para la directiva de firewall de Windows 10. Con cada instancia de este perfil, puede configurar hasta 150 reglas de firewall para cumplimentar los perfiles de firewall de Microsoft Defender.
  - La directiva de seguridad de protección de cuentas permanece en versión preliminar.
- Ahora puede **crear un duplicado de directivas de seguridad de puntos de conexión**. Los duplicados conservan la configuración de opciones de la directiva original, pero con un nuevo nombre. La nueva instancia de directiva no incluye ninguna asignación a grupos hasta que se edita la nueva instancia de directiva para agregarlas. Puede duplicar las siguientes directivas:
  - Antivirus
  - Cifrado de discos
  - Firewall
  - Detección de puntos de conexión y respuesta
  - Reducción de la superficie expuesta a ataques
  - Protección de cuentas
- Ahora puede **crear un duplicado de una línea base de seguridad**. Los duplicados conservan la configuración de opciones de la línea base original, pero con un nuevo nombre. La nueva instancia de línea base no incluye ninguna asignación a grupos hasta que no se edita la nueva instancia de línea de base para agregarlas.

- Hay disponible un nuevo informe de la directiva de antivirus de Seguridad de los puntos de conexión: **Puntos de conexión incorrectos de Windows 10**. Este informe es una nueva página que puede seleccionar cuando vea la directiva de antivirus de Seguridad de los puntos de conexión. El informe muestra el estado del antivirus de los dispositivos Windows 10 administrados por MDM.

Compatibilidad con certificados de firma S/MIME y cifrado con Outlook en Android

Ahora puede usar certificados de firma S/MIME y cifrado con Outlook en Android. Con esta compatibilidad, puede aprovisionar estos certificados mediante perfiles de certificado SCEP, PKCS y PKCS importados. Se admiten las siguientes plataformas Android:

- Perfil de trabajo de Android Enterprise
- Administrador de dispositivos Android

Pronto va a estar disponible la compatibilidad con dispositivos Android Enterprise totalmente administrados.

Para obtener más información, vea Etiquetado de sensibilidad y protección en Outlook para iOS y Android en la

documentación de Exchange.

Uso de la directiva de detección de puntos de conexión y respuesta para incorporar dispositivos a Defender for Endpoint

Use la directiva de detección de puntos de conexión y respuesta (EDR) de Seguridad de los puntos de conexión para incorporar y configurar dispositivos para la implementación de Microsoft Defender for Endpoint. EDR admite la directiva para dispositivos Windows administrados por Intune (MDM) y una directiva independiente para dispositivos Windows administrados por Configuration Manager.

Para usar la directiva para dispositivos de Configuration Manager, debe configurar Configuration Manager para admitir la directiva de EDR. La configuración incluye:

- Configure Configuration Manager para la *asociación de inquilinos*.
- Instale una actualización en consola para Configuration Manager a fin de habilitar la compatibilidad con las directivas de EDR. Esta actualización solo se aplica a las jerarquías que tienen habilitada la *asociación de inquilinos*.
- Sincronice las colecciones de dispositivos de la jerarquía con el Centro de administración de Microsoft Endpoint Manager.

Supervisión y solución de problemas

Actualización de la interfaz de usuario de informes de dispositivos

Ahora, el panel de información general de informes proporciona un **Resumen** y una pestaña **Informes**. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Informes** y luego la pestaña **Informes** para ver los tipos de informes disponibles. Para obtener información relacionada, vea Informes de Intune.

Scripting

Compatibilidad con scripts de macOS

La compatibilidad con scripts para macOS ya está disponible con carácter general. Además, se ha agregado compatibilidad con los scripts asignados por el usuario y los dispositivos macOS que se han inscrito con Inscripción de dispositivos automatizada de Apple (anteriormente Programa de inscripción de dispositivos). Para obtener más información, vea Uso de scripts de shell para dispositivos macOS en Intune.

Administración de aplicaciones

Cambio del nombre de Microsoft Office 365 ProPlus

El nombre de Microsoft Office 365 ProPlus se va a cambiar por **Aplicaciones de Microsoft 365 para empresas**. Para obtener más información, vea Cambio de nombre para Office 365 ProPlus. En nuestra documentación, normalmente se hace referencia a este producto como Aplicaciones de Microsoft 365. En el Centro de administración de Microsoft Endpoint Manager, puede encontrar el conjunto de aplicaciones si selecciona **Aplicaciones** > **Windows** > **Agregar**. Para obtener más información sobre cómo agregar aplicaciones, vea Incorporación de aplicaciones a Microsoft Intune.

Administración de la configuración de S/MIME para Outlook en dispositivos Android Enterprise

Podrá usar las directivas de configuración de aplicaciones para administrar la configuración de S/MIME para Outlook en los dispositivos que ejecutan Android Enterprise. También puede elegir si quiere permitir que los usuarios del dispositivo habiliten o deshabiliten S/MIME en la configuración de Outlook. Si quiere usar las directivas de configuración de aplicaciones para Android, en el Centro de administración de Microsoft Endpoint Manager, vaya a **Aplicaciones** > **Directivas de configuración de aplicaciones** > **Agregar** > **Dispositivos administrados**. Para obtener más información sobre la configuración de Outlook, vea Opciones de configuración de Microsoft Outlook.

Pruebas de versión preliminar para aplicaciones de Google Play administrado

Las organizaciones que usan canales de pruebas cerradas de Google Play para las pruebas de versión preliminar de las aplicaciones pueden administrar dichos canales con Intune. Puede asignar de forma selectiva las aplicaciones de línea de negocio publicadas en canales de preproducción de Google Play a grupos piloto para realizar las pruebas. En Intune, puede ver si una aplicación tiene publicado un canal de compilación de pruebas de preproducción, así como asignar ese canal a grupos de dispositivos o de usuarios de Azure AD. Esta

característica está disponible para todos los escenarios de Android Enterprise que se admiten actualmente (perfil de trabajo, totalmente administrado y dedicado). En el Centro de administración de Microsoft Endpoint Manager, puede agregar una aplicación administrada de Google Play. Para ello, seleccione **Aplicaciones** > **Android** > **Agregar**. Para obtener más información, vea Uso de canales de pruebas cerradas de Google Play administrado.

Microsoft Teams ahora se incluye en Microsoft 365 para macOS

Los usuarios a los que se les asigne Microsoft 365 para macOS en Microsoft Endpoint Manager ahora recibirán Microsoft Teams, además de las aplicaciones de Microsoft 365 existentes (Word, Excel, PowerPoint, Outlook y OneNote). Intune reconocerá los dispositivos Mac existentes que tengan instaladas las demás aplicaciones de Office para macOS e intentará instalar Microsoft Teams la próxima vez que el dispositivo se registre con Intune. En el Centro de administración de Microsoft Endpoint Manager, encontrará el **conjunto de aplicaciones de Office 365** para macOS. Para ello, seleccione **Aplicaciones** > **macOS** > **Agregar**. Para obtener más información, vea Asignación de Office 365 a dispositivos macOS con Microsoft Intune.

Actualización para las directivas de configuración de aplicaciones de Android

Las directivas de configuración de aplicaciones de Android se han actualizado para permitir que los administradores seleccionen el tipo de inscripción del dispositivo antes de crear un perfil de configuración de aplicación. La funcionalidad se agregará para tener en cuenta los perfiles de certificado que se basan en el tipo de inscripción (perfil de trabajo o propietario del dispositivo). En esta actualización se ofrece lo siguiente:

1. Si se crea un perfil y se han seleccionado los perfiles de trabajo y de propietario del dispositivo para el tipo de inscripción del dispositivo, no podrá asociar un perfil de certificado a la directiva de configuración de la aplicación.
2. Si se crea un perfil y solo se selecciona el perfil de trabajo, se podrán usar las directivas de certificado del perfil de trabajo creadas en la configuración del dispositivo.
3. Si se crea un perfil y solo se selecciona el perfil de propietario del dispositivo, se podrán usar las directivas de certificado del propietario del dispositivo creadas en la configuración del dispositivo.

> **IMPORTANT**
> Las directivas existentes creadas antes del lanzamiento de esta característica (versión de abril de 2020: 2004) que no tengan ningún perfil de certificado asociado usarán de forma predeterminada los perfiles de trabajo y de propietario del dispositivo para el tipo de inscripción del dispositivo. Además, las directivas existentes creadas antes del lanzamiento de esta característica que tengan perfiles de certificado asociados usarán de forma predeterminada únicamente el perfil de trabajo.

Además, agregamos perfiles de configuración de correo electrónico de Gmail y Nine que funcionarán con los tipos de inscripción de perfil de trabajo y de propietario del dispositivo, e incluirán el uso de perfiles de certificado en ambos tipos de configuración de correo electrónico. Todas las directivas de Gmail o Nine que haya creado en la configuración del dispositivo para perfiles de trabajo seguirán aplicándose al dispositivo, sin necesidad de trasladarlas a las directivas de configuración de aplicaciones.

En el Centro de administración de Microsoft Endpoint Manager, puede buscar directivas de configuración de aplicaciones. Para ello, seleccione **Aplicaciones** > **Directivas de configuración de aplicaciones**. Para obtener más información sobre las directivas de configuración de aplicaciones, consulte Directivas de configuración de aplicaciones para Microsoft Intune.

Notificaciones de inserción al cambiar el tipo de propiedad del dispositivo

Se puede configurar una notificación de inserción para enviársela a los usuarios del Portal de empresa de Android y de iOS como gesto de cortesía hacia su privacidad cuando el tipo de propiedad del dispositivo cambie de Personal a Corporativo. Esta notificación de inserción se establece como desactivada de forma predeterminada. Para encontrar esta opción en Microsoft Endpoint Manager, seleccione **Administración de inquilinos** > **Personalización**. Para obtener más información sobre cómo afecta la propiedad del dispositivo a

los usuarios finales, vea Cambiar la propiedad del dispositivo.

Compatibilidad del panel de personalización con destinatarios de grupo

Puede establecer el destino de la configuración en el panel **Personalización** en grupos de usuarios. Para encontrar estas opciones en Intune, vaya al Centro de administración del Administrador de puntos de conexión de Microsoft y seleccione **Administración de inquilinos** > **Personalización**. Para obtener más información sobre la personalización, vea Personalización de las aplicaciones del Portal de empresa de Intune, sitio web del Portal de empresa y aplicación de Intune.

Configuración del dispositivo

Se admiten varias reglas de VPN a petición "Evaluar cada intento de conexión" en iOS, iPadOS y macOS

La experiencia del usuario de Intune permite agregar varias reglas de VPN a petición en el mismo perfil de VPN con la acción **Evaluar cada intento de conexión** (**Dispositivos** > **Perfiles de configuración** > **Crear perfiles** > **iOS/iPadOS** o **macOS** > para la plataforma > **VPN** para el perfil > **VPN automática** > **A petición**).

Solo se respetaba la primera regla de la lista. Este comportamiento se ha corregido e Intune evalúa todas las reglas de la lista. Cada regla se evalúa en el orden en que aparece en la lista de reglas a petición.

> **NOTE**
> Si tiene perfiles de VPN existentes que usan estas reglas de VPN a petición, la corrección se aplica la próxima vez que cambie el perfil de VPN. Por ejemplo, realice un cambio menor, como cambiar el nombre de la conexión, y guarde el perfil.
>
> Si usa certificados SCEP para la autenticación, este cambio hace que se vuelvan a emitir los certificados para este perfil de VPN.

Se aplica a:

- iOS/iPadOS
- macOS

Para obtener más información sobre los perfiles de VPN, vea Crear perfiles de VPN.

Opciones adicionales en los perfiles de SSO y de extensión de la aplicación de SSO en dispositivos iOS/iPadOS

En dispositivos iOS/iPadOS, puede hacer lo siguiente:

- En los perfiles de SSO (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** para la plataforma > **Características de los dispositivos** para el perfil > **Inicio de sesión único**), establezca el nombre de la entidad de seguridad de Kerberos en el nombre de cuenta del administrador de cuentas de seguridad (SAM) en perfiles de SSO.
- En los perfiles de extensión de la aplicación de SSO (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** para la plataforma > **Características del dispositivo** para el perfil > **Extensión de aplicación de inicio de sesión único**) puede configurar la extensión de Microsoft Azure AD de iOS/iPadOS con menos clics si usa un nuevo tipo de extensión de la aplicación de SSO. Puede habilitar la extensión de Azure AD para dispositivos en modo de dispositivo compartido y enviarle a la extensión datos específicos de esta.

Se aplica a:

- iOS/iPadOS 13.0 y versiones posteriores

Para obtener más información sobre el uso del inicio de sesión único en dispositivos iOS/iPadOS, consulte la introducción a la extensión de aplicación de inicio de sesión único y la lista de opciones de inicio de sesión único.

Nueva configuración de script de shell para dispositivos macOS

Al configurar scripts de shell para dispositivos macOS, ahora puede configurar las siguientes opciones nuevas:

- Ocultar las notificaciones de scripts en los dispositivos
- Frecuencia del script
- Número máximo de reintentos en caso de error del script

Para obtener más información, vea Uso de scripts de shell para dispositivos macOS en Intune.

Inscripción de dispositivos

Eliminación del token de inscripción de dispositivos automatizada de Apple cuando el perfil predeterminado está presente

Anteriormente, no se podía eliminar un perfil predeterminado, lo que implicaba que no se podía eliminar el token de inscripción de dispositivos automatizada asociado. Ahora, puede eliminar el token cuando:

- No haya dispositivos asignados al token
- Haya un perfil predeterminado presente. Para ello, elimine el perfil predeterminado y, luego, el token asociado. Para obtener más información, vea el artículo sobre eliminación de un token de ADE de Intune.

Compatibilidad ampliada con dispositivos de Inscripción de dispositivos automatizada de Apple y Apple Configurator 2, perfiles y tokens

Para ayudar a las organizaciones y los departamentos de TI distribuida, Intune admite ahora hasta 1000 perfiles de inscripción por token, 2000 tokens de inscripción de dispositivos automatizada (anteriormente conocida como DEP) por cuenta de Intune y 75 000 dispositivos por token. No hay ningún límite específico para dispositivos por perfil de inscripción más allá del número máximo de dispositivos por token.

Intune ahora admite hasta 1000 perfiles de Apple Configurator 2.

Para obtener más información, vea Volumen admitido.

Cambios en la entrada de columna de la página Todos los dispositivos

En la página **Todos los dispositivos**, las entradas de la columna **Administrado por** han cambiado:

- Ahora se muestra *Intune* en lugar de *MDM*
- Ahora se muestra *Con administración conjunta* en lugar de *Agente de MDM/ConfigMgr*

Los valores de exportación no han cambiado.

Administración de dispositivos

Información de versión de Trusted Platform Manager (TPM) ahora en la página Hardware de dispositivo

Ahora puede ver el número de versión de TPM en la página de hardware de un dispositivo (Centro de administración del Administrador de puntos de conexión de Microsoft > **Dispositivos** > elegir un dispositivo > **Hardware** > buscar en **Revestimiento de hardware del sistema**).

Asociación de inquilinos de Microsoft Endpoint Manager: sincronización de dispositivos y acciones de dispositivo

Microsoft Endpoint Manager reúne Configuration Manager e Intune en una misma consola. A partir de la versión 2002 de Configuration Manager, puede cargar los dispositivos de Configuration Manager en el servicio en la nube y realizar acciones en ellos en el centro de administración. Para obtener más información, vea Asociación de inquilinos de Microsoft Endpoint Manager: sincronización de dispositivos y acciones de dispositivo.

Supervisión y solución de problemas

Recopilación de registros para mejorar la solución de problemas de scripts asignados a dispositivos macOS

Ahora puede recopilar registros para una mejor solución de problemas de scripts asignados a dispositivos macOS. Puede recopilar registros de hasta 60 MB (comprimidos) o 25 archivos, lo que ocurra primero. Para obtener más información, vea Solución de problemas de directivas de script del shell en macOS mediante la recopilación de registros.

Seguridad

Credenciales derivadas para aprovisionar dispositivos Android Enterprise totalmente administrados con certificados

Intune ahora admite el uso de credenciales derivadas como método de autenticación para dispositivos Android.

Las credenciales derivadas son una implementación de la norma 800-157 del National Institute of Standards and Technology (NIST) relativa a la implementación de certificados en dispositivos. Nuestra compatibilidad con Android amplía nuestra compatibilidad con dispositivos que ejecutan iOS/iPadOS.

Las credenciales derivadas se basan en el uso de una tarjeta de verificación de identidad personal (PIV) o una tarjeta de acceso común (CAC), como una tarjeta inteligente. Para obtener una credencial derivada para un dispositivo móvil, los usuarios comienzan en la aplicación Microsoft Intune y siguen un flujo de trabajo de inscripción que es único para el proveedor que usen. Un requisito común a todos los proveedores es usar una tarjeta inteligente en un equipo para autenticarse en el proveedor de las credenciales derivadas. Tras ello, dicho proveedor emite un certificado para el dispositivo que viene derivado de la tarjeta inteligente del usuario.

Las credenciales derivadas se usan como método de autenticación de los perfiles de configuración de dispositivos de VPN y Wi-Fi. También se pueden usar para la autenticación de aplicaciones y el cifrado y la firma S/MIME de las aplicaciones que lo admiten.

Intune admite ahora los siguientes proveedores de credenciales derivadas con Android:

- Entrust
- Intercede

Un tercer proveedor, DISA Purebred, estará disponible para Android en una versión futura.

Línea de base de seguridad de Microsoft Edge ya está disponible con carácter general

Ya está disponible una nueva versión de la característica Línea de base de seguridad de Microsoft Edge y se publica como disponible con carácter general (GA). La línea de base de Microsoft Edge anterior estaba en versión preliminar. La nueva versión de línea de base corresponde a abril de 2020 (Microsoft Edge versión 80 y posteriores).

Con el lanzamiento de esta nueva línea de base, ya no podrá crear perfiles basados en las versiones de línea de base anteriores, pero puede seguir usando los perfiles que haya creado con esas versiones. También puede optar por actualizar los perfiles existentes para usar la versión de línea de base más reciente.

Marzo de 2020

Administración de aplicaciones

Experiencia de inicio de sesión mejorada en la aplicación Portal de empresa para Android

Hemos actualizado el diseño de varias pantallas de inicio de sesión en la aplicación Portal de empresa para Android a fin de que la experiencia sea más moderna, sencilla y limpia para los usuarios. Para comprobar las mejoras, vea Novedades de la interfaz de usuario de aplicaciones.

Configuración del agente de optimización de entrega al descargar contenido de aplicaciones Win32

El agente de optimización de distribución se puede configurar para descargar contenido de aplicaciones Win32 en primer o segundo plano en función de la asignación. En el caso de las aplicaciones Win32 existentes, el contenido se seguirá descargando en el modo de segundo plano. En el Centro de administración del Administrador de puntos de conexión de Microsoft, seleccione **Aplicaciones** > **Todas las aplicaciones** > *seleccione la aplicación Win32* > **Propiedades**. Seleccione **Editar** junto a **Asignaciones**. Edite la asignación seleccionando **Incluir** en **Modo**, en la sección **Requerido**. Verá la nueva configuración en la sección **Configuración de la aplicación**. Para obtener más información sobre la Optimización de entrega, vea Administración de aplicaciones Win32: Optimización de entrega.

Modo horizontal admitido en Portal de empresa para iOS

Los usuarios ahora pueden inscribir sus dispositivos, buscar aplicaciones y obtener soporte técnico de TI con la orientación de pantalla que prefieran. La aplicación detectará y ajustará automáticamente las pantallas para ajustarse al modo horizontal o vertical, a menos que los usuarios bloqueen la pantalla en modo vertical.

Compatibilidad con scripts para dispositivos macOS (Versión preliminar pública)

Se podrán agregar e implementar scripts en dispositivos macOS. Esta compatibilidad amplía la capacidad de

configurar dispositivos macOS más allá de lo que es posible con las funcionalidades de MDM nativas en dispositivos macOS. Para obtener más información, vea Uso de scripts de shell para dispositivos macOS en Intune.

Actualizaciones del Portal de empresa de iOS y macOS

El panel Perfil del Portal de empresa en macOS e iOS se ha actualizado para incluir el botón Cerrar sesión. Además, se han realizado mejoras de la interfaz de usuario en el panel Perfil en el Portal de empresa para macOS. Para más información sobre Portal de empresa, vea Configuración de la aplicación Portal de empresa de Microsoft Intune.

Cambio del destino de clips web a Microsoft Edge en dispositivos iOS

Los clips web recién implementados (aplicaciones web ancladas) en los dispositivos iOS que se necesitan para abrirse en un explorador protegido se abrirán en Microsoft Edge en lugar de en Intune Managed Browser. Debe cambiar el destino de los clips web existentes para asegurarse de que se abran en Microsoft Edge en lugar de en Managed Browser. Para obtener más información, consulte Administración del acceso web mediante Microsoft Edge con Microsoft Intune y Agregar aplicaciones web a Microsoft Intune.

Uso de la herramienta de diagnóstico de Intune con Microsoft Edge para Android

Microsoft Edge para Android ahora está integrado con la herramienta de diagnóstico de Intune. De forma similar a la experiencia en Microsoft Edge para iOS, al escribir "about:intunehelp" en la barra de dirección URL (el cuadro de dirección) de Microsoft Edge en el dispositivo se iniciará la herramienta de diagnóstico de Intune. Esta herramienta proporcionará registros detallados. Los usuarios pueden recibir la solicitud de recopilar y enviar estos registros a su departamento de informática, o bien ver los registros de MAM para aplicaciones específicas.

Actualización de la marca y la personalización de Intune

Hemos actualizado el panel de Intune que se denominaba "Personalización de marca y personalización" con mejoras, como las siguientes:

- Se va a cambiar el nombre del panel a **Personalización**.
- Se va a mejorar la organización y el diseño de las opciones.
- Se va a mejorar el texto y la información sobre herramientas de las opciones.

Para encontrar estas opciones en Intune, vaya al Centro de administración del Administrador de puntos de conexión de Microsoft y seleccione **Administración de inquilinos** > **Personalización**. Para obtener información sobre la personalización existente, vea Configuración de la aplicación Portal de empresa de Microsoft Intune.

Clave de recuperación cifrada personal del usuario

Hay una nueva característica de Intune disponible que permitirá a los usuarios recuperar su clave de recuperación de **FileVault** cifrada personal para dispositivos Mac a través de la aplicación Portal de empresa de Android o la aplicación de Intune de Android. Hay un vínculo en la aplicación Portal de empresa y en la aplicación de Intune que abrirá un explorador Chrome en el Portal de empresa web, donde el usuario puede ver la clave de recuperación de **FileVault** necesaria para acceder a sus dispositivos Mac. Para obtener más información sobre el cifrado, vea Uso del cifrado de dispositivos con Intune.

Optimización de inscripción de dispositivos dedicados

Estamos optimizando la inscripción para dispositivos dedicados de Android Enterprise y facilitando la aplicación de certificados SCEP asociados a Wi-Fi a dispositivos dedicados inscritos antes del 22 de noviembre de 2019. En el caso de las nuevas inscripciones, la aplicación de Intune se seguirá instalando, pero los usuarios finales ya no tendrán que realizar el paso para **habilitar el agente de Intune** durante la inscripción. La instalación se realizará en segundo plano automáticamente y los certificados SCEP asociados a Wi-Fi se pueden implementar y establecer sin interacción del usuario final.

Estos cambios se implementarán por fases a lo largo del mes de marzo, a medida que se implemente el back-end de servicio de Intune. Todos los inquilinos tendrán este nuevo comportamiento hasta el final de marzo. Para

ver información relacionada, consulte Compatibilidad con certificados de SCEP en dispositivos dedicados de Android Enterprise.

Configuración del dispositivo

Nueva experiencia del usuario al crear plantillas administrativas en dispositivos Windows

A raíz de los comentarios de los clientes y nuestro cambio a la nueva experiencia de pantalla completa de Azure, hemos vuelto a generar la experiencia de perfil de plantillas administrativas con una vista de carpeta. No hemos realizado cambios en ninguna configuración o perfil existente. Por lo tanto, los perfiles existentes seguirán siendo los mismos y se podrán usar en la nueva vista. Todavía puede desplazarse por todas las opciones de configuración seleccionando **Toda la configuración** y usando la búsqueda. La vista de árbol se divide por configuraciones de equipo y usuario. Encontrará la configuración de Windows, Office y Microsoft Edge en sus carpetas asociadas.

Se aplica a:

- Windows 10 y versiones posteriores

Uso permanente de Always On por parte de los perfiles de VPN con conexiones VPN IKEv2 con dispositivos iOS/iPadOS

En dispositivos iOS/iPadOS, puede crear un perfil de VPN que use una conexión IKEv2 (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** para plataforma > **VPN** para tipo de perfil). Ahora puede configurar AlwaysOn con IKEv2. Cuando los perfiles de VPN IKEv2 están configurados, se conectan automáticamente y permanecen conectados (o se vuelven a conectar rápidamente) a la VPN. Permanecen conectados incluso al moverse entre redes o al reiniciar dispositivos.

En iOS/iPadOS, la VPN de Always On está limitada a perfiles de IKEv2.

Para ver la configuración IKEv2 que puede establecer, vaya a Incorporación de VPN en dispositivos iOS en Microsoft Intune.

Se aplica a:

- iOS/iPadOS

Eliminación de agrupaciones y matrices de agrupaciones en perfiles de configuración de dispositivos OEMConfig en dispositivos Android Enterprise

En los dispositivos Android Enterprise, puede crear y actualizar perfiles de OEMConfig (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Android Enterprise** para plataforma > **OEMConfig** para tipo de perfil). Los usuarios pueden ahora eliminar agrupaciones y matrices de agrupaciones mediante el **Diseñador de configuraciones** de Intune.

Para obtener más información sobre los perfiles OEMConfig, vea Uso y administración de dispositivos Android Enterprise con OEMConfig en Microsoft Intune.

Se aplica a:

- Android Enterprise

Configuración de la extensión de aplicación de inicio de sesión único de Microsoft Azure AD en iOS/iPadOS

El equipo de Microsoft Azure AD creó una extensión de aplicación de inicio de sesión único (SSO) de redireccionamiento que permite a los usuarios de iOS/iPadOS 13.0+ obtener acceso a aplicaciones y sitios web de Microsoft con un inicio de sesión. Todas las aplicaciones que anteriormente tenían autenticación asincrónica con la aplicación Microsoft Authenticator seguirán recibiendo SSO con la nueva extensión de SSO. Con la versión de la extensión de aplicación de SSO de Azure AD, puede configurar la extensión de SSO con el tipo de extensión de aplicación de SSO de redireccionamiento (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPad** para la plataforma > **Características del dispositivo** para el tipo de perfil > **Extensión de aplicación de inicio de sesión único**).

Se aplica a:

- iOS 13.0 y versiones más recientes
- IPadOS 13.0 y versiones más recientes

Para obtener más información sobre las extensiones de aplicación de SSO de iOS, consulte Extensión de aplicación de inicio de sesión único.

La opción de modificación de la configuración de confianza de aplicaciones empresariales se ha quitado de los perfiles de restricción de dispositivos iOS/iPadOS.

En los dispositivos iOS/iPadOS puede crear un perfil de restricciones de dispositivo (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** para la plataforma > **Restricciones de dispositivos** para el tipo de perfil). Apple ha quitado la opción **Modificación de la configuración de confianza de aplicaciones empresariales**, y también se ha quitado de Intune. Si usa actualmente esta configuración en un perfil, no tiene ningún impacto y se quita de los perfiles existentes. Esta opción también se ha quitado de los informes en Intune.

Se aplica a:

- iOS/iPadOS

Para ver los valores que puede restringir, vaya a Configuración de dispositivos iOS e iPadOS para permitir o restringir características.

Solución de problemas: Cambio de la notificación de directiva de MAM pendiente a icono informativo

El icono de notificación de una directiva de MAM pendiente en la hoja de solución de problemas se ha cambiado a un icono informativo.

Actualización de la interfaz de usuario al configurar la directiva de cumplimiento

Hemos actualizado la interfaz de usuario para crear directivas de cumplimiento en el Administrador de puntos de conexión de Microsoft (**Dispositivos** > **Directivas de cumplimiento** > **Directivas** > **Crear directiva**). Tenemos una nueva experiencia de usuario que proporciona la misma configuración y los mismos detalles que ha usado anteriormente. La nueva experiencia sigue un proceso similar a un asistente para crear una directiva de cumplimiento e incluye una página en la que puede agregar *Asignaciones* a la directiva, y una página *Revisar y crear* en la que puede revisar la configuración antes de crear la directiva.

Retirar dispositivos no compatibles

Hemos agregado una nueva acción para dispositivos no compatibles que puede agregar a cualquier directiva para retirar el dispositivo no compatible. La nueva acción, **Retirar el dispositivo no compatible**, da como resultado la eliminación de todos los datos de la compañía del dispositivo, y también quita el dispositivo de la administración de Intune. Esta acción se ejecuta cuando se alcanza el valor configurado en días y, en ese momento, el dispositivo se puede retirar. El valor mínimo es 30 días. Se requerirá la aprobación explícita del administrador de TI para retirar los dispositivos mediante la sección *Retirada de los dispositivos no compatibles*, donde los administradores pueden retirar todos los dispositivos que cumplan los requisitos.

Compatibilidad con WPA y WPA2 en perfiles de Wi-Fi Empresarial de iOS

Los perfiles de Wi-Fi de empresa para iOS admiten ahora el campo *Tipo de seguridad*. En *Tipo de seguridad*, puede seleccionar **WPA Enterprise** o **WPA/WPA2 Enterprise** y, a continuación, especificar una selección para el *tipo de EAP*. (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** y seleccione **iOS/iPad** para *Plataforma* y **Wi-Fi** para *Perfil*).

Las nuevas opciones de empresa son similares a las que están disponibles para un perfil de Wi-Fi básico para iOS.

Nueva experiencia de usuario para perfiles de certificado, correo electrónico, VPN y Wi-Fi

Se ha actualizado la experiencia del usuario en el Centro de administración del Administrador de puntos de conexión (**Dispositivos** > **Perfiles de configuración** > **Crear perfil**) para crear y modificar los siguientes tipos de perfil. La nueva experiencia presenta las mismas opciones que antes, pero usa una experiencia similar a un asistente que no requiere tanto desplazamiento horizontal. Con la nueva experiencia no tendrá que modificar las configuraciones existentes.

- Credencial derivada
- Correo electrónico
- Certificado PKCS
- Certificado PKCS importado
- Certificado SCEP
- Certificado de confianza
- VPN
- Wi-Fi

Experiencia de interfaz de usuario mejorada al crear perfiles de restricciones de dispositivo en dispositivos Android y Android Enterprise

Al crear un perfil para dispositivos Android o Android Enterprise, se actualizará la experiencia en el Centro de administración de Microsoft Endpoint Manager. Este cambio afecta a los perfiles de configuración de dispositivo siguientes (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **Administrador de dispositivos Android** o **Android Enterprise** para la plataforma):

- Restricciones de dispositivos: Administrador de dispositivos Android
- Restricciones de dispositivos: Propietario del dispositivo Android Enterprise
- Restricciones de dispositivos: Perfil de trabajo de Android Enterprise

Para obtener más información sobre las restricciones de dispositivos que se pueden configurar, vea Administrador de dispositivos Android y Android Enterprise.

Experiencia de interfaz de usuario mejorada al crear perfiles de configuración en dispositivos iOS/iPadOS y macOS

Al crear un perfil para dispositivos iOS o macOS, se actualizará la experiencia en el Centro de administración de Microsoft Endpoint Manager. Este cambio afecta a los siguientes perfiles de configuración de dispositivos (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **iOS/iPadOS** o **macOS** para plataforma):

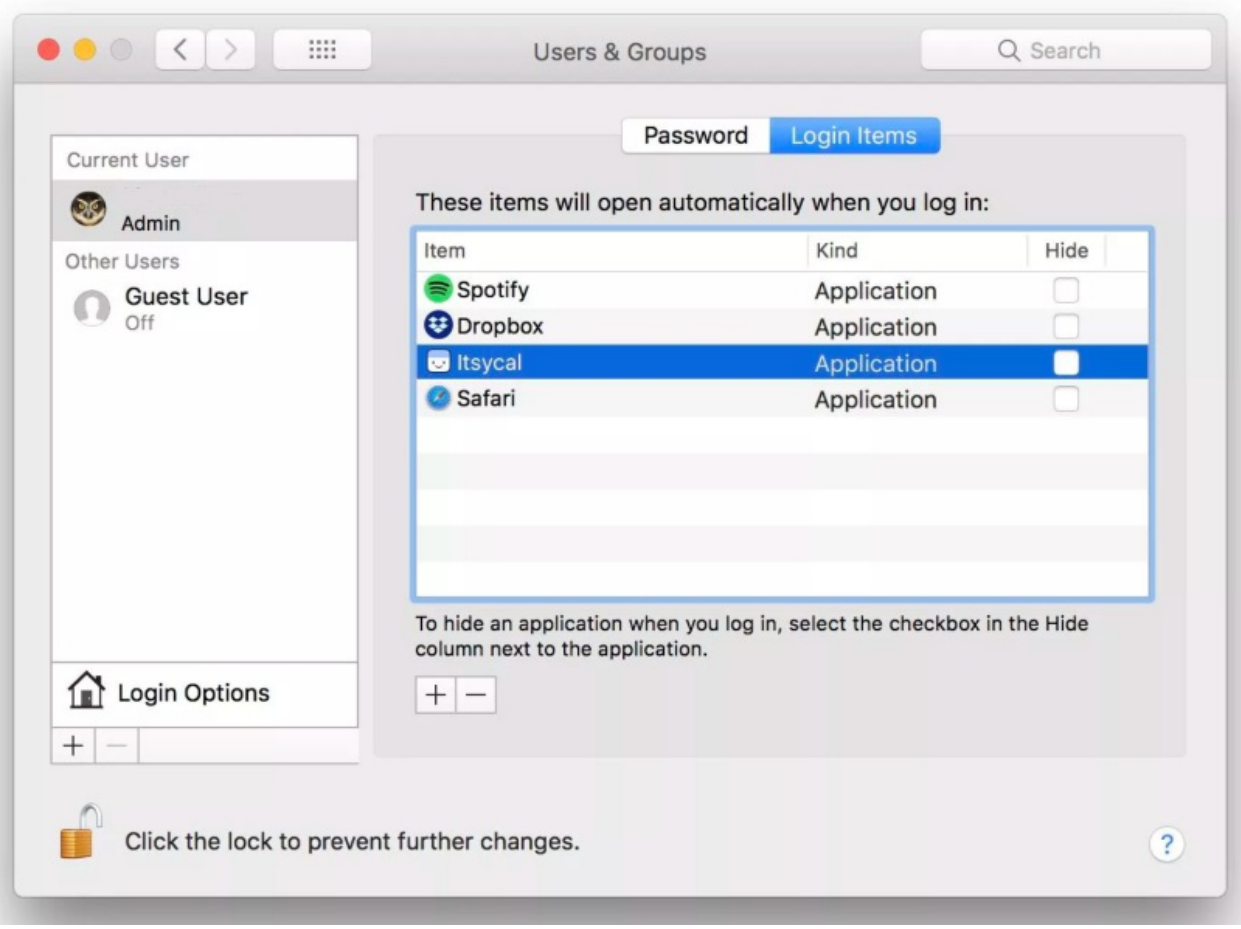
- Personalizado: iOS/iPadOS y macOS
- Características del dispositivo: iOS/iPadOS y macOS
- Restricciones de dispositivos: iOS/iPadOS y macOS
- Endpoint Protection: macOS
- Extensiones: macOS
- Archivo de preferencias: macOS

Opción Ocultar en la configuración del usuario en características del dispositivo en dispositivos macOS

Al crear un perfil de dispositivo de configuración de características en dispositivos macOS, hay una nueva opción **Ocultar en la configuración del usuario** (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** para plataforma > **Características del dispositivo** para perfil > **Elementos de inicio de sesión**).

Esta característica establece la marca de verificación ocultar de una aplicación en la lista de aplicaciones de elementos de inicio de sesión **Usuarios y grupos** en dispositivos macOS. Los perfiles existentes muestran este valor en la lista como sin configurar. Para configurar esta opción, los administradores pueden actualizar los perfiles existentes.

Cuando se establece en **Ocultar**, la casilla ocultar está activada para la aplicación y los usuarios no pueden cambiarla. También oculta la aplicación a los usuarios después de que estos inicien sesión en sus dispositivos.



Para obtener más información sobre los parámetros que se pueden configurar, vea Configuración de características de dispositivos macOS.

Esta característica se aplica a:

- macOS

Inscripción de dispositivos

Configuración de la disponibilidad de la inscripción en Portal de empresa para iOS y Android

Puede configurar si la inscripción de dispositivos en el Portal de empresa en dispositivos iOS y Android está disponible con mensajes o sin mensajes o no está disponible para los usuarios. Para encontrar estas opciones en Intune, vaya al Centro de administración de Microsoft Endpoint Manager y seleccione **Administración de inquilinos** > **Personalización** > **Editar** > **Inscripción de dispositivos**.

La compatibilidad con la configuración de inscripción de dispositivos requiere que los usuarios finales tengan estas versiones del Portal de empresa:

- Portal de empresa en iOS: versión 4.4 o posterior
- Portal de empresa en Android: versión 5.0.4715.0 o posterior

Para obtener más información sobre la personalización existente del Portal de empresa, vea Configuración de la aplicación Portal de empresa de Microsoft Intune.

Administración de dispositivos

Nuevo informe de Android en la página de información general de dispositivos Android

Hemos agregado un informe a la consola de administración del Administrador de puntos de conexión de Microsoft en la página de información general de dispositivos Android, en la que se muestra el número de dispositivos Android inscritos en cada solución de administración de dispositivos. En este gráfico (como en el de la consola de Azure) se muestra la cantidad de dispositivos inscritos de perfil de trabajo, totalmente administrados, dedicados y de administrador de dispositivos. Para ver el informe, elija **Dispositivos** > **Android** > **Información general**.

Guía para usuarios desde la administración de administradores de dispositivos Android a la administración de perfiles de trabajo

Se va a publicar una nueva opción de cumplimiento para la plataforma de administrador de dispositivos Android. Esta opción permite hacer que un dispositivo no sea compatible si se administra con el administrador de dispositivos.

En estos dispositivos no compatibles, en la página **Actualizar configuración del dispositivo**, los usuarios verán el mensaje **Mover a la nueva configuración de administración de dispositivos**. Si pulsa el botón **Resolver**, se les guiará por lo siguiente:

1. Anulación de la inscripción desde la administración de administradores de dispositivos
2. Inscripción en la administración de perfiles de trabajo
3. Resolución de problemas de cumplimiento

En un esfuerzo por cambiar a la administración de dispositivos moderna, más completa y segura, Google va a reducir la compatibilidad con el administrador de dispositivos en las nuevas versiones de Android. Intune solo puede proporcionar compatibilidad completa con dispositivos Android administrados por el administrador de dispositivos que ejecuten Android 10 y versiones posteriores hasta el segundo trimestre de 2020. Los dispositivos administrados por el administrador de dispositivos (menos Samsung) que ejecuten Android 10 o versiones posteriores después de este periodo ya no se podrán administrar de forma completa. En concreto, los dispositivos afectados no recibirán nuevos requisitos de contraseña.

Para obtener más información acerca de esta configuración, consulte Transferencia de dispositivos Android desde el administrador de dispositivos a la administración de perfiles de trabajo.

Dirección URL nueva para el Centro de administración de Microsoft Endpoint Manager

En consonancia con el anuncio del año pasado relativo a Microsoft Endpoint Manager en Ignite, hemos cambiado la dirección URL del Centro de administración de Microsoft Endpoint Manager (anteriormente Administración de dispositivos de Microsoft 365) a https://endpoint.microsoft.com. La dirección URL del centro de administración anterior (https://devicemanagement.microsoft.com) continuará funcionando, pero se recomienda empezar a acceder al Centro de administración de Microsoft Endpoint Manager con la dirección URL nueva.

Para obtener más información, vea Simplificación de las tareas de TI mediante el Centro de administración de Microsoft Endpoint Manager.

Cambio del usuario primario para dispositivos Windows

Puede cambiar el usuario primario de dispositivos híbridos de Windows y unidos a Azure AD. Para ello, vaya a **Intune** > **Dispositivos** > **Todos los dispositivos** > elija un dispositivo > **Propiedades** > **Usuario primario**. Para más información, vea Cambio del usuario principal de un dispositivo.

También se ha creado un nuevo permiso RBAC (Dispositivos administrados/Establecer usuario primario) para esta tarea. El permiso se ha agregado a diversos roles integrados como, por ejemplo, Departamento de soporte técnico, Administrador educativo y Administrador de seguridad de puntos de conexión.

Esta característica se está implementando en los clientes de forma global en su versión preliminar. Debería verla en las próximas semanas.

Asociación de inquilinos de Microsoft Endpoint Manager: sincronización de dispositivos y acciones de dispositivo

Microsoft Endpoint Manager reúne Configuration Manager e Intune en una misma consola. A partir de la versión 2002.2 de Technical Preview de Configuration Manager, se pueden cargar dispositivos de Configuration Manager en el servicio en la nube y realizar acciones en ellos en el centro de administración. Para más información, vea de Características de la versión 2002.2 de Technical Preview de Configuration Manager.

Revise el artículo de Technical Preview de Configuration Manager antes de instalar esta actualización. Ese artículo le ayuda a familiarizarse con los requisitos generales y las limitaciones para usar una versión Technical Preview, cómo actualizar entre versiones y cómo proporcionar comentarios.

Acciones remotas en masa

Ahora puede emitir comandos en masa para las siguientes acciones remotas: reiniciar, cambiar el nombre, restablecer Autopilot, borrar y eliminar. Para ver las nuevas acciones en masa, vaya al Centro de administración del Administrador de puntos de conexión de Microsoft > **Dispositivos** > **Todos los dispositivos** > **Acciones en masa**.

Lista de todos los dispositivos búsqueda, ordenación y filtro mejorados

La lista Todos los dispositivos se ha mejorado para optimizar el rendimiento, la búsqueda, la ordenación y el filtrado. Para más información, vea esta sugerencia de soporte técnico.

Supervisión y solución de problemas

Ahora, el almacenamiento de datos proporciona la dirección MAC.

El almacenamiento de datos de Intune proporciona la dirección MAC como una nueva propiedad (`EthernetMacAddress`) en la entidad `device` para permitir que los administradores se correspondan entre el usuario y la dirección Mac del host. Esta propiedad ayuda a llegar a usuarios específicos y a solucionar los incidentes que se producen en la red. Los administradores también pueden usar esta propiedad en Informes de Power BI para generar informes más completos. Para obtener más información, vea la entidad de dispositivo en el Almacenamiento de datos de Intune.

Propiedades de inventario de dispositivos de almacenamiento de datos adicionales

Las propiedades adicionales de inventario de dispositivos están disponibles mediante el Almacenamiento de datos de Intune. Las propiedades siguientes ahora se exponen por medio de la colección beta devices:

- `ethernetMacAddress` : identificador de red único de este dispositivo.
- `model` : modelo del dispositivo.
- `office365Version` : versión de Microsoft 365 instalada en el dispositivo.
- `windowsOsEdition` : versión del sistema operativo.

Las propiedades siguientes ahora se exponen por medio de la colección beta devicePropertyHistory:

- `physicalMemoryInBytes` : memoria física en bytes.
- `totalStorageSpaceInBytes` : capacidad total de almacenamiento en bytes.

Para obtener más información, vea API de Data Warehouse de Microsoft Intune.

Actualización del flujo de trabajo de ayuda y soporte técnico para admitir servicios adicionales

Hemos actualizado la página de ayuda y soporte técnico en el centro de administración del Administrador de puntos de conexión de Microsoft, donde ahora elige el tipo de administración que usa. Con este cambio podrá seleccionar de entre los tipos de administración siguientes:

- Configuration Manager (incluye Análisis de escritorio)
- Intune
- Administración conjunta

Seguridad

Uso de una versión preliminar de las directivas centradas en el administrador de seguridad como parte de la seguridad del punto de conexión

Como versión preliminar pública, se han agregado varios grupos de directivas nuevos en el nodo de seguridad del punto de conexión en el centro de administración de puntos de conexión de Microsoft. Como administrador de seguridad, puede usar estas nuevas directivas para centrarse en aspectos específicos de la seguridad de los dispositivos con el fin de administrar grupos discretos de configuración relacionada sin la sobrecarga del cuerpo de directivas de configuración de dispositivos, más grande.

A excepción de la nueva *directiva antivirus para el antivirus de Microsoft Defender* (consulte a continuación), la configuración de cada una de estas nuevas directivas y perfiles en versión preliminar es la misma que ya ha configurado hoy a través de los perfiles de configuración de dispositivos.

Estos son los nuevos tipos de directivas que se encuentran en versión preliminar y sus tipos de perfil

disponibles:

- **Antivirus (versión preliminar)** :
  - macOS:
    - **Antivirus**: administre la configuración de directivas antivirus para macOS para administrar Microsoft Defender for Endpoint para Mac.
  - Windows 10 y versiones posteriores:
    - **Antivirus de Microsoft Defender**: administre la configuración de directivas antivirus para protección en la nube, exclusiones del antivirus, correcciones, opciones de análisis, etc.

      El perfil antivirus para el *antivirus de Microsoft Defender* es una excepción que introduce una nueva instancia de la configuración que se encuentra como parte de un perfil de restricción de dispositivos. Estas nuevas opciones de configuración del antivirus:

      - Son las mismas opciones que se encuentran en las restricciones de dispositivos, pero admiten una tercera opción de configuración que no está disponible cuando se configura como una restricción de dispositivo.
      - Se aplican a los dispositivos que se administran conjuntamente con Configuration Manager, cuando el control deslizante de carga de trabajo de administración conjunta para Endpoint Protection está establecido en Intune.

      Planean usar el nuevo perfil *Antivirus* > *Antivirus de Microsoft Defender* en lugar de configurarlos a través de un perfil de restricción de dispositivos.
    - **Experiencia de seguridad de Windows**: administre la configuración de seguridad de Windows que los usuarios finales pueden ver en el centro de seguridad de Microsoft Defender y las notificaciones que reciben. Estos valores no se modifican respecto a los disponibles como perfil de Endpoint Protection en la configuración de dispositivos.
- **Cifrado de disco (versión preliminar)** :
  - macOS:
    - **FileVault**
  - Windows 10 y versiones posteriores:
    - **BitLocker**
- **Firewall (versión preliminar)** :
  - macOS:
    - **Firewall de macOS**
  - Windows 10 y versiones posteriores:
    - **Firewall de Microsoft Defender**
- **Detección de puntos de conexión y respuesta (versión preliminar)** :
  - Windows 10 y versiones posteriores: -**Windows 10 Intune**
- **Reducción de la superficie expuesta a ataques (versión preliminar)** :
  - Windows 10 y versiones posteriores:
    - **Aislamiento de aplicaciones y navegador**
    - **Protección web**
    - **Control de la aplicación**
    - **Reglas de reducción de la superficie expuesta a ataques**
    - **Control de dispositivos**
    - **Protección contra vulnerabilidades**

- **Protección de cuentas (versión preliminar)** :
  - Windows 10 y versiones posteriores:
    - **Protección de cuentas**

Febrero de 2020

Administración de aplicaciones

Aplicación Microsoft Defender for Endpoint para macOS

Intune proporciona una manera sencilla de implementar la aplicación Microsoft Defender for Endpoint para macOS en dispositivos Mac administrados. Para más información, consulte el artículo sobrecómo agregar Microsoft Defender for Endpoint a dispositivos macOS con Microsoft Intune y Microsoft Defender for Endpoint para Mac.

mejoras en la experiencia del usuario del Portal de empresa de macOS

Se han realizado mejoras en la experiencia de inscripción de dispositivos macOS y en la aplicación Portal de empresa para Mac. Verá las siguientes mejoras:

- Mejora de la experiencia de Microsoft **AutoUpdate** durante la inscripción que garantizará que los usuarios tengan la versión más reciente del Portal de empresa.
- Paso de comprobación de cumplimiento mejorado durante la inscripción.
- Compatibilidad con los identificadores de incidentes copiados, por lo que los usuarios pueden enviar los errores más rápido desde sus dispositivos al equipo de soporte técnico de su empresa.

Para obtener más información sobre la inscripción y la aplicación Portal de empresa aplicación para Mac, vea Inscripción del dispositivo macOS mediante la aplicación Portal de empresa.

Ahora las directivas de protección de aplicaciones para Better Mobile admiten iOS e iPadOS

En octubre de 2019, la directiva de protección de aplicaciones de Intune agregó la capacidad de usar datos de nuestros asociados de Microsoft Threat Defense. Con esta actualización, ahora puede usar una directiva de protección de aplicaciones para bloquear o borrar de forma selectiva los datos corporativos de los usuarios en función del estado de un dispositivo mediante Better Mobile en iOS e iPadOS. Para más información, consulte Creación de una directiva de protección de aplicaciones de Mobile Threat Defense con Intune.

Microsoft Edge versión 77 y posteriores en dispositivos con Windows 10

Intune ahora admite la desinstalación de la versión 77 y posteriores de Microsoft Edge en dispositivos con Windows 10. Para obtener más información, consulte Adición de Microsoft Edge para Windows 10 a Microsoft Intune.

Pantalla quitada del Portal de empresa, inscripción del perfil de trabajo de Android

La pantalla **¿Cuál es el paso siguiente?** se ha quitado del flujo de inscripción del perfil de trabajo de Android en el Portal de empresa para simplificar la experiencia del usuario. Vaya a Inscripción con el perfil de trabajo de Android para ver el flujo de inscripción del perfil de trabajo de Android actualizado.

Rendimiento mejorado de la aplicación Portal de empresa

La aplicación Portal de empresa se ha actualizado para admitir un rendimiento mejorado en los dispositivos que usan procesadores ARM64, como Surface Pro X. Anteriormente, el Portal de empresa operaba en un modo ARM32 emulado. Ahora, en la versión 10.4.7080.0 y en versiones posteriores, la aplicación Portal de empresa se compila de forma nativa para ARM64. Para más información sobre la aplicación Portal de empresa, consulte Configuración de la aplicación Portal de empresa de Microsoft Intune.

Nueva aplicación de Office de Microsoft

La nueva aplicación de Office de Microsoft ya está disponible con carácter general para su descarga y uso. La aplicación de Office es una experiencia consolidada en la que los usuarios pueden trabajar en Word, Excel y PowerPoint en una sola aplicación. Puede dirigirse a la aplicación con una directiva de protección de aplicaciones para asegurarse de que los datos a los que se accede están protegidos.

Para obtener más información, vea Procedimiento para habilitar las directivas de protección de aplicaciones de Intune con la aplicación de Office en versión preliminar para dispositivos móviles.

Configuración del dispositivo

Habilitación del control de acceso a la red (NAC) con la VPN de Cisco AnyConnect en dispositivos iOS

En los dispositivos iOS, puede crear un perfil de VPN y usar tipos de conexión diferentes, entre los que se incluyen Cisco AnyConnect (**Configuración de dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para la plataforma > **VPN** para el tipo de perfil > **Cisco AnyConnect** para el tipo de conexión).

Puede habilitar el control de acceso a la red (NAC) con Cisco AnyConnect. Para usar esta característica,:

1. En la Guía del administrador del motor de Cisco Identity Services, siga los pasos de **Configuración de Microsoft Intune como servidor MDM** para configurar el motor de Cisco Identity Services (ISE) en Azure.
2. En el perfil de configuración de dispositivos de Intune, seleccione la opción **Habilitar el control de acceso a la red (NAC)** .

Para ver las opciones de VPN disponibles, vaya a Configuración de VPN en dispositivos iOS.

Inscripción de dispositivos

Número de serie en la página del certificado push MDM de Apple

Ahora en la página del certificado push MDM de Apple se muestra el número de serie. El número de serie es necesario para recuperar el acceso al certificado de extracción MDM de Apple si se pierde el acceso al id. de Apple que creó el certificado. Para ver el número de serie, vaya a **Dispositivos** > **iOS** > **Inscripción de iOS** > **Certificado push MDM de Apple**.

Administración de dispositivos

Nuevas opciones de programación de actualización para insertar actualizaciones del sistema operativo en dispositivos iOS/iPadOS inscritos

Puede elegir entre las opciones siguientes al programar las actualizaciones del sistema operativo para dispositivos iOS/iPadOS. Estas opciones se aplican a los dispositivos que usaron los tipos de inscripción Apple Business Manager o Apple School Manager.

- Actualización en la siguiente inserción
- Actualización durante la hora programada
- Actualización fuera de la hora programada

En las dos últimas opciones, puede crear varias ventanas de tiempo.

Para ver las nuevas opciones, vaya a MEM > **Dispositivos** > **iOS** > **Directivas de actualización para iOS/iPadOS** > **Crear perfil**.

Elección de las actualizaciones de iOS/iPadOS que se van a insertar en los dispositivos inscritos

Puede elegir una actualización específica de iOS/iPadOS (excepto para la más reciente) para insertarla en los dispositivos inscritos mediante Apple Business Manager o Apple School Manager. Estos dispositivos deben tener una directiva de configuración de dispositivos establecida para retrasar la visibilidad de las actualizaciones de software durante un número determinado de días. Para ver esta característica, vaya a MEM > **Dispositivos** > **iOS** > **Directivas de actualización para iOS/iPadOS** > **Crear perfil**.

Las exportaciones de la lista Todos los dispositivos ahora en formato CSV comprimido

Ahora las exportaciones de la página **Dispositivos** > **Todos los dispositivos** están en formato CSV comprimido.

Finalización del soporte extendido de Windows 7

El 14 de enero de 2020 finalizó el soporte extendido de Windows 7. En Intune ha quedado en desuso el soporte para los dispositivos que ejecutan Windows 7 al mismo tiempo. La asistencia técnica y las actualizaciones automáticas que ayudan a proteger su equipo ya no están disponibles. Se debe actualizar a Windows 10. Para más información, vea la entrada de blog sobre el plan de cambios.

Seguridad de dispositivos

Mejora de la experiencia de informes de Intune

Intune ahora proporciona una experiencia de informes mejorada, con nuevos tipos de informes, una mejor organización de informes, vistas más centradas y una funcionalidad de informes más eficiente, así como datos más coherentes y precisos. La experiencia de informes pasará de la versión preliminar pública a GA (disponibilidad general). Además, la versión de GA proporcionará compatibilidad para la localización, correcciones de errores, mejoras de diseño y datos de cumplimiento de dispositivos agregados en los mosaicos del Centro de administración de Microsoft Endpoint Manager .

Los nuevos tipos de informe se centran en la información siguiente:

- **Operativo**: proporciona registros nuevos con un enfoque de estado negativo.
- **Organizativo**: proporciona un resumen más amplio del estado general.
- **Histórico**: proporciona patrones y tendencias a lo largo de un período de tiempo.
- **Especialista**: le permite usar datos sin procesar para crear sus propios informes personalizados.

El primer conjunto de informes nuevos se centra en el cumplimiento de los dispositivos. Para obtener más información, vea Blog:marco de creación de informes de Microsoft Intune e Informes de Intune.

Consolidación de la ubicación de las líneas de base de seguridad en la interfaz de usuario

Se han consolidado las rutas de acceso para encontrar líneas de base de seguridad en el Centro de administración del Administrador de puntos de conexión de Microsoft mediante la eliminación de *Líneas de base de seguridad* de varias ubicaciones de la interfaz de usuario. Para buscar líneas de base de seguridad, ahora se usa la ruta de acceso siguiente: **Seguridad de los puntos de conexión** > **Líneas de base de seguridad**.

Compatibilidad ampliada con certificados PKCS importados

Se ha ampliado la compatibilidad con el uso de certificados PKCS importados para admitir *dispositivos Android Enterprise totalmente administrados*. Por lo general, la importación de certificados PFX se usa para escenarios de cifrado S/MIME, donde los certificados de cifrado de un usuario son necesarios en todos sus dispositivos para que se pueda realizar el descifrado del correo electrónico.

Las siguientes plataformas admiten la importación de certificados PFX:

- Android: Administrador de dispositivos
- Android Enterprise: Totalmente administrado
- Android Enterprise: Perfil de trabajo
- iOS
- Mac
- Windows 10

Visualización de la configuración de seguridad de los puntos de conexión para dispositivos

Se ha actualizado el nombre de la opción en el Centro de administración del Administrador de puntos de conexión de Microsoft para ver las configuraciones de seguridad de los puntos de conexión que se aplican a un dispositivo específico. Se ha cambiado el nombre de esta opción por **Configuración de seguridad de los puntos de conexión** porque muestra las líneas base de seguridad aplicables y las directivas adicionales creadas fuera de las líneas de base de seguridad. Esta opción antes se denominaba *Líneas de base de seguridad*.

Control de acceso basado en roles.

Próximos cambios en la interfaz de usuario de roles de Intune

La interfaz de usuario del Centro de administración de Microsoft Endpoint Manager > **Administración de inquilinos** > **Roles** se ha mejorado con un diseño más sencillo e intuitivo. Esta experiencia proporciona la misma configuración y los mismos detalles que se usan ahora, pero la nueva experiencia emplea un proceso similar a un asistente.

Enero de 2020

Administración de aplicaciones

Compatibilidad de Intune con el canal de implementación adicional de Microsoft Edge versión 77 para macOS

Microsoft Intune ahora admite el canal de implementación **estable** para la aplicación Microsoft Edge para macOS. El canal **estable** es el canal recomendado para la implementación de Microsoft Edge en general en entornos empresariales. Se actualiza cada seis semanas y cada versión incorpora mejoras del canal **beta**. Además de canales **estable** y **beta**, Intune admite un canal de **desarrollo**. La versión preliminar pública ofrece los canales estable y de desarrollo para la versión 77 y posteriores de Microsoft Edge para macOS. Las actualizaciones automáticas del explorador están activadas de forma predeterminada. Para obtener más información, consulte Adición de Microsoft Edge a dispositivos macOS con Microsoft Intune.

Retirada de Intune Managed Browser

Se va a retirar Intune Managed Browser. Use Microsoft Edge para la experiencia de explorador de Intune protegida.

Cambio en la experiencia del usuario al agregar aplicaciones a Intune

Verá una nueva experiencia de usuario al agregar aplicaciones a través de Intune. Esta experiencia proporciona la misma configuración y los mismos detalles que ha usado anteriormente, pero la nueva experiencia emplea un proceso similar a un asistente antes de agregar una aplicación a Intune. Esta nueva experiencia también proporciona una página de revisión antes de agregar la aplicación. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Todas las aplicaciones** > **Agregar**. Para más información, vea Agregar aplicaciones a Microsoft Intune.

Requisito de reinicio de las aplicaciones Win32

Puede requerir que una aplicación Win 32 se reinicie después de una instalación correcta. Además, puede elegir el tiempo (el período de gracia) que transcurrirá antes de que se produzca el reinicio.

Cambio en la experiencia del usuario al configurar aplicaciones en Intune

Verá una nueva experiencia de usuario al crear directivas de configuración de aplicaciones en Intune. Esta experiencia proporciona la misma configuración y los mismos detalles que ha usado anteriormente, pero la nueva experiencia emplea un proceso similar a un asistente antes de agregar una directiva a Intune. En el Centro de administración de Microsoft Endpoint Manager, seleccione **Aplicaciones** > **Directivas de configuración de aplicaciones** > **Agregar**. Para obtener más información, vea Directivas de configuración de aplicaciones para Microsoft Intune.

Compatibilidad de Intune con el canal de implementación adicional de Microsoft Edge para Windows 10

Microsoft Intune ahora admite el canal de implementación adicional **estable** para la aplicación Microsoft Edge (versión 77 y posteriores) para Windows 10. El canal **estable** es el canal recomendado para la implementación de Microsoft Edge para Windows 10 en general en entornos empresariales. Este canal se actualiza cada seis semanas y cada versión incorpora mejoras del canal **beta**. Además de canales **estable** y **beta**, Intune admite un canal de **desarrollo**. Para obtener más información, vea Microsoft Edge para Windows 10 - Configuración de aplicaciones.

Compatibilidad de S/MIME con Microsoft Outlook para iOS

Intune admite la entrega de certificados de cifrado y firma S/MIME que se pueden usar con Outlook para iOS en dispositivos iOS. Para más información, consulte Etiquetado de sensibilidad y protección en Outlook para iOS y Android.

Almacenamiento en caché del contenido de la aplicación Win32 mediante el servidor de caché con conexión de Microsoft

Puede instalar un servidor de caché con conexión de Microsoft en los puntos de distribución de Configuration Manager para almacenar en caché el contenido de la aplicación Win32 de Intune. Para más información, consulte Caché con conexión de Microsoft en Configuration Manager - Compatibilidad con aplicaciones Win32 de Intune.

Configuración del dispositivo

Mejor experiencia de interfaz de usuario al configurar la interfaz de usuario del conector local de Exchange ActiveSync

Hemos actualizado para experiencia para configurar el conector local de Exchange ActiveSync. La experiencia actualizada usa un solo panel para configurar, editar y resumir los detalles de los conectores locales.

Adición de configuración de proxy automática a perfiles de Wi-Fi para perfiles de trabajo de Android Enterprise

En los dispositivos de perfil de trabajo de Android Enterprise, puede crear perfiles de Wi-Fi. Al elegir el tipo Wi-Fi Enterprise, también puede especificar el tipo de protocolo de autenticación extensible (EAP) que se usa en la red Wi-Fi.

Ahora, al elegir el tipo de empresa, también puede especificar la configuración de proxy automática, incluida una dirección URL del servidor proxy, como `proxy.contoso.com`.

Para ver la configuración de Wi-Fi actual que puede establecer, vaya a Incorporación de la configuración de Wi-Fi en Microsoft Intune para dispositivos que ejecutan Android Enterprise y el Quiosco de Android.

Se aplica a:

- Perfil de trabajo de Android Enterprise

Inscripción de dispositivos

Bloqueo de las inscripciones de Android por el fabricante del dispositivo

Puede bloquear la inscripción de dispositivos en función del fabricante del dispositivo. Esta característica se aplica al administrador de dispositivos Android y los dispositivos de perfil de trabajo de Android Enterprise. Para ver las restricciones de inscripción, vaya al Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **Restricciones de inscripción**.

Mejoras en la interfaz de usuario para Crear un perfil de tipo de inscripción en iOS/iPadOS

Para la inscripción de usuarios de iOS/iPadOS, se ha simplificado la página **Crear un perfil de tipo de inscripción Configuración** para mejorar el proceso de elección del **Tipo de inscripción** manteniendo la misma funcionalidad. Para ver la interfaz de usuario nueva, vaya a la página Centro de administración de Microsoft Endpoint Manager > **Dispositivos** > **iOS** > **Inscripción de iOS** > **Tipos de inscripción** > **Crear perfil** > **Configuración**. Para obtener más información, consulte Creación de un perfil de inscripción de usuario en Intune.

Administración de dispositivos

Nueva información en los detalles del dispositivo

La siguiente información está ahora en la página de **información general** para dispositivos:

- Capacidad de memoria (cantidad de memoria física en el dispositivo)
- Capacidad de almacenamiento (cantidad de almacenamiento físico en el dispositivo)
- Arquitectura de CPU

Cambio de nombre de la acción remota Omisión del bloqueo de activación de iOS a Deshabilitación del bloqueo de activación

Se ha cambiado el nombre de la acción remota **Omisión del bloqueo de activación** a **Deshabilitación del bloqueo de activación**. Para obtener más información, consulte Deshabilitación del bloqueo de activación de iOS con Intune.

Compatibilidad con la implementación de actualizaciones de características de Windows 10 para dispositivos AutoPilot

Intune ahora admite dispositivos registrados con AutoPilot mediante implementaciones de actualizaciones de características de Windows 10.

Las directivas de actualización de características de Windows 10 no se pueden aplicar durante la configuración rápida (OOBE) de Autopilot y solo se aplican en el primer análisis de Windows Update una vez que el dispositivo haya finalizado el aprovisionamiento (que suele ser un día).

Supervisión y solución de problemas

Informes de implementación de Windows Autopilot (versión preliminar)

Un nuevo informe detalla cada dispositivo implementado mediante Windows Autopilot. Para más información,

vea Informe de implementaciones de Autopilot.

Control de acceso basado en roles.

Nuevo rol de Administrador de seguridad de los puntos de conexión integrado en Intune

Hay un nuevo rol integrado de Intune disponible: el administrador de seguridad de los puntos de conexión. Este nuevo rol concede a los administradores acceso completo al nodo del administrador de puntos de conexión en Intune y acceso de solo lectura a otras áreas. El rol es una expansión del rol "Administrador de seguridad" de Azure AD. Si actualmente solo tiene administradores globales como roles, no es necesario realizar ningún cambio. Si usa roles y desea la granularidad que proporciona el Administrador de seguridad de puntos de conexión, asigne ese rol cuando esté disponible. Para más información acerca de roles integrados, vea Control de acceso basado en rol.

Los perfiles de plantillas administrativas de Windows 10 (ADMX) ahora admiten etiquetas de ámbito

Ahora puede asignar etiquetas de ámbito a los perfiles de plantilla administrativa (ADMX). Para ello, vaya a **Intune** > **Dispositivos** > **Perfiles de configuración** > elija un perfil de plantillas administrativas en la lista > **Propiedades** > **Etiquetas de ámbito**. Para más información sobre las etiquetas de ámbito, vea Asignar etiquetas de ámbito a otros objetos.

Diciembre de 2019

Administración de aplicaciones

Recuperación de una clave de recuperación personal desde dispositivos macOS con cifrado de MEM

Los usuarios finales pueden recuperar su clave de recuperación personal (clave de FileVault) mediante la aplicación Portal de empresa de iOS. El dispositivo que tiene la clave de recuperación personal se debe inscribir en Intune y cifrar con FileVault a través de Intune. Con la aplicación Portal de empresa de iOS, un usuario final puede recuperar su clave de recuperación personal en su dispositivo macOS cifrado haciendo clic en **Obtener clave de recuperación**. También puede recuperar la clave de recuperación en Intune si selecciona **Dispositivos** > *el dispositivos macOS cifrado e inscrito* > **Obtener clave de recuperación**. Para más información sobre FileVault, consulte Cifrado de FileVault para macOS.

Aplicaciones de VPP con licencia de usuario de iOS y iPadOS

En el caso de los dispositivos iOS y iPadOS inscritos por el usuario, los usuarios finales ya no verán las aplicaciones de VPP con licencia de dispositivo recién creadas implementadas como disponibles. Sin embargo, los usuarios finales seguirán viendo todas las aplicaciones de VPP con licencia de usuario en el Portal de empresa. Para más información relacionada con las aplicaciones VPP, vea Administración de aplicaciones de iOS y macOS compradas a través del Programa de Compras por Volumen de Apple con Microsoft Intune.

Aviso: La compatibilidad de Windows 10 1703 (RS2) finalizará

A partir del 9 de octubre de 2018, finalizó la compatibilidad de Windows 10 1703 (RS2) con la plataforma de Microsoft para las ediciones Home, Pro y Pro for Workstations. En el caso de las ediciones Windows 10 Enterprise y Education, la compatibilidad de Windows 10 1703 (RS2) con la plataforma finalizó el 8 de octubre de 2019. A partir del 26 de diciembre de 2019, actualizaremos la versión mínima de la aplicación Portal de empresa de Windows a Windows 10 1709 (RS3). Los equipos que ejecutan versiones anteriores a 1709 dejarán de recibir las versiones actualizadas de la aplicación desde Microsoft Store. Comunicamos anteriormente este cambio a los clientes que administran versiones anteriores de Windows 10 a través del centro de mensajes. Para más información, consulte Hoja de datos del ciclo de vida de Windows.

Administración de aplicaciones

Migración a Microsoft Edge para escenarios de exploración administrados

A medida que se acerca la retirada de Intune Managed Browser, se han realizado cambios en las directivas de protección de aplicaciones para simplificar los pasos necesarios para trasladar a los usuarios a Edge. Se han actualizado las opciones de la configuración de directiva de protección de aplicaciones **Restringir la transferencia de contenido web con otras aplicaciones** para que sea una de las siguientes:

- Cualquier aplicación

- Intune Managed Browser
- Microsoft Edge
- Explorador no administrado

Al seleccionar **Microsoft Edge**, los usuarios finales verán que la mensajería de acceso condicional les notifica que Microsoft Edge es necesario para escenarios de exploración administrados. Se les pedirá que descarguen e inicien sesión en Microsoft Edge con sus cuentas de Azure AD, si todavía no lo han hecho. Este será el equivalente a tener como destino las aplicaciones habilitadas para MAM con la configuración de la aplicación `com.microsoft.intune.useEdge` establecida en **true**. Las directivas de protección de aplicaciones existentes en las que se usaba la opción **Exploradores administrados por directivas** ahora tendrán **Intune Managed Browser** seleccionado y no verá ningún cambio de comportamiento. Esto significa que los usuarios verán mensajes para usar Microsoft Edge si ha establecido la opción de configuración de la aplicación **useEdge** en **true**. Animamos a todos los clientes que aprovechan los escenarios de exploración administrados para actualizar sus directivas de protección de aplicaciones con **Restringir la transferencia de contenido web con otras aplicaciones** para asegurarse de que los usuarios vean las instrucciones adecuadas para realizar la transición a Microsoft Edge, con independencia de la aplicación desde la que inicien los vínculos.

Configuración del contenido de las notificaciones de una aplicación para las cuentas de organización

Las directivas de protección de aplicaciones (APP) de Intune en dispositivos iOS y Android permiten controlar el contenido de las notificaciones de una aplicación para las cuentas de organización. Puede seleccionar una opción (permitir, bloquear datos de la organización o bloqueado) para especificar cómo se muestran las notificaciones de las cuentas de la organización para la aplicación seleccionada. Esta característica requiere compatibilidad de las aplicaciones y puede que no esté disponible para todas las aplicaciones habilitadas para la aplicación. Outlook para iOS versión 4.15.0 (o posterior) y Outlook para Android 4.83.0 (o posterior) serán compatibles con esta configuración. La configuración está disponible en la consola, pero la funcionalidad entrará en vigor después del 16 de diciembre de 2019. Consulte ¿Qué son las directivas de protección de aplicaciones? para obtener más información sobre APP.

Actualización de los iconos de las aplicaciones de Microsoft

Se han actualizado los iconos que se usan para las aplicaciones de Microsoft en el panel de la aplicación objetivo para las directivas de protección de aplicaciones y las directivas de configuración de aplicaciones.

Requerir el uso de teclados aprobados en Android

Como parte de una directiva de protección de aplicaciones, puede especificar la configuración **Teclados aprobados** para administrar los teclados Android que se pueden usar con aplicaciones Android administradas. Cuando un usuario abra la aplicación administrada y aún no use un teclado aprobado para esa aplicación, se le pedirá que cambie a uno de los teclados aprobados que ya están instalados en el dispositivo. Si es necesario, verá un vínculo para descargar un teclado aprobado en Google Play Store, que puede instalar y configurar. El usuario solo puede editar campos de texto en una aplicación administrada cuando su teclado activo no sea uno de los teclados aprobados.

Configuración del dispositivo

Actualizaciones de Plantillas administrativas para dispositivos Windows 10

Puede usar plantillas ADMX en Microsoft Intune para controlar y administrar la configuración de Microsoft Edge, Office y Windows. Las Plantillas administrativas en Intune realizaron estas actualizaciones en la configuración de las directivas:

- Se agregó compatibilidad con las versiones 78 y 79 de Microsoft Edge.
- Incluye los archivos ADMX del 11 de noviembre de 2019 en Archivos de Plantillas administrativas (ADMX/ADML) y la Herramienta de personalización de Office para Aplicaciones de Microsoft 365 para empresas, Office 2019 y Office 2016.

Para más información sobre las plantillas ADMX en Intune, consulte Usar plantillas de Windows 10 para configurar opciones de directiva de grupo en Microsoft Intune.

Se aplica a:

- Windows 10 y versiones posteriores

Experiencia de inicio de sesión único actualizada para aplicaciones y sitios web en dispositivos iOS, iPadOS y macOS

Intune agregó una configuración de inicio de sesión único (SSO) para dispositivos iOS, iPadOS y macOS. Ahora puede configurar las extensiones de aplicación de SSO de redireccionamiento escritas por su organización o por el proveedor de identidades. Use estas opciones para configurar una experiencia de inicio de sesión único sin problemas para aplicaciones y sitios web que usan métodos de autenticación modernos, como OAuth y SAML2.

Estas nuevas opciones expanden la configuración anterior de las extensiones de aplicación SSO y la extensión Kerberos integrada de Apple (**Dispositivos** > **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS/iPadOS** o **macOS** para el tipo de plataforma > **Características del dispositivo** para el tipo de perfil).

Para ver todas las opciones de la extensión de aplicación SSO que puede configurar, vaya a SSO en iOS y SSO en macOS.

Se aplica a:

- iOS/iPadOS
- macOS

Actualizamos dos opciones de restricción de dispositivos para dispositivos iOS e iPados para corregir su comportamiento

En los dispositivos iOS, puede crear los perfiles de restricción de dispositivos **Permitir actualizaciones móviles de PKI** y **Bloqueo del modo restringido de USB** (**Dispositivos** > **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS/iPadOS** para la plataforma > **Restricciones de dispositivos** para el tipo de perfil). Antes de esta versión, la configuración de la interfaz de usuario y las descripciones de las siguientes opciones no eran correctas, algo que ahora se corrigió. A partir de esta versión, el comportamiento de la configuración es el siguiente:

Bloquear actualizaciones móviles de PKI: **Bloquear** impide que los usuarios reciban actualizaciones de software, a menos que el dispositivo esté conectado a un equipo. **No configurado** (valor predeterminado): permite que un dispositivo reciba actualizaciones de software sin estar conectado a un equipo.

- Anteriormente, esta configuración le permitía configurarla como: **Permitir**, que permite a los usuarios recibir actualizaciones de software sin tener que conectar los dispositivos a un equipo. **Permitir accesorios USB con el dispositivo bloqueado**: **Permitir** permite que los accesorios USB intercambien datos con un dispositivo que ha estado bloqueado durante más de una hora. **No configurado** (valor predeterminado) no actualiza el modo restringido de USB en el dispositivo y los accesorios USB no podrán transferir datos del dispositivo si están bloqueados durante más de una hora.
- Anteriormente, esta configuración le permitía configurarla como: **Bloquear** para deshabilitar el modo restringido de USB en los dispositivos supervisados.

Para más información sobre los valores que puede configurar, consulte Configuración de dispositivos iOS e iPadOS para permitir o restringir características mediante Intune.

Esta característica se aplica a:

- OS/iPadOS

Impedir que los usuarios configuren las credenciales de certificado en el almacén de claves administrado en dispositivos propietarios de dispositivos Android Enterprise

En dispositivos propietarios de dispositivos Android Enterprise, puede establecer una nueva configuración que impide que los usuarios configuren sus credenciales de certificado en el almacén de claves administrado (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** para la plataforma > **Solo el propietario del dispositivo** > **Restricciones de dispositivos** para el tipo de perfil > **Users + Accounts** [Usuarios y cuentas]).

Nueva licencia de administración conjunta de Microsoft Endpoint Configuration Manager

Los clientes de Configuration Manager con Software Assurance pueden obtener la administración conjunta de Intune para equipos con Windows 10 sin tener que comprar una licencia de Intune adicional para la administración conjunta. Los clientes ya no necesitan asignar licencias de Intune y EMS individuales a los usuarios finales para la administración conjunta de Windows 10.

- Los dispositivos administrados por Configuration Manager e inscritos en la administración conjunta tienen casi los mismos derechos que los equipos administrados por MDM de Intune independiente. Pero después de restablecerlos, no se pueden volver a aprovisionar con Autopilot.
- Los dispositivos Windows 10 inscritos en Intune mediante otros medios requieren licencias completas de Intune.
- Los dispositivos de otras plataformas siguen requiriendo licencias de Intune completas.

Para más información, vea Términos de Licencia.

Administración de dispositivos

La acción de borrado protegido ya está disponible

Ahora tiene la opción de usar la acción Borrar dispositivo para realizar el borrado protegido de un dispositivo. Los borradores protegidos equivalen a los borrados estándar, salvo que no se pueden eludir apagando el dispositivo. Un borrado protegido seguirá intentando restablecer el dispositivo hasta que se complete de forma correcta. En algunas configuraciones, esta acción puede hacer que el dispositivo no se pueda reiniciar. Para más información, consulte Retirada o borrado de los dispositivos.

Dirección MAC de Ethernet de un dispositivo agregada a la página Información general del dispositivo

Ahora puede ver la dirección MAC de Ethernet de un dispositivo en la página de detalles del dispositivo (**Dispositivos** > **Todos los dispositivos** > elija un dispositivo > **Información general**).

Seguridad de dispositivos

Experiencia mejorada en un dispositivo compartido cuando se habilitan las directivas de acceso condicional basadas en el dispositivo

Mejoramos la experiencia en un dispositivo compartido con varios usuarios a los que se les aplica la directiva de acceso condicional basada en los dispositivos mediante la comprobación de la evaluación de cumplimiento más reciente para el usuario al aplicar la directiva. Para más información, consulte estos artículos de información general:

- Información general de Azure sobre el Acceso condicional
- Información general sobre el cumplimiento de los dispositivos de Intune

Uso de perfiles de certificado PKCS para aprovisionar dispositivos con certificados

Ahora puede usar perfiles de certificado PKCS para emitir certificados a *dispositivos* que ejecuten Android for Work, iOS/iPadOS y Windows, cuando estén asociados a perfiles como los de Wi-Fi y VPN. Anteriormente, estas tres plataformas solo admitían certificados basados en el usuario, con la compatibilidad basada en dispositivos limitada a macOS.

> **NOTE**
> No se admiten los perfiles de certificado PKCS con perfiles Wi-FI. En su lugar, use perfiles de certificado SCEP cuando use un tipo EAP.

Para usar un certificado basado en dispositivos, al crear un perfil de certificado PKCS para las plataformas admitidas, seleccione **Configuración**. Ahora verá el valor de **Tipo de certificado**, que admite las opciones de dispositivo o usuario.

Supervisión y solución de problemas

Registros de auditoría centralizados

Una nueva experiencia de registros de auditoría centralizados ahora recopila los registros de auditoría de todas las categorías en una sola página. Puede filtrar los registros para obtener los datos que está buscando. Para ver los registros de auditoría, vaya a **Administración de inquilinos** > **Registros de auditoría**.

Información de etiqueta de ámbito incluida en los detalles de la actividad de registro de auditoría

Los detalles de la actividad de registro de auditoría ahora incluyen información de etiqueta de ámbito (para los objetos de Intune que admiten etiquetas de ámbito). Para más información sobre los registros de auditoría, consulte Uso de registros de auditoría para realizar un seguimiento de los eventos y supervisarlos.

Noviembre de 2019

Administración de aplicaciones

Actualización de la interfaz de usuario al borrar datos de la aplicación de forma selectiva

La interfaz de usuario para borrar selectivamente los datos de la aplicación en Intune se ha actualizado. Los cambios de la UI son:

- Una experiencia más sencilla, dado el uso de un formato de tipo asistente condensado dentro de un panel.
- Una actualización del flujo de creación para incluir asignaciones.
- Una página de resumen de todos los elementos establecidos al ver las propiedades, antes de crear una nueva directiva o al editar una propiedad. Además, al editar las propiedades, el resumen solo mostrará una lista de elementos de la categoría de propiedades que se están editando.

Para obtener más información, consulte Borrado solo de datos corporativos de aplicaciones administradas por Intune.

Compatibilidad con el teclado de terceros de iOS y iPadOS

En marzo de 2019, anunciamos el fin del la compatibilidad del parámetro de la directiva de protección de aplicaciones de iOS "Teclados de terceros". La característica está de vuelta en Intune con compatibilidad tanto con iOS como con iPadOS. Para habilitar esta configuración, visite la pestaña **Protección de datos** de una directiva de protección de aplicaciones iOS/iPadOS nueva o existente y busque la opción **Teclados de terceros** en **Transferencia de datos**.

El comportamiento de esta configuración de directiva difiere ligeramente de la implementación anterior. En las aplicaciones de varias identidades que usan la versión de SDK 12.0.16 y versiones posteriores que son el destino de directivas de protección de aplicaciones con esta opción configurada en **Bloquear**, los usuarios finales no podrán elegir los teclados de terceros en sus cuentas personales y de organización. Las aplicaciones que usan versiones de SDK 12.0.12 y anteriores seguirán mostrando el comportamiento documentado en la entrada de blog que lleva por título Problema conocido: Los teclados de terceros no se bloquean en iOS para cuentas personales.

Experiencia mejorada de inscripción de macOS en el Portal de empresa

La experiencia de inscripción del Portal de empresa para macOS cuenta con un proceso de inscripción más sencillo que es más coherente con la experiencia de inscripción en el Portal de empresa para iOS. Los usuarios del dispositivo ahora ven lo siguiente:

- Una interfaz de usuario más elegante.
- Una lista de comprobación de inscripción mejorada.
- Instrucciones más claras sobre cómo inscribir sus dispositivos.
- Mejores opciones de solución de problemas.

Aplicaciones web iniciadas desde la aplicación Portal de empresa de Windows

Los usuarios finales ahora pueden iniciar aplicaciones web directamente desde la aplicación Portal de empresa de Windows. Los usuarios finales pueden seleccionar la aplicación web y, a continuación, elegir la opción **Abrir en el explorador**. La dirección URL web publicada se abre directamente en un explorador web. Esta funcionalidad se implementará durante la próxima semana. Para más información sobre las aplicaciones web,

consulteAgregar aplicaciones web a Microsoft Intune.

Nueva columna de tipo de asignación en el Portal de empresa para Windows 10

Se ha cambiado el nombre de la columna Portal de empresa > **Aplicaciones instaladas** > **Tipo de asignación** a **Requerida por la organización**. En esa columna, los usuarios verán un valor de **Sí** o **No** para indicar si una aplicación es obligatoria o es opcional para su organización. La razón de estos cambios es la confusión que despertaba en los usuarios de los dispositivos el concepto de aplicaciones disponibles. Los usuarios pueden obtener más información sobre cómo instalar aplicaciones en el Portal de empresa en Instalar y compartir aplicaciones en el dispositivo. Para obtener más información sobre cómo configurar la aplicación Portal de empresa para sus usuarios, vea Configuración de la aplicación Portal de empresa de Microsoft Intune.

Configuración del dispositivo

Requerimiento de administración de Jamf a grupos de usuarios de macOS

Puede dirigirse a grupos específicos de usuarios cuyos dispositivos macOS serán administrados por Jamf. Esto le permite aplicar la integración de cumplimiento de Jamf a un subconjunto de dispositivos macOS mientras que otros dispositivos se administran mediante Intune. Si ya usa la integración de Jamf, la integración se destinará a todos los usuarios de manera predeterminada.

Nueva configuración de Exchange ActiveSync al crear un perfil de configuración de dispositivo de correo electrónico en dispositivos iOS

En dispositivos iOS/iPadOS, puede configurar la conectividad del correo electrónico en un perfil de configuración de dispositivos (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **iOS/iPadOS** como plataforma > **Correo electrónico** para tipo de perfil).

Hay nuevas opciones de configuración de Exchange ActiveSync disponibles, entre las que se incluyen:

- **Datos de Exchange para sincronizar**: elija los servicios de Exchange que se sincronizarán (o cuya sincronización se bloqueará) con el calendario, los contactos, los recordatorios, las notas y el correo electrónico.
- **Permitir a los usuarios cambiar la configuración de sincronización**: permita (o impida) a los usuarios cambiar la configuración de sincronización para estos servicios en sus dispositivos.

Para obtener más información sobre esta configuración, vaya a Incorporación de la configuración de correo electrónico para dispositivos iOS en Microsoft Intune.

Se aplica a:

- iOS 13.0 y versiones más recientes
- IPadOS 13.0 y versiones más recientes

Evitación de que los usuarios agreguen cuentas personales de Google a dispositivos Android Enterprise dedicados y totalmente administrados

En los dispositivos Android Enterprise dedicados y totalmente administrados, hay una nueva opción que impide que los usuarios creen cuentas de Google personales (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **Android Enterprise** para plataforma > **Solo el propietario del dispositivo** > **Restricciones de dispositivos** para tipo de perfil > **configuración de Usuarios y cuentas** > **Cuentas personales de Google**).

Para ver los valores que puede configurar, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

Se aplica a:

- Dispositivos totalmente administrados de Android Enterprise
- Dispositivos Android Enterprise dedicados

Eliminación del parámetro de registro del servidor para los comandos de Siri en el perfil de restricciones de dispositivos de iOS/iPadOS

En dispositivos iOS y iPadOS, el parámetro **Registro del servidor para los comandos de Siri** se ha quitado

de la consola de administración de Microsoft Endpoint Manager (**Configuración de dispositivo** > **Perfiles** > **Crear perfil** > **iOS/iPadOS** para plataforma > **Restricciones de dispositivos** para tipo de perfil > **Aplicaciones integradas**).

Esta configuración no tiene ningún efecto en los dispositivos. Para quitar el parámetro de los perfiles existentes, abra el perfil, realice cualquier cambio y, a continuación, guarde el perfil. El perfil se actualiza y la configuración se elimina de los dispositivos.

Para ver todos los valores que puede configurar, vea Configuración de dispositivos iOS y iPadOS para permitir o restringir características mediante Intune.

Se aplica a:

- iOS/iPadOS

Actualizaciones de características de Windows 10 (versión preliminar pública)

Ahora puede implementar actualizaciones de características de Windows 10 en dispositivos Windows 10. Las actualizaciones de características de Windows 10 son una nueva directiva de actualización de software que establece la versión de Windows 10 que desea que se instale y permanezca en los dispositivos. Puede usar este nuevo tipo de directiva junto con los anillos de actualización de Windows 10 existentes.

Los dispositivos que reciben la directiva de actualizaciones de características de Windows 10 instalarán la versión especificada de Windows y, a continuación, permanecerán con esa versión hasta que se edite o se quite la directiva. Los dispositivos que ejecutan una versión posterior de Windows permanecen en su versión actual. Los dispositivos que se encuentran en una versión específica de Windows pueden seguir instalando actualizaciones de calidad y seguridad para esa versión desde los anillos de actualización de Windows 10.

Este nuevo tipo de directiva comienza a implementarse en los inquilinos esta semana. Si esta directiva todavía no está disponible para el inquilino, lo estará pronto.

Adición y cambio de información clave en archivos PLIST para aplicaciones macOS

En los dispositivos macOS, ahora puede crear un perfil de configuración de dispositivos que cargue un archivo de lista de propiedades (. plist) asociado a una aplicación o el dispositivo (**Dispositivos** > **Perfiles de configuración** > **Crear perfil** > **macOS** para la plataforma > **Archivo de preferencias** para el tipo de perfil).

Solo algunas aplicaciones admiten preferencias administradas, y es posible que estas aplicaciones no le permitan administrar toda la configuración. Asegúrese de cargar un archivo de lista de propiedades que configure los valores del canal del dispositivo, no la configuración del canal del usuario.

Para obtener más información sobre esta característica, consulte Adición de un archivo de lista de propiedades a dispositivos macOS mediante Microsoft Intune.

Se aplica a:

- dispositivos macOS con 10.7 y versiones más recientes

Administración de dispositivos

Edición del valor de nombre de dispositivo para dispositivos Autopilot

Puede editar el valor del nombre de dispositivo para los dispositivos Autopilot unidos a Azure AD. Para obtener más información, consulte Edición de atributos de dispositivo Autopilot.

Edición del valor de etiqueta de grupo para dispositivos Autopilot

Puede editar el valor Etiqueta de grupo para dispositivos Autopilot. Para obtener más información, consulte Edición de atributos de dispositivo Autopilot.

Supervisión y solución de problemas

Experiencia de soporte técnico actualizada

A partir de hoy, se está implantando en los inquilinos una experiencia actualizada y simplificada en la consola

para obtener ayuda y soporte técnico para Intune. Si esta experiencia todavía no está disponible para usted, lo estará pronto.

Se ha mejorado la búsqueda en la consola, los comentarios de incidencias comunes y el flujo de trabajo que se usa para ponerse en contacto con el servicio de soporte técnico. Al abrir una incidencia de soporte técnico, verá estimaciones en tiempo real de cuándo pueda esperar una devolución de llamada o una respuesta por correo electrónico; los clientes de soporte técnico Premier y Unified pueden especificar fácilmente la gravedad de su incidencia con el fin de obtener soporte técnico más rápido.

Mejora de la experiencia de informes de Intune (versión preliminar pública)

Intune ahora proporciona una experiencia de informes mejorada, con nuevos tipos de informes, una mejor organización de informes, vistas más centradas y una funcionalidad de informes más eficiente, así como datos más coherentes y precisos. Los nuevos tipos de informe se centran en lo siguientes aspectos:

- **Operativo**: proporciona registros nuevos con un enfoque de estado negativo.
- **Organizativo**: proporciona un resumen más amplio del estado general.
- **Histórico**: proporciona patrones y tendencias a lo largo de un período de tiempo.
- **Especialista**: le permite usar datos sin procesar para crear sus propios informes personalizados.

El primer conjunto de informes nuevos se centra en el cumplimiento de los dispositivos. Para obtener más información, vea Blog:marco de creación de informes de Microsoft Intune e Informes de Intune.

Control de acceso basado en roles.

Duplicación de roles personalizados o integrados

Ahora puede copiar tanto roles integrados como roles personalizados. Para obtener más información, vea Copia de un rol.

Nuevos permisos para el rol de administrador escolar

Se han agregado dos nuevos permisos, **Asignar perfil** y **Sincronizar dispositivo**, al rol de administrador escolar > **Permisos** > **Programas de inscripción**. El permiso de sincronizar perfil permite a los administradores de grupos sincronizar dispositivos Windows Autopilot. El permiso de asignar perfil les permite eliminar perfiles de inscripción de Apple iniciados por el usuario. También les concede permiso para administrar las asignaciones de dispositivos Autopilot y las asignaciones del perfil de implementación de Autopilot. Para obtener una lista de todos los permisos de administrador de grupo y administrador escolar, consulte Asignación de un grupo de administración.

Seguridad

Rotación de clave de BitLocker

Puede usar una acción de dispositivo de Intune para rotar de forma remota las claves de recuperación de BitLocker para dispositivos administrados que ejecutan la versión 1909 o posterior de Windows. Para que se puedan rotar las claves de recuperación, los dispositivos deben configurarse para admitir la rotación de claves de recuperación.

Actualizaciones en la inscripción de dispositivos dedicada para admitir la implementación de certificados de dispositivos SCEP

Intune ahora admite la implementación de certificados de dispositivos SCEP en dispositivos Android Enterprise dedicados para permitir el acceso basado en certificados a los perfiles de Wi-Fi. La aplicación Microsoft Intune debe estar presente en el dispositivo para que funcione la implementación. Como resultado, hemos actualizado la experiencia de inscripción para dispositivos Android Enterprise dedicados. Las nuevas inscripciones siguen empezando de la misma manera (con QR, NFC, sin interacción o con identificador de dispositivo) pero ahora tienen un paso que requiere que los usuarios instalen la aplicación Intune. Los dispositivos existentes comenzarán a instalar la aplicación automáticamente de manera gradual.

Registros de auditoría de Intune para colaboración de negocio a negocio

La colaboración de negocio a negocio (B2B) le permite compartir de forma segura las aplicaciones y los servicios de la empresa con usuarios invitados de cualquier otra organización, manteniendo al mismo tiempo el control sobre sus propios datos corporativos. Intune ahora admite registros de auditoría para usuarios invitados

de B2B. Por ejemplo, cuando los usuarios invitados realizan cambios, Intune podrá capturar estos datos a través de registros de auditoría. Para obtener más información, consulte ¿Qué es el acceso de usuarios invitados en Azure Active Directory B2B?

Las líneas de base de seguridad se admiten en Microsoft Azure Government

Las instancias de Intune que se hospedan en *Microsoft Azure Government* ahora pueden usar líneas base de seguridad para ayudarle a proteger sus usuarios y dispositivos.

Octubre de 2019

Administración de aplicaciones

Diseño de la lista de comprobación mejorado en la aplicación Portal de empresa para Android

La lista de comprobación de configuración de la aplicación Portal de empresa para Android se ha actualizado con un diseño ligero y nuevos iconos. Los cambios se alinean con las actualizaciones recientes realizadas en la aplicación Portal de empresa para iOS. Para una comparación en paralelo de los cambios, consulte Novedades de la interfaz de usuario de aplicaciones. Para ver los pasos de inscripción actualizados, consulte Inscripción con el perfil de trabajo Android e Inscripción de su dispositivo Android.

Aplicaciones Win32 en dispositivos de modo Windows 10 S

Puede instalar y ejecutar aplicaciones Win32 en dispositivos administrados en modo Windows 10 S. Para ello, puede crear una o varias directivas complementarias para el modo S mediante las herramientas de PowerShell de Control de aplicaciones de Windows Defender (WDAC). Firme las directivas complementarias con el portal de firma de Device Guard y, después, cargue y distribuya las directivas mediante Intune. En Intune, encontrará esta funcionalidad seleccionando **Aplicaciones cliente** > **Directivas complementarias de Windows 10 S**. Para más información, consulte Habilitación de aplicaciones Win32 en modo S.

Establecimiento de la disponibilidad de las aplicaciones Win32 basada en una fecha y hora

Como administrador, puede configurar la hora de inicio y la hora de la fecha límite para una aplicación Win32 necesaria. A la hora de inicio, la extensión de administración de Intune iniciará la descarga del contenido de la aplicación y lo almacenará en caché. La aplicación se instalará a la hora de la fecha límite. Para las aplicaciones disponibles, la hora de inicio determinará cuando la aplicación está visible en Portal de empresa. Para más información, consulte Administración de aplicaciones Win32 de Intune.

Reinicio necesario del dispositivo basado en el período de gracia después de la instalación de la aplicación Win32

Puede requerir que un dispositivo se reinicie después de que una aplicación Win32 se instale correctamente. Para más información, vea Administración de aplicaciones Win32.

Modo oscuro para el Portal de empresa de iOS

El modo oscuro está disponible para el Portal de empresa de iOS. Los usuarios pueden descargar aplicaciones de empresa, administrar sus dispositivos y obtener soporte técnico de TI en la combinación de colores de su elección en función de la configuración del dispositivo. El Portal de empresa de iOS hará coincidir automáticamente la configuración del dispositivo del usuario final con el modo oscuro o claro. Para más información, consulte Introducción al modo oscuro en el Portal de empresa de Microsoft Intune para iOS. Para más información sobre el Portal de empresa de iOS, consulte Configuración de la aplicación Portal de empresa de Microsoft Intune.

Versión mínima de la aplicación aplicada por el Portal de empresa de Android

Con la opción **Min Company Portal version** (Versión mínima del Portal de empresa) de una directiva de protección de aplicaciones, puede especificar una versión definida mínima determinada del Portal de empresa que se aplique a un dispositivos de usuario final. Esta configuración de inicio condicional permite **bloquear el acceso**, **borrar datos** o **advertir** como posibles acciones cuando no se cumple el valor. Los posibles formatos de este valor siguen el patrón *[Principal].[Secundaria]* , *[Principal].[Secundaria].[Compilación]* o *[Principal].[Secundaria].[Compilación].[Revisión]* .

La opción **Min Company Portal version** (Versión mínima del Portal de empresa), si está configurada, afectará a cualquier usuario final que obtenga la versión 5.0.4560.0 del Portal de empresa y todas sus versiones futuras.

Esta configuración no afectará a los usuarios que usen una versión del Portal de empresa anterior a la versión con la que se publique esta característica. Los usuarios finales que usen actualizaciones automáticas de aplicaciones en su dispositivo probablemente no verán ningún cuadro de diálogo de esta característica, dado que es posible que estén en la versión más reciente del Portal de empresa. Esta opción es solo para Android con la protección de aplicaciones para dispositivos inscritos y no inscritos. Para más información, consulte Configuración de directivas de protección de aplicaciones de Android: inicio condicional.

Incorporación de aplicaciones de Mobile Threat Defense a dispositivos no inscritos

Puede crear una directiva de protección de aplicaciones de Intune que puede bloquear o borrar de forma selectiva los datos corporativos de los usuarios en función del estado de un dispositivo. El estado del dispositivo se determina mediante la solución Mobile Threat Defense (MTD) seleccionada. Esta funcionalidad existe en la actualidad con los dispositivos inscritos en Intune como una configuración de cumplimiento de dispositivos. Con esta nueva característica, ampliamos la detección de amenazas de un proveedor de Mobile Threat Defense para que funcione en dispositivos no inscritos. En Android, esta característica requiere la versión más reciente de Portal de empresa. En iOS, esta característica se podrá usar cuando las aplicaciones integren el SDK de Intune más reciente (v 12.0.15 +). Se actualizará el tema Novedades cuando la primera aplicación adopte el SDK de Intune más reciente. El resto de aplicaciones irán estando disponibles de manera gradual. Para más información, consulte Creación de una directiva de protección de aplicaciones de Mobile Threat Defense con Intune.

Notificación de aplicaciones de Google Play disponibles para perfiles de trabajo de Android

En las instalaciones de aplicaciones disponibles en dispositivos dedicados, totalmente administrados y de perfil de trabajo de Android Enterprise, puede ver el estado de instalación de la aplicación, así como la versión instalada de aplicaciones administradas de Google Play. Para obtener más información, vea Supervisión de las directivas de protección de aplicaciones, Administrar dispositivos de perfil de trabajo Android con Intune y Tipo de aplicación de Google Play administrado.

Microsoft Edge versión 77 y posteriores para Windows 10 y macOS (versión preliminar pública)

Microsoft Edge versión 77 y posteriores ya está disponible para implementarlo en equipos que ejecutan Windows 10 y macOS.

La versión preliminar pública ofrece los canales **Dev** y **Beta** para Windows 10 y un canal **Beta** para macOS. La implementación solo está en inglés (EN), pero los usuarios finales pueden cambiar el idioma para mostrar en el explorador desde **Configuración** > **Idiomas**. Microsoft Edge es una aplicación Win32 que se instala en el contexto del sistema y en arquitecturas similares (aplicación x86 en sistemas operativos x86 y aplicación x64 en sistemas operativos x64). Además, las actualizaciones automáticas del explorador están **Activadas** de forma predeterminada, y Microsoft Edge no se puede desinstalar. Para más información, vea Adición de Microsoft Edge para Windows 10 a Microsoft Intune y la documentación de Microsoft Edge.

Actualización de la interfaz de usuario de protección de aplicaciones y de la interfaz de usuario de aprovisionamiento de aplicaciones de iOS

La interfaz de usuario para crear y editar directivas de protección de aplicaciones y perfiles de aprovisionamiento de aplicaciones de iOS en Intune se ha actualizado. Los cambios de la UI son:

- Una experiencia más sencilla, dado el uso de un formato de tipo asistente condensado dentro de una hoja.
- Una actualización del flujo de creación para incluir asignaciones.
- Una página de resumen de todos los elementos establecidos al ver las propiedades, antes de crear una nueva directiva o al editar una propiedad. Además, al editar las propiedades, el resumen solo mostrará una lista de elementos de la categoría de propiedades que se están editando.

Para más información, vea Creación y asignación de directivas de protección de aplicaciones y Uso de perfiles de aprovisionamiento de aplicaciones para iOS.

Escenarios guiados de Intune

Ahora, Intune proporciona escenarios guiados que ayudan a realizar una tarea concreta o un conjunto de tareas en Intune. Un escenario guiado es una serie personalizada de pasos (flujo de trabajo) en torno a un caso de uso completo. Los escenarios más habituales se definen en función del rol que un administrador, un usuario o un

dispositivo desempeñan en la organización. Estos flujos de trabajo suelen requerir una colección de perfiles, opciones, aplicaciones y controles de seguridad cuidadosamente organizados para proporcionar la mejor experiencia de usuario y seguridad. Estos son los nuevos escenarios guiados:

- Implementación de Microsoft Edge para dispositivos móviles
- Aplicaciones móviles seguras de Microsoft Office
- Escritorio moderno administrado en la nube

Para más información, vea Introducción a los escenarios guiados de Intune.

Variable de configuración de aplicaciones adicional disponible

Al crear una directiva de configuración de aplicaciones, puede incluir la variable de configuración `AAD_Device_ID` como parte de los valores de configuración. En Intune, seleccione **Aplicaciones cliente** > **Directivas de configuración de aplicaciones** > **Agregar**. Especifique los detalles de la directiva de configuración y seleccione **Opciones de configuración** para ver la hoja **Opciones de configuración**. Para más información, vea la sección Uso del diseñador de configuración en Adición de directivas de configuración de aplicaciones para dispositivos Android Enterprise administrados.

Creación de grupos de objetos de administración denominados conjuntos de directivas

Los conjuntos de directivas permiten crear una agrupación de referencias a entidades de administración ya existentes que se deben identificar, establecer como destino y supervisar como una sola unidad conceptual. Los conjuntos de directivas no reemplazan los conceptos ni los objetos existentes. Puede seguir asignando objetos individuales en Intune y hacer referencia a objetos individuales como parte de un conjunto de directivas. Por lo tanto, cualquier cambio que se realice en esos objetos individuales se verá reflejado en el conjunto de directivas. En Intune, deberá seleccionar **Conjuntos de directivas** > **Crear** para crear un conjunto de directivas desde cero.

Configuración del dispositivo

'

Nuevo perfil de interfaz de configuración de firmware de dispositivo para dispositivos con Windows 10 y versiones posteriores (versión preliminar pública)

En Windows 10 y versiones posteriores, puede crear un perfil de configuración de dispositivo para controlar la configuración y las características (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** como plataforma). En esta actualización, existe un nuevo tipo de perfil de interfaz de configuración de firmware de dispositivo que permite a Intune administrar la configuración de UEFI (BIOS).

Para más información sobre esta característica, vea Uso de perfiles de DFCI en dispositivos Windows en Microsoft Intune.

Se aplica a:

- Windows 10 RS5 (1809) y versiones más recientes en firmware compatible

Actualización de la interfaz de usuario para crear y editar anillos de actualización de Windows 10

Hemos actualizado la experiencia de interfaz de usuario para crear y editar anillos de actualización de Windows 10 para Intune. Los cambios en la interfaz de usuario son los siguientes:

- Formato de tipo asistente condensado en una sola hoja de la consola, bastante alejado de la dispersión de la hoja anterior cuando se configuraban anillos de actualización.
- El flujo de trabajo revisado incluye las asignaciones antes de completar la configuración inicial del anillo.
- Una página de resumen que se puede usar para revisar todas las configuraciones realizadas antes de guardar e implementar un anillo de actualización nuevo. Al editar un anillo de actualización, en el resumen solo muestra la lista de elementos establecidos en la categoría de las propiedades que se hayan editado.

Actualización de la interfaz de usuario para crear y editar una directiva de actualización de software de iOS

Hemos actualizado la experiencia de interfaz de usuario para crear y editar directivas de actualización de

software de iOS para Intune. Los cambios en la interfaz de usuario son los siguientes:

- Formato de tipo asistente condensado en una sola hoja de la consola, bastante alejado de la dispersión de la hoja anterior cuando se configuraban directivas de actualización.
- El flujo de trabajo revisado incluye las asignaciones antes de completar la configuración inicial de la directiva.
- Una página de resumen que se puede usar para revisar todas las configuraciones realizadas antes de guardar e implementar una directiva nueva. Al editar una directiva, en el resumen solo muestra la lista de elementos establecidos en la categoría de las propiedades que se hayan editado.

La configuración Reinicio establecido se ha quitado de los anillos de Windows Update

Como ya anunciamos en su día, ahora los anillos de actualización de Windows 10 de Intune admiten la configuración de fechas límite y ya no admiten *Reinicio establecido*. Las opciones de *Reinicio establecido* ya no están disponibles cuando al configurar o administrar anillos de actualización en Intune.

Este cambio viene de la mano de algunos cambios recientes en el Servicio de actualización de Windows y en los dispositivos que ejecutan Windows 10 1903 o versiones posteriores, las *fechas límite* reemplazan las configuraciones de *Reinicio establecido*.

Imposibilidad de instalar aplicaciones desde orígenes desconocidos en dispositivos de perfil de trabajo de Android Enterprise

En los dispositivos de perfil de trabajo de Android Enterprise, los usuarios no pueden instalar aplicaciones procedentes de orígenes desconocidos en ninguna circunstancia. En esta actualización hay una nueva configuración, **Impedir la instalación de aplicaciones de orígenes desconocidos en el perfil personal**. Esta opción impide de forma predeterminada que los usuarios carguen aplicaciones de orígenes desconocidos en el perfil personal del dispositivo.

Para ver los valores que se pueden configurar, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

Se aplica a:

- Perfil de trabajo de Android Enterprise

Creación de un proxy HTTP global en los dispositivos de propietario de dispositivos de Android Enterprise

En los dispositivos de Android Enterprise, se puede configurar un proxy HTTP global para cumplir los estándares de exploración web de la organización (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** como plataforma > **Propietario del dispositivo** > **Restricciones de dispositivos** como tipo de perfil > **Conectividad**). Una vez configurado, todo el tráfico HTTP usará este proxy.

Para configurar esta característica y ver los valores que se pueden configurar, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

Se aplica a:

- Propietario del dispositivo Android Enterprise

La opción Conectar automáticamente se ha quitado de los perfiles de Wi-Fi del administrador de dispositivos Android y Android Enterprise

En los dispositivos de administrador de dispositivos Android y Android Enterprise, puede crear un perfil de Wi-Fi para configurar diferentes opciones (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Administrador de dispositivos Android** o **Android Enterprise** como plataforma > **Wi-Fi** como tipo de perfil). En esta actualización, la opción **Conectar automáticamente** se ha quitado, ya que no es compatible con Android.

Si utiliza esta configuración en un perfil de Wi-Fi, posiblemente haya notado que **Conectar automáticamente** no funciona. No es necesario realizar ninguna acción, pero tenga en cuenta que esta configuración se ha quitado en la interfaz de usuario de Intune.

Para ver la configuración actual, vaya a Configuración de Wi-Fi de Android y Configuración de Wi-Fi de Android

Enterprise.

Se aplica a:

- Administrador de dispositivos Android
- Android Enterprise

Nuevos valores de configuración de dispositivo para dispositivos iOS e iPadOS supervisados

En los dispositivos iOS e iPad se puede crear un perfil para restringir las características y la configuración de esos dispositivos (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS/iPadOS** como plataforma > **Restricciones de dispositivos** como tipo de perfil). En esta actualización, hay nuevas opciones de configuración que puede controlar:

- El acceso a la unidad de red en la aplicación de archivos
- El acceso a la unidad USB en la aplicación de archivos
- La posibilidad tener Wi-Fi siempre activado

Para ver estas opciones, vaya a Configuración de dispositivos iOS para permitir o restringir características mediante Intune.

Se aplica a:

- iOS 13.0 y versiones más recientes
- IPadOS 13.0 y versiones más recientes

Inscripción de dispositivos

Cambiar a mostrar solo la página Estado de inscripción en los dispositivos aprovisionados mediante la configuración rápida (OOBE)

Ahora puede elegir mostrar solo la página Estado de inscripción en los dispositivos aprovisionados mediante OOBE de Autopilot.

Para ver el nuevo control de alternancia, elija **Intune** > **Inscripción de dispositivos** > **Inscripción de Windows** > **página Estado de inscripción** > **Crear perfil** > **Configuración** > **Mostrar solo la página en los dispositivos aprovisionados por la configuración rápida (OOBE)** .

Especificar qué versiones de sistema operativo del dispositivo Android se inscriben con el perfil de trabajo o la inscripción del administrador de dispositivos

Con las restricciones del tipo de dispositivo de Intune, puede usar la versión del sistema operativo del dispositivo para especificar qué dispositivos de usuario usarán la inscripción de perfil de trabajo de Android Enterprise o la inscripción de administrador de dispositivos Android. Para obtener más información, consulte Establecer restricciones de inscripción.

Administración de dispositivos

Intune admite iOS 11 y posterior

La inscripción en Intune y el Portal de empresa ahora admiten las versiones de iOS 11 y posteriores. No se admiten versiones anteriores.

Nuevas restricciones para cambiar el nombre de los dispositivos Windows

Al cambiar el nombre de un dispositivo Windows, se deben seguir reglas nuevas:

- 15 caracteres o menos (debe ser menor o igual que 63 bytes, sin incluir el valor NULL final).
- No puede ser una cadena nula o vacía.
- Caracteres ASCII permitidos: letras (a-z, A-Z), números (0-9) y guiones.
- Caracteres Unicode permitidos: caracteres >=0x80, debe tener un formato UTF8 válido, debe ser asignable mediante IDN (es decir, el proceso RtlIdnToNameprepUnicode debe finalizar correctamente. Consulte el documento RFC 3492).
- El nombre no debe contener números exclusivamente.
- El nombre no debe contener espacios.

- Caracteres no permitidos: { | } ~ [\ ] ^ ' : ; < = > ? & @ ! " # $ % ` ( ) + / , . _ *)

Para más información, vea Cambio de nombre de un dispositivo en Intune.

Nuevo informe de Android en la página de información general de dispositivos

Un nuevo informe en la página de información general de dispositivos muestra la cantidad de dispositivos Android inscritos en cada solución de administración de dispositivos. Este gráfico muestra la cantidad de dispositivos inscritos de perfil de trabajo, totalmente administrados, dedicados y de administrador de dispositivos. Para ver el informe, elija **Intune** > **Dispositivos** > **Información general**.

Seguridad de dispositivos

Línea de base de Microsoft Edge (versión preliminar)

Hemos agregado una versión preliminar de la línea de base de seguridad para la configuración de Microsoft Edge.

Certificados PKCS para macOS

Ahora puede usar certificados PKCS con macOS. Puede seleccionar el certificado PKCS como un tipo de perfil para macOS e implementar certificados de usuario y de dispositivo que tengan campos de firmante y de nombre alternativo del firmante personalizados.

El certificado PKCS para macOS también admite una nueva opción, *Permitir el acceso de todas las aplicaciones*. Con ella, puede permitir el acceso de todas las aplicaciones asociadas a la clave privada del certificado. Para más información sobre esta opción, vea la documentación de Apple en https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf.

Credenciales derivadas para aprovisionar dispositivos móviles iOS con certificados

Intune admite el uso de credenciales derivadas como método de autenticación y para el cifrado y la firma S/MIME de dispositivos iOS. Las credenciales derivadas son una implementación de la norma *800-157 del National Institute of Standards and Technology (NIST)* relativa a la implementación de certificados en dispositivos.

Las credenciales derivadas se basan en el uso de una tarjeta de verificación de identidad personal (PIV) o una tarjeta de acceso común (CAC), como una tarjeta inteligente. Para obtener una credencial derivada para un dispositivo móvil, los usuarios comienzan en la aplicación Portal de empresa y siguen un flujo de trabajo de inscripción que es único para el proveedor que usen. Un requisito común a todos los proveedores es usar una tarjeta inteligente en un equipo para autenticarse en el proveedor de las credenciales derivadas. Tras ello, dicho proveedor emite un certificado para el dispositivo que viene derivado de la tarjeta inteligente del usuario.

Intune admite los siguientes proveedores de credenciales derivadas:

- DISA Purebred
- Entrust
- Intercede

Las credenciales derivadas se usan como método de autenticación de los perfiles de configuración de dispositivos de VPN, Wi-Fi y correo electrónico. También se pueden usar para la autenticación de aplicaciones y el cifrado y la firma S/MIME.

Para más información sobre la norma, vea el documento sobre credenciales PIV derivadas en www.nccoe.nist.gov.

Uso de Graph API para especificar un nombre principal de usuario local como variable en certificados SCEP

Cuando use Graph API de Intune, puede especificar onPremisesUserPrincipalName como variable del nombre alternativo del firmante (SAN) de los certificados SCEP.

'

Administración de dispositivos de Microsoft 365

Experiencia de administración mejorada en Administración de dispositivos de Microsoft 365

Existe ahora una experiencia de administración actualizada y optimizada que está disponible con carácter general en el área de trabajo de especialistas de Administración de dispositivos de Microsoft 365 en https://endpoint.microsoft.com, por ejemplo:

- **Navegación actualizada**: encontrará una navegación de primer nivel simplificada que agrupa las características de manera lógica.
- **Nuevos filtros de plataforma**: puede seleccionar una sola plataforma, que muestra solo las directivas y las aplicaciones de la plataforma seleccionada, en las páginas Dispositivos y Aplicaciones.
- **Nueva página principal**: vea rápidamente el estado del servicio, el estado de su inquilino, noticias, etc., en la nueva página principal. Para más información sobre estas mejoras, vea la entrada de blog de Enterprise Mobility + Security en el sitio web de la comunidad tecnológica de Microsoft.

Introducción al nodo Seguridad del punto de conexión en Administración de dispositivos de Microsoft 365

El nodo **Seguridad del punto de conexión** está ahora disponible con carácter general en el área de trabajo de especialistas de Administración de dispositivos de Microsoft 365 en https://endpoint.microsoft.com, que agrupa las funcionalidades para proteger los puntos de conexión como:

- Líneas de base de seguridad: grupo preconfigurado de valores de configuración que le ayudan a aplicar un grupo conocido de valores de configuración y valores predeterminados que recomienda Microsoft.
- Tareas de seguridad: aproveche las ventajas de la administración de amenazas y vulnerabilidades (TVM) de Microsoft Defender for Endpoint y use Intune para corregir las debilidades del punto de conexión.
- Microsoft Defender for Endpoint: integración de Microsoft Defender for Endpoint para ayudar a evitar infracciones de seguridad en dispositivos móviles.""

Esta configuración seguirá siendo accesible desde otros nodos aplicables, como los dispositivos, y el estado configurado actual será el mismo, sin importar dónde tenga acceso a estas funcionalidades y las habilite.

Para más información sobre estas mejoras, consulte la entrada de blog sobre el éxito de clientes de Intune en el sitio web de la comunidad tecnológica de Microsoft.

Septiembre de 2019

Administración de aplicaciones

Aplicaciones de LOB privadas de Google Play administrado'

Ahora, Intune permite a los administradores de TI publicar aplicaciones de LOB de Android privadas en Google Play administrado a través de un iframe incrustado en la consola de Intune. Anteriormente, los administradores de TI tenían que publicar aplicaciones de LOB directamente en la consola de publicación de Google Play, lo cual requería varios pasos y llevaba mucho tiempo. Esta nueva característica permite publicar fácilmente aplicaciones de LOB siguiendo solo unos pocos pasos, sin necesidad de salir de la consola de Intune. Los administradores ya no tendrán que registrarse manualmente como desarrolladores en Google, y tampoco será necesario abonar la tasa de registro de Google de 25 $. Cualquiera de los escenarios de administración de Android Enterprise en que se use Google Play administrado pueden beneficiarse de esta característica (dispositivos con perfil de trabajo, dedicados, totalmente administrados y no inscritos). En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > **Agregar**. Luego, en la lista **Tipo de aplicación**, seleccione **Google Play administrado**. Para obtener más información sobre las aplicaciones de Google Play administrado, consulte Incorporación de aplicaciones de Google Play administrado a dispositivos Android Enterprise con Intune.

Experiencia en el Portal de empresa de Windows

El Portal de empresa de Windows se está actualizando. Podrá usar varios filtros en la página Aplicaciones del Portal de empresa de Windows. La página Detalles del dispositivo también se está actualizando con una experiencia de usuario mejorada. Estamos en proceso de implementar estas actualizaciones para todos los clientes, que se espera que finalicen al final de la semana próxima.

Compatibilidad de macOS con aplicaciones web

Las aplicaciones web, que le permiten agregar un acceso directo a una dirección URL en la web, se pueden instalar en el Dock mediante Portal de empresa para macOS. Los usuarios finales pueden acceder a la acción de **Instalar** desde la página de detalles de la aplicación para una aplicación web en Portal de empresa para macOS. Para más información sobre el tipo de aplicación de **vínculo web**, consulte Incorporación de aplicaciones a Microsoft Intune y Agregar aplicaciones web a Microsoft Intune.

Compatibilidad de macOS con las aplicaciones de VPP

Las aplicaciones macOS, compradas con Apple Business Manager, se muestran en la consola cuando se sincronizan los tokens de VPP de Apple en Intune. Puede asignar, revocar y reasignar licencias basadas en dispositivos y usuarios para grupos mediante la consola de Intune. Microsoft Intune le ayuda a administrar las aplicaciones de VPP compradas para su uso en su empresa:

- Informes sobre la información de licencia desde la tienda de aplicaciones.
- Realizando un seguimiento de cuántas licencias ha usado.
- Le ayudamos a impedir la instalación de más copias de la aplicación que las que tiene.

Para más información, consulte Administración de aplicaciones y libros comprados por volumen con Microsoft Intune.

Compatibilidad con iframe de Google Play administrado

Intune ahora proporciona compatibilidad para agregar y administrar vínculos web directamente en la consola de Intune a través del iframe de Google Play administrado. Esto permite a los administradores de TI enviar una dirección URL y un gráfico de iconos y, a continuación, implementar esos vínculos en dispositivos como aplicaciones Android normales. Cualquiera de los escenarios de administración de Android Enterprise en que se use Google Play administrado pueden beneficiarse de esta característica (dispositivos con perfil de trabajo, dedicados, totalmente administrados y no inscritos). En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > **Agregar**. Luego, en la lista **Tipo de aplicación**, seleccione **Google Play administrado**. Para obtener más información sobre las aplicaciones de Google Play administrado, consulte Incorporación de aplicaciones de Google Play administrado a dispositivos Android Enterprise con Intune.

Instalación silenciosa de aplicaciones de LOB de Android en dispositivos Zebra

Al instalar aplicaciones de línea de negocio (LOB) de Android en dispositivos Zebra, en lugar de que se le solicite la descarga e instalación de la aplicación de LOB, podrá instalar la aplicación de forma silenciosa. En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > **Agregar**. En el panel **Seleccionar un tipo de aplicación**, seleccione **Aplicación de línea de negocio**. Para obtener más información, consulte Incorporación de una aplicación de línea de negocio de Android a Microsoft Intune.

Actualmente, una vez descargada la aplicación de LOB, aparecerá una notificación informando de la **descarga correcta** en el dispositivo del usuario. La notificación solo se puede descartar pulsando **Borrar todo** en el sombreado de la notificación. Este problema se corregirá en una próxima versión y la instalación será totalmente silenciosa sin ningún indicador visual.

Operaciones de lectura y escritura de Graph API para aplicaciones de Intune

Las aplicaciones pueden llamar a Graph API de Intune con operaciones de lectura y escritura mediante la identidad de la aplicación y sin credenciales de usuario. Para obtener más información sobre cómo obtener acceso a Microsoft Graph API para Intune, consulte Trabajar con Intune en Microsoft Graph.

Cifrado y uso compartido de datos protegidos para el SDK de aplicaciones de Intune para iOS

El SDK de aplicaciones de Intune para iOS usará claves de cifrado de 256 bits cuando el cifrado esté habilitado mediante las directivas de protección de aplicaciones. Todas las aplicaciones deberán tener una versión de SDK 8.1.1 para permitir el uso compartido de datos protegidos.

Actualizaciones a la aplicación de Microsoft Intune

La aplicación de Microsoft Intune para Android se ha actualizado con las siguientes mejoras:

- Se ha actualizado y mejorado el diseño para incluir la navegación inferior para las acciones más importantes.
- Se ha agregado una página adicional que muestra el perfil del usuario.

- Se ha agregado la muestra de notificaciones interactivas en la aplicación para el usuario, como la necesidad de actualizar la configuración del dispositivo.
- Se ha agregado la muestra de notificaciones push personalizadas, alineando la aplicación con la compatibilidad agregada recientemente en la aplicación Portal de empresa para iOS y Android. Para más información, consulte Envío de notificaciones personalizadas en Intune. ""

Para dispositivos iOS, personalice la pantalla de privacidad del proceso de inscripción del Portal de empresa.

Con Markdown, puede personalizar la pantalla de privacidad del Portal de empresa que los usuarios finales ven durante la inscripción de iOS. En concreto, podrá personalizar la lista de elementos que la organización no puede ver o realizar en el dispositivo. Para más información, consulte Configuración de la aplicación Portal de empresa de Intune.

Configuración del dispositivo

Compatibilidad con perfiles VPN de IKEv2 para iOS

En esta actualización, puede crear perfiles VPN para el cliente VPN nativo de iOS mediante el protocolo IKEv2. IKEv2 es un nuevo tipo de conexión en **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para plataforma > **VPN** para tipo de perfil > **Tipo de conexión**.

Estos perfiles de VPN configuran el cliente de VPN nativo, por lo que no se instalan ni insertan aplicaciones cliente de VPN en los dispositivos administrados. Esta característica exige que los dispositivos estén inscritos en Intune (inscripción de MDM).

Para ver la configuración VPN actual que puede establecer, vaya a Configuración de VPN en dispositivos iOS.

Se aplica a:

- iOS

Las características del dispositivo, las restricciones de dispositivos y los perfiles de extensión de la configuración de iOS y macOS se muestran mediante el tipo de inscripción.

En Intune, puede crear perfiles para dispositivos iOS y macOS (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **iOS** o **macOS** como plataforma > **Características del dispositivo**, **Restricciones de dispositivos** o **Extensiones** para tipo de perfil).

En esta actualización, la configuración disponible en el portal de Intune se clasifica por el tipo de inscripción al que se aplica:

- iOS
  - Inscripción de usuarios""
  - Inscripción de dispositivos
  - Inscripción de dispositivo automatizada (supervisado)
  - Todos los tipos de inscripción
- macOS
  - Aprobada por el usuario
  - Inscripción de dispositivos
  - Inscripción de dispositivo automatizada
  - Todos los tipos de inscripción

Se aplica a:

- iOS

Nueva configuración del control de voz para dispositivos iOS supervisados que se ejecutan en pantalla completa

En Intune, puede crear directivas para ejecutar dispositivos iOS supervisados como una pantalla completa, o un dispositivo dedicado (**Configuración de dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para plataforma >

Restricciones de dispositivos para tipo de perfil > **Pantalla completa**).

En esta actualización, hay nuevas opciones de configuración que puede controlar:

- **Control de voz**: Habilita el control de voz en el dispositivo mientras se encuentra en pantalla completa.
- **Modificación del control de voz**: Permite a los usuarios cambiar el ajuste del control de voz del dispositivo mientras se encuentra en pantalla completa.

Para ver la configuración actual, vaya a los parámetros de pantalla completa de iOS.

Se aplica a:

- iOS 13.0 y versiones posteriores

Uso del inicio de sesión único para aplicaciones y sitios web en los dispositivos iOS y macOS

En esta actualización, hay algunos nuevos ajustes para el inicio de sesión único para dispositivos iOS y macOS (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **iOS** o **macOS** como plataforma > **Características del dispositivo** para tipo de perfil).

Use estas opciones para configurar una experiencia de inicio de sesión único, especialmente para aplicaciones y sitios web que usan la autenticación Kerberos. Puede elegir entre una extensión de aplicación de inicio de sesión único de credencial genérica y la extensión integrada de Kerberos de Apple.

Para ver las características de dispositivo actuales que puede configurar, vaya a las características de dispositivo de iOS y Características de dispositivo de macOS.

Se aplica a:

- iOS 13." y versiones más recientes
- macOS 10.15 y versiones más recientes

Asociación de dominios a aplicaciones en dispositivos macOS 10.15 y versiones posteriores

En los dispositivos macOS, puede configurar diferentes características e incorporar estas características a los dispositivos mediante una directiva (**Configuración de dispositivo** > **Perfiles** > **Crear perfil** > **macOS** para plataforma > **Características de dispositivo** para tipo de perfil). En esta actualización, puede asociar dominios a sus aplicaciones. Esta característica ayuda a compartir credenciales con sitios web relacionados con la aplicación, y se puede usar con la extensión de inicio de sesión único de Apple, vínculos universales y relleno automático de contraseñas.

Para ver los parámetros actuales que puede configurar, vaya a Configuración de características de dispositivos macOS en Intune.

Se aplica a:

- macOS 10.15 y versiones más recientes

Uso de "iTunes" y "apps" en la dirección URL de iTunes App Store al mostrar u ocultar aplicaciones en dispositivos iOS supervisados

En Intune, puede crear directivas para mostrar u ocultar aplicaciones en los dispositivos iOS supervisados (**Configuración de dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para plataforma > **Restricciones de dispositivos** para tipo de perfil > **Mostrar u ocultar aplicaciones**).

Puede especificar la dirección URL de iTunes App Store, como `https://itunes.apple.com/us/app/work-folders/id950878067?mt=8`. En esta actualización, se pueden usar `apps` y `itunes` en la dirección URL, como:

- `https://itunes.apple.com/us/app/work-folders/id950878067?mt=8`
- `https://apps.apple.com/us/app/work-folders/id950878067?mt=8`

Para obtener más información acerca de esta configuración, consulte Mostrar u ocultar aplicaciones.

Se aplica a:

- iOS

Los valores de tipo de contraseña de la directiva de cumplimiento de Windows 10 son más claros y coinciden con CSP.

En los dispositivos Windows 10, puede crear una directiva de cumplimiento que requiera características de contraseña específicas (**Cumplimiento de dispositivos** > **Directivas** > **Crear directiva** > **Windows 10 y versiones posteriores** para plataforma > **Seguridad del sistema**). En esta actualización:

- Los valores de **Tipo de contraseña** son más claros y se han actualizado para coincidir con DeviceLock/AlphanumericDevicePasswordRequired CSP.
- El valor de **Expiración de contraseña (días)** se ha actualizado para permitir valores entre 1 y 730 días.

Para obtener más información sobre la configuración del cumplimiento de Windows 10, consulte Configuración de Windows 10 y versiones posteriores para marcar dispositivos como compatibles o no compatibles con Intune.

Se aplica a:

- Windows 10 y versiones posteriores

Actualización de la interfaz de usuario para configurar el acceso local de Microsoft Exchange

Hemos actualizado la consola en la que configura el acceso local a Microsoft Exchange. Todas las configuraciones para el acceso local de Exchange están ahora disponibles en el mismo panel de la consola donde *habilita el control de acceso local de Exchange*.

Permiso o restricción para la adición de widgets de aplicaciones a la pantalla principal en dispositivos de perfil de trabajo de Android Enterprise

En dispositivos Android Enterprise, puede configurar características en el perfil de trabajo (**Configuración de dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** para plataforma > **Solo perfil de trabajo** > **Restricciones de dispositivos** para tipo de perfil). En esta actualización, puede permitir que los usuarios agreguen widgets expuestos por las aplicaciones del perfil de trabajo a la pantalla principal del dispositivo.

Para ver los valores que puede configurar, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

Se aplica a:

- Perfil de trabajo de Android Enterprise

Inscripción de dispositivos

Los nuevos inquilinos desaparecerán de forma predeterminada de la administración del administrador de dispositivos de Android.

Las funcionalidades del administrador de dispositivos de Android se han sustituido por Android Enterprise. Por lo tanto, se recomienda usar Android Enterprise para nuevas inscripciones. En una actualización futura, los nuevos inquilinos deberán completar los siguientes requisitos previos en la inscripción de Android para usar la administración del administrador de dispositivos: Vaya a **Intune** > **Inscripción de dispositivos** > **Inscripción de Android** > **Personal and corporate-owned devices with device administration privileges**(Dispositivos personales y corporativos con privilegios de administración de dispositivos) > **Use el administrador de dispositivos para administrar los dispositivos**.

Los inquilinos existentes no experimentarán cambio alguno en sus entornos.

Para obtener más información sobre el administrador de dispositivos Android en Intune, consulte Inscripción del administrador de dispositivos Android.

Lista de dispositivos DEP asociados a un perfil

Ahora puede ver una lista paginada de los dispositivos del Programa de inscripción de dispositivos (DEP) automatizados de Apple que están asociados a un perfil. Puede buscar en la lista desde cualquier página. Para ver la lista, vaya a **Intune** > **Inscripción de dispositivos** > **Inscripción de Apple** > **Tokens del programa**

de inscripción > elija un token > **Perfiles** > elija un perfil > **Dispositivos asignados** (bajo **Supervisar**).

Inscripción de usuario de iOS en versión preliminar

La versión iOS 13.1 de Apple incluye Inscripción de usuario, una nueva forma de administración ligera para dispositivos iOS. Se puede usar en lugar de Inscripción de dispositivos o de Inscripción de dispositivo automatizada (anteriormente Programa de inscripción de dispositivos) para dispositivos de propiedad personal. La versión preliminar de Intune es compatible con este conjunto de características, ya que permite:

- Realizar la inscripción de usuarios de destino en grupos de usuarios.
- Ofrecer a los usuarios finales la posibilidad de seleccionar entre la inscripción de usuarios más ligera o la inscripción de dispositivos más segura cuando inscriban sus dispositivos.

A partir del 24/9/2019 con la versión 13.1 de iOS, estaremos en el proceso de implementar estas actualizaciones para todos los clientes y se espera que finalicen al final de la semana próxima.

Se aplica a:

- iOS 13.1 y versiones posteriores

Administración de dispositivos

Más compatibilidad con dispositivos Android totalmente administrados

Hemos agregado la siguiente compatibilidad con dispositivos Android totalmente administrados:

- Los certificados SCEP para dispositivos Android totalmente administrados están disponibles para la autenticación de certificados en dispositivos administrados como propietario del dispositivo. Los certificados SCEP ya se admiten en los dispositivos con perfil de trabajo. Con los certificados SCEP para el propietario del dispositivo, podrá:
  - crear un perfil de SCEP en la sección correspondiente de Android Enterprise
  - vincular certificados SCEP con el perfil de Wi-Fi del propietario del dispositivo para la autenticación
  - vincular certificados SCEP con los perfiles VPM del propietario del dispositivo para la autenticación
  - vincular certificados SCEP con los perfiles de correo electrónico del propietario del dispositivo para la autenticación (a través de AppConfig)
- Las aplicaciones del sistema son compatibles con dispositivos de Android Enterprise. En Intune, agregue una aplicación del sistema Android Enterprise seleccionando **Aplicaciones cliente** > **Aplicaciones** > **Agregar**. En la lista **Tipo de aplicación**, seleccione **Aplicación del sistema Android Enterprise**. Para más información, vea Agregar aplicaciones del sistema Android Enterprise a Microsoft Intune.
- En **Cumplimiento de dispositivos** > **Android Enterprise** > **Propietario del dispositivo**, puede crear una directiva de cumplimiento que cumpla con el nivel de atestación de Google SafetyNet.
- En dispositivos Android Enterprise totalmente administrados, se admiten los proveedores de Mobile Threat Defense. En **Cumplimiento de dispositivos** > **Android Enterprise** > **Propietario del dispositivo**, puede elegir un nivel de amenaza aceptable. En Configuración de Android Enterprise para marcar dispositivos como compatibles o no compatibles con Intune se muestra la configuración actual.
- En los dispositivos Android Enterprise totalmente administrados, la aplicación Microsoft Launcher ahora se puede configurar a través de directivas de configuración de aplicaciones para permitir una experiencia de usuario final estandarizada en el dispositivo totalmente administrado. La aplicación Microsoft Launcher se puede usar para personalizar el dispositivo Android. Usando la aplicación con una cuenta Microsoft o una cuenta profesional o educativa, puede acceder a su calendario, documentos y actividades recientes en la fuente personalizada.

Con esta actualización, nos complace anunciar que la compatibilidad de Intune con Android Enterprise totalmente administrado ya está disponible con carácter general.

Se aplica a:

- Dispositivos totalmente administrados de Android Enterprise

Envío de notificaciones personalizadas a un solo dispositivo

Ahora puede seleccionar un solo dispositivo y, a continuación, usar una acción de dispositivo remoto para enviar una notificación personalizada solo a ese dispositivo.

Las acciones de borrado y restablecimiento de código de acceso no están disponibles para los dispositivos iOS inscritos mediante la inscripción de usuarios.

La inscripción de usuarios es un nuevo tipo de inscripción de dispositivos de Apple. Al inscribir dispositivos mediante la inscripción de usuarios, las acciones remotas de borrado y restablecimiento de código de acceso no estarán disponibles para dichos dispositivos.

Compatibilidad de Intune con dispositivos iOS 13 y macOS Catalina

Intune admite ahora la administración de dispositivos iOS 13 y macOS Catalina. Para más información, vea la entrada de blog sobre la compatibilidad de Microsoft Intune con iOS 13 y iPadOS.

Compatibilidad de Intune con dispositivos iPadOS e iOS 13.1

Intune admite ahora la administración de dispositivos iPadOS e iOS 13.1. Para más información, vea esta entrada de blog.

Seguridad de dispositivos

Compatibilidad de BitLocker con la rotación de contraseñas de recuperación controlada por el cliente

Use la configuración de Endpoint Protection de Intune para configurar la rotación de contraseñas de recuperación controlada por el cliente para BitLocker en dispositivos que ejecutan la versión 1909 de Windows o una posterior.

Esta configuración inicia una actualización de la contraseña de recuperación controlada por el cliente después de la recuperación de la unidad del sistema operativo (mediante bootmgr o WinRE) y un desbloqueo de la contraseña de recuperación en una unidad de datos fija. Esta opción actualiza la contraseña de recuperación específica que se usó, y otras contraseñas no usadas en el volumen permanecen sin cambios. Para obtener más información, consulte la documentación de CSP de BitLocker para ConfigureRecoveryPasswordRotation.

Protección contra alteraciones para el antivirus de Windows Defender

Use Intune para administrar la *Protección contra alteraciones* para el antivirus de Windows Defender. Encontrará el ajuste para la Protección contra alteraciones en el grupo del centro de seguridad de Microsoft Defender al usar perfiles de configuración de dispositivos para Windows 10 Endpoint Protection. Puede establecer la protección contra alteraciones en **Habilitado** para activar sus restricciones; en **Deshabilitado** para desactivarlas; o en **No configurado** para mantener la configuración actual de los dispositivos.

Para obtener más información acerca de la Protección contra alteraciones, vea Evitar cambios de la configuración de seguridad con Protección contra alteraciones en la documentación de Windows.

La configuración avanzada del Firewall de Windows Defender ya está disponible con carácter general.

Las reglas de firewall personalizadas de Windows Defender para Endpoint Protection, que se configuran como parte de un perfil de configuración de dispositivos, ya están disponibles con carácter general en tanto que versión preliminar pública. Puede usar estas reglas para especificar un comportamiento entrante y saliente en las aplicaciones, las direcciones de red y los puertos. Estas reglas se publicaron en julio como una versión preliminar pública.

Supervisión y solución de problemas

Actualización de la interfaz de usuario de Intune: panel Estado del inquilino

La interfaz de usuario para el panel Estado del inquilino se actualizó para alinearla con los estilos de interfaz de usuario de Azure. Para más información, consulte Estado del inquilino.

Control de acceso basado en roles.

Las etiquetas de ámbito ahora son compatibles con las directivas de términos de uso.

Ahora puede asignar etiquetas de ámbito a las directivas de términos de uso. Para ello, vaya a **Intune** > **Inscripción de dispositivos** > **Términos y condiciones** > elija un elemento de la lista > **Propiedades** > **Etiquetas de ámbito** > elija una etiqueta de ámbito.

Agosto de 2019

Administración de aplicaciones

Control del comportamiento de desinstalación de aplicaciones iOS en anulación de la inscripción de dispositivos

Los administradores pueden administrar si una aplicación se quita de un dispositivo o se conserva en este cuando se anula la inscripción de dicho dispositivo en el nivel de grupo de usuarios o dispositivos.

Categorización de aplicaciones de Microsoft Store para Empresas

Puede categorizar las aplicaciones de la Tienda Microsoft para Empresas. Para ello, elija aplicaciones > **cliente** > de **Intune aplicaciones** > seleccione una aplicación de Microsoft Store para empresas > **categoría** de **información** de la aplicación. En el menú desplegable, asigne una categoría.

Notificaciones personalizadas para usuarios de aplicaciones de Microsoft Intune

La aplicación de Microsoft Intune para Android ahora admite la visualización de notificaciones de envío personalizadas y se alinea con la compatibilidad agregada recientemente en las aplicaciones de Portal de empresa para iOS y Android. Para más información, consulte Envío de notificaciones personalizadas en Intune.

Configuración del dispositivo

Configuración de Microsoft Edge mediante plantillas administrativas para Windows 10 y versiones más recientes

En los dispositivos Windows 10 y más recientes, puede crear plantillas administrativas para configurar las opciones de directiva de grupo en Intune. En esta actualización, puede configurar las opciones que se aplican a la versión 77 y posteriores de Microsoft Edge.

Para más información sobre las plantillas administrativas, vea Usar plantillas de Windows 10 para configurar opciones de directiva de grupo en Intune.

Se aplica a:

- Windows 10 y versiones más recientes (Windows RS4+)

Nuevas características para dispositivos dedicados de Android Enterprise en el modo de varias aplicaciones

En Intune, puede controlar las características y las configuraciones en una experiencia de estilo de quiosco en dispositivos dedicados (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** para la plataforma > **Solo el propietario del dispositivo, Restricciones de dispositivos** para el tipo de perfil).

En esta actualización, se agregan las siguientes características:

- **Dispositivos dedicados** > **Varias aplicaciones:** el **botón Inicio virtual** se puede mostrar al avanzar en el dispositivo o flotar en la pantalla para que los usuarios puedan moverla.
- **Dispositivos dedicados** > **Varias aplicaciones: Acceso a la linterna** permite a los usuarios usar la linterna.
- **Dispositivos dedicados** > **Varias aplicaciones: Control del volumen de elementos multimedia** permite a los usuarios controlar el volumen multimedia del dispositivo con un control deslizante.
- **Dispositivos dedicados** > **Varias aplicaciones: habilite un protector de pantalla**, cargue una imagen personalizada y controle cuándo se muestra el protector.

Para ver la configuración actual, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características mediante Intune.

Se aplica a:

- Dispositivos Android Enterprise dedicados

Nueva aplicación y perfiles de configuración para dispositivos Android Enterprise totalmente administrados

Mediante el uso de perfiles, puede configurar las opciones que aplican la configuración de VPN, correo

electrónico y Wi-Fi al propietario de dispositivos (totalmente administrados) Android Enterprise. En esta actualización, puede:

- Use las directivas de configuración de aplicaciones para implementar la configuración de correo electrónico de Outlook, Gmail y Nine Work.
- Use los perfiles de configuración de dispositivos para implementar la configuración de certificados raíz de confianza.
- Use los perfiles de configuración de dispositivos para implementar la configuración de VPN y Wi-Fi.

> **IMPORTANT**
> Con esta característica, los usuarios se autentican con su nombre de usuario y contraseña para los perfiles de VPN, Wi-Fi y correo electrónico. Actualmente, la autenticación basada en certificados no está disponible.

Se aplica a:

- Propietario del dispositivo Android Enterprise (totalmente administrado)

Control de las aplicaciones, los archivos, los documentos y las carpetas que se abren cuando los usuarios inician sesión en dispositivos macOS

Puede habilitar y configurar características de dispositivos macOS (**Configuración del dispositivos** > **Perfiles** > **Crear perfil** > **macOS** para la plataforma >**Características del dispositivo** para el tipo de perfil).

En esta actualización, hay una nueva configuración de elementos de inicio de sesión para controlar qué aplicaciones, archivos, documentos y carpetas se abren cuando un usuario inicia sesión en el dispositivo inscrito.

Para ver la configuración actual, vaya a Configuración de dispositivos iOS para permitir o restringir características mediante Intune.

Se aplica a:

- macOS

Las fechas límite reemplazan la configuración del reinicio establecido de los anillos de Windows Update

Para estar en consonancia con los cambios recientes en el servicio de Windows, los anillos de actualización de Windows 10 de Intune ahora admiten la configuración de fechas límite. Las *fechas límite* determinan cuándo un dispositivo instala las actualizaciones de características y seguridad. En los dispositivos que ejecutan Windows 10 1903 o una versión posterior, las *fechas límite* sustituyen a las configuraciones del *reinicio establecido*. En el futuro, las *fechas límite* reemplazarán también al *reinicio establecido* de las versiones anteriores de Windows 10.

Si no se configuran las *fechas límite*, los dispositivos seguirán usando la configuración de *Reinicio establecido*, pero Intune dejará de admitir la configuración de Reinicio establecido en una actualización futura.

Planee el uso de *fechas límite* para todos los dispositivos Windows 10. Una vez que haya establecido la configuración de las *fechas límite*, puede cambiar las configuraciones de Intune para que el *reinicio establecido* sea Sin configurar. Si se establece en Sin configurar, Intune deja de administrar esa configuración en los dispositivos, pero no quitará las últimas opciones de la configuración del dispositivo. Por lo tanto, las últimas configuraciones que se establecieron para el *reinicio establecido* permanecen activas y en uso en los dispositivos hasta que dichas configuraciones se modifican mediante un método distinto de Intune. Más adelante, cuando la versión de los dispositivos de Windows cambia o cuando la compatibilidad de Intune con las *fechas límite* se expande a la versión de Windows de los dispositivos, el dispositivo comenzará a usar la nueva configuración, que ya está en su lugar.

Compatibilidad con varias instancias de Microsoft Intune Certificate Connector

Intune ahora admite la instalación y el uso de varias instancias de Microsoft Intune Certificate Connectors para operaciones PKCS. Este cambio admite el equilibrio de carga y la alta disponibilidad del conector. Cada instancia

de conector puede procesar solicitudes de certificado desde Intune. Si un conector no está disponible, otros conectores continúan procesando las solicitudes.

Para usar varios conectores, no es necesario actualizar a la versión más reciente del software del conector.

Nuevas configuraciones y cambios en la configuración existente para restringir características en dispositivos iOS y macOS

Puede crear perfiles para restringir configuraciones en dispositivos que ejecutan iOS y macOS (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** o **macOS** para el tipo de plataforma > **Restricciones de dispositivos**). En esta actualización se incluyen las características siguientes:

- En **macOS** > **Restricciones de dispositivos** > **Nube y almacenamiento** use la nueva configuración **Handoff** para impedir que los usuarios empiecen a trabajar en un dispositivo macOS y sigan trabajando en otro dispositivo macOS o iOS.

  Para ver la configuración actual, vaya a Configuración de dispositivos macOS para permitir o restringir características mediante Intune.

- En **iOS** > **Restricciones de dispositivos**, hay algunos cambios:

  - **Aplicaciones integradas** > **Buscar mi iPhone (solo supervisado)** : nueva configuración que bloquea esta característica en la característica Buscar mi aplicación.
  - **Aplicaciones integradas** > **Find My Friends (solo supervisado)** : nueva configuración que bloquea esta característica en la característica Buscar mi aplicación.
  - **Inalámbrica** > **Modificación del estado de Wi-Fi (solo supervisado)** : nueva configuración que impide que los usuarios activen o desactiven la conexión Wi-Fi en el dispositivo.
  - **Teclado y diccionario** > **QuickPath (solo supervisado)** : nueva configuración que bloquea la característica QuickPath.
  - **Nube y almacenamiento**: **Continuación de la actividad** pasa a llamarse **Handoff**.

  Para ver la configuración actual, vaya a Configuración de dispositivos iOS para permitir o restringir características mediante Intune.

Se aplica a:

- macOS 10.15 y versiones más recientes
- iOS 13 y versiones más recientes

Algunas restricciones de dispositivos iOS no supervisadas se supervisarán solo con la versión iOS 13.0

En esta actualización, algunas configuraciones se aplican a los dispositivos solo supervisados con la versión iOS 13.0. Si esta configuración se definen y asignan a dispositivos no supervisados antes de la versión de iOS 13.0, dicha configuración se seguirá aplicando a esos dispositivos no supervisados. También se aplican después de que los dispositivos se actualicen a iOS 13.0. Estas restricciones se quitan de los dispositivos no supervisados de los que se realiza una copia de seguridad y se restauran.

Estas opciones incluyen:

- Tienda de aplicaciones, presentación de documentos, juegos
  - Tienda de aplicaciones
  - Música, podcasts o contenido de noticias explícitos de iTunes
  - Incorporación de amigos a Game Center
  - Juego multijugador
- Aplicaciones integradas
  - Cámara
    - FaceTime
  - Safari
    - Autorrellenar

- Nube y almacenamiento
  - Copia de seguridad en iCloud
  - Bloquear la sincronización de documentos de iCloud
  - Bloquear la sincronización de Keychain en iCloud

Para ver la configuración actual, vaya a Configuración de dispositivos iOS para permitir o restringir características mediante Intune.

Se aplica a:

- iOS 13.0 y versiones más recientes

Estado de dispositivo mejorado para el cifrado de FileVault de macOS

Hemos actualizado varios mensajes de estado de dispositivo para el cifrado de FileVault en dispositivos macOS.

Algunas configuraciones de examen del Antivirus de Windows Defender en el informe muestran un estado de error

En Intune, puede crear directivas para usar el Antivirus de Windows Defender para examinar los dispositivos Windows 10 (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Restricciones del dispositivo** para el tipo de perfil > **Antivirus de Windows Defender**). Los informes **Hora a la que se realizará un examen rápido diario** y **Tipo de examen del sistema para realizar** muestran un estado de error, cuando es realmente un estado correcto.

En esta actualización se ha corregido este comportamiento. Por lo tanto las configuraciones **Hora a la que se realizará un examen rápido diario** y **Tipo de examen del sistema para realizar** muestran un estado correcto cuando los exámenes se completan correctamente y muestran un estado de error cuando la configuración no se puede aplicar.

Para más información sobre la configuración de Windows Defender Antivirus consulte Configuración de dispositivos con Windows 10 y versiones posteriores para permitir o restringir características mediante Intune.

Zebra Technologies es un OEM admitido para OEMConfig en dispositivos Android Enterprise

En Intune, puede crear perfiles de configuración de dispositivo y aplicar la configuración a los dispositivos Android Enterprise mediante OEMConfig (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** para la plataforma > **OEMConfig** para el tipo de perfil).

En esta actualización, Zebra Technologies es un fabricante de equipos originales (OEM) admitido para OEMConfig. Para obtener más información sobre OEMConfig, consulte Uso y administración de dispositivos Android Enterprise con OEMConfig.

Se aplica a:

- Android Enterprise

Inscripción de dispositivos

Etiquetas de ámbito predeterminadas

Ahora hay disponible una nueva etiqueta de ámbito predeterminada integrada. Todos los objetos de Intune no etiquetados que admiten etiquetas de ámbito se asignan automáticamente a la etiqueta de ámbito predeterminada. La etiqueta de ámbito **predeterminada** se agrega a todas las asignaciones de roles existentes para mantener la paridad con la experiencia de administración hoy en día. Si no desea que un administrador vea los objetos de Intune con la etiqueta de ámbito predeterminada, quítela de la asignación de roles. Esta característica es similar a la característica de ámbitos de seguridad de Configuration Manager. Para más información, consulte Usar control de acceso basado en rol (RBAC) y etiquetas de ámbito para TI distribuida.

Soporte técnico del administrador de dispositivos de inscripción de Android

La opción de inscripción del administrador de dispositivos Android se ha agregado a la página Inscripción de Android (**Intune** > **Inscripción de dispositivos** > **Inscripción de Android**). El administrador de dispositivos Android seguirá estando habilitado de forma predeterminada para todos los inquilinos. Para más información,

consulte Inscripción del administrador de dispositivos Android.

Omisión de más pantallas en el Asistente de configuración

Puede establecer perfiles de Programa de inscripción de dispositivos para omitir las siguientes pantallas del Asistente de configuración:

- Para iOS
  - Apariencia
  - Express Language (Idioma rápido)
  - Idioma preferido
  - Device to Device Migration (Migración entre dispositivos)
- Para macOS
  - Tiempo de pantalla
  - Configuración de Touch ID

Para más información sobre la personalización del Asistente de configuración, consulte Creación de un perfil de inscripción de Apple y Creación de un perfil de inscripción de Apple para macOS.

Incorporación de una columna de usuario al proceso de carga de CSV del dispositivo AutoPilot

Ahora puede agregar una columna de usuario a la carga CSV para Dispositivos Autopilot. Esto le permite asignar usuarios en masa en el momento de importar el archivo CSV. Para más información, consulte Inscripción de dispositivos Windows en Intune con Windows Autopilot.

Administración de dispositivos

Configuración del límite de tiempo de limpieza automática de dispositivos en treinta días

Puede establecer el límite de tiempo de limpieza automática de dispositivos en un plazo de 30 días (en lugar del límite anterior de noventa días) después del último inicio de sesión. Para ello, vaya a **Intune** > **configuración** > de **dispositivos** > **limpiar reglas**.

Número de compilación incluido en la página Hardware del dispositivo Android

Una nueva entrada en la página Hardware de cada dispositivo Android incluye el número de compilación del sistema operativo del dispositivo. Para más información, consulte Ver detalles del dispositivo en Intune.

Julio de 2019

Administración de aplicaciones

Notificaciones personalizadas para usuarios y grupos

Envíe notificaciones de inserción personalizadas desde la aplicación del Portal de empresa a los usuarios en dispositivos iOS y Android que administra con Intune. Estas notificaciones de inserción móviles son altamente personalizables con texto libre y se pueden usar con cualquier fin. Puede dirigirlas a diferentes grupos de usuarios de su organización. Para obtener más información, consulte Notificaciones personalizadas.

Aplicación de controlador de directiva de dispositivo de Google

La aplicación de Pantalla principal administrada ahora proporciona acceso a la aplicación de directiva de dispositivo Android de Google. La aplicación de Pantalla principal administrada es un iniciador personalizado que se usa para dispositivos inscritos en Intune, como dispositivos dedicados de Android Enterprise (AE) que usan el modo de pantalla completa de varias aplicaciones. Puede acceder a la aplicación de directiva de dispositivo Android o guiar a los usuarios a esta aplicación, con fines de soporte técnico y depuración. Esta capacidad de inicio está disponible en el momento en que el dispositivo se inscribe y se bloquea en la Pantalla principal administrada. No se necesitan instalaciones adicionales para usar esta funcionalidad.

Configuración de protección de Outlook para dispositivos iOS y Android

Ahora puede configurar los valores de configuración de protección generales de datos y aplicaciones para Outlook para iOS y Android mediante controles de administración de Intune simples sin inscripción de dispositivos. Los valores de configuración generales de aplicaciones proporcionan paridad con la configuración

que pueden habilitar los administradores al administrar Outlook para iOS y Android en dispositivos inscritos. Para obtener más información sobre la configuración de Outlook, consulte Implementación de Outlook para iOS y opciones de configuración de aplicación de Android.

Iconos Managed Home Screen y Configuración administrada

El icono de la aplicación Managed Home Screen y el icono **Configuración administrada** se han actualizado. La aplicación Managed Home Screen solo la usan dispositivos inscritos en Intune, como dispositivos dedicados de Android Enterprise (AE) y que se ejecutan en modo de pantalla completa con varias aplicaciones. Para obtener más información sobre la aplicación de Pantalla principal administrada, consulte Configuración de la aplicación Managed Home Screen de Microsoft para Android Enterprise.

Directiva de dispositivos Android en dispositivos dedicados de Android Enterprise

Puede obtener acceso a la aplicación Directiva de dispositivos Android en la pantalla de depuración de la aplicación Managed Home Screen. La aplicación Managed Home Screen solo la usan dispositivos inscritos en Intune, como dispositivos dedicados de Android Enterprise (AE) y que se ejecutan en modo de pantalla completa con varias aplicaciones. Para obtener más información, consulte Configuración de la aplicación Managed Home Screen de Microsoft para Android Enterprise.

Actualizaciones del Portal de empresa de iOS

El nombre de la empresa reemplazará el texto "i.manage.microsoft.com" actual en los mensajes de administración de aplicaciones iOS. Por ejemplo, los usuarios verán el nombre de la empresa en lugar de "i.manage.microsoft.com" cuando intenten instalar una aplicación iOS desde el portal de empresa o cuando permitan la administración de la aplicación. Esto se implantará para todos los clientes en los próximos días.

Azure AD y APP en dispositivos Android Enterprise

Ahora, al incorporar dispositivos Android Enterprise totalmente administrados, los usuarios se registrarán en Azure Active Directory (Azure AD) durante la configuración inicial de su nuevo dispositivo o el restablecimiento de fábrica del dispositivo. Anteriormente, en el caso de un dispositivo totalmente administrado, una vez completada la configuración, el usuario tenía que iniciar manualmente la aplicación de Microsoft Intune para iniciar el registro de Azure AD. Ahora, cuando el usuario tiene acceso a la página principal del dispositivo tras la configuración inicial, el dispositivo se inscribe y registra.

Además de las actualizaciones de Azure AD, las directivas de protección de aplicaciones (APP) de Intune se admiten ahora en dispositivos Android Enterprise totalmente administrados. Esta funcionalidad estará disponible a medida que la implementemos. Para obtener más información, consulte Incorporación de aplicaciones de Google Play administrado a dispositivos Android Enterprise con Intune.

Configuración del dispositivo

Uso de "reglas de aplicabilidad" al crear perfiles de configuración de dispositivo Windows 10

Puede crear perfiles de configuración de dispositivo Windows 10 (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **Windows 10** para la plataforma > **Reglas de aplicabilidad**). En esta actualización, puede crear una **regla de aplicabilidad** para que el perfil solo se aplique a una edición o una versión en concreto. Por ejemplo, cree un perfil que permita algunas opciones de configuración de BitLocker. Una vez que agregue el perfil, use una regla de aplicabilidad para que este solo se aplique a los dispositivos que ejecuten Windows 10 Enterprise.

Para agregar una regla de aplicabilidad, consulte Reglas de aplicabilidad.

Se aplica a: Windows 10 y versiones posteriores

Uso de tokens para agregar información específica del dispositivo en perfiles personalizados para dispositivos iOS y macOS

Puede usar perfiles personalizados en dispositivos iOS y macOS para configurar opciones y características no integradas en Intune (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** o **macOS** para la plataforma > **Personalizado** para el tipo de perfil). En esta actualización, puede agregar tokens a sus archivos `.mobileconfig` para agregar información específica del dispositivo. Por ejemplo, puede agregar `Serial Number: {{serialnumber}}` a su archivo de configuración para mostrar el número de serie del dispositivo.

Para crear un perfil personalizado, consulte Configuración personalizada de iOS o Configuración personalizada de macOS.

Se aplica a:

- iOS
- macOS

Nuevo diseñador de configuraciones al crear un perfil OEMConfig para Android Enterprise

En Intune, puede crear un perfil de configuración de dispositivo que use una aplicación OEMConfig (Configuración del dispositivo > Perfiles > Crear perfil > Android Enterprise para la plataforma > OEMConfig para el tipo de perfil). Al hacerlo, se abre un editor JSON con una plantilla y valores que debe cambiar.

Esta actualización incluye un diseñador de configuraciones con una experiencia de usuario mejorada que muestra detalles insertados en la aplicación entre los que se incluyen títulos, descripciones, etc. El editor JSON sigue estando disponible y muestra cualquier cambio que realiza en el diseñador de aplicaciones.

Para ver la configuración actual, vaya a Uso y administración de dispositivos Android Enterprise con OEMConfig.

Se aplica a: Android Enterprise

Interfaz de usuario actualizada para configurar Windows Hello

Hemos actualizado la consola donde configura Intune para usar Windows Hello para empresas. Ya están disponibles todas las opciones de configuración en el mismo panel de la consola donde habilita compatibilidad con Windows Hello.

SDK de PowerShell de Intune

El SDK de PowerShell de Intune, que proporciona compatibilidad con la API de Intune a través de Microsoft Graph, se ha actualizado a la versión 6.1907.1.0. Ahora, el SDK admite lo siguiente:

- Funciona con Azure Automation.
- Admite operaciones de lectura de autenticación de solo aplicación.
- Admite nombres abreviados descriptivos como alias.
- Se ajusta a las convenciones de nomenclatura de PowerShell. De forma específica, se ha cambiado el nombre del parámetro `PSCredential` (en el cmdlet `Connect-MSGraph`) por `Credential`.
- Admite la especificación manual del valor del encabezado `Content-Type` al usar el cmdlet `Invoke-MSGraphRequest`.

Para obtener más información, consulte SDK de PowerShell para Graph API de Microsoft Intune.

Administración de FileVault para macOS

Puede usar Intune para administrar el cifrado de claves de FileVault para dispositivos macOS. Para cifrar los dispositivos, debe usar un perfil de configuración de dispositivos de Endpoint Protection.

Nuestra compatibilidad con FileVault incluye el cifrado de dispositivos descifrados, la custodia de la clave de recuperación personal de un dispositivo, la rotación automática o manual de claves de cifrado personales y la recuperación de clave para sus dispositivos corporativos. Los usuarios finales también pueden utilizar el sitio web del Portal de empresa para obtener la clave de recuperación personal para sus dispositivos cifrados.

También hemos expandido el informe de cifrado para incluir información sobre FileVault con información para BitLocker, de modo que puede ver todos los detalles del cifrado del dispositivo en un solo lugar.

Nueva configuración de Office, Windows y OneDrive en las plantillas administrativas de Windows 10

Puede crear plantillas administrativas en Intune que imiten la administración de directivas de grupo locales (**Administración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y posterior** para la plataforma > **Plantilla administrativa** para el tipo de perfil).

En esta actualización se incluyen más opciones de configuración de Office, Windows y OneDrive que pueden

agregar a sus plantillas. Con esta nueva configuración, ahora puede configurar más de 2500 opciones totalmente basadas en la nube.

Para obtener más información sobre esta característica, consulte Usar plantillas de Windows 10 para configurar opciones de directiva de grupo en Intune.

Se aplica a: Windows 10 y versiones posteriores

Inscripción de dispositivos

Actualizaciones de las restricciones de inscripción

Las restricciones de inscripción para nuevos inquilinos se han actualizado para que se permitan los perfiles de trabajo de Android Enterprise de forma predeterminada. Los inquilinos existentes no experimentarán cambio alguno. Para usar los perfiles de trabajo de Android Enterprise, aún deberá conectar su cuenta de Intune a su cuenta de Google Play administrada.

Actualizaciones de interfaz de usuario de las restricciones de inscripción y la inscripción de Apple

Los dos procesos siguientes usan una interfaz de usuario de estilo de asistente:

- Inscripción de dispositivos de Apple. Para obtener más información, consulte Inscripción automática de dispositivos iOS con el Programa de inscripción de dispositivos de Apple.
- Creación de restricciones de inscripción. Para obtener más información, consulte Establecer restricciones de inscripción.

Control de la configuración previa de identificadores de dispositivos corporativos para dispositivos Android Q

En Android Q (v10), Google no permitirá a los agentes MDM de dispositivos Android (administrador de dispositivos) administrados heredados recopilar información del identificador de dispositivo. Intune tiene una característica que permite a los administradores de TI configurar de forma previa una lista de números de serie del dispositivo para etiquetar automáticamente estos dispositivos como propiedad corporativa. Esta característica no funcionará para los dispositivos Android Q que administre el administrador de dispositivos. Independientemente de si se carga el número de serie o IMEI del dispositivo, siempre se considerará personal durante la inscripción de Intune. Puede cambiar manualmente la propiedad a corporativa tras la inscripción. Esto solo afecta a las nuevas inscripciones, no a los dispositivos inscritos existentes. Los dispositivos Android administrados con perfiles de trabajo no se ven afectados por este cambio y continuarán funcionando como lo hacen en la actualidad. Además, los dispositivos Android Q inscritos como administrador de dispositivos ya no podrán informar sobre el número de serie o IMEI en la consola de Intune como propiedades del dispositivo.

Los iconos han cambiado para las inscripciones de Android Enterprise (perfil de trabajo, dispositivos dedicados y dispositivos completamente administrados)

Los iconos de los perfiles de inscripción de Android Enterprise han cambiado. Para ver los nuevos iconos, vaya a **Intune** > **Inscripción** > **Inscripción de Android** > busque en **Perfiles de inscripción**.

Cambio en la recopilación de datos de diagnóstico de Windows

El valor predeterminado de la recopilación de datos de diagnóstico ha cambiado para los dispositivos con la versión 1903 de Windows 10 y posteriores. A partir de Windows 10 1903, la recopilación de datos de diagnóstico se habilita de forma predeterminada. Los datos de diagnóstico de Windows son datos técnicos vitales de dispositivos Windows sobre el dispositivo y el rendimiento de Windows y el software relacionado. Para obtener más información, consulte Configurar los datos de diagnóstico de Windows en la organización. Los dispositivos Autopilot también participan en la telemetría "completa", a menos que se establezca lo contrario en el perfil de Autopilot con System/AllowTelemetry.

El restablecimiento de Windows Autopilot quita el usuario primario del dispositivo

Al usarse el restablecimiento de Autopilot en un dispositivo, se quitará el usuario primario del dispositivo. El próximo usuario que inicie sesión tras el restablecimiento se establecerá como usuario primario. Esta característica se implantará para todos los clientes en los próximos días.

Administración de dispositivos

Mejora de la ubicación del dispositivo

Puede acercar las coordenadas exactas de un dispositivo mediante la acción **Buscar dispositivo**. Para obtener más información sobre cómo buscar dispositivos iOS perdidos, consulte Búsqueda de dispositivos iOS perdidos.

Seguridad de dispositivos

Configuración avanzada del Firewall de Windows Defender (versión preliminar pública)

Use Intune para administrar las reglas de firewall personalizadas como parte de un perfil de configuración de dispositivo para Endpoint Protection en Windows 10. Las reglas pueden especificar un comportamiento entrante y saliente en las aplicaciones, las direcciones de red y los puertos.

Interfaz de usuario actualizada para administrar líneas de base de seguridad

Hemos actualizado la experiencia de creación y edición en la consola de Intune para nuestras líneas de base de seguridad. Los cambios son:

Un formato de estilo de asistente que se ha comprimido en una sola hoja. en una hoja. Este nuevo diseño elimina la expansión de la hoja que requiere que los profesionales de TI exploren en profundidad varios paneles independientes.
Ahora puede crear asignaciones como parte de la experiencia de creación y edición, en lugar de tener que volver posteriormente para asignar líneas de base. Hemos agregado un resumen de la configuración que puede ver antes de crear una nueva línea de base y al editar una existente. Al editar, en el resumen solo se muestra la lista de elementos establecidos en la primera categoría de propiedades editadas.

Junio de 2019

Administración de aplicaciones

Configuración del explorador que se puede vincular a datos organizativos

Ahora, las directivas de protección de aplicaciones (APP) de Intune en dispositivos iOS y Android permiten transferir vínculos web Org a un explorador determinado más allá de Intune Managed Browser o Microsoft Edge. Consulte ¿Qué son las directivas de protección de aplicaciones? para obtener más información sobre APP.

En la página Todas las aplicaciones se identifican las aplicaciones de Microsoft Store para Empresas en línea o sin conexión

En la página **Todas las aplicaciones** ahora se incluye el etiquetado para identificar las aplicaciones de Microsoft Store para Empresas (MSFB) como aplicaciones en línea o sin conexión. Ahora, en cada aplicación MSFB se incluye un sufijo para **En línea** o **Sin conexión**. En la página de detalles de la aplicación también se incluye información sobre **Tipo de licencia** y **Supports device context installation** (Admite la instalación de contexto de dispositivo) (solo aplicaciones con licencia sin conexión).

Aplicación del Portal de empresa en los dispositivos compartidos de Windows

Ahora, los usuarios pueden tener acceso a la aplicación del Portal de empresa en los dispositivos compartidos de Windows. Los usuarios finales verán una etiqueta **Compartida** en el icono de dispositivo. Esto se aplica a la versión 10.3.45609.0 y posteriores de la aplicación del Portal de empresa de Windows.

Ver todas las aplicaciones instaladas desde la página web del Portal de empresa

La nueva página **Aplicaciones instaladas** del sitio web del Portal de empresa muestra todas las aplicaciones administradas (requeridas y disponibles) que están instaladas en los dispositivos de un usuario. Además del tipo de asignación, los usuarios pueden ver el editor de la aplicación, la fecha de publicación y el estado de instalación actual. Si todavía no hay ninguna aplicación requerida o disponible para los usuarios, estos verán un mensaje en el que se explica que no hay ninguna aplicación de la empresa instalada. Para ver la página nueva en la Web, vaya al sitio web del Portal de empresa y haga clic en **Aplicaciones instaladas**.

La vista nueva permite que los usuarios de las aplicaciones vean todas las aplicaciones administradas instaladas en el dispositivo

La aplicación Portal de empresa para Windows ahora muestra todas las aplicaciones administradas (tanto las requeridas como las disponibles) que están instaladas en el dispositivo de un usuario. Los usuarios también pueden ver las instalaciones de aplicaciones intentadas y pendientes, además de sus estados actuales. Si todavía no hay ninguna aplicación requerida o disponible para los usuarios, estos verán un mensaje en el que se explica que no hay ninguna aplicación de la empresa instalada. Para ver la vista nueva, vaya al panel de navegación del Portal de empresa y seleccione **Aplicaciones** > **Aplicaciones instaladas**.

Características nuevas de la aplicación Microsoft Intune

Hemos agregado características nuevas a la aplicación Microsoft Intune (versión preliminar) para Android. Los usuarios de dispositivos Android totalmente administrados ahora pueden:

- Ver y administrar los dispositivos inscritos mediante la aplicación Portal de empresa de Intune o Microsoft Intune.
- Ponerse en contacto con su organización para obtener soporte técnico.
- Enviar comentarios a Microsoft.
- Consultar los términos y condiciones, si la organización los estableció.

Aplicaciones de ejemplo nuevas que muestran la integración del SDK de Intune disponible en GitHub

La cuenta de GitHub msintuneappsdk agregó aplicaciones de ejemplo nuevas para iOS (Swift), Android, Xamarin.iOS, Xamarin Forms y Xamarin.Android. Estas aplicaciones están pensadas para complementar la documentación existente y ofrecen demostraciones sobre cómo integrar el SDK de la aplicación Intune en sus propias aplicaciones móviles. Si es desarrollador de aplicaciones y necesita más orientación sobre el SDK de Intune, consulte estos ejemplos vinculados:

- Chatr: una aplicación de mensajería instantánea nativa de iOS (Swift) que usa la Biblioteca de autenticación de Azure Active Directory (ADAL) para la autenticación intermediada.
- Taskr: una aplicación de listas de tareas pendientes nativa de Android que usa ADAL para la autenticación intermediada.
- Taskr: una aplicación de listas de tareas pendientes de Xamarin.Android que usa ADAL para la autenticación intermediada. Este repositorio también tiene la aplicación Xamarin.Forms.
- Aplicación de ejemplo de Xamarin.iOS: una aplicación de ejemplo esencial de Xamarin.iOS.

Configuración del dispositivo

Configuración de las extensiones de kernel en dispositivos macOS

En dispositivos macOS, puede crear un perfil de configuración de dispositivos (**Configuración de dispositivo** > **Perfiles** > **Crear perfil** > elija **macOS** como plataforma). Esta actualización incluye un nuevo grupo de opciones de configuración que permite configurar y usar las extensiones de kernel en los dispositivos. Puede agregar extensiones específicas o permitir todas las extensiones de un asociado o desarrollador específico.

Para obtener más información sobre esta característica, consulte los artículos sobre información general de las extensiones de kernel y la configuración de las extensiones de kernel.

Se aplica a: macOS 10.13.2 y versiones posteriores

La opción Permitir solo aplicaciones de la Tienda para dispositivos Windows 10 incluye más opciones de configuración

Al crear un perfil de restricciones de dispositivos para dispositivos Windows, se puede usar la opción **Permitir solo aplicaciones de la Tienda** de modo que los usuarios solo instalen aplicaciones de la Tienda Windows (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para plataforma > **Restricciones de dispositivos** para tipo de perfil). En esta actualización, este valor se amplía para admitir más opciones.

Para ver la nueva configuración, vaya al artículo sobre la configuración de dispositivos con Windows 10 y versiones posteriores para permitir o restringir características.

Se aplica a: Windows 10 y versiones posteriores

Implementación de varios perfiles de dispositivo de extensiones de movilidad de Zebra en un dispositivo, el mismo grupo de usuarios o el mismo grupo de dispositivos

En Intune, puede usar extensiones de movilidad (MX) de Zebra en un perfil de configuración de dispositivo para personalizar la configuración de dispositivos Zebra que no se integran en Intune. Actualmente, puede implementar un perfil en un único dispositivo. En esta actualización, puede implementar varios perfiles en:

- Mismo grupo de usuarios

- Mismo grupo de dispositivos
- Dispositivo único

En Usar y administrar dispositivos Zebra con extensiones de movilidad de Zebra en Microsoft Intune se muestra cómo usar MX en Intune.

Se aplica a: Android

Algunas opciones de configuración de pantalla completa en dispositivos iOS se establecen mediante "Bloquear", en sustitución de "Permitir"

Al crear un perfil de restricciones de dispositivos en dispositivos iOS (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para plataforma > **Restricciones de dispositivos** para tipo de perfil > **Pantalla completa**), se establecen el **Bloqueo automático**, el **Cambio de timbre**, la **Rotación de pantalla**, el **Botón de suspensión de pantalla** y los **Botones de volumen**.

En esta actualización, los valores son **Bloquear** (bloquea la característica) o **Sin configurar** (permite la característica). Para ver la configuración, vaya a Configuración de dispositivos iOS para permitir o restringir características .

Se aplica a iOS.

Uso de Face ID para la autenticación de contraseña en dispositivos iOS

Al crear un perfil de restricciones de dispositivos para dispositivos iOS, puede usar una huella digital para una contraseña. En esta actualización, la configuración de contraseña de huella digital también permite el reconocimiento facial (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para la plataforma > **Restricciones de dispositivos** para el tipo de perfil > **Contraseña**). Como resultado, han cambiado las opciones de configuración siguientes:

- **Desbloqueo con huella digital** es ahora **Desbloqueo de Touch ID y Face ID**.
- **Modificación de huella digital (solo con supervisión)** es ahora **Modificación de Touch ID y Face ID (solo con supervisión)** .

Face ID está disponible en iOS 11.0 y versiones posteriores. Para ver la configuración, vaya a Configuración de dispositivos iOS para permitir o restringir características mediante Intune.

Se aplica a iOS.

La restricción de características de juegos y aplicaciones de la tienda en dispositivos iOS depende ahora de la región de clasificación

En dispositivos iOS, puede permitir o restringir características relacionadas con los juegos, la tienda de aplicaciones y la visualización de documentos (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para plataforma > **Restricciones de dispositivos** para tipo de perfil > **App Store, presentación de documentos, juegos**). También puede elegir la región de clasificación, por ejemplo, Estados Unidos.

En esta actualización, la característica **Aplicaciones** pasa a ser un elemento secundario de **Región de clasificación** y a depender de **Región de clasificación**. Para ver la configuración, vaya a Configuración de dispositivos iOS para permitir o restringir características mediante Intune.

Se aplica a iOS.

Inscripción de dispositivos

Compatibilidad de Windows Autopilot con Unión a Azure AD híbrido

Ahora, Windows Autopilot para los dispositivos existentes admite Unión a Azure AD híbrido (además de la compatibilidad con Unión a Azure AD existente). Se aplica a dispositivos con la versión 1809 de Windows 10 y posteriores. Para obtener más información, consulte Windows Autopilot para dispositivos existentes.

Administración de dispositivos

Consulta del nivel de revisión de seguridad para dispositivos Android

Ahora puede consultar el nivel de revisión de seguridad para dispositivos Android. Para ello, seleccione **Intune**

> **Dispositivos** > **Todos los dispositivos** > seleccione un dispositivo > **Hardware**. El nivel de revisión se muestra en la sección **Sistema operativo**.

Asignación de etiquetas de ámbito a todos los dispositivos administrados de un grupo de seguridad

Ahora puede asignar etiquetas de ámbito a un grupo de seguridad y todos los dispositivos del grupo de seguridad también se asociarán a esas etiquetas de ámbito. La etiqueta de ámbito también se asigna a todos los dispositivos de estos grupos. Las etiquetas de ámbito establecidas con esta característica sobrescriben a las establecidas con el flujo de etiquetas de ámbito de dispositivo actual. Para obtener más información, consulte el artículo sobre el uso de RBAC y las etiquetas de ámbito para TI distribuida.

Seguridad de dispositivos

Uso de la búsqueda de palabras clave con Líneas de base de seguridad

Al crear o editar perfiles de línea de base de seguridad, puede especificar las palabras clave en la nueva barra de *búsqueda* para filtrar los grupos disponibles de opciones de configuración a aquellos que incluyen sus criterios de búsqueda.

La característica Líneas de base de seguridad ya está disponible con carácter general

La característica **Líneas de base de seguridad** está fuera de la versión preliminar y ya está disponible con carácter general (GA). Esto significa que la característica está lista para usarse en producción. Sin embargo, las plantillas de línea de base individuales pueden permanecer en versión preliminar y se evalúan y publican con carácter general según su propia programación.

La plantilla Línea de base de seguridad MDM ya está disponible con carácter general

La plantilla Línea de base de seguridad MDM se ha sacado de la versión preliminar y ya está disponible con carácter general (GA). La plantilla con disponibilidad general se identifica como **Línea de base de seguridad MDM de mayo de 2019**. Se trata de una nueva plantilla y no de una actualización de la versión preliminar. Como nueva plantilla, deberá revisar la configuración que contiene y, después, crear nuevos perfiles para implementar la plantilla en su dispositivo. Otras plantillas de línea de base de seguridad pueden permanecer en versión preliminar. Para ver una lista de líneas de base disponibles, consulte Líneas de base de seguridad disponibles.

Además de ser una nueva plantilla, *Línea de base de seguridad MDM de mayo de 2019* incluye las dos opciones de configuración que hemos anunciado recientemente en nuestro artículo En desarrollo:

- Above Lock (Por encima de la pantalla de bloqueo): la voz activa las aplicaciones de una pantalla bloqueada
- DeviceGuard: use la seguridad basada en la virtualización (VBS) la próxima vez que reinicie los dispositivos.

Línea de base de seguridad MDM de mayo de 2019 también incluye la incorporación de varias opciones de configuración nuevas, la eliminación de otras y una revisión del valor predeterminado de una configuración. Para ver una lista detallada de los cambios realizados de la versión preliminar a la disponibilidad general, consulte los **cambios en la nueva plantilla**.

Control de versiones de líneas de base de seguridad

Líneas de base de seguridad para el control de versiones del soporte técnico de Intune. Con este soporte técnico, a medida que se publican nuevas versiones de cada línea de base de seguridad, puede actualizar sus perfiles de línea de base de seguridad para usar la versión de línea de base más reciente sin tener que volver a crear e implementar una nueva línea de base desde cero. Además, en la consola de Intune puede ver información sobre cada una de las líneas de base, como, por ejemplo, el número de perfiles individuales que tiene y que usan la línea de base, cuántas de las diferentes versiones de línea de base usan sus perfiles y de qué fecha data la versión más reciente de una línea de base de seguridad específica. Para obtener más información, consulte **Líneas de base de seguridad**.

Se ha movido la opción Utilice las claves de seguridad para el inicio de sesión

La opción de configuración del dispositivo para la protección de identidad llamada **Utilice las claves de seguridad para el inicio de sesión** ya no se encuentra como configuración secundaria de *Configurar Windows Hello para empresas*. Ahora se trata de una opción de nivel superior que está siempre disponible,

incluso si no habilita el uso de Windows Hello para empresas. Para obtener más información, consulte Protección de identidad.

Control de acceso basado en roles.

Nuevos permisos para administradores de grupos asignados

Ahora, el rol de administrador de la escuela integrado de Intune tiene permisos de creación, lectura, actualización y eliminación (CRUD) para Aplicaciones administradas. Esta actualización significa que si se le asigna como administrador de grupos en Intune for Education, ahora puede crear, ver, actualizar y eliminar el certificado push MDM de iOS, los tokens de servidor de MDM de iOS y los tokens de VPP de iOS, junto con todos los permisos existentes que tenga. Para tomar alguna de estas medidas, vaya a **Configuración de inquilinos** > **Administración de dispositivos iOS**.

Las aplicaciones pueden usar Graph API para llamar a operaciones de lectura sin credenciales de usuario

Las aplicaciones pueden llamar a operaciones de lectura de Graph API de Intune con la identidad de la aplicación y sin credenciales de usuario. Para obtener más información sobre cómo obtener acceso a Microsoft Graph API para Intune, consulte Trabajar con Intune en Microsoft Graph.

Aplicación de etiquetas de ámbito a las aplicaciones de Microsoft Store para Empresas

Ahora puede aplicar etiquetas de ámbito a las aplicaciones de Microsoft Store para Empresas. Para obtener más información sobre las etiquetas de ámbito, consulte Uso del control de acceso basado en roles y de las etiquetas de ámbito para la TI distribuida.

Mayo de 2019

Administración de aplicaciones

Informes de aplicaciones potencialmente peligrosas en dispositivos Android

Intune ahora proporciona más datos sobre informes de aplicaciones potencialmente peligrosas en dispositivos Android.

Aplicación Portal de empresa de Windows

La aplicación Portal de empresa de Windows ahora tiene una nueva página denominada **Dispositivos**. La página **Dispositivos** ahora mostrará a los usuarios finales los dispositivos inscritos. Los usuarios verán este cambio en Portal de empresa cuando usen la versión 10.3.4291.0 o una posterior. Para obtener información sobre cómo configurar Portal de empresa, vea Configuración de la aplicación Portal de empresa de Microsoft Intune.

Método de autenticación de actualizaciones de directivas de Intune e instalación de aplicaciones de Portal de empresa

En los dispositivos ya inscritos mediante el Asistente de configuración a través de uno de los métodos de inscripción de dispositivos corporativos de Apple, Intune ya no será compatible con Portal de empresa cuando los usuarios finales de la tienda de aplicaciones lo instalen manualmente. Este cambio solo es pertinente cuando se realiza la autenticación con el Asistente de configuración de Apple durante la inscripción. Este cambio solo afecta a los dispositivos iOS inscritos a través de:

- Apple Configurator
- Apple Business Manager
- Apple School Manager
- Programa de inscripción de dispositivos (DEP) de Apple

Si los usuarios instalan la aplicación Portal de empresa desde la tienda de aplicaciones y luego intentan inscribir estos dispositivos a través de ella, recibirán un error. Se espera que estos dispositivos solo usen la aplicación Portal de empresa cuando Intune lo inserta, automáticamente, durante la inscripción. Se actualizarán los perfiles de inscripción de Intune en Azure Portal para que pueda especificar cómo los dispositivos se autentican y si reciben la aplicación Portal de empresa. Si quiere que los usuarios de dispositivos DEP tengan la aplicación Portal de empresa, deberá especificar sus preferencias en un perfil de inscripción.

Además, se va a quitar la pantalla **Identificar el dispositivo** de la aplicación Portal de empresa de iOS. Por lo

tanto, los administradores que quieren habilitar el acceso condicional o implementar aplicaciones de la empresa deben actualizar el perfil de inscripción de DEP. Este requisito solo se aplica si la inscripción de DEP se autentica con el Asistente para la configuración. En ese caso, debe insertar la aplicación Portal de empresa en el dispositivo. Para ello, elija **Intune** > **Inscripción de dispositivos** > **Inscripción de Apple** > **Tokens del programa de inscripción** > elija un token > **Perfiles** > elija un perfil > **Propiedades** > establezca **Instalar Portal de empresa** en **Sí**.

Para instalar la aplicación Portal de empresa en dispositivos DEP ya inscritos, deberá ir a Intune > Aplicaciones cliente e insertarla como una aplicación administrada con directivas de configuración de aplicación.

Configurar cómo los usuarios finales actualizan una aplicación de línea de negocio (LOB) con una directiva de protección de aplicaciones

Ahora puede configurar dónde los usuarios finales pueden obtener una versión actualizada de una aplicación de línea de negocio (LOB). Los usuarios finales verán esta característica en el cuadro de diálogo de inicio condicional **Versión mínima de la aplicación**, que le pedirá a los usuarios finales que actualicen a una versión mínima de la aplicación de LOB. Debe proporcionar estos detalles de actualización como parte de la directiva de protección de aplicaciones (APP) de LOB. Esta característica está disponible en iOS y en Android. En iOS, esta característica requiere que la aplicación esté integrada (o encapsulada con la herramienta de encapsulado) con el SDK de Intune para iOS v. 10.0.7 o superior. En Android, esta característica requeriría la versión más reciente de la aplicación Portal de empresa. Para configurar cómo un usuario final actualiza una aplicación de LOB, la aplicación necesita que se le envíe una directiva de configuración de aplicación administrada con la clave `com.microsoft.intune.myappstore`. El valor enviado definirá desde qué tienda descargará la aplicación el usuario final. Si la aplicación se implementa a través de Portal de empresa, el valor debe ser `CompanyPortal`. En el caso de cualquier otra tienda, debe escribir una dirección URL completa.

Scripts de PowerShell de extensión de administración de Intune

Puede configurar los scripts de PowerShell para que se ejecuten con los privilegios de administración del usuario en el dispositivo. Para más información, consulte Uso de scripts de PowerShell para dispositivos Windows 10 en Intune y Administración de aplicaciones Win32.

Administración de aplicaciones de Android Enterprise

Para facilitar a los administradores de TI la configuración y el uso de la administración de Android Enterprise, Intune agregará automáticamente cuatro aplicaciones comunes relacionadas con Android Enterprise a la consola de administración de Intune. Las cuatro aplicaciones de Android Enterprise son las siguientes:

- **Microsoft Intune** : se usa para escenarios totalmente administrados de Android Enterprise.
- **Microsoft Authenticator** : ayuda a iniciar sesión en las cuentas si se usa la verificación de dos fases.
- **Portal de empresa de Intune** : se usa para las directivas de protección de aplicación y escenarios de perfil de trabajo de Android Enterprise.
- Managed Home Screen: se usa para los escenarios de pantalla completa o dedicados de Android Enterprise.

Anteriormente, los administradores de TI tenían que buscar y aprobar manualmente estas aplicaciones en la Tienda de Google Play administrada como parte de la configuración. Este cambio elimina los pasos que antes eran manuales para facilitar y agilizar el uso de la administración de Android Enterprise por parte de los clientes.

Los administradores verán que estas cuatro aplicaciones se agregan automáticamente a la lista de aplicaciones de Intune en el momento en que conecten por primera vez a su inquilino de Intune con Google Play administrado. Para más información, consulte Conexión de una cuenta de Intune a una cuenta de Google Play administrado. Para los inquilinos que ya han conectado a su inquilino o que ya utilizan Android Enterprise, no hay nada que los administradores tengan que hacer. Estas cuatro aplicaciones aparecerán automáticamente dentro de los siete días siguientes a la finalización de la implementación del servicio en mayo de 2019.

Configuración del dispositivo

Conector de certificados PFX actualizado para Microsoft Intune

Hemos publicado una actualización del Conector de certificado PFX para Microsoft Intune que resuelve un

problema por el que los certificados PFX existentes se siguen reprocesando, lo que provoca que el conector deje de procesar nuevas solicitudes.

Tareas de seguridad de Intune para Defender for Endpoint (en versión preliminar pública)

En la versión preliminar pública, puede usar Intune para administrar las tareas de seguridad para Microsoft Defender for Endpoint. Esta integración con Defender for Endpoint agrega un enfoque basado en riesgos para detectar vulnerabilidades y errores de configuración de puntos de conexión, establecer su prioridad y corregirlos, a la vez que reduce el tiempo entre la detección y la mitigación.

Buscar un conjunto de chips TPM en una directiva de cumplimiento de dispositivos Windows 10

Muchos dispositivos Windows 10 y posteriores tienen conjuntos de chips del Módulo de plataforma segura (TPM). Esta actualización incluye una nueva configuración de cumplimiento que comprueba la versión del chip TPM en el dispositivo.

La configuración de directivas de cumplimiento de Windows 10 y versiones posteriores describe esta configuración.

Se aplica a: Windows 10 y versiones posteriores

Impedir que los usuarios finales modifiquen su punto de acceso personal y deshabilitar el registro del servidor Siri en dispositivos iOS

Crear un perfil de restricciones de dispositivo en el dispositivo iOS (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para la plataforma y **Restricciones de dispositivo** para el tipo de perfil). Esta actualización incluye nuevas opciones que puede configurar:

- **Aplicaciones integradas**: registro del servidor para los comandos de Siri
- **Inalámbrica**: modificación por el usuario del punto de acceso personal (solo con supervisión)

Para ver esta configuración, vaya a la configuración de aplicaciones integradas para iOS y configuración inalámbrica para iOS.

Se aplica a iOS 12.2 y versiones más recientes.

Nueva configuración de restricción de dispositivos de aplicaciones en el aula para dispositivos macOS

Puede crear un perfil de configuración de dispositivos para dispositivos MacOS (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **macOS** como plataforma >**Restricciones del dispositivo** para tipo de perfil). Esta actualización incluye una nueva configuración de aplicaciones en el aula, la opción para bloquear capturas de pantalla y la opción para deshabilitar la Fototeca de iCloud.

Para ver la configuración actual, vaya a Configuración de dispositivos macOS para permitir o restringir características mediante Intune.

Se aplica a: macOS

Se cambia el nombre de la configuración Contraseña para acceder a la tienda de aplicaciones de iOS

El nombre de la configuración **Contraseña para acceder a la tienda de aplicaciones** se cambia a **Require iTunes Store password for all purchases** (Requerir contraseña de iTunes Store para todas las compras) (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **iOS** para la plataforma > **Restricciones de dispositivos** para el tipo de perfil > **Tienda de aplicaciones, presentación de documentos y juegos**).

Para ver la configuración disponible, vaya a Tienda de aplicaciones, presentación de documentos, juegos de iOS.

Se aplica a iOS.

Línea de base de Microsoft Defender for Endpoint (versión preliminar)

Agregamos una versión preliminar de la línea de base de seguridad para la configuración de Microsoft Defender for Endpoint. Esta línea de base está disponible cuando el entorno cumple con los requisitos previos para usar Microsoft Defender for Endpoint.

Configuración de biometría y firma de Outlook para dispositivos iOS y Android

Ahora puede especificar si la firma predeterminada está habilitada en Outlook en dispositivos iOS y Android. Además, puede elegir permitir que los usuarios cambien la configuración de biometría en Outlook en iOS.

Compatibilidad del control de acceso de red (NAC) con F5 Access para dispositivos iOS

F5 ha publicado una actualización para BIG-IP 13 que permite la funcionalidad NAC para F5 Access para iOS en Intune. Para usar esta característica,:

- Actualice BIG-IP a 13.1.1.5. No se admite BIG-IP 14.
- Integre BIG-IP con Intune para NAC. Los pasos se describen en Overview: Configuring APM for device posture checks with endpoint management systems (Información general: Configuración de APM para comprobaciones de posición del dispositivo con sistemas de administración de puntos de conexión).
- Active la opción **Habilitar el control de acceso a la red (NAC)** del perfil de VPN en Intune.

Para ver las opciones disponibles, vaya a Configuración de VPN en dispositivos iOS.

Se aplica a iOS.

Conector de certificados PFX actualizado para Microsoft Intune

Se ha publicado una actualización para el Conector de certificados PFX para Microsoft Intune que reduce el intervalo de sondeo de 5 minutos a 30 segundos.

Inscripción de dispositivos

Nombre del atributo OrderID del dispositivo de Autopilot cambiado a Etiqueta de grupo

Para hacer que sea más intuitivo, el nombre del atributo **OrderID** en los dispositivos de Autopilot se ha cambiado a **Etiqueta de grupo**. Al usar archivos CSV para cargar información de dispositivos de Autopilot, debe usar Etiqueta de grupo como encabezado de columna, en lugar de OrderID.

La página Estado de inscripción (ESP) de Windows ya está disponible con carácter general

La página Estado de inscripción dejó de estar en versión preliminar. Para más información, consulte Configurar una página de estado de inscripción.

Actualización de la interfaz de usuario de Intune: creación de un perfil de inscripción de Autopilot

La interfaz de usuario para crear un perfil de inscripción de Autopilot se actualizó para alinearla con los estilos de interfaz de usuario de Azure. Para obtener más información, consulte cómo crear un perfil de inscripción de Autopilot. Más adelante, se actualizarán más escenarios de Intune a este nuevo estilo de interfaz de usuario.

Habilitar Restablecimiento de Autopilot para todos los dispositivos Windows

Restablecimiento de Autopilot ahora funciona para todos los dispositivos Windows, incluso para los que no están configurados para usar la página Estado de inscripción. Si no se configuró una página de estado de inscripción para el dispositivo durante la inscripción de dispositivo inicial, el dispositivo irá directamente al escritorio después de iniciar sesión. Puede tardar hasta ocho horas en sincronizar y aparecer como compatible en Intune. Para más información, consulte el artículo sobre cómo restablecer dispositivos con Restablecimiento de Windows Autopilot.

No se requiere un formato IMEI exacto al buscar en todos los dispositivos

No será necesario que incluya espacios en los números IMEI cuando busca en **Todos los dispositivos**.

Reflejo de la eliminación de un dispositivo del portal de Apple en el portal de Intune

Si se elimina un dispositivo de los portales del Programa de inscripción de dispositivos de Apple o de Apple Business Manager, el dispositivo se eliminará automáticamente de Intune durante la siguiente sincronización.

La página de estado de inscripción ahora realiza un seguimiento de las aplicaciones de Win32

Esto solo se aplica a dispositivos que ejecutan Windows 10 versión 1903 y posteriores. Para más información, consulte Configurar una página de estado de inscripción.

Administración de dispositivos

Restablecimiento y borrado de dispositivos de forma masiva mediante Graph API

Ahora podrá restablecer y borrar hasta 100 dispositivos de forma masiva mediante Graph API.

Supervisión y solución de problemas

El informe de cifrado dejó de estar en versión preliminar pública

El informe sobre BitLocker y el cifrado de dispositivo está disponible con carácter general y ya no forma parte de la versión preliminar pública.

Abril de 2019

Administración de aplicaciones

Actualización de la experiencia de usuario para la aplicación Portal de empresa para iOS

Se ha rediseñado la página principal de la aplicación Portal de empresa para dispositivos iOS. Con este cambio, la página principal seguirá mejor los patrones de la interfaz de usuario de iOS y ofrecerá una función de detección mejorada para aplicaciones y libros electrónicos.

Cambios en la inscripción del Portal de empresa para los usuarios de dispositivos iOS 12

Se han actualizado los pasos y las pantallas de inscripción del Portal de empresa para iOS con el fin de ajustarlos a los cambios en la inscripción de MDM que se introdujeron en Apple iOS 12.2. En el nuevo flujo de trabajo, se pide a los usuarios que hagan esto:

- Permitir que Safari abra el sitio web del Portal de empresa y descargue el perfil de administración antes de volver a la aplicación Portal de empresa.
- Abrir la aplicación Ajustes para instalar el perfil de administración en el dispositivo.
- Volver a la aplicación Portal de empresa para completar la inscripción.

Para conocer los pasos y las pantallas de inscripción actualizados, vea Enroll iOS device in Intune (Inscripción de dispositivos iOS en Intune).

Cifrado de OpenSSL para las directivas de protección de aplicaciones Android

Las directivas de protección de aplicaciones (APP) de Intune en dispositivos Android ahora usan una biblioteca de cifrado de OpenSSL que es compatible con FIPS 140-2. Para más información, vea la sección sobre cifrado de Configuración de directivas de protección de aplicaciones Android en Microsoft Intune.

Habilitar dependencias de la aplicación Win32

Como administrador, puede exigir que otras aplicaciones se instalen como dependencias antes de instalar la aplicación Win32. En concreto, el dispositivo debe instalar las aplicaciones dependientes antes de que se instale la aplicación Win32. En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > **Agregar** para mostrar la hoja **Agregar aplicación**. Seleccione **Aplicación de Windows (Win32)** como **Tipo de aplicación**. Después de agregar la aplicación, puede seleccionar **Dependencias** para agregar las aplicaciones dependientes que se deben instalar antes de poder instalar la aplicación Win32. Para más información, vea Intune independiente: administración de aplicaciones Win32.

Información de instalación de la versión para aplicaciones de Microsoft Store para Empresas

Los informes de instalación de aplicaciones incluyen información de la versión de la aplicación para aplicaciones de Microsoft Store para Empresas. En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones**. Elija una **Aplicación de Microsoft Store para Empresas** y luego seleccione **Estado de instalación del dispositivo** en la sección **Supervisión**.

Adiciones a las reglas de requisitos de las aplicaciones Win32

Puede crear reglas de requisitos basadas en los scripts de PowerShell, los valores del Registro y la información del sistema de archivos. En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > **Agregar**. Después, seleccione **Aplicación de Windows (Win32)** como **Tipo de aplicación** en la hoja **Agregar aplicación**. Seleccione **Requisitos** > **Agregar** para configurar más reglas de requisitos. Después, seleccione **Tipo de archivo**, **Registro** o **Script** como **Tipo de requisito**. Para más información, vea Administración de aplicaciones Win32.

Configurar las aplicaciones Win32 para instalarlas en dispositivos unidos a Azure AD inscritos en Intune

Puede asignar las aplicaciones Win32 para instalarlas en dispositivos unidos a Azure AD inscritos en Intune. Para

más información sobre las aplicaciones Win32 en Intune, vea Administración de aplicaciones Win32.

Usuario primario mostrado en Resumen del dispositivo

La página Resumen del dispositivo mostrará el usuario primario, también denominado el usuario de afinidad de dispositivo de usuario (UDA). Para ver el usuario primario de un dispositivo, seleccione **Intune** > **Dispositivos** > **Todos los dispositivos** y elija un dispositivo. El usuario primario se muestra cerca de la parte superior de la página **Resumen**.

Otros informes de aplicaciones de Google Play administrado para dispositivos de perfil de trabajo de Android Enterprise

Para aplicaciones de Google Play administrado implementadas en dispositivos de perfil de trabajo de Android Enterprise, puede ver el número de versión específica de la aplicación instalada en un dispositivo. Esto se aplica solo a las aplicaciones necesarias.

Teclados de terceros de iOS

La compatibilidad de la directiva de protección de aplicaciones (APP) de Intune con la configuración **Teclados de terceros** para iOS ya no se admite debido a un cambio de la plataforma iOS. No podrá configurar esta opción en la consola de administración de Intune y no se aplicará en el cliente en el SDK de aplicaciones de Intune.

Configuración del dispositivo

Conectores de certificado actualizados

Se han publicado actualizaciones para Intune Certificate Connector y el conector de certificados PFX para Microsoft Intune. Las nuevas versiones corrigen varios problemas conocidos.

Establecer configuración de inicio de sesión y opciones de reinicio de control en dispositivos macOS

En dispositivos macOS, puede crear un perfil de configuración de dispositivos (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > elija **macOS** como plataforma > **Características del dispositivo** para tipo de perfil). Esta actualización incluye una nueva configuración de la ventana de inicio de sesión, como mostrar un encabezado personalizado, elegir cómo inician sesión los usuarios, mostrar u ocultar la configuración de energía y mucho más.

Para ver esta configuración, vaya a macOS device feature settings (Configuración de características de dispositivos macOS).

Configurar Wi-Fi en Android Enterprise para dispositivos dedicados de propietario del dispositivo que se ejecutan en pantalla completa con varias aplicaciones

Puede habilitar la configuración de propietario del dispositivo en Android Enterprise cuando se ejecuta como un dispositivo dedicado en pantalla completa con varias aplicaciones. En esta actualización, puede permitir que los usuarios configuren y se conecten a Wi-Fi (**Intune** > **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** para la plataforma > **Solo el propietario del dispositivo, Restricciones de dispositivo** para el tipo de perfil > **Dispositivos dedicados** > **Pantalla completa**: **Varias aplicaciones** > **Configuración de Wi-Fi**).

Para ver todos los valores que puede configurar, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características.

Se aplica a: Dispositivos dedicados de Android Enterprise que se ejecutan en pantalla completa con varias aplicaciones

Configurar Bluetooth y emparejamiento en Android Enterprise para dispositivos dedicados de propietario del dispositivo que se ejecutan en pantalla completa con varias aplicaciones

Puede habilitar la configuración de propietario del dispositivo en Android Enterprise cuando se ejecuta como un dispositivo dedicado en pantalla completa con varias aplicaciones. En esta actualización, puede permitir que los usuarios finales habiliten Bluetooth y emparejen sus dispositivos mediante Bluetooth (**Intune** > **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** para la plataforma > **Solo el propietario del dispositivo, Restricciones de dispositivo** para el tipo de perfil > **Dispositivos dedicados** > **Pantalla completa**: **Varias aplicaciones** > **Configuración de Bluetooth**).

Para ver todos los valores que puede configurar, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características.

Se aplica a: Dispositivos dedicados de Android Enterprise que se ejecutan en pantalla completa con varias aplicaciones

Crear y usar perfiles de configuración de dispositivos OEMConfig en Intune

En esta actualización, Intune admite la configuración de dispositivos Android Enterprise con OEMConfig. En concreto, puede crear un perfil de configuración de dispositivo y aplicar la configuración a los dispositivos Android Enterprise mediante OEMConfig (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** para la plataforma).

Actualmente, la compatibilidad con fabricantes de equipos originales depende del fabricante. Si quiere una aplicación OEMConfig que no está disponible en la lista de aplicaciones OEMConfig, póngase en contacto con `IntuneOEMConfig@microsoft.com`.

Para más información sobre esta característica, vaya a Use and manage Android Enterprise devices with OEMConfig in Microsoft Intune (Uso y administración de dispositivos Android Enterprise con OEMConfig en Microsoft Intune).

Se aplica a: Android Enterprise

Notificaciones de Windows Update

Se han agregado dos valores de *Configuración de la experiencia de usuario* a las configuraciones de anillo de Windows Update que puede administrar desde la consola de Intune. Ahora puede:

- Bloquear o permitir que los usuarios busquen actualizaciones de Windows.
- Administrar el nivel de notificación de Windows Update que los usuarios pueden ver.

Nueva configuración de restricción de dispositivos para Propietario del dispositivo en Android Enterprise

En dispositivos Android Enterprise, puede crear un perfil de restricción de dispositivos para permitir o restringir características, establecer reglas de contraseña y mucho más (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > elija **Android Enterprise** para plataforma > **Solo el propietario del dispositivo** > **Restricciones de dispositivos** para el tipo de perfil).

Esta actualización incluye nuevas opciones de contraseña, permite el acceso completo a las aplicaciones en Google Play Store para dispositivos totalmente administrados y mucho más. Para ver la lista actual de configuraciones, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características.

Se aplica a: Dispositivos totalmente administrados de Android Enterprise

Buscar un conjunto de chips TPM en una directiva de cumplimiento de dispositivos Windows 10

El lanzamiento de esta característica se ha retrasado y está previsto que sea más adelante.

Cambios de la interfaz de usuario actualizada para el explorador Microsoft Edge en dispositivos con Windows 10 y versiones posteriores

Cuando se crea un perfil de configuración de dispositivo, puede permitir o restringir las características de Microsoft Edge en dispositivos con Windows 10 y versiones posteriores (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Restricciones de dispositivos** para el tipo de perfil > **Explorador Microsoft Edge**). En esta actualización, la configuración de Microsoft Edge es más descriptiva y fácil de entender.

Para ver estas características, vaya a Configuración de restricción de dispositivos del explorador Microsoft Edge.

Se aplica a:

- Windows 10 y versiones posteriores
- Microsoft Edge versión 45 y anteriores

Compatibilidad ampliada para dispositivos totalmente administrados de Android Enterprise (versión preliminar)

Aún en versión preliminar pública, hemos ampliado la compatibilidad de dispositivos totalmente administrados de Android Enterprise. Se anunció por primera vez en enero de 2019 para incluir lo siguiente:

- En dispositivos totalmente administrados y dedicados, puede crear directivas de cumplimiento para incluir las reglas de contraseña y requisitos del sistema operativo (**Cumplimiento del dispositivo** > **Directivas** > **Crear directiva** > **Android Enterprise** para plataforma > **Propietario del dispositivo** para tipo de perfil).

  En dispositivos dedicados, el dispositivo puede aparecer como **No compatible**. El acceso condicional no está disponible en dispositivos dedicados. Asegúrese de completar las tareas o acciones para obtener dispositivos dedicados compatibles con las directivas asignadas.

- Acceso condicional: las directivas de acceso condicional que se aplican a Android también se aplican a dispositivos totalmente administrados de Android Enterprise. Los usuarios ahora pueden registrar su dispositivo totalmente administrado en Azure Active Directory mediante la **aplicación Microsoft Intune**. Después, pueden ver y resolver los problemas de cumplimiento para acceder a recursos de la organización.

- Nueva aplicación de usuario final (aplicación Microsoft Intune): hay una nueva aplicación de usuario final para dispositivos Android totalmente administrados denominada **Microsoft Intune**. Esta nueva aplicación, ligera y moderna, ofrece funciones similares a las de la aplicación Portal de empresa, pero para dispositivos totalmente administrados. Para más información, vea la aplicación Microsoft Intune en Google Play.

Para configurar dispositivos Android totalmente administrados, vaya a **Dispositivo administrado** > **Inscripción de Android** > **Corporate-owned, fully managed user devices** (Dispositivos de usuario totalmente administrados de propiedad corporativa). La compatibilidad con dispositivos Android totalmente administrados sigue en versión preliminar y algunas características de Intune podrían no ser totalmente funcionales.

Para más información sobre esta versión preliminar, lea nuestro blog Microsoft Intune - Versión preliminar 2 para dispositivos totalmente administrados de Android Enterprise.

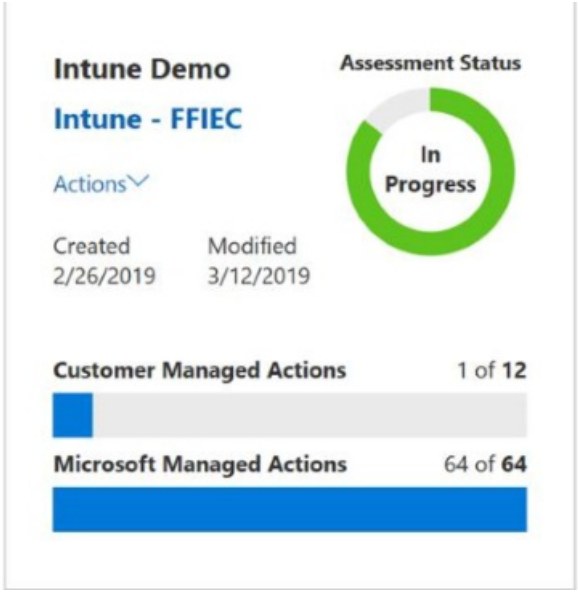
Usar el Administrador de cumplimiento para crear evaluaciones para Microsoft Intune

El Administrador de cumplimiento (abre otro sitio de Microsoft) es una herramienta de evaluación de riesgos según el flujo de trabajo que se encuentra en el Portal de confianza de servicios de Microsoft. Permite asignar y comprobar las actividades de cumplimiento normativo de la organización relacionadas con los servicios de Microsoft, y realizar un seguimiento de dichas actividades. Puede crear su propia evaluación de cumplimiento con Microsoft 365, Azure, Dynamics, Servicios profesionales e Intune. Intune tiene dos evaluaciones disponibles: FFIEC y RGPD.

Con el Administrador de cumplimiento es más fácil centrarse en las actividades, ya que divide los controles en controles administrados por Microsoft y controles administrados por la organización. Permite completar las evaluaciones y, después, exportarlas e imprimirlas.

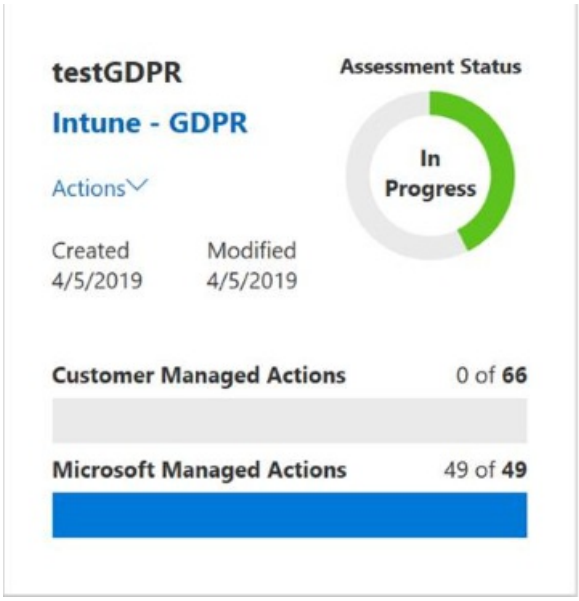
El cumplimiento normativo del Consejo federal de examen de instituciones financieras (FFIEC, del inglés Federal Financial Institutions Examination Council) (abre otro sitio de Microsoft) es un conjunto de estándares para la banca electrónica emitido por el FFIEC. Es la evaluación para instituciones financieras más solicitada que se usa en Intune. Interpreta cómo Intune le permite cumplir las directrices de ciberseguridad del FFIEC relacionadas con cargas de trabajo en la nube pública. La evaluación del FFIEC de Intune es la segunda evaluación del FFIEC en el Administrador de cumplimiento.

En este ejemplo puede ver el desglose de los controles del FFIEC. Microsoft abarca 64 controles. El usuario se encarga de los 12 controles restantes.



El Reglamento general de protección de datos (RGPD) (abre otro sitio de Microsoft) es una ley de la Unión Europea (UE) que permite proteger los derechos de los usuarios y sus datos. El RGPD es la evaluación más solicitada para cumplir con las normas de privacidad.

En este ejemplo puede ver el desglose de los controles del RGPD. Microsoft abarca 49 controles. El usuario se encarga de los 66 controles restantes.



Inscripción de dispositivos

Configuración del perfil para omitir algunas pantallas durante el Asistente para configuración

Cuando se crea un perfil de inscripción de macOS, se puede configurar para que omita cualquiera de las siguientes pantallas cuando un usuario realiza los pasos del Asistente para configuración:

- Aspecto
- Tono de visualización
- iCloudStorage: si crea un nuevo perfil o edita uno, las pantallas de omisión seleccionadas deben sincronizarse con el servidor MDM de Apple. Los usuarios pueden emitir una sincronización manual de los dispositivos para que no haya ningún retraso en la recogida de los cambios de perfil. Para más información, consulte el artículo Inscripción automática de dispositivos macOS con el Programa de inscripción de dispositivos o Apple School Manager.

Asignar nombres en masa a dispositivos al inscribir dispositivos iOS corporativos

Al usar uno de los métodos de inscripción corporativa de Apple (DEP/ABN/ASM), puede establecer un formato

de nombre de dispositivo para que asigne un nombre automáticamente a los dispositivos iOS entrantes. Puede especificar un formato que incluya el tipo de dispositivo y el número de serie en la plantilla. Para hacerlo, elija **Intune** > **Inscripción de dispositivos** > **Inscripción de Apple** > **Tokens del programa de inscripción** > **Seleccione un token** >**Crear perfil** > **Formato de nomenclatura de dispositivo**. Puede editar los perfiles existentes, pero el nombre se aplicará solamente a los dispositivos que acaba de sincronizar.

Actualizado el mensaje de tiempo de espera predeterminado en la página de estado de inscripción

Hemos actualizado el mensaje de tiempo de espera predeterminado que se muestra a los usuarios cuando la página de estado de inscripción (ESP) supera el valor de tiempo de espera especificado en el perfil de ESP. El nuevo mensaje predeterminado es lo que los usuarios ven y les permite comprender las siguientes acciones que deben realizar con su implementación de ESP.

Administración de dispositivos

Retirar dispositivos no compatibles

Esta característica se ha retrasado y se incluirá en una versión futura.

Supervisión y solución de problemas

Cambios de Intune Data Warehouse V1.0 reflejados hasta la versión beta

Cuando V1.0 apareció por primera vez en agosto de 2018, difería en algunos aspectos importantes de la versión beta de API. En marzo de 2019 esos cambios se reflejan en la versión beta de la API. Si tiene informes importantes que usan la versión beta de API, se recomienda encarecidamente cambiar dichos informes a V1.0 para evitar cambios bruscos. Para más información, vea Registro de cambios en la API Almacenamiento de datos de Intune.

Supervisar el estado de las líneas bases de seguridad (versión preliminar)

Hemos agregado una vista por categorías para la supervisión de las líneas bases de seguridad. (Las líneas base de seguridad siguen en versión preliminar). La vista por categorías muestra cada categoría desde la línea base junto con el porcentaje de dispositivos que pertenecen a cada grupo de estado para esa categoría. Ahora puede ver cuántos dispositivos no coinciden con las categorías individuales, están mal configurados o no son aplicables.

Control de acceso basado en roles.

Etiquetas de ámbito para los tokens del Programa de compras por volumen (VPP) de Apple

Ahora puede agregar etiquetas de ámbito a los tokens de VPP de Apple. Solo los usuarios que tienen asignada la misma etiqueta de ámbito tendrán acceso al token de VPP de Apple con esa etiqueta. Las aplicaciones y libros electrónicos de VPP comprados con ese token heredan sus etiquetas de ámbito. Para más información sobre las etiquetas de ámbito, vea Use RBAC and scope tags (Usar RBAC y etiquetas de ámbito).

Marzo de 2019

Administración de aplicaciones

Implementar Microsoft Visio y Microsoft Project

Ahora puede implementar Microsoft Visio Pro para Microsoft 365 y el cliente de escritorio de Microsoft Project Online como aplicaciones independientes para dispositivos Windows 10 con Microsoft Intune, si dispone de licencias para estas aplicaciones. En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > **Agregar** para mostrar la hoja **Agregar aplicación**. En la hoja **Agregar aplicación**, seleccione **Windows 10** como **Tipo de aplicación**. Después, elija **Configurar conjunto de aplicaciones** para seleccionar las aplicaciones que instalará. Para obtener más información sobre las aplicaciones de Microsoft 365 para dispositivos Windows 10, vea Asignación de aplicaciones de Microsoft 365 a dispositivos Windows 10 con Microsoft Intune.

Cambio de nombre de producto de Microsoft Visio Pro para Office 365

Microsoft Visio Pro para Office 365 ahora se conocerá como **Microsoft Visio Online Plan 2**. Para más información sobre Microsoft Visio, vea Visio Online Plan 2. Para más información sobre cómo las aplicaciones de Office 365 para dispositivos Windows 10, vea Asignación de aplicaciones de Office 365 a dispositivos Windows 10 con Microsoft Intune.

Configuración de límite de caracteres de la directiva de protección de aplicaciones (APP) de Intune

Los administradores de Intune pueden especificar una excepción en la configuración de la directiva **Restringir cortar, copiar y pegar con otras aplicaciones** de la APP de Intune. También pueden especificar el número de caracteres que se pueden cortar o copiar de una aplicación administrada. Esto permitirá compartir el número especificado de caracteres en cualquier aplicación, independientemente de la opción "Restringir cortar, copiar y pegar con otras aplicaciones". Tenga en cuenta que para la aplicación Portal de empresa de Intune para Android se necesita la versión 5.0.4364.0 o posterior. Para más información, vea Configuración de directivas de protección de aplicaciones de iOS, Configuración de directivas de protección de aplicaciones Android en Microsoft Intune y Revisión de los registros de protección de aplicaciones cliente.

XML de la Herramienta de implementación de Office (ODT) para Aplicaciones de Microsoft 365 para el desarrollo empresarial

Será capaz de proporcionar el XML de la Herramienta de implementación de Office (ODT) al crear una instancia de Aplicaciones de Microsoft 365 para el desarrollo empresarial en la consola de administración de Intune. Esto permite mayor capacidad de personalización si las opciones actuales de la interfaz de usuario de Intune no satisfacen sus necesidades. Para obtener más información, vea Asignación de aplicaciones de Microsoft 365 a dispositivos Windows 10 con Microsoft Intune y Opciones de configuración de la Herramienta de implementación de Office.

Los iconos de aplicación se mostrarán con un fondo generado automáticamente

En la aplicación Portal de empresa, ahora los iconos de aplicación se muestran con un fondo generado automáticamente según el color dominante del icono (si se puede detectar). Si procede, este fondo reemplaza el borde gris que antes se veía en los iconos de aplicación. Los usuarios verán este cambio en las versiones posteriores de Portal de empresa posteriores a 10.3.3451.0.

Instalar aplicaciones disponibles mediante la aplicación Portal de empresa después de la inscripción masiva de dispositivos Windows

Los dispositivos Windows inscritos en Intune mediante Inscripción masiva de Windows (paquetes de aprovisionamiento) podrán usar la aplicación Portal de empresa para instalar aplicaciones disponibles. Para más información sobre cómo configurar la aplicación Portal de empresa, vea Adición manual de la aplicación Portal de empresa para Windows 10 con Microsoft Intune y Configuración de la aplicación Portal de empresa de Microsoft Intune.

Posibilidad de seleccionar la aplicación Microsoft Teams como parte del conjunto de aplicaciones de Office

La aplicación Microsoft Teams se puede incluir o excluir como parte de la instalación del conjunto de Aplicaciones de Microsoft 365 para la implementación empresarial. Esta característica funciona para las Aplicaciones de Microsoft 365 para la implementación empresarial con el número de compilación 16.0.11328.20116+. El usuario debe cerrar sesión y después iniciar sesión en el dispositivo para que se complete la instalación. En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > **Agregar**. Seleccione uno de los tipos de aplicación del **Conjunto de aplicaciones Office 365** y elija **Configurar conjunto de aplicaciones**.

Configuración del dispositivo

Iniciar automáticamente una aplicación cuando se ejecutan varias aplicaciones en modo de pantalla completa en dispositivos con Windows 10 y versiones posteriores

En dispositivos con Windows 10 y versiones posteriores, puede ejecutar un dispositivo en modo de pantalla completa y ejecutar muchas aplicaciones. En esta actualización, hay un valor **Ejecución automática** configuración (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para plataforma > **Pantalla completa** para el tipo de perfil > **Pantalla completa con varias aplicaciones**). Con este valor se puede iniciar automáticamente una aplicación cuando el usuario inicia sesión en el dispositivo.

Para ver una lista y una descripción de todos los valores de pantalla completa, vea Windows 10 and later device settings to run as a kiosk in Intune (Configuración de dispositivos con Windows 10 y versiones posteriores para ejecutarlos en pantalla completa en Intune).

Se aplica a: Windows 10 y versiones posteriores

Registros operativos también muestran detalles en dispositivos no compatibles

Al enrutar registros de Intune a características de supervisión de Azure, también puede enrutar los registros operativos. En esta actualización, los registros operativos también proporcionan información sobre los dispositivos no compatibles.

Para más información sobre esta característica, vea Envío de datos de registro al almacenamiento, a Event Hubs o a Log Analytics en Intune (versión preliminar).

Enrutar registros a Azure Monitor en más cargas de trabajo de Intune

En Intune, puede enrutar los registros operativos y de auditoría a centros de eventos, almacenamiento y análisis de registros en Azure Monitor (**Intune** > **Supervisión** > **Configuración de diagnósticos**). En esta actualización, puede enrutar estos registros en más cargas de trabajo de Intune, incluido el cumplimiento, las configuraciones, las aplicaciones cliente y mucho más.

Para más información sobre el enrutamiento de registros a Azure Monitor, vea Envío de datos de registro al almacenamiento, a Event Hubs o a Log Analytics en Intune (versión preliminar).

Crear y usar extensiones de movilidad en dispositivos Android Zebra en Intune

En esta actualización, Intune admite la configuración de dispositivos Android Zebra. En concreto, puede crear un perfil de configuración de dispositivo y aplicar la configuración a dispositivos Android Zebra mediante perfiles de movilidad extensiones (MX) generados por StageNow (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android** para plataforma > **Perfil de MX (solo Zebra)** para tipo de perfil).

Para más información sobre esta característica, vea Use and manage Zebra devices with mobility extensions in Intune (Uso y administración de dispositivos Zebra con extensiones de movilidad en Intune).

Se aplica a: Android

Administración de dispositivos

Informe de cifrado para dispositivos Windows 10 (en versión preliminar pública)

Use la nueva opción Informe de cifrado (vista previa) para ver los detalles sobre el estado de cifrado de los dispositivos Windows 10. Entre los detalles disponibles se incluye una versión de TPM de los dispositivos, el estado y la preparación para cifrado, informes de errores y mucho más.

Acceder a claves de recuperación de BitLocker desde el portal de Intune (en versión preliminar pública)

Ahora puede usar Intune para ver detalles sobre el identificador de clave de BitLocker y las claves de recuperación de BitLocker, desde Azure Active Directory.

Compatibilidad de Microsoft Edge con escenarios de Intune en dispositivos iOS y Android

Microsoft Edge será compatible con los mismos escenarios de administración que Intune Managed Browser con la adición de mejoras en la experiencia del usuario final. Entre las características para empresas de Microsoft Edge que se habilitan mediante las directivas de Intune se incluyen la identidad dual, la integración de la directiva de protección de aplicaciones, la integración del proxy de aplicación de Azure, favoritos administrados y accesos directos a la página principal. Para más información, vea Compatibilidad con Microsoft Edge.

Exchange Online y Conector de Intune retiran su compatibilidad para dispositivos EAS solamente

La consola de Intune ya no admite la visualización y la administración de dispositivos de EAS solamente conectados a Exchange Online con el Conector de Intune. Dispone de estas otras opciones:

- Inscribir dispositivos en Administración de dispositivos móviles (MDM)
- Usar las directivas de Intune App Protection para administrar los dispositivos
- Usar controles de Exchange como se describe en Clients and mobile in Exchange Online (Clientes y dispositivos móviles en Exchange Online)

Buscar la página Todos los dispositivos para un dispositivo concreto mediante el uso de [nombre]

Ahora puede buscar un nombre de dispositivo exacto. Vaya a **Intune** > **Dispositivos** > **Todos los dispositivos** > en el cuadro de búsqueda, escriba el nombre de dispositivo entre {} para buscar una coincidencia exacta. Por ejemplo, **{Device12345}** .

Supervisión y solución de problemas

Compatibilidad con conectores adicionales en la página Estado del inquilino

La página Estado del inquilino ahora muestra información de estado de los conectores adicionales, incluidos *Windows Defender for Endpoint* y otros conectores de Mobile Threat Defense.

Compatibilidad con la aplicación de cumplimiento de Power BI en la hoja Almacenamiento de datos en Microsoft Intune

Antes, el vínculo **Descargar archivo de Power BI** en la hoja **Almacenamiento de datos de Intune** descargaba un informe de Almacenamiento de datos de Intune (archivo .pbix). Este informe se ha reemplazado por la aplicación de cumplimiento de Power BI. Para la aplicación de cumplimiento de Power BI no se necesitará ninguna configuración o carga especial. Se abrirá directamente en el portal en línea de Power BI y mostrará datos específicamente para el inquilino de Intune según sus credenciales. En Intune, seleccione el vínculo **Configurar el almacenamiento de datos de Intune** en el lado derecho de la hoja de Intune. Después, haga clic en **Obtener aplicación de Power BI**. Para más información, vea Connect to the Data Warehouse with Power BI (Conectarse al almacenamiento de datos con Power BI).

Control de acceso basado en roles.

Concesión del acceso de solo lectura a Intune a algunos roles de Azure Active Directory

Se ha concedido acceso de solo lectura de Intune a estos roles de Azure AD. Los permisos concedidos con roles de Azure AD sustituyen a los permisos concedidos con control de acceso basado en roles (RBAC) de Intune.

Acceso de solo lectura a los datos de auditoría de Intune:

- Administrador de cumplimiento
- Administrador de datos de cumplimiento

Acceso de solo lectura a todos los datos de Intune:

- Administrador de seguridad
- Operador de seguridad
- Lector de seguridad

Para más información, vea Control de acceso basado en roles.

Etiquetas de ámbito para perfiles de aprovisionamiento de aplicaciones iOS

Puede agregar una etiqueta de ámbito a un perfil de aprovisionamiento de aplicaciones iOS para que solo los usuarios con roles que también tengan asignada esa etiqueta de ámbito puedan acceder al perfil de aprovisionamiento de aplicaciones iOS. Para más información, vea Use RBAC and scope tags (Usar RBAC y etiquetas de ámbito).

Etiquetas de ámbito para directivas de configuración de aplicaciones

Puede agregar una etiqueta de ámbito a una directiva de configuración de aplicaciones para que solo los usuarios con roles que también tengan asignada esa etiqueta de ámbito puedan acceder a la directiva de configuración de aplicaciones. La directiva de configuración de aplicaciones solo puede asociarse a aplicaciones que tengan asignada la misma etiqueta de ámbito. Para más información, vea Use RBAC and scope tags (Usar RBAC y etiquetas de ámbito).

Compatibilidad de Microsoft Edge con escenarios de Intune en dispositivos iOS y Android

Microsoft Edge será compatible con los mismos escenarios de administración que Intune Managed Browser con la adición de mejoras en la experiencia del usuario final. Entre las características para empresas de Microsoft Edge que se habilitan mediante las directivas de Intune se incluyen la identidad dual, la integración de la directiva de protección de aplicaciones, la integración del proxy de aplicación de Azure, favoritos administrados y accesos directos a la página principal. Para más información, vea Compatibilidad con Microsoft Edge.

Febrero de 2019

Administración de aplicaciones

Modo oscuro del Portal de empresa de macOS para Intune

El Portal de empresa de macOS para Intune ahora admite el Modo oscuro para macOS. Cuando habilita el Modo oscuro en un dispositivo macOS 10.14 o una versión posterior, el Portal de empresa ajustará su apariencia para que los colores reflejen ese modo.

Intune aprovechará las API de Google Play Protect en dispositivos Android

Algunos administradores de TI se enfrentan a un panorama BYOD donde los usuarios finales pueden acabar por obtener privilegios de usuario root o realizar jailbreaking en sus teléfonos móviles. Este comportamiento, aunque en ocasiones no sea malintencionado, tiene como resultado la omisión de muchas directivas de Intune que se establecen con el fin de proteger los datos de la organización en los dispositivos de los usuarios finales. Por tanto, Intune proporciona la detección de jailbreak y de obtención de permisos de usuario root para los dispositivos inscritos y no inscritos. Con esta versión, ahora Intune aprovechará las API de Google Play Protect para agregarlas a nuestras comprobaciones de detección de modificaciones existentes para los dispositivos no inscritos. Aunque Google no comparte la totalidad de las comprobaciones de detección de modificaciones que se producen, esperamos que estas API detecten los usuarios que han modificado sus dispositivos por cualquier motivo, desde la personalización del dispositivo a la obtención de las actualizaciones más recientes del sistema operativo en dispositivos más antiguos. Después, se puede bloquear el acceso de estos usuarios a los datos corporativos, o bien se pueden eliminar sus cuentas de empresa desde sus aplicaciones habilitadas para la directiva. Para obtener valor adicional, ahora los administradores de TI tendrán varias actualizaciones de informes en la hoja Protección de aplicaciones de Intune: en el informe "Usuarios marcados" se mostrarán los usuarios que se han detectado mediante el examen de la API SafetyNet de Google Play Protect, y en el informe "Aplicaciones potencialmente peligrosas" se mostrarán las aplicaciones que se hayan detectado mediante el examen de la API Verify Apps de Google. Esta característica está disponible en Android.

Información de aplicaciones Win32 disponible en la hoja Solución de problemas

Ya puede recopilar archivos de registro de errores de la instalación de una aplicación Win32 desde la hoja **Solución de problemas** de la aplicación Intune. Para más información sobre la solución de problemas de instalación de aplicaciones, vea Troubleshoot app installation issue (Solución de problemas de instalación de aplicaciones) y Solucionar los problemas de aplicaciones Win32.

Detalles del estado de la aplicación para aplicaciones iOS

Hay nuevos mensajes de error de instalación de aplicaciones relacionados con lo siguiente:

- Error de las aplicaciones VPP cuando se instalan en un iPad compartido
- Error cuando la tienda de aplicaciones está deshabilitada
- No se puede encontrar la licencia VPP de la aplicación
- No se pueden instalar las aplicaciones del sistema con el proveedor de MDM
- No se pueden instalar aplicaciones cuando el dispositivo está en modo de pantalla completa o modo perdido
- No se puede instalar la aplicación cuando el usuario no ha iniciado sesión en la App Store

En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > "Nombre de la aplicación" > **Estado de instalación del dispositivo**. Los mensajes de error nuevos estarán disponibles en el estado **Detalles del estado**.

Nuevas pantalla de categorías de aplicaciones en la aplicación Portal de empresa para Windows 10

Se ha agregado una nueva pantalla denominada **Categorías de aplicaciones** para mejorar la experiencia de exploración y selección en la aplicación Portal de empresa para Windows 10. Los usuarios ahora verán sus aplicaciones ordenadas en categorías como **Destacadas**, **Educación** y **Productividad**. Este cambio aparece en las versiones 10.3.3451.0 y posteriores de Portal de empresa. Para ver la nueva pantalla, vea Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune. Para más información sobre las aplicaciones del Portal de empresa, vea Instalar y compartir aplicaciones en el dispositivo.

Aplicación de cumplimiento de Power BI

Acceda al almacenamiento de datos de Intune en Power BI Online mediante la aplicación Cumplimiento de Intune (Almacenamiento de datos). Con esta aplicación de Power BI, ahora puede acceder y compartir informes

creados previamente sin necesidad de configuración y sin salir de su explorador web. Para más información, vea el registro de cambios en la aplicación del cumplimiento de Power BI.

Configuración del dispositivo

Los scripts de PowerShell se pueden ejecutar en un host de 64 bits en dispositivos de 64 bits

Al agregar un script de PowerShell a un perfil de configuración de dispositivo, el script siempre se ejecuta en 32 bits, incluso en sistemas operativos de 64 bits. Con esta actualización, un administrador puede ejecutar el script en un host de PowerShell de 64 bits en dispositivos de 64 bits (**Configuración del dispositivo** > **Scripts de PowerShell** > **Agregar** > **Configurar** > **Ejecutar script en el host de PowerShell de 64 bits**).

Para obtener más detalles sobre el uso de PowerShell, vea Scripts de PowerShell en Intune.

Se aplica a: Windows 10 y versiones posteriores

Se pide a los usuarios de macOS que actualicen su contraseña

Intune está exigiendo el valor **ChangeAtNextAuth** en los dispositivos macOS. Esta opción afecta a los usuarios finales y los dispositivos que tienen directivas de contraseña de cumplimiento o perfiles de contraseña de restricción de dispositivo. Se pide a los usuarios finales que actualicen su contraseña una vez. Este mensaje se produce cada vez que un usuario realiza por primera vez una tarea que necesita autenticación, como iniciar sesión en el dispositivo. También se pide a los usuarios que actualicen su contraseña cuando hagan algo que necesite privilegios administrativos, como por ejemplo, pedir acceso a cadenas de llaves.

Cuando el administrador cambia la directiva de contraseña nueva o existente, se pide a los usuarios finales que vuelvan a actualizar su contraseña.

Se aplica a:
macOS

Asignar certificados SCEP en un dispositivo macOS sin usuarios

Puede asignar los certificados del Protocolo de inscripción de certificados simple (SCEP) mediante los atributos del dispositivo para dispositivos macOS, incluidos los dispositivos sin afinidad de usuario y asociar el perfil de certificado con perfiles de Wi-Fi o VPN. Esto amplía la compatibilidad que ya tenemos para asignar certificados del SCEP a dispositivos con y sin afinidad de usuario que tienen instalado Windows, iOS y Android. Esta actualización agrega la opción de seleccionar un tipo de certificado de *Dispositivo* al configurar un perfil de certificado SCEP para macOS.

Se aplica a:

- macOS

Actualización de la interfaz de usuario del acceso condicional de Intune

Hemos realizado mejoras en la interfaz de usuario para el acceso condicional en la consola de Intune. Entre ellos, se incluye:

- Hemos reemplazado la hoja *Acceso condicional* de Intune con la hoja de Azure Active Directory. Esto garantiza que tendrá acceso a toda la gama de opciones y configuraciones para el acceso condicional (que sigue siendo una tecnología de Azure AD) desde la consola de Intune.
- Hemos cambiado el nombre de la hoja *Acceso local* a *Acceso de Exchange* y hemos cambiado de sitio el programa de instalación del *Conector de servicio de Exchange* a esta hoja con el nuevo nombre. Este cambio consolida donde se puede configurar y supervisar los detalles relacionados con Exchange en línea y local.

Las aplicaciones de explorador del Quiosco y Microsoft Edge se pueden ejecutar en dispositivos Windows 10 en modo de pantalla completa

Puede usar dispositivos Windows 10 en modo de pantalla completa para ejecutar una o varias aplicaciones. En esta actualización se incluyen varios cambios en el uso de las aplicaciones de explorador en modo de pantalla completa, incluidos los siguientes:

- Se agrega el explorador Microsoft Edge o Kiosk Browser para que se ejecuten como aplicaciones en el

dispositivo de pantalla completa (**Configuración del dispositivo** > **Perfiles** > **Nuevo perfil** > **Windows 10 y versiones posteriores** para plataforma > **Pantalla completa** para el tipo de perfil).

- Hay disponibles nuevas características y configuraciones para permitir o restringir (**Configuración del dispositivo** > **Perfiles** > **Nuevo perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Restricciones de dispositivos** para el tipo de perfil), incluidos:
- Explorador Microsoft Edge:
  - Usar el modo de pantalla completa de Microsoft Edge
  - Actualizar el explorador después del tiempo de inactividad
- Favoritos y búsqueda:
  - Permitir cambios en el motor de búsqueda

Para obtener una lista de estos valores, vea:

- Configuración de dispositivos con Windows 10 y versiones posteriores para ejecutarse como una pantalla completa
- Restricciones de dispositivos del explorador Microsoft Edge versión 45 y anteriores
- Favoritos y restricciones de búsqueda de dispositivos

Se aplica a: Windows 10 y versiones posteriores

Nueva configuración de restricción de dispositivos para dispositivos iOS y macOS

Puede restringir algunas opciones y características de los dispositivos que ejecutan iOS y macOS (**Configuración del dispositivo** > **Perfiles** > **Nuevo perfil** > **iOS** o **macOS** para plataforma > **Restricciones de dispositivos** para tipo de perfil). En esta actualización se agregan más características y valores de configuración que puede controlar, incluida la configuración del tiempo de pantalla, el cambio de la configuración eSIM, planes de telefonía móvil y mucho más en dispositivos iOS. También la opción de retrasar la visibilidad para el usuario de las actualizaciones de software y el bloqueo de almacenamiento en caché de contenido en dispositivos macOS.

Para ver las características y la configuración que se pueden restringir, vea:

- Configuración de restricciones de dispositivos iOS
- Configuración de restricciones de dispositivos macOS

Se aplica a:

- iOS
- macOS

Los dispositivos de "Pantalla completa" ahora se denominan "Dispositivos dedicados" en dispositivos Android Enterprise

Para alinear con la terminología de Android, **Pantalla completa** cambia a **Dispositivos dedicados** para dispositivos Android Enterprise (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > ** Android Enterprise para la plataforma > **Solo el propietario del dispositivo** > **Restricciones de dispositivos** > **Dispositivos dedicados**).

Para ver los valores disponibles, vaya a Android Enterprise device settings to allow or restrict features using Intune (Configuración de dispositivos Android Enterprise para permitir o restringir características con Intune).

Se aplica a:
Android Enterprise

Las opciones de Safari y Retrasar la visibilidad de las actualizaciones de software iOS se cambian a la interfaz de usuario de Intune

Para los dispositivos iOS, puede establecer la configuración de Safari y configurar actualizaciones de software. En esta actualización, estas opciones se van a cambiar a otra partes de la interfaz de usuario de Intune:

- La configuración de Safari cambia de **Safari** (**Configuración del dispositivo** > **Perfiles** > **Nuevo perfil** > **iOS** para la plataforma > **Restricciones de dispositivos** para el tipo de perfil) a **Aplicaciones integradas** .
- La opción **Delaying user software update visibility for supervised iOS devices** (Retrasar la visibilidad de las actualizaciones de software para los dispositivos iOS supervisados) (**Actualizaciones de software** > **Directivas de actualización para iOS**) se va a cambiar a **Restricciones de dispositivos** > **General** . Para más información sobre el impacto en las directivas existentes, vea Configuración de directivas de actualización de iOS en Intune.

Para obtener una lista de estos valores, vea:

- Restricciones de dispositivos iOS
- Actualizaciones del software iOS

Esta característica se aplica a:

- iOS

En los dispositivos iOS se ha cambiado el nombre de Habilitar restricciones en la configuración del dispositivo por Tiempo de uso

Puede configurar **Habilitar restricciones en la configuración del dispositivo** en dispositivos iOS supervisados (**Configuración del dispositivo** > **Perfiles** > **Nuevo perfil** > **iOS** para plataforma > **Restricciones de dispositivos** para tipo de perfil > **General**). En esta actualización, se ha cambiado el nombre de esta opción por **Tiempo de uso (solo con supervisión)** .

El comportamiento es el mismo. De manera específica:

- iOS 11.4.1 y versiones anteriores: **Bloquear** impide que los usuarios finales establezcan sus propias restricciones en la configuración del dispositivo.
- iOS 12.0 y versiones posteriores: **Bloquear** impide que los usuarios finales establezcan su propio **Tiempo de uso** en la configuración del dispositivo, incluidas las restricciones de contenido y privacidad. En los dispositivos actualizados a iOS 12.0 ya no aparecerá la pestaña Restricciones en la configuración del dispositivo. Estas opciones se encuentran en **Tiempo de uso**.

Para obtener una lista de los valores, vea Restricciones de dispositivos iOS.

Se aplica a:

- iOS

Módulo de PowerShell de Intune

El módulo de PowerShell de Intune, que proporciona compatibilidad con la API de Intune a través de Microsoft Graph, ya está disponible en la Galería de Microsoft PowerShell.

- Detalles sobre cómo usar este módulo
- Ejemplos de escenarios de uso de este módulo

Compatibilidad mejorada para la optimización de entrega

Hemos ampliado la compatibilidad de Intune para configurar la optimización de entrega. Ahora puede configurar una lista expandida de Configuración de optimización de entrega y aplicarla a los dispositivos directamente desde la consola de Intune.

Administración de dispositivos

Cambio del nombre de un dispositivo Windows inscrito

Ahora puede cambiar el nombre de un dispositivo Windows 10 inscrito (RS4 o posterior). Para ello, seleccione **Intune** > **Dispositivos** > **Todos los dispositivos** > elija un dispositivo > **Cambiar el nombre del dispositivo**. Esta característica no es compatible actualmente con el cambio de nombre de dispositivos Windows híbridos con Azure AD.

Asignación automática de etiquetas de ámbito a los recursos creados por un administrador con ese ámbito

Cuando un administrador crea un recurso, las etiquetas de ámbito asignadas al administrador se asignarán de forma automática a esos recursos nuevos.

Supervisión y solución de problemas

El informe Errores de inscripción se mueve a la hoja Inscripción de dispositivos

El informe **Errores de inscripción** se ha movido a la sección **Supervisar** de la hoja **Inscripción de dispositivos**. Se han agregado dos columnas nuevas (Método de inscripción y Versión del sistema operativo).

Se ha cambiado el nombre del informe Abandono del Portal de empresa a Inscripciones de usuario incompletas

Se ha cambiado el nombre del informe **Abandono del Portal de empresa** a **Inscripciones de usuario incompletas**.

Enero de 2019

Administración de aplicaciones

PIN de aplicación de Intune

Como administrador de TI, podrá configurar el número de días que un usuario final puede esperar hasta que se tenga que cambiar el PIN de aplicación de Intune. La nueva configuración es *Restablecimiento del PIN después de un número de días* y está disponible en Azure Portal; para acceder a esta configuración, seleccione **Intune** > **Aplicaciones cliente** > **Directivas de protección de aplicaciones** > **Crear directiva** > **Configuración** > **Requisitos de acceso**. Esta característica está disponible para dispositivos iOS y Android, y admite un valor entero positivo.

Campos de informes de dispositivo de Intune

Intune proporciona campos adicionales con información sobre el dispositivo, como el identificador de registro de aplicación, el fabricante de Android, el modelo, la versión de la revisión de seguridad y el modelo de iOS. En Intune, estos campos estarán disponibles en **Aplicaciones cliente** > **Estado de protección de aplicaciones** y **Informe de protección de aplicaciones: iOS, Android**. Además, estos parámetros lo ayudarán a configurar la lista de **admitidos** correspondiente al fabricante de dispositivo (Android), la lista de **admitidos** del modelo de dispositivo (iOS y Android) y la configuración de versión de la revisión de seguridad mínima de Android.

Notificaciones del sistema para aplicaciones Win32

Puede suprimir notificaciones del sistema para el usuario final por asignación de aplicaciones. En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > seleccione la aplicación > **Asignaciones** > **Incluir grupos**.

Actualización de la interfaz de usuario de las directivas de protección de aplicaciones de Intune

Hemos cambiado las etiquetas para las opciones y los botones de la protección de aplicaciones de Intune para que sean más fáciles de entender. Algunos de los cambios son:

- Los controles han cambiado de **sí** / **no** a principalmente **bloquear** / **permitir** y **deshabilitar** / **habilitar**. Las etiquetas también se actualizaron.
- Se cambió el formato de las opciones, de tal forma que la opción y su etiqueta aparezcan una al lado de la otra en el control, para así facilitar la navegación.

La configuración predeterminada y el número de opciones se conservan, pero este cambio permite al usuario entender, navegar y utilizar la configuración con más facilidad para aplicar las directivas de protección de aplicaciones seleccionadas. Para información, consulte la configuración para iOS y la configuración para Android.

Configuración adicional para Outlook

Ahora puede cambiar estos otros valores de configuración de Outlook para iOS y Android mediante Intune:

- Permitir que solo se usen cuentas profesionales o educativas en iOS y Android.

- Implementar la autenticación moderna para Microsoft 365 y la autenticación moderna híbrida para cuentas locales.
- Usar `SAMAccountName` para el campo de nombre de usuario en el perfil de correo electrónico al tener seleccionada la autenticación básica.
- Permitir que se guarden contactos.
- Configurar información sobre el correo electrónico de destinatarios externos.
- Configurar la **Bandeja de entrada Prioritarios**.
- Requerir autenticación biométrica para acceder a Outlook para iOS.
- Bloquear las imágenes externas.

> **NOTE**
> Si usa directivas de Intune App Protection para administrar el acceso de las identidades corporativas, le recomendamos que no habilite el **requisito de autenticación biométrica**. Para más información, vea **Requerir credenciales corporativas en acceso**, en los artículos relativos a la configuración de acceso de iOS y la configuración de acceso de Android, respectivamente.

Para más información, vea Opciones de configuración de Microsoft Outlook.

Eliminación de aplicaciones de Android Enterprise

Puede eliminar aplicaciones de Google Play administrado desde Microsoft Intune. Para eliminar una aplicación de Google Play administrado, abra Microsoft Intune en Azure Portal y seleccione **Aplicaciones cliente** > **Aplicaciones**. En la lista de aplicaciones, seleccione los puntos suspensivos (...) a la derecha de la aplicación de Google Play administrado y luego seleccione **Eliminar** en la lista que aparece. Cuando se elimina una aplicación de Google Play administrada de la lista de aplicaciones, automáticamente se desactiva la aprobación de la aplicación administrada de Google Play.

Tipo de aplicaicón de Google Play administrado

El tipo de aplicación **administrada de Google Play** le permitirá agregar específicamente aplicaciones de Google Play administradas a Intune. Como administrador de Intune, ahora podrá examinar, buscar, aprobar, sincronizar y asignar aplicaciones de Google Play administrado aprobadas dentro de Intune. Ya no necesita ir a la consola de Google Play administrado por separado ni tiene que volver a autenticarse. En Intune, seleccione **Aplicaciones cliente** > **Aplicaciones** > **Agregar**. En la lista **Tipo de aplicación**, seleccione **Google Play administrada** como tipo de aplicación.

Teclado de PIN de Android predeterminado

Los usuarios finales que hayan establecido un PIN de directiva de Intune App Protection (APP) en sus dispositivos Android con el tipo de PIN "Numérico" ahora verán el teclado de Android predeterminado en lugar de la interfaz de usuario de teclado de Android que se había diseñado anteriormente. Este cambio se ha llevado a cabo para que sea coherente al usar los teclados predeterminados en Android e iOS, para ambos tipos de PIN "Numérico" o "Código de acceso". Para obtener más información sobre la configuración de acceso de los usuarios finales en Android, como el PIN de APP, consulte Requisitos de acceso de Android.

Configuración del dispositivo

Las plantillas administrativas están en versión preliminar pública y se movieron a su propio perfil de configuración

Las plantillas administrativas de Intune (**Configuración del dispositivo** > **Plantillas administrativas**) están actualmente en versión preliminar pública. Con esta actualización:

- Las plantillas administrativas contienen unos 300 valores de configuración que se pueden administrar en Intune. Anteriormente, estas configuraciones solo existían en el editor de directivas de grupo.
- Las plantillas administrativas están disponibles en versión preliminar pública.
- Las plantillas administrativas están disponibles en versión preliminar pública y se han migrado desde **Configuración del dispositivo** > **Plantillas administrativas** a **Configuración del dispositivo** >

Perfiles > **Crear perfil**. Luego, en **Plataforma**, seleccione **Windows 10 y versiones posteriores**, en **Tipo de perfil**, y haga clic en **Plantillas administrativas**.

- Se han habilitado los informes.

Para obtener más información sobre esta característica, vaya a Plantillas de Windows 10 para configurar opciones de directiva de grupo.

Se aplica a: Windows 10 y versiones posteriores

Uso de S/MIME para cifrar y firmar varios dispositivos para un usuario

Esta actualización incluye cifrado de correo electrónico S/MIME mediante un nuevo perfil de certificado importado (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > seleccione la plataforma > tipo de perfil **Certificado PKCS importado**). En Intune, puede importar los certificados en formato PFX. Después, Intune puede entregar esos mismos certificados a varios dispositivos inscritos por un solo usuario. Esto también incluye lo siguiente:

- El perfil de correo electrónico de iOS nativo permite habilitar el cifrado S/MIME mediante certificados importados en formato PFX.
- La aplicación de correo nativo de los dispositivos Windows Phone 10 usa automáticamente el certificado S/MIME.
- Los certificados privados se pueden entregar en varias plataformas. Aun así, no todas las aplicaciones de correo electrónico son compatibles con S/MIME.
- En otras plataformas, podría tener que configurar manualmente la aplicación de correo electrónico para habilitar S/MIME.
- Las aplicaciones de correo electrónico que admiten el cifrado S/MIME pueden controlar la recuperación de certificados para el cifrado de correo electrónico S/MIME de una manera que no es compatible con un servicio MDM, por ejemplo, si los lee desde el almacén de certificados del publicador. Para obtener más información sobre esta característica, vea Información general sobre S/MIME para firmar y cifrar correos electrónicos. Compatible con: Windows, Windows Phone 10, macOS, iOS, Android

Nuevas opciones para conectarse automáticamente y conservar las reglas al usar la configuración DNS en dispositivos Windows 10 y posteriores

En dispositivos Windows 10 y versiones posteriores, podrá crear un perfil de configuración de VPN que incluya una lista de servidores DNS para resolver dominios, como contoso.com. En esta actualización se incluirá una nueva configuración para la resolución de nombres (**Configuración del dispositivo** > **Perfiles** > **Crear perfil**; seleccione **Windows 10 y versiones posteriores** como la plataforma, **VPN** como el tipo de perfil, y **Configuración DNS** >**Agregar**):

- **Conectar automáticamente**: si esta opción está **Habilitada**, el dispositivo se conecta automáticamente a la VPN cuando se comunica con un dominio especificado, como contoso.com.
- **Persistente**: de manera predeterminada, todas las reglas de la tabla de directivas de resolución de nombres (NRPT) están activas siempre que el dispositivo esté conectado mediante este perfil de VPN. Si esta opción está **habilitada** en una regla de NRPT, la regla sigue activa en el dispositivo incluso si la VPN se desconecta. La regla se mantiene hasta que se el perfil de VPN se quita o hasta que la regla se quita manualmente, lo cual puede hacerse mediante PowerShell. En Configuración de VPN de Windows 10, se describe la configuración.

Uso de la detección de redes de confianza para perfiles de VPN en dispositivos Windows 10

Al usar la detección de redes de confianza, podrá impedir que los perfiles VPN creen automáticamente una conexión VPN cuando el usuario ya esté en una red de confianza. Con esta actualización, podrá agregar sufijos DNS para habilitar la detección de redes de confianza en dispositivos que ejecuten Windows 10 y versiones posteriores (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **VPN** para el tipo de perfil). Configuración de VPN de Windows 10 muestra la configuración de VPN actual.

Administración de dispositivos con Windows Holographic for Business empleados por varios usuarios

Actualmente, puede configurar parámetros de equipos compartidos en Windows 10 y dispositivos Windows Holographic for Business mediante una configuración personalizada de OMA-URI. En esta actualización se agregará un nuevo perfil para configurar las opciones de dispositivos compartidos (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** > **Dispositivo multiusuario compartido**). Para obtener más información sobre esta característica, vaya a Configuración de Intune para administrar dispositivos compartidos. Se aplica a: Windows 10 y versiones posteriores, Windows Holographic for Business

Nueva configuración de actualizaciones de Windows 10

Para sus Círculos de actualizaciones de Windows 10, puede configurar lo siguiente:

- **Comportamiento de actualizaciones automáticas**: use una nueva opción (*Restablecer valores predeterminados*) para restaurar la configuración de actualizaciones automáticas original en equipos con Windows 10 que ejecuten la *actualización de octubre de 2018*.
- **Impedir al usuario pausar las actualizaciones de Windows**: establezca una nueva configuración de actualizaciones de software que impida o permita que los usuarios pausen la instalación de actualizaciones en el menú *Configuración* de sus equipos.

Los perfiles de correo electrónico de iOS pueden usar cifrado y firma de S/MIME

Podrá crear un perfil de correo electrónico que incluya otra configuración. En esta actualización, se incluye la configuración de S/MIME que se puede usar para firmar y cifrar las comunicaciones por correo electrónico de dispositivos iOS (**Configuración del dispositivo** > **Perfiles** > **Crear perfil**; elija **iOS** para la plataforma y **Correo electrónico** para el tipo de perfil). La configuración actual se muestra en Opciones de configuración de correo electrónico de iOS.

Algunos valores de configuración de BitLocker admiten Windows 10 Pro Edition

Podrá crear un perfil de configuración que establezca los ajustes de Endpoint Protection en dispositivos con Windows 10, incluido BitLocker. En esta actualización se agrega la compatibilidad con Windows 10 Professional Edition en algunas opciones de configuración de BitLocker. Para ver estos ajustes de protección, vaya a Configuración de Endpoint Protection para Windows 10.

Cambio del nombre de Configuración de dispositivo compartido a Mensaje de la pantalla de bloqueo para dispositivos iOS en Azure Portal

Al crear un perfil de configuración de dispositivos iOS, puede agregar la opción **Configuración de dispositivo compartido** para mostrar texto específico en la pantalla de bloqueo. En esta actualización se incluyen los cambios siguientes:

- El nombre de la opción **Configuración de un dispositivo compartido** en Azure Portal se cambia a "Mensaje de la pantalla de bloqueo (solo con supervisión)" (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > Elegir **iOS** para la plataforma > Elegir **Características del dispositivo** para el tipo de perfil > **Mensaje de la pantalla de bloqueo**).
- Al agregar mensajes de la pantalla de bloqueo, puede insertar un número de serie, un nombre de dispositivo u otro valor específico del dispositivo como una variable en **Información de etiqueta del activo** y **Nota al pie en la pantalla de bloqueo**. Por ejemplo, puede escribir `Device name: {{devicename}}` o `Serial number is {{serialnumber}}` entre llaves. Tokens de iOS muestra los tokens disponibles que se pueden usar. En Configuración para mostrar mensaje en la pantalla de bloqueo, se muestra la configuración actual.

Adición en dispositivos iOS de nuevo App Store, visualización de documentos y configuración de restricción de dispositivos de juego

En **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para la plataforma y **Restricciones de dispositivo** para el tipo de perfil, en **App Store, visualización de documentos y juegos**, se han agregado las siguientes opciones de configuración: Permitir a las aplicaciones administradas escribir contactos en cuentas de contactos no administradas y Permitir a las aplicaciones no administradas leer en cuentas de contactos administradas. Para ver estas opciones de configuración, vaya a Restricciones de dispositivos iOS.

Nueva configuración de notificaciones, sugerencias y bloqueo del teclado para dispositivos de propietarios de dispositivos Android Enterprise

Esta actualización incluye varias características de los dispositivos Android Enterprise cuando se ejecutan como propietario del dispositivo. Para usar estas características, vaya a **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > en **Plataforma**, elija **Android Enterprise** > en **Tipo de perfil**, elija **Solo el propietario del dispositivo** > **Restricciones de dispositivos**.

Nuevas características:

- Deshabilitar la visualización de las notificaciones del sistema, incluidas las llamadas entrantes, las alertas del sistema, los errores del sistema, etc.
- Sugerir omitir los tutoriales de inicio y las sugerencias para las aplicaciones que se abren por primera vez.
- Deshabilitar la configuración avanzada del bloqueo del teclado, como la cámara, las notificaciones, el desbloqueo con huella digital, etc.

Para ver la configuración actual, vaya a Configuración de restricciones de dispositivos Android Enterprise.

Los dispositivos de propietarios de dispositivos Android Enterprise pueden usar conexiones VPN siempre activas

En esta actualización, puede usar conexiones VPN siempre activas en dispositivos propietarios del dispositivo Android Enterprise. Las conexiones VPN siempre activas permanecen conectadas o se vuelven a conectar inmediatamente cuando el usuario desbloquea el dispositivo, cuando se reinicia el dispositivo o cuando cambia la red inalámbrica. También puede poner la conexión en modo "bloqueo", que bloquea todo el tráfico de red hasta que la conexión VPN esté activa. Puede habilitar la VPN siempre activa en **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** para la plataforma > **Restricciones de dispositivos** solo para el propietario del dispositivo > **Conectividad**. Para ver la configuración actual, vaya a Configuración de restricciones de dispositivos Android Enterprise.

Nueva configuración para terminar procesos en el Administrador de tareas de dispositivos Windows 10

Esta actualización incluye una configuración nueva para terminar los procesos con el Administrador de tareas en dispositivos Windows 10. Con un perfil de configuración de dispositivo (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > en **Plataforma**, elija **Windows 10** > en **Tipo de perfil**, elija **Restricciones de dispositivos** > **Configuración general**), elige si permitir o impedir esta configuración. Para ver la configuración actual, vaya a Configuración de restricciones de dispositivos Windows 10. Se aplica a: Windows 10 y versiones posteriores

Uso de la configuración recomendada por Microsoft con líneas de base de seguridad (versión preliminar pública)

Intune se integra con otros servicios centrados en la seguridad, incluidos Windows Defender for Endpoint y Office 365 Defender for Endpoint. Los clientes solicitan una estrategia común y un conjunto coherente de flujos de trabajo de seguridad integrales entre los servicios de Microsoft 365. Nuestro objetivo es alinear las estrategias para crear soluciones que actúen de puente entre las operaciones de seguridad y las tareas de administración comunes. En Intune, este objetivo se pretende lograr mediante la publicación de un conjunto de "Líneas de base de seguridad" recomendadas de Microsoft (**Intune** > **Líneas de base de seguridad**). Un administrador puede crear directivas de seguridad directamente a partir de estas líneas de base y, después, implementarlas en sus usuarios. También puede personalizar los procedimientos recomendados para satisfacer las necesidades de su organización. Intune garantiza que los dispositivos cumplan estas líneas de base y notifica a los administradores los usuarios o dispositivos que no están en cumplimiento.

Esta característica está en versión preliminar pública, por lo que los perfiles creados ahora no se moverán a las plantillas de líneas base de seguridad que están disponibles con carácter general (GA). No debería planear usar estas plantillas de versión preliminar en el entorno de producción.

Para más información sobre las líneas de base de seguridad, vea Create a Windows 10 security baseline in Intune (Crear una línea de base de seguridad de Windows 10 en Intune).

Esta característica se aplica a: Windows 10 y versiones posteriores

Quienes no son administradores pueden habilitar BitLocker en dispositivos Windows 10 unidos a Azure AD

Cuando se habilita la configuración de BitLocker en dispositivos Windows 10 (**Configuración del dispositivo**

> **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para la plataforma > **Endpoint Protection** para el tipo de perfil > **Cifrado de Windows**), se agrega la configuración de BitLocker.

Esta actualización incluye una configuración de BitLocker nueva para permitir que los usuarios estándar (no administradores) habiliten el cifrado.

Para ver esta configuración, vaya a Configuración de Windows 10 (y versiones posteriores) para proteger dispositivos mediante Intune.

Comprobación de cumplimiento de Configuration Manager

Esta actualización incluye una nueva configuración de conformidad de Configuration Manager (**Conformidad de dispositivos** > **Directivas** > **Crear directiva** > **Windows 10 y versiones posteriores** > **Cumplimiento de Configuration Manager**). Configuration Manager envía señales a la conformidad de Intune. Mediante esta configuración, puede exigir que todas las señales de Configuration Manager devuelvan "conforme".

Por ejemplo, exige que todas las actualizaciones de software se instalen en los dispositivos. En Configuration Manager, este requisito tiene el estado "Instalado". Si algún programa del dispositivo se encuentra en un estado desconocido, dicho dispositivo no será conforme en Intune.

Cumplimiento de Configuration Manager describe esta configuración.

Se aplica a: Windows 10 y versiones posteriores

Personalización del papel tapiz en dispositivos iOS supervisados mediante un perfil de configuración de dispositivo

Cuando cree un perfil de configuración de dispositivos para dispositivos iOS, podrá personalizar algunas características (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** para la plataforma > **Características del dispositivo** para el tipo de perfil). Esta actualización incluye nuevas configuraciones **Fondo de pantalla** que permiten a un administrador usar una imagen .png, .jpg o .jpeg en la pantalla de inicio o en la pantalla de bloqueo. Esta configuración de fondo de pantalla solo se aplica a los dispositivos supervisados.

Para una lista de esta configuración, consulte iOS device feature settings (Configuración de características de dispositivos iOS).

Pantalla completa de Windows 10 disponible con carácter general

En esta actualización, la característica Pantalla completa en dispositivos con Windows 10 y versiones posteriores está disponible con carácter general (GA). Para ver todas las configuraciones que puede agregar y definir, consulte Configuración de dispositivos con Windows 10 y versiones posteriores para ejecutarse como una pantalla completa dedicada con Intune.

Se eliminó la opción para compartir contacto a través de Bluetooth en Restricciones del dispositivo > Propietario del dispositivo para Android Enterprise

Cuando se crea un perfil de restricciones de dispositivos para dispositivos de Android Enterprise, hay una configuración para **Compartir contacto a través de Bluetooth**. En esta actualización, se elimina la configuración **Compartir contacto a través de Bluetooth** (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android Enterprise** para la plataforma > **Restricciones de dispositivos** > **Propietario del dispositivo** para el tipo de perfil > **General**).

La configuración **Compartir contacto a través de Bluetooth** no es compatible con la administración de Propietario del dispositivo Android Enterprise. Por lo que cuando se quite esta configuración, no afectará a ningún dispositivo ni inquilino, incluso si esta opción está habilitada y configurada en su entorno.

Para ver la lista actual de configuraciones, vaya a Configuración de dispositivos Android Enterprise para permitir o restringir características.

Se aplica a: Propietario del dispositivo Android Enterprise

Inscripción de dispositivos

Mensajes de error de restricción de inscripción más detallados

Los mensajes de error más detallados estarán disponibles cuando no se cumplan las restricciones de inscripción. Para ver estos mensajes, vaya a **Intune** > **Solucionar problemas** > y revise la tabla Errores de inscripción. Para obtener más información, vea la lista de errores de inscripción.

Administración del dispositivo

Versión preliminar de la compatibilidad con dispositivos Android totalmente administrados de propiedad corporativa

Intune ya admite dispositivos Android totalmente administrados; un escenario de "propietario de dispositivo" de propiedad corporativa en el que el departamento de TI administra de manera rigurosa los dispositivos y estos se asocian a usuarios individuales. Esto permite que los administradores administren todo el dispositivo, apliquen una amplia variedad de controles de directivas no disponibles para los perfiles de trabajo y restrinjan las instalaciones de aplicaciones por parte de los usuarios solo a Google Play administrado. Para obtener más información, vea Set up Intune enrollment of Android fully managed devices (Configuración de la inscripción en Intune de dispositivos Android totalmente administrados) y Enroll your dedicated devices or fully managed devices (Inscripción de dispositivos dedicados o dispositivos totalmente administrados). Tenga en cuenta que esta característica está en versión preliminar. Algunas funcionalidades de Intune, como certificados, cumplimiento y acceso condicional, no están disponibles actualmente con dispositivos Android totalmente administrados.

Compatibilidad con el borrado selectivo para dispositivos con trabajos en curso sin inscripción

Windows Information Protection Without Enrollment (WIP-WE) permite a los clientes proteger sus datos corporativos en dispositivos con Windows 10 sin necesidad de realizar una inscripción de MDM completa. Una vez que los documentos están protegidos con una directiva de WIP-WE, un administrador de Intune puede borrar de forma selectiva los datos protegidos. Mediante la selección del usuario y dispositivo, y el envío de una solicitud de borrado, todos los datos protegidos mediante la directiva de WIP-WE quedarán inservibles. En Intune en Azure Portal, seleccione **Aplicación móvil** > **Borrado selectivo de aplicaciones**.

Supervisión y solución de problemas

Panel Estado del inquilino

En la nueva página Estado del inquilino se proporciona una ubicación única donde puede ver el estado del inquilino y los detalles relacionados. El panel se divide en cuatro áreas:

- **Detalles del inquilino**: se muestra información como el nombre del inquilino y la ubicación, la entidad de MDM, el número total de dispositivos inscritos en el inquilino y el número de licencias. En esta sección también se indica la versión de mantenimiento actual del inquilino.
- **Estado del conector**: muestra información sobre conectores disponibles que ha configurado y, además, se puede mostrar una lista de los que aún no ha habilitado.
  Basándose en el estado actual de cada conector, se marcan como Correcto, Advertencia o Incorrecto. Seleccione un conector para explorarlo en profundidad y ver sus detalles, o bien para configurar información adicional sobre este.
- **Estado del servicio Intune**: muestra detalles sobre incidentes activos o interrupciones del inquilino. La información de esta sección se obtiene directamente del Centro de mensajes de Office.
- **Noticias de Intune**: muestra mensajes activos para el inquilino. En estos mensajes, se incluyen notificaciones cuando el inquilino recibe las características de Intune más recientes. La información de esta sección se obtiene directamente del Centro de mensajes de Office.

Nueva experiencia de ayuda y soporte técnico en el Portal de empresa para Windows 10

La nueva página de ayuda y soporte técnico del Portal de empresa ayuda a los usuarios a solucionar problemas y solicitar ayuda para problemas de acceso y de aplicaciones. Desde la nueva página, puede enviar por correo electrónico detalles de registros de diagnóstico y errores, así como obtener los detalles del departamento de soporte técnico de su organización. También encontrará una sección de preguntas más frecuentes con vínculos a la documentación de Intune relevante.

Nueva experiencia de ayuda y soporte técnico para Intune

Implementaremos la nueva experiencia de ayuda y soporte técnico a todos los inquilinos en los próximos días. Esta experiencia está disponible para Intune y puede accederse al usar las hojas de Intune en Azure Portal. La nueva experiencia le permite describir el problema con sus propias palabras y recibir información sobre solución de problemas y contenido de corrección basado en la Web. Estas soluciones se ofrecen mediante un algoritmo de aprendizaje automático con reglas, basado en las consultas de los usuarios. Además de instrucciones específicas del problema, también puede usar el nuevo flujo de trabajo de creación de casos para abrir una incidencia de soporte técnico por teléfono o correo electrónico. Esta nueva experiencia reemplaza a la experiencia de ayuda y soporte técnico anterior de un conjunto estático de opciones seleccionadas previamente que se basan en el área de la consola en la que se encuentra cuando abre la sección Ayuda y soporte técnico. Para obtener más información, vea Cómo obtener asistencia para Microsoft Intune.

Nuevos registros operativos y posibilidad de enviar registros a los servicios de Azure Monitor

Intune tiene el registro de auditoría integrado que realiza el seguimiento de eventos cuando se realizan cambios. Esta actualización incluye nuevas características de registro, como las siguientes:

- Registros operativos (versión preliminar) que se muestran detalles sobre los usuarios y dispositivos que se inscribieron, incluidos los intentos correctos y erróneos.
- Los registros de auditoría y los registros operativos también se pueden enviar a Azure Monitor, incluidas las cuentas de almacenamiento, Event Hubs y Log Analytics. Estos servicios permiten almacenar, usar análisis como Splunk y QRadar y obtener visualizaciones de los datos de registro.

En Send log data to storage, event hubs, or log analytics in Intune (Envío de datos de registro al almacenamiento, Event Hubs o Log Analytics en Intune) se proporciona más información sobre esta característica.

Omisión de más pantallas del Asistente de configuración de un dispositivo DEP iOS

Además de las pantallas que actualmente se pueden omitir, podrá establecer dispositivos DEP de iOS para omitir las pantallas siguientes en el Asistente para la configuración cuando un usuario inscribe el dispositivo: Tono de pantalla, Privacidad, Migración de Android, botón Inicio, iMessage y FaceTime, Incorporación, Migración de Watch, Apariencia, Tiempo de uso, Actualización de software, Configuración de SIM. Para elegir qué pantallas omitir, vaya a **Inscripción de dispositivos** > **Inscripción de Apple** > **Tokens del programa de inscripción** > elija un token > **Perfiles** > elija un perfil > **Propiedades** > **Personalización del Asistente de configuración** > elija **Ocultar** en todas las pantallas que quiera omitir > **Aceptar**. Si crea un nuevo perfil o edita uno, las pantallas de omisión seleccionadas deben sincronizarse con el servidor MDM de Apple. Los usuarios pueden emitir una sincronización manual de los dispositivos para que no haya ningún retraso en la recogida de los cambios de perfil.

Implementación de aplicaciones APP-WE de Android Enterprise

En el caso de los dispositivos Android en un escenario de implementación de directiva de protección de aplicaciones sin inscripción (APP-WE) no inscrito, ahora puede usar Google Play administrado para implementar aplicaciones de la tienda y aplicaciones de LOB en los usuarios. En concreto, puede brindar a los usuarios finales un catálogo de aplicaciones y experiencia de instalación que ya no requiere que los usuarios finales flexibilicen la posición de seguridad de sus dispositivos al permitir instalaciones de orígenes desconocidos. Además, este escenario de implementación proporcionará una mejor experiencia del usuario final.

Control de acceso basado en roles.

Etiquetas de ámbito para las aplicaciones

Puede crear etiquetas de ámbito para limitar el acceso a roles y aplicaciones. Puede agregar una etiqueta de ámbito a una aplicación para que solo los usuarios con roles que también tengan asignada esa etiqueta de ámbito puedan acceder a la aplicación. Actualmente, no es posible asignar etiquetas de ámbito a las aplicaciones que se agregan a Intune desde Google Play administrado o a aquellas que se compran mediante el Programa de Compras por Volumen de Apple (VPP), si bien será posible en el futuro. Para obtener más información, vea Uso de etiquetas de ámbito para filtrar directivas.

Diciembre de 2018

Administración de aplicaciones

Actualizaciones para Seguridad de transporte de aplicaciones

Microsoft Intune admite la versión 1.2+ del protocolo Seguridad de la capa de transporte (TLS) para proporcionar el mejor cifrado en su clase, a fin de garantizar que Intune sea más seguro de forma predeterminada, y alinearlo con otros servicios de Microsoft, como Microsoft 365. Con el fin de satisfacer este requisito, en los portales de empresa de iOS y macOS se exigirán los requisitos de Seguridad de transporte de aplicaciones (ATS) actualizados de Apple que también requieren TLS 1.2+. ATS se utiliza para exigir una seguridad más estricta en todas las comunicaciones de aplicación a través de HTTPS. Este cambio afecta a los clientes de Intune que usan las aplicaciones Portal de empresa para iOS y macOS. Para más información, vea el blog de soporte técnico de Intune.

El SDK de aplicaciones de Intune admitirá claves de cifrado de 256 bits

El SDK de aplicaciones de Intune para Android ahora usa claves de cifrado de 256 bits cuando el cifrado esté habilitado mediante las directivas de protección de aplicaciones. El SDK seguirá siendo compatible con las claves de 128 bits para mantener la compatibilidad con el contenido y las aplicaciones que usen las versiones anteriores del SDK.

Versión de actualización automática 4.5.0 de Microsoft necesaria para dispositivos macOS

Para seguir recibiendo actualizaciones del Portal de empresa y otras aplicaciones de Office, los dispositivos macOS administrados por Intune se deben actualizar a la actualización automática 4.5.0 de Microsoft. Es posible que los usuarios ya tengan esta versión para sus aplicaciones de Office.

Administración de dispositivos

Intune requiere macOS 10.12 o versiones posteriores

Intune ahora requiere macOS versión 10.12 o posterior. Los dispositivos con versiones anteriores de macOS no pueden usar el Portal de empresa para inscribirse en Intune. Para recibir asistencia de soporte técnico y nuevas características, los usuarios deben actualizar su dispositivo a macOS 10.12 o posterior y actualizar el Portal de empresa a la versión más reciente.

Noviembre de 2018

Administración de aplicaciones

Desinstalación de aplicaciones en dispositivos iOS supervisados corporativos

Puede quitar cualquier aplicación en dispositivos iOS corporativos supervisados. Puede quitar cualquier aplicación estableciendo como destino grupos de usuarios o dispositivos con un tipo de asignación **Desinstalar**. Para dispositivos iOS personales o no supervisados, podrá quitar solo las aplicaciones que se instalaron mediante Intune.

Descarga de contenido de aplicaciones Win32 de Intune

Los clientes Windows 10 RS3 y versiones posterior descargarán contenido de aplicaciones Win32 de Intune mediante un componente de Optimización de distribución del cliente Windows 10. La Optimización de distribución proporciona la funcionalidad punto a punto está activada de manera predeterminada. Actualmente, la Optimización de distribución se puede configurar según la directiva de grupo. Para más información, consulte el artículo sobre la Optimización de distribución para Windows 10.

Menú de contenido de aplicaciones y dispositivos del usuario final

Los usuarios finales ahora pueden usar el menú contextual del dispositivo y las aplicaciones para desencadenar acciones comunes, como cambiar el nombre de un dispositivo o comprobar el cumplimiento.

Establecer un fondo personalizado en la aplicación Managed Home Screen

Se está agregando una configuración que permitirá personalizar la apariencia del fondo de la aplicación Managed Home Screen en dispositivos Android Enterprise en pantalla completa con varias aplicaciones. Para configurar el **fondo de dirección URL personalizado**, vaya a Intune en Azure Portal > Configuración del

dispositivo. Seleccione un perfil de configuración del dispositivo actual o cree uno para editar su configuración de quiosco. Para ver la configuración de pantalla completa, consulte las restricciones de los dispositivos Android Enterprise.

Guardar y aplicar asignaciones de la directiva de protección de la aplicación

Ahora puede controlar mejor las asignaciones de la directiva de protección de la aplicación. Cuando selecciona *Asignaciones* para establecer o editar las asignaciones de una directiva, debe **guardar** la configuración antes de que se aplique el cambio. Use **Descartar** para borrar todos los cambios que haga sin guardar ningún cambio en las listas de inclusión o exclusión. Como se requiere guardar o descartar, solo los usuarios deseados tienen asignada una directiva de protección de la aplicación.

Nueva configuración del explorador Microsoft Edge en Windows 10 y versiones posteriores

Esta actualización incluye una nueva configuración para ayudar a controlar y administrar el explorador Microsoft Edge versión 45 y anteriores en los dispositivos. Para ver una lista de estas configuraciones, consulteRestricciones de dispositivos para Windows 10 (y versiones posteriores).

Las nuevas aplicaciones son compatibles con las directivas de protección de aplicaciones

Ahora puede administrar las aplicaciones siguientes con las directivas de protección de aplicaciones de Intune:

- Stream (iOS)
- To DO (Android, iOS)
- PowerApps (Android, iOS)
- Flow (Android, iOS)

Use las directivas de protección de aplicaciones para proteger los datos corporativos y controlar la transferencia de datos de estas aplicaciones, como otras aplicaciones administradas por las directivas de Intune. Nota: Si Flow todavía no aparece en la consola, lo agregará al crear o editar directivas de protección de aplicaciones. Para hacerlo, use la opción **+ Más aplicaciones** y especifique el *id. de la aplicación* para Flow en el campo de entrada. Para Android use *com.microsoft.flow* y para iOS, *com.microsoft.procsimo*.

Configuración del dispositivo

Compatibilidad con OAuth de iOS 12 en perfiles de correo electrónico de iOS

Los perfiles de correo electrónico iOS de Intune son compatibles con Open Authorization (OAuth) para iOS 12. Para ver esta característica, cree un perfil (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **iOS** como plataforma > **Correo electrónico** como tipo de perfil) o actualice un perfil de correo electrónico iOS existente. Si habilita OAuth en un perfil que ya se ha implementado en los usuarios, se les pedirá que se vuelvan a autenticar y que vuelvan a descargar su correo electrónico.

En Perfiles de correo electrónico iOS hay más información sobre cómo usar OAuth en un perfil de correo electrónico.

Compatibilidad del control de acceso de red (NAC) con Citrix SSO para iOS

Citrix lanzó una actualización para Citrix Gateway para permitir el control de acceso de red (NAC) para Citrix SSO para iOS en Intune. Puede optar por incluir un identificador de dispositivo en un perfil de VPN en Intune y luego insertar este perfil en los dispositivos iOS. Deberá instalar la actualización más reciente de Citrix Gateway para usar esta funcionalidad.

Configuración de VPN en dispositivos iOS proporciona más información sobre el uso de NAC, incluidos algunos requisitos adicionales.

Se muestran los números de versión y los números de compilación de iOS y macOS

En **Conformidad de dispositivos** > **Conformidad de dispositivos** se muestran las versiones de los sistemas operativos iOS y macOS, que se pueden usar en las directivas de cumplimiento. Esta actualización incluye el número de compilación, que se puede configurar para ambas plataformas. Cuando se publican las actualizaciones de seguridad, Apple normalmente deja el número de versión como está, pero actualiza el número de compilación. Si usa el número de compilación en una directiva de cumplimiento, puede comprobar

fácilmente si hay instalada una actualización de vulnerabilidad. Para usar esta característica, consulte las directivas de cumplimiento de iOS y macOS.

Los círculos de actualizaciones se reemplazan por la configuración Optimización de distribución para Windows 10 y versiones posteriores

Optimización de distribución es un perfil de configuración nuevo para Windows 10 y versiones posteriores. Esta característica proporciona una experiencia más simplificada para brindar actualizaciones de software a los dispositivos de la organización. Esta actualización también ayuda a entregar la configuración en círculos de actualizaciones nuevos y existentes con un perfil de configuración. Para configurar un perfil de configuración de optimización de distribución, consulte la configuración de Optimización de distribución de Windows 10 (y versiones posteriores).

Nueva configuración de restricción de dispositivos agregada a dispositivos iOS y macOS

Esta actualización incluye nuevas configuraciones para los dispositivos iOS y Mac OS que se lanzan con iOS 12:

Configuración de iOS:

- General: bloquear la eliminación de aplicaciones (solo supervisado)
- General: bloquear el modo restringido USB (solo supervisado)
- General: exigir fecha y hora automáticas (solo supervisado)
- Contraseña: bloquear el relleno automático de contraseñas (solo supervisado)
- Contraseña: bloquear las solicitudes de proximidad de contraseñas (solo supervisadas)
- Contraseña: bloquear el uso compartido de contraseñas (solo supervisado)

Configuración de macOS:

- Contraseña: bloquear el relleno automático de contraseñas
- Contraseña: bloquear las solicitudes de proximidad de contraseñas
- Contraseña: bloquear el uso compartido de contraseñas

Para más información sobre estas configuraciones, consulte la configuración de restricciones de dispositivos iOS y macOS.

Inscripción de dispositivos

Compatibilidad con Autopilot para dispositivos híbridos unidos a Azure Active Directory (versión preliminar)

Ahora puede configurar dispositivos híbridos unidos a Azure Active Directory mediante AutoPilot. Los dispositivos deben estar unidos a la red de la organización para usar la característica de AutoPilot híbrida. Para más información, vea Implementar dispositivos unidos a Azure AD híbrido mediante Intune y Windows Autopilot (versión preliminar). Esta característica se implementará en toda la base de usuarios durante los próximos días. Por tanto, es posible que no pueda seguir estos pasos hasta que se implemente en su cuenta.

Seleccionar las aplicaciones de las que se realiza un seguimiento en la página de estado de la inscripción

Puede elegir de qué aplicaciones se realiza un seguimiento en la página de estado de la inscripción. El usuario no puede usar el dispositivo hasta que se instalen estas aplicaciones. Para más información, consulte Configurar una página de estado de inscripción.

Búsqueda del dispositivo Autopilot por número de serie

Ahora puede buscar dispositivos Autopilot por número de serie. Para hacerlo, elija **Inscripción de dispositivos** > **Inscripción de Windows** > **Dispositivos** > escriba un número de serie en el cuadro **Buscar por número de serie** > presione ENTRAR.

Seguimiento de la instalación de Office Pro Plus

Los usuarios pueden realizar un seguimiento del progreso de instalación de Office ProPlus en la página de estado de la inscripción. Para más información, consulte Configurar una página de estado de inscripción.

Alertas sobre tokens de VPP que expiran próximamente o licencias del Portal de empresa a punto de agotarse

Si usa el Programa de Compras por Volumen (VPP) para tener en servicio el Portal de empresa durante la

inscripción de DEP, Intune le avisará cuando el token de VPP esté a punto de expirar y las licencias del Portal de empresa se estén agotando.

Compatibilidad del Programa de inscripción de dispositivos macOS para cuentas de Apple School Manager

Intune permite usar el Programa de inscripción de dispositivos en dispositivos macOS para las cuentas de Apple School Manager. Para más información, consulte el artículo sobre la inscripción automática de dispositivos macOS con el Programa de inscripción de dispositivos de Apple o Apple School Manager.

Nueva SKU de suscripción a dispositivos de Intune

Para ayudar a reducir el costo de administración de dispositivos en las empresas, ahora tiene a su disposición una nueva SKU de suscripción basada en dispositivos. Las licencias de esta SKU de dispositivos de Intune se conceden mensualmente por dispositivo. El precio varía según el programa de licencias. Está disponible directamente mediante el centro de administración de Microsoft 365 y el Contrato Enterprise (EA), el contrato de productos y servicios de Microsoft (MPSA), los contratos abiertos de Microsoft y los proveedores de soluciones en la nube (CSP).

Administración de dispositivos

Detener temporalmente el modo de pantalla completa en dispositivos Android para realizar cambios

Al usar dispositivos Android en modo quiosco con varias aplicaciones, puede que un administrador de TI deba realizar cambios en el dispositivo. Esta actualización incluye una configuración nueva de pantalla completa con varias aplicaciones que permite que un administrador de TI pause de manera temporal la pantalla completa con un PIN y obtener acceso a todo el dispositivo. Para ver la configuración de pantalla completa, consulte las restricciones de los dispositivos Android Enterprise.

Habilitar el botón de inicio virtual en dispositivos Android Enterprise en pantalla completa

Una nueva configuración permitirá a los usuarios pulsar un botón de tecla programable en su dispositivo para cambiar entre la aplicación Managed Home Screen y otras aplicaciones asignadas en su dispositivo de quiosco con varias aplicaciones asignadas. Esta configuración es especialmente útil en escenarios donde una aplicación de quiosco del usuario no responde correctamente al botón "Atrás". Podrá configurar esta opción para dispositivos Android corporativos de un solo uso. Para habilitar o deshabilitar el **botón de inicio virtual**, vaya a Intune en Azure Portal > Configuración del dispositivo. Seleccione un perfil de configuración del dispositivo actual o cree uno para editar su configuración de quiosco. Para ver la configuración de pantalla completa, consulte las restricciones de los dispositivos Android Enterprise.

Octubre de 2018

Administración de aplicaciones

Acceso a las propiedades de perfil principales mediante la aplicación del Portal de empresa

Los usuarios finales pueden acceder ahora a las propiedades y acciones de cuenta principales, como el restablecimiento de contraseña, desde la aplicación del Portal de empresa.

Configuración de la directiva de protección de aplicaciones para el bloqueo de teclados de terceros en iOS

En dispositivos iOS, los administradores de Intune pueden bloquear el uso de teclados de terceros al acceder a datos de la organización en aplicaciones protegidas mediante directivas. Cuando la directiva de protección de aplicaciones (APP) está configurada para bloquear teclados de terceros, el usuario del dispositivo recibe un mensaje la primera vez que interactúa con los datos corporativos al usar un teclado de terceros. Todas las demás opciones, que no afecten al teclado nativo, se bloquean y los usuarios de los dispositivos no podrán verlas. Los usuarios de los dispositivos verán el mensaje del cuadro de diálogo una vez.

Acceso a la cuenta de usuario de aplicaciones de Intune en dispositivos iOS y Android administrados

Como administrador de Microsoft Intune, puede controlar qué cuentas de usuario se agregan a las aplicaciones de Microsoft Office en dispositivos administrados. Puede limitar el acceso solo a las cuentas de usuario de la organización permitidas y bloquear las cuentas personales en los dispositivos inscritos.

Directiva de configuración de aplicaciones iOS y Android para Outlook

Ahora, puede crear una directiva de configuración de aplicaciones de Outlook iOS y Android para usuarios

locales que aprovechan la autenticación básica con el protocolo ActiveSync. Se agregarán opciones de configuración adicionales a medida que se habiliten en Outlook para iOS y Android.

Paquetes de idioma de las Aplicaciones de Microsoft 365 para empresas

Como administrador de Intune, podrá implementar idiomas adicionales para las Aplicaciones de Microsoft 365 para aplicaciones empresariales administradas mediante Intune. La lista de idiomas disponibles incluye el **Tipo** de paquete de idioma (núcleo, parcial y corrección). En Azure Portal, seleccione **Microsoft Intune** > **Aplicaciones cliente** > **Aplicaciones** > **Agregar**. En la lista **Tipo de aplicación** de la hoja **Agregar aplicación**, seleccione **Windows 10** en **Conjunto de aplicaciones de Office 365**. Seleccione **Idiomas** en la hoja **Configuración del conjunto de aplicaciones**.

Extensiones de los archivos de aplicaciones de línea de negocio (LOB) de Windows

Ahora, las extensiones de archivo de las aplicaciones de LOB de Windows incluirán las extensiones *.msi*, *.appx*, *.appxbundle*, *.msix* y *.msixbundle*. Puede agregar una aplicación en Microsoft Intune seleccionando **Aplicaciones cliente** > **Aplicaciones** > **Agregar**. Se mostrará el panel **Agregar aplicación**, que permite seleccionar el **tipo de aplicación**. En el caso de las aplicaciones de LOB de Windows, seleccione la aplicación de **línea de negocio** como el tipo de aplicación, elija el **archivo de paquete de aplicación** y, después, especifique un archivo de instalación con la extensión adecuada.

Implementación de aplicaciones Windows 10 con Intune

Aprovechando la compatibilidad actual con aplicaciones de línea de negocio (LOB) y Microsoft Store para aplicaciones empresariales, los administradores pueden usar Intune para implementar la mayoría de las aplicaciones existentes de su organización a los usuarios finales en dispositivos Windows 10. Los administradores pueden agregar, instalar y desinstalar aplicaciones para los usuarios de Windows 10 en una variedad de formatos, como archivos MSI, Setup.exe o MSP. Intune evaluará las reglas de requisitos antes de realizar la descarga y la instalación, y notificará a los usuarios finales del estado o los requisitos de reinicio a través del Centro de actividades de Windows 10. Esta función desbloqueará de manera eficaz las organizaciones interesadas en el desplazamiento de esta carga de trabajo a Intune y la nube. Esta característica está actualmente en versión preliminar pública y esperamos poder agregarle nuevas funciones importantes en los próximos meses.

Configuración de directiva de protección de la aplicación (APP) de datos web

La configuración de directiva APP de contenido web en dispositivos iOS y Android se actualizará para controlar mejor los vínculos web http y https, así como la transferencia de datos a través de vínculos universales de iOS y vínculos de aplicación de Android.

Menú de contenido de aplicaciones y dispositivos del usuario final

Los usuarios finales ahora pueden usar el menú contextual de aplicaciones y dispositivos para desencadenar acciones comunes, como cambiar el nombre de un dispositivo o comprobar su cumplimiento.

Métodos abreviados de teclado del Portal de empresa de Windows

Ahora, los usuarios finales podrán desencadenar acciones de aplicación y dispositivo en el Portal de empresa de Windows mediante métodos abreviados de teclado (aceleradores).

Solicitar PIN que no sea biométrico después de un tiempo de expiración especificado

Al exigir un número de identificación personal no biométrico después de transcurrir un tiempo de expiración especificado por el administrador, Intune proporcionará una mayor seguridad para las aplicaciones compatibles con Administración de aplicaciones de móviles (MAM), ya que restringe el uso de identificación biométrica para el acceso a datos corporativos. La configuración afectará a los usuarios que dependen de Touch ID (iOS), Face ID (iOS), Android Biometric u otros métodos de autenticación biométrica futuros para tener acceso a aplicaciones compatibles con APP/MAM. Con esta configuración, los administradores de Intune tendrán un control más exhaustivo del acceso de los usuarios. De este modo, se evitan situaciones en las que un dispositivo con varias huellas digitales u otros métodos de acceso biométrico pueda revelar datos corporativos a un usuario incorrecto. En Azure Portal, abra **Microsoft Intune**. Seleccione **Aplicaciones cliente** > **Directivas de protección de aplicaciones** > **Agregar una directiva** > **Configuración**. En la **Acceso** encontrará ajustes específicos. Para obtener información sobre la configuración del acceso, vea la configuración para iOS y la

configuración para Android.

Configuración de transferencia de datos de APP de Intune en dispositivos iOS inscritos en MDM

Podrá controlar por separado la configuración de la transferencia de datos de la aplicación de Intune en dispositivos iOS inscritos en MDM y la especificación de la identidad del usuario inscrito, que se conoce también como nombre principal de usuario (UPN). Los administradores que no usen el IntuneMAMUPN no observarán un cambio de comportamiento. Cuando esta función esté disponible, los administradores que usan el IntuneMAMUPN para controlar el comportamiento de la transferencia de datos en los dispositivos inscritos deben revisar la nueva configuración y actualizar la configuración de APP según sea necesario.

Aplicaciones Win32 de Windows 10

Puede configurar las aplicaciones Win32 para instalarlas en el contexto de usuario para usuarios individuales, en comparación con la instalación de la aplicación para todos los usuarios del dispositivo.

Aplicaciones Win32 de Windows y scripts de PowerShell

Los usuarios finales ya no tienen que iniciar sesión en el dispositivo para instalar las aplicaciones Win32 o ejecutar scripts de PowerShell.

Solución de problemas de instalación de la aplicación cliente

Puede solucionar los problemas para que las aplicaciones cliente se instalen correctamente si consulta la columna etiquetada como **Instalación de la aplicación** en la hoja **Solución de problemas**. Para ver la hoja **Solución de problemas**, en el portal de Intune, seleccione **Solución de problemas** en **Ayuda y soporte técnico**.

Configuración del dispositivo

Creación de sufijos DNS en los perfiles de configuración de VPN en dispositivos que ejecutan Windows 10

Cuando se crea un perfil de configuración del dispositivo VPN (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para plataforma > **VPN** para tipo de perfil), se escriben algunos valores de DNS. Con esta actualización, también puede especificar varios **sufijos DNS** en Intune. Al usar los sufijos DNS, puede buscar un recurso de red mediante su nombre corto, en lugar del nombre de dominio completo (FQDN). Esta actualización también le permite cambiar el orden de los sufijos DNS en Intune. Configuración de VPN de Windows 10 muestra la configuración de DNS actual. Se aplica a: Dispositivos Windows 10

Compatibilidad con VPN siempre activa para perfiles de trabajo empresarial de Android

En esta actualización, puede usar conexiones VPN siempre activas en dispositivos empresariales Android con perfiles de trabajo administrados. Las conexiones VPN siempre activas permanecen conectadas o se vuelven a conectar inmediatamente cuando el usuario desbloquea el dispositivo, cuando se reinicia el dispositivo o cuando cambia la red inalámbrica. También puede poner la conexión en modo "bloqueo", que bloquea todo el tráfico de red hasta que la conexión VPN esté activa. Puede habilitar la VPN siempre activa en **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Android empresarial** para plataforma > **Restricciones de dispositivo** > **Conectividad**.

Emitir certificados SCEP para los dispositivos sin usuario

Actualmente, los certificados se emiten a los usuarios. Con esta actualización, se pueden emitir certificados SCEP para los dispositivos, incluidos los dispositivos sin usuario, como los quioscos multimedia (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para plataforma > **Certificado SCEP** para perfil). Otras actualizaciones incluyen:

- La propiedad **Asunto** en un perfil SCEP pasará a ser un cuadro de texto personalizado y puede incluir nuevas variables.
- La propiedad **Nombre alternativo del firmante (SAN)** en un perfil SCEP ahora es un formato de tabla y puede incluir nuevas variables. En la tabla un administrador puede agregar un atributo y rellenar el valor en un cuadro de texto personalizado. La SAN será compatible con los siguientes atributos:
  - DNS

- Dirección de correo electrónico
- UPN

Estas nuevas variables se pueden agregar con texto estático en un cuadro de texto de valor personalizado. Por ejemplo, el atributo DNS puede agregarse como `DNS = {{AzureADDeviceId}}.domain.com`.

> **NOTE**
> Las llaves, los puntos y coma y los símbolos de barra vertical " { } ; | " no funcionará en el texto estático de la SAN. Las llaves solo deben rodear una de las nuevas variables de certificado de dispositivo que debe aceptar `Subject` o `Subject alternative name`.

Nuevas variables de certificado de dispositivo:

```
"{{AAD_Device_ID}}",
"{{Device_Serial}}",
"{{Device_IMEI}}",
"{{SerialNumber}}",
"{{IMEINumber}}",
"{{AzureADDeviceId}}",
"{{WiFiMacAddress}}",
"{{IMEI}}",
"{{DeviceName}}",
"{{FullyQualifiedDomainName}}",
"{{MEID}}",
```

> **NOTE**
> - `{{FullyQualifiedDomainName}}` solo funciona para Windows y dispositivos unidos a dominios.
> - Al especificar las propiedades del dispositivo como el IMEI, el número de serie y el nombre de dominio completo en el asunto o SAN para un certificado de dispositivo, tenga en cuenta que una persona con acceso al dispositivo podría suplantar estas propiedades.

Crear un perfil de certificado SCEP enumera las variables actuales al crear un perfil de configuración de SCEP.

Se aplica a: Windows 10 y posterior e iOS, compatible con Wi-Fi

Bloquear dispositivos no compatibles de forma remota

Cuando un dispositivo no cumple los requisitos, puede crear una acción en la directiva de cumplimiento que bloquee el dispositivo de forma remota. En Intune > **Cumplimiento del dispositivo**, cree una nueva directiva o seleccione una directiva existente > **Propiedades**. Seleccione **Acciones en caso de incumplimiento** > **Agregar** y elija bloquear de forma remota el dispositivo. Compatible con:

- Android
- iOS
- macOS
- Windows 10 Mobile
- Windows Phone 8.1 y versiones posteriores

Mejoras de perfil de quiosco multimedia de Windows 10 y versiones posteriores en Azure Portal

Esta actualización incluye las siguientes mejoras para el perfil de configuración de dispositivo de quiosco multimedia de Windows 10 (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** para plataforma > **Versión preliminar de quiosco** para tipo de perfil):

- Actualmente, puede crear varios perfiles de quiosco multimedia en el mismo dispositivo. Con esta

actualización, Intune admitirá un solo perfil de quiosco multimedia por dispositivo. Si necesita varios perfiles de quiosco multimedia en un único dispositivo, puede usar un URI personalizado.

- En un perfil de **Quiosco con varias aplicaciones**, puede seleccionar el tamaño del icono de la aplicación y el orden del **Diseño del menú inicio** en la cuadrícula de la aplicación. Si prefiere una mayor personalización, puede cargar un archivo XML.
- La configuración del explorador de quiosco multimedia pasará a estar en la configuración de **Quiosco**. Actualmente, la configuración **Explorador web del quiosco** tiene su propia categoría en Azure Portal. Se aplica a: Windows 10 y versiones posteriores

Solicitud de PIN al cambiar las huellas digitales o Face ID en un dispositivo iOS

Ahora se solicitará a los usuarios un PIN después de realizar cambios biométricos en su dispositivo iOS. Esto incluye los cambios en Face ID o huellas digitales registrados. El tiempo de la solicitud depende de la configuración del tiempo de expiración de *Volver a comprobar los requisitos de acceso después de (minutos)* . Cuando no se establece ningún PIN, se solicita al usuario que establezca uno.

Esta característica solo está disponible para iOS y requiere la participación de aplicaciones que integran Intune APP SDK para iOS, versión 9.0.1 o posterior. La integración del SDK es necesaria para poder aplicar el comportamiento en las aplicaciones de destino. Esta integración ocurre de manera gradual y depende de los equipos de la aplicación específica. Algunas aplicaciones participantes incluyen WXP, Outlook, Managed Browser y Yammer.

Compatibilidad del control de acceso a la red en clientes VPN de iOS

Con esta actualización, hay una nueva configuración para habilitar el control de acceso de red (NAC) al crear un perfil de configuración de VPN de Cisco AnyConnect, F5 Access y Citrix SSO para iOS. Esta configuración permite que el identificador de NAC del dispositivo se incluya en el perfil de VPN. Actualmente, no existe ningún cliente de VPN ni solución de asociados de NAC que admita este nuevo identificador de NAC, pero le mantendremos informado en nuestra entrada de blog de soporte técnico cuando estén disponibles.

Para usar NAC, deberá:

1. Optar por permitir que Intune incluya los identificadores de dispositivo en perfiles de VPN
2. Actualizar el software/firmware del proveedor de NAC con instrucciones directas de dicho proveedor

Para obtener información sobre esta configuración en un perfil de VPN para iOS, vea Configuración de VPN en Microsoft Intune para dispositivos que ejecutan iOS. Para obtener más información sobre el control de acceso de red, vea Integración del control de acceso de red (NAC) con Intune.

Se aplica a iOS.

Eliminación de un perfil de correo electrónico de un dispositivo, incluso cuando solo hay un perfil

Antes no se podía quitar un perfil de correo electrónico de un dispositivo *si* era el único perfil de correo electrónico. Con esta actualización, se ha cambiado este comportamiento y ahora se puede quitar un perfil de correo electrónico aunque sea el único perfil de este tipo del dispositivo. Vea Configuración del correo electrónico en Microsoft Intune para obtener más información.

Scripts de PowerShell y Azure AD

Los scripts de PowerShell en Intune pueden estar dirigidos a grupos de seguridad de dispositivos de Azure AD.

Nueva configuración predeterminada "Tipo de contraseña requerida" para Android, Android Enterprise

Al crear una directiva de cumplimiento (**Intune** > **Conformidad de dispositivos** > **Directivas** > **Crear directiva** > **Android** o **Android Enterprise** para Plataforma > Seguridad del sistema), el valor predeterminado de **Tipo de contraseña requerida** cambiará:

Desde: Valor predeterminado del dispositivo Hasta: Al menos numérica

Se aplica a: Android, Android Enterprise

Para ver esta configuración, vaya a Android y Android Enterprise.

Usar una clave precompartida en un perfil de Wi-Fi de Windows 10

Con esta actualización, puede usar una clave precompartida (PSK) con el protocolo de seguridad WPA o WPA2-Personal para autenticar un perfil de configuración de Wi-Fi para Windows 10. También puede especificar la configuración de costo para una red de uso medido para la actualización del 10 de octubre de 2018 en dispositivos Windows 10.

Actualmente, debe importar un perfil de Wi-Fi o crear un perfil personalizado para usar una clave precompartida. Configuración de Wi-Fi para Windows 10 muestra la configuración actual.

Eliminación de certificados PKCS y SCEP de los dispositivos

En algunos casos, los certificados PKCS y SCEP se conservaban en los dispositivos incluso si se quitaba una directiva de un grupo, se eliminaba una configuración o una implementación de cumplimiento, o bien un administrador actualizaba un perfil SCEP o PKCS existente. Esta actualización cambia el comportamiento. Hay algunos casos en los que los certificados PKCS y SCEP se quitan de los dispositivos y otros casos en los que dichos certificados se conservan. Vea Eliminación de certificados SCEP y PKCS en Microsoft Intune para conocer estos casos.

Usar un equipo selector para cumplimiento en dispositivos macOS

Esta actualización incluye el equipo selector de macOS para evaluar el cumplimiento de los dispositivos. Para configurar la directiva del equipo selector, vea Incorporación de una directiva de cumplimiento de dispositivos macOS con Intune.

Inscripción de dispositivos

Aplicar perfil de Autopilot para dispositivos Windows 10 inscritos que aún no están registrados para Autopilot

Puede aplicar perfiles de Autopilot para dispositivos Windows 10 inscritos que aún no se han registrado para Autopilot. En el perfil de Autopilot, elija la opción **Convertir todos los dispositivos de destino a Autopilot** para registrar automáticamente los dispositivos que no se han registrado para Autopilot con los servicios de implementación de Autopilot. Permita un plazo de 48 horas para que se procese el registro. Cuando se anule la inscripción del dispositivo y este se restablezca, Autopilot lo aprovisionará.

Crear y asignar varios perfiles de la página Estado de inscripción a grupos de Azure AD

Ya puede crear y asignar varios perfiles de la página Estado de inscripción a grupos de Azure AD.

Migración desde el Programa de inscripción de dispositivos a Apple Business Manager en Intune

Apple Business Manager (ABM) funciona en Intune, así que puede actualizar su cuenta desde el Programa de inscripción de dispositivos (DEP) a ABM. El proceso en Intune es el mismo. Para actualizar la cuenta de Apple de DEP a ABN, vaya a https://support.apple.com/HT208817.

Pestañas de estado de alerta e inscripción en la página de información general de inscripción de dispositivos

Ahora, las alertas y los errores de inscripción aparecen en pestañas distintas en la página de información general de inscripción de dispositivos.

Informe de abandono de la inscripción

Un nuevo informe en el que se proporciona información detallada sobre las inscripciones abandonadas está disponible en **Inscripción de dispositivos** > **Supervisión**. Para obtener más información, vea Company portal abandonment report (Informe de abandono del portal de empresa).

Nuevos característica de términos de uso de Azure Active Directory

Azure Active Directory tiene una característica de términos de uso que puede usar en lugar de los términos y condiciones existentes de Intune. La característica de términos de uso de Azure AD proporciona más flexibilidad sobre qué términos se van a mostrar y cuándo, mejor compatibilidad de localización, mayor control sobre cómo se representan los términos y creación de informes mejorada. La característica de términos de uso de Azure AD requiere Azure Active Directory Premium P1, que también forma parte del conjunto de aplicaciones Enterprise Mobility + Security E3. Para más información, vea el artículo Administrar los términos y condiciones de acceso de los usuarios de su empresa.

Compatibilidad con el modo de propietario del dispositivo Android

Para Samsung Knox Mobile Enrollment, Intune ahora admite la inscripción de dispositivos en el modo de administración de propietario del dispositivo Android. Los usuarios en redes Wi-Fi o de telefonía móvil se pueden inscribir con unas pocas pulsaciones al encender sus dispositivos por primera vez. Para más información, vea Automatically enroll Android devices by using Samsung's Knox Mobile Enrollment (Inscripción automática de dispositivos Android mediante Samsung Knox Mobile Enrollment).

Administración de dispositivos

Nuevas configuraciones para actualizaciones de software

- Ahora puede configurar algunas notificaciones para avisar a los usuarios finales sobre los reinicios necesarios para finalizar la instalación de las actualizaciones de software más recientes.
- Ahora puede configurar un mensaje de advertencia de reinicio para los reinicios que se producen fuera de las horas de trabajo. Estos mensajes admiten escenarios BYOD.

Agrupación de dispositivos inscritos en Windows Autopilot por identificador de correlación

Intune ahora admite la agrupación de dispositivos Windows mediante un identificador de correlación cuando se inscriban mediante AutoPilot para dispositivos existentes con Configuration Manager. El identificador de correlación es un parámetro del archivo de configuración de AutoPilot. Intune establecerá de forma automática el atributo enrollmentProfileName de dispositivo de Azure AD para que sea igual a "OfflineAutopilotprofile-". Esto permite la creación de grupos dinámicos de Azure AD arbitrarios en función del identificador de correlación a través del atributo enrollmentprofileName para las inscripciones de AutoPilot sin conexión. Para obtener más información, consulte Windows Autopilot para dispositivos existentes.

Directivas de protección de aplicaciones de Intune

Las directivas de protección de aplicaciones de Intune permiten configurar varias opciones de protección de datos para aplicaciones protegidas de Intune, como Microsoft Outlook y Microsoft Word. Se ha cambiado la apariencia de estas opciones para iOS y Android a fin de facilitar su detección de forma individual. Hay tres categorías de configuraciones de directiva:

- **Reubicación de datos** : este grupo incluye los controles de prevención de pérdida de datos (DLP), como restricciones para cortar, copiar, pegar y guardar como. Esta configuración determina cómo los usuarios interactúan con los datos en las aplicaciones.
- **Requisitos de acceso**: este grupo contiene las opciones de PIN por aplicación que determinan cómo el usuario final tiene acceso a las aplicaciones en un contexto de trabajo.
- **Inicio condicional** : este grupo contiene configuraciones como la configuración mínima del sistema operativo, la detección de dispositivos liberados o modificados y períodos de gracia sin conexión.

No cambia la funcionalidad de la configuración, pero será más fácil encontrarla cuando se trabaja en el flujo de creación de la directiva.

Restricción de aplicaciones y bloqueo del acceso a los recursos de la compañía dispositivos Android

En **Conformidad de dispositivos** > **Directivas** > **Crear directiva** > **Android** > **Seguridad del sistema**, hay un nuevo valor en la sección *Seguridad del dispositivo* que se llama **Aplicaciones restringidas**. El valor **Aplicaciones restringidas** usa una directiva de cumplimiento para bloquear el acceso a recursos de la compañía si ciertas aplicaciones están instaladas en el dispositivo. El dispositivo se considera no compatible hasta que las aplicaciones restringidas se quitan del dispositivo. Se aplica a:

- Android

Aplicaciones de Intune

Intune admitirá un tamaño de paquete máximo de 8 GB para las aplicaciones de línea de negocio

Intune aumentó el tamaño de paquete máximo a 8 GB para las aplicaciones de línea de negocio (LOB). Para más información, vea Agregar aplicaciones a Microsoft Intune.

Adición de una imagen de marca personalizada para la aplicación Portal de empresa

Como administrador de Microsoft Intune, puede cargar una imagen de marca personalizada que se mostrará como imagen de fondo en la página de perfil del usuario en la aplicación Portal de empresa de iOS. Para

obtener más información sobre cómo configurar la aplicación Portal de empresa, vea How to configure the Microsoft Intune Company Portal app (Cómo configurar la aplicación Portal de empresa de Microsoft Intune).

Intune mantendrá el idioma de Office localizado al actualizar Office en los equipos de los usuarios finales

Cuando Intune instala Office en los equipos de los usuarios finales, estos recibirán automáticamente los mismos paquetes de idioma que tenían con las instalaciones de Office .MSI anteriores. Para obtener más información, vea Asignación de aplicaciones de Microsoft 365 a dispositivos Windows 10 con Microsoft Intune.

Supervisión y solución de problemas

Nueva experiencia de soporte técnico de Intune en el portal de administración de dispositivos de Microsoft 365

Se va a lanzar una nueva experiencia de ayuda y soporte técnico para Intune en el portal de administración de dispositivos de Microsoft 365. La nueva experiencia le permite describir el problema con sus propias palabras y recibir información sobre solución de problemas y contenido de corrección basado en la Web. Estas soluciones se ofrecen mediante un algoritmo de aprendizaje automático con reglas, basado en las consultas de los usuarios.

Además de instrucciones específicas del problema, también puede utilizar el nuevo flujo de trabajo de creación de casos para abrir una incidencia de soporte técnico por teléfono o correo electrónico.

Los clientes que forman parte del lanzamiento, esta nueva experiencia reemplaza la actual experiencia de ayuda y soporte técnico de un conjunto estático de opciones previamente seleccionadas que se basan en el área de la consola en la que se encuentra cuando abre la sección Ayuda y soporte técnico.

Esta nueva experiencia de ayuda y soporte técnico se va a lanzar para algunos pero no todos los inquilinos y está disponible en el portal de administración de dispositivos. Los participantes de esta nueva experiencia se seleccionan aleatoriamente entre los inquilinos de Intune disponibles. Se agregarán nuevos inquilinos a medida que se expanda el lanzamiento.

Para obtener más información, vea Nueva experiencia de Ayuda y soporte técnico en Cómo obtener asistencia para Microsoft Intune.

Módulo de PowerShell para Intune: versión preliminar disponible

Ya hay disponible en GitHub una versión preliminar de un nuevo módulo de PowerShell, que proporciona compatibilidad con la API de Intune a través de Microsoft Graph. Para obtener más información sobre cómo usar este módulo, consulte el archivo Léame en esa ubicación.

Septiembre de 2018

Administración de aplicaciones

Eliminación de la duplicación de los iconos de estado de protección de la aplicación

Los iconos **Estado del usuario para iOS** y **Estado del usuario para Android** estaban presentes en las páginas **Aplicaciones cliente: Información general** y **Aplicaciones cliente: Estado de protección de la aplicación**. Se han quitado los iconos de estado de la página **Aplicaciones cliente: Información general** para evitar la duplicación.

Configuración del dispositivo

Compatibilidad con más entidades de certificación de terceros (CA)

Si usa el protocolo de inscripción de certificados Simple (SCEP), ya puede emitir nuevos certificados y renovarlos en dispositivos móviles con Windows, iOS, Android y macOS.

Inscripción de dispositivos

Intune cambia para admitir iOS 10 y versiones posteriores

Ahora la inscripción de Intune, el Portal de empresa y el explorador administrado incluyen dispositivos iOS que tengan solo la versión iOS 10 y posteriores. Para comprobar si hay dispositivos o usuarios que se vean afectados en la organización, vaya a Intune en Azure Portal > **Dispositivos** > **Todos los dispositivos**. Filtre por sistema operativo y, después, haga clic en **Columnas** para mostrar los detalles de la versión de sistema

operativo. Pida a los usuarios que actualicen sus dispositivos a una versión del sistema operativo que sea compatible.

Si posee o quiere inscribir alguno de los siguientes dispositivos, debe estar al tanto de que solo admiten iOS 9 y versiones anteriores. Para seguir accediendo al Portal de empresa de Intune, debe actualizar estos dispositivos a dispositivos compatibles con iOS 10 o versiones posteriores:

- iPhone 4S
- iPod Touch
- iPad 2
- iPad (3ª generación)
- iPad Mini (1ª generación)

Administración de dispositivos

Centro de Administración de dispositivos de Microsoft 365

Una de las promesas de Microsoft 365 es la simplificación de la administración. Con los años, hemos ido integrando servicios de Microsoft 365 back-end para entregar escenarios de extremo a extremo, como el acceso condicional de Intune y Azure AD. El nuevo Centro de administración de Microsoft 365 consolida, simplifica e integra la experiencia de administración. El área de trabajo especialista en administración de dispositivos proporciona fácil acceso a todas las tareas y la información relacionadas con la administración de dispositivos y aplicaciones que necesita su organización. Esperamos que esto se convierta en el área de trabajo principal en la nube para los equipos informáticos de usuario final de empresa.

Agosto de 2018

Administración de aplicaciones

Compatibilidad de túnel de paquete para perfiles de VPN por aplicación de iOS para los tipos de conexión Pulse Secure y personalizados

Al usar perfiles de VPN por aplicación de iOS, puede elegir entre usar tunelización de capa de aplicación (app-proxy) o tunelización de nivel de paquete (packet-tunnel). Estas opciones están disponibles con los tipos de conexión siguientes:

- VPN personalizada
- Pulse Secure. Si no está seguro de qué valor usar, consulte la documentación de su proveedor de VPN.

Retraso cuando las actualizaciones de software de iOS se muestran en el dispositivo

En Intune > **Actualizaciones de software** > **Directivas de actualización para iOS**, puede configurar los días y las horas en los que no desea que los dispositivos instalen ninguna actualización. En una actualización futura, podrá retrasar entre 1 y 90 días el momento en el que una actualización de software se muestra de forma visible en el dispositivo. Configurar directivas de actualización de iOS en Microsoft Intune enumera la configuración actual.

Versión de las Aplicaciones de Microsoft 365 para empresas

Al asignar las Aplicaciones de Microsoft 365 para aplicaciones empresariales a dispositivos Windows 10 mediante Intune, podrá seleccionar la versión de Office. En Azure Portal, seleccione **Microsoft Intune** > **Aplicaciones** > **Agregar aplicación**. Después, seleccione **Conjunto de aplicaciones Office 365 ProPlus (Windows 10)** en la lista desplegable **Tipo**. Seleccione **Configuración del conjunto de aplicaciones** para mostrar la hoja asociada. Establezca **Canal de actualización** en un valor, como **Mensualmente**. Si lo desea, quite otra versión de Office (msi) de los dispositivos del usuario final seleccionando **Sí**. Seleccione **Específico** para instalar una versión específica de Office del canal seleccionado en los dispositivos del usuario final. En este momento, en **Versión específica**, puede seleccionar la versión de Office que desee usar. Las versiones disponibles cambiarán con el tiempo. Por lo tanto, al crear una nueva implementación, las versiones disponibles pueden ser más recientes y no tener determinadas versiones anteriores disponibles. Las implementaciones actuales seguirán implementando la versión anterior, pero la lista de versiones se actualizará continuamente por

canal. Para más información, vea Información general de los canales de actualización para Aplicaciones de Microsoft 365.

Compatibilidad con la configuración de DNS de registro para VPN de Windows 10

Con esta actualización, puede configurar perfiles de VPN de Windows 10 para registrar dinámicamente las direcciones IP asignadas a la interfaz VPN con el DNS interno, sin necesidad de usar perfiles personalizados. Para obtener información sobre la configuración de perfil de VPN actual disponible, vea Configuración de VPN de Windows 10.

El instalador de Portal de empresa para macOS ahora incluye el número de versión en el nombre de archivo del instalador

Actualizaciones de aplicaciones automáticas de iOS

Las actualizaciones de aplicaciones automáticas funcionan para las aplicaciones con licencia de dispositivo y usuario para la versión 11.0 de iOS y versiones posteriores.

Configuración del dispositivo

Windows Hello estará dirigido a usuarios y dispositivos

Cuando crea una directiva Windows Hello para empresas, se aplica a todos los usuarios dentro de la organización (inquilinos). Con esta actualización, la directiva también se puede aplicar a determinados usuarios o específicos mediante una directiva de configuración de dispositivo (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Identity Protection** > **Windows Hello para empresas**). En Intune en Azure Portal, la configuración de Windows Hello ahora existe tanto en **Inscripción del dispositivo** como en **Configuración del dispositivo**. **Inscripción del dispositivo** tiene como destino toda la organización (inquilinos) y es compatible con Windows AutoPilot (OOBE). **Configuración del dispositivo** tiene como destino los dispositivos y usuarios mediante una directiva que se aplica durante la inserción en el repositorio. Esta característica se aplica a:

- Windows 10 y versiones posteriores
- Windows Holographic for Business

Zscaler es una conexión disponible para los perfiles VPN en iOS

Cuando crea un perfil de configuración de dispositivo de VPN para iOS (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > plataforma **iOS** > tipo de perfil **VPN**), hay varios tipos de conexión, incluidos Cisco, Citrix, etc. Esta actualización agrega Zscaler como un tipo de conexión. Configuración de VPN para dispositivos que ejecutan iOS enumera los tipos de conexión disponibles.

Modo FIPS para perfiles de Wi-Fi de empresa para Windows 10

Ahora puede habilitar el modo Estándar federal de procesamiento de información (FIPS) para los perfiles de Wi-Fi de empresa para Windows 10 en Intune en Azure Portal. Asegúrese de que el modo FIPS está habilitado en la infraestructura de Wi-Fi si lo habilita en los perfiles de Wi-Fi. En Configuración de Wi-Fi para dispositivos Windows 10 y versiones posteriores en Intune se muestra cómo crear un perfil de Wi-Fi.

Control del modo S en Windows 10 y dispositivos posteriores: versión preliminar pública

Con esta actualización de características, puede crear un perfil de configuración de dispositivo que haga cambiar el modo S de un dispositivo Windows 10 o evitar que los usuarios cambien el modo S del dispositivo. Esta característica está en Intune > **Configuración del dispositivo** > **Perfiles** > **Windows 10 y versiones posteriores** > **Edition upgrade and mode switch (Actualización de edición y conmutación de modo)** . En Presentamos Windows 10 en modo S se proporciona más información sobre el modo S. Se aplica a: la compilación más reciente de Windows Insider (todavía en versión preliminar).

Paquete de configuración de Windows Defender for Endpoint agregado automáticamente al perfil de configuración

Al usar Defender for Endpoint y la incorporación de dispositivos en Intune, antes era necesario descargar un paquete de configuración y agregarlo al perfil de configuración. Con esta actualización, Intune obtiene de forma automática el paquete del Centro de seguridad avanzada de Windows Defender y lo agrega al perfil. Se aplica a Windows 10 y versiones posteriores.

Requerir que los usuarios se conecten durante la instalación del dispositivo

Ahora puede establecer los perfiles de dispositivo para requerir que el dispositivo se conecte a una red antes de

continuar más allá de la página Red durante la instalación de Windows 10. Aunque esta característica está en versión preliminar, se requiere una compilación 1809 de Windows Insider o una versión posterior para usar esta configuración. Se aplica a: la compilación más reciente de Windows Insider (todavía en versión preliminar).

Restricción de aplicaciones y bloqueo del acceso a los recursos de la empresa en dispositivos iOS y Android Enterprise

En **Conformidad de dispositivos** > **Directivas** > **Crear directiva** > **iOS** > **Seguridad del sistema**, hay una nueva opción **Aplicaciones restringidas**. Esta nueva opción usa una directiva de cumplimiento para bloquear el acceso a recursos de la compañía si ciertas aplicaciones están instaladas en el dispositivo. El dispositivo se considera no compatible hasta que las aplicaciones restringidas se quitan del dispositivo. Se aplica a iOS.

Actualizaciones de compatibilidad con VPN moderna para iOS

Esta actualización agrega compatibilidad con los siguientes clientes VPN de iOS:

- F5 Access (versión 3.0.1 y versiones posteriores)
- SSO de Citrix
- GlobalProtect de Palo Alto Networks versión 5.0 y versiones posteriores. También en esta actualización:
- El nombre del tipo de conexión de **F5 Access** existente se cambia a **F5 Access Legacy** para iOS.
- El nombre del tipo de conexión de **GlobalProtect de Palo Alto Networks** existente se cambia a **GlobalProtect de Palo Alto Networks (legacy)** para iOS. Los perfiles existentes con estos tipos de conexión siguen funcionando con su correspondiente cliente heredado de VPN. Si usa Cisco Legacy AnyConnect, F5 Access Legacy, Citrix VPN o GlobalProtect de Legacy Palo Alto Networks versión 4.1 y versiones anteriores con iOS, debe cambiar a las nuevas aplicaciones. Hágalo tan pronto como sea posible para garantizar que el acceso VPN esté disponible para dispositivos iOS a medida que se actualicen a iOS 12. Para obtener más información sobre iOS 12 y los perfiles de VPN, vea el blog del equipo de soporte técnico de Microsoft Intune.

Exportación de las directivas de cumplimiento del Portal de Azure clásico para volver a crearlas en Intune en Azure Portal

Las directivas de cumplimiento creadas en el Portal de Azure clásico dejarán de utilizarse. Puede revisar y eliminar todas las directivas de cumplimiento existentes, pero no podrá actualizarlas. Si tiene que migrar las directivas de cumplimiento a Intune en Azure Portal, puede exportarlas como un archivo separado por comas (archivo *.csv*). Después, use los detalles del archivo para volver a crear estas directivas en Intune en Azure Portal.

> **IMPORTANT**
> Cuando se retire el Portal de Azure clásico, ya no podrá acceder ni ver las directivas de cumplimiento. Por tanto, asegúrese de exportar las directivas y volverlas a crear en Azure Portal antes de la retirada del Portal de Azure clásico.

Better Mobile: nuevo socio de Mobile Threat Defense

Puede controlar el acceso desde dispositivos móviles a los recursos corporativos mediante el acceso condicional basado en la evaluación de riesgos efectuada por Better Mobile, una solución de Mobile Threat Defense integrada en Microsoft Intune.

Inscripción de dispositivos

Bloqueo del Portal de empresa en el modo de aplicación única hasta el inicio de sesión del usuario

Ahora tiene la opción de ejecutar Portal de empresa en el modo de aplicación única si autentica un usuario a través de Portal de empresa en lugar del Asistente para configuración durante la inscripción de DEP. Esta opción bloquea el dispositivo inmediatamente después de completar el Asistente para configuración, de manera que un usuario debe iniciar sesión para acceder al dispositivo. Este proceso garantiza que el dispositivo completa la incorporación y no está huérfano en un estado sin ningún usuario asociado.

Asignación de un usuario y un nombre descriptivo a un dispositivo AutoPilot

Ahora puede asignar un usuario a un único dispositivo Autopilot . Los administradores también podrán proporcionar nombres descriptivos para saludar a los usuarios al configurar sus dispositivos con AutoPilot. Se

aplica a: la compilación más reciente de Windows Insider (todavía en versión preliminar).

Uso de licencias de dispositivo de VPP para el aprovisionamiento previo de Portal de empresa durante la inscripción de DEP

Ahora puede usar licencias de dispositivo del Programa de compras por volumen (VPP) para aprovisionar previamente Portal de empresa durante las inscripciones en el Programa de inscripción de dispositivos (DEP). Para ello, al crear o editar un perfil de inscripción, especifique el token de VPP que quiera usar para instalar Portal de empresa. Asegúrese de que el token no expire y que dispone de suficientes licencias para la aplicación de Portal de empresa. En los casos en los que el token expire o se agoten las licencias, Intune instalará el Portal de empresa del App Store (se solicitará un identificador de Apple).

Confirmación requerida para eliminar el token de VPP que se usa para preaprovisionar el Portal de empresa

Ahora se solicita confirmación para eliminar un token del Programa de Compras por Volumen (VPP) si se usa para preaprovisionar el Portal de empresa durante la inscripción de DEP.

Bloqueo de inscripciones de dispositivos personales Windows

Puede bloquear la inscripción de dispositivos personales Windows con la administración de dispositivos móviles en Intune. Los dispositivos inscritos con el agente de PC de Intune no se puede bloquear con esta característica. Esta característica se desplegará gradualmente durante las próximas semanas, por lo que quizá no la vea de inmediato en la interfaz de usuario.

Especificación de patrones de nombre de equipo en un perfil de AutoPilot

Puede especificar una plantilla de nombre de equipo para generar y establecer el nombre de equipo durante la inscripción de AutoPilot. Se aplica a: la compilación más reciente de Windows Insider (todavía en versión preliminar).

Para los perfiles de Windows AutoPilot, se ocultan las opciones de cambio de cuenta en las páginas de inicio de sesión y de error de dominio de la empresa

Hay nuevas opciones de perfil de Windows AutoPilot para que los administradores oculten las opciones de cambio de cuenta en las páginas de inicio de sesión de la empresa y de error de dominio. La ocultación de estas opciones requiere que se configure la personalización de marca de empresa en Azure Active Directory. Se aplica a: la compilación más reciente de Windows Insider (todavía en versión preliminar).

Compatibilidad de macOS para el Programa de inscripción de dispositivos de Apple

Intune ahora admite la inscripción de dispositivos macOS el Programa de inscripción de dispositivos de Apple (DEP). Para obtener más información, vea Inscripción automática de dispositivos macOS con el Programa de inscripción de dispositivos de Apple.

Administración de dispositivos

Eliminación de dispositivos Jamf

Puede eliminar los dispositivos administrados por JAMF desde **Dispositivos** > seleccione el dispositivo de Jamf > **Eliminar**.

Cambio de terminología para "retirar" y "borrar"

Para mantener la coherencia con Graph API, en la documentación y la interfaz de usuario de Intune se han cambiado los términos siguientes:

- **Eliminar datos de la compañía** se cambiará por "retirar".
- **Restablecimiento de fábrica** cambiará a **borrar**

Cuadro de diálogo de confirmación si el administrador intenta eliminar el certificado push MDM

Si alguien intenta eliminar un certificado push MDM de Apple, en un cuadro de diálogo de confirmación se muestra el número de dispositivos iOS y macOS relacionados. Si se elimina el certificado, será necesario volver a inscribir estos dispositivos.

Configuración de seguridad adicional de Windows Installer

Puede dejar que los usuarios controlen las instalaciones de aplicaciones. Si lo permite, las instalaciones que antes se detendrían debido a una infracción de seguridad podrán seguir funcionando. Puede indicar a Windows Installer que use permisos elevados cuando instale un programa en un sistema. Además, los elementos

protegidos por WIP (Windows Information Protection) se pueden indexar y los metadatos relativos a estos elementos se pueden almacenar en una ubicación sin cifrar. Cuando la directiva está deshabilitada, los elementos protegidos por WIP no se indexan y no se muestran en los resultados de Cortana o del explorador de archivos. La funcionalidad de estas opciones está deshabilitada de forma predeterminada.

Nueva actualización de la experiencia de usuario para el sitio web del Portal de empresa

Tras escuchar los comentarios de los clientes, hemos agregado características nuevas al sitio web de Portal de empresa. Experimentará una mejora considerable en las funciones y la facilidad de uso actual de los dispositivos. Se ha aplicado un nuevo diseño moderno y dinámico a las áreas del sitio, como los detalles del dispositivo, los comentarios, el soporte técnico y la descripción general del dispositivo. También verá:

- Flujos de trabajo optimizados en todas las plataformas de dispositivo
- Flujos mejorados para la inscripción e identificación de dispositivos
- Mensajes de error más útiles
- Lenguaje más descriptivo y menos terminología técnica
- Capacidad de compartir vínculos directos a aplicaciones
- Rendimiento mejorado de los catálogos de aplicaciones de gran tamaño
- Aumento de accesibilidad para todos los usuarios

Se ha actualizado la documentación del sitio web de Portal de empresa de Intune para reflejar estos cambios. Para ver un ejemplo de las mejoras de la aplicación, vea Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune.

Supervisión y solución de problemas

Detección de jailbreak mejorada en informes de cumplimiento

Ahora la configuración de detección de jailbreak mejorada aparece en todos los informes de cumplimiento en la consola de administración.

Control de acceso basado en roles.

Etiquetas de ámbito para las directivas

Puede crear etiquetas de ámbito para limitar el acceso a los recursos de Intune. Agregue una etiqueta de ámbito a una asignación de roles y luego agregue dicha etiqueta a un perfil de configuración. El rol solo tendrá acceso a los recursos con perfiles de configuración que tengan etiquetas de ámbito coincidentes (o no tengan ninguna etiqueta de ámbito).

Julio de 2018

Administración de aplicaciones

Compatibilidad con aplicaciones de línea de negocio (LOB) para macOS

Microsoft Intune permite implementar aplicaciones de LOB macOS como **Required** (Obligatoria) o como **Available with enrollment** (Disponible con inscripción). Los usuarios finales pueden obtener las aplicaciones implementadas como **Available** (Disponible) a través del Portal de empresa para macOS o del sitio web del Portal de empresa.

Compatibilidad con aplicaciones integradas de iOS para pantalla completa

Además de las aplicaciones de la Tienda y las aplicaciones administradas, ahora puede seleccionar una aplicación integrada (como Safari) que se ejecuta en pantalla completa en un dispositivo iOS.

Edición de las Aplicaciones de Microsoft 365 para implementaciones de aplicaciones empresariales

Como administrador de Microsoft Intune, tiene más capacidad para editar las Aplicaciones de Microsoft 365 para implementaciones de aplicaciones empresariales. Además, ya no tiene que eliminar las implementaciones para cambiar las propiedades del conjunto. En Azure Portal, seleccione **Microsoft Intune** > **Aplicaciones cliente** > **Aplicaciones**. En la lista de aplicaciones, seleccione su conjunto de Aplicaciones de Microsoft 365 para empresas.

El SDK de aplicaciones de Intune para Android ya está disponible

Hay disponible una versión actualizada del SDK para aplicaciones de Intune para Android compatible con la versión de Android P. Si es desarrollador de aplicaciones y usa el SDK de Intune para Android, debe instalar la versión actualizada del SDK para aplicaciones de Intune a fin de garantizar que la funcionalidad de Intune dentro de las aplicaciones Android seguirá funcionando según lo esperado en dispositivos de Android P. Esta versión del SDK de aplicaciones de Intune ofrece un complemento integrado que realiza las actualizaciones del SDK. No es necesario que reescriba ningún código existente que ya esté integrado. Para detalles, consulte el artículo sobre el SDK de Intune para Android. Si usa el anterior estilo de distintivo para Intune, se recomienda usar el icono de maletín. Para detalles de personalización de la marca, consulte este repositorio de GitHub.

Más oportunidades para la sincronización en la aplicación de Portal de empresa para Windows

La aplicación Portal de empresa para Windows ahora permite iniciar una sincronización directamente desde la barra de tareas de Windows y el menú Inicio. Esta característica es especialmente útil si la única tarea es sincronizar los dispositivos y obtener acceso a los recursos corporativos. Para acceder a la nueva característica, haga clic con el botón derecho en el icono de Portal de empresa que está anclado a la barra de tareas o el menú Inicio. En las opciones de menú (también denominada lista de accesos directos), seleccione **Sincronizar este dispositivo**. El Portal de empresa se abrirá en la página **Configuración** e iniciará la sincronización. Para comprobar la nueva funcionalidad, vea Novedades de la interfaz de usuario.

Nuevas experiencias de navegación en la aplicación Portal de empresa para Windows

Ahora al examinar o buscar aplicaciones en la aplicación Portal de empresa para Windows, puede alternar entre la vista **Iconos** existente y la vista **Detalles** recién agregada. En la nueva vista se muestran detalles de la aplicación, como el nombre, el editor, la fecha de publicación y el estado de la instalación.

La vista **Instaladas** de la página **Aplicaciones** le permite ver detalles sobre las instalaciones de aplicaciones completadas y en curso. Para ver el aspecto de la vista nueva, vea Novedades de la interfaz de usuario.

Mejora de la experiencia en la aplicación Portal de empresa para administradores de inscripciones de dispositivos

Cuando un administrador de inscripciones de dispositivos (DEM) inicia sesión en la aplicación Portal de empresa para Windows, ahora la aplicación solo mostrará el dispositivo en ejecución actual de DEM. Esta mejora reducirá los tiempos de espera que se producían anteriormente cuando la aplicación intentaba mostrar todos los dispositivos inscritos en DEM.

Bloqueo del acceso a aplicaciones según proveedores y modelos de dispositivos no aprobados

El administrador de TI de Intune puede aplicar una lista específica de fabricantes de dispositivos Android o modelos de iOS a través de las directivas de Intune App Protection. El administrador de TI puede brindar una lista de fabricantes separados por punto y coma para las directivas Android y los modelos de dispositivo para las directivas iOS. Las directivas de Intune App Protection solo son para Android e iOS. Se pueden realizar dos acciones independientes en esta lista especificada:

- Bloquear el acceso a la aplicación en dispositivos no especificados.
- O bien, borrar de manera selectiva los datos corporativos en dispositivos no especificados.

El usuario no podrá acceder a la aplicación de destino si no se cumplen los requisitos que establece la directiva. En función de la configuración, se podrá bloquear al usuario o borrar de manera selectiva sus datos corporativos dentro de la aplicación. En dispositivos iOS, esta característica requiere el uso de ciertas aplicaciones (como WXP, Outlook, Managed Browser o Yammer) para integrar Intune APP SDK para que esta característica se aplique en las aplicaciones de destino. Esta integración ocurre de manera gradual y depende de los equipos de la aplicación específica. En Android, esta característica requiere la versión más reciente de Portal de empresa.

En dispositivos de usuario final, el cliente de Intune actúa en función de una coincidencia simple de las cadenas especificadas en la hoja de Intune para directivas de protección de aplicaciones. Esto depende por completo del valor que informa el dispositivo. Por lo tanto, se recomienda que el administrador de TI se asegure de que el comportamiento previsto sea preciso. Para ello, pruebe esta configuración en función de una variedad de fabricantes de dispositivos y de modelos dirigidos a un grupo de usuarios pequeño. En Microsoft Intune,

seleccione **Aplicaciones cliente** > **Directivas de protección de aplicaciones** para ver y agregar directivas de protección de aplicaciones. Para obtener más información sobre las directivas de protección de aplicaciones, vea ¿Qué son las directivas de protección de aplicaciones? y Borrar los datos de forma selectiva mediante acciones de acceso de la directiva de protección de aplicaciones en Intune.

Acceso a la compilación de versión preliminar del Portal de empresa de macOS

Con Microsoft AutoUpdate, puede registrarse para recibir antes las compilaciones si se une al programa Insider. El registro le permite usar Portal de empresa actualizado antes de que esté disponible para los usuarios finales. Para obtener más información, vea el blog de Microsoft Intune.

Configuración del dispositivo

Creación de directivas de cumplimiento de dispositivos mediante la configuración de firewall en dispositivos macOS

Cuando se crea una directiva de cumplimiento de macOS (**Conformidad de dispositivos** > **Directivas** > **Crear directiva** > **Plataforma: macOS** > **Seguridad del sistema**), hay nuevas opciones de **Firewall** disponibles:

- **Firewall**: configure cómo se administran las conexiones entrantes en el entorno.
- **Conexiones entrantes**: **bloquee** todas las conexiones entrantes excepto las necesarias para los servicios básicos de Internet, como DHCP, Bonjour e IPSec. Esta opción también bloquea todos los servicios de uso compartido.
- **Modo sigiloso**: **habilite** el modo sigiloso para evitar que el dispositivo responda a solicitudes de sondeo. El dispositivo sigue respondiendo a las solicitudes entrantes de las aplicaciones autorizadas.

Se aplica a: macOS 10.12 y versiones posteriores

Nuevo perfil de configuración de dispositivos Wi-Fi para Windows 10 y versiones posteriores

Actualmente, puede importar y exportar perfiles de Wi-Fi mediante archivos XML. Con esta actualización, puede crear un perfil de configuración de dispositivo Wi-Fi directamente en Intune, igual que en otras plataformas.

Para crear el perfil, abra **Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** > **Wi-Fi**.

Se aplica a Windows 10 y versiones posteriores.

La característica Quiosco (obsoleto) aparece atenuada y no se puede cambiar

La característica Quiosco (versión preliminar) (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Windows 10 y versiones posteriores** > **Restricciones de dispositivos**) está obsoleta y se sustituye por la configuración de Quiosco para Windows 10 y versiones posteriores. Con esta actualización, la característica **Quiosco (obsoleto)** está atenuada y la interfaz de usuario no se puede modificar ni actualizar.

Para habilitar el modo quiosco, vea Configuración de quiosco para Windows 10 (y versiones posteriores).

Se aplica a Windows 10 y versiones posteriores, Windows Holographic for Business

API para usar entidades de certificación de terceros

En esta actualización, hay una API de Java que permite que las entidades de certificación de terceros se integren con Intune y SCEP. Después, los usuarios pueden agregar el certificado SCEP a un perfil y aplicarlo a los dispositivos mediante MDM.

Actualmente, Intune admite solicitudes SCEP mediante Servicios de certificados de Active Directory.

Alternar para mostrar u ocultar el botón Finalizar sesión en un explorador de Quiosco

Ahora puede configurar si los exploradores de Quiosco muestran o no el botón Finalizar sesión. Puede ver el control en **Configuración del dispositivo** > **Quiosco (versión preliminar)** > **Kiosk Web Browser**. Si está activado, cuando un usuario hace clic en el botón, la aplicación solicita confirmación para finalizar la sesión. Cuando se confirma, el explorador borra todos los datos de exploración y vuelve a la dirección URL predeterminada.

Creación de un perfil de configuración de red de telefonía móvil eSIM

En **Configuración del dispositivo**, puede crear un perfil de red de telefonía móvil eSIM. Puede importar un archivo que contenga códigos de activación de red de telefonía móvil proporcionados por el operador de telefonía móvil. Después, puede implementar estos perfiles en sus dispositivos Windows 10 habilitados para eSIM LTE, como Surface Pro LTE y otros dispositivos compatibles con eSIM.

Compruebe si sus dispositivos admiten perfiles de eSIM.

Se aplica a Windows 10 y versiones posteriores.

Selección de las categorías de dispositivos mediante la configuración de acceso profesional o educativo

Si ha habilitado la asignación de grupos de dispositivos, ahora se pedirá a los usuarios de Windows 10 que seleccionen una categoría de dispositivo después de la inscripción a través del botón **Conectar** en **Configuración** > **Cuentas** > **Obtener acceso a trabajo o escuela**.

Uso de sAMAccountName como nombre de usuario de cuenta para perfiles de correo electrónico

Puede usar el nombre local **sAMAccountName** como nombre de usuario de cuenta de los perfiles de correo electrónico para Android, iOS y Windows 10. También puede obtener el dominio de los atributos `domain` o `ntdomain` en Azure Active Directory (Azure AD). O si lo prefiere, podrá especificar un dominio estático personalizado.

Para usar esta característica, debe sincronizar el atributo `sAMAccountName` desde el entorno de Active Directory local con Azure AD.

Se aplica a Android, iOS, Windows 10 y versiones posteriores

Visualización de perfiles de configuración de dispositivos en conflicto

En **Configuración del dispositivo**, se muestra una lista de los perfiles existentes. Con esta actualización, se agrega una nueva columna que proporciona información detallada sobre los perfiles que tienen un conflicto. Puede seleccionar una fila en conflicto para ver la configuración y el perfil que tiene el conflicto.

Obtenga más información sobre cómo administrar perfiles de configuración.

Nuevo estado para dispositivos en la conformidad de dispositivos

En **Conformidad de dispositivos** > **Directivas** > seleccione una directiva > **Información general**, se han agregado los estados nuevos siguientes:

- Correcto
- error
- Conflicto
- pending
- No aplicable: una imagen que también muestra el número de dispositivos de una plataforma diferente. Por ejemplo, si está buscando un perfil de iOS, el nuevo icono muestra el número de dispositivos que no son de iOS que también están asignados a este perfil. Vea Directivas de cumplimiento de dispositivos.

Conformidad de dispositivos compatible con soluciones antivirus de terceros

Cuando se crea una directiva de cumplimiento del dispositivo (**Cumplimiento del dispositivo** > **Directivas** > **Crear directiva** > **Plataforma: Windows 10 y versiones posteriores** > **Configuración** > **Seguridad del sistema**), hay nuevas opciones de **Seguridad del dispositivo** :

- **Antivirus**: cuando se establece en **Requerir**, puede comprobar el cumplimiento mediante soluciones antivirus registradas con Windows Security Center, como Symantec y Windows Defender.
- **Antispyware**: cuando se establece en **Requerir**, puede comprobar el cumplimiento mediante soluciones antispyware registradas con Windows Security Center, como Symantec y Windows Defender.

Se aplica a: Windows 10 y versiones posteriores

Inscripción de dispositivos

Marcado automático de dispositivos Android inscritos mediante Samsung Knox Mobile Enrollment como "corporativos".

De forma predeterminada, los dispositivos Android inscritos mediante Samsung Knox Mobile Enrollment ahora se marcan como **corporativos** en **Propiedad del dispositivo**. No es necesario identificar manualmente los dispositivos corporativos mediante IMEI o números de serie antes de realizar la inscripción mediante Knox Mobile Enrollment.

Dispositivos sin columna de perfiles en la lista de tokens del programa de inscripción

En la lista de tokens del programa de inscripción hay una nueva columna que muestra el número de dispositivos sin un perfil asignado. Esto ayuda a los administradores a asignar perfiles a estos dispositivos antes de entregarlos a los usuarios. Para ver la nueva columna, vaya a **Inscripción de dispositivos** > **Inscripción de Apple** > **Tokens del programa de inscripción**.

Administración de dispositivos

Eliminación en masa de dispositivos en la hoja de dispositivos

Ahora puede eliminar varios dispositivos a la vez en la hoja de dispositivos. Elija **Dispositivos** > **Todos los dispositivos** > seleccione los dispositivos que quiere eliminar > **Eliminar**. En el caso de los dispositivos que no se puedan eliminar, se mostrará una alerta.

Cambio de nombre en Google para Android for Work y Play for Work

Intune ha actualizado el término "Android for Work" para reflejar los cambios de personalización de marca de Google. Ya no se usan los términos "Android for Work" ni "Play for Work". Se usa otra terminología en función del contexto:

- "Android Enterprise" hace referencia a la pila de administración general de Android moderna.
- "Perfil de trabajo" o "Propietario de perfil" hacen referencia a dispositivos BYOD administrados con perfiles de trabajo.
- "Google Play administrada" hace referencia a la tienda de aplicaciones de Google.

Reglas para quitar dispositivos

Hay disponibles nuevas reglas que permiten quitar automáticamente dispositivos que no se hayan protegido durante un número de días que establezca. Para ver la nueva regla, vaya al panel **Intune**, seleccione **Dispositivos** y, luego, **Reglas de limpieza de dispositivos**.

Compatibilidad con dispositivos Android de un solo uso y propiedad corporativa

Ahora, Intune admite dispositivos Android de estilo quiosco, que estén bloqueados y con una elevada administración. De este modo, los administradores pueden bloquear aún más el uso de un dispositivo para restringir su uso a una sola aplicación o un pequeño conjunto de aplicaciones, impidiendo así que los usuarios habiliten otras aplicaciones o realicen otras acciones en el dispositivo. Para configurar el quiosco de Android, vaya a Intune > **Inscripción de dispositivos** > **Inscripción de Android** > **Inscripciones de dispositivos de tareas y quiosco**. Para obtener más información, vea Set up enrollment of Android enterprise kiosk devices (Configurar la inscripción de dispositivos de quiosco de Android Enterprise).

Revisión por fila de los identificadores de dispositivos corporativos duplicados cargados

Ahora, al cargar identificadores corporativos, Intune facilita una lista de cualquier dispositivo duplicado y ofrece la posibilidad de reemplazar o conservar la información existente. El informe se mostrará si hay duplicados después de elegir **Inscripción de dispositivos** > **Identificadores de dispositivos corporativos** > **Agregar identificadores**.

Adición manual de identificadores de dispositivos corporativos

Ahora puede agregar manualmente identificadores de dispositivos corporativos. Elija **Inscripción de dispositivos** > **Identificadores de dispositivos corporativos** > **Agregar**.

Junio de 2018

Administración de aplicaciones

Compatibilidad móvil de Microsoft Edge para directivas de protección de aplicaciones de Intune

El navegador Microsoft Edge para dispositivos móviles ahora admite las directivas de protección de aplicaciones

definidas en Intune.

Recuperación del identificador de modelo de usuario de la aplicación (AUMID) asociado para aplicaciones de Microsoft Store para Empresas en pantalla completa

Intune ya puede recuperar los identificadores de modelo de usuario de la aplicación (AUMID) para aplicaciones de Microsoft Store para Empresas (WSfB) con el fin de mejorar la configuración del perfil de pantalla completa.

Para más información sobre las aplicaciones de Microsoft Store para Empresas, consulte el artículo sobre la administración de aplicaciones de Microsoft Store para Empresas.

Nueva página de personalización de marca del Portal de empresa

La página de personalización de marca del Portal de empresa tiene un nuevo diseño, mensajes e información sobre herramientas.

Configuración del dispositivo

Pradeo: nuevo colaborador de Mobile Threat Defense

Puede controlar el acceso desde dispositivos móviles a recursos corporativos en función de la evaluación de riesgos efectuada por Pradeo, una solución de Mobile Threat Defense integrada con Microsoft Intune.

Uso del modo FIPS con el conector de certificado NDES

Al instalar el conector de certificado NDES en un equipo con el modo Estándar federal de procesamiento de información (FIPS) habilitado, la emisión y revocación de certificados no funciona según lo previsto. Con esta actualización, con el conector de certificado NDES se incluye la compatibilidad con FIPS.

Esta actualización también incluye:

- El conector de certificado NDES requiere .NET 4.5 Framework, que se incluye automáticamente con Windows Server 2016 y Windows Server 2012 R2. Anteriormente, .NET 3.5 Framework era la versión mínima requerida.
- Con el conector de certificado NDES se incluye la compatibilidad con TLS 1.2. Por tanto, si el servidor con el conector de certificado NDES instalado es compatible con TLS 1.2, entonces se usará TLS 1.2. Si el servidor no admite TLS 1.2, entonces se usará TLS 1.1. Actualmente, se usa TLS 1.1 para la autenticación entre los dispositivos y el servidor.

Para obtener más información, vea Configuración y uso de certificados SCEP y Configuración y uso de certificados PKCS.

Compatibilidad con perfiles de VPN de Palo Alto Networks GlobalProtect

Con esta actualización, puede elegir Palo Alto Networks GlobalProtect como un tipo de conexión VPN para perfiles de VPN en Intune (**Configuración del dispositivo** > **Perfiles** > **Crear perfil** > **Tipo de perfil** > **VPN**). En esta versión, se admiten las siguientes plataformas:

- iOS
- Windows 10

Adiciones a la configuración de opciones de seguridad del dispositivo local

Ya puede configurar opciones adicionales de seguridad del dispositivo local para dispositivos con Windows 10. Las opciones adicionales están disponibles en las áreas Cliente de redes de Microsoft, Servidor de red Microsoft, Acceso y seguridad de red e Inicio de sesión interactivo. Encuentre estos valores en la categoría de Endpoint Protection cuando cree una directiva de configuración de dispositivo de Windows 10.

Habilitación de la pantalla completa en dispositivos Windows 10

En los dispositivos Windows 10, puede crear un perfil de configuración y habilitar la pantalla completa (**Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **Windows 10** > **Restricciones de dispositivos** > **Quiosco**). En esta actualización, la configuración **Quiosco (versión preliminar)** cambia de nombre a **Quiosco (obsoleto)** . Ya no se recomienda usar **Quiosco (obsoleto)** , pero seguirá funcionando hasta la actualización de julio. El nuevo tipo de perfil **Quiosco** reemplaza a **Quiosco (obsoleto)** (**Crear perfil** > **Windows 10** > **Quiosco (versión preliminar)**), que contendrá los valores para configurar Quioscos en

Windows 10 RS4 y versiones posteriores.

Se aplica a Windows 10 y versiones posteriores.

Vuelve el gráfico de usuario del perfil del dispositivo

Si bien mejoraba el valor numérico que aparece en el gráfico del perfil del dispositivo (**Configuración de dispositivos** > **Perfiles** > seleccione un perfil existente > **Información general**), el gráfico de usuario se quitó de manera temporal.

Con esta actualización, dicho gráfico vuelve y aparece en Azure Portal.

Inscripción de dispositivos

Compatibilidad con la inscripción de Windows Autopilot sin autenticación de usuario

Intune admite la inscripción de Windows Autopilot sin autenticación de usuario. Se trata de una nueva opción en el perfil de implementación de Windows Autopilot "Modo de implementación Autopilot" establecido en "Self-Deploying" (Autoimplementable). El dispositivo debe ejecutar Windows 10 Insider Preview, compilación 17672 o posterior, y poseer un chip de TPM 2.0 para completar correctamente este tipo de inscripción. Puesto que no se requiere ninguna autenticación de usuario, solo puede asignar esta opción a dispositivos sobre los que tenga control físico.

Nueva configuración de idioma y región al realizar la configuración rápida de Autopilot

Hay disponible una nueva configuración para establecer el idioma y la región de los perfiles de Autopilot durante la configuración rápida. Para ver la nueva configuración, elija **Inscripción de dispositivos** > **Inscripción de Windows** > **Implementación perfiles** > **Crear perfil** > **Modo de implementación** = **Self-deploying (Autoimplementable)** > **Valores predeterminados configurados**.

Nuevo valor para configurar el teclado del dispositivo

Habrá disponible un valor nuevo para configurar el teclado de los perfiles de Autopilot durante la configuración rápida. Para ver la nueva configuración, elija **Inscripción de dispositivos** > **Inscripción de Windows** > **Implementación perfiles** > **Crear perfil** > **Modo de implementación** = **Self-deploying (Autoimplementable)** > **Valores predeterminados configurados**.

Los perfiles AutoPilot se migran a un destinatario de grupo

Se pueden asignar perfiles de implementación de AutoPilot a grupos de Azure AD que contengan dispositivos AutoPilot.

Administración de dispositivos

Establecimiento del cumplimiento por ubicación del dispositivo

En algunas situaciones, es posible que desee restringir el acceso a los recursos corporativos a una ubicación específica, definida por una conexión de red. Ya puede crear una directiva de cumplimiento (**Cumplimiento de dispositivos** > **Ubicaciones**) en función de la dirección IP del dispositivo. Si el dispositivo sale del intervalo IP, no podrá acceder a los recursos corporativos.

Se aplica a: Solo para dispositivos Android 6.0 y versiones posteriores, con la aplicación Portal de empresa actualizada.

Evitar aplicaciones y experiencias de consumidor en dispositivos Windows 10 Enterprise RS4 Autopilot

Puede evitar la instalación de aplicaciones y experiencias de consumidor en los dispositivos Windows 10 Enterprise RS4 Autopilot. Para ver esta característica, vaya a **Intune** > **Configuración de dispositivos** > **Perfiles** > **Crear perfil** > **Plataforma** = **Windows 10 o versiones posteriores** > **Tipo de perfil** = **Restricciones de dispositivo** > **Configurar** > **Windows Spotlight** > **Características de consumidor**.

Desinstalar las últimas actualizaciones de software de Windows 10

En caso de que detecte un problema importante en las máquinas con Windows 10, puede optar por desinstalar (revertir) la última actualización de características o la última actualización de calidad. La desinstalación de una actualización de característica o de calidad solo está disponible para el canal de servicio en el que se encuentra el dispositivo. La desinstalación desencadenará una directiva para restaurar la actualización anterior en las

máquinas con Windows 10. Para las actualizaciones de características concretamente, puede limitar el tiempo de 2 a 60 días durante el cual se puede aplicar una desinstalación de la versión más reciente. Para configurar las opciones de desinstalación de actualización de software, seleccione **Actualizaciones de software** en la hoja **Microsoft Intune** en el portal de Azure. Después, seleccione **Anillos de actualización de Windows 10** en la hoja **Actualizaciones de software**. Elija después la opción **Desinstalar** en la sección **Información general**.

Búsqueda del IMEI y número de serie en todos los dispositivos

Ya puede buscar IMEI y los números de serie en la hoja Todos los dispositivos (correo electrónico, UPN, nombre de dispositivo y nombre de la administración siguen estando disponibles). En Intune, elija **Dispositivos** > **Todos los dispositivos** y escriba la búsqueda en el cuadro de búsqueda.

El campo de nombre de administración se podrá editar

Ya puede editar el campo de nombre de administración en la hoja **Propiedades** de un dispositivo. Para editar este campo, elija **Dispositivos** > **Todos los dispositivos** > elija el dispositivo > **Propiedades**. Puede usar el campo de nombre de administración para identificar un dispositivo de manera única.

Nuevo filtro Todos los dispositivos: Categoría de dispositivo

Ya puede filtrar la lista **Todos los dispositivos** por categoría de dispositivo. Para ello, elija **Dispositivos** > **Todos los dispositivos** > **Filtro** > **Categoría de dispositivo**.

Uso de TeamViewer para compartir la pantalla de dispositivos iOS y macOS

Los administradores podrán conectarse a TeamViewer e iniciar una sesión de uso compartido de pantalla con dispositivos iOS y macOS. Los usuarios de iPhone, iPad y macOS pueden compartir sus pantallas en vivo con cualquier otro dispositivo móvil o de escritorio.

Compatibilidad con múltiples instancias de Exchange Connector

Ya no estará limitado a una instancia de Microsoft Intune Exchange Connector por inquilino. Intune admite varias instancias de Exchange Connector para que pueda configurar el acceso condicional de Intune con varias organizaciones de Exchange local.

Con un conector de Exchange local de Intune, se puede controlar el acceso de los dispositivos a los buzones de Exchange locales en función de si un dispositivo está inscrito en Intune y cumple con las directivas de cumplimiento de dispositivos de Intune. Para configurar un conector, descargue el conector de Exchange local de Intune desde Azure Portal e instálelo en un servidor en la organización de Exchange. En el panel de Microsoft Intune, elija **Acceso local** y, después, en **Instalación**, elija **Conector de Exchange ActiveSync**. Descargue el conector de Exchange local e instálelo en un servidor en la organización de Exchange. Ahora que ya no está limitado a un conector de Exchange por inquilino, si tiene otras organizaciones de Exchange, puede seguir el mismo proceso para descargar e instalar un conector para cada organización de Exchange adicional.

Nuevos detalles de hardware de dispositivo: CCID

La información de dispositivo de interfaz de tarjeta de chip (CCID) ya se incluye para cada dispositivo. Para verla, elija **Dispositivos** > **Todos los dispositivos** > elija un dispositivo > **Hardware**> compruebe en **Detalles de red**>

Asignación de todos los usuarios y dispositivos como grupos de ámbito

Podrá asignar todos los usuarios, todos los dispositivos y todos los usuarios y dispositivos en los grupos de ámbito. Para ello, elija **Roles de Intune** > **Todos los roles** > **Policy and profile manager (Administrador de directivas y perfiles)** > **Asignaciones** > elija una asignación > **Ámbito (grupos)** .

La información de UDID ahora se incluye para dispositivos iOS y macOS

Para ver el identificador único de dispositivo (UDID) para dispositivos iOS y macOS, vaya a **Dispositivos** > **Todos los dispositivos** > elija un dispositivo > **Hardware**. UDID solo está disponible para dispositivos corporativos, tal y como se configura en **Dispositivos** > **Todos los dispositivos** > dispositivo > **Propiedades** > **Propiedad del dispositivo**.

Aplicaciones de Intune

Solución de problemas mejorada para la instalación de aplicaciones

En algunas ocasiones, las instalaciones de aplicaciones en los dispositivos administrados por MDM de Microsoft Intune pueden presentar errores. Cuando esto ocurre, puede ser complicado entender el motivo del error o cómo solucionarlo. Incluimos una Versión preliminar pública de las características de solución de problemas de las aplicaciones. Verá un nodo nuevo bajo cada dispositivo individual denominado **Aplicaciones administradas**. En él aparecen las aplicaciones que se han entregado a través de MDM de Intune. Dentro del nodo, verá una lista de los estados de instalación de las aplicaciones. Si selecciona una aplicación individual, aparecerá la vista de solución de problemas de esa aplicación específica. En la vista de solución de problemas, verá el ciclo de vida completo de la aplicación, como cuándo se creó y modificó la aplicación, el momento en que se estableció su destino y cuándo se entregó a un dispositivo. Además, si la instalación de la aplicación no se realizó correctamente, verá el código de error y un mensaje útil sobre la causa del mismo.

Directivas de protección de aplicaciones de Intune y Microsoft Edge

Ahora, el explorador Microsoft Edge para dispositivos móviles (iOS y Android) admite directivas de protección de aplicaciones de Microsoft Intune. Intune protegerá a los usuarios de dispositivos iOS y Android que inicien sesión con sus cuentas corporativas de Azure AD en la aplicación Microsoft Edge. En dispositivos iOS, la directiva **Require managed browser for web content** (Requerir explorador administrado para contenido web) permitirá a los usuarios abrir vínculos en Microsoft Edge cuando esté administrado.

Mayo de 2018

Administración de aplicaciones

Configuración de las directivas de protección de aplicaciones

En Azure Portal, en lugar de dirigirse a la hoja del servicio Intune App Protection, solo tiene que ir a Intune. Ahora hay una única ubicación para las directivas de protección de aplicaciones en Intune. Tenga en cuenta que todas las directivas de protección de aplicaciones se encuentran en la hoja **Aplicación móvil** de Intune, en **Directivas de protección de aplicaciones**. Esta integración ayuda a simplificar la administración en la nube. Recuerde que todas las directivas de protección de aplicaciones ya están en Intune y que puede modificar cualquiera de las directivas configuradas anteriormente. Las directivas de protección de aplicaciones (APP) y acceso condicional (CA) de Intune se encuentran ahora en **Acceso condicional**, que se encuentra en la sección **Administrar** de la hoja **Microsoft Intune** o en la sección **Seguridad** de la hoja **Azure Active Directory**. Para más información sobre cómo modificar directivas de acceso condicional, consulte Acceso condicional en Azure Active Directory. Para obtener más información, vea ¿Qué son las directivas de protección de aplicaciones?

Configuración del dispositivo

Exigencia de instalación de perfiles de directivas, aplicaciones, certificados y red

Los administradores pueden evitar que los usuarios finales accedan al escritorio de Windows 10 RS4 hasta que Intune instale los perfiles de red y certificado, las aplicaciones y las directivas durante el aprovisionamiento de dispositivos AutoPilot. Para obtener más información, consulte Configurar una página de estado de inscripción.

Inscripción de dispositivos

Compatibilidad con Samsung Knox Mobile Enrollment

Al usar Intune con Samsung Knox Mobile Enrollment (KME), puede inscribir un gran número de dispositivos Android propiedad de la empresa. Los usuarios en redes Wi-Fi o de telefonía móvil se pueden inscribir con unas pocas pulsaciones al encender sus dispositivos por primera vez. Con la aplicación de implementación Knox, los dispositivos se pueden inscribir mediante Bluetooth o NFC. Para más información, vea Automatically enroll Android devices by using Samsung's Knox Mobile Enrollment (Inscripción automática de dispositivos Android mediante Samsung Knox Mobile Enrollment).

Supervisión y solución de problemas

Solicitud de ayuda en el Portal de empresa para Windows 10

El Portal de empresa para Windows 10 ahora enviará registros de aplicaciones directamente a Microsoft cuando el usuario inicie el flujo de trabajo para obtener ayuda con un problema. Esto permitirá que sea más fácil solucionar los problemas que se envían a Microsoft.

Abril de 2018

Administración de aplicaciones

Compatibilidad de código de acceso con el PIN de MAM en Android

Los administradores de Intune pueden establecer un requisito de inicio de aplicación para exigir un código de acceso en lugar de un PIN numérico de MAM. Si se configura, se le pide al usuario que establezca y use un código de acceso cuando se le solicite antes de obtener acceso a aplicaciones habilitadas para MAM. Un código de acceso se define como un PIN numérico con al menos un carácter especial o un carácter alfabético en mayúsculas/minúsculas. Intune admite un código de acceso de forma similar al PIN numérico existente... puede establecer una longitud mínima y permite la repetición de caracteres y secuencias en la consola de administración. Esta característica requiere la versión más reciente del Portal de empresa en Android. Esta característica ya está disponible para iOS.

Compatibilidad con aplicaciones de línea de negocio (LOB) para macOS

Microsoft Intune proporciona la capacidad de instalar aplicaciones LOB de macOS desde Azure Portal. Se puede agregar una aplicación LOB de macOS a Intune una vez procesada por la herramienta disponible en GitHub. En Azure Portal, seleccione **Aplicaciones cliente** en la hoja **Intune**. En la hoja **Aplicaciones cliente**, elija **Aplicaciones** > **Agregar**. En la hoja **Agregar aplicación**, seleccione **Aplicación de línea de negocio**.

Grupo integrado Todos los usuarios y Todos los dispositivos para la asignación de aplicaciones de perfil de trabajo de Android Enterprise

Puede aprovechar los grupos integrados **Todos los usuarios** y **Todos los dispositivos** para la asignación de aplicaciones de perfil de trabajo de Android Enterprise. Para obtener más información, vea Inclusión y exclusión de asignaciones de aplicaciones en Microsoft Intune.

Intune volverá a instalar las aplicaciones requeridas desinstaladas por los usuarios

Si un usuario final desinstala una aplicación requerida, Intune la reinstala de forma automática antes de que transcurran 24 horas en lugar de esperar al ciclo de reevaluación de siete días.

Actualización de la ubicación donde se configuran las directivas de protección de aplicaciones

En el servicio Microsoft Intune en Azure Portal, vamos a redirigirle temporalmente de la hoja del servicio **Intune App Protection** a la hoja **Aplicación móvil**. Tenga en cuenta que todas las directivas de protección de aplicaciones ya se encuentran en la hoja **Aplicación móvil** de Intune, en Configuración de aplicaciones. En lugar de ir a Intune App Protection, simplemente irá a Intune. En abril de 2018, se suspenderá el redireccionamiento y se quitará por completo la hoja del servicio **Intune App Protection**, para que haya una sola ubicación para las directivas de protección de aplicaciones en Intune.

¿Cómo me afecta esto a mí? Este cambio afectará tanto a los clientes de Intune independientes como a los clientes híbridos (Intune con Configuration Manager). Esta integración le ayudará a simplificar la administración en la nube.

¿Qué he de hacer para prepararme para este cambio? Etiquete **Intune** como favorito en lugar de la hoja del servicio **Intune App Protection** y asegúrese de que conoce el flujo de trabajo de la directiva de protección de aplicaciones de la hoja de la aplicación **Móvil** en Intune. Se le redirigirá durante un breve período de tiempo y, luego, se quitará la hoja **Intune App Protection**. Recuerde que todas las directivas de protección de aplicaciones ya están en Intune y que puede modificar las directivas de acceso condicional. Para más información sobre cómo modificar directivas de acceso condicional, consulte Acceso condicional en Azure Active Directory. Para obtener más información, vea ¿Qué son las directivas de protección de aplicaciones?

Configuración del dispositivo

Representación de todos los dispositivos de un grupo en el gráfico de perfiles de dispositivos y la lista de estado

Al configurar un perfil de dispositivo (**Configuración del dispositivo** > **Perfiles**), elija el perfil del dispositivo, por ejemplo, iOS. Este perfil se asigna a un grupo que incluye los dispositivos iOS y los dispositivos que no son iOS. El recuento del gráfico muestra que el perfil se aplica a dispositivos iOS *y* no iOS (**Configuración del dispositivo** > **Perfiles** > seleccionar un perfil existente > **Información general**). Cuando se selecciona el

gráfico en la pestaña **Información general**, el **Estado del dispositivo** enumera todos los dispositivos del grupo, en lugar de solo los dispositivos iOS.

Con esta actualización, el gráfico (**Configuración del dispositivo** > **Perfiles** > seleccionar un perfil existente > **Información general**) solo muestra el recuento del perfil de dispositivo determinado. Por ejemplo, si el perfil de dispositivo de configuración se aplica a dispositivos iOS, el gráfico muestra solo el número de dispositivos iOS. Al seleccionar el gráfico y abrir **Estado del dispositivo**, solo se muestran los dispositivos iOS.

Mientras se realiza esta actualización, se quita temporalmente el gráfico de usuario.

VPN de Always On para Windows 10

Actualmente, Always On puede usarse en dispositivos Windows 10 mediante un perfil de red privada virtual (VPN) personalizado creado con OMA-URI.

Con esta actualización, los administradores pueden habilitar Always On para perfiles de VPN de Windows 10 directamente en Intune en Azure Portal. Los perfiles VPN de Always On se conectarán automáticamente cuando:

- Los usuarios inicien sesión en sus dispositivos
- La red del dispositivo cambie
- La pantalla del dispositivo se vuelva a activar después de haberse desactivado

Nueva configuración de impresora para perfiles de educación

Para los perfiles de educación, hay nuevos valores de configuración disponibles en la categoría **Impresoras**: **Impresoras**, **Impresora predeterminada**, **Agregar nuevas impresoras**.

Mostrar el identificador de llamada en el perfil personal: perfil de trabajo de Android Enterprise

Al usar un perfil personal en un dispositivo, es posible que los usuarios finales no vean los detalles del identificador del autor de la llamada de un contacto de trabajo.

Con esta actualización, hay una nueva opción en **Android Enterprise** > **Restricciones de dispositivos** > **Configuración del perfil de trabajo**:

- Mostrar el identificador de llamada de contacto profesional en el perfil personal

Cuando se habilita (sin configurar), se muestran los detalles del autor de la llamada del contacto en el perfil personal. Cuando se bloquea, no se muestra el número del autor de la llamada del contacto en el perfil personal.

Se aplica a: Dispositivos de perfil de trabajo Android con la versión del sistema operativo Android 6.0 y versiones más recientes

Nueva configuración de Credential Guard de Windows Defender agregada a la configuración de Endpoint Protection

Con esta actualización, Credential Guard de Windows Defender (**Configuración de dispositivos** > **Perfiles** > **Endpoint Protection**) incluye la siguiente configuración:

- **Credential Guard de Windows Defender**: activa Credential Guard con seguridad basada en virtualización. Habilitar esta característica ayuda a proteger las credenciales en el siguiente reinicio cuando las opciones **///Platform Security Level with Secure Boot** (Nivel de seguridad de plataforma con arranque seguro) y **///Virtualization Based Security** (Seguridad basada en virtualización) are están ambas habilitadas. Las opciones son:
  - **Deshabilitado**: si Credential Guard se activó anteriormente con la opción **Habilitar sin bloqueo**", entonces Credential Guard se desactiva de forma remota.
  - **Habilitado con el bloqueo UEFI**: garantiza que Credential Guard no se puede deshabilitar mediante una clave de Registro o por medio de la directiva de grupo. Para deshabilitar Credential Guard después de usar esta opción, debe establecer la directiva de grupo en "Deshabilitado". A continuación, quite la funcionalidad de seguridad de cada equipo, con un usuario físicamente presente. Estos pasos borrar la configuración almacenada en UEFI. Mientras se conserve la configuración de UEFI, Credential Guard estará habilitado.

- **Habilitar sin bloqueo**: permite deshabilitar Credential Guard de forma remota mediante la directiva de grupo. Los dispositivos que usen esta configuración deben ejecutar al menos Windows 10 (versión 1511).

Las siguientes tecnologías dependientes se habilitan automáticamente al configurar Credential Guard:

- **Enable Virtualization-based Security (VBS)** (Habilitar la seguridad basada en la virtualización [VBS]): activa la seguridad basada en la virtualización (VBS) en el siguiente reinicio. La seguridad basada en la virtualización emplea el hipervisor de Windows para proporcionar compatibilidad con servicios de seguridad, y requiere arranque seguro.
- **Secure Boot with Direct Memory Access (DMA)** (Arranque seguro con acceso directo a memoria [DMA]): activa VBS con arranque seguro y acceso directo a memoria. La protección de DMA requiere compatibilidad con el hardware y solo se habilita en los dispositivos configurados correctamente.

Uso de un nombre de firmante personalizado en certificados SCEP

Puede usar el nombre común **OnPremisesSamAccountName** de un sujeto personalizado en un perfil de certificado SCEP. Por ejemplo, puede usar `CN={OnPremisesSamAccountName})`.

Bloqueo de la cámara y capturas de pantalla en los perfiles de trabajo de Android Enterprise

Hay dos nuevas propiedades disponibles para bloquear al configurar restricciones de dispositivo para dispositivos Android:

- Cámara: bloquea el acceso a todas las cámaras en el dispositivo.
- Captura de pantalla: bloquea la captura de pantalla y además evita que el contenido se muestre en los dispositivos de pantalla que no tengan una salida de vídeo segura.

Se aplica a los perfiles de trabajo de Android Enterprise.

Uso del cliente de Cisco AnyConnect para iOS

Al crear un nuevo perfil de VPN para iOS, ahora hay dos opciones: **Cisco AnyConnect** y **Cisco Legacy AnyConnect**. Los perfiles de Cisco AnyConnect admiten las versiones 4.0.7x y más recientes. Los perfiles de VPN existentes de Cisco AnyConnect para iOS se etiquetan como **Cisco Legacy AnyConnect**, y siguen funcionando con Cisco AnyConnect 4.0.5x y versiones posteriores, como lo hacen en la actualidad.

> **NOTE**
> Este cambio sólo se aplica a iOS. Sigue habiendo una única opción de Cisco AnyConnect para perfiles de trabajo de Android y Android Enterprise y las plataformas macOS.

Inscripción de dispositivos

Nuevos pasos de inscripción para los usuarios en dispositivos con macOS High Sierra 10.13.2+

macOS high Sierra 10.13.2 presentó el concepto de inscripción de inscripción de MDM "aprobada por el usuario". Las inscripciones aprobadas permiten a Intune administrar algunas configuraciones dependientes de la seguridad. Para obtener más información, vea la documentación de soporte técnico de Apple aquí: https://support.apple.com/HT208019.

Los dispositivos inscritos mediante el Portal de empresa de macOS se consideran "No aprobados por el usuario", a menos que el usuario final abra las preferencias del sistema y los apruebe de forma manual. Así, el Portal de empresa de macOS ahora insta a los usuarios de macOS 10.13.2 y versiones posteriores a aprobar manualmente su inscripción al final del proceso de inscripción. La consola de administración de Intune indicará si un dispositivo inscrito está aprobado por el usuario.

Ahora los dispositivos macOS inscritos en Jamf se pueden registrar en Intune

Las versiones 1.3 y 1.4 del portal de empresa de macOS no registraban correctamente los dispositivos Jamf en Intune. La versión 1.4.2 del portal de macOS corrige este problema.

Experiencia de ayuda actualizada en la aplicación Portal de empresa para Android

Se ha actualizado la experiencia de ayuda en la aplicación Portal de empresa para Android de acuerdo con los procedimientos recomendados para la plataforma Android. Ahora, cuando los usuarios detectan un problema en la aplicación, pueden pulsar en **Menú** > **Ayuda** y:

- Cargar registros de diagnóstico en Microsoft.
- Enviar un mensaje de correo electrónico que describe el problema y un Id. de incidente a un miembro del equipo de soporte técnico de la empresa.

Para ver la experiencia de ayuda actualizada, vaya a Send logs using email (Enviar registros por correo electrónico) y Send errors to Microsoft (Enviar errores a Microsoft).

Nuevo gráfico de tendencias sobre errores de inscripción y tabla de motivos de error

En la página de información general de inscripción, puede ver la tendencia de los errores de inscripción y los cinco motivos de error principales. Al hacer clic en el gráfico o la tabla, puede explorar los detalles para obtener consejos de resolución de problemas y sugerencias de corrección.

Administración de dispositivos

Intune y Defender for Endpoint están totalmente integrados

Defender for Endpoint muestra el nivel de riesgo de los dispositivos Windows 10. En el Centro de seguridad de Windows Defender, puede crear una conexión a Microsoft Intune. Una vez creada, se usa una directiva de cumplimiento de Intune para determinar un nivel de amenaza aceptable. Si se supera el nivel de amenaza, una directiva de acceso condicional de Azure Active Directory (AD) puede bloquear el acceso a diferentes aplicaciones dentro de su organización.

Esta característica permite que Defender for Endpoint examine archivos, detecte amenazas y notifique cualquier riesgo en los dispositivos Windows 10.

Consulte Habilitación de Defender for Endpoint con acceso condicional en Intune.

Compatibilidad con dispositivos sin usuario

Intune ofrece la posibilidad de evaluar el cumplimiento en dispositivos sin usuario, como Microsoft Surface Hub. La directiva de cumplimiento puede tener como destino dispositivos concretos. Así, es posible determinar el cumplimiento (y no cumplimiento) de dispositivos sin un usuario asociado.

Eliminación de dispositivos Autopilot

Los administradores de Intune pueden eliminar dispositivos Autopilot.

Experiencia de eliminación de dispositivos mejorada

Ya no se le pide que quite los datos de la empresa o que restablezca el dispositivo a los valores de fábrica para eliminar un dispositivo de Intune.

Para ver la nueva experiencia, inicie sesión en Intune y seleccione **Dispositivos** > **Todos los dispositivos** > el nombre del dispositivo > **Eliminar**.

Si todavía quiere confirmar el borrado o eliminación, puede usar la ruta de ciclo de vida de dispositivo estándar al usar **Eliminar datos de la compañía** y **Restablecimiento de fábrica** antes de **Eliminar**.

Reproducción de sonidos en iOS en modo Perdido

Cuando los dispositivos iOS supervisados están en el modo perdido de administración de dispositivos móviles (MDM), puede reproducir un sonido (**Dispositivos** > **Todos los dispositivos** > seleccionar un dispositivo iOS > **Información general** > **Más**). El sonido sigue reproduciéndose hasta que el dispositivo se quita del modo Perdido o un usuario deshabilita el sonido en el dispositivo. Se aplica a dispositivos iOS 9.3 y versiones más recientes.

Bloquear o permitir resultados web en búsquedas realizadas en un dispositivo de Intune

Ahora, los administradores pueden bloquear los resultados web en las búsquedas realizadas en un dispositivo.

Mensajes de error mejorados para errores de carga del certificado push MDM de Apple

El mensaje de error explica que se debe usar el mismo identificador de Apple al renovar un certificado MDM existente.

Probar el Portal de empresa para macOS en máquinas virtuales

Se han publicado instrucciones para ayudar a los administradores de TI a probar la aplicación Portal de empresa para macOS en máquinas virtuales en Parallels Desktop y VMware Fusion. Encuentre más información en Inscribir máquinas virtuales macOS para realizar pruebas.

Aplicaciones de Intune

Actualización de la experiencia de usuario para la aplicación Portal de empresa para iOS

Hemos publicado una importante actualización de la experiencia de usuario para la aplicación Portal de empresa para iOS. La actualización incluye un completo cambio de diseño visual con una apariencia modernizada. Hemos mantenido la funcionalidad de la aplicación, pero hemos mejorado su facilidad de uso y accesibilidad.

También verá:

- Compatibilidad con el iPhone X.
- Inicio de la aplicación y carga de las respuestas más rápidos, para ahorrar tiempo a los usuarios.
- Barras de progreso adicionales para proporcionar a los usuarios la información de estado más reciente.
- Mejoras en la forma en que los usuarios cargan los registros, de modo que, si hay algún problema, sea más fácil de informar al respecto.

Para ver el aspecto actualizado vaya a Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune.

Protección de los datos locales de Exchange mediante APP y CA de Intune

Ahora puede usar directivas de protección de aplicaciones (APP) y acceso condicional (CA) de Intune para proteger el acceso a datos locales de Exchange con Outlook Mobile. Para agregar o modificar una directiva de protección de aplicaciones en Azure Portal, seleccione **Microsoft Intune** > **Aplicaciones cliente** > **Directivas de protección de aplicaciones**. Antes de usar esta característica, asegúrese de cumplir los requisitos de Outlook para iOS y Android.

Interfaz de usuario

Iconos de dispositivo mejorados en el Portal de empresa de Windows 10

Se han actualizado los iconos para que sean más accesibles para los usuarios con deficiencia visual y para que funcionen mejor con las herramientas de lectura de pantalla.

Enviar informes de diagnóstico en la aplicación Portal de empresa para macOS

La aplicación Portal de empresa para dispositivos macOS se ha actualizado para mejorar la forma en que los usuarios notifican errores relacionados con Intune. Desde la aplicación Portal de empresa, los empleados pueden:

- Cargar informes de diagnóstico directamente para el equipo de desarrollo de Microsoft.
- Enviar por correo electrónico un identificador de incidente al equipo de soporte técnico de TI de la empresa.

Para más información, consulte Envío de errores de macOS.

Intune se adapta a Fluent Design System en la aplicación de Portal de empresa para Windows 10

La aplicación Portal de empresa de Intune para Windows 10 se ha actualizado con la vista de navegación de Fluent Design System. En la parte lateral de la aplicación, verá una lista estática vertical de todas las páginas de nivel superior. Haga clic en cualquier vínculo para ver y cambiar entre páginas rápidamente. Esta es la primera de varias actualizaciones que verá como parte de nuestros esfuerzos para crear una experiencia más adaptable, empática y familiar en Intune. Para ver el aspecto actualizado vaya a Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune.

Marzo de 2018

Administración de aplicaciones

Alertas para aplicaciones de línea de negocio (LOB) iOS a punto de expirar para Microsoft Intune

En Azure Portal, Intune le avisa de las aplicaciones de línea de negocio iOS que están a punto de expirar. Al cargar una nueva versión de la aplicación de línea de negocio iOS, Intune quita la notificación de expiración de la lista de aplicaciones. Esta notificación de expiración solo está activa para las aplicaciones de línea de negocio iOS recién cargadas. 30 días antes de que expire el perfil de aprovisionamiento de la aplicación LOB iOS, aparece una advertencia. Cuando expira, la alerta cambia a Expirada.

Personalización de los temas del Portal de empresa con códigos hexadecimales

Puede personalizar el color del tema de las aplicaciones del Portal de empresa mediante códigos hexadecimales. Cuando escribe el código hexadecimal, Intune determina el color del texto que proporciona el nivel más alto de contraste entre el color del texto y el color del fondo. Puede obtener una vista previa del color de texto y el logotipo de la empresa con el color en **Aplicaciones cliente** > **Portal de empresa**.

Inclusión o exclusión de la asignación de aplicaciones con base en grupos para Android Enterprise

Android Enterprise (anteriormente conocido como Android for Work) admite la inclusión y exclusión de grupos, pero no los grupos integrados creados previamente **Todos los usuarios** y **Todos los dispositivos**. Para obtener más información, vea Inclusión y exclusión de asignaciones de aplicaciones en Microsoft Intune.

Administración de dispositivos

Exportación de todos los dispositivos a archivos CSV en IE, Microsoft Edge o Chrome

En **Dispositivos** > **Todos los dispositivos**, puede **Exportar** los dispositivos a una lista con formato CSV. Los usuarios de Internet Explorer (IE) con >10.000 dispositivos pueden exportar correctamente sus dispositivos a varios archivos. Cada archivo tiene un máximo de 10.000 dispositivos.

Los usuarios de Microsoft Edge y Chrome con más de 30 000 dispositivos pueden exportar correctamente sus dispositivos a varios archivos. Cada archivo tiene un máximo de 30.000 dispositivos.

Administrar dispositivos proporciona más detalles sobre lo que puede hacer con los dispositivos que administra.

Nuevas mejoras de seguridad en el servicio de Intune

Se ha incorporado un botón de alternancia en Intune en Azure que los clientes independientes de Intune pueden usar para tratar dispositivos sin ninguna directiva asignada como **Compatible** (característica de seguridad desactivada) o como **No compatible** (característica de seguridad activada). Esto garantiza el acceso a los recursos únicamente después de que se haya evaluado el cumplimiento del dispositivo.

Esta característica afecta al usuario de forma distinta según tenga ya directivas de cumplimiento asignadas o no.

- Si es una cuenta nueva o existente y no tiene ninguna directiva de cumplimiento asignada a los dispositivos, el botón de alternancia se establece automáticamente en **Compatible**. La característica está desactivada como opción predeterminada en la consola. Los usuarios finales no se ven afectados.
- Si es una cuenta existente y tiene algún dispositivo con una directiva de cumplimiento asignada, el botón de alternancia se establece automáticamente en **No compatible**. La característica está activada como opción predeterminada en cuanto se lanza la actualización de marzo.

Si usa directivas de cumplimiento con acceso condicional (CA) y tiene la característica activada, los dispositivos que no tengan asignada como mínimo una directiva de cumplimiento son bloqueados por CA. Los usuarios finales asociados a estos dispositivos y a los que se haya concedido acceso previamente al correo electrónico pierden el acceso a menos que se asigne como mínimo una directiva de cumplimiento a todos los dispositivos.

Tenga en cuenta que aunque el estado predeterminado del botón de alternancia se muestra en la interfaz de usuario inmediatamente con las actualizaciones de marzo del servicio de Intune, este estado del botón de alternancia no se aplica de inmediato. Los cambios que realice en el botón de alternancia no afectan al

cumplimiento del dispositivo hasta la distribución de paquetes piloto a la cuenta para que tenga un botón de alternancia que funcione. Se le informa mediante el centro de mensajes una vez que se terminan de distribuir paquetes piloto a la cuenta. Esto podría tardar unos días después de la actualización del servicio de Intune de marzo.

Información adicional: https://aka.ms/compliance_policies

Detección de jailbreak mejorada

La detección de jailbreak mejorada es una nueva opción de cumplimiento que mejora la forma en que Intune evalúa los dispositivos con Jailbreak. La opción hace que el dispositivo se comunique con Intune con más frecuencia, lo que usa los servicios de ubicación del dispositivo y afecta al uso de la batería.

Restablecimiento de contraseñas para dispositivos Android O

Puede restablecer las contraseñas de los dispositivos Android 8.0 inscritos con perfiles de Work. Cuando se envía una solicitud de "Restablecer contraseña" a un dispositivo Android 8.0, se establece una nueva contraseña de desbloqueo de dispositivo o un desafío de perfil administrado al usuario actual. La contraseña o el desafío se envían y se aplican de inmediato.

Destinación de las directivas de cumplimiento a dispositivos en grupos de dispositivos

Puede destinar directivas de cumplimiento a usuarios de grupos de usuarios. Con esta actualización, puede destinar directivas de cumplimiento a dispositivos de grupos de dispositivos. Los dispositivos de destino como parte de grupos de dispositivos no reciben ninguna acción de cumplimiento.

Nueva columna Nombre de administración

Hay una nueva columna denominada **Nombre de administración** disponible en la hoja de dispositivos. Se trata de un nombre generado automáticamente y que no se puede modificar asignado por cada dispositivo, en función de la fórmula siguiente:

- Nombre predeterminado para todos los dispositivos:
- Para dispositivos agregados en masa: <IdentificadorPaquete/IdentificadorPerfil>

Se trata de una columna opcional en la hoja de dispositivos. No está disponible de forma predeterminada y solo se puede acceder a ella mediante el selector de columnas. El nombre del dispositivo no se ve afectado por esta nueva columna.

Los dispositivos iOS solicitan un PIN cada 15 minutos

Después de aplicar una directiva de configuración o cumplimiento a un dispositivo iOS, cada 15 minutos se pide al usuario que establezca un PIN, y se le sigue pidiendo hasta que lo hace.

Programación de las actualizaciones automáticas

Intune le permite controlar la instalación de las actualizaciones automáticas por medio de la opción Anillo de actualización de Windows. Con esta actualización, puede programar actualizaciones recurrentes, incluidos la semana, el día y la hora.

Uso de un nombre completo como sujeto de un certificado SCEP

Cuando se crea un perfil de certificado SCEP, hay que indicar el nombre del sujeto. Con esta actualización, puede usar el nombre completo como sujeto. En **Nombre del sujeto**, seleccione **Personalizado** y, después, escriba `CN={{OnPrem_Distinguished_Name}}`. Para usar la variable `{{OnPrem_Distinguished_Name}}`, no olvide sincronizar el atributo de usuario `onpremisesdistingishedname` por medio de Azure Active Directory (AD) Connect con Azure AD.

Configuración del dispositivo

Habilitación del uso compartido de contactos a través de Bluetooth: Android for Work

Android impide de forma predeterminada que los contactos del perfil del trabajo se sincronicen con dispositivos Bluetooth. Como consecuencia, los contactos del perfil de trabajo no aparecen en la identificación de llamadas en los dispositivos Bluetooth.

Con esta actualización, hay una nueva opción en **Android for Work** > **Restricciones de dispositivos** >

Configuración del perfil de trabajo:

- Uso compartido de contactos a través de Bluetooth

El administrador de Intune puede configurar esta opción para permitir el uso compartido de contactos. Esto resulta útil para emparejar un dispositivo con el dispositivo Bluetooth de un coche que muestra el identificador de llamada cuando se usa el manos libres. Si se habilita, se mostrarán los contactos del perfil de trabajo. Si no, no se mostrarán.

Configuración del equipo selector para controlar el origen de descarga de las aplicaciones macOS

Puede configurar el equipo selector para proteger los dispositivos desde las aplicaciones mediante el control del origen de descarga de las aplicaciones. Puede configurar los orígenes de descarga siguientes: **Mac App Store**, **Mac App Store y desarrolladores identificados** o **Cualquier sitio**. Puede configurar si los usuarios pueden instalar una aplicación al presionar Control+clic para invalidar estos controles del equipo selector.

Esta configuración se puede encontrar en **Configuración del dispositivo** -> **Crear perfil** -> **macOS** -> **Endpoint Protection**.

Configuración del firewall de aplicaciones Mac

Puede configurar el firewall de aplicaciones Mac. Puede usarlo para controlar las conexiones en cada aplicación, en lugar de en cada puerto. Esto facilita la capacidad de aprovechar las ventajas de protección de firewall y ayuda a evitar que aplicaciones no deseadas tomen el control de los puertos de red abiertos para las aplicaciones legítimas.

Esta característica se puede encontrar en **Configuración del dispositivo** -> **Crear perfil** -> **macOS** -> **Endpoint Protection**.

Una vez que habilite la opción Firewall, puede configurar el firewall con dos estrategias:

- Bloqueo de todas las conexiones entrantes

  Puede bloquear todas las conexiones entrantes para los dispositivos de destino. Si decide hacerlo, las conexiones entrantes se bloquean para todas las aplicaciones.

- Permiso o bloqueo de aplicaciones específicas

  Puede permitir o bloquear la recepción de conexiones entrantes en aplicaciones específicas. También puede habilitar el modo sigiloso para impedir respuestas a las solicitudes de sondeo.

Códigos de error y mensajes detallados

En la configuración del dispositivo, se pueden ver mensajes y códigos de error más detallados. Este informe detallado muestra la configuración, el estado de esta configuración y los detalles sobre cómo solucionar problemas.

Más información

- Bloqueo de todas las conexiones entrantes

  Esto impide que todos los servicios de uso compartido (como Uso compartido de archivos y Pantalla compartida) reciban conexiones entrantes. Los servicios del sistema a los que se sigue permitiendo recibir conexiones entrantes son los siguientes:

  - configd: implementa DHCP y otros servicios de configuración de red
  - mDNSResponder: implementa Bonjour
  - racoon: implementa IPSec

    Para usar los servicios de uso compartido, asegúrese de que **Conexiones entrantes** esté establecido en **Sin configurar**, y no en **Bloquear**.

- Modo sigiloso

Habilite esta opción para impedir que el equipo responda a las solicitudes de sondeo. El equipo seguirá respondiendo a las solicitudes entrantes de las aplicaciones autorizadas. Las solicitudes inesperadas, como ICMP (ping), se ignoran.

Deshabilitación de las comprobaciones al reiniciar el dispositivo

Intune le permite controlar la administración de las actualizaciones de software. Con esta actualización, la propiedad **Comprobaciones de reinicio** está disponible y habilitada de forma predeterminada. Para omitir las comprobaciones típicas que tienen lugar cuando un dispositivo se reinicia (por ejemplo, usuarios activos, niveles de batería, etc.), seleccione **Omitir**.

Nuevos canales de Windows 10 Insider Preview disponibles para anillos de implementación

Ahora tiene la opción de seleccionar los siguientes canales de servicio de Windows 10 Insider Preview al crear un anillo de implementación de Windows 10:

- Compilación de Windows Insider: Rápida
- Compilación de Windows Insider: Lenta
- Versión de lanzamiento de Windows Insider

Para obtener más información sobre estos canales, vea Manage Insider Preview Builds (Administrar compilaciones de Insider Preview). Para obtener más información sobre cómo crear canales de implementación en Intune, vea Manage software updates in Intune (Administrar actualizaciones de software en Intune).

Nueva configuración de Protección contra vulnerabilidades de seguridad de Windows Defender

Seis nuevas opciones de **reducción de la superficie expuesta a ataques** y funcionalidades ampliadas de **Acceso controlado a carpetas: protección de carpetas** están ahora disponibles. Estas opciones se pueden encontrar en: Configuración del dispositivo\Perfiles
Crear perfil\Endpoint protection\Protección contra vulnerabilidades de seguridad de Windows Defender.

Reducción de la superficie expuesta a ataques

NOMBRE DE LA CONFIGURACIÓN	OPCIONES DE CONFIGURACIÓN	DESCRIPCIÓN
Protección de ransomware avanzada	Habilitado, Auditoría, No configurado	Usar protección ransomware intensa.
Marcar el robo de credenciales desde el subsistema de autoridad de seguridad local de Windows	Habilitado, Auditoría, No configurado	Marcar el robo de credenciales desde el subsistema de autoridad de seguridad local de Windows (lsass.exe).
Creación del proceso desde comandos PSExec y WMI	Bloquear, Auditoría, No configurado	Bloquear creaciones del proceso que se originan desde comandos PSExec y WMI.
Procesos que no son de confianza y sin firma que se ejecutan desde una unidad USB	Bloquear, Auditoría, No configurado	Bloquee la ejecución desde USB de procesos que no sean de confianza y estén sin firmar.
Archivos ejecutables que no cumplen unos criterios de uso habitual, edad o lista de confianza	Bloquear, Auditoría, No configurado	Bloquee la ejecución de archivos ejecutables a menos que cumplan una¡os criterios de prevalencia, antigüedad o lista de confianza.

Acceso controlado a carpetas

NOMBRE DE LA CONFIGURACIÓN	OPCIONES DE CONFIGURACIÓN	DESCRIPCIÓN

NOMBRE DE LA CONFIGURACIÓN	OPCIONES DE CONFIGURACIÓN	DESCRIPCIÓN
Protección de carpetas (ya implementado)	No configurado, Habilitar, Solo auditoría (ya implementado) **Nuevo** Impedir la modificación del disco, Auditar la modificación del disco	

Proteger los archivos y carpetas frente a cambios no autorizados de aplicaciones hostiles.

Habilitar: impida que las aplicaciones que no son de confianza modifiquen o eliminen archivos de carpetas protegidas y que escriban en los sectores de disco.

Solo impedir la modificación del disco:
Impedir que las aplicaciones que no son de confianza escriban en los sectores de disco. Las aplicaciones que no son de confianza todavía podrán modificar o eliminar archivos en las carpetas protegidas.

Aplicaciones de Intune

Los sitios web de Azure Active Directory pueden requerir la aplicación Intune Managed Browser y compatibilidad con el inicio de sesión único para Managed Browser (versión preliminar pública)

Con Azure Active Directory (Azure AD), ya puede restringir el acceso a sitios web en dispositivos móviles para la aplicación Intune Managed Browser. En Managed Browser, los datos del sitio web permanecen seguros y separados de los datos personales del usuario final. Además, Managed Browser admitirá la función de inicio de sesión único para sitios protegidos por Azure AD. Al iniciar sesión en Managed Browser o al usar Managed Browser en un dispositivo con otra aplicación administrada por Intune, Managed Browser puede acceder a sitios corporativos protegidos por Azure AD sin que el usuario tenga que escribir sus credenciales. Esta función se aplica a sitios como Outlook Web Access (OWA) y SharePoint Online, además de otros sitios corporativos, como los recursos de la intranet a los que se accede mediante Azure App Proxy. Para más información, consulte Controles de acceso en el acceso condicional de Azure Active Directory.

Actualizaciones visuales de la aplicación Portal de empresa para Android

Hemos actualizado la aplicación Portal de empresa para Android para seguir las directrices de Material Design de Android. Puede ver las imágenes de los iconos nuevos en el artículo Novedades de la interfaz de usuario de aplicaciones.

Mejora de la inscripción de Portal de empresa

Los usuarios que inscriben un dispositivo mediante el Portal de empresa en Windows 10, compilación 1709 y versiones posteriores, ahora pueden realizar el primer paso de la inscripción sin salir de la aplicación.

HoloLens y Surface Hub ahora aparecen en las listas de dispositivos

Se ha agregado compatibilidad para mostrar los dispositivos HoloLens y Surface Hub inscritos en Intune en la aplicación Portal de empresa para Android.

Categorías personalizadas para libros electrónicos comprados a través de un programa de compras por volumen (VPP)

Puede crear categorías personalizadas de libros electrónicos y, después, asignar libros electrónicos de VPP a esas categorías personalizadas. Después, los usuarios finales podrán ver las categorías de libros electrónicos recién creadas y los libros asignados a las categorías. Para obtener más información, vea Administración de aplicaciones y libros comprados por volumen con Microsoft Intune.

Cambios de compatibilidad con la opción Enviar comentarios de la aplicación Portal de empresa para Windows

A partir del 30 de abril de 2018 la opción Enviar comentarios de la aplicación Portal de empresa para Windows solo funcionará en dispositivos que ejecuten la Actualización de aniversario de Windows 10 (1607) y versiones posteriores. La opción Enviar comentarios ya no se admite cuando se usa la aplicación Portal de empresa para Windows con:

- Windows 10, versión 1507
- Windows 10, versión 1511
- Windows Phone 8.1

Si su dispositivo ejecuta Windows 10 RS1 o una versión posterior, descargue de la tienda la versión más reciente de la aplicación Portal de empresa para Windows. Si ejecuta una versión no compatible, siga enviando los comentarios a través de los canales siguientes:

- La aplicación Concentrador de comentarios en Windows 10
- Un correo electrónico a WinCPfeedback@microsoft.com

Nueva configuración de Protección de aplicaciones de Windows Defender

- **Habilitar la aceleración gráfica**: los administradores pueden habilitar un procesador de gráficos virtuales para Windows Defender Application Guard. Esta configuración permite que la CPU descargue el procesamiento de gráficos a la vGPU. Esto puede mejorar el rendimiento cuando se trabaja con sitios web con gran cantidad de datos gráficos o se ve un vídeo dentro del contenedor.
- **SaveFilestoHost**: los administradores pueden permitir que los archivos pasen de Microsoft Edge que se ejecuta en el contenedor al sistema de archivos host. Su activación permite que los usuarios descarguen archivos de Microsoft Edge en el contenedor al sistema de archivos de host.

Destino de directivas de protección de MAM en función del estado de administración

Puede destinar las directivas de MAM en función del estado de administración del dispositivo:

- **Dispositivos Android**: puede tener como destino dispositivos no administrados, dispositivos administrados con Intune y perfiles de Android Enterprise administrados con Intune (anteriormente Android for Work).
- **Dispositivos iOS**: puede tener como destino dispositivos no administrados (solo MAM) o dispositivos administrados con Intune.

> **NOTE**
> - La compatibilidad de iOS con esta funcionalidad se ha ido lanzando a lo largo de abril de 2018.

Para obtener más información, vea Target app protection policies based on device management state (Destinar directivas de protección de aplicaciones en función del estado de administración del dispositivo).

Mejoras en el lenguaje de la aplicación Portal de empresa para Windows

Se ha mejorado el lenguaje del Portal de empresa para Windows 10 para que sea más fácil de usar y más específico para la empresa. Para ver algunas imágenes de ejemplo de lo que se ha hecho, vea Novedades en la UI de la aplicación.

Nuevas adiciones a los documentos sobre privacidad del usuario

Como parte del esfuerzo por proporcionar a los usuarios finales más control sobre sus datos y su privacidad, se han publicado actualizaciones de los documentos que explican cómo ver y quitar datos almacenados localmente por las aplicaciones del Portal de empresa. Puede encontrar estas actualizaciones en:

- **Android**: Cómo quitar un dispositivo Android de Intune
- **Android, si el usuario ha rechazado los términos de uso**: Quitar un dispositivo de la administración si ha rechazado los "términos de uso"
- **iOS**: Quitar un dispositivo iOS de Intune
- **Windows**: Quitar el dispositivo Windows de Intune

Febrero de 2018

Inscripción de dispositivos

Compatibilidad de Intune con varias cuentas del programa del Programa de inscripción de dispositivos (DEP) de Apple o de Apple School Manager

Intune ahora admite la inscripción de dispositivos de hasta 100 cuentas distintas del Programa de inscripción de dispositivos de Apple o de Apple School Manager. Cada token cargado puede administrarse por separado para los perfiles y los dispositivos de inscripción. Es posible asignar un perfil de inscripción diferente para cada token de DEP/School Manager. Si se cargan varios tokens de School Manager, solo pueden compartirse de uno en uno con Microsoft School Data Sync.

Tras la migración, la versión beta de las API Graph y los scripts publicados para la administración de Apple DEP o ASM en Graph ya no funcionará. Las nuevas versiones beta de las API Graph están en desarrollo y se publicarán después de la migración.

Visualización de las restricciones de inscripción por usuario

En la hoja **Solución de problemas**, ahora puede ver las restricciones de inscripción que están en vigor para cada usuario si selecciona **Restricciones de inscripción** en la lista **Asignaciones**.

Nueva opción para la autenticación de usuario para la inscripción masiva de Apple

> **NOTE**
> Los nuevos inquilinos verán esta característica inmediatamente. En cambio, en el caso de los inquilinos existentes, se implementará en abril. Es posible que no tenga acceso a estas nuevas características hasta que la implementación se haya completado.

Intune ofrece ahora la opción de autenticar los dispositivos mediante la aplicación Portal de empresa para los siguientes métodos de inscripción:

- Programa de inscripción de dispositivos de Apple
- Apple School Manager
- Inscripción de Apple Configurator

Al usar la opción Portal de empresa, se puede aplicar la autenticación multifactor de Azure Active Directory sin bloquear estos métodos de inscripción.

Al usar la opción Portal de empresa, Intune omite la autenticación de usuario en el Asistente de configuración de iOS para la inscripción de afinidad del usuario. Esto significa que el dispositivo se inscribe inicialmente como un dispositivo sin usuario, por lo que no recibe las configuraciones ni las directivas de grupos de usuarios. Solo recibe las configuraciones y las directivas de grupos de dispositivos. Sin embargo, Intune instalará automáticamente la aplicación Portal de empresa en el dispositivo. El primer usuario que inicie la aplicación Portal de empresa e inicie sesión en ella se asociará con el dispositivo en Intune. En este momento, el usuario recibirá las configuraciones y las directivas de sus grupos de usuarios. No se puede cambiar la asociación del usuario sin volver a realizar la inscripción.

Compatibilidad de Intune con varias cuentas del programa del Programa de inscripción de dispositivos (DEP) de Apple o de Apple School Manager

Intune ahora admite la inscripción de dispositivos de hasta 100 cuentas distintas del Programa de inscripción de dispositivos de Apple o de Apple School Manager. Cada token cargado puede administrarse por separado para los perfiles y los dispositivos de inscripción. Es posible asignar un perfil de inscripción diferente para cada token de DEP/School Manager. Si se cargan varios tokens de School Manager, solo pueden compartirse de uno en uno con Microsoft School Data Sync.

Tras la migración, la versión beta de las API Graph y los scripts publicados para la administración de Apple DEP o ASM en Graph ya no funcionará. Las nuevas versiones beta de las API Graph están en desarrollo y se publicarán después de la migración.

Impresión remota a través de una red segura

Las soluciones de impresión móvil inalámbricas de PrinterOn permitirán a los usuarios imprimir remotamente desde cualquier lugar en cualquier momento a través de una red segura. PrinterOn se integrará con el SDK de aplicaciones de Intune para iOS y Android. Podrá destinar las directivas de protección de aplicaciones a esta aplicación a través de la hoja **Directivas de protección de aplicaciones** de Intune de la consola de administración. Los usuarios finales podrán descargar la aplicación "PrinterOn for Microsoft" a través de Play Store o iTunes para usarla dentro de su ecosistema de Intune.

Compatibilidad del Portal de empresa de macOS para las inscripciones que usen el administrador de inscripciones de dispositivos

Los usuarios ya pueden usar el administrador de inscripciones de dispositivos cuando se inscriban con Portal de empresa para macOS.

Administración de dispositivos

Informes de estado de mantenimiento y de estado de amenazas de Windows Defender

Conocer el estado de mantenimiento de Windows Defender es clave para la administración de equipos de Windows. Con esta actualización, Intune agrega nuevos informes y acciones para el estado y el mantenimiento del agente de Windows Defender. Con un informe de resumen de estado en la carga de trabajo Cumplimiento de dispositivos, puede ver los dispositivos que necesitan alguna de las acciones siguientes:

- actualización de la firma
- Reiniciar
- intervención manual
- examen completo
- otros estados del agente que requieren intervención

Un informe de obtención de detalles para cada categoría de estado muestra los equipos individuales que requieren atención o identificados como **limpios**.

Nueva configuración de privacidad para las restricciones de dispositivos

Hay dos nuevas opciones de privacidad disponibles para los dispositivos:

- **Publicar las actividades del usuario**: establezca esta opción en **Bloquear** para evitar experiencias compartidas y la detección de recursos usados recientemente en el selector de tareas.
- **Solo actividades locales**: establezca esta opción en **Bloquear** para evitar experiencias compartidas y la detección de recursos usados recientemente en el selector de tareas según la actividad local únicamente.

Nueva configuración para el explorador Microsoft Edge

Hay dos opciones nuevas disponibles para dispositivos con el explorador Microsoft Edge versión 45 y anteriores: **Ruta de acceso al archivo de favoritos** y **Cambios a Favoritos**.

Administración de aplicaciones

Excepciones de protocolo para las aplicaciones

Puede crear excepciones a la directiva de transferencia de datos de la administración de aplicaciones móviles (MAM) de Intune para abrir determinadas aplicaciones no administradas. Dichas aplicaciones deben ser de confianza para el departamento de TI. Aparte de las excepciones que cree, la transferencia de datos sigue estando limitada a las aplicaciones que se administran mediante Intune cuando la directiva de transferencia de datos se establece en **Managed apps only** (Solo aplicaciones administradas). Puede crear las restricciones mediante protocolos (iOS) o paquetes (Android).

Por ejemplo, puede agregar el paquete de WebEx como una excepción a la directiva de transferencia de datos de MAM. Esto permitirá que los vínculos de WebEx en un mensaje de correo electrónico de Outlook administrado se abran directamente en la aplicación de WebEx. Se seguirá restringiendo la transferencia de datos en otras aplicaciones no administradas. Para obtener más información, consulte Data transfer policy exceptions for apps (Excepciones de la directiva de transferencia de datos para aplicaciones).

Datos cifrados de Windows Information Protection (WIP) en los resultados de la búsqueda de Windows

Un parámetro de configuración de la directiva de Windows Information Protection (WIP) le permite controlar si los datos cifrados por WIP se incluyen en los resultados de la búsqueda de Windows. Para establecer esta opción de la directiva de protección de aplicaciones, seleccione **Permitir que el indizador de Windows Search busque elementos cifrados** en la **Configuración avanzada** de la directiva de Windows Information Protection. La directiva de protección de aplicaciones debe establecerse en la plataforma *Windows 10* y la directiva de aplicación **Estado de inscripción** debe establecerse en **Con inscripción**. Para obtener más información, consulte Permitir que el indizador de Windows Search busque elementos cifrados.

Configuración de una aplicación MSI móvil de auto-actualización

Puede configurar una aplicación móvil MSI con auto-actualización para que omita el proceso de comprobación de versión. Esta capacidad resulta útil para evitar que se produzca una condición de carrera. Por ejemplo, este tipo de condición de carrera podría producirse cuando la aplicación que el desarrollador de aplicaciones actualiza automáticamente también la estuviera actualizando Intune. Ambos podrían tratar de aplicar una versión de la aplicación en un cliente de Windows, lo que podría crear un conflicto. Para estas aplicaciones MSI que se actualizan automáticamente, puede configurar el valor **Omitir la versión de la aplicación** en la hoja **Información de la aplicación**. Cuando se cambia esta configuración a **Sí**, Microsoft Intune omite la versión de la aplicación instalada en el cliente de Windows.

Conjuntos de licencias de aplicaciones relacionadas admitidas en Intune

Intune en Azure Portal ya admite conjuntos de licencias de aplicaciones relacionadas como un elemento de aplicación único en la interfaz de usuario. Además, las aplicaciones con licencia sin conexión sincronizadas desde Microsoft Store para Empresas se consolidarán en una entrada de aplicación única y los detalles de implementación de los paquetes individuales se migrarán a la entrada única. Para ver los conjuntos de licencias de aplicaciones relacionadas en Azure Portal, seleccione **Licencias de aplicación** en la hoja **Aplicaciones cliente**.

Configuración del dispositivo

Extensiones de archivo de Windows Information Protection (WIP) para el cifrado automático

Un valor de la directiva de Windows Information Protection (WIP) le permite ahora especificar qué extensiones de archivo se cifran automáticamente al copiar desde un recurso compartido del bloque de mensajes del servidor (SMB) dentro de los límites corporativos, como se define en la directiva de WIP.

Configurar las opciones de la cuenta del recurso para Surface Hubs

Ya puede configurar de forma remota las opciones de la cuenta del recurso para Surface Hubs.

Una instancia de Surface Hub usa la cuenta del recurso para autenticarse en Skype o Exchange y así poder unirse a una reunión. Deberá crear una cuenta del recurso única para que Surface Hub pueda aparecer en la reunión como la sala de conferencias. Por ejemplo, una cuenta del recurso como **Sala de conferencias B41/6233**.

> **NOTE**
>
> - Si deja campos en blanco invalidará los atributos configurados previamente en el dispositivo.
> - Las propiedades de la cuenta del recurso pueden cambiar dinámicamente en Surface Hub. Por ejemplo, si el cambio de contraseñas está activado. Por lo tanto, es posible que los valores de la consola de Azure tarden algún tiempo en reflejar la realidad en el dispositivo.
>
>   Para entender lo que está configurado actualmente en Surface Hub, se puede incluir la información de la cuenta del recurso en el inventario de hardware (que ya tiene un intervalo de 7 días) o como propiedades de solo lectura. Para mejorar la precisión después de llevar a cabo la acción remota, puede obtener el estado de los parámetros inmediatamente después de ejecutar la acción para actualizar la cuenta o los parámetros en Surface Hub.

NOMBRE DE LA CONFIGURACIÓN	OPCIONES DE CONFIGURACIÓN	DESCRIPCIÓN
Ejecución de contenido ejecutable protegido por contraseña del correo electrónico	Bloquear, Auditoría, No configurado	Evitar que se ejecuten los archivos ejecutables protegidos por contraseña descargados a través del correo electrónico.
Protección de ransomware avanzada	Habilitado, Auditoría, No configurado	Usar protección ransomware intensa.
Marcar el robo de credenciales desde el subsistema de autoridad de seguridad local de Windows	Habilitado, Auditoría, No configurado	Marcar el robo de credenciales desde el subsistema de autoridad de seguridad local de Windows (lsass.exe).
Creación del proceso desde comandos PSExec y WMI	Bloquear, Auditoría, No configurado	Bloquear creaciones del proceso que se originan desde comandos PSExec y WMI.
Procesos que no son de confianza y sin firma que se ejecutan desde una unidad USB	Bloquear, Auditoría, No configurado	Bloquee la ejecución desde USB de procesos que no sean de confianza y estén sin firmar.
Archivos ejecutables que no cumplen unos criterios de uso habitual, edad o lista de confianza	Bloquear, Auditoría, No configurado	Bloquee la ejecución de archivos ejecutables a menos que cumplan una¡os criterios de prevalencia, antigüedad o lista de confianza.

Acceso controlado a carpetas

NOMBRE DE LA CONFIGURACIÓN	OPCIONES DE CONFIGURACIÓN	DESCRIPCIÓN
Protección de carpetas (ya implementado)	No configurado, Habilitar, Solo auditoría (ya implementado) **Nuevo** Impedir la modificación del disco, Auditar la modificación del disco	

Proteger los archivos y carpetas frente a cambios no autorizados de aplicaciones hostiles.

Habilitar: impida que las aplicaciones que no son de confianza modifiquen o eliminen archivos de carpetas protegidas y que escriban en los sectores de disco.

Solo impedir la modificación del disco:
Impedir que las aplicaciones que no son de confianza escriban en los sectores de disco. Las aplicaciones que no son de confianza todavía podrán modificar o eliminar archivos en las carpetas protegidas.

Adiciones a la configuración de seguridad del sistema para las directivas de cumplimiento de Windows 10 y posteriores

Ya hay disponibles adiciones a la configuración de cumplimiento de Windows 10, incluida la necesidad del Firewall y el Antivirus de Windows Defender.

Aplicaciones de Intune

Compatibilidad con aplicaciones sin conexión de Microsoft Store para Empresas

Las aplicaciones sin conexión que ha adquirido en Microsoft Store para Empresas ahora se sincronizan con Azure Portal. Puede implementar estas aplicaciones en grupos de usuarios o dispositivos. Las aplicaciones sin conexión se instalan mediante Intune, no Microsoft Store.

Impedir que los usuarios finales agreguen o quiten cuentas manualmente en el perfil de trabajo

Al implementar la aplicación Gmail en un perfil de Android for Work, puede impedir que los usuarios finales

agreguen o quiten cuentas en el perfil de trabajo mediante la opción de configuración **Agregar y quitar cuentas** del perfil de restricciones del dispositivo Android for Work.

Enero de 2018

Inscripción de dispositivos

Alertas de tokens caducados y tokens que caducan pronto

Ahora en la página de introducción se muestran las alertas de los tokens caducados y los tokens que caducan pronto. Al hacer clic en una alerta para un único token, se le dirigirá a la página de detalles del token. Si hace clic en la alerta con varios tokens, se le dirigirá a una lista de todos los tokens con su estado. Los administradores deben renovar sus tokens antes de la fecha de caducidad.

Administración de dispositivos

Compatibilidad con el comando "Borrar" de forma remota en dispositivos macOS

Los administradores pueden emitir un comando Borrar de forma remota en dispositivos macOS.

> **IMPORTANT**
> El comando de borrado no se puede deshacer y debe utilizarse con precaución.

El comando de borrado quita todos los datos, incluido el sistema operativo, de un dispositivo. También quita el dispositivo de la administración de Intune. No se genera ninguna advertencia al usuario y el borrado se produce inmediatamente al emitir el comando.

Debe configurar un PIN de recuperación de 6 dígitos. Este código PIN se puede usar para desbloquear el dispositivo borrado, momento en que comenzará la reinstalación del sistema operativo. Una vez iniciado el borrado, el PIN aparece en una barra de estado en la hoja de información general del dispositivo en Intune. El PIN permanecerá mientras el borrado esté en curso. Una vez completada la eliminación, el dispositivo desaparecerá por completo de la administración de Intune. Asegúrese de registrar el PIN de recuperación para que la persona que esté restaurando el dispositivo lo pueda usar.

Revocación de las licencias de un token del programa de compras por volumen de iOS

Puede revocar la licencia de todas las aplicaciones del programa de compras por volumen (VPP) de iOS para un token de VPP determinado.

Administración de aplicaciones

Revocación de las aplicaciones del programa de compras por volumen de iOS

En el caso de un dispositivo determinado con una o más aplicaciones del programa de compras por volumen (VPP) de iOS, puede revocar la licencia de aplicación basada en dispositivo asociada para el dispositivo. Revocar una licencia de aplicación no desinstalará la aplicación VPP desde el dispositivo. Para desinstalar una aplicación VPP, debe cambiar la acción de asignación a **Desinstalar**. Para más información, consulte Administrar aplicaciones de iOS compradas a través de un programa de compras por volumen con Microsoft Intune.

Asignación de aplicaciones móviles de Microsoft 365 a dispositivos iOS y Android mediante el tipo de aplicación integrada

El tipo de aplicación **integrada** facilita la creación y la asignación de aplicaciones de Microsoft 365 a los dispositivos iOS y Android administrados. Entre estas aplicaciones están las de Microsoft 365, como Word, Excel, PowerPoint y OneDrive. Puede asignar aplicaciones específicas al tipo de aplicación y, luego, editar la configuración de la información de la aplicación.

Inclusión o exclusión de la asignación de aplicaciones con base en grupos

Durante la asignación de aplicaciones y después de seleccionar un tipo de asignación, puede seleccionar los grupos para incluir, así como los grupos para excluir.

Configuración del dispositivo

Puede asignar una directiva de configuración de aplicación a grupos mediante asignaciones de inclusión o exclusión

Puede asignar una directiva de configuración de aplicación a un grupo de usuarios y dispositivos mediante una combinación de asignaciones de inclusión y exclusión. Las asignaciones se pueden elegir como una selección personalizada de grupos o como un grupo virtual. Un grupo virtual puede incluir **Todos los usuarios**, **Todos los dispositivos** o **Todos los usuarios + todos los dispositivos**.

Compatibilidad con una directiva de actualización de la edición de Windows 10

Puede crear una directiva de actualización de la edición de Windows 10 que actualice los dispositivos con Windows 10 a Windows 10 Education, Windows 10 Education N, Windows 10 Professional, Windows 10 Professional N, Windows 10 Professional Education y Windows 10 Professional Education N. Para obtener más información sobre las actualizaciones de la edición de Windows 10, vea Configuración de actualizaciones de la edición de Windows 10.

Directivas de acceso condicional de Intune solo disponibles en Azure Portal

A partir de esta versión, debe configurar y administrar las directivas de acceso condicional en Azure Portal desde **Azure Active Directory** > **Acceso condicional**. Para su comodidad, también puede acceder a esta hoja de Intune en Azure Portal en **Intune** > **Acceso condicional**.

Actualizaciones de los correos electrónicos sobre compatibilidad

Cuando se envía un correo electrónico para informar de un dispositivo no compatible, se incluyen detalles sobre dicho dispositivo.

Aplicaciones de Intune

Nueva funcionalidad para la acción "Resolver" en dispositivos Android

La aplicación Portal de empresa para Android expande la acción "Resolver" para la opción **Actualizar configuración del dispositivo** para resolver problemas con el cifrado del dispositivo.

Bloqueo remoto disponible en la aplicación de Portal de empresa para Windows 10

Los usuarios finales ya pueden bloquear de forma remota sus dispositivos desde la aplicación del Portal de empresa para Windows 10. No se mostrará para el dispositivo local que usen activamente.

Resolución más sencilla de los problemas de compatibilidad de la aplicación Portal de empresa para Windows 10

Los usuarios finales que tengan dispositivos Windows podrán seleccionar el motivo de no compatibilidad en la aplicación Portal de empresa. Cuando sea posible, esta acción les llevará directamente a la ubicación correcta en la aplicación de configuración para solucionar el problema.

2017

Diciembre de 2017

Nueva configuración de la reimplementación automática

La opción de configuración **Reimplementación automática** permite a los usuarios con derechos administrativos eliminar todos los datos de usuario y las opciones de configuración con **Ctrl + Win + R** en la pantalla de bloqueo del dispositivo. En este caso, el dispositivo se vuelve a configurar e inscribir automáticamente para la administración. Esta opción de configuración se puede encontrar en Windows 10 > Restricciones de dispositivos > General > Reimplementación automática. Para más detalles, consulte Configuración de restricciones de dispositivo de Intune para Windows 10.

Compatibilidad con las ediciones de origen adicionales en la directiva de actualización de edición de Windows 10

Ahora puede usar la directiva de actualización de edición de Windows 10 para actualizar desde ediciones de Windows 10 adicionales (Windows 10 Pro, Windows 10 Pro Education, Windows 10 Cloud, etc.). Antes de esta versión, las rutas de actualización de edición admitidas estaban más limitadas. Para obtener más información, consulte Configuración de actualizaciones de la edición de Windows 10.

Nueva configuración del perfil de configuración de dispositivo del Centro de seguridad de Windows Defender (WDSC)

Intune agrega una sección nueva de configuración del perfil de configuración de dispositivo en la protección del punto de conexión denominada **Centro de seguridad de Windows Defender**. Los administradores de TI pueden configurar a qué pilares de la aplicación Centro de seguridad de Windows Defender pueden acceder los

usuarios finales. Si un administrador de TI oculta un pilar en la aplicación Centro de seguridad de Windows Defender, las notificaciones relativas al pilar oculto no se mostrarán en el dispositivo del usuario.

Estos son los pilares que los administradores pueden ocultar de la configuración del perfil de configuración de dispositivo del Centro de seguridad de Windows Defender:

- Protección contra amenazas y virus
- Mantenimiento y estado del dispositivo
- Firewall y protecciones de red
- Control de aplicaciones y explorador
- Opciones de familia

Los administradores de TI también pueden personalizar las notificaciones que recibirán los usuarios. Por ejemplo, puede configurar si los usuarios reciben todas las notificaciones que generan los pilares visibles en WDSC o solo las notificaciones críticas. Las notificaciones no críticas incluyen resúmenes periódicos de la actividad de Antivirus de Windows Defender y las notificaciones cuando se completan las detecciones. Todas las otras notificaciones se consideran críticas. Además, también puede personalizar el contenido mismo de la notificación. Por ejemplo, puede proporcionar la información de contacto de TI para insertarla en las notificaciones que aparecen en los dispositivos de los usuarios.

Compatibilidad de varios conectores con el control de certificados SCEP y PFX

Los clientes que usan el conector NDES local para entregar los certificados a los dispositivos ahora pueden configurar varios conectores en un solo inquilino.

Esta funcionalidad nueva admite el siguiente escenario:

- Alta disponibilidad

Cada conector NDES extrae solicitudes de certificado desde Intune. Si un conector NDES queda sin conexión, el otro puede seguir procesando las solicitudes.

El nombre de sujeto de cliente puede usar la variable AAD_DEVICE_ID

Cuando se crea un perfil de certificado de SCEP en Intune, ahora puede usar la variable AAD_DEVICE_ID cuando se compila el nombre de sujeto personalizado. Si se solicita el certificado con este perfil SCEP, la variable se reemplaza por el identificador de dispositivo de Azure AD del dispositivo que realiza la solicitud de certificado.

Administración de dispositivos macOS inscritos en Jamf con el motor de conformidad de dispositivos de Intune

Ahora puede usar Jamf para enviar la información del estado del dispositivo macOS a Intune, y este a continuación evaluará su conformidad con las directivas definidas en la consola de Intune. En función del estado de conformidad del dispositivo, así como otras condiciones tales como la ubicación, el riesgo del usuario, etc., el acceso condicional aplicará la conformidad para los dispositivos macOS que accedan a la nube y a aplicaciones locales conectadas a Azure AD, incluido Microsoft 365. Consulte más información sobre la configuración de la integración de Jamf y la exigencia de compatibilidad para dispositivos administrados por Jamf.

Nueva acción de dispositivo iOS

Ahora puede apagar los dispositivos iOS 10.3 supervisados. Esta acción apaga inmediatamente el dispositivo sin enviar una advertencia al usuario final. La acción **Shut down (supervised only)** [Apagar (solo con supervisión)] se puede encontrar en las propiedades de dispositivos cuando se selecciona un dispositivo en la carga de trabajo del **dispositivo**.

No permitir cambios de fecha y hora en dispositivos Samsung Knox

Hemos agregado una nueva característica que permite bloquear los cambios de fecha y hora en los dispositivos Samsung Knox. Puede encontrarla en **Perfiles de configuración de dispositivo** > **Device restrictions (Android)** (Restricciones de dispositivos [Android]) > **General**.

Compatibilidad con la cuenta del recurso de Surface Hub

Se ha agregado una nueva acción de dispositivo para que los administradores puedan definir y actualizar la

cuenta del recurso asociada con Surface Hub.

Una instancia de Surface Hub usa la cuenta del recurso para autenticarse con Skype o Exchange y así poder unirse a una reunión. Puede crear una cuenta del recurso única para que Surface Hub aparezca en la reunión como la sala de conferencias. Por ejemplo, la cuenta del recurso puede aparecer como *Sala de conferencias B41/6233*. La cuenta del recurso (conocida como la cuenta del dispositivo) de Surface Hub habitualmente se debe configurar para la ubicación de la sala de conferencias y cuando sea necesario cambiar otros parámetros de la cuenta del recurso.

Cuando los administradores deseen actualizar la cuenta del recurso de un dispositivo, deben proporcionar las credenciales actuales de Active Directory o Azure Active Directory asociadas con el dispositivo. Si la rotación de contraseñas está activada en el dispositivo, los administradores deben ir a Azure Active Directory para encontrar la contraseña.

> **NOTE**
> Todos los campos se envían en un conjunto y sobrescriben todos los campos que ya estaban configurados. Los campos vacíos también sobrescriben los campos existentes.

Los administradores pueden configurar los valores siguientes:

- Cuenta del recurso
  - Usuario de Active Directory

    NombreDeUsuario\nombredeusuario o nombre principal de usuario (UPN): user@domainname.com
  - Contraseña
- Parámetros opcionales de la cuenta del recurso (se deben establecer con la cuenta del recurso especificada)
  - Período de rotación de contraseñas

    Garantiza que Surface Hub actualice automáticamente la contraseña de la cuenta cada semana por motivos de seguridad. Para configurar cualquier parámetro una vez que esto esté habilitado, la cuenta en Azure Active Directory debe tener primero el restablecimiento de contraseña.
  - Dirección de SIP (protocolo de inicio de sesión)

    Solo se usa cuando se produce un error en la detección automática.
  - Correo electrónico

    Dirección de correo electrónico de la cuenta del recurso o dispositivo.
  - Exchange Server

    Solo se necesita cuando se produce un error en la detección automática.
  - Sincronización de calendario

    Especifica si la sincronización de calendario y otros servicios de Exchange Server están habilitados. Por ejemplo: sincronización de reunión.

Instalación de aplicaciones de Office en dispositivos macOS

Ahora podrá instalar aplicaciones de Office en dispositivos macOS. Este nuevo tipo de aplicación le permitirá instalar Word, Excel, PowerPoint, Outlook y OneNote. Estas aplicaciones también incluyen Microsoft AutoUpdater (MAU) para ayudar a mantener aplicaciones seguras y actualizadas.

Eliminación de un token del programa de compras por volumen de iOS

Puede eliminar el token del programa de compras por volumen (VPP) de iOS con la consola. Esto puede resultar necesario cuando tiene instancias duplicadas de un token de VPP.

Limitación de la nueva colección de entidades Usuario actual a los datos de los usuarios activos actualmente

La colección de entidades **Usuarios** muestra todos los usuarios de Azure Active Directory (Azure AD) con licencias asignadas en la empresa. Por ejemplo, es posible que durante el último mes se haya agregado a un usuario a Intune y, luego, se haya eliminado. A pesar de que no esté presente a la hora de generar el informe, el usuario en cuestión y su estado sí que figuran en los datos. Una opción podría ser crear un informe que incluya el historial relativo a la duración de la presencia del usuario en sus datos.

Por otro lado, la nueva colección de entidades **Usuario actual** solo contiene los usuarios que no se hayan eliminado. En otras palabras, la colección de entidades **Usuario actual** solo contiene los usuarios que estén activos actualmente. Para obtener más información sobre la colección de entidades **Usuario actual**, consulte Referencia de la entidad de usuario actual.

Actualización de las API Graph

En esta versión, hemos actualizado algunas de las API Graph para Intune que están en versión beta. Consulte el registro de cambios de API Graph mensual para obtener más información.

Intune admite aplicaciones denegadas de Windows Information Protection (WIP)

En Intune puede especificar aplicaciones denegadas. Si una aplicación queda denegada, se la bloquea para que no pueda acceder a la información de la empresa, es decir, lo contrario a la lista de aplicaciones permitidas. Para obtener más información, consulte Recommended deny list for Windows Information Protection (Recomendación de lista de aplicaciones denegadas para Windows Information Protection).

Noviembre de 2017

Solución de problemas de inscripción

En el área de trabajo **Solución de problemas** ahora se muestran los problemas de inscripción del usuario. Los detalles del problema y los pasos de corrección sugeridos pueden ayudar a los administradores y a los operadores del departamento de soporte técnico a solucionar los problemas. Ciertos problemas de inscripción no se capturan, y es posible que no se sugieran correcciones para algunos errores.

Restricciones de inscripción asignada a grupos

Como administrador de Intune, ahora puede crear restricciones de inscripción personalizadas de tipo de dispositivo y de límite de dispositivos para grupos de usuarios.

Azure Portal de Intune permite crear un máximo de 25 instancias de cada tipo de restricción que pueden asignarse luego a grupos de usuarios. Las restricciones asignadas por grupo invalidan las restricciones predeterminadas.

Todas las instancias de un tipo de restricción se mantienen en una lista ordenada de forma estricta. Este orden define un valor de prioridad para la resolución de conflictos. Un usuario afectado por más de una instancia de la restricción solo está limitado por la instancia con el valor de prioridad más alto. Para cambiar la prioridad de una determinada instancia, arrástrela a una posición diferente en la lista.

Esta funcionalidad se publicará con la migración de la configuración de Android for Work desde el menú de inscripción de Android for Work al menú de restricciones de inscripción. Puesto que esta migración puede tardar varios días, la versión de noviembre puede afectar primero a otras partes de su cuenta antes de habilitar la asignación de grupo para las restricciones de inscripción.

Compatibilidad con varios conectores de Servicio de inscripción de dispositivos de red (NDES)

NDES permite que los dispositivos móviles que se ejecutan sin credenciales de dominio puedan obtener certificados a través del Protocolo de inscripción de certificados simple (SCEP). Con esta actualización, se admiten varios conectores NDES.

Administración independiente de dispositivos Android for Work y dispositivos Android

Intune admite la administración de inscripciones de dispositivos Android for Work independientemente de la plataforma Android. Esta configuración se administra en **Inscripción de dispositivos** > **Restricciones de inscripción** > **Restricciones de tipo de dispositivo**. (Anteriormente se encontraban bajo **Inscripción de dispositivos** > **Inscripción en Android for Work** > **Configuración de la inscripción de Android for Work**).

De forma predeterminada, la configuración de los dispositivos Android for Work es igual que la configuración de los dispositivos Android. Sin embargo, dejará de ser así tras modificar la configuración de Android for Work.

Si bloquea la inscripción de Android for Work personal, tan solo los dispositivos Android corporativos podrán inscribirse como Android for Work.

Cuando trabaje con la nueva configuración, tenga en cuenta estos puntos:

Si es la primera vez que incorpora inscripciones de Android for Work

La nueva plataforma Android for Work está bloqueada de manera predeterminada en Restricciones de tipo de dispositivo. Después de incorporar la característica, puede permitir que los dispositivos se inscriban con Android for Work. Para ello, cambie el valor predeterminado o cree una nueva restricción de tipo de dispositivo que sustituya a la predeterminada.

Si ya ha incorporado inscripciones de Android for Work

Si no es la primera que realiza una incorporación, su situación depende de la configuración elegida:

SETTING	ESTADO DE ANDROID FOR WORK EN EL VALOR PREDETERMINADO DE RESTRICCIÓN DE TIPO DE DISPOSITIVO	NOTAS
Administrar todos los dispositivos como Android	Bloqueado	Todos los dispositivos Android deben inscribirse sin Android for Work.
Administrar los dispositivos compatibles como Android for Work	Permitido	Todos los dispositivos que admiten Android for Work deben inscribirse con Android for Work.
Administrar los dispositivos compatibles para usuarios solo en estos grupos como Android for Work	Bloqueado	Para invalidar el valor predeterminado, se creó una directiva de restricción de tipo de dispositivo independiente. Esta directiva define los grupos que se seleccionaron previamente para permitir la inscripción de Android for Work. Los usuarios de los grupos seleccionados seguirán teniendo permiso para inscribir sus dispositivos Android for Work. Todos los demás usuarios tienen restringida la inscripción con Android for Work.

En todos los casos, se conserva la normativa que haya previsto. No se requiere ninguna acción por su parte para seguir permitiendo Android for Work en su entorno, tanto de forma global como por grupo.

Compatibilidad con Google Play Protect en Android

Con el lanzamiento de Android Oreo, Google presenta un conjunto de características de seguridad denominado Google Play Protect que permite a los usuarios y las organizaciones ejecutar aplicaciones e imágenes de Android seguras. Intune ya admite las características de Google Play Protect, incluida la atestación remota de SafetyNet. Los administradores pueden establecer requisitos para directivas de cumplimiento que exijan que Google Play Protect esté configurado y en buen estado. La opción **SafetyNet device attestation** (Atestación de dispositivo SafetyNet) requiere que el dispositivo se conecte con un servicio de Google para comprobar que se encuentra en buen estado y no está en riesgo. Los administradores también pueden establecer una opción en

el perfil de configuración de Android for Work para requerir que se comprueben las aplicaciones instaladas por los servicios de Google Play. Si un dispositivo no es compatible con los requisitos de Google Play Protect, el acceso condicional puede impedir que los usuarios accedan a los recursos corporativos.

- Obtenga información sobre la Creación de una directiva de cumplimiento de dispositivos para habilitar Google Play Protect.

Protocolo de texto permitido en aplicaciones administradas

Las aplicaciones administradas por Intune App SDK pueden enviar mensajes SMS.

Actualización del informe de instalación de aplicaciones para incluir el estado Instalación pendiente

El informe **Estado de instalación de la aplicación**, accesible para todas las aplicaciones a través de la lista **Aplicación** de la carga de trabajo **Aplicaciones cliente**, contiene ahora un recuento **Instalación pendiente** para usuarios y dispositivos.

API de inventario de aplicaciones iOS 11 para la detección de amenazas en dispositivos móviles

Intune recopila la información de inventario de aplicaciones de los dispositivos personales y corporativos, y la pone a disposición de los proveedores de detección de amenazas en dispositivos móviles (MTD), como Lookout for Work. Puede recopilar un inventario de aplicaciones de los usuarios de dispositivos iOS 11 y posteriores.

Inventario de aplicaciones

Los inventarios de los dispositivos iOS 11 y versiones posteriores, tanto de empresa como personales, se envían al proveedor de servicios MTD. El inventario de aplicaciones incluye los datos siguientes:

- Identificador de la aplicación
- Versión de la aplicación
- Nombre corto de la versión
- Nombre de la aplicación
- Tamaño del lote de aplicaciones
- Tamaño dinámico de la aplicación
- Aplicación validada o no validada
- Aplicación administrada o no administrada

Migración de dispositivos y usuarios de MDM híbrida a Intune independiente

Ya hay disponibles nuevos procesos y herramientas para mover usuarios y sus dispositivos de MDM híbrida a Intune en Azure Portal, lo que le permitirá llevar a cabo las tareas siguientes:

- Copiar directivas y perfiles de la consola de Configuration Manager a Intune en Azure Portal
- Mover un subconjunto de usuarios a Intune en Azure Portal conservando el resto en MDM híbrida
- Migrar dispositivos a Intune en Azure Portal sin tener que volver a inscribirlos

Compatibilidad de alta disponibilidad de On-premises Exchange Connector

Una vez que el conector de Exchange cree una conexión a Exchange mediante el servidor de acceso de cliente (CAS) especificado, el conector tendrá la capacidad de detectar otros CAS. Si la CAS principal deja de estar disponible, el conector efectuará una conmutación por error en otra CAS, si está disponible, hasta que la CAS principal esté disponible. Para obtener más información, consulte Compatibilidad de alta disponibilidad de On-premises Exchange Connector.

Reinicio remoto de dispositivos iOS (solo supervisado)

Con una acción del dispositivo, ahora puede reiniciar un dispositivo supervisado de iOS 10.3 y versiones posteriores. Para obtener más información sobre el uso de la acción de reinicio del dispositivo, consulte Reinicio remoto de los dispositivos con Intune.

> **NOTE**
> Para usar este comando es necesario que el dispositivo esté supervisado y disponer del derecho de acceso **Bloqueo del dispositivo**. El dispositivo se reinicia inmediatamente. Después de un reinicio, los dispositivos iOS bloqueados mediante código de acceso no volverán a unirse a una red Wi-Fi y es posible que no puedan comunicarse con el servidor.

Compatibilidad del inicio de sesión único con iOS

En el caso de los usuarios de iOS, puede usar el inicio de sesión único. Las aplicaciones de iOS que están codificadas para buscar las credenciales de usuario en la carga de inicio de sesión único funcionarán con esta actualización de la configuración de carga. También puede utilizar el UPN y el identificador de dispositivo de Intune para configurar el nombre de la entidad de seguridad y el dominio Kerberos. Para obtener más información, consulte Configuración del inicio de sesión único de Intune para dispositivos iOS.

Adición de "Buscar mi iPhone" para dispositivos personales

Ahora puede ver si los dispositivos iOS tienen activado el Boqueo de activación. Esta característica se encontraba anteriormente en Intune, en el portal clásico.

Bloqueo remoto de los dispositivos macOS administrados con Intune

Si pierde un dispositivo macOS, puede bloquearlo y establecer un PIN de recuperación de seis dígitos. Una vez bloqueado, la hoja de **información general del dispositivo** muestra el PIN hasta que se envía otra acción de dispositivo.

Para obtener más información, consulte Bloqueo remoto de los dispositivos administrados con Intune.

Nuevos detalles admitidos del perfil SCEP

Ahora los administradores pueden establecer configuraciones adicionales al crear un perfil de SCEP en las plataformas Windows, iOS, macOS y Android. Los administradores pueden establecer el IMEI, el número de serie o el nombre común, incluido el correo electrónico en el formato de nombre de sujeto.

Conservación de los datos durante un restablecimiento de fábrica

Al restablecer la versión 1709 de Windows 10 y versiones posteriores a la configuración de fábrica, está disponible una nueva funcionalidad. Los administradores pueden especificar si la inscripción de dispositivos y otros datos aprovisionados se conservan en un dispositivo tras un restablecimiento de fábrica.

Los siguientes datos se conservan tras un restablecimiento de fábrica:

- Cuentas de usuario asociadas con el dispositivo
- Estado del equipo (unión a un dominio, unido a Azure Active Directory)
- Inscripción de MDM
- Aplicaciones instaladas por OEM (aplicaciones de Win32 y tienda)
- Perfil de usuario
- Datos de usuario fuera del perfil de usuario
- Inicio de sesión automático del usuario

Los datos siguientes no se conservan:

- Archivos de usuario
- Aplicaciones instaladas por el usuario (aplicaciones de Win32 y tienda)
- Configuración del dispositivo no predeterminada

Se muestran las asignaciones del círculo de actualizaciones de Windows 10

Cuando esté **solucionando problemas**, y en relación al usuario que está visualizando, puede ver las asignaciones de círculos de actualizaciones de Windows 10.

Configuración de frecuencia de informes de Windows Defender for Endpoint

El servicio Defender for Endpoint permite a los administradores gestionar la frecuencia con la que se generan

informes relativos a los dispositivos administrados. Con la nueva opción **Frecuencia de informes de telemetría urgentes**, Defender for Endpoint recopila datos y evalúa los riesgos con una frecuencia mayor. El valor predeterminado para los informes optimiza el rendimiento y la velocidad. Aumentar la frecuencia de los informes puede ser muy útil para dispositivos de alto riesgo. Esta configuración puede encontrarse en el perfil **Windows Defender for Endpoint** en **Configuraciones de dispositivos**.

Actualizaciones de auditoría

La auditoría de Intune proporciona un registro de las operaciones que implican cambios en Intune. Todas las operaciones de creación, actualización, eliminación y tareas remotas se registran y se conservan durante un año. Azure Portal proporciona una vista filtrable de los datos auditados durante los últimos 30 días en cada carga de trabajo. Con la correspondiente API de Graph es posible recuperar los datos de auditoría almacenados durante el último año.

La auditoría se encuentra en el grupo **MONITOR**. El elemento de menú **Registros de auditoría** está disponible para cada una de las carga de trabajo.

Aplicación Portal de empresa ya disponible para macOS

El Portal de empresa de Intune en macOS tiene una experiencia actualizada, que se ha optimizado para mostrar correctamente toda la información y las notificaciones de cumplimiento que los usuarios necesitan en todos los dispositivos que han inscrito. Además, una vez que Portal de empresa se haya implementado en un dispositivo, las actualizaciones se proporcionarán a través de Microsoft AutoUpdate para macOS. Inicie sesión en el sitio web del Portal de empresa de Intune desde un dispositivo macOS para descargar el nuevo Portal de empresa de Intune para macOS.

Inclusión de Microsoft Planner en la lista de aplicaciones aprobadas para la administración de aplicaciones móviles (MAM)

La aplicación de Microsoft Planner para iOS y Android ahora forma parte de las aplicaciones aprobadas para la administración de aplicaciones móviles (MAM). La aplicación puede configurarse para todos los inquilinos mediante la hoja Intune App Protection de Azure Portal.

- Para obtener más información, consulte la lista de aplicaciones aprobadas para MAM.

Frecuencia de actualización de requisitos de VPN por aplicación en dispositivos iOS

En el caso de las aplicaciones en dispositivos iOS, los administradores ahora pueden quitar los requisitos de VPN por aplicación. Los dispositivos afectados se actualizarán tras la siguiente validación de Intune, que por lo general se produce cada 15 minutos.

Compatibilidad con el módulo de administración de System Center Operations Manager para Exchange Connector

El módulo de administración de System Center Operations Manager para Exchange Connector ya está disponible para ayudarle a analizar los registros de Exchange Connector. Esta característica ofrece distintas maneras de supervisar el servicio cuando haya que resolver problemas.

Administración conjunta para dispositivos de Windows 10

La administración conjunta es una solución que sirve para ofrecer un vínculo entre la administración tradicional y la administración moderna. Además, le proporciona una guía para llevar a cabo la transición con un enfoque por fases. Básicamente, la administración conjunta es una solución en la que los dispositivos de Windows 10 se administran de forma simultánea mediante Configuration Manager y Microsoft Intune. También se unen a Active Directory (AD) y a Azure Active Directory (Azure AD). Esta configuración proporciona un método para poder modernizar la administración con el tiempo, a la velocidad que sea adecuada para su organización si no puede moverlo todo a la vez.

Restricción de la inscripción de Windows según la versión del sistema operativo

Como administrador de Intune, ahora puede especificar una versión mínima y máxima de Windows 10 para poder inscribir dispositivos. Estas restricciones se pueden establecer en la hoja **Configuraciones de plataforma**.

Intune seguirá permitiendo la inscripción de teléfonos y equipos con Windows 8.1, pero solo se pueden establecer los límites mínimo y máximo de las versiones de Windows 10. Para permitir la inscripción de

dispositivos 8.1, deje vacío el límite mínimo.

Alertas de dispositivos sin asignar de Windows Autopilot

Hay una nueva alerta disponible relativa a los dispositivos sin asignar de Windows AutoPilot en la página **Microsoft Intune** > **Inscripción de dispositivos** > **Información general**. Esta alerta indica cuántos dispositivos del programa AutoPilot no tienen asignados perfiles de implementación de AutoPilot. Use la información provista en la alerta para crear perfiles y asignarlos a los dispositivos sin asignar. Al hacer clic en la alerta, verá una lista completa de dispositivos de Windows AutoPilot e información detallada sobre ellos. Para obtener más información, vea Inscribir dispositivos mediante el programa Windows AutoPilot Deployment.

Botón Actualizar de la lista de dispositivos

La lista de dispositivos no se actualiza automáticamente, de modo que puede usar el nuevo botón Actualizar para actualizar los dispositivos que figuran en esa lista.

Compatibilidad con la entidad de certificación (CA) en la nube de Symantec

Intune admite ahora la entidad de certificación en la nube de Symantec, que permite que Intune Certificate Connector emita certificados PKCS desde la entidad de certificación en la nube de Symantec para dispositivos administrados por Intune. Si ya usa Intune Certificate Connector con la entidad de certificación de Microsoft, puede usar la configuración existente de Intune Certificate Connector para agregar compatibilidad con la entidad de certificación de Symantec.

Nuevos elementos agregados al inventario de dispositivos

Los nuevos elementos que se indican a continuación ya están disponibles en el inventario de los dispositivos inscritos:

- Dirección MAC de Wi-Fi
- Espacio de almacenamiento total
- Espacio disponible total
- MEID
- Operador del suscriptor

Establecimiento del acceso para las aplicaciones mediante una revisión de seguridad mínima de Android en el dispositivo

Un administrador puede definir la revisión de seguridad mínima de Android que debe estar instalada en el dispositivo para poder obtener acceso a una aplicación administrada en una cuenta administrada.

> **NOTE**
> Esta característica solamente restringe las revisiones de seguridad publicadas por Google en dispositivos Android 6.0 y versiones posteriores.

Compatibilidad con inicio condicional de aplicación

Los administradores de TI ahora pueden establecer un requisito a través del portal de administración de Azure para exigir un código de acceso en lugar de un PIN numérico mediante la administración de aplicaciones móviles (MAM) cuando se inicia la aplicación. Si se configura, se le pide al usuario que establezca y use un código de acceso cuando se le solicite antes de obtener acceso a aplicaciones habilitadas para MAM. Un código de acceso se define como un PIN numérico con al menos un carácter especial o un carácter alfabético en mayúsculas/minúsculas. Esta versión de Intune habilitará esta característica **solo en iOS**. Intune admite un código de acceso de forma similar al PIN numérico. Establece una longitud mínima y permite la repetición de caracteres y secuencias. Esta característica requiere el uso de ciertas aplicaciones (es decir, WXP, Outlook, Managed Browser o Yammer) para integrar Intune App SDK con el código de esta y aplicar la configuración del código de acceso en las aplicaciones de destino.

Número de versión de la aplicación para línea de negocio en el informe de estado de instalación del dispositivo

Con esta versión, el informe de estado de instalación del dispositivo mostrará el número de versión de aplicación de las aplicaciones de línea de negocio para iOS y Android. Puede usar esta información para

solucionar problemas de las aplicaciones o buscar los dispositivos que ejecuten versiones obsoletas de la aplicación.

Los administradores ya pueden configurar las opciones del firewall en un dispositivo mediante un perfil de configuración de dispositivo

Los administradores pueden activar el firewall para los dispositivos y, además, configurar varios protocolos para redes públicas, privadas y de dominio. Esta configuración del firewall se encuentra en el perfil "Endpoint Protection".

Protección de aplicaciones de Windows Defender ayuda a proteger los dispositivos de sitios web que no son de confianza, en función de la definición de la organización

Los administradores pueden definir sitios como "de confianza" o "corporativos" mediante un flujo de trabajo de Windows Information Protection o el nuevo perfil de "límite de red" en las configuraciones del dispositivo. Si se visualizan con Microsoft Edge, todos los sitios que no aparezcan en un límite de red de confianza de un dispositivo de Windows 10 de 64 bits se abrirán en un explorador de un equipo virtual de Hyper-V.

La Protección de aplicaciones se encuentra en los perfiles de configuración del dispositivo, en el perfil "Endpoint Protection". Desde allí, los administradores pueden configurar la interacción entre el explorador virtualizado y el equipo host, los sitios que son y que no son de confianza, y el almacenamiento de datos generado en el explorador virtualizado. Para usar la Protección de aplicaciones en un dispositivo, debe configurarse primero un límite de red. Es importante definir un solo límite de red para un dispositivo.

Control de aplicaciones de Windows Defender en Windows 10 Enterprise ofrece el modo de confiar solo en aplicaciones autorizadas

Teniendo en cuenta que cada día se crean miles de archivos malintencionados, el uso de la detección antivirus basada en firma para luchar contra el malware podría ser insuficiente para proporcionar una defensa adecuada contra nuevos ataques. Mediante Windows Defender Application Control en Windows 10 Enterprise, puede cambiar la configuración del dispositivo de un modo en el que las aplicaciones son de confianza a menos que las bloquee un antivirus u otra solución de seguridad, a un modo en el que el sistema operativo solo confía en las aplicaciones autorizadas por la empresa. La confianza se asigna a las aplicaciones en Windows Defender Application Control.

Mediante Intune, puede configurar las directivas de control de aplicaciones en modo de "solo auditoría" o en el modo de uso forzoso. Las aplicaciones no se bloquean cuando se ejecutan en modo "Solo auditoría". El modo "Solo auditoría" registra todos los eventos en registros locales del cliente. También puede configurar si solo se pueden ejecutar componentes de Windows y aplicaciones de Microsoft Store, o si también se pueden ejecutar otras aplicaciones con buena reputación de acuerdo con la definición de Intelligent Security Graph.

Protección contra vulnerabilidades de seguridad de Windows Defender es un nuevo conjunto de funciones de prevención de intrusiones para Windows 10

La Protección contra vulnerabilidades de seguridad de Windows Defender incluye reglas personalizadas para reducir la explotabilidad de las aplicaciones. También impide las amenazas de macros y scripts, bloquea automáticamente las conexiones de red a direcciones IP de mala reputación y puede proteger los datos contra el ransomware y amenazas desconocidas. La Protección contra vulnerabilidades de seguridad de Windows Defender consta de los componentes siguientes:

- La **reducción de la superficie expuesta a ataques** proporciona reglas que permiten impedir las amenazas de macros, scripts y correos electrónicos.
- El **acceso controlado a carpetas** bloquea automáticamente el acceso a contenido en las carpetas protegidas.
- El **filtro de red** bloquea las conexiones salientes desde cualquier aplicación a IP o dominios de mala reputación.
- La **protección contra vulnerabilidades** proporciona restricciones de memoria, flujo de control y directivas que pueden usarse para proteger una aplicación contra las vulnerabilidades.

Administrar scripts de PowerShell en Intune para dispositivos Windows 10

La extensión de administración de Intune permite cargar los scripts de PowerShell en Intune para ejecutarse en dispositivos Windows 10. Esta extensión complementa las capacidades de administración de dispositivos

móviles (MDM) de Windows 10 y facilita la transición a una administración moderna. Para conocer más detalles, vea Administrar scripts de PowerShell en Intune para dispositivos Windows 10.

Nueva configuración de restricciones de dispositivos para Windows 10

- Mensajería (solo móvil): deshabilitar pruebas o mensajes MMS
- Contraseña: configuración para habilitar FIPS y el uso de dispositivos secundarios Windows Hello para la autenticación
- Pantalla: configuración para activar o desactivar el ajuste de escala de GDI para las aplicaciones heredadas

Restricciones de dispositivos Windows 10 a pantalla completa

Puede restringir usuarios de dispositivos Windows 10 a pantalla completa, lo que les limita a un conjunto de aplicaciones predefinidas. Para ello, cree un perfil de restricción de dispositivo Windows 10 y defina la configuración de pantalla completa.

La pantalla completa admite dos modos: **aplicación única**, que permite que un usuario ejecute una sola aplicación, o **varias aplicaciones**, que permite el acceso a un conjunto de aplicaciones. Para determinar las aplicaciones compatibles, debe definir la cuenta de usuario y el nombre del dispositivo. Cuando el usuario ha iniciado sesión, verá únicamente las aplicaciones definidas. Para obtener más información, vea AssignedAccess CSP (CSP AssignedAccess).

La pantalla completa requiere lo siguiente:

- Intune debe ser la entidad de MDM.
- Las aplicaciones deben estar ya instaladas en el dispositivo de destino.
- El dispositivo debe estar aprovisionado correctamente.

Nuevo perfil de configuración de dispositivo para crear límites de red

En los otros perfiles de configuración de dispositivo encontrará un nuevo perfil de configuración de dispositivo llamado **Límite de red**. Use este perfil para definir los recursos en línea que quiere que se consideren corporativos y de confianza. Debe definir un límite de red para un dispositivo *antes* de que en el dispositivo se puedan usar características como la Protección de aplicaciones de Windows Defender y Windows Information Protection. Es importante definir un solo límite de red para cada dispositivo.

Puede definir los recursos de empresa en la nube, los intervalos de direcciones IP y los servidores proxy internos que quiere que se consideren de confianza. Una vez definidos, pueden usar el límite de red otras características como la Protección de aplicaciones de Windows Defender y Windows Information Protection.

Dos opciones de configuración adicionales para Antivirus de Windows Defender

Nivel de bloqueo de archivos

CONFIGURACIÓN	DETALLES
No configurado	**No configurado** usa el nivel de bloqueo predeterminado de Antivirus de Windows Defender y proporciona una detección segura sin aumentar el riesgo de detectar archivos legítimos.
Alto	**Alto** se aplica a un alto nivel de detección.
Alto +	**Alto +** proporciona el nivel Alto con medidas de protección adicionales que podrían afectar al rendimiento del cliente.
Tolerancia cero	**Tolerancia cero** bloquea todos los ejecutables desconocidos.

Aunque es improbable, si se establece en **Alto** puede hacer que se detecten algunos archivos legítimos. Se recomienda establecer el nivel de bloqueo de archivos en el valor predeterminado (**No configurado**).

Ampliación del tiempo de espera para la detección de archivos en la nube

SETTING	DETALLE
Número de segundos (0-50)	Especifique el tiempo máximo durante el que Antivirus de Windows Defender debe bloquear un archivo mientras espera un resultado de la nube. El valor predeterminado es de 10 segundos. El tiempo adicional que se especifique aquí (hasta 50 segundos) se agregará a los 10 segundos. En la mayoría de los casos, la detección tarda mucho menos que el tiempo máximo. Si amplía el tiempo, permitirá que la nube investigue a fondo los archivos sospechosos. Se recomienda que habilite esta opción y que especifique al menos 20 segundos adicionales.

Adición de la VPN de Citrix a dispositivos Windows 10

Puede configurar la VPN de Citrix para sus dispositivos Windows 10. Puede elegir la VPN de Citrix en la lista *Seleccione un tipo de conexión* en la hoja **VPN base** al configurar una VPN para Windows 10 y versiones posteriores.

> **NOTE**
> La configuración de Citrix ya existía para iOS y Android.

Las conexiones Wi-Fi admiten claves precompartidas en iOS

Los clientes pueden configurar perfiles de Wi-Fi para usar claves precompartidas (PSK) en las conexiones WPA o WPA2 Personal en dispositivos iOS. Estos perfiles se insertan en el dispositivo del usuario al inscribirlo en Intune.

Cuando el perfil se haya insertado en el dispositivo, el siguiente paso dependerá de la configuración del perfil. Si está establecido para conectarse automáticamente, lo hace cuando la red se necesite. Cuando el perfil se conecta de forma manual, el usuario deberá activar manualmente la conexión.

Acceso a los registros de aplicación administrada de iOS

Ahora, los usuarios finales que tengan Managed Browser instalado pueden ver el estado de administración de todas las aplicaciones publicadas de Microsoft y enviar registros para solucionar problemas con sus aplicaciones iOS administradas.

Para más información sobre cómo habilitar el modo de solución de problemas en Managed Browser en un dispositivo iOS, vea Cómo tener acceso a los registros de aplicación administrada con Managed Browser en iOS.

Mejoras en el flujo de trabajo de configuración de dispositivos en la versión 2.9.0 de Portal de empresa para iOS

El flujo de trabajo de configuración de dispositivos se ha mejorado en la aplicación Portal de empresa para iOS. El lenguaje resulta más fácil de usar y se han combinado pantallas donde era posible. Además, hemos utilizado el nombre de su empresa en el texto del proceso de configuración para que el lenguaje sea más específico. Puede consultar el flujo de trabajo actualizado en la página de novedades de la interfaz de usuario de la aplicación.

La entidad de usuario contiene los datos de usuario más recientes en el modelo de datos de Data Warehouse

La primera versión del modelo de datos del Almacenamiento de datos de Intune solo contenía datos de Intune recientes e históricos. Los creadores de informes no podían capturar el estado actual de un usuario. En esta actualización, la **entidad de usuario** se rellena con los datos más recientes del usuario.

Octubre de 2017

El número de versión de la aplicación de línea de negocio de Android y iOS es visible

Las aplicaciones de Intune ahora muestran el número de versión para las aplicaciones de línea de negocio de iOS y Android. El número se muestra en la lista de aplicaciones de Azure Portal y en la hoja de información

general de la aplicación. Los usuarios finales pueden ver este número en la aplicación Portal de empresa y en el portal web.

Número de versión completo El número de versión completo identifica una versión específica de la aplicación. El número aparece como *versión*(*compilación*). Por ejemplo, 2.2(2.2.17560800).

El número de versión completo consta de dos componentes:

- **Versión**
  El número de versión es el número que pueden ver los usuarios. Sirve para que los usuarios finales distingan las diferentes versiones de la aplicación.
- **Número de compilación**
  El número de compilación es un número interno que puede usarse para la detección de la aplicación y para administrar la aplicación mediante programación. El número de compilación alude a una iteración de la aplicación que hace referencia a los cambios en el código.

Obtenga más información sobre los números de versión y el desarrollo de aplicaciones de línea de negocio en Introducción al SDK para aplicaciones de Microsoft Intune.

Integración de la administración de dispositivos y aplicaciones

Ahora que se puede acceder a la administración de dispositivos móviles (MDM) y a la administración de aplicaciones móviles (MAM) de Intune desde Azure Portal, Intune ha empezado a integrar la experiencia de administración de TI en torno a la administración de aplicaciones y dispositivos. Estos cambios están pensados para simplificar la experiencia de administración de dispositivos y aplicaciones.

Obtenga más información sobre los cambios anunciados en MDM y MAM en el blog del equipo de soporte técnico de Intune.

Nuevas alertas de inscripción de dispositivos de Apple

En la página de información general de la inscripción se mostrarán alertas relacionadas con la administración de dispositivos de Apple que resultarán útiles para los administradores de TI. Las alertas se mostrarán en la página de información general cuando el certificado de inserción MDM de Apple esté a punto de expirar o ya lo haya hecho; cuando el token del Programa de inscripción de dispositivos vaya a expirar o ya lo haya hecho; y cuando haya dispositivos sin asignar en el Programa de inscripción de dispositivos.

Reemplazo de tokens en la configuración de aplicaciones sin inscripción de dispositivos

Puede usar tokens para valores dinámicos de la configuración de las aplicaciones en dispositivos que no están inscritos. Para obtener más información, consulte Agregar directivas de configuración para aplicaciones administradas sin inscripción de dispositivos.

Actualizaciones de la aplicación Portal de empresa para Windows 10

La página Configuración de la aplicación de Portal de empresa para Windows 10 se ha actualizado para que las opciones y las acciones de usuario previstas sean más coherentes en relación con el resto de opciones de configuración. También se ha actualizado para que el diseño coincida con el de otras aplicaciones de Windows. Puede ver imágenes del antes y el después en la página de novedades de la interfaz de usuario de la aplicación.

Detalles para los usuarios finales sobre qué información del dispositivo se puede ver para dispositivos Windows 10

Se agregó **Tipo de propiedad** en la pantalla Detalles del dispositivo en la aplicación Portal de empresa para Windows 10. Esto permitirá que los usuarios obtengan más información sobre la privacidad directamente en esta página de los documentos para el usuario final de Intune. También se podrán encontrar estos detalles en la pantalla **Información**.

Solicitudes de comentarios sobre la aplicación Portal de empresa para Android

Ahora la aplicación Portal de empresa para Android solicita comentarios del usuario final. Estos comentarios se envían directamente a Microsoft, además de ofrecer a los usuarios finales una oportunidad para revisar la aplicación en Google Play Store público. Los comentarios no son obligatorios, por lo que los usuarios pueden descartarlos y continuar usando la aplicación.

Ayuda a los usuarios con la aplicación Portal de empresa para Android

La aplicación Portal de empresa para Android incorpora instrucciones adicionales para los usuarios finales con la finalidad de ayudarles a comprender y, siempre que sea posible, resolver por ellos mismos los nuevos casos de uso.

- Se guiará a los usuarios finales al portal de Azure Active Directory para quitar un dispositivo si han alcanzado el número máximo de dispositivos que pueden agregar.
- A los usuarios finales se les indican los pasos que deben seguir para ayudarles a corregir errores de activación en dispositivos Samsung Knox o a desactivar el modo de ahorro de energía. Si ninguna de estas soluciones resuelve su problema, se proporcionará una explicación de cómo enviar registros a Microsoft.

Nueva acción "Resolver" disponible para dispositivos Android

La aplicación Portal de empresa para Android presenta una acción "Resolver" en la página *Actualizar configuración del dispositivo*. Si se selecciona esta opción, se remitirá al usuario final directamente a la configuración que causa el incumplimiento del dispositivo. La aplicación Portal de empresa para Android admite actualmente esta acción para las opciones de configuración código de acceso de dispositivo, depuración USB y orígenes desconocidos.

Indicador de progreso de configuración de dispositivos en Portal de empresa para Android

La aplicación Portal de empresa para Android muestra un indicador de progreso de instalación de dispositivos cuando un usuario inscribe sus dispositivos. El indicador muestra estados nuevos, comenzando con "Configurando el dispositivo...", sigue con "Registrando el dispositivo..." y "Finalizando el registro del dispositivo...", y acaba con "Finalizando la configuración del dispositivo...".

Compatibilidad con la autenticación basada en certificados en Portal de empresa para iOS

Se ha agregado compatibilidad con la autenticación basada en certificados (CBA) en la aplicación Portal de empresa para iOS. Los usuarios con CBA escriben su nombre de usuario y luego pulsan el vínculo “Iniciar sesión con un certificado”. CBA ya se admite en las aplicaciones del Portal de empresa de Android y Windows. Puede aprender más sobre la página de inicio de sesión en la aplicación del Portal de empresa.

Las aplicaciones que están disponibles con o sin inscripción ahora se pueden instalar sin que se les solicite la inscripción.

Ahora, las aplicaciones de empresa que se han puesto a disposición de los usuarios con o sin inscripción en la aplicación de Portal de empresa de Android pueden instalarse sin necesidad de una solicitud de inscripción.

Compatibilidad del programa Windows AutoPilot Deployment en Microsoft Intune

Ahora puede usar Microsoft Intune con el programa Windows AutoPilot Deployment para que los usuarios puedan aprovisionar sus dispositivos de empresa sin necesidad de recurrir al departamento de TI. Puede personalizar la experiencia de configuración rápida y guiar a los usuarios durante la combinación de sus dispositivos con Azure AD y la inscripción en Intune. Al usar conjuntamente Microsoft Intune y Windows AutoPilot, se acaba con la necesidad de implementar, mantener y administrar imágenes del sistema operativo. Para obtener información, consulte Inscribir dispositivos mediante el programa Windows AutoPilot Deployment.

Inicio rápido para la inscripción de dispositivos

Ahora el inicio rápido está disponible en **Inscripción de dispositivos** y proporciona una tabla de referencias para administrar plataformas y configurar el proceso de inscripción. Para simplificar la iniciación, se ofrece documentación útil en forma de una breve descripción de cada elemento y enlaces a documentación con instrucciones paso a paso.

Categorización de dispositivos

En el gráfico de la plataforma de dispositivos inscritos de la hoja **Dispositivos** > **Información general** se organizan los dispositivos por plataforma, incluidos Android, iOS, macOS, Windows y Windows Mobile. Los dispositivos que ejecutan otros sistemas operativos se agrupan en "Otros", por ejemplo, dispositivos fabricados por Blackberry, NOKIA u otros fabricantes.

Para obtener información sobre los dispositivos que se ven afectados en el inquilino, elija **Administrar** > **Todos los dispositivos** y después use **Filtrar** para limitar el campo **Sistema operativo**.

Zimperium: nuevo socio de defensa contra amenazas móviles

Puede controlar el acceso desde dispositivos móviles a recursos corporativos mediante el acceso condicional basado en la evaluación de riesgos efectuada por Zimperium, una solución de defensa contra amenazas móviles integrada en Microsoft Intune.

Funcionamiento de la integración con Intune

El riesgo se evalúa según la telemetría recopilada de dispositivos con Zimperium. Se pueden configurar directivas de acceso condicional de EMS según la evaluación de riesgos de Zimperium habilitada mediante las directivas de cumplimiento de los dispositivos de Intune, que puede usar para permitir o bloquear el acceso de los dispositivos no compatibles a los recursos corporativos en función de las amenazas detectadas.

Nueva configuración del perfil de restricción de dispositivos Windows 10

Estamos agregando nuevas configuraciones al perfil de restricción de dispositivos Windows 10 en la categoría de SmartScreen de Windows Defender.

Para obtener información sobre el perfil de restricción de dispositivos Windows 10, vea Configuración de restricciones de dispositivos Windows 10 y versiones posteriores.

Soporte remoto para dispositivos Windows y Windows Mobile

Ahora Intune puede usar el software TeamViewer, que se compra por separado, para que pueda ofrecer asistencia remota a los usuarios que estén ejecutando Windows y dispositivos Windows Mobile.

Examen de dispositivos con Windows Defender

Ahora puede ejecutar un **Examen rápido** y un **Examen completo**, además de **Actualizar firmas**, con el antivirus Windows Defender en los dispositivos Windows 10 administrados. En la hoja de información general del dispositivo, elija la acción que desea ejecutar en el dispositivo. Se le pide que confirme la acción antes de que el comando se envíe al dispositivo.

Examen rápido: un examen rápido examina las ubicaciones donde el malware se registra para iniciarse, como las claves del Registro y las carpetas de inicio de Windows conocidas. Un examen rápido tarda de media cinco minutos. Al combinarlo con la opción **Always-on real-time protection** (Protección en tiempo real siempre activa), que examina los archivos cuando están abiertos o cerrados y siempre que un usuario navega a una carpeta, el examen rápido ayuda a proporcionar protección frente a malware que podría estar en el sistema o el kernel. Los usuarios ven los resultados del examen en sus dispositivos cuando termina.

Examen completo: un examen completo puede resultar útil en los dispositivos que han encontrado una amenaza de malware para identificar si existe algún componente inactivo que requiera una limpieza más exhaustiva, además de para ejecutar exámenes a petición. El examen completo puede tardar una hora en ejecutarse. Los usuarios ven los resultados del examen en sus dispositivos cuando termina.

Actualizar firmas: el comando de actualización de firmas actualiza las definiciones y las firmas de malware del antivirus de Windows Defender. Esto le ayuda a asegurarse de que el antivirus de Windows Defender es eficaz en la detección de malware. Esta característica es para dispositivos Windows 10 únicamente, está pendiente la conectividad a Internet de los dispositivos.

Se ha quitado el botón Habilitar/Deshabilitar de la página de la entidad emisora de certificados de Azure Portal de Intune

Se está eliminando un paso adicional para configurar el conector de certificados en Intune. Actualmente, descarga el conector del certificado y después lo habilita en la consola de Intune. En cambio, si deshabilita el conector en la consola de Intune, el conector sigue emitiendo certificados.

¿Cómo me afecta esto?

A partir de octubre, el botón Habilitar/Deshabilitar ya no aparecerá en la página de la entidad emisora de certificados en Azure Portal. La funcionalidad del conector sigue siendo la misma. Los certificados todavía se implementan en dispositivos inscritos en Intune. Puede continuar descargando e instalando el conector del certificado. Para detener la emisión de certificados, ahora deberá desinstalar el conector del certificado en vez de deshabilitarlo.

¿Qué debo hacer para prepararme para este cambio?

Si actualmente tiene el conector del certificado deshabilitado, primero debe desinstalarlo.

Nueva configuración del perfil de restricción de dispositivo de Windows 10 Team

En esta versión, hemos agregado muchas nuevas configuraciones al perfil de restricción de dispositivo de Windows 10 Team para ayudarle a controlar los dispositivos de Surface Hub.

Para obtener más información sobre este perfil, vea Configuración de restricciones de dispositivos Windows 10 Team en Microsoft Intune.

Impedir que los usuarios de dispositivos Android puedan cambiar la fecha y la hora de los dispositivos

Puede usar una directiva de dispositivo personalizada de Android para impedir que los usuarios de dispositivos Android cambien la fecha y la hora del dispositivo.

Para ello, configure una directiva personalizada de Android con el URI de configuración ./Vendor/MSFT/PolicyManager/My/System/AllowDateTimeChange. Establezca este parámetro en **TRUE** y luego asígnelo a los grupos requeridos.

Configuración de dispositivo de BitLocker

La opción **Cifrado de Windows > Configuración base** incluye el nuevo ajuste **Advertencia para otro cifrado de disco** que le permite deshabilitar el mensaje de advertencia para otro cifrado de disco que podría estar en uso en el dispositivo del usuario. El mensaje de advertencia requiere el consentimiento del usuario final antes de configurar BitLocker en el dispositivo y bloquea la instalación de BitLocker hasta que este la confirme. La nueva configuración deshabilita la advertencia del usuario final.

Ahora el programa de compras por volumen para las aplicaciones de empresa se sincronizará con el inquilino de Intune

Los desarrolladores de terceros también pueden distribuir aplicaciones de forma privada a miembros autorizados del Programa de compras por volumen (VPP) para Empresas, especificados en iTunes Connect. Estos miembros pueden iniciar sesión en la tienda de aplicaciones del Programa de Compras por Volumen y comprar aplicaciones.

Con esta versión, el VPP para aplicaciones de empresa que haya comprado el usuario final se sincronizarán con sus inquilinos de Intune.

Selección de la instancia de App Store de Apple del país o región para la sincronización de aplicaciones de VPP

Puede configurar la instancia de App Store del país o la región para el Programa de Compras por Volumen de Apple (VPP) al cargar el token de VPP. Intune sincroniza las aplicaciones de VPP para todas las configuraciones regionales desde la instancia de App Store del país o la región de VPP especificada.

> **NOTE**
> En la actualidad, Intune solo sincroniza las aplicaciones de VPP de la instancia de App Store del país o la región de VPP que coinciden con la configuración regional de Intune en la que se creó el inquilino de Intune.

Bloqueo de las acciones de copiar y pegar entre perfiles profesionales y personales en Android for Work

Con esta versión, es posible configurar el perfil del trabajo para Android for Work a fin de bloquear las acciones de copiar y pegar entre aplicaciones profesionales y personales. Puede encontrar esta nueva opción de configuración en el perfil **Restricciones de dispositivos** para la plataforma **Android for Work** en **Configuración del perfil de trabajo**.

Creación de aplicaciones iOS limitada a determinadas instancias regionales de App Store de Apple

Podrá especificar la configuración regional del país o la región durante la creación de una aplicación administrada de App Store de Apple.

> **NOTE**
> Actualmente, solo puede crear aplicaciones administradas del App Store de Apple que se encuentren en tiendas de Estados Unidos o la región.

Actualización de aplicaciones con licencia para dispositivos y usuarios de VPP de iOS

Podrá configurar el token de VPP de iOS para actualizar todas las aplicaciones adquiridas para ese token a través del servicio de Intune. Intune detectará las actualizaciones de la aplicación de VPP dentro de la App Store y las insertará automáticamente en el dispositivo cuando este se registra.

Para consultar los pasos necesarios para establecer un token de VPP y habilitar las actualizaciones automáticas, consulte [Administrar aplicaciones de iOS compradas a través de un programa de compras por volumen con Microsoft Intune] (../apps/vpp-apps-ios).

Colección de entidades de asociación de dispositivos de usuario agregada al modelo de datos Data Warehouse de Intune

Ahora puede generar informes y visualizaciones de datos con la información de asociación de dispositivo de usuario que asocia las colecciones de la entidad de dispositivo y de usuario. Es posible tener acceso al modelo de datos a través del archivo de Power BI (PBIX) recuperado de la página de almacenamiento de datos de Intune, a través del punto de conexión de OData o mediante el desarrollo de un cliente personalizado.

Revisión del cumplimiento de directivas para los anillos de actualizaciones de Windows 10

Podrá revisar un informe de directiva para los círculos de actualizaciones de Windows 10 desde Actualizaciones de software > Estado de implementación por anillo de actualización. El informe de directiva incluye el estado de implementación para los anillos de actualización que ha configurado.

Nuevo informe en el que se muestran los dispositivos iOS con versiones anteriores de iOS

El informe **Dispositivos iOS obsoletos** está disponible desde el área de trabajo **Actualizaciones de software**. En el informe, puede ver una lista de dispositivos iOS supervisados destinados mediante una directiva de actualización iOS y que tienen actualizaciones disponibles. Para cada dispositivo, puede ver un estado por el que el dispositivo no se ha actualizado automáticamente.

Visualización de las asignaciones de directivas de protección de aplicaciones para la solución de problemas

En la próxima versión, la opción **Directiva de protección de aplicaciones** se agregará a la lista desplegable **Asignaciones** disponible en la hoja de la solución de problemas. Ahora puede seleccionar las directivas de protección de aplicaciones para ver las directivas de protección de aplicaciones asignadas a los usuarios seleccionados.

Mejoras en el flujo de trabajo de configuración de dispositivos en el Portal de empresa

Se ha mejorado el flujo de trabajo de instalación de dispositivos en la aplicación del Portal de empresa para Android. El lenguaje es más fácil de usar y es específico de su empresa. Además, hemos combinado pantallas siempre que hemos podido. Puede ver estas mejoras en la página Novedades de la interfaz de usuario de aplicaciones.

Instrucciones mejoradas sobre la solicitud de acceso a los contactos en dispositivos Android

La aplicación del Portal de empresa para Android requiere a menudo que el usuario final acepte el permiso de contactos. Si un usuario final no acepta este acceso, ahora verá una notificación en la aplicación en la que se le alerta de concederlo para el acceso condicional.

Corrección del inicio seguro para Android

Los usuarios finales con dispositivos Android podrán pulsar en la razón de no compatibilidad en la aplicación del Portal de empresa. Cuando sea posible, esta acción les llevará directamente a la ubicación correcta en la aplicación de configuración para solucionar el problema.

Notificaciones de inserción adicionales para los usuarios finales en la aplicación Portal de empresa para Android Oreo

Los usuarios finales verán notificaciones adicionales que indican cuando la aplicación Portal de empresa para

Android Oreo realiza tareas en segundo plano, como recuperar directivas desde el servicio Intune. Con esto se aumenta la transparencia para los usuarios finales con respecto a cuando Portal de empresa realiza tareas administrativas en el dispositivo. Esto forma parte de la optimización general de la UI de Portal de empresa para la aplicación Portal de empresa para Android Oreo.

Existen más optimizaciones para nuevos elementos de la IU que ya están habilitados para Android Oreo. Los usuarios finales verán notificaciones adicionales en las que se les indicará el momento en el que la aplicación Portal de empresa esté realizando tareas en segundo plano, como la recuperación de directivas desde el servicio Intune. Esto aumenta la transparencia para los usuarios finales sobre cuándo el Portal de empresa está realizando tareas administrativas en el dispositivo.

Nuevos comportamientos para la aplicación de Portal de empresa para Android con perfiles de trabajo

Cuando inscribe un dispositivo de Android for Work con un perfil de trabajo, es la aplicación del Portal de empresa del perfil de trabajo la que realiza las tareas de administración en el dispositivo.

A menos que vaya a usar una aplicación habilitada para MAM en el perfil personal, la aplicación del Portal de empresa para Android ya no satisface todos los usos. Para mejorar la experiencia del perfil de trabajo, Intune oculta automáticamente la aplicación personal del Portal de empresa después de una inscripción correcta del perfil de trabajo.

La aplicación del Portal de empresa para Android se puede habilitar en cualquier momento en el perfil personal; para ello, vaya al Portal de empresa en Play Store y pulse **Habilitar**.

El Portal de empresa para Windows 8.1 y Windows Phone 8.1 se mueve al modo de mantenimiento

A partir de octubre de 2017, las aplicaciones del Portal de empresa para Windows 8.1 y Windows Phone 8.1 se moverán al modo de mantenimiento. Esto significa que las aplicaciones y los escenarios existentes, como inscripción y cumplimiento, se seguirán admitiendo en estas plataformas. Estas aplicaciones seguirán estando disponibles para su descarga mediante los canales de lanzamiento existentes, como Microsoft Store.

Una vez que se encuentre en modo de mantenimiento, estas aplicaciones solo recibirán actualizaciones de seguridad críticas. No habrá actualizaciones adicionales ni se lanzarán características para ellas. En el caso de nuevas características, se recomienda actualizar los dispositivos a Windows 10 o Windows 10 Mobile.

Bloqueo de la inscripción de dispositivos Samsung KNOX no compatibles

La aplicación del Portal de empresa solo intenta inscribir los dispositivos Samsung Knox compatibles. Para evitar errores de activación de Knox que impidan la inscripción de MDM, la inscripción de dispositivos solo se intenta si el dispositivo aparece en la lista de dispositivos publicados por Samsung. Los dispositivos Samsung pueden tener números de modelo que admitan Knox, mientras que otros no. Compruebe la compatibilidad de Knox con su revendedor de dispositivos antes de su compra e implementación. Encontrará la lista completa de dispositivos comprobados en la configuración de directivas de Android y Samsung Knox Standard.

Finalización del soporte para Android 4.3 y versiones inferiores

Las aplicaciones administradas y la aplicación Portal de empresa para Android exigirán Android 4.4 y versiones posteriores para acceder a recursos de empresa. En diciembre, todos los dispositivos inscritos se eliminarán, lo que provocará su pérdida de acceso a los recursos de empresa. Si está usando directivas de protección de aplicaciones sin MDM, las aplicaciones no recibirán actualizaciones y la calidad de su experiencia empeorará con el tiempo.

Detalles para los usuarios finales sobre qué información del dispositivo se puede ver en los dispositivos inscritos

Se va a agregar la opción **Tipo de propiedad** a la pantalla Detalles del dispositivo en todas las aplicaciones del Portal de empresa. De esta manera, los usuarios podrán obtener más información sobre privacidad directamente en el artículo ¿Qué información puede ver mi empresa cuando inscribo mi dispositivo?. Esta funcionalidad se implementará en todas las aplicaciones del Portal de empresa en un futuro cercano. Esto se anunció para iOS en septiembre.

Septiembre de 2017

Intune es compatible con iOS 11

Intune es compatible con iOS 11. Ya se anunció anteriormente en el blog de soporte técnico de Intune.

Finalización del soporte de iOS 8.0

Las aplicaciones administradas y la aplicación Portal de empresa para iOS necesitan iOS 9.0 y posterior para poder acceder a los recursos de la empresa. Los dispositivos que no estén actualizados antes de septiembre de este año ya no podrán acceder a esas aplicaciones ni al Portal de empresa.

Adición de acción de actualización a la aplicación de Portal de empresa para Windows 10

La aplicación de Portal de empresa para Windows 10 permite a los usuarios actualizar los datos de la aplicación tirando para actualizar o, en equipos de escritorio, presionando F5.

Detalles para los usuarios finales sobre qué información del dispositivo se puede ver para iOS

Hemos agregado **Tipo de propiedad** a la pantalla Detalles del dispositivo en la aplicación Portal de empresa para iOS. Esto permitirá que los usuarios obtengan más información sobre la privacidad directamente en esta página de los documentos para el usuario final de Intune. También se podrán encontrar estos detalles en la pantalla Información.

Permitir que los usuarios finales accedan a la aplicación Portal de empresa para Android sin inscripción

Pronto los usuarios finales no tendrán que inscribir sus dispositivos para acceder a la aplicación Portal de empresa para Android. Los usuarios finales de las organizaciones que usen directivas de protección de aplicaciones dejarán de recibir mensajes para inscribir sus dispositivos cuando abran la aplicación Portal de empresa. Los usuarios finales también podrán instalar aplicaciones desde el Portal de empresa sin inscribir el dispositivo.

Frases más fáciles de entender para la aplicación Portal de empresa para Android

El proceso de inscripción de la aplicación Portal de empresa para Android se simplificó con texto nuevo para facilitar la inscripción de los usuarios finales. Si tiene documentación de inscripción personalizada, deberá actualizarla para reflejar las pantallas nuevas. Puede encontrar imágenes de ejemplo en la página Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune.

Adición de la aplicación de Portal de empresa de Windows 10 a la directiva de permiso de Windows Information Protection

La aplicación Portal de empresa de Windows 10 se actualizó para admitir Windows Information Protection (WIP). La aplicación se puede agregar a la directiva de autorización de WIP. Con este cambio, ya no es necesario agregar la aplicación a la lista de **exentos**.

Agosto de 2017

Mejoras en la información general de dispositivos

La información general de dispositivos ahora muestra los que están inscritos, pero excluye a los que administra Exchange ActiveSync. Los dispositivos de Exchange ActiveSync no ofrecen las mismas opciones de administración que los inscritos. Para ver el número de dispositivos inscritos y el de dispositivos inscritos por plataforma en la sección Intune de Azure Portal, vaya a **Dispositivos** > **Información general**.

Mejoras en el inventario de dispositivos recopilado mediante Intune

En esta versión, hemos realizado las siguientes mejoras en la información de inventario que recopilan los dispositivos que administra:

- En dispositivos Android, ahora puede agregar una columna al inventario de dispositivos que muestra el nivel de revisión más reciente de cada uno. Agregue la columna **Nivel de revisión de seguridad** a la lista de dispositivos para verlo.
- Al filtrar la vista de dispositivos, podrá filtrarlos según su fecha de inscripción. Por ejemplo, puede mostrar solo los dispositivos que se hayan inscrito después de una fecha específica.
- Hemos realizado mejoras en el filtro que usa el elemento **Fecha de la última inserción**.
- En la lista de dispositivos, ahora puede mostrar el número de teléfono de los dispositivos corporativos. Además, puede usar el panel de filtros para buscar dispositivos por el número de teléfono.

Para obtener más información sobre el inventario de dispositivos, consulte Visualización del inventario de dispositivos de Intune.

Compatibilidad del acceso condicional con dispositivos macOS

Ahora puede establecer una directiva de acceso condicional que exija que los dispositivos Mac se inscriban en Intune y cumplan las directivas de cumplimiento de dispositivos. Por ejemplo, los usuarios pueden descargar la aplicación Portal de empresa de Intune para macOS e inscribir los dispositivos Mac en Intune. Intune evalúa si el dispositivo Mac es conforme o no con requisitos como el PIN, el cifrado, la versión del sistema operativo y la integridad del sistema.

- Obtenga más información sobre la compatibilidad con el acceso condicional para dispositivos macOS.

La aplicación Portal de empresa para macOS está en versión preliminar pública

La aplicación Portal de empresa para macOS ya está disponible como parte de la versión preliminar pública para el acceso condicional en Enterprise Mobility + Security. Esta versión admite macOS 10.11 y versiones posteriores. Obténgala en https://aka.ms/macOScompanyportal.

Nueva configuración de restricciones de dispositivos para Windows 10

En esta versión, se han agregado opciones nuevas para el perfil de restricción de dispositivos Windows 10 en las siguientes categorías:

- SmartScreen de Windows Defender
- Tienda de aplicaciones

Actualizaciones en el perfil de dispositivo de Endpoint Protection de Windows 10 para la configuración de BitLocker

En esta versión, se han realizado las siguientes mejoras en el funcionamiento de la configuración de BitLocker en un perfil de dispositivo de Endpoint Protection de Windows 10:

- En **Configuración de BitLocker para unidades de sistema operativo**, en el ajuste **BitLocker con un chip TPM no compatible** BitLocker estaba permitido tras seleccionar **Bloquear**. Se ha corregido este problema para poder bloquear BitLocker cuando se selecciona.
- En **Configuración de BitLocker para unidades de sistema operativo**, en el ajuste **Agente de recuperación de datos basada en certificado**, ya puede bloquear explícitamente el agente de recuperación de datos basada en certificado. De forma predeterminada, el agente está permitido.
- En **Configuración de BitLocker para unidades de datos fijas**, en el ajuste **Agente de recuperación de datos**, ya puede bloquear explícitamente el agente de recuperación de datos. Para obtener más información, vea Endpoint protection settings for Windows 10 and later (Configuración de Endpoint Protection para Windows 10 y versiones posteriores).

Nueva experiencia de sesión iniciada para los usuarios del Portal de empresa para Android y para los usuarios de las directivas de App Protection

Los usuarios finales pueden ahora examinar aplicaciones, administrar dispositivos y ver la información de contacto de TI mediante la aplicación del Portal de empresa de Android sin inscribir sus dispositivos Android. Además, si un usuario final ya usa una aplicación protegida por directivas de protección de aplicaciones de Intune y se inicia el Portal de empresa Android, el usuario final ya no recibirá un aviso para inscribir el dispositivo.

Nueva configuración de la aplicación Portal de empresa para Android para alternar la optimización de la batería

La página **Configuración** de la aplicación Portal de empresa para Android tiene una nueva opción que permite a los usuarios desactivar fácilmente la optimización de la batería para las aplicaciones Portal de empresa y Microsoft Authenticator. El nombre de la aplicación que se muestra en la configuración variará dependiendo de qué aplicación administre la cuenta profesional. Recomendamos que los usuarios desactiven la optimización de la batería para obtener un rendimiento mejor de las aplicaciones de trabajo que sincronizan el correo electrónico y los datos.

Compatibilidad con varias identidades en OneNote para iOS

Los usuarios finales ahora pueden usar cuentas diferentes (profesionales o educativas) en Microsoft OneNote para iOS. Las directivas de protección de aplicaciones se pueden aplicar a los datos corporativos en blocs de notas del trabajo sin que esto afecte a sus blocs de notas personales. Por ejemplo, una directiva puede permitir

que un usuario busque información en blocs de notas del trabajo, pero impedir que copie datos corporativos desde un bloc de notas del trabajo a uno personal.

- Obtenga más información sobre las aplicaciones que admiten protección de aplicaciones y varias identidades con Intune.

Nueva configuración para permitir y bloquear aplicaciones en dispositivos Samsung Knox Standard

En esta versión, se ha agregado una nueva configuración de restricción de dispositivos que permite especificar las listas de aplicaciones siguientes:

- Aplicaciones que los usuarios pueden instalar
- Aplicaciones que los usuarios no pueden ejecutar
- Aplicaciones ocultas para el usuario en el dispositivo

Puede especificar la aplicación por dirección URL, nombre del paquete o desde la lista de aplicaciones que administra.

Nuevo vínculo de interfaz de usuario de la directiva de acceso condicional basado en la aplicación de Azure AD desde Intune

Ahora los administradores de TI pueden establecer directivas condicionales basadas en aplicaciones mediante la nueva interfaz de usuario de directivas de acceso condicional en la carga de trabajo de Azure AD. El acceso condicional basado en la aplicación de la sección de Intune App Protection en Azure Portal por el momento no se moverá y se aplicará en paralelo. También encontrará un práctico vínculo a la interfaz de usuario de la nueva directiva de acceso condicional en la carga de trabajo de Intune.

- Obtenga más información sobre el acceso condicional basado en la aplicación en Azure AD.

Julio de 2017

Restricción de la inscripción de dispositivos Android e iOS por versión del SO

Intune ya permite restringir la inscripción de Android e iOS por número de versión del sistema operativo. En **Restricción de tipo de dispositivo**, los administradores de TI ahora pueden establecer una configuración de plataforma para restringir la inscripción entre un valor del sistema operativo mínimo y máximo. Las versiones del sistema operativo Android se deben especificar como Principal.Secundaria.Compilación.Revisión, donde Secundaria, Compilación y Revisión son opcionales. Las versiones de iOS deben especificarse como Principal.Secundaria.Compilación, donde Compilación es opcional. Obtenga más información sobre las restricciones de inscripción de dispositivos.

> **NOTE**
> No se restringe la inscripción a través de los programas de inscripción de Apple o Apple Configurator.

Restricción de la inscripción de dispositivos Android, iOS y macOS de propiedad personal

Intune puede restringir la inscripción de dispositivos personales al incluir los números IMEI de los dispositivos corporativos en una lista de permitidos. Intune ha ampliado esta funcionalidad para iOS, Android y macOS con números de serie del dispositivo. Al cargar los números de serie en Intune, puede declarar los dispositivos como de propiedad corporativa. Con las restricciones de inscripción puede bloquear los dispositivos de propiedad personal (BYOD), lo que permitiría la inscripción de dispositivos de propiedad corporativa únicamente. Obtenga más información sobre las restricciones de inscripción de dispositivos.

Para importar números de serie, vaya a **Inscripción de dispositivos** > **Identificadores de dispositivo corporativos** y haga clic en **Agregar**; luego, cargue un archivo .CSV (sin encabezado, dos columnas para el número de serie y detalles como los números IMEI). Para restringir dispositivos de propiedad personal, vaya a **Inscripción de dispositivos** > **Restricciones de inscripción**. En **Restricciones de tipo de dispositivo**, seleccione **Predeterminado** y luego **Configuraciones de plataforma**. Puede **Permitir** o **Bloquear** dispositivos de propiedad personal iOS, Android y macOS.

Nueva acción de dispositivo para forzar la sincronización de los dispositivos con Intune

En esta versión, se ha agregado una nueva acción de dispositivo que fuerza al dispositivo seleccionado a registrarse inmediatamente en Intune. Cuando un dispositivo se registra, recibe de inmediato las acciones o las directivas pendientes que se le han asignado. Esta acción puede ayudarle a validar y a solucionar problemas de directivas que se le hayan asignado inmediatamente, sin tener que esperar al siguiente registro programado. Para obtener detalles, vea Synchronize device (Sincronizar dispositivos).

Forzar a los dispositivos iOS supervisados a instalar automáticamente la última actualización de software disponible

En el área de trabajo Actualizaciones de software hay disponible una nueva directiva que permite forzar a los dispositivos iOS supervisados a instalar automáticamente la última actualización de software disponible. Para obtener información detallada, consulte Configure iOS update policies (Configuración de directivas de actualización de iOS).

SandBlast Mobile de Check Point: nuevo socio de defensa contra amenazas móviles

Puede controlar el acceso desde dispositivos móviles a recursos corporativos mediante el acceso condicional basado en la evaluación de riesgos efectuada por SandBlast Mobile de Check Point, una solución de defensa contra amenazas móviles integrada en Microsoft Intune.

Funcionamiento de la integración con Intune

El riesgo se evalúa según la telemetría recopilada de dispositivos que ejecutan SandBlast Mobile de Check Point. Puede configurar directivas de acceso condicional de EMS basadas en la evaluación de riesgos de SandBlast Mobile de Check Point habilitada mediante las directivas de cumplimiento de los dispositivos de Intune. Puede permitir o bloquear el acceso de dispositivos no compatibles a recursos corporativos en función de las amenazas detectadas.

Implementación de una aplicación como disponible en Microsoft Store para Empresas

Con esta versión, ahora los administradores pueden asignar la Tienda Microsoft para Empresas como disponible. Cuando se establece como disponible, los usuarios finales pueden instalar la aplicación desde la aplicación de Portal de empresa o un sitio web sin que se les redirija a Microsoft Store.

Actualizaciones de la interfaz de usuario en el sitio web del Portal de empresa

Hemos realizado varias actualizaciones en la interfaz de usuario del sitio web del portal de empresa para mejorar la experiencia del usuario final.

- **Mejoras en los iconos de aplicación**: los iconos de aplicación ahora se muestran con un fondo generado automáticamente según el color dominante del icono (si se puede detectar). Si procede, este fondo reemplaza el borde gris que antes era visible en los iconos de aplicación.

  En una próxima versión, el sitio web del Portal de empresa mostrará iconos grandes siempre que sea posible. Recomendamos que los administradores de TI publiquen aplicaciones con iconos de alta resolución, con un tamaño mínimo de 120 x 120 píxeles.

- **Cambios de navegación**: los elementos de barra de navegación se han movido al menú lateral de la parte superior izquierda. Se ha quitado la página Categorías. Los usuarios ahora pueden filtrar el contenido por categoría durante la exploración.

- **Actualizaciones de aplicaciones destacadas**: Hemos agregado una página dedicada al sitio donde los usuarios pueden buscar aplicaciones que ha decidido presentar, y hemos realizado algunos ajustes a la interfaz de usuario de la sección Destacado en la página principal.

Compatibilidad de iBooks con el sitio web del Portal de empresa

Hemos agregado una página dedicada al sitio web del Portal de empresa que permite a los usuarios buscar y descargar iBooks.

Detalles adicionales para la solución de problemas del departamento de soporte técnico

Intune ha actualizado la visualización de información para la solución de problemas, y la ha agregado a la información que se proporciona a los administradores y al personal del departamento de soporte técnico. Ahora puede consultar la tabla **Asignaciones**, en la que se resumen todas las asignaciones para el usuario en función de la pertenencia al grupo. La lista incluye lo siguiente:

- Aplicaciones móviles
- Directivas de cumplimiento
- Perfiles de configuración

Además, en la tabla **Dispositivos** se incluyen ahora las columnas **Tipo de combinación de Azure AD** y **Conforme con Azure AD**. Para obtener más información, consulte Help users troubleshoot problems (Ayudar a los usuarios a solucionar problemas).

Almacenamiento de datos de Intune (versión preliminar pública)

El Almacenamiento de datos de Intune muestrea los datos a diario para proporcionar una vista histórica del inquilino. Puede tener acceso a los datos mediante un archivo de Power BI (PBIX), un vínculo de OData que es compatible con muchas herramientas de análisis o al interactuar con la API de REST. Para obtener más información, vea Usar el Almacenamiento de datos de Intune.

Modos claro y oscuro disponibles para la aplicación Portal de empresa para Windows 10

Los usuarios finales podrán personalizar el modo de color de la aplicación Portal de empresa para Windows 10. El usuario puede realizar el cambio en la sección Configuración de la aplicación Portal de empresa. El cambio aparecerá una vez que el usuario haya reiniciado la aplicación. En Windows 10 versión 1607 y posteriores, el valor predeterminado del modo de la aplicación es la configuración del sistema. En Windows 10 versión 1511 y anteriores, el valor predeterminado del modo de la aplicación es el modo claro.

Permitir que los usuarios finales etiqueten su grupo de dispositivos en la aplicación Portal de empresa para Windows 10

Los usuarios finales ahora pueden seleccionar el grupo al que pertenece su dispositivo al etiquetarlo directamente desde la aplicación de portal de empresa para Windows 10.

Junio de 2017

Nuevo acceso de administración basada en roles para los administradores de Intune

Se va a agregar un nuevo rol de administrador de acceso condicional para ver, crear, modificar y eliminar directivas de acceso condicional de Azure AD. Anteriormente, solo los administradores globales y de seguridad tenían este permiso. Se puede conceder a los administradores de Intune el permiso de este rol para que tengan acceso a las directivas de acceso condicional.

Etiquetado de los dispositivos corporativos con el número de serie

Intune ahora admite la carga de números de serie de iOS, macOS y Android como identificadores de dispositivos corporativos. No puede usar en este momento números de serie para impedir que los dispositivos personales se inscriban, ya que los números de serie no se comprueban durante la inscripción. Próximamente se podrán bloquear los dispositivos personales por el número de serie.

Nuevas acciones remotas para dispositivos iOS

En esta versión, hemos agregado dos nuevas acciones de dispositivo remoto para los dispositivos iPad compartidos que administran la aplicación Classroom de Apple:

- Cerrar sesión del usuario actual: cierra la sesión del usuario actual del dispositivo iOS que seleccione.
- Quitar usuario: elimina un usuario que seleccione de la memoria caché local en un dispositivo iOS.

Compatibilidad con dispositivos iPad compartidos con la aplicación Aula de iOS

En esta versión, hemos ampliado la compatibilidad con la administración de la aplicación Classroom en iOS, a fin de incluir a los estudiantes que se registran en dispositivos iPad compartidos con sus identificadores de Apple administrados.

Cambios en las aplicaciones integradas de Intune

Anteriormente, Intune tenía numerosas aplicaciones integradas que se podían asignar rápidamente. Basándonos en los comentarios de los usuarios, hemos quitado esta lista y ya no se verán las aplicaciones integradas. Sin embargo, si las aplicaciones integradas ya están asignadas, seguirán mostrándose en la lista de aplicaciones. Las aplicaciones podrán seguir asignándose según se necesite. En una versión posterior, vamos a agregar un método sencillo para seleccionar y asignar aplicaciones integradas de Azure Portal.

Instalación más sencilla de las aplicaciones de Microsoft 365

El nuevo tipo de aplicación **Aplicaciones de Microsoft 365 para empresas** facilita la asignación de Aplicaciones de Microsoft 365 para empresas a dispositivos que administre con la versión más reciente de Windows 10. Además, también puede instalar Microsoft Project y Microsoft Visio si dispone de licencias para ellos. Las aplicaciones que quiera se agrupan y aparecen como una única aplicación en la lista de aplicaciones de la consola de Intune. Para obtener más información, consulte el artículo sobre cómo agregar aplicaciones de Microsoft 365 para Windows 10.

Compatibilidad con aplicaciones sin conexión de Microsoft Store para Empresas

Las aplicaciones sin conexión que ha adquirido en la Tienda Microsoft para Empresas ahora se sincronizarán con Azure Portal. Así, puede implementar estas aplicaciones en grupos de usuarios o grupos de dispositivos. Las aplicaciones sin conexión no se instalan desde la Tienda, sino mediante Intune.

Microsoft Teams ahora forma parte de la lista de CA basada en aplicación de aplicaciones aprobadas.

La aplicación Microsoft Teams para iOS y Android ahora forma parte de las aplicaciones aprobadas para las directivas de acceso condicional basado en la aplicación en Exchange y SharePoint Online. La aplicación puede configurarse para todos los inquilinos mediante la hoja Intune App Protection de Azure Portal en estos momentos mediante el acceso condicional basado en la aplicación.

Integración de Proxy de aplicación y Managed Browser

Intune Managed Browser ahora puede integrarse con el servicio de Azure AD Application Proxy para permitir que los usuarios tengan acceso a los sitios web internos incluso cuando están trabajando en remoto. Los usuarios del explorador simplemente especifican la URL del sitio como lo harían normalmente y Managed Browser enruta la solicitud mediante la puerta de enlace web de Application Proxy. Para obtener más información, vea Administrar el acceso a Internet mediante directivas de Managed Browser.

Nuevas opciones de configuración de aplicaciones para Intune Managed Browser

En esta versión, hemos agregado más configuraciones para la aplicación Intune Managed Browser para iOS y Android. Ahora puede usar una directiva de configuración de aplicaciones para configurar la página principal predeterminada y los marcadores para el explorador. Para obtener más información, vea Administrar el acceso a Internet mediante directivas de Managed Browser.

Configuración de BitLocker para Windows 10

Ahora puede configurar las opciones de BitLocker para dispositivos Windows 10 con un nuevo perfil de dispositivo de Intune. Por ejemplo, puede que necesite que los dispositivos estén cifrados, y también configurar más opciones que se apliquen cuando BitLocker esté activado. Para obtener más información, vea Endpoint protection settings for Windows 10 and later (Configuración de Endpoint Protection para Windows 10 y versiones posteriores).

Nueva configuración del perfil de restricción de dispositivos Windows 10

En esta versión, hemos agregado nuevas opciones para el perfil de restricción de dispositivos Windows 10, en las categorías siguientes:

- Windows Defender
- Red de telefonía móvil y conectividad
- Experiencia de pantalla bloqueada
- Privacidad
- Búsqueda
- Contenido destacado de Windows
- Explorador Microsoft Edge

Para obtener más información sobre la configuración de Windows 10, vea Configuración de restricciones de dispositivos Windows 10 y versiones posteriores.

La aplicación Portal de empresa para Android ahora tiene una nueva experiencia de usuario final para las directivas App Protection

Basándonos en los comentarios de los clientes, hemos modificado la aplicación del portal de empresa para

Android para mostrar un botón **Acceso al contenido de la empresa**. El objetivo es impedir que los usuarios finales pasen innecesariamente por el proceso de inscripción cuando solo necesitan tener acceso a las aplicaciones que admiten directivas de protección de aplicaciones, una característica de administración de aplicaciones móviles de Intune. Puede ver estos cambios en la página Novedades en la interfaz de usuario de la aplicación.

Nueva acción de menú para quitar fácilmente Portal de empresa

Según los comentarios de los usuarios, se agregó una nueva acción de menú en la aplicación Portal de empresa de Intune para Android con el fin de iniciar su eliminación del dispositivo. Con esta acción se quita el dispositivo de administración de Intune para que la aplicación se pueda quitar del dispositivo por parte del usuario. Puede ver estos cambios en la página de novedades en la UI de la aplicación y en la documentación para el usuario final de Android.

Mejoras en la sincronización de aplicaciones con Windows 10 Creators Update

La aplicación Portal de empresa de Intune para Windows 10 ahora iniciará automáticamente una sincronización de las solicitudes de instalación de aplicaciones para dispositivos con Windows 10 Creators Update (versión 1709). De esta forma, se reducirá el problema de estancamiento de las instalaciones de aplicaciones durante el estado "Pending Sync" (Sincronización pendiente). Además, los usuarios podrán iniciar manualmente la sincronización desde dentro de la aplicación. Puede ver estos cambios en la página Novedades en la interfaz de usuario de la aplicación.

Nueva experiencia guiada del Portal de empresa de Windows 10

La aplicación del Portal de empresa para Windows 10 incluirá la experiencia de un tutorial de Intune guiado para dispositivos que no se han identificado ni inscrito. La nueva experiencia proporciona instrucciones paso a paso que llevan al usuario por el registro en Azure Active Directory (que es necesario para las características de acceso condicional) y la inscripción en MDM (que es necesaria para las características de administración de dispositivos). La experiencia guiada será accesible desde la página principal del Portal de empresa. Los usuarios pueden seguir utilizando la aplicación si no completan el registro y la inscripción, pero experimentarán una funcionalidad limitada.

Esta actualización solo es visible en dispositivos que ejecuten la Actualización de aniversario de Windows 10 (compilación 1607) o superior. Puede ver estos cambios en la página Novedades en la interfaz de usuario de la aplicación.

Las consolas de administración de Microsoft Intune y Acceso condicional están disponibles con carácter general

Se anuncia la disponibilidad general de la nueva consola de administración tanto de Intune en Azure Portal como de Acceso condicional. A través de Intune en Azure Portal, ahora puede administrar todas las funcionalidades MAM y MDM de Intune en una experiencia de administración consolidada y aprovechar la agrupación y la selección de destino de Azure AD. Acceso condicional de Azure reúne las amplias funcionalidades de Azure AD e Intune en una consola unificada. Y, desde una experiencia administrativa, migrar a la plataforma Azure permite usar exploradores modernos.

Intune ya está visible sin la etiqueta de **versión preliminar** en Azure portal en portal.azure.com.

No es necesario que los clientes existentes tomen ninguna medida en este momento, a menos que se haya recibido un mensaje de una serie de estos en el centro de mensajes en el que se le solicite llevar a cabo una acción para que sea posible migrar sus grupos. Es posible que también haya recibido una notificación del centro de mensajes en el que se le informe que la migración está tardando más de lo debido producto de errores en nuestro lado. Seguimos trabajando con diligencia para migrar cualquier cliente afectado.

Mejoras de los iconos de aplicación en la aplicación Portal de empresa de Intune para iOS

Se ha actualizado el diseño de los iconos de aplicación en la página principal para reflejar el color de personalización de marca que establezca para el Portal de empresa. Para más información, consulte las novedades en la UI de la aplicación.

Ahora el selector de cuenta está disponible en la aplicación Portal de empresa de Intune para iOS

Los usuarios de dispositivos iOS pueden ver el nuevo selector de cuenta cuando inician sesión en Portal de

empresa de Intune si usan su cuenta profesional o educativa para iniciar sesión en otras aplicaciones de Microsoft. Para más información, consulte las novedades en la UI de la aplicación.

Mayo de 2017

Cambio de la entidad de MDM sin anular la inscripción de dispositivos administrados

Ahora puede cambiar la entidad de MDM sin tener que ponerse en contacto con el Soporte técnico de Microsoft y sin necesidad de anular la inscripción ni de volver a inscribir los dispositivos administrados existentes. En la consola de Configuration Manager, puede cambiar la entidad de MDM de Configurar como Configuration Manager (híbrido) a Microsoft Intune (independiente), o viceversa.

Notificación mejorada para PIN de inicio en Samsung Knox

Si los usuarios finales necesitan establecer un PIN de inicio en dispositivos Samsung Knox a efectos de compatibilidad con el cifrado, cuando dichos usuarios pulsen en la notificación que aparece, se les remitirá al lugar exacto de la aplicación de configuración. Anteriormente, la notificación remitía al usuario final a la pantalla de cambio de contraseña.

Compatibilidad de Apple School Manager (ASM) con iPad compartido

Intune ahora admite el uso de Apple School Manager (ASM) en lugar del Programa de inscripción de dispositivos de Apple para permitir la inscripción inmediata de dispositivos iOS. Es necesario incorporar ASM para usar la aplicación Classroom para Shared iPads, así como habilitar la sincronización de datos de ASM en Azure Active Directory mediante Microsoft School Data Sync (SDS). Para más información, consulte el artículo sobre la habilitación de la inscripción de dispositivos iOS con Apple School Manager.

> **NOTE**
> Configurar iPad compartidos para que funcionen con la aplicación Classroom requiere configuraciones de dispositivos iOS para Education en Azure que todavía no están disponibles. Esta funcionalidad se agregará pronto.

Asistencia remota para dispositivos Android con TeamViewer

Intune ahora puede usar el software TeamViewer, que se compra de forma independiente, para permitirle ofrecer asistencia remota a los usuarios que ejecutan dispositivos Android. Para más información, consulte Asistencia remota para dispositivos Android administrados con Intune.

Nuevas condiciones de las directivas de protección de aplicaciones para MAM

Ahora puede establecer un requisito para MAM sin inscripción de usuarios que exige las siguientes directivas:

- Versión mínima de la aplicación
- Versión mínima del sistema operativo
- Versión mínima del SDK para aplicaciones de Intune de la aplicación de destino (solo iOS)

Esta característica está disponible en iOS y Android. Intune admite el cumplimiento del requisito de versiones mínimas de la plataforma de SO, las aplicaciones y el SDK para aplicaciones de Intune. En iOS, las aplicaciones que tienen el SDK integrado también pueden establecer el cumplimiento de una versión mínima a nivel del SDK. El usuario no podrá acceder a la aplicación de destino si no se cumplen los requisitos mínimos a través de la directiva de protección de aplicaciones a los tres niveles distintos mencionados anteriormente. En este punto, el usuario puede quitar la cuenta (en aplicaciones con varias identidades), cerrar la aplicación o actualizar la versión del SO o de la aplicación.

También puede configurar valores adicionales para proporcionar una notificación sin bloqueo que recomienda una actualización del SO o de la aplicación. Puede cerrar esta notificación, y la aplicación puede usarse de la forma habitual.

Para más información, consulte Configuración de directivas de protección de aplicaciones de iOS y Configuración de directivas de protección de aplicaciones de Android.

Configuración de aplicaciones para Android for Work

Algunas aplicaciones Android de la tienda admiten opciones de configuración administradas que permiten que un administrador de TI controle cómo se ejecuta la aplicación en el perfil de trabajo. Con Intune, ahora puede ver las configuraciones que son compatibles con una aplicación y configurarlas desde Azure Portal con un diseñador de configuración o un editor de JSON. Para más información, consulte el artículo sobre el uso de configuraciones de aplicación para Android for Work.

Nueva funcionalidad de configuración de aplicaciones para MAM sin inscripción

Ahora puede crear directivas de configuración de aplicación a través de MAM sin canal de inscripción. Esta característica es equivalente a las directivas de configuración de aplicación disponibles en la configuración de aplicación de administración de dispositivos móviles (MDM). Si desea un ejemplo de configuración de aplicación con MAM sin inscripción, consulte Administrar el acceso a Internet mediante directivas de Managed Browser con Microsoft Intune.

Configuración de las listas de direcciones URL permitidas y bloqueadas para Managed Browser

Ahora puede configurar una lista de direcciones URL y dominios permitidos y bloqueados para Intune Manager Browser con los valores de configuración de aplicación en Azure Portal. Estos valores se pueden configurar independientemente de si se usa en un dispositivo administrado o no administrado. Para más información, consulte Administrar el acceso a Internet mediante directivas de Managed Browser con Microsoft Intune.

Vista de departamento de soporte técnico de directiva de protección de aplicaciones

Los usuarios del departamento de soporte técnico de TI ahora pueden comprobar el estado de la licencia de usuario y el estado de las aplicaciones de directiva de protección de aplicaciones asignadas a los usuarios en la hoja Solución de problemas. Para información detallada, consulte Solución de problemas.

Control de las visitas a sitios web en dispositivos iOS

Ahora puede controlar qué sitios web pueden visitar los usuarios de dispositivos iOS mediante uno de los dos métodos siguientes:

- Agregar direcciones URL permitidas y bloqueadas mediante el filtro de contenido web integrado de Apple.
- Permitir que el explorador Safari acceda solo a sitios web especificados. Se crean marcadores en Safari para cada sitio que especifique.

Para más información, consulte Configuración de filtro de contenido web para dispositivos iOS.

Configuración previa de permisos de dispositivo para aplicaciones de Android for Work

En el caso de las aplicaciones implementadas en perfiles de trabajo de dispositivos Android for Work, ahora puede configurar el estado de los permisos en cada aplicación. De forma predeterminada, las aplicaciones de Android que requieren permisos de dispositivo como el acceso a la ubicación o la cámara del dispositivo solicitarán a los usuarios que acepten o denieguen permisos. Por ejemplo, si una aplicación usa el micrófono del dispositivo, se solicita al usuario final que conceda a la aplicación el permiso para usar el micrófono. Esta característica le permite definir permisos en nombre del usuario final. Ahora puede configurar permisos para a) denegar automáticamente sin notificar al usuario, b) aprobar automáticamente sin notificar al usuario, o c) pedirle al usuario que acepte o deniegue los permisos. Para más información, consulte Configuración de restricciones de dispositivos Android for Work en Microsoft Intune.

Establecimiento de un PIN específico de la aplicación para dispositivos Android for Work

Los dispositivos Android 7.0 y versiones posteriores con un perfil de trabajo administrado como un dispositivo Android for Work permiten que el administrador defina una directiva de código de acceso que solo se aplique a aplicaciones del perfil de trabajo. Las opciones son:

- Definir una contraseña de código de acceso a nivel de dispositivo: se trata del código de acceso que el usuario debe usar para desbloquear todo el dispositivo.
- Definir una directiva de código de acceso solo a nivel de perfil de trabajo: a los usuarios se les pedirá que escriban un código de acceso cada vez que se abra cualquier aplicación del perfil de trabajo.
- Definir una directiva para el dispositivo y el perfil de trabajo: el administrador de TI tiene la opción de definir

una directiva de código de acceso para el dispositivo y otra para el perfil de trabajo con diferentes intensidades (por ejemplo, un PIN de cuatro dígitos para desbloquear el dispositivo y uno de seis para abrir cualquier aplicación de trabajo).

Para más información, consulte Configuración de restricciones de dispositivos Android for Work en Microsoft Intune.

> **NOTE**
> Esta opción solo está disponible en Android 7.0 y versiones posteriores. De forma predeterminada, el usuario final puede usar los dos PIN definidos por separado o de optar por combinar los dos en el más seguro de ellos.

Nuevas opciones de configuración para dispositivos Windows 10

Agregamos una nueva configuración de restricción de dispositivos Windows que controla características como la proyección inalámbrica, la detección de dispositivos, la conmutación de tareas y los mensajes de error de tarjetas SIM.

Actualizaciones de la configuración de certificados

Cuando crea un perfil de certificado SCEP, en el **formato del nombre del sujeto**, la opción **Personalizar** está disponible para dispositivos iOS, Android y Windows. Antes de esta actualización, el campo **Personalizar** solo estaba disponible para dispositivos iOS. Para obtener más información, vea Creación de un perfil de certificado SCEP.

Cuando crea un perfil de certificado PKCS, en el **nombre alternativo del sujeto**, está disponible la opción **Atributo de Azure AD personalizado**. La opción **Departamento** está disponible cuando se selecciona **Atributo de Azure AD personalizado**. Para obtener más información, vea Creación de un perfil de certificado PKCS.

Configuración de varias aplicaciones que se pueden ejecutar cuando un dispositivo Android está en el modo de pantalla completa

Si un dispositivo Android está en el modo de pantalla completa, anteriormente solo podía configurar una aplicación que se podía ejecutar. Ahora puede configurar varias aplicaciones con el id. de la aplicación, la dirección URL de la tienda o seleccionando una aplicación Android que ya administra. Para más información, consulte Configuración del modo de pantalla completa.

Abril de 2017

Compatibilidad para administrar la aplicación Classroom de Apple

Ahora puede administrar la aplicación Classroom de iOS en dispositivos iPad. Configure la aplicación Classroom en el iPad de los profesores con los datos correctos de la clase y los estudiantes y, a continuación, configure los iPad de los estudiantes registrados en la clase, de modo que pueda controlarlos mediante la aplicación. Para obtener más detalles, vea Configuración de dispositivos iOS para el entorno educativo.

Compatibilidad con las opciones de configuración administradas para aplicaciones Android

Intune ahora puede configurar las aplicaciones Android de Play Store que admiten opciones de configuración administradas. Esta característica permite a TI ver la lista de valores de configuración que admite una aplicación y proporciona una interfaz de usuario guiada y de primera clase que permite configurar esos valores.

Nueva directiva de Android para PIN complejos

Ahora puede establecer un tipo de contraseña obligatoria de complejo numérico en un perfil de dispositivo Android para dispositivos que ejecutan Android 5.0 y versiones posteriores. Utilice esta opción para impedir que los usuarios de dispositivos creen un PIN que contenga números repetidos o consecutivos, como 1111 o 1234.

Soporte adicional para dispositivos Android for Work

- **Administración de la configuración del perfil de trabajo y la contraseña**

  Esta nueva directiva de restricción de dispositivos Android for Work ahora permite administrar la configuración del perfil de trabajo y la contraseña en los dispositivos Android for Work que administre.

- **Permitir uso compartido de datos entre perfiles de trabajo y perfiles personales**

Este perfil de restricción de dispositivos Android for Work ahora tiene opciones nuevas que le ayudarán a configurar el uso compartido de datos entre el perfil profesional y el perfil personal.

- **Restricción de las acciones de copiar y pegar entre perfiles profesionales y personales**

  Un perfil de dispositivo personalizado para dispositivos Android for Work ahora permite restringir si se permiten las acciones de copiar y pegar entre aplicaciones profesionales y personales.

Para más información, consulte Restricciones de dispositivos para Android for Work.

Asignación de aplicaciones de LOB a dispositivos iOS y Android

Ahora puede asignar aplicaciones de línea de negocio para iOS (archivos .ipa) y Android (archivos .apk) a usuarios o dispositivos.

Nuevas directivas de dispositivo para iOS

- **Aplicaciones en la pantalla principal**: controla qué aplicaciones ven los usuarios en la pantalla principal de sus dispositivos iOS. Esta directiva cambia el diseño de la pantalla principal, pero no implementa ninguna aplicación.
- **Conexiones con dispositivos AirPrint**: controla a qué dispositivos AirPrint (impresoras de red) se pueden conectar los usuarios finales de dispositivos iOS.
- **Conexiones con dispositivos AirPlay**: controla a qué dispositivos AirPlay (como Apple TV) se pueden conectar los usuarios finales de dispositivos iOS.
- **Mensaje personalizado de la pantalla de bloqueo**: configurar un mensaje personalizado que verán los usuarios en la pantalla de bloqueo de sus dispositivos iOS y que reemplaza al mensaje predeterminado de esa pantalla. Para más información, consulte Activación del modo perdido en dispositivos iOS

Restricción de las notificaciones de inserción para aplicaciones iOS

En un perfil de restricción de dispositivos de Intune, ahora puede configurar los siguientes ajustes de notificación para dispositivos iOS:

- Activar o desactivar totalmente la notificación para una aplicación especificada.
- Activar o desactivar la notificación en el centro de notificaciones para una aplicación especificada.
- Especificar el tipo de alerta como **None** (Ninguna), **Banner** (Mensaje emergente) o **Modal Alert** (Alerta modal).
- Especificar si se permiten los distintivos para esta aplicación.
- Especificar si se permiten los sonidos de notificaciones.

Configuración de aplicaciones iOS para que se ejecuten en el modo de aplicación única de forma autónoma

Puede usar un perfil de dispositivo de Intune para configurar dispositivos iOS de modo que ejecuten aplicaciones especificadas en modo de aplicación única autónoma. Cuando se configura este modo y se ejecuta la aplicación, el dispositivo se bloquea para que solo pueda ejecutar esa aplicación. Un ejemplo es cuando se configura una aplicación que permite a los usuarios hacer un examen en el dispositivo. Cuando se completan las acciones de la aplicación, o quita esta directiva, el dispositivo vuelve a su estado normal.

Configuración de dominios de confianza para el correo electrónico y la exploración web en dispositivos iOS

Desde un perfil de restricción de dispositivos iOS, ahora puede configurar los valores de dominio siguientes:

- **Dominios de correo electrónico sin marcar**: los correos electrónicos que el usuario envía o recibe y no coinciden con los dominios que especifique aquí se marcarán como que no son de confianza.
- **Dominios web administrados**: los documentos que se descargan de las direcciones URL que especifique aquí se considerarán administrados (solo en Safari).

- **Dominios de relleno automático de contraseña de Safari**: los usuarios pueden guardar en Safari las contraseñas solo de las direcciones URL que coincidan con los patrones que especifique aquí. Para usar esta opción, el dispositivo debe estar en modo supervisado y no estar configurado para varios usuarios. (iOS 9.3 y versiones posteriores)

Aplicaciones de PCV disponibles en el Portal de empresa de iOS

Ahora puede asignar aplicaciones de compras por volumen (PCV) de iOS como instalaciones **Disponibles** para usuarios finales. Los usuarios finales necesitarán una cuenta de Apple Store para instalar la aplicación.

Sincronización de libros electrónicos de la tienda de compras por volumen de Apple

Ahora puede sincronizar los libros que haya adquirido a través de la tienda del Programa de Compras por Volumen de Apple con Intune y asignarlos a los usuarios.

Administración de varios usuarios para dispositivos Samsung Knox Standard

Intune es compatible ahora con dispositivos que ejecutan Samsung Knox Standard para la administración de varios usuarios. Esto significa que los usuarios finales pueden iniciar y cerrar sesión en el dispositivo con sus credenciales de Azure Active Directory, y que el dispositivo se administra centralmente tanto si está en uso como si no. Cuando los usuarios finales inician sesión, tienen acceso a las aplicaciones y se les aplican las directivas. Cuando los usuarios cierran sesión, se borran todos los datos de la aplicación.

Configuración adicional de restricción de dispositivos Windows

Hemos agregado compatibilidad con opciones de configuración adicionales de restricción de dispositivos Windows, como la compatibilidad adicional con el explorador Microsoft Edge, la personalización de la pantalla de bloqueo del dispositivo, las personalizaciones del menú Inicio, el papel tapiz del conjunto de búsqueda de Contenido destacado de Windows y la configuración de proxy.

Compatibilidad con varios usuarios para Windows 10 Creators Update

Hemos agregado compatibilidad para la administración de varios usuarios en dispositivos que ejecutan Windows 10 Creators Update y están unidos al dominio de Azure Active Directory. Esto significa que cuando varios usuarios estándar inicien sesión en el dispositivo con sus credenciales de Azure AD, recibirán las aplicaciones y las directivas que se hayan asignado a sus nombres de usuario. Actualmente, los usuarios no puede usar Portal de empresa para escenarios de autoservicio, como la instalación de aplicaciones.

Fresh Start para equipos con Windows 10

Ahora hay disponible una nueva acción de dispositivo Fresh Start para equipos Windows 10. Cuando se lleva a cabo esta acción, se quitan las aplicaciones que hubiera instaladas en el equipo y este se actualiza automáticamente a la versión más reciente de Windows. Esto puede servir para ayudar a quitar las aplicaciones de OEM preinstaladas que a menudo se entregan con los nuevos PC. Puede configurar si se conservan los datos de usuario cuando se lleva a cabo esta acción de dispositivo.

Rutas de actualización adicionales de Windows 10

Ahora puede crear una directiva de actualización de edición para actualizar los dispositivos a las siguientes ediciones adicionales de Windows 10:

- Windows 10 Professional
- Windows 10 Professional N
- Windows 10 Professional Education
- Windows 10 Professional Education N

Inscripción masiva de dispositivos Windows 10

Ahora puede unir grandes cantidades de dispositivos que ejecutan Windows 10 Creator Update a Azure Active Directory e Intune con Windows Configuration Designer (WCD). Para habilitar la inscripción masiva de MDM para el inquilino de Azure AD, cree un paquete de aprovisionamiento que una dispositivos al inquilino de Azure AD a través de Windows Configuration Designer y aplique el paquete a los dispositivos corporativos que desea inscribir y administrar de forma masiva. Una vez que el paquete se aplica a los dispositivos, se unirán a Azure AD, se inscribirán en Intune y estarán listos para que los usuarios de Azure AD inicien sesión. Los usuarios de

Azure AD son usuarios estándar en estos dispositivos y reciben las aplicaciones requeridas y las directivas asignadas. En este momento, no se admiten los escenarios de autoservicio ni de portal de empresa.

Nueva configuración de MAM para PIN y ubicaciones de almacenamiento administrado

Ahora hay disponibles dos nuevas opciones de configuración de aplicaciones que le ayudarán con los escenarios de administración de aplicaciones móviles (MAM):

- **Disable app PIN when device PIN is managed (Deshabilitar el PIN de aplicación cuando se administra el PIN del dispositivo)** : detecta si hay un PIN de dispositivo en el dispositivo inscrito y, si es así, omite el PIN de aplicación desencadenado por las directivas de protección de aplicaciones. Esta configuración permitirá reducir el número de veces que se muestra una solicitud de PIN a los usuarios que abran una aplicación habilitada para MAM en un dispositivo inscrito. Esta característica está disponible para iOS y Android.
- **Seleccione en qué servicios de almacenamiento se puede guardar datos empresariales**: permite especificar en qué ubicaciones de almacenamiento quiere guardar los datos corporativos. Los usuarios pueden guardar en los servicios de ubicación de almacenamiento seleccionados, lo que implica que se bloquearán todos los demás servicios de ubicación de almacenamiento no indicados.

  Lista de servicios de ubicación de almacenamiento compatibles:

  - OneDrive
  - OneDrive para la Empresa/SharePoint Online
  - Almacenamiento local

Portal de solución de problemas del departamento de soporte técnico

El nuevo portal de solución de problemas permite que los operadores del departamento de soporte técnico y los administradores de Intune vean a los usuarios y sus dispositivos y, además, realicen tareas para solucionar problemas técnicos de Intune.

Marzo de 2017

Compatibilidad con Modo Perdido de iOS

En iOS 9.3 y dispositivos posteriores, Intune agrega compatibilidad con **Modo Perdido**. Ahora puede bloquear un dispositivo para evitar su uso, así como mostrar un mensaje y llamar al número de teléfono de la pantalla de bloqueo del dispositivo.

El usuario final no podrá desbloquear el dispositivo hasta que un administrador deshabilite Modo Perdido. Cuando está activado el Modo Perdido, puede usar la acción **Buscar dispositivo** para ver la ubicación geográfica del dispositivo en un mapa en la consola de Intune.

El dispositivo debe ser un dispositivo iOS de la empresa, inscrito mediante DEP, que esté en modo supervisado.

Para obtener más información, consulte ¿Qué es la administración de dispositivos de Microsoft Intune?

Mejoras en los informes de las acciones del dispositivo

Hemos realizado mejoras en el informe de las acciones del dispositivo para mejorar el rendimiento. Además, ahora puede filtrar el informe por estado. Por ejemplo, puede filtrar el informe para mostrar únicamente las acciones de dispositivo que se han completado."

Categorías de aplicaciones personalizadas

Ahora puede crear, editar y asignar categorías a las aplicaciones que agregue a Intune. En estos momentos, las categorías solo pueden especificarse en inglés. Consulte How to add an app to Intune (Cómo agregar una aplicación a Intune).

Asignación de aplicaciones de LOB a usuarios con dispositivos no inscritos

Ahora puede asignar aplicaciones de línea de negocio desde la tienda a usuarios tengan o no inscritos sus dispositivos con Intune. Si el dispositivo de los usuarios no está inscrito con Intune, deben ir al sitio web del Portal de empresa para instalarlo, en lugar de a la aplicación del Portal de empresa.

Nuevos informes de cumplimiento

Ahora dispone de informes de cumplimiento que proporcionan la posición de cumplimiento de los dispositivos de su empresa y le permiten solucionar rápidamente los problemas relacionados con el cumplimiento detectados por los usuarios. Puede ver información acerca de

- Estado de cumplimiento general de los dispositivos
- Estado de cumplimiento de una configuración individual
- Estado de cumplimiento de una directiva individual

También puede usar estos informes para profundizar en un dispositivo individual para ver la configuración específica y las directivas que afectan a dicho dispositivo.

Acceso directo a los escenarios de inscripción de Apple

Para las cuentas de Intune creadas después de enero de 2017, Intune habilitó el acceso directo a los escenarios de inscripción de Apple mediante la carga de trabajo de inscripción de dispositivos en Azure Portal. Anteriormente, la vista preliminar de inscripción de Apple solo era accesible desde los vínculos de Azure Portal. Las cuentas de Intune creadas antes de enero de 2017 requerirán una migración única antes de que estas características estén disponibles en Azure. Aún no se ha anunciado la programación para la migración, pero pronto habrá detalles disponibles. Se recomienda encarecidamente crear una cuenta de prueba para probar la nueva experiencia si su cuenta no tiene acceso a la versión preliminar.

Febrero de 2017

Capacidad para restringir la inscripción de dispositivos móviles

Intune está agregando nuevas restricciones de inscripción que controlan qué plataformas de dispositivos móviles pueden inscribir. Intune separa las plataformas de dispositivos móviles como iOS, Mac OS, Android, Windows y Windows Mobile.

- La restricción la inscripción de dispositivos móviles no restringe la inscripción del cliente de PC.
- Solo para iOS y Android, hay una opción adicional para bloquear la inscripción de dispositivos de propiedad personal.

Intune marca todos los dispositivos nuevos como personal a menos que el administrador de TI tome la medida de marcarlos como propiedad de la empresa, como se explica en este artículo.

Visualización de todas las acciones en los dispositivos administrados

Un nuevo informe **Acciones de dispositivo** muestra quién ha realizado acciones remotas como el restablecimiento de fábrica en dispositivos y, además, muestra el estado de esa acción. Vea ¿Qué es la administración de dispositivos?.

Los dispositivos no administrados pueden acceder a aplicaciones asignadas

Como parte de los cambios de diseño en el sitio web del portal de empresa, los usuarios de iOS y Android podrán instalar aplicaciones asignadas a ellos como "disponibles sin inscripción" en sus dispositivos no administrados. Con sus credenciales de Intune, los usuarios podrán iniciar sesión en el sitio web del portal de empresa y ver la lista de aplicaciones asignadas. Los paquetes de aplicación de las aplicaciones "disponibles sin inscripción" se encuentran disponibles para descargar a través del sitio web del portal de empresa. Las aplicaciones que requieren la inscripción para la instalación no se ven afectadas por este cambio, ya que se les pedirá a los usuarios que inscriban su dispositivo si quieren instalar esas aplicaciones.

Categorías de aplicaciones personalizadas

Ahora puede crear, editar y asignar categorías a las aplicaciones que agregue a Intune. En estos momentos, las categorías solo pueden especificarse en inglés. Consulte How to add an app to Intune (Cómo agregar una aplicación a Intune).

Representación de categorías de dispositivos

Ahora puede ver la categoría del dispositivo como una columna en la lista de dispositivos. También puede editar la categoría desde la sección de propiedades de la hoja de propiedades del dispositivo. Consulte How to add an

app to Intune (Cómo agregar una aplicación a Intune).

Configuración de Windows Update para empresas

Windows como servicio es la nueva forma de proporcionar actualizaciones para Windows 10. A partir de Windows 10, todas las nuevas actualizaciones de calidad y características contienen las actualizaciones anteriores. Es decir, siempre que haya instalado la más reciente, sabrá que sus dispositivos Windows 10 están completamente actualizados. A diferencia de las versiones anteriores de Windows, ahora debe instalar la actualización completa en lugar de una parte.

Gracias a Windows Update para empresas, puede simplificar la administración de actualizaciones, ya que no tendrá que aprobar actualizaciones individuales para grupos de dispositivos. Todavía puede administrar los riesgos en sus entornos configurando una estrategia de implementación de actualizaciones; Windows Update se asegurará de que las actualizaciones se instalen en el momento oportuno. Microsoft Intune ofrece la posibilidad de configurar las actualizaciones en los dispositivos y de aplazar su instalación. Intune no almacena las actualizaciones, sino únicamente la asignación de las directivas de actualización. Los dispositivos acceden a Windows Update directamente para instalar las actualizaciones. Use Intune para configurar y administrar los **anillos de actualización de Windows 10**. Un anillo de actualización contiene un grupo de opciones que configuran cuándo y cómo se instalan las actualizaciones de Windows 10. Para obtener más información, consulte Configuración de Windows Update para empresas.

Novedades del portal clásico de Intune: meses anteriores

14/05/2021 • 29 minutes to read

Se aplica a: Intune en el portal clásico

> **IMPORTANT**
> La administración de equipos heredados ya no se admite a partir del 16 de octubre de 2020. Actualice los dispositivos a Windows 10 y vuelva a inscribirlos como dispositivos MDM de Intune para administrarlos mediante Intune. Los equipos administrados con el cliente de software de PC dejarán de recibir aplicaciones y actualizaciones de seguridad y ya no podrá configurarlas.
>
> Más información

En esta página aparecen las nuevas características y las notificaciones anunciadas anteriormente en la página de novedades del portal clásico de Intune.

Abril de 2017

Nuevas funcionalidades

MyApps disponible para Managed Browser

Microsoft MyApps tiene ahora mejor compatibilidad con Managed Browser. A los usuarios de Managed Browser que no estén destinados a la administración se les llevará directamente al servicio MyApps, donde podrán acceder a sus aplicaciones SaaS aprovisionadas por el administrador. Los usuarios que tengan como destino la administración de Intune seguirán teniendo acceso a MyApps desde el marcador integrado de Managed Browser.

Nuevos iconos para Managed Browser y el Portal de empresa

Managed Browser está recibiendo iconos actualizados para las versiones de iOS y Android de la aplicación. El nuevo icono contendrá el distintivo de Intune actualizado para que sea más coherente con otras aplicaciones de Enterprise Mobility + Security (EM+S). Puede ver el nuevo icono de Managed Browser en la página de novedades de la interfaz de usuario de la aplicación de Intune.

El Portal de empresa también está recibiendo iconos actualizados para las versiones de Windows, iOS y Android de la aplicación con el objetivo de mejorar la coherencia con otras aplicaciones de EM+S. Estos iconos se lanzarán gradualmente en las distintas plataformas desde abril hasta finales de mayo.

Indicador de progreso de inicio de sesión en Portal de empresa de Android

Una actualización de la aplicación Portal de empresa de Android muestra un indicador de progreso de inicio de sesión cuando el usuario inicia o reanuda la aplicación. El indicador avanza por los nuevos estados, desde "Conectando..." e "Iniciando sesión..." hasta "Comprobando los requisitos de seguridad...", antes de permitir que el usuario acceda a la aplicación. Puede ver las nuevas pantallas de la aplicación Portal de empresa para Android en la página de novedades de la UI de la aplicación Intune.

Bloqueo del acceso de las aplicaciones a SharePoint Online

Ahora puede crear una directiva de acceso condicional basada en aplicaciones para bloquear el acceso a SharePoint Online a aquellas aplicaciones a las que no se apliquen directivas de protección. En el escenario de acceso condicional basado en aplicaciones, puede especificar las aplicaciones que quiere que tengan acceso a SharePoint Online mediante Azure Portal.

Compatibilidad del inicio de sesión único desde el Portal de empresa para iOS con Outlook para iOS

Los usuarios ya no tienen que iniciar sesión en la aplicación de Outlook si ya lo han hecho en la aplicación Portal de empresa para iOS en el mismo dispositivo con la misma cuenta. Cuando los usuarios inicien la aplicación de Outlook, podrán seleccionar su cuenta e iniciar sesión automáticamente. También estamos trabajando para agregar esta funcionalidad para otras aplicaciones de Microsoft.

Mejora de los mensajes de estado en la aplicación Portal de empresa para iOS

Ahora se mostrarán nuevos mensajes de error más específicos en la aplicación Portal de empresa para iOS con el objetivo de ofrecer información más accesible sobre lo que ocurre en los dispositivos. Estos casos de error anteriormente se incluían en un mensaje de error general titulado "Portal de empresa no disponible temporalmente". Además, si un usuario inicia el Portal de empresa en iOS sin conexión a Internet, ahora aparecerá una barra de estado persistente en la página principal con el mensaje "No hay conexión a Internet".

Mejora del estado de instalación de la aplicación para la aplicación Portal de empresa de Windows 10

A continuación se mencionan las nuevas mejoras para las instalaciones de aplicaciones iniciadas en la aplicación Portal de empresa de Windows 10:

- Informe de progreso de instalación más rápido para paquetes MSI
- Informe de progreso de instalación más rápido para aplicaciones modernas en dispositivos que ejecutan la Actualización de aniversario de Windows 10 o superior
- Nueva barra de progreso para instalaciones de aplicaciones modernas en dispositivos que ejecutan la Actualización de aniversario de Windows 10 o superior

Puede ver la nueva barra de progreso en la página de novedades de la interfaz de usuario de la aplicación de Intune.

Inscripción masiva de dispositivos Windows 10

Ahora puede unir grandes cantidades de dispositivos que ejecutan Windows 10 Creator Update a Azure Active Directory e Intune con Windows Configuration Designer (WCD). Para habilitar la inscripción masiva de MDM para el inquilino de Azure AD, cree un paquete de aprovisionamiento que una dispositivos al inquilino de Azure AD a través de Windows Configuration Designer y aplique el paquete a los dispositivos corporativos que desea inscribir y administrar de forma masiva. Una vez que el paquete se aplica a los dispositivos, se unirán a Azure AD, se inscribirán en Intune y estarán listos para que los usuarios de Azure AD inicien sesión. Los usuarios de Azure AD son usuarios estándar en estos dispositivos y reciben las aplicaciones requeridas y las directivas asignadas. En este momento, no se admiten los escenarios de autoservicio ni de portal de empresa.

Novedades de la versión preliminar pública de Intune en Azure Portal

A principios de 2017 migraremos nuestra experiencia de administración completa a Azure, lo que permitirá una administración eficaz e integrada de los flujos de trabajo principales de EMS en una moderna plataforma de servicios que es extensible mediante las Graph API.

Nuevos inquilinos de prueba comenzarán a ver la versión preliminar pública de la nueva experiencia de administración en el portal de Azure de este mes. Durante el estado de versión preliminar, se proporcionarán funcionalidades y paridad con la consola de Intune existente de manera iterativa.

La experiencia de administración de Azure Portal usará la nueva funcionalidad de agrupación y destino ya anunciadas; cuando el inquilino existente se migra a la nueva experiencia de agrupación, también se migra a la versión preliminar la nueva experiencia de administración en el inquilino. Mientras tanto, si desea probar o consultar cualquiera de las nuevas funcionalidades hasta que se migre el inquilino, regístrese para una nueva cuenta de prueba de Intune o consulte la nueva documentación.

Puede encontrar las novedades en la vista previa de Intune en Azure aquí.

Notificaciones

Acceso directo a los escenarios de inscripción de Apple

Para las cuentas de Intune creadas después de enero de 2017, Intune ha habilitado el acceso directo a los

escenarios de inscripción de Apple mediante la carga de trabajo de inscripción de dispositivos en el portal de vista previa de Azure. Anteriormente, la vista preliminar de inscripción de Apple solo era accesible desde los vínculos de Azure Portal. Las cuentas de Intune creadas antes de enero de 2017 requerirán una migración única antes de que estas características estén disponibles en Azure. Aún no se ha anunciado la programación para la migración, pero pronto habrá detalles disponibles. Se recomienda encarecidamente crear una cuenta de prueba para probar la nueva experiencia si su cuenta no tiene acceso a la versión preliminar.

Novedades para Appx en Intune en Azure Portal

Como parte de la migración a Intune en Azure Portal, estamos realizando tres cambios de appx:

1. Agregar un nuevo tipo de aplicación appx en la consola de Intune que solo se puede implementar en dispositivos inscritos en MDM.
2. Reasignar el tipo de aplicación appx existente para que solo esté dirigido a equipos administrados mediante el agente de PC de Intune.
3. Convertir todos los appxs existentes en appxs de MDM con la migración.

¿Cómo me afecta esto?

Esto no afectará a ninguna de sus implementaciones actuales en dispositivos administrados a través del agente de PC de Intune. No obstante, tras la migración, no podrá implementar esos appxs migrados en ningún dispositivo nuevo administrado mediante el agente de PC de Intune que no estuviera seleccionado anteriormente.

Acciones necesarias

Tras la migración, deberá volver a cargar el appx de nuevo como un appx de PC si quiere realizar nuevas implementaciones de PC. Para obtener más información, consulte Appx changes in Intune in the Azure portal (Cambios de appx en Intune en Azure Portal) en el blog del equipo de soporte técnico de Intune.

Roles de administración que se reemplazan en el Portal de Azure

Los roles de administración de aplicaciones móviles (MAM) existentes (colaborador, propietario y de solo lectura) usados en el portal clásico de Intune (Silverlight) se reemplazan por un conjunto completo de nuevos controles de administración basada en roles (RBAC) en el Portal de Intune Azure. Cuando haya migrado al Portal de Azure, tendrá que reasignar estos nuevos roles de administración a los administradores. Para más información sobre RBAC y los nuevos roles, consulte Roles de Intune (RBAC) para Microsoft Intune.

Próximas novedades

Mejora de la experiencia de inicio de sesión en todas las aplicaciones del Portal de empresa para todas las plataformas

Estamos anunciando un cambio que aparecerá en los próximos meses que mejorará la experiencia de inicio de sesión para las aplicaciones de Portal de empresa de Intune para Android, iOS y Windows. La nueva experiencia del usuario aparecerá automáticamente en todas las plataformas de la aplicación Portal de empresa cuando Azure AD haga este cambio. Además, los usuarios ahora pueden iniciar sesión en Portal de empresa desde otro dispositivo con un código generado de un solo uso. Esto resulta útil especialmente en casos en los que los usuarios necesitan iniciar sesión sin credenciales.

Puede encontrar capturas de pantalla de la experiencia de inicio de sesión anterior, la nueva experiencia de inicio de sesión con credenciales y la nueva experiencia de inicio de sesión desde otro dispositivo en la página Novedades en la UI de la aplicación.

Plan de cambio: Intune está cambiando la experiencia del portal de partners de Intune.

Estamos quitando la página Partner de Intune de manage.microsoft.com a partir de la actualización de servicio de mediados de mayo de 2017.

Si es un administrador de partners, ya no podrá ver y realizar acciones en nombre de sus clientes desde la página Partner de Intune pero, en su lugar, tendrá que iniciar sesión en uno de los dos portales de partners de Microsoft.

Tanto el Centro de partners de Microsoft como el Centro de administración de Microsoft 365 le permitirán iniciar sesión en las cuentas de cliente que administre. En adelante, como partner, use uno de estos sitios para

administrar a sus clientes.

Apple requerirá actualizaciones para la Seguridad de transporte de aplicaciones

Apple ha anunciado que se aplicarán requisitos específicos para la Seguridad de transporte de aplicaciones (ATS). ATS se utiliza para exigir una seguridad más estricta en todas las comunicaciones de aplicación a través de HTTPS. Este cambio afecta a los clientes de Intune que usan aplicaciones del portal de empresa de iOS.

Hay disponible una versión de la aplicación Portal de empresa para iOS a través del programa Apple TestFlight que aplica los nuevos requisitos de ATS. Si desea probarla para que pueda experimentar el cumplimiento de ATS, envíe un correo electrónico a CompanyPortalBeta@microsoft.com con su nombre, apellidos, dirección de correo electrónico y nombre de la empresa. Revise nuestro blog de soporte técnico de Intune para más detalles.

Marzo de 2017

Nuevas funcionalidades

Compatibilidad con Skycure

Ahora puede controlar el acceso desde dispositivos móviles a recursos corporativos mediante el acceso condicional basado en la evaluación de riesgos efectuada por Skycure, una solución de defensa contra amenazas móviles integrada con Microsoft Intune. El riesgo se evalúa según la telemetría recopilada de dispositivos que ejecutan Skycure, que incluye:

- Defensa física
- Defensa de red
- Defensa de aplicaciones
- Defensa de vulnerabilidades

Puede configurar directivas de acceso condicional de EMS basadas en la evaluación de riesgos de Symantec Endpoint Protection Mobile (Skycure) habilitada mediante las directivas de cumplimiento de dispositivos de Intune. Puede usar estas directivas para permitir o bloquear el acceso de dispositivos no compatibles a recursos corporativos en función de las amenazas detectadas. Para obtener más información, consulte Conector de Symantec Endpoint Protection Mobile.

Nueva experiencia del usuario en la aplicación Portal de empresa para Android

La aplicación de Portal de empresa para Android va a actualizar su interfaz de usuario para un aspecto más moderno y una mejor experiencia de usuario. Las actualizaciones importantes son:

- Colores: los encabezados de la pestaña de Portal de empresa están coloreados según la información de la marca definida por TI.
- Aplicaciones: en la pestaña **Aplicaciones**, los botones **Aplicaciones destacadas** y **Todas las aplicaciones** se han actualizado.
- Búsqueda: en la pestaña **Aplicaciones**, el botón **Buscar** ahora es un botón de acción flotante.
- Aplicaciones de navegación: la vista **Todas las aplicaciones** muestra una vista con las pestañas **Destacadas**, **Todas** y **Categorías** para navegar más fácilmente.
- Soporte: **Mis dispositivos** y **Contactar con TI** se actualizan para mejorar la legibilidad.

Para obtener más información sobre estos cambios, consulte Actualizaciones de la interfaz de usuario para las aplicaciones de usuario final de Intune.

Los dispositivos no administrados pueden acceder a aplicaciones asignadas

Como parte de los cambios de diseño en el sitio web del portal de empresa, los usuarios de iOS y Android podrán instalar aplicaciones asignadas a ellos como "disponibles sin inscripción" en sus dispositivos no administrados. Con sus credenciales de Intune, los usuarios podrán iniciar sesión en el sitio web del portal de empresa y ver la lista de aplicaciones asignadas. Los paquetes de aplicación de las aplicaciones "disponibles sin inscripción" se encuentran disponibles para descargar a través del sitio web del portal de empresa. Las aplicaciones que requieren la inscripción para la instalación no se ven afectadas por este cambio, ya que se les

pedirá a los usuarios que inscriban su dispositivo si quieren instalar esas aplicaciones.

Script de firma para Portal de empresa para Windows 10

Si necesita descargar y transferir localmente la aplicación del Portal de empresa para Windows 10, ahora puede usar un script para simplificar y agilizar el proceso de firma de aplicaciones en su organización. Para descargar el script y las instrucciones de uso, consulte el artículo Microsoft Intune Signing Script for Windows 10 Company Portal (Script de firma de Microsoft Intune para el Portal de empresa para Windows 10) de la Galería de TechNet. Para obtener más información sobre este anuncio, consulte Updating your Windows 10 Company Portal app (Actualización de la aplicación del Portal de empresa para Windows 10) en el blog del equipo de asistencia técnica de Intune.

Notificaciones

Compatibilidad con iOS 10.3

La versión de iOS 10.3 empezó a implementarse el 27 de marzo de 2017 a los usuarios de iOS. Todos los escenarios MDM y MAM existentes de Intune son compatibles con la versión más reciente del sistema operativo de Apple. Se prevé que todas las características existentes de Intune actualmente disponibles para administrar dispositivos iOS seguirán funcionando cuando los usuarios actualicen sus dispositivos a iOS 10.3.

Actualmente no hay ningún problema conocido que compartir. Si tiene algún problema con iOS 10.3, póngase en contacto con el equipo de soporte técnico de Intune.

Compatibilidad mejorada para usuarios de Android radicados en China

Debido a la ausencia de Google Play Store en China, los dispositivos Android deben obtener aplicaciones en los mercados chinos. El Portal de empresa admitirá este flujo de trabajo al redirigir a los usuarios de Android de China para que descarguen las aplicaciones de Portal de empresa y de Outlook desde tiendas de aplicaciones locales. Esto mejorará la experiencia del usuario cuando se habiliten las directivas de acceso condicional, tanto para administración de dispositivos móviles como para la administración de aplicaciones móviles. Las aplicaciones de Portal de empresa y Outlook para Android están disponibles en los siguientes tiendas de aplicaciones chinas:

- Baidu
- Tencent
- Huawei
- Wandoujia

Procedimiento recomendado: asegurarse de que las aplicaciones de Portal de empresa están actualizadas

En diciembre de 2016, se publicó una actualización que permitía aplicar la autenticación multifactor (MFA) en un grupo de usuarios cuando registraban un dispositivo iOS, Android, Windows 8.1 + o Windows Phone 8.1 +. Esta característica no puede funcionar sin determinadas versiones de línea de base de la aplicación del Portal de empresa para iOS (2.1.17 y posteriores) y Android (5.0.3419.0 y posteriores).

Microsoft mejora continuamente Intune agregando nuevas funciones en la consola y las aplicaciones del Portal de empresa en todas las plataformas compatibles. Como resultado, solo lanza correcciones para problemas detectados en la versión actual de la aplicación del Portal de empresa. Por lo tanto, se recomienda utilizar las versiones más recientes de las aplicaciones del Portal de empresa para mejorar la experiencia de usuario.

> **TIP**
> Pida a los usuarios que configuren sus dispositivos para actualizar automáticamente las aplicaciones de la tienda de aplicaciones correspondiente. Si ha publicado la aplicación del Portal de empresa para Android en un recurso compartido de red, puede descargar la versión más reciente desde el Centro de descarga de Microsoft.

Microsoft Teams ahora está habilitado para MAM en iOS y Android

Microsoft ha anunciado la disponibilidad general de Microsoft Teams. Las aplicaciones de Microsoft Teams actualizadas para iOS y Android están habilitadas con las funcionalidades de administración de aplicaciones

móviles (MAM) de Intune, por lo que sus equipos podrán trabajar con libertad en todos los dispositivos. De esta forma, se asegurará de que las conversaciones y datos corporativos estén protegidos en todo momento. Para obtener más información, consulte el anuncio de Microsoft Teams en el blog de seguridad y la movilidad empresarial.

Febrero de 2017

Nuevas funcionalidades

Renovación del sitio web del portal de empresa

El sitio web del portal de empresa admitirá aplicaciones destinadas a aquellos usuarios que no tienen dispositivos administrados. El sitio web se asemejará a otros productos y servicios de Microsoft gracias a una nueva combinación de colores de contraste, ilustraciones dinámicas y un "menú hamburguesa",  .

Notificaciones

La migración de grupo no requiere actualizaciones a grupos ni directivas para dispositivos iOS

Para cada grupo de dispositivos de Intune previamente asignado mediante un perfil de inscripción de dispositivos corporativos, se creará un grupo de dispositivos dinámico correspondiente en Azure AD según el nombre del perfil de inscripción de dispositivos corporativos, durante la migración a grupos de dispositivos de Azure Active Directory. Esto garantizará que, según se inscriban dispositivos, estos se agrupen de manera automática y reciban las mismas directivas y aplicaciones que el grupo de Intune original.

Una vez que un inquilino empieza el proceso de migración para agrupar y seleccionar el destino, Intune creará de forma automática un grupo dinámico de Azure AD que se corresponda con un grupo de Intune de destino mediante un perfil de inscripción de dispositivos corporativos. Si el administrador de Intune elimina el grupo de destino de Intune, no se eliminará el correspondiente grupo dinámico de Azure AD. Se borrarán los miembros del grupo y la consulta dinámica, pero el propio grupo permanecerá hasta que el administrador de TI lo quite a través del portal de Azure AD.

De forma similar, si el administrador de TI cambia qué grupo de Intune es el destino de un perfil de inscripción de dispositivos corporativos, Intune crea un nuevo grupo dinámico que refleje la nueva asignación de perfil, pero no quitará el grupo dinámico creado para la asignación anterior.

Administración predeterminada de los dispositivos de escritorio Windows mediante la configuración de Windows

El comportamiento predeterminado para inscribir equipos de escritorio de Windows 10 está cambiando. Las nuevas inscripciones seguirán el típico flujo de inscripción del agente MDM en lugar del agente de PC. El sitio web de portal de empresa proporcionará a los usuarios de escritorio de Windows 10 las instrucciones de inscripción que les guiarán a través del proceso de agregar equipos de escritorio de Windows 10 como dispositivos móviles. Esto no afectará a los PC inscritos en estos momentos, y su organización todavía puede administrar equipos de escritorio de Windows 10 con el agente de PC si lo prefiere.

Mejora de la asistencia de la administración de aplicaciones móviles para el borrado selectivo

A los usuarios finales se les proporcionarán instrucciones adicionales sobre cómo recuperar el acceso a los datos profesionales o educativos si estos se quitaron automáticamente debido a la directiva "Intervalo sin conexión antes de que se borren los datos de la aplicación".

Los vínculos de Portal de empresa para iOS se abren dentro de la aplicación

Los vínculos dentro de la aplicación de portal de empresa para iOS, incluidos los de documentación y aplicaciones, se abrirán directamente en la aplicación de portal de empresa con una vista desde la aplicación de Safari. Esta actualización se enviará por separado desde la actualización del servicio en enero.

Nueva dirección del servidor MDM para dispositivos Windows

Se producirá un error en la inscripción del dispositivo si los usuarios de Windows y Windows Phone especifican **manage.microsoft.com** como la dirección del servidor MDM (si se le pide). La dirección del servidor MDM cambia de **manage.microsoft.com** a **enrollment.manage.microsoft.com**. Notifique al usuario que use

enrollment.manage.microsoft.com como la dirección del servidor MDM si se le pide durante la inscripción de un dispositivo Windows o Windows Phone. No se requieren cambios para la configuración de CNAME. Para obtener información adicional sobre este cambio, visite aka.ms/intuneenrollsvrchange.

Nueva experiencia del usuario en la aplicación Portal de empresa para Android

A partir de marzo, la aplicación del portal de empresa para Android seguirá las directrices de Material Design para crear una apariencia más moderna. Esta experiencia del usuario mejorada incluye:

- **Colores**: los encabezados de pestaña pueden colorearse según la paleta de colores personalizada.
- **Interfaz**: los botones Aplicaciones destacadas y Todas las aplicaciones se han actualizado en la pestaña Aplicaciones. El botón Buscar ahora es un botón de acción flotante.
- **Navegación**: Todas las aplicaciones muestra una vista con pestañas de Destacadas, Todas y Categorías para navegar más fácilmente.
- **Servicio**: las pestañas Mis dispositivos y Contactar con TI han mejorado la legibilidad.

Puede encontrar imágenes de antes y después en la página de actualizaciones de la interfaz de usuario.

Asociación de varias herramientas de administración con Microsoft Store para Empresas

Si usa más de una herramienta de administración para implementar las aplicaciones de la Tienda Microsoft para Empresas, anteriormente solo podía asociar una de ellas con la Tienda Microsoft para Empresas. Ahora puede asociar varias herramientas de administración con la tienda, por ejemplo, Intune y Configuration Manager. Para obtener más información, vea Administrar las aplicaciones adquiridas a través de la Tienda Microsoft para Empresas con Microsoft Intune.

Novedades de la versión preliminar pública de Intune en Azure Portal

A principios de 2017 migraremos nuestra experiencia de administración completa a Azure, lo que permitirá una administración eficaz e integrada de los flujos de trabajo principales de EMS en una moderna plataforma de servicios que es extensible mediante las Graph API.

Nuevos inquilinos de prueba comenzarán a ver la versión preliminar pública de la nueva experiencia de administración en el portal de Azure de este mes. Durante el estado de versión preliminar, se proporcionarán funcionalidades y paridad con la consola de Intune existente de manera iterativa.

La experiencia de administración de Azure Portal usará la nueva funcionalidad de agrupación y destino ya anunciadas; cuando el inquilino existente se migra a la nueva experiencia de agrupación, también se migra a la versión preliminar la nueva experiencia de administración en el inquilino. Mientras tanto, si desea probar o consultar cualquiera de las nuevas funcionalidades hasta que se migre el inquilino, regístrese para una nueva cuenta de prueba de Intune o consulte la nueva documentación.

Puede encontrar las novedades en la vista previa de Intune en Azure aquí.

Enero de 2017

Nuevas funcionalidades

Informes en la consola para MAM sin inscripción

Se han agregado nuevos informes de protección de aplicaciones para los dispositivos inscritos y no inscritos. Obtenga más información sobre cómo puede supervisar directivas de administración de aplicaciones móviles con Intune.

Compatibilidad con Android 7.1.1

Intune ahora es totalmente compatible con Android 7.1.1 y lo administra.

Resolver el problema en el que los dispositivos iOS están inactivos o la consola de administración no puede comunicarse con ellos

Cuando los dispositivos de los usuarios pierden el contacto con Intune, puede proporcionarles nuevos pasos de solución de problemas para ayudarles a volver a obtener acceso a los recursos de la empresa. Vea Los

dispositivos están inactivos o la consola de administración no puede comunicarse con ellos.

Notificaciones

Administración predeterminada de los dispositivos de escritorio Windows mediante la configuración de Windows

El comportamiento predeterminado para inscribir equipos de escritorio de Windows 10 está cambiando. Las nuevas inscripciones seguirán el típico flujo de inscripción del agente MDM en lugar del agente de PC.

El sitio web de portal de empresa proporcionará a los usuarios de escritorio de Windows 10 las instrucciones de inscripción que les guiarán a través del proceso de agregar equipos de escritorio de Windows 10 como dispositivos móviles. Esto no afectará a los PC inscritos en estos momentos, y su organización todavía puede administrar equipos de escritorio de Windows 10 con el agente de PC si lo prefiere.

Mejora de la asistencia de la administración de aplicaciones móviles para el borrado selectivo

A los usuarios finales se les proporcionarán instrucciones adicionales sobre cómo recuperar el acceso a los datos profesionales o educativos si estos se quitaron automáticamente debido a la directiva "Intervalo sin conexión antes de que se borren los datos de la aplicación".

Los vínculos de Portal de empresa para iOS se abren dentro de la aplicación

Los vínculos dentro de la aplicación de portal de empresa para iOS, incluidos los de documentación y aplicaciones, se abrirán directamente en la aplicación de portal de empresa con una vista desde la aplicación de Safari. Esta actualización se enviará por separado desde la actualización del servicio en enero.

Renovación del sitio web del portal de empresa

A partir de febrero, el sitio web del portal de empresa admitirá aplicaciones destinadas a aquellos usuarios que no tienen dispositivos administrados. El sitio web se asemejará a otros productos y servicios de Microsoft gracias a una nueva combinación de colores de contraste, ilustraciones dinámicas y un "menú hamburguesa",  .

Nueva documentación para las directivas de protección de aplicaciones

Hemos actualizado nuestra documentación para administradores y desarrolladores de aplicaciones que quieran habilitar directivas de protección de aplicaciones (conocidas como directivas de MAM) en sus aplicaciones iOS y Android con la herramienta de ajuste de aplicaciones de Intune o con el SDK para aplicaciones de Intune.

Se han actualizado los siguientes artículos:

- Decidir cómo preparar las aplicaciones para la administración de aplicaciones móviles mediante Microsoft Intune
- Preparar aplicaciones iOS para la administración de aplicaciones móviles con la Herramienta de ajuste de aplicaciones de Intune
- Introducción al SDK para aplicaciones de Microsoft Intune
- Guía para desarrolladores sobre el SDK de aplicaciones de Intune para iOS

Se han agregado los siguientes artículos nuevos a la biblioteca de documentos:

- Complemento Cordova del SDK para aplicaciones de Intune
- Componente Xamarin del SDK para aplicaciones de Intune

Barra de progreso cuando se inicia el portal de empresa en iOS

El portal de empresa para iOS presenta una barra de progreso en la pantalla de inicio para proporcionar información al usuario sobre los procesos de carga que se producen. Habrá una implementación por fases de la barra de progreso para reemplazar el control de número. Esto significa que algunos usuarios verán la nueva barra de progreso y otros seguirán viendo el control de número.

Diciembre de 2016

Versión preliminar pública de Intune en Azure Portal

A principios de 2017 migraremos nuestra experiencia de administración completa a Azure, lo que permitirá una

administración eficaz e integrada de los flujos de trabajo principales de EMS en una moderna plataforma de servicios que es extensible mediante las Graph API. Antes de la disponibilidad general de este portal para todos los inquilinos de Intune, nos complace anunciar que comenzaremos a implementar una versión preliminar de esta nueva experiencia de administración dentro de este mes para seleccionar inquilinos.

La experiencia de administración del portal de Azure usará la nueva funcionalidad de agrupación y selección de destino ya anunciada; cuando se migre su inquilino existente a la nueva experiencia de agrupación también se migrará a la versión preliminar la nueva experiencia de administración en el inquilino. Mientras tanto, encuentre más información sobre lo que tenemos en Azure Portal para Microsoft Azure en nuestra documentación nueva.

Integración de la administración de gastos de telecomunicaciones en la versión preliminar pública de Azure Portal Ahora estamos comenzando a realizar la integración de la versión preliminar con los servicios de administración de gastos de telecomunicaciones (TEM) dentro del portal de Azure. Puede usar Intune para exigir límites sobre el uso de datos nacionales y móviles. Comenzaremos estas integraciones con Saaswedo. Para habilitar esta característica en su inquilino de prueba, póngase en contacto con el soporte técnico de Microsoft.

Nuevas funcionalidades

Autenticación multifactor en todas las plataformas Ahora puede exigir la autenticación multifactor (MFA) en un grupo de usuarios seleccionado cuando inscriben un dispositivo iOS, Android, Windows 8.1 + o Windows Phone 8.1 + desde el Portal de administración de Azure mediante la configuración de MFA en la aplicación de inscripción de Microsoft Intune en Azure Active Directory.

Capacidad para restringir la inscripción de dispositivos móviles Intune está agregando nuevas restricciones de inscripción que controlan qué plataformas de dispositivos móviles pueden inscribir. Intune separa las plataformas de dispositivos móviles como iOS, Mac OS, Android, Windows y Windows Mobile.

- La restricción la inscripción de dispositivos móviles no restringe la inscripción del cliente de PC.
- Solo para iOS, hay una opción adicional para bloquear la inscripción de dispositivos de propiedad personal.

Intune marca todos los dispositivos nuevos como personal a menos que el administrador de TI tome la medida de marcarlos como propiedad de la empresa, como se explica en este artículo.

Notificaciones

Multi-Factor Authentication para la inscripción se mueve a Azure Portal Anteriormente, los administradores iban a la consola de Intune o a la consola de Configuration Manager (antes de la versión de octubre de 2016) para establecer MFA para las inscripciones de Intune. Con esta característica actualizada, ahora iniciará sesión en el portal de Microsoft Azure con sus credenciales de Intune y configurará MFA mediante Azure AD. Aprenda más al respecto aquí.

La aplicación del Portal de empresa para Android ahora disponible en China Publicaremos la aplicación del Portal de empresa para Android para su descarga en China.Debido a la ausencia de Google Play Store en China, los dispositivos Android deben obtener aplicaciones de mercados de aplicaciones chinos. La aplicación Portal de empresa para Android estará disponible para su descarga en las siguientes tiendas:

- Baidu
- Huawei
- Tencent
- Wandoujia

La aplicación de portal de empresa para Android utiliza Google Play Services para comunicarse con el servicio de Microsoft Intune. Como Google Play Services no está todavía disponible en China, la realización de cualquiera de las siguientes tareas puede tardar hasta 8 horas en completarse.

CONSOLA DE ADMINISTRACIÓN DE INTUNE	APLICACIÓN DEL PORTAL DE EMPRESA DE INTUNE PARA ANDROID	SITIO WEB DEL PORTAL DE EMPRESA DE INTUNE
Borrar todos los datos	Quitar un dispositivo remoto	Quitar dispositivo (local y remoto)
Borrado selectivo	Restablecer dispositivo	Restablecer dispositivo
Implementaciones de la aplicación nuevas o actualizadas	Instalar aplicaciones de línea de negocio disponibles	Restablecimiento del código de acceso del dispositivo
Bloqueo remoto		
Restablecimiento de la contraseña		

Elementos obsoletos

Firefox ya no admitirá Silverlight Mozilla quitará la compatibilidad con Silverlight en la versión 52 del explorador Firefox, a partir de marzo de 2017. Como resultado de lo anterior, ya no podrá iniciar sesión en la consola de Intune existente con las versiones de Firefox superiores a la versión 51. Se recomienda usar Internet Explorer 10 u 11 para obtener acceso a la consola de administración, o bien una versión de Firefox anterior a la versión 52. La transición de Intune a Azure Portal le permitirá admitir varios exploradores modernos sin depender de Silverlight.

Eliminación de directivas de bandeja de entrada móvil de Exchange Online A partir de diciembre, los administradores ya no podrán ver ni configurar directivas de buzón móvil de Exchange Online (EAS) en la consola de Intune. Este cambio se implementará en todos los inquilinos de Intune durante diciembre y enero. Todas las directivas existentes permanecerán como están configuradas; para configurar nuevas directivas, use el Shell de administración de Exchange. Puede encontrar más información aquí.

Ya no se admiten las aplicaciones AV Player, Image Viewer y PDF Viewer de Intune en Android Desde mediados de diciembre de 2016 en adelante, los usuarios ya no podrán utilizar las aplicaciones AV Player, Image Viewer, y PDF Viewer de Intune. Estas aplicaciones se han reemplazado por la aplicación Azure Information Protection. Descubra más sobre la aplicación Azure Information Protection aquí.

Noviembre de 2016

Nuevas funcionalidades

Nuevo portal de empresa de Microsoft Intune disponible para los dispositivos Windows 10 Microsoft ha lanzado una nueva aplicación de portal de empresa de Microsoft Intune para los dispositivos Windows 10. Esta aplicación, que aprovecha el nuevo formato de Windows 10 Universal, proporcionará al usuario una experiencia de usuario actualizada dentro de la aplicación y experiencias idénticas en todos los dispositivos Windows 10, PC y móvil, mientras sigue permitiendo las mismas funcionalidades que usa hoy en día.

La nueva aplicación también permitirá a los usuarios aprovechar características de plataforma adicional como el inicio de sesión único (SSO) y la autenticación basada en certificados en dispositivos Windows 10. La aplicación estará disponible como una actualización del Portal de empresa de Windows 8.1 existente. El Portal de empresa de Windows Phone 8.1 se instala desde la Microsoft Store. Para más información, vaya a aka.ms/intunecp_universalapp.

> **IMPORTANT**
>
> **Actualización de Intune y Android for Work** Aunque se pueden implementar aplicaciones de Android for Work con una acción **Requerido**, solo puede implementar aplicaciones como **Disponible** si los grupos de Intune se han migrado a la nueva experiencia de grupos de Azure AD.

El complemento Intune App SDK para Cordova ahora admite MAM sin inscripción Los desarrolladores de aplicaciones ahora pueden usar el complemento Intune App SDK para Cordova para habilitar la funcionalidad MAM sin inscribir el dispositivo en sus aplicaciones de Cordova para Android e iOS/iPadOS.

El componente Xamarin de Intune App SDK ahora admite MAM sin suscripción Los desarrolladores de aplicaciones ahora pueden usar el componente Xamarin de Intune App SDK para habilitar la funcionalidad MAM sin inscribir el dispositivo en sus aplicaciones basadas en Xamarin para Android e iOS/iPadOS. El componente Xamarin del SDK para aplicaciones de Intune se puede encontrar aquí.

Notificaciones

El certificado de firma de Symantec ya no requiere el portal de empresa firmado de Windows Phone 8 para la carga La carga del certificado de firma de Symantec ya no requiere una aplicación firmada del portal de empresa de Windows Phone 8. El certificado se puede cargar de forma independiente.

Elementos obsoletos

Compatibilidad con el portal de empresa de Windows Phone 8 La compatibilidad con el portal de empresa de Windows Phone 8 ahora está en desuso. La compatibilidad con las plataformas Windows Phone 8 y WinRT ha quedado en desuso en octubre de 2016. La compatibilidad con el portal de empresa de Windows 8 ha quedado en desuso en octubre de 2016.

Vea también

Vea Novedades de Microsoft Intune para obtener más información sobre los desarrollos recientes.

¿Dónde está mi característica de Intune en Azure?

14/05/2021 • 6 minutes to read

Hemos aprovechado la oportunidad para organizar algunas tareas de forma más lógica durante el traslado de Intune a Azure Portal. Pero, como ocurre con todas las mejoras, deberá aprender la nueva organización. Esta guía de referencia está dirigida a aquellos que están familiarizados con Intune en el portal clásico y se preguntan dónde se encuentra una determinada función en Intune en Azure Portal. Si en este artículo no se incluye una característica que intenta encontrar, deje un comentario al final para que podamos actualizarlo.

Guía de referencia rápida

CARACTERÍSTICA	RUTA DE ACCESO DEL PORTAL CLÁSICO	RUTA DE ACCESO EN INTUNE EN AZURE PORTAL
Programa de inscripción de dispositivos (DEP) [solo iOS]	Administración > Administración de dispositivos móviles > iOS > Programa de inscripción de dispositivos	Inscripción de dispositivos > Inscripción de Apple > Token del Programa de inscripción
Programa de inscripción de dispositivos (DEP) [solo iOS]	Administración > Administración de dispositivos móviles > iOS y Mac OS X > Programa de inscripción de dispositivos	Inscripción de dispositivos > Inscripción de Apple > Números de serie del Programa de inscripción
Reglas de inscripción	Administración > Administración de dispositivos móviles > Reglas de inscripción	Inscripción de dispositivos > Restricciones de inscripción
Grupos mediante número de serie de iOS	Grupos > Todos los dispositivos > Dispositivos corporativos inscritos previamente > Mediante número de serie de iOS	Inscripción de dispositivos > Inscripción de Apple > Números de serie del Programa de inscripción
Grupos mediante número de serie de iOS	Grupos > Todos los dispositivos > Dispositivos corporativos inscritos previamente > Mediante número de serie de iOS	Inscripción de dispositivos > Inscripción de Apple > Números de serie de AC
Grupos mediante IMEI (todas las plataformas)	Grupos > Todos los dispositivos > Dispositivos corporativos inscritos previamente > Mediante IMEI (todas las plataformas)	Inscripción de dispositivos > Identificadores de dispositivo corporativos
Perfil de inscripción de dispositivos corporativos	Directiva > Inscripción de dispositivos corporativos	Inscripción de dispositivos > Inscripción de Apple > Perfiles del Programa de inscripción
Perfil de inscripción de dispositivos corporativos	Directiva > Inscripción de dispositivos corporativos	Inscripción de dispositivos > Inscripción de Apple > Perfiles de AC
Android for Work	Administración > Administración de dispositivos móviles > Android for Work	Inscripción de dispositivos > Inscripción en Android

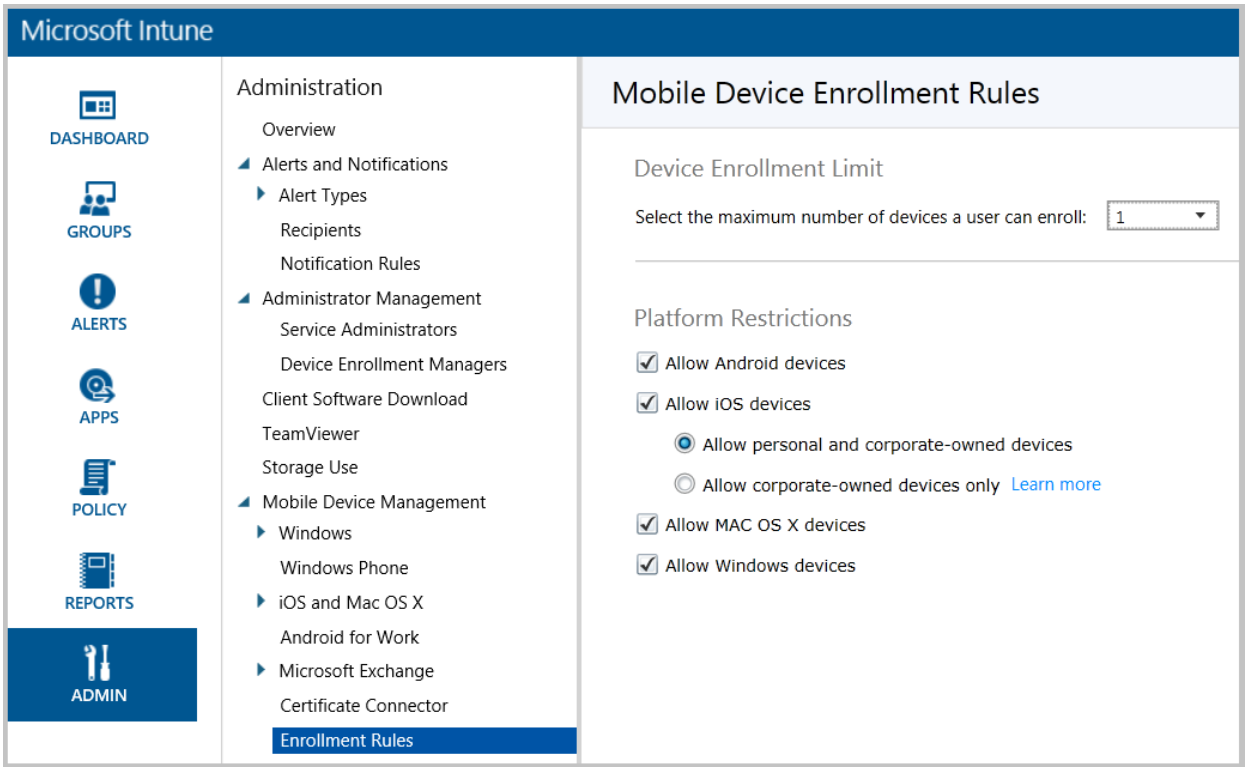
CARACTERÍSTICA	RUTA DE ACCESO DEL PORTAL CLÁSICO	RUTA DE ACCESO EN INTUNE EN AZURE PORTAL
Términos y condiciones	Directiva > Términos y condiciones	Inscripción de dispositivos > Términos y condiciones
Configuración del Portal de empresa	Admin > Portal de empresa	**Administrar** > Aplicaciones móviles **Configurar** > Personalización de marca del Portal de empresa

¿Dónde se administran los grupos?

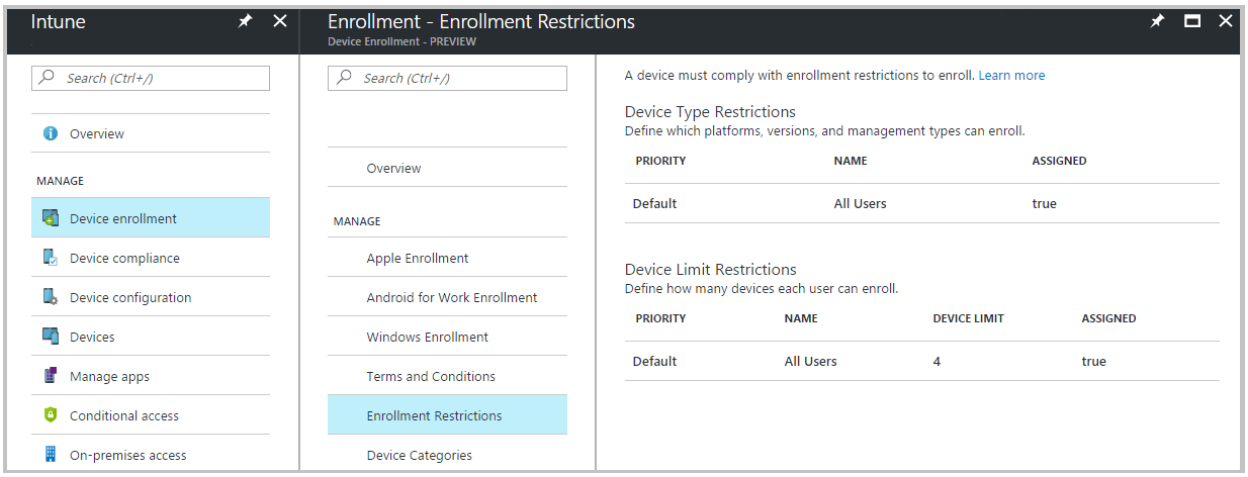
Intune en Azure Portal usa Azure Active Directory (AD) para administrar grupos.

¿Dónde están las reglas de inscripción?

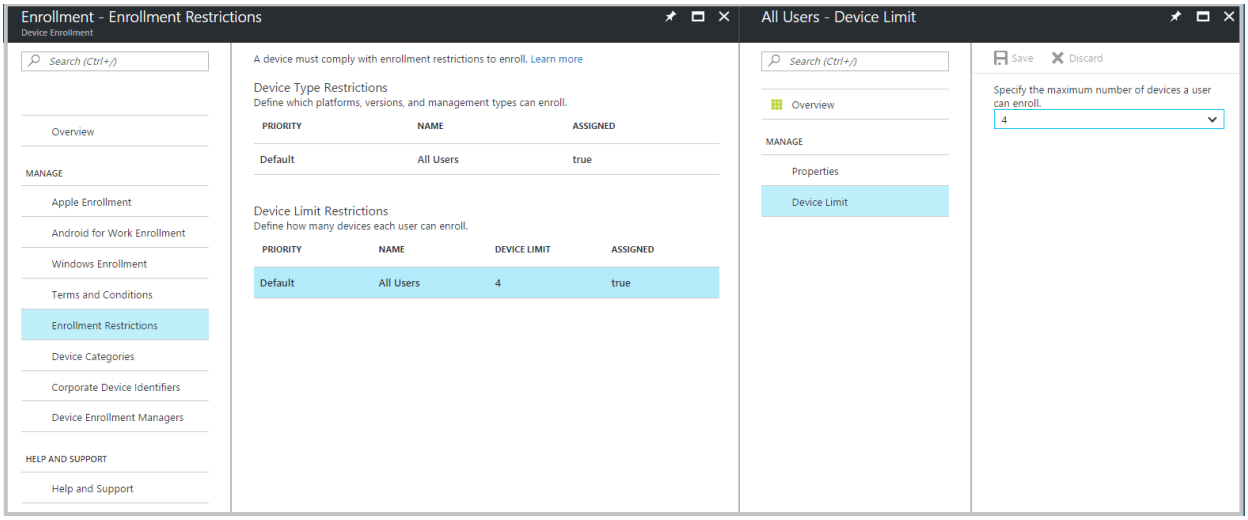
En el portal clásico, podía establecer reglas que controlaran la inscripción de MDM de dispositivos macOS y Windows móviles y modernos.



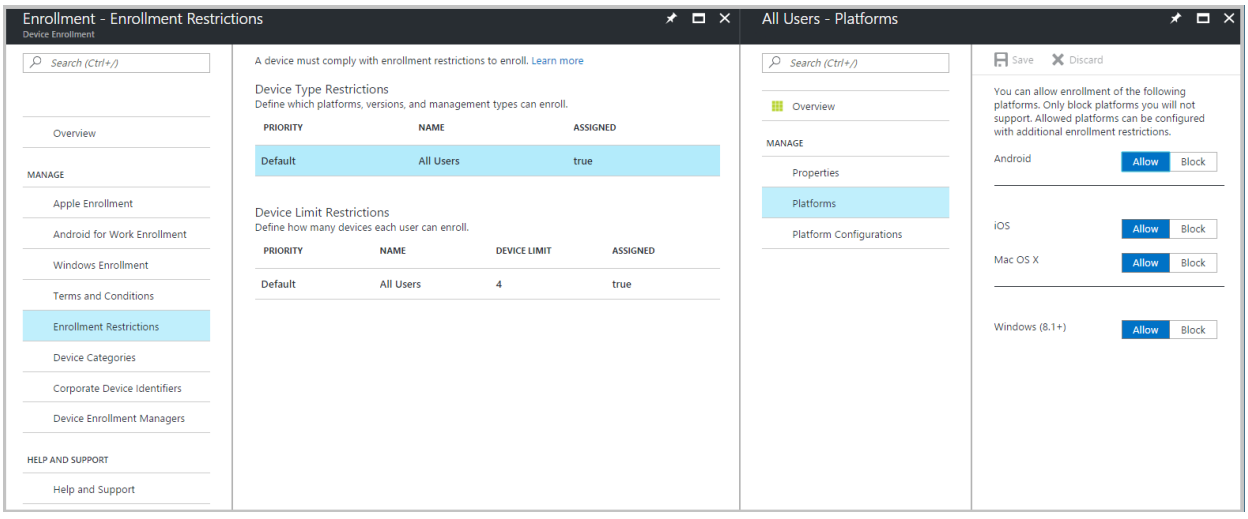
Estas reglas se aplicaban a todos los usuarios de su cuenta de Intune sin excepciones. En Azure Portal, ahora estas reglas aparecen en dos tipos de directiva distintos: Restricciones de tipo de dispositivo y Restricciones de límite de dispositivos.



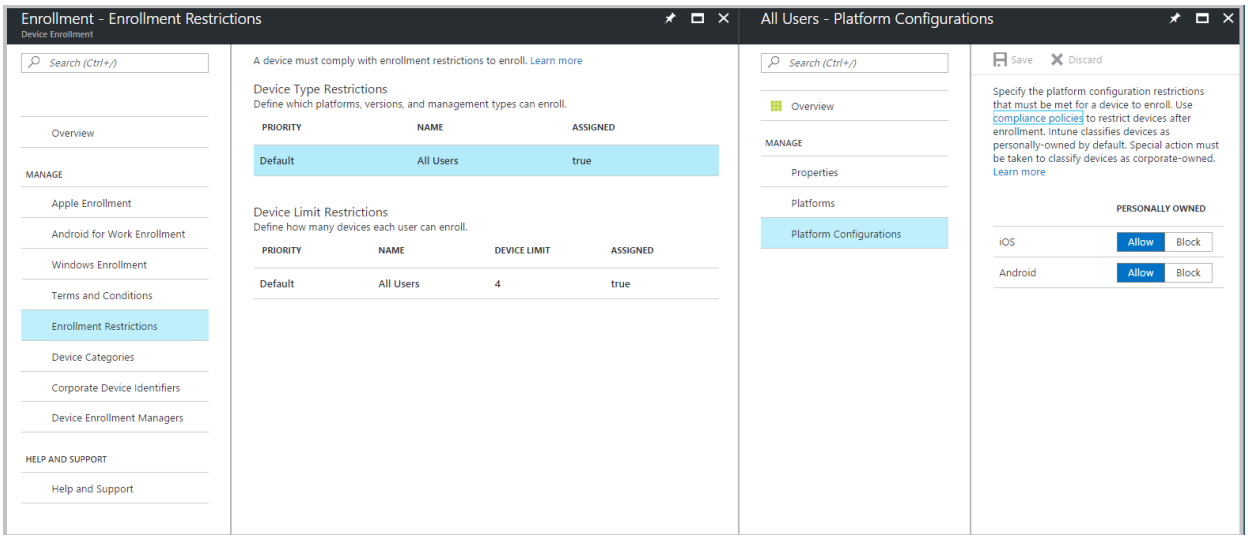
El valor predeterminado de Restricción de límite de dispositivos corresponde al Límite de inscripción de dispositivos del portal clásico.



El valor predeterminado de Restricciones de tipo de dispositivo corresponde a las Restricciones de la plataforma del portal clásico.



La capacidad de permitir o bloquear dispositivos de propiedad personal se administra ahora en las Configuraciones de plataforma de Restricciones de tipo de dispositivo.



Se agregarán nuevas capacidades de restricción únicamente a Azure Portal.

¿Dónde puedo encontrar mis directivas de acceso condicional?

Las directivas de acceso condicional del inquilino se seguirán aplicando cuando el inquilino se haya migrado a Azure Portal. Sin embargo, no podrá ver o modificarlas desde Intune en Azure Portal.

Si quiere ver y modificar las directivas de acceso condicional desde Azure Portal, deberá quitar del portal clásico las directivas anteriores. Después, deberá volver a crearlas en Azure Portal. Para obtener más información sobre la migración de directivas de acceso condicional, vea Migración de directivas clásicas en Azure Portal.

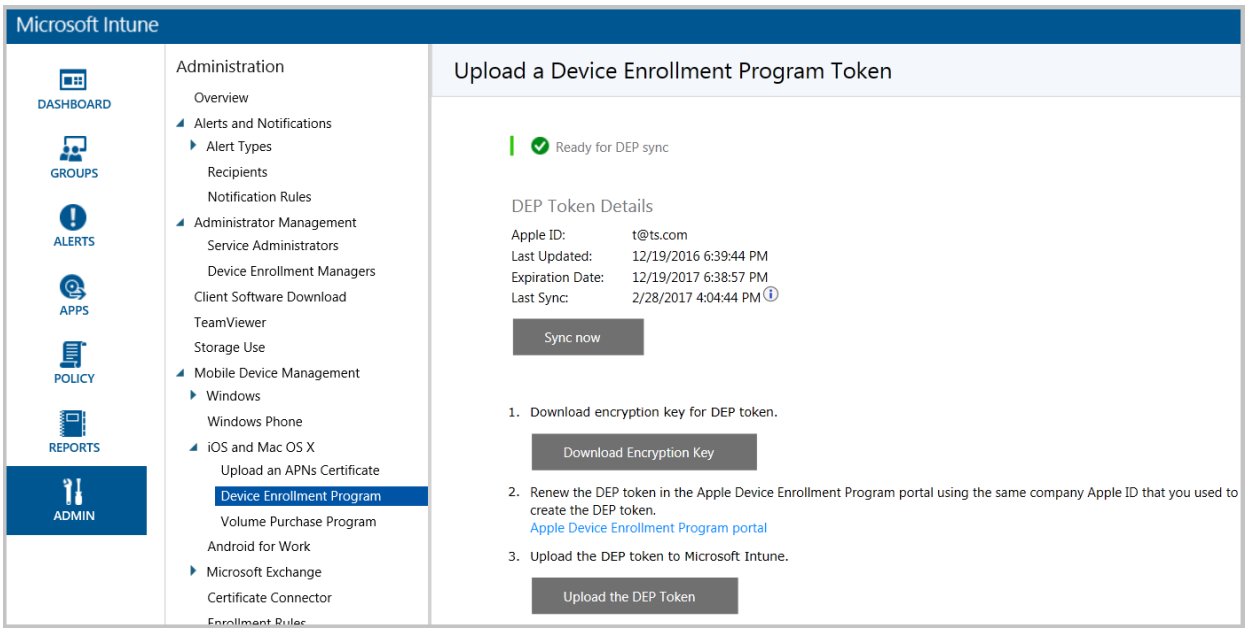
¿Dónde puedo encontrar mis directivas de cumplimiento?

Las directivas de cumplimiento del inquilino se seguirán aplicando cuando el inquilino se haya migrado a Azure Portal. Sin embargo, no podrá ver o modificarlas desde Intune en Azure Portal.

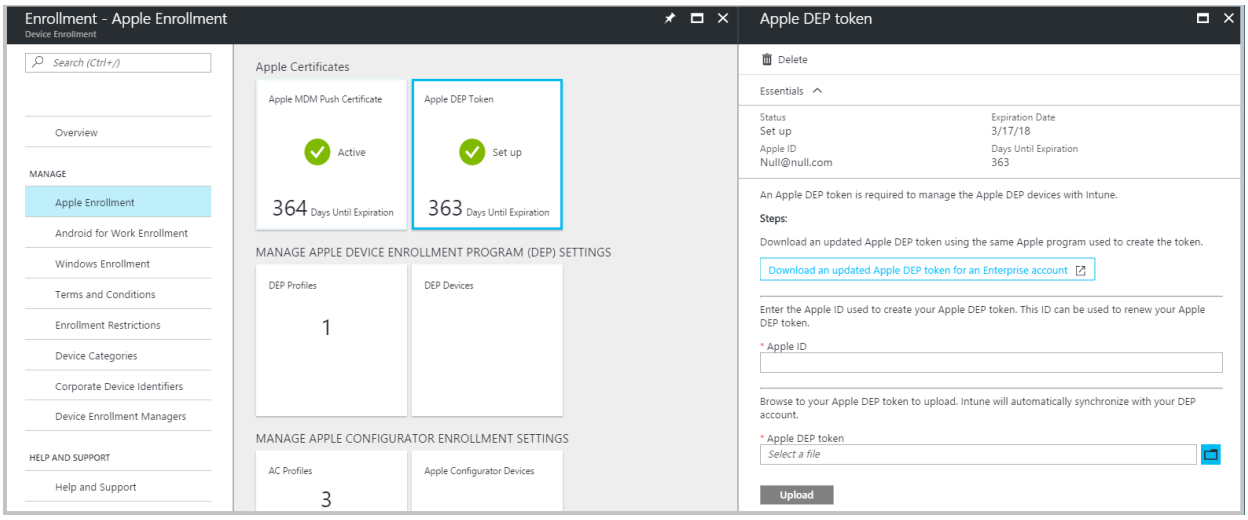
Si quiere ver y modificar las directivas de cumplimiento desde Azure Portal, deberá quitar del portal clásico las directivas anteriores. Después, deberá volver a crearlas en Azure Portal. Para obtener más información sobre las directivas de cumplimiento de dispositivos, consulte la introducción a las directivas de cumplimiento de dispositivos en Intune.

¿Dónde está el servicio DEP de Apple?

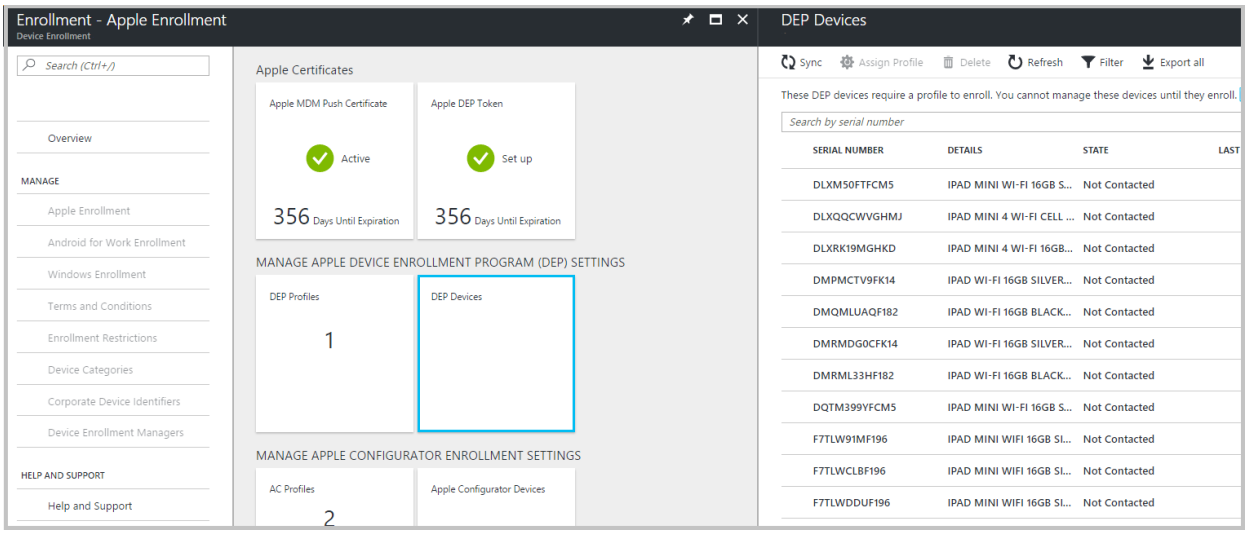
En el portal clásico, podía configurar Intune para que se integrara con el Programa de inscripción de dispositivos de Apple y solicitar manualmente la sincronización con el servicio de Apple:



En Azure Portal, configure el Programa de inscripción de dispositivos de Apple siguiendo los mismos pasos que en la consola clásica de Intune:



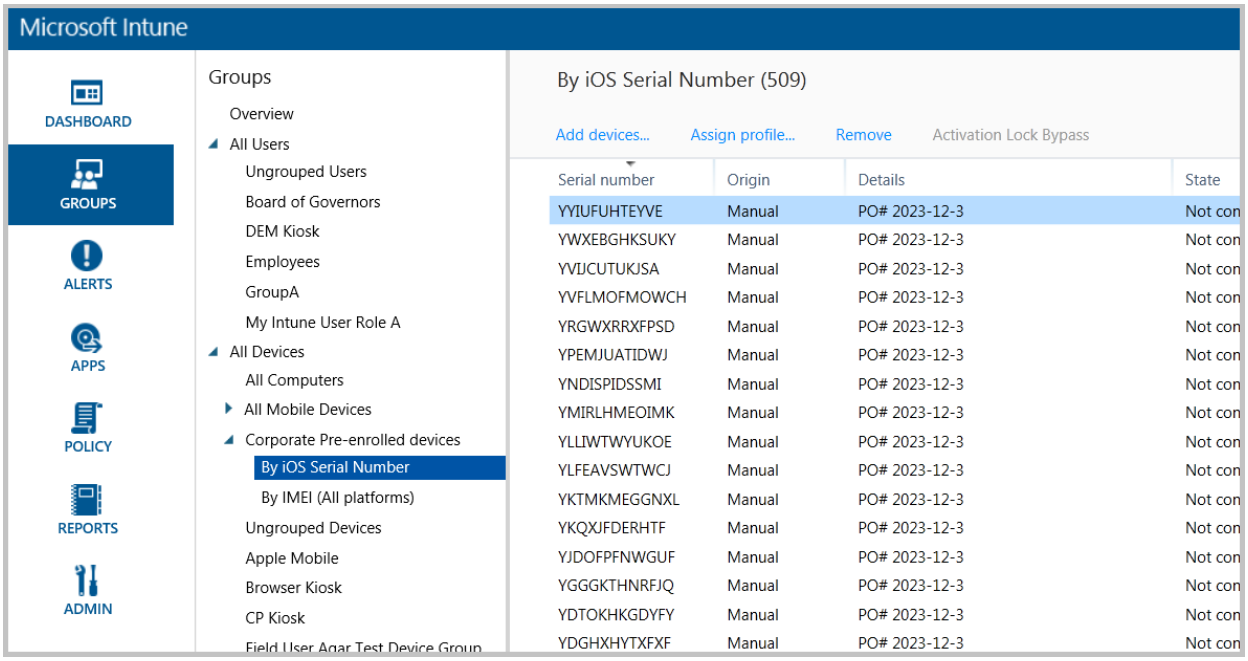
En cambio, la opción **Sincronizar** del portal clásico se ha movido al flujo de trabajo de administración de número de serie, puesto que los resultados de una sincronización manual aparecen ahí:



¿Dónde están los dispositivos corporativos inscritos previamente?

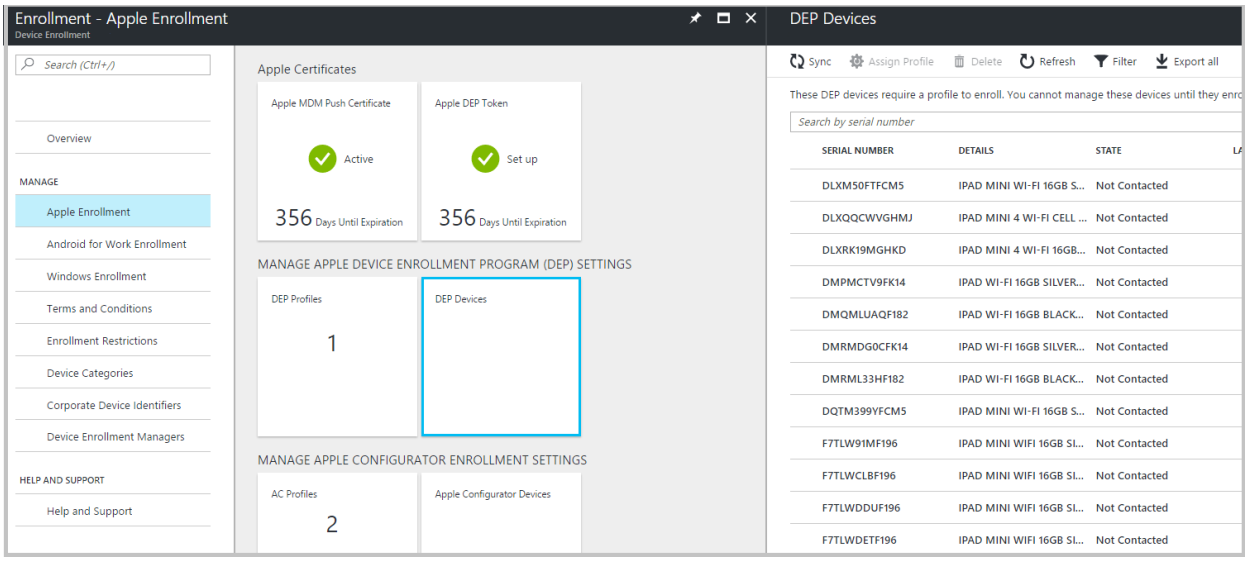
Mediante número de serie de iOS

En el portal clásico, puede inscribir dispositivos iOS mediante el Programa de inscripción de dispositivos (DEP) de Apple y la herramienta Apple Configurator. Ambos métodos ofrecen la inscripción previa de dispositivos mediante número de serie e implican la asignación de perfiles de inscripción de dispositivos corporativos especiales. Antes de la inscripción, se puede administrar la asignación de perfiles de inscripción a través del grupo de dispositivos **Dispositivos corporativos inscritos previamente mediante número de serie de iOS**:

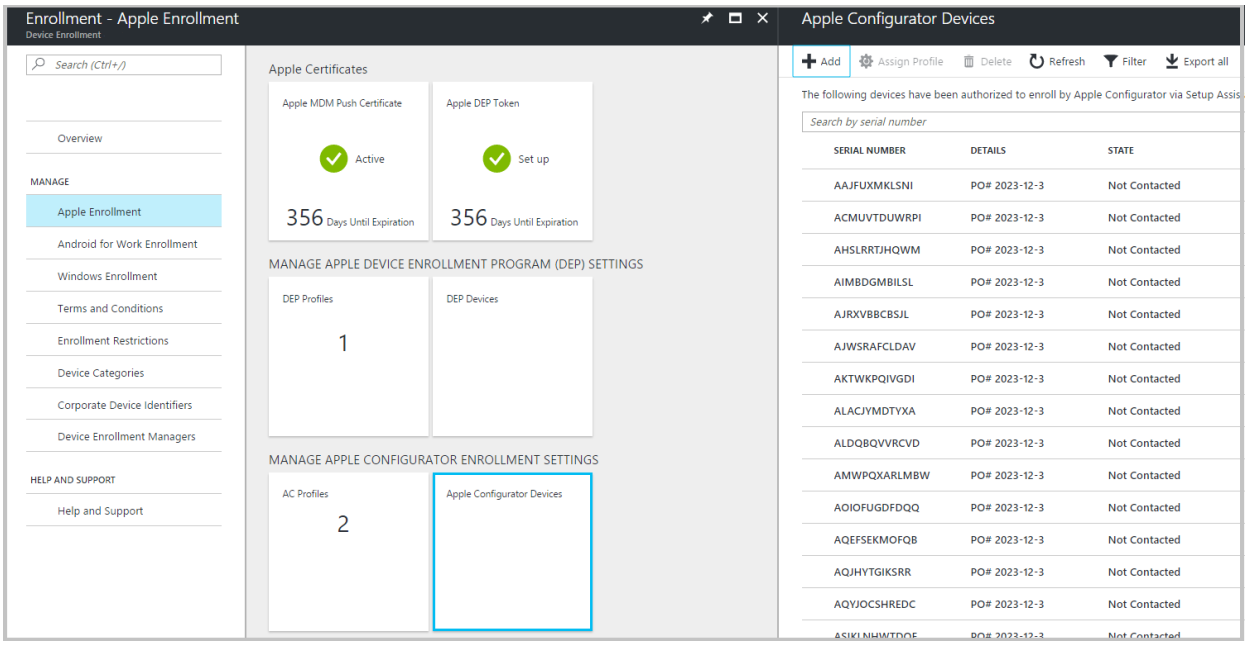


Este enumera los números de serie para la inscripción de DEP de Apple y Configurator en una sola lista. Para reducir los errores de coincidencia en la asignación de perfiles (de perfil DEP al número de serie de CA y viceversa), hemos separado los números de serie en dos listas en Azure Portal:

Números de serie de DEP

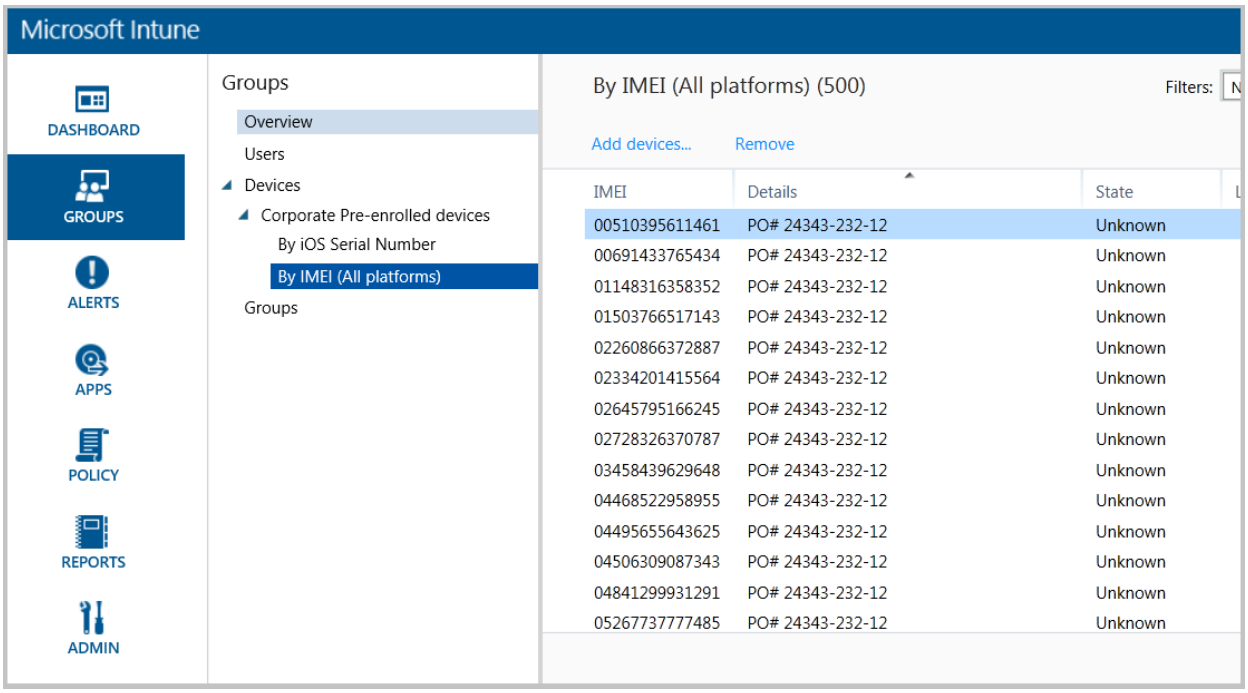


Números de serie de Apple Configurator

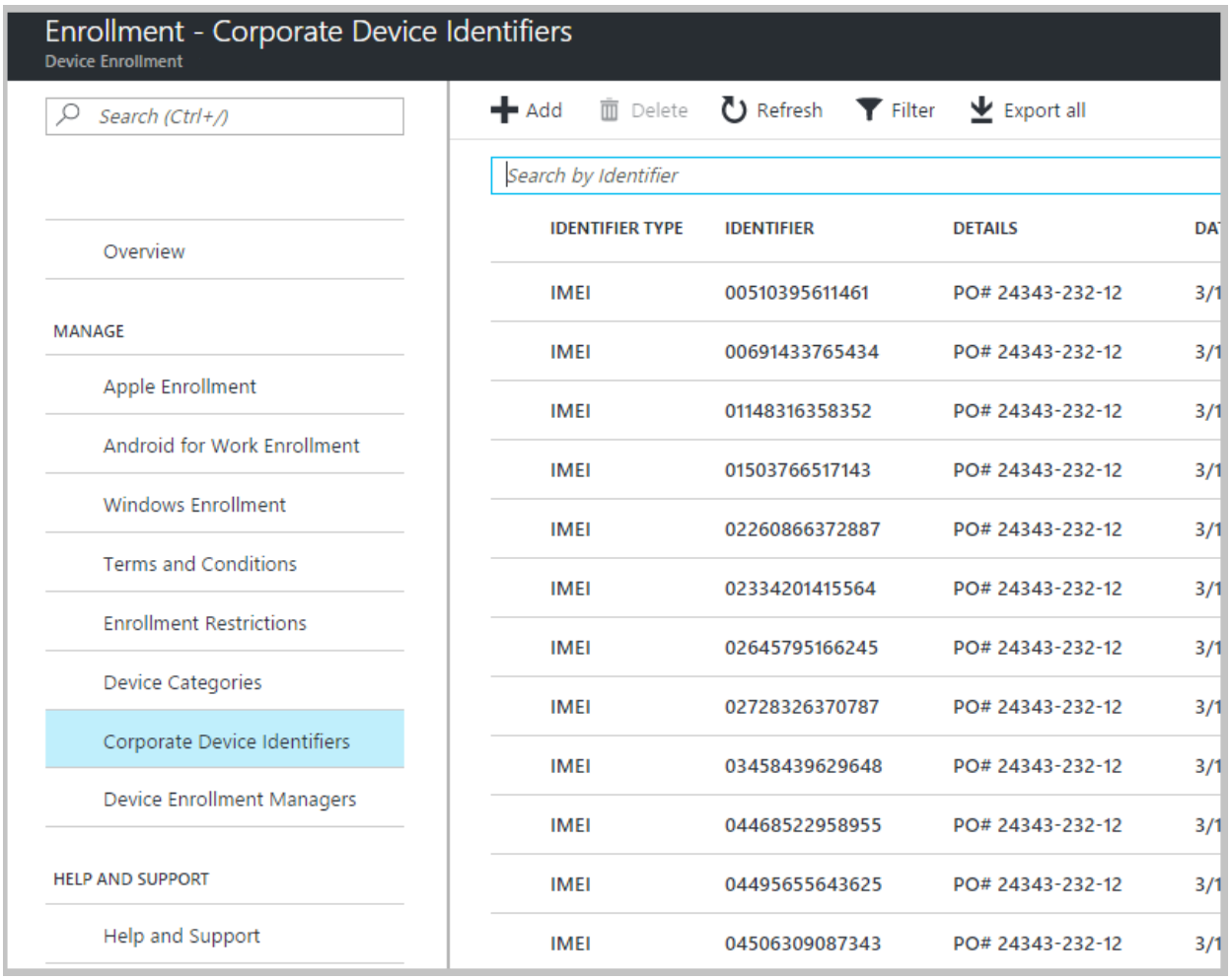


Mediante IMEI (todas las plataformas)

En el portal clásico, puede enumerar previamente los números IMEI de los dispositivos para marcarlos como corporativos cuando se inscriben en Intune:



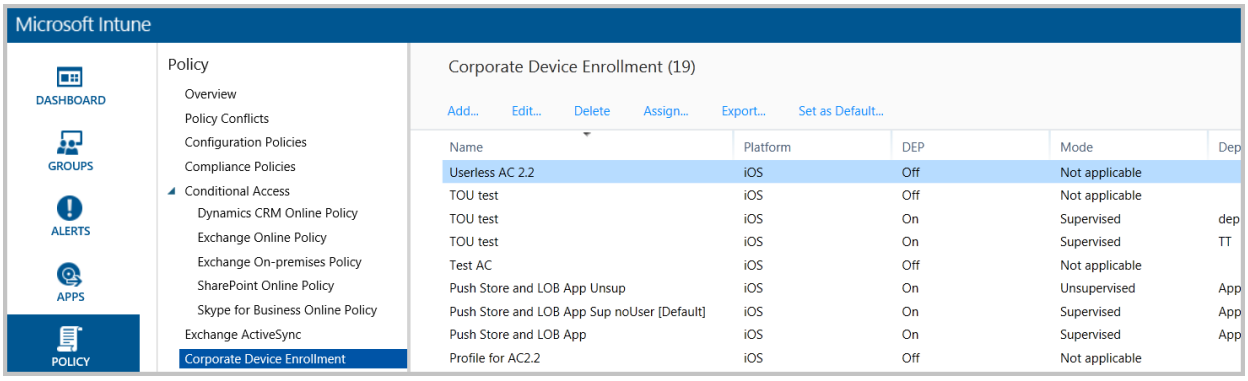
En Azure Portal, debe cargar los mismos IMEI a la lista Identificadores de dispositivo corporativos con un archivo de valores separados por comas (CSV). El nuevo portal no admite la entrada manual de números IMEI:



Intune en Azure Portal está preparado para el futuro, puesto que será compatible con otros tipos de identificadores aparte de IMEI, aunque actualmente solo admite números IMEI en las listas previas.

¿Dónde están los perfiles de inscripción de dispositivos corporativos?

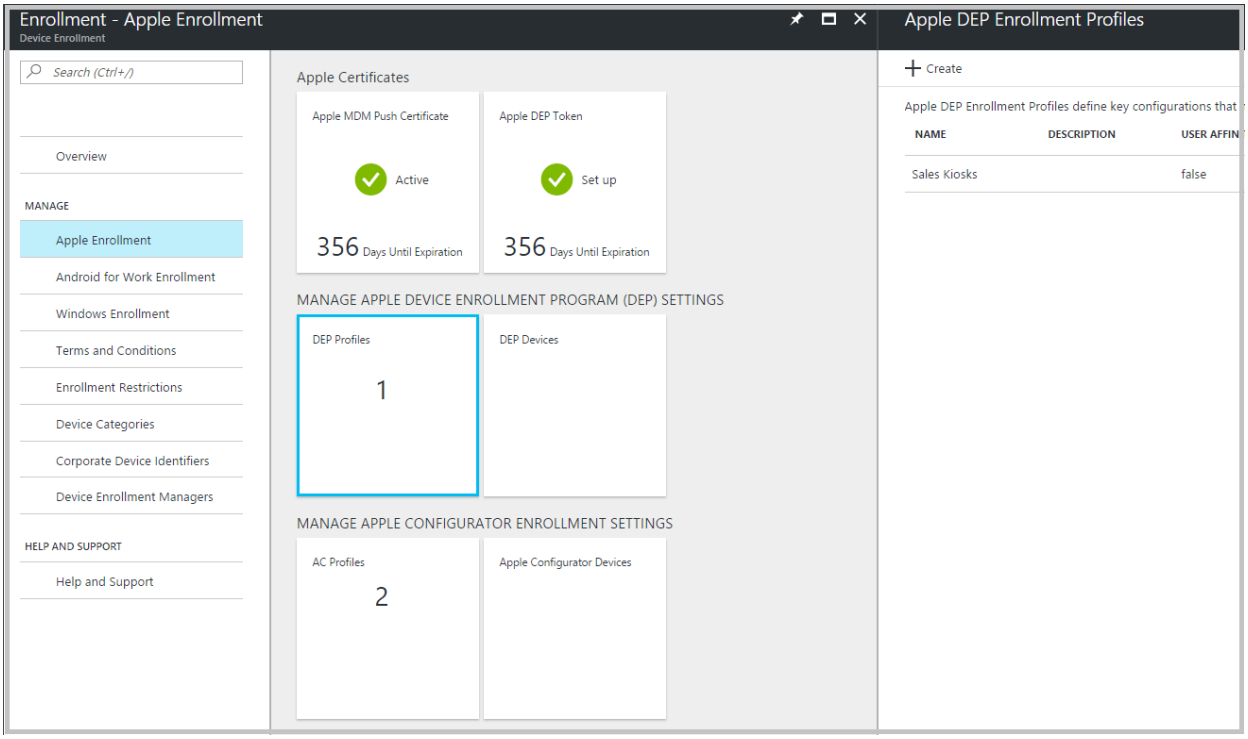
Para inscribir dispositivos iOS a través del Programa de inscripción de dispositivos de Apple o con la herramienta Apple Configurator, debe proporcionar un perfil de inscripción de dispositivos corporativos para asignar al dispositivo. En el portal clásico, la creación y administración de estos perfiles se encontraba en una sola lista:



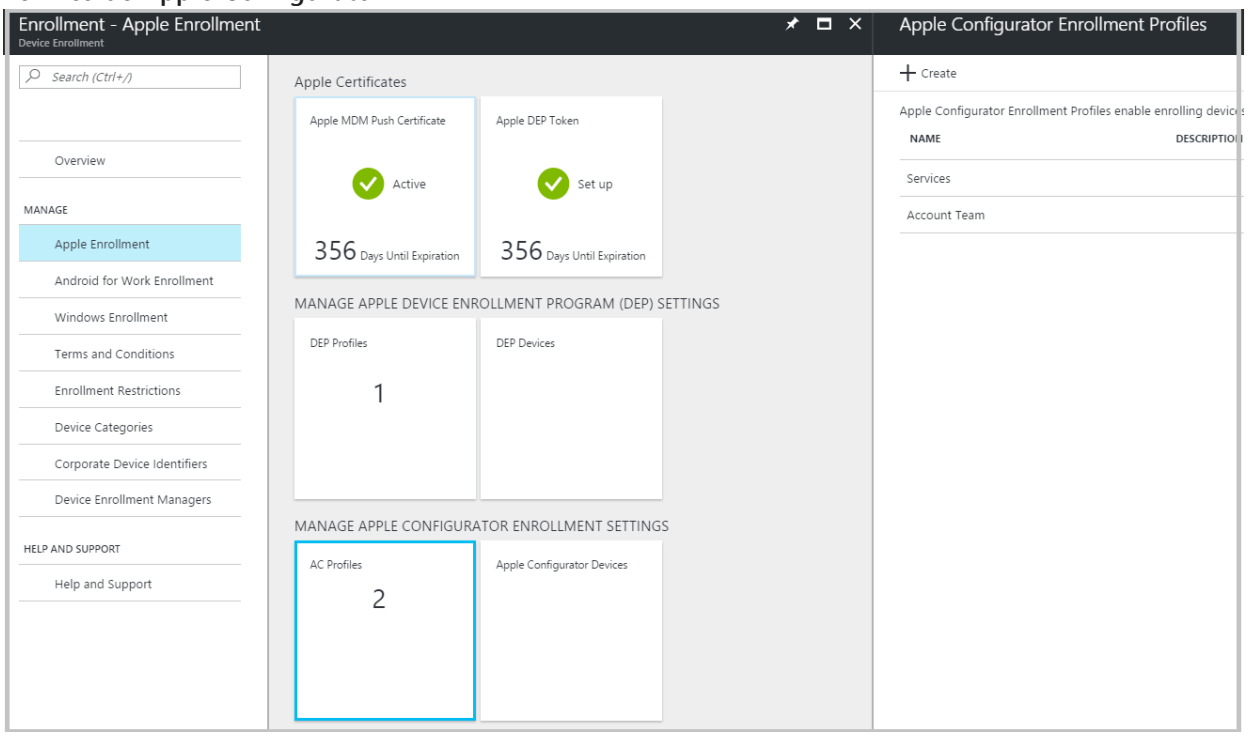
En esta lista se muestran los perfiles habilitados para su uso con el Programa de inscripción de dispositivos de Apple (**DEP Activado**) y los perfiles habilitados solo para su uso con la herramienta Apple Configurator (**DEP Desactivado**).

Para reducir la confusión entre los dos tipos de perfiles y los posibles errores de coincidencia de asignaciones (perfil de DEP a dispositivos de Configurator y viceversa), hemos separado la creación y la administración de los perfiles del programa de inscripción (compatible con el Programa de inscripción de dispositivos de Apple y Apple School Manager) y los perfiles de Apple Configurator:

Perfiles de DEP



Perfiles de Apple Configurator



Grupos clásicos de Microsoft Intune en Azure Portal

14/05/2021 • 4 minutes to read

Hemos escuchado sus comentarios y hemos realizado algunos cambios sobre cómo trabaja con los grupos en Microsoft Intune. Si usa Intune desde el portal de Azure, los grupos de Intune se han migrado a grupos de seguridad de Azure Active Directory.

La ventaja es que ahora usa la misma experiencia de grupos en Enterprise Mobility + Security y en las aplicaciones de Azure AD. Además, puede usar PowerShell y Graph API para extender y personalizar esta nueva función.

Los grupos de seguridad de Azure AD admiten todos los tipos de implementaciones de Intune para los usuarios y los dispositivos. Además, puede usar los grupos dinámicos de Azure AD que se actualizan automáticamente basándose en los atributos que proporcione. Por ejemplo, puede crear un grupo de dispositivos que ejecute iOS 9. Cuando se inscriba un dispositivo que ejecuta iOS 9, el dispositivo se muestra automáticamente en el grupo dinámico.

¿Qué características no están disponibles?

Algunas de las funcionalidades de los grupos que podría haber usado anteriormente no están disponibles en Azure AD:

- Los grupos de Intune **Usuarios sin agrupar** y **Dispositivos sin agrupar** ya no están disponibles.
- La opción para **excluir miembros específicos** de un grupo no existe en el portal de Azure. En cambio, puede usar un grupo de seguridad de Azure AD con reglas avanzadas para replicar este comportamiento. Por ejemplo, para crear una regla avanzada que incluya a todas las personas del departamento de ventas en un grupo de seguridad, pero excluya a esos grupos que tengan la palabra "Assistant" (Asistente) en el nombre de su puesto, puede usar esta regla avanzada:

  `(user.department -eq "Sales") -and -not (user.jobTitle -contains "Assistant")`.
- El grupo **Todos los dispositivos administrados por Exchange ActiveSync** de la consola de Intune clásica no se ha migrado a Azure AD. En cambio, todavía puede acceder a la información sobre dispositivos administrados de EAS desde Azure Portal.

Cómo empezar

- Lea los siguientes temas para obtener información sobre los grupos de seguridad de Azure AD y su funcionamiento:
  - Administración del acceso a los recursos con grupos de Azure Active Directory.
  - Administración de grupos en Azure Active Directory.
  - Uso de atributos para crear reglas avanzadas.
- Asegúrese de que los administradores que necesiten crear grupos se agreguen al rol de Azure AD **Administrador del servicio de Intune**. El rol Administrador del servicio de Azure AD no tiene permisos de **Administrar grupo**.
- Si los grupos de Intune han usado la opción **Excluir miembros específicos**, decida si puede volver a diseñar estos grupos sin exclusiones, o si necesita reglas avanzadas para satisfacer las necesidades empresariales.

¿Qué ha sucedido con los grupos de Intune?

Cuando los grupos se migran de Azure Portal a Intune en Azure Portal, se aplican las siguientes reglas:

GRUPOS DE INTUNE	GRUPOS EN AZURE AD
Grupo de usuarios estáticos	Grupo de seguridad de Azure AD estático
Grupo de usuarios dinámicos	Grupos de seguridad estáticos de Azure AD con una jerarquía de grupos de seguridad de Azure AD
Grupo de dispositivos estáticos	Grupo de seguridad de Azure AD estático
Grupo de dispositivos dinámicos	Grupo de seguridad de Azure AD dinámico
Grupo con una condición de inclusión	Grupo de seguridad de Azure AD estático que contiene cualquier miembro dinámico o estático de la condición de inclusión de Intune
Grupo con una condición de exclusión	No se migra
Los grupos integrados: - **Todos los usuarios** - **Usuarios no agrupados** - **Todos los dispositivos** - **Dispositivos no agrupados** - **Todos los equipos** - **Todos los dispositivos móviles** - **Todos los dispositivos administrados de MDM** - **Todos los dispositivos administrados de EAS**	Grupos de seguridad de Azure AD

Jerarquía de grupos

En la consola de Intune, todos los grupos tienen un grupo primario. Los grupos solo pueden contener miembros de su grupo primario. En Azure AD, los grupos secundarios pueden contener miembros que no se incluyen en su grupo primario.

Atributos de grupo

Los atributos son propiedades de dispositivos que se pueden usar para definir grupos. En esta tabla se describe cómo se migran estos criterios a grupos de seguridad de Azure AD.

ATRIBUTO EN INTUNE	ATRIBUTO EN AZURE AD
Atributo de unidad organizativa (UO) para grupos de dispositivos	Atributo de UO para grupos dinámicos.
Atributo de nombre de dominio para grupos de dispositivos	Atributo de nombre de dominio para grupos dinámicos.
Grupo de seguridad como atributo de grupos de usuarios	Los grupos no pueden ser atributos en consultas dinámicas de Azure AD. Los grupos dinámicos solo pueden contener atributos específicos de dispositivo o de usuario.
Atributo de administrador para grupos de usuarios	Regla avanzada para el atributo *manager* en grupos dinámicos

ATRIBUTO EN INTUNE	ATRIBUTO EN AZURE AD
Todos los usuarios del grupo de usuarios primario	Grupo estático con ese grupo como miembro
Todos los dispositivos móviles del grupo de dispositivos primario	Grupo estático con ese grupo como miembro
Todos los dispositivos móviles administrados por Intune	Atributo de tipo de administración con "MDM" como valor del grupo dinámico
Grupos anidados dentro de grupos estáticos	Grupos anidados dentro de grupos estáticos
Grupos anidados dentro de grupos dinámicos	Grupo dinámico con un nivel de anidamiento

¿Qué sucede con las directivas y las aplicaciones que ya ha implementado?

Las directivas y las aplicaciones siguen implementándose en grupos, como antes. En cambio, ahora administra estos grupos desde Azure Portal en lugar de usar la consola de Intune.

Configuración de Intune de la aplicación Classroom para iOS/iPadOS

14/05/2021 • 6 minutes to read

> **NOTE**
> Actualmente, Intune no admite la configuración de la aplicación Classroom. Este artículo solo se aplica a los usuarios que tienen perfiles educativos de iOS/iPadOS en Intune.

Introducción

Classroom es una aplicación que ayuda a los profesores a guiar el aprendizaje y controlar los dispositivos de los estudiantes en el aula. Por ejemplo, la aplicación permite a los profesores:

- Abrir aplicaciones en los dispositivos de los estudiantes
- Bloquear y desbloquear la pantalla de un iPad
- Ver la pantalla del iPad de un estudiante
- Navegar por los iPad de los estudiantes hasta un marcador o el capítulo de un libro
- Mostrar la pantalla del iPad de un estudiante en un televisor Apple

Para configurar Classroom en el dispositivo, debe crear y configurar un perfil educativo de dispositivo iOS/iPadOS para Intune.

Antes de empezar

Tenga en cuenta lo siguiente antes de comenzar a configurar estas opciones:

- Tanto los iPad de los profesores como de los estudiantes deben estar inscritos en Intune.
- Asegúrese de que haya instalado la aplicación Classroom de Apple en el dispositivo del profesor. Puede instalar la aplicación manualmente o usar la administración de aplicaciones de Intune.
- Debe configurar certificados para autenticar las conexiones entre los dispositivos de profesores y alumnos (consulte el paso 2, Creación y asignación de un perfil educativo de iOS/iPadOS en Intune).
- Los iPad de los profesores y estudiantes deben estar en la misma red Wi-Fi y también tener habilitado Bluetooth.
- La aplicación Classroom se ejecuta en dispositivos iPad supervisados que ejecutan iOS/iPadOS 9.3 o una versión posterior.
- En esta versión, Intune admite la administración de un escenario 1:1, donde cada estudiante tiene su propio iPad exclusivo.

Paso 1: importar los datos de la escuela en Azure Active Directory

Use School Data Sync (SDS) de Microsoft para importar los registros de la escuela desde un sistema de información de estudiantes (SIS) existente a Azure Active Directory (Azure AD). SDS sincroniza la información de su SIS y la almacena en Azure AD. Azure AD es un sistema de administración de Microsoft que ayuda a organizar los usuarios y los dispositivos. Luego, puede utilizar estos datos para administrar sus estudiantes y clases. Obtenga más información sobre cómo implementar SDS.

Cómo importar datos con SDS

Puede importar información a SDS mediante uno de los siguientes métodos:

- Archivos CSV: exporte manualmente y compile archivos de valores separados por comas (.csv)
- API de PowerSchool: proveedor de SIS que simplifica la sincronización con Azure AD
- OneRoster: formato CSV que puede exportar y convertir para sincronizar con Azure AD

Obtenga más información

- Obtener más información sobre la experiencia completa de sincronización de datos locales de escuelas en Azure AD
- Obtener más información sobre School Data Sync de Microsoft
- Obtener más información sobre las licencias en Azure Active Directory

Paso 2: Creación y asignación de un perfil educativo de iOS/iPadOS en Intune

Configuración de las opciones generales

1. Inicie sesión en Intune.
2. En el panel **Intune**, elija **Configuración del dispositivo**.
3. En el panel **Configuración del dispositivo**, en la sección **Administrar**, elija **Perfiles**.
4. En el panel Perfiles, elija **Crear perfil**.
5. En el panel **Crear perfil**, rellene los campos **Nombre** y **Descripción** del perfil educativo de iOS/iPadOS.
6. En la lista desplegable **Plataforma**, elija **iOS**.
7. En la lista desplegable **Tipo de perfil**, elija **Educación**.
8. Elija **Configuración** > **Configurar**.

En la siguiente sección, creará certificados para establecer una relación de confianza entre los iPad de profesores y estudiantes. Se utilizan certificados para autenticar sin problemas y de forma silenciosa las conexiones entre los dispositivos sin tener que escribir nombres de usuario ni contraseñas.

> **IMPORTANT**
> Los certificados de profesores y estudiantes que utilice deben ser emitidos por diferentes entidades de certificación (CA). Debe crear dos nuevas CA subordinadas conectadas a la infraestructura de certificados existente; una para los profesores y otra para los estudiantes.

Los perfiles de educación de iOS solo admiten certificados PFX. No se admiten certificados SCEP.

Los certificados creados deben admitir la autenticación de servidor y autenticación de usuario.

Configuración de certificados de profesores

En el panel **Educación**, elija **Certificados de profesor**.

Configuración de certificado raíz de profesor

En **Certificado de raíz de profesor**, elija el botón Examinar. Seleccione el certificado de raíz con una de las siguientes extensiones:

- Extensión .cer (DER o con codificación Base64)
- Extensión. P7B (con o sin cadena completa)

Configuración de certificados de profesores PKCS#12

En **Teacher PKCS#12 certificate** (Certificado de profesor PKCS#12), configure los siguientes valores:

- **Formato de nombre de sujeto**: Intune pone automáticamente el prefijo **leader** a los nombres comunes de los certificados de profesor. Los nombres comunes de los certificados de estudiantes tienen el prefijo

member.

- **Entidad de certificación**: entidad de certificación (CA) empresarial que se ejecuta en una edición Enterprise de Windows Server 2008 R2 o versión posterior. No se admiten CA independientes.
- **Nombre de la entidad de certificación**: escriba el nombre de la entidad de certificación.
- **Nombre de plantilla de certificado**: escriba el nombre de una plantilla de certificado que se haya agregado a una CA emisora.
- **Umbral de renovación (%)** : especifique qué porcentaje de la duración del certificado tiene que quedar para que el dispositivo solicite la renovación del certificado.
- **Período de validez del certificado**: especifique la cantidad de tiempo que queda antes de que expire el certificado. Puede especificar un valor inferior al período de validez de la plantilla de certificado especificada, pero no superior. Por ejemplo, si el período de validez del certificado en la plantilla de certificado es de dos años, puede especificar un valor de un año, pero no un valor de cinco años. El valor también debe ser menor que el período de validez restante del certificado de la CA emisora.

Cuando haya terminado la configuración de los certificados, haga clic en **Aceptar**.

Configuración de certificados de estudiantes

1. En el panel **Educación**, elija **Certificados de alumno**.
2. En el panel **Certificados de alumno** de la lista **Tipos de certificados de dispositivo de alumno**, elija **1:1**.

Configuración de certificado raíz de estudiantes

En **Certificado de raíz de alumno**, elija el botón Examinar. Seleccione el certificado de raíz con una de las siguientes extensiones:

- Extensión .cer (DER o con codificación Base64)
- Extensión. P7B (con o sin cadena completa)

Configuración de certificados de estudiantes PKCS#12

En **Student PKCS#12 certificate** (Certificado de estudiante PKCS#12), configure los siguientes valores:

- **Formato de nombre de sujeto**: Intune pone automáticamente el prefijo **leader** a los nombres comunes de los certificados de profesor. Los nombres comunes de los certificados de estudiantes tienen el prefijo **member**.
- **Entidad de certificación**: entidad de certificación (CA) empresarial que se ejecuta en una edición Enterprise de Windows Server 2008 R2 o versión posterior. No se admiten CA independientes.
- **Nombre de la entidad de certificación**: escriba el nombre de la entidad de certificación.
- **Nombre de plantilla de certificado**: escriba el nombre de una plantilla de certificado que se haya agregado a una CA emisora.
- **Umbral de renovación (%)** : especifique qué porcentaje de la duración del certificado tiene que quedar para que el dispositivo solicite la renovación del certificado.
- **Período de validez del certificado**: especifique la cantidad de tiempo que queda antes de que expire el certificado. Puede especificar un valor inferior al período de validez de la plantilla de certificado especificada, pero no superior. Por ejemplo, si el período de validez del certificado en la plantilla de certificado es de dos años, puede especificar un valor de un año, pero no un valor de cinco años. El valor también debe ser menor que el período de validez restante del certificado de la CA emisora.

Cuando haya terminado la configuración de los certificados, haga clic en **Aceptar**.

Finalizar

1. En el panel **Educación**, elija Aceptar.
2. En el panel **Crear perfil**, elija **Crear**.

Se creará el perfil y aparecerá en el panel con la lista de perfiles.

Asigne el perfil a los dispositivos de estudiante en los grupos de aula que se crearon al sincronizar los datos de la escuela con Azure AD (consulte Asignación de perfiles de dispositivo.

Pasos siguientes

Ahora cuando los profesores utilicen la aplicación Classroom, tendrán el control total sobre los dispositivos de los estudiantes.

Para obtener más información sobre la aplicación Classroom, vea Ayuda de Classroom en el sitio web de Apple.

Si quiere configurar dispositivos iPad compartidos para los estudiantes, vea Cómo configurar las opciones de educación de Intune para los dispositivos iPad compartidos.

Configuración del entorno educativo de Intune para dispositivos iPad compartidos

14/05/2021 • 8 minutes to read

> **NOTE**
> Actualmente, Intune no admite la configuración de la aplicación Classroom. Este artículo solo se aplica a los usuarios que tienen perfiles educativos de iOS/iPadOS en Intune.

Intune admite la aplicación Classroom para iOS/iPadOS, que ayuda a los profesores a guiar el aprendizaje y controlar los dispositivos de los alumnos en el aula. Además, para la aplicación Classroom, Apple admite la capacidad de que los dispositivos iPad de los estudiantes se configure de manera que varios estudiantes puedan compartir un único dispositivo. Este documento le guía para conseguir este objetivo con Intune.

Para obtener información sobre la configuración de los dispositivos iPad (1:1) dedicados para usar la aplicación Classroom, vea Configuración de Intune para la aplicación Classroom para iOS/iPadOS.

Antes de empezar

Los requisitos previos para usar las funciones de iPad compartidas son:

- Instale Apple School Manager y School Data Sync (SDS).
- Como parte de la instalación de Apple School Manager, configure identificadores de Apple administrados para los estudiantes. Más información sobre los identificadores de Apple administrados.
- Cree un perfil de inscripción para los números de serie del dispositivo sincronizado desde Apple School Manager.

Paso 1: importar los datos de la escuela en Azure Active Directory

Use School Data Sync (SDS) de Microsoft para importar los registros de la escuela desde un sistema de información de estudiantes (SIS) existente a Azure Active Directory (Azure AD). SDS sincroniza la información de su SIS y la almacena en Azure AD. Azure AD es un sistema de administración de Microsoft que ayuda a organizar los usuarios y los dispositivos. Luego, puede utilizar estos datos para administrar sus estudiantes y clases. Obtenga más información sobre cómo implementar SDS.

Cómo importar datos con SDS

Puede importar información a SDS mediante uno de los siguientes métodos:

- Archivos CSV: exporte manualmente y compile archivos de valores separados por comas (.csv)
- API de PowerSchool: proveedor de SIS que simplifica la sincronización con Azure AD
- OneRoster: formato CSV que puede exportar y convertir para sincronizar con Azure AD

Obtenga más información

- Obtener más información sobre la experiencia completa de sincronización de datos locales de escuelas en Azure AD
- Obtener más información sobre School Data Sync de Microsoft
- Obtener más información sobre las licencias en Azure Active Directory

Paso 2: Creación y asignación de un perfil educativo de iOS/iPadOS en Intune

Configuración de las opciones generales

1. Inicie sesión en Intune.
2. En el panel **Intune**, elija **Configuración del dispositivo**.
3. En el panel **Configuración del dispositivo**, en la sección **Administrar**, elija **Perfiles**.
4. En el panel Perfiles, elija **Crear perfil**.
5. En el panel **Crear perfil**, rellene los campos **Nombre** y **Descripción** del perfil educativo de iOS/iPadOS.
6. En la lista desplegable **Plataforma**, elija **iOS**.
7. En la lista desplegable **Tipo de perfil**, elija **Educación**.
8. Elija **Configuración** > **Configurar**.

A continuación, necesita certificados para establecer una relación de confianza entre los iPad de profesores y estudiantes. Se utilizan certificados para autenticar sin problemas y de forma silenciosa las conexiones entre los dispositivos sin tener que escribir nombres de usuario ni contraseñas.

> **IMPORTANT**
> Los certificados de profesores y estudiantes que use deben ser emitidos por diferentes entidades de certificación (CA). Debe crear dos nuevas CA subordinadas conectadas a la infraestructura de certificados existente; una para los profesores y otra para los estudiantes.

Los perfiles de educación de iOS solo admiten certificados PFX. No se admiten certificados SCEP.

Los certificados que crea deben admitir la autenticación de servidor además de la autenticación de usuario.

Configuración de certificados de profesores

En el panel **Educación**, elija **Certificados de profesor**.

Configuración de certificado raíz de profesor

En **Teacher root certificate** (Certificado raíz de profesor), elija el botón Examinar para seleccionar el certificado raíz del profesor con la extensión .cer (DER o Base64 codificado) o .P7B (con o sin la cadena completa).

Configuración de certificados de profesores PKCS#12

En **Teacher PKCS#12 certificate** (Certificado de profesor PKCS#12), configure los siguientes valores:

- **Formato de nombre de sujeto**: Intune agrega automáticamente el prefijo **líder**, para el certificado del profesor, y **miembro**, para el certificado de los estudiantes, a los nombres comunes del certificado.
- **Entidad de certificación**: entidad de certificación (CA) empresarial que se ejecuta en una edición Enterprise de Windows Server 2008 R2 o versión posterior. No se admiten CA independientes.
- **Nombre de la entidad de certificación**: escriba el nombre de la entidad de certificación.
- **Nombre de plantilla de certificado**: escriba el nombre de una plantilla de certificado que se haya agregado a una CA emisora.
- **Umbral de renovación (%)** : especifique qué porcentaje de la duración del certificado tiene que quedar para que el dispositivo solicite la renovación del certificado.
- **Período de validez del certificado**: especifique la cantidad de tiempo que queda antes de que expire el certificado. Puede especificar un valor inferior al período de validez de la plantilla de certificado especificada, pero no superior. Por ejemplo, si el período de validez del certificado en la plantilla de certificado es de dos años, puede especificar un valor de un año, pero no un valor de cinco años. El valor también debe ser menor que el período de validez restante del certificado de la CA emisora.

Cuando haya terminado la configuración de los certificados de profesores, seleccione **Aceptar**.

Configuración de certificados de estudiantes

1. En el panel **Educación**, elija **Certificados de alumno**.
2. En el panel **Certificados de alumno**, en la lista **Tipo de certificados de dispositivo de alumno**, seleccione **iPad compartido**.

Configuración de certificado raíz de estudiantes

En **Certificado raíz de dispositivo**, seleccione el botón Examinar para seleccionar el certificado raíz del estudiante con la extensión .cer (DER o Base64 codificado) o .P7B (con o sin la cadena completa).

Configuración de certificados de dispositivos PKCS#12

En **Student PKCS#12 certificate** (Certificado de estudiante PKCS#12), configure los siguientes valores:

- **Formato de nombre de sujeto**: Intune agrega automáticamente el prefijo líder, para el certificado del profesor, y miembro, para el certificado de los dispositivos, a los nombres comunes del certificado.
- **Entidad de certificación**: entidad de certificación (CA) empresarial que se ejecuta en una edición Enterprise de Windows Server 2008 R2 o versión posterior. No se admiten CA independientes.
- **Nombre de la entidad de certificación**: escriba el nombre de la entidad de certificación.
- **Nombre de plantilla de certificado**: escriba el nombre de una plantilla de certificado que se haya agregado a una CA emisora.
- **Umbral de renovación (%)** : especifique qué porcentaje de la duración del certificado tiene que quedar para que el dispositivo solicite la renovación del certificado.
- **Período de validez del certificado**: especifique la cantidad de tiempo que queda antes de que expire el certificado. Puede especificar un valor inferior al período de validez de la plantilla de certificado especificada, pero no superior. Por ejemplo, si el período de validez del certificado en la plantilla de certificado es de dos años, puede especificar un valor de un año, pero no un valor de cinco años. El valor también debe ser menor que el período de validez restante del certificado de la CA emisora.

Cuando haya terminado la configuración de los certificados, haga clic en **Aceptar**.

Completar la configuración de certificado

1. En el panel **Educación**, elija **Aceptar**.
2. En el panel **Crear perfil**, elija **Crear**.

Se creará el perfil y aparecerá en el panel con la lista de perfiles.

Paso 3: Crear una categoría de dispositivo

1. Inicie sesión en Intune.
2. En el panel **Intune**, seleccione **Inscripción de dispositivos**.
3. En el panel **Inscripción de dispositivos: introducción**, elija **Categorías de dispositivos**.
4. En el panel **Inscripción de dispositivos: categorías de dispositivos**, elija **Crear**.
5. En el panel **Crear categoría de dispositivos**, escriba un **Nombre** y una **Descripción** para la categoría.
6. En el panel **Crear categoría de dispositivos**, seleccione **Crear**.

La categoría de dispositivos se crea en el panel **Inscripción: categorías de dispositivos**.

Paso 4: Crear un grupo dinámico

1. Inicie sesión en Intune.
2. En el panel **Intune**, elija **Grupos**.
3. En el panel **Usuarios y grupos: todos los grupos**, seleccione **Nuevo grupo**.
4. En el panel **Grupo**, elija un **Tipo de grupo** y, después, escriba un **Nombre** y una **Descripción** para el

grupo.

5. En la lista desplegable **Tipo de pertenencia**, seleccione **Dispositivo dinámico**.
6. Seleccione **Miembros del dispositivo dinámico** para crear reglas de pertenencia.
7. En el panel **Reglas de pertenencia dinámica**:
8. Seleccione **deviceCategory** de la lista desplegable **Lugar donde agregar dispositivos**.
9. Seleccione **Igual a**.
10. Escriba la categoría de dispositivos que ha creado en el cuadro de texto en blanco.
11. En el panel **Reglas de pertenencia dinámica**, seleccione **Agregar consulta**.
12. En el panel **Grupo**, elija **Crear**.

El grupo dinámico se crea en el panel **Usuarios y grupos: todos los grupos**.

Paso 5: Asignar un dispositivo a una categoría (Carros)

1. Inicie sesión en Intune.
2. En el panel **Intune**, elija **Dispositivos**.
3. En el panel **Dispositivos**, seleccione **Todos los dispositivos**.
4. En el panel **Dispositivos: todos los dispositivos**, seleccione un dispositivo.
5. En el panel Dispositivos, elija **Propiedades**.
6. En el panel Propiedades del dispositivo, escriba la categoría de dispositivo en el cuadro de texto **Categoría de dispositivo**.
7. En el panel Dispositivos, elija **Guardar**.

Ahora el dispositivo está asociado a la categoría de dispositivo. Repita este proceso para todos los dispositivos que quiera asociar a la categoría de dispositivo que ha creado.

Paso 6: Crear perfiles de aulas

1. Inicie sesión en Intune.
2. En el panel **Intune**, elija **Configuración del dispositivo**.
3. En el panel **Configuración del dispositivo**, seleccione **Administrar** > **Perfiles de carro**.
4. En el panel Perfiles, elija **Crear perfil**.
5. En el panel **Crear asociación**, escriba un **Nombre** y una **Descripción**.
6. Pulse **Seleccionar clases** > **Configurar** para asociar grupos al perfil de carro.
7. Seleccione las clases que se van a incluir en el perfil de carro y, después, pulse **Seleccionar**.
8. Pulse **Seleccionar carros** > **Configurar** para asociar grupos al perfil de carro.
9. Seleccione los grupos que se van a incluir en el perfil de carro y, después, pulse **Seleccionar**.
10. En el panel **Crear asociación**, seleccione **Guardar** para guardar el perfil de carro.

Se creará el perfil y aparecerá en el panel con la lista de perfiles.

Paso 7: Asignar el perfil de carro a las clases

1. Inicie sesión en Intune.
2. En el panel **Intune**, elija **Configuración del dispositivo**.
3. En el panel **Configuración del dispositivo**, elija **Supervisar** > **Estado de la asignación**.
4. En el panel **Estado de la asignación**, seleccione el **Perfil de carro** que ha creado.
5. En el panel **Perfil de carro**, elija **Asignaciones** y, después, en **Incluir**, elija **Seleccionar grupos para incluir**.
6. Seleccione las clases que quiere que se dirijan al perfil de carro (no seleccione un grupo) y, después, pulse

Seleccionar.

7. Cuando termine, elija **Guardar**.

La asignación se completa e Intune implementa el perfil de Classroom a los dispositivos de destino basándose en la asignación del aula.

Pasos siguientes

Ahora los estudiantes pueden compartir dispositivos entre ellos y pueden seleccionar cualquier iPad del aula, iniciar sesión con un PIN y personalizarlo con su contenido. Para obtener más información sobre los dispositivos iPad compartidos, vea el sitio web de Apple.

¿Qué ha ocurrido con el cliente de software de PC de Intune?

14/05/2021 • 5 minutes to read

WARNING

La administración de equipos heredados ya no se admite a partir del 16 de octubre de 2020. Actualice los dispositivos a Windows 10 y vuelva a inscribirlos en MDM de Intune para administrarlos mediante Intune. Los dispositivos administrados con el cliente de software de PC dejarán de recibir aplicaciones y actualizaciones de seguridad y ya no podrá configurarlas.

Anuncio de desuso

A continuación se ofrece información del anuncio de desuso original publicado en el blog del equipo de soporte técnico de Intune:

IMPORTANT

Microsoft Intune retirará la compatibilidad con la consola de Intune basada en Silverlight el 15 de octubre de 2020. Esta retirada incluye el fin del soporte para el cliente de software de equipos configurados en la consola de Silverlight (también conocido como agente de equipo) que se usa para la administración de PC Windows. Además, Intune finalizará la oferta de licencia del complemento de almacenamiento de Intune, que solo se usaba para el almacenamiento de aplicaciones en Silverlight. Traslade la administración diaria de Intune de Silverlight al Centro de administración de Microsoft Endpoint Manager.

¿Cómo me afecta esto a mí?

Nuestra telemetría nos indica que tiene dispositivos Windows administrados por el cliente de software de PC que deberán inscribirse en MDM para que los siga administrando Intune a partir de la fecha indicada anteriormente.

¿Qué tengo que hacer?

1. Abra el Centro de administración de Microsoft Endpoint Manager.
2. Vuelva a crear las directivas de Windows 10 existentes como directivas MDM. Tenga en cuenta que muchas directivas de administración de dispositivos se migraron hace varios años como parte de la migración de la consola de administración. Compruebe la administración de dispositivos en Azure antes de crear directivas.
3. Revise los informes en la consola de administración de Microsoft Intune para buscar los dispositivos administrados por el cliente de software de PC de Intune.
4. Determine el método de inscripción moderno adecuado para su organización. Para obtener más información, consulte Métodos de inscripción de Intune para dispositivos Windows.
5. Anule la inscripción de dispositivos con el cliente de software de PC de Intune y vuelva a inscribirlos con MDM de Intune. Le recomendamos encarecidamente que actualice a la versión más reciente de Windows 10. A partir del 14 de enero de 2020, Intune ya no será compatible con Windows 7.
6. Agregue aplicaciones a MDM de Intune. Para obtener más información, consulte Incorporación de aplicaciones a Microsoft Intune.

Tenga en cuenta lo siguiente : Si actualmente tiene licencias de complementos de almacenamiento de Intune, con MDM de Intune no es necesario administrar los equipos con Windows 10.

Este cambio le permitirá aprovechar las capacidades mejoradas que están disponibles a través del canal de MDM para la administración de Windows. Le recomendamos que realice la migración lo antes posible, a más tardar el 15 de octubre de 2020. Después de esa fecha, ya no se podrá acceder a la consola de Intune basada en Silverlight. Los equipos administrados con el cliente de software de PC dejarán de recibir aplicaciones y actualizaciones de seguridad y ya no podrán configurarse.

Póngase en contacto con su socio de registro o de soporte técnico para obtener ayuda.

Desinstalación del cliente de software de PC de Intune

Desde un símbolo del sistema con privilegios elevados en el dispositivo cuya inscripción se va a anular, ejecute uno de los siguientes comandos.

Método 1

```
"C:\Program Files\Microsoft\OnlineManagement\Common\ProvisioningUtil.exe" /UninstallAgents /MicrosoftIntune
```

Método 2

En cada SKU de Windows están instalados los agentes siguientes:

```
wmic product where name="Microsoft Endpoint Protection Management Components" call uninstall
wmic product where name="Microsoft Intune Notification Service" call uninstall
wmic product where name="System Center 2012 - Operations Manager Agent" call uninstall
wmic product where name="Microsoft Online Management Policy Agent" call uninstall
wmic product where name="Microsoft Policy Platform" call uninstall
wmic product where name="Microsoft Security Client" call uninstall
wmic product where name="Microsoft Online Management Client" call uninstall
wmic product where name="Microsoft Online Management Client Service" call uninstall
wmic product where name="Microsoft Easy Assist v2" call uninstall
wmic product where name="Microsoft Intune Monitoring Agent" call uninstall
wmic product where name="Windows Intune Endpoint Protection Agent" call uninstall
wmic product where name="Windows Firewall Configuration Provider" call uninstall
wmic product where name="Microsoft Intune Center" call uninstall
wmic product where name="Microsoft Online Management Update Manager" call uninstall
wmic product where name="Microsoft Online Management Agent Installer" call uninstall
wmic product where name="Microsoft Intune" call uninstall
wmic product where name="Windows Endpoint Protection Management Components" call uninstall
wmic product where name="Windows Intune Notification Service" call uninstall
wmic product where name="System Center 2012 - Operations Manager Agent" call uninstall
wmic product where name="Windows Online Management Policy Agent" call uninstall
wmic product where name="Windows Policy Platform" call uninstall
wmic product where name="Windows Security Client" call uninstall
wmic product where name="Windows Online Management Client" call uninstall
wmic product where name="Windows Online Management Client Service" call uninstall
wmic product where name="Windows Easy Assist v2" call uninstall
wmic product where name="Windows Intune Monitoring Agent" call uninstall
wmic product where name="Windows Intune Endpoint Protection Agent" call uninstall
wmic product where name="Windows Firewall Configuration Provider" call uninstall
wmic product where name="Windows Intune Center" call uninstall
wmic product where name="Windows Online Management Update Manager" call uninstall
wmic product where name="Windows Online Management Agent Installer" call uninstall
wmic product where name="Windows Intune" call uninstall
```

TIP

Al anular la inscripción del cliente de software de PC de Intune, se conserva un registro obsoleto del lado del servidor para el dispositivo. El proceso de anulación de la suscripción es asincrónico y hay nueve agentes que desinstalar, por lo que puede tardar hasta 30 minutos en completarse.

Comprobar el estado de la anulación de la suscripción

Compruebe "%ProgramFiles%\Microsoft\OnlineManagement" y asegúrese de que solo se muestran los siguientes directorios a la izquierda:

- AgentInstaller
- Registros
- Actualizaciones
- Comunes

Quitar la carpeta OnlineManagement

El proceso de anulación de la suscripción no elimina la carpeta OnlineManagement. Espere 30 minutos después de la desinstalación y luego ejecute este comando. Si se ejecuta demasiado pronto, la desinstalación podría quedar en un estado desconocido. Para quitar la carpeta, abra una ventana de símbolo del sistema con privilegios elevados y ejecute:

```
rd /s /q %ProgramFiles%\Microsoft\OnlineManagement
```

Recursos

Anuncio de desuso en el blog de soporte técnico de Intune

Pasos siguientes

Métodos de inscripción de Intune para dispositivos Windows

¿Qué es la inscripción de dispositivos?

14/05/2021 • 4 minutes to read

Para obtener acceso a los recursos profesionales o educativos desde su dispositivo, debe inscribirlo con la aplicación Portal de empresa de Intune o con la aplicación Microsoft Intune.

Durante la inscripción de dispositivos:

- El dispositivo se registra en la organización. Este paso garantiza que está autorizado para acceder al correo electrónico, las aplicaciones y la red Wi-Fi de su organización.
- Las directivas de administración de dispositivos de su organización se aplican en el dispositivo. Estas directivas pueden incluir requisitos sobre aspectos como las contraseñas de los dispositivos y el cifrado. El propósito de estos requisitos es mantener el dispositivo y los datos de la organización seguros frente a posibles accesos no autorizados.

Una vez que actualice la configuración del dispositivo para satisfacer los requisitos de la organización, la inscripción se habrá completado. Podrá iniciar sesión de forma segura en su cuenta profesional o educativa desde prácticamente cualquier lugar.

En este artículo se describen otros aspectos de la inscripción, como de qué manera obtener las aplicaciones, cuáles son los dispositivos admitidos y cómo eliminar o restablecer un dispositivo.

Portal de empresa y la aplicación Microsoft Intune

Portal de empresa y la aplicación Microsoft Intune avisan de los cambios en la directiva o la configuración, lo que permite tomar medidas sin perder el acceso al material educativo o profesional.

La aplicación Portal de empresa mantiene la información personal y profesional por separado, con lo cual puede seguir siendo productivo y mantener la concentración. También pone a su disposición aplicaciones profesionales y educativas para que pueda buscar e instalar las que sean relevantes según su línea de trabajo.

Obtención del Portal de empresa

En algunos casos, la organización instalará la aplicación Portal de empresa en el dispositivo. La aplicación también está disponible para instalarse desde tiendas de aplicaciones, como Microsoft Store, App Store y Google Play Store. Para acceder a la aplicación desde un explorador web, inicie sesión en el sitio web del Portal de empresa con su cuenta profesional o educativa.

Obtención de la aplicación de Microsoft Intune

Si es necesario usar la aplicación Microsoft Intune, su organización la instalará en el dispositivo.

¿Cuál es la diferencia entre las aplicaciones y el sitio web?

La aplicación Portal de empresa está disponible para dispositivos Windows 10, iOS, macOS y Android. Se integra perfectamente con la plataforma correspondiente del dispositivo. Se puede acceder a la versión del sitio web desde cualquier dispositivo y este le ofrece la misma experiencia universal sin importar el dispositivo que use.

La aplicación Microsoft Intune está pensada para usarse en los dispositivos Android que sean propiedad de la empresa, y no tiene sitio web.

¿Qué tipo de dispositivos se pueden inscribir con Portal de empresa?

Se pueden inscribir los siguientes dispositivos con Portal de empresa:

- Dispositivos Windows
  - Windows 10 Móvil
  - Windows 10 Escritorio
  - Windows 8.1
- Dispositivos Apple
  - iOS
  - macOS
- Dispositivos Android

¿Qué tipo de dispositivos se pueden inscribir con la aplicación Microsoft Intune?

Se pueden inscribir dispositivos Android propiedad de la empresa que la organización haya configurado para usarse con la aplicación. La aplicación es compatible con Android 6.0 y versiones posteriores.

¿Se puede quitar un dispositivo del Portal de empresa?

Puede quitar o restablecer un dispositivo del Portal de empresa. Hay una diferencia entre **quitar** y **restablecer**.

Durante la eliminación del dispositivo, el Portal de empresa anula la inscripción y el registro del dispositivo. Ese dispositivo dejará de poder acceder al Portal de empresa. También se pueden quitar datos profesionales o educativos.

Durante el restablecimiento de un dispositivo, el Portal de empresa intenta devolver el dispositivo a la configuración predeterminada del fabricante. Todos los datos profesionales o educativos y todos los datos personales se quitan del dispositivo. Un restablecimiento es útil si, por ejemplo, pierde el dispositivo. Puede restablecerlo de forma remota desde el sitio web del Portal de empresa.

¿Se puede quitar un dispositivo desde la aplicación Microsoft Intune?

No, no hay ninguna manera de quitar un dispositivo propiedad de la empresa de la aplicación Microsoft Intune.

¿Qué ocurre si no aparece mi dispositivo en el Portal de empresa o en la aplicación Microsoft Intune?

Para ver un dispositivo en el Portal de empresa, antes debe inscribirlo. Si, tras inscribirlo, sigue sin ver todos los dispositivos, pruebe a sincronizar o comprobar el acceso a través del Portal de empresa. No podrá ver los dispositivos que posee y administra su empresa.

En la aplicación Microsoft Intune, solo verá el dispositivo que esté usando actualmente. Los demás dispositivos inscritos no estarán visibles en la aplicación.

¿Dónde más se puede obtener ayuda?

Consulte los artículos de este conjunto de documentos para ver explicaciones y ayuda paso a paso. En la tabla de contenido, seleccione entre las categorías de administración de dispositivos de Android, iOS, Windows o macOS. Luego, seleccione **Actualizar configuración del dispositivo** para ver una lista de los artículos de procedimientos que abordan los mensajes comunes del Portal de empresa.

También puede ponerse en contacto con el personal de soporte técnico de TI. El Portal de empresa y la aplicación Microsoft Intune ofrecen páginas de ayuda y de soporte técnico con información de contacto y las diversas formas de informar de un problema. La información de contacto de TI también está disponible en el

sitio web del Portal de empresa de la organización.

Pasos siguientes

Si está listo para acceder a su cuenta profesional o educativa, siga las instrucciones de la organización para inscribir su dispositivo. También encontrará instrucciones de inscripción paso a paso en los siguientes artículos.

- Inscripción de dispositivos Windows 10
- Inscripción de su dispositivo Android
- Inscripción con el perfil de trabajo Android
- Inscripción con la aplicación Microsoft Intune
- Inscripción de dispositivos iOS
- Inscripción de un dispositivo iOS proporcionado por la organización
- Inscripción de dispositivos macOS
- Inscripción de un dispositivo macOS proporcionado por la organización