Contents

¿Qué es Microsoft Defender para Empresas?

21/06/2022 • 2 minutes to read

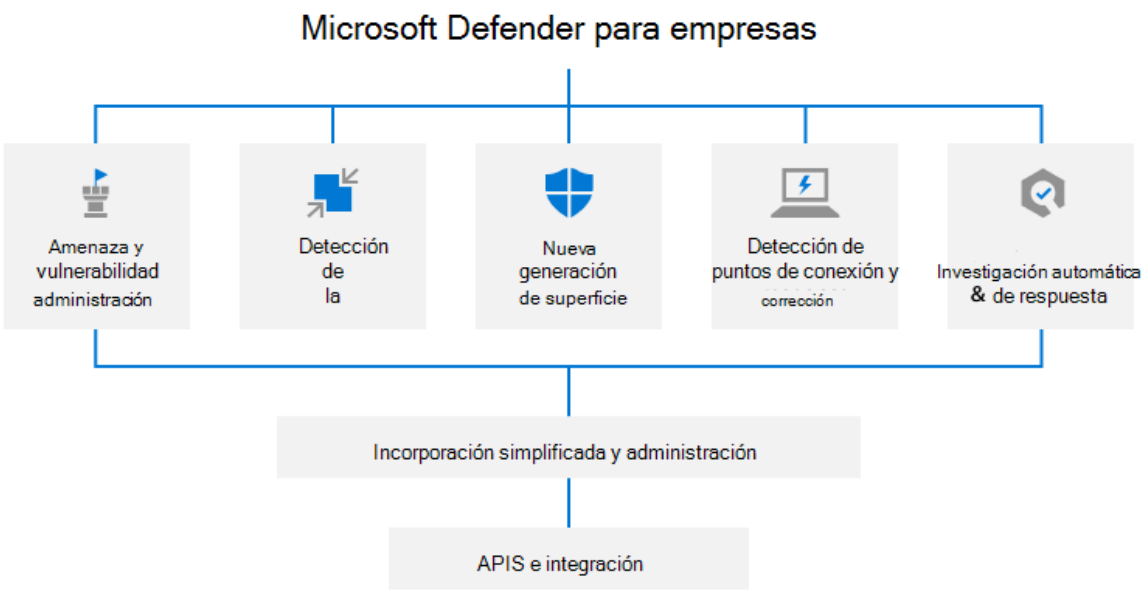
Microsoft Defender para Empresas es una nueva solución de seguridad de puntos de conexión diseñada especialmente para la pequeña y mediana empresa (hasta 300 empleados). Con esta solución de seguridad de punto de conexión, los dispositivos de su empresa están mejor protegidos contra ransomware, malware, suplantación de identidad (phishing) y otras amenazas.

En este artículo se describe lo que se incluye en Defender para empresas, con vínculos para obtener más información sobre estas características y funcionalidades.

Vídeo: protección Enterprise para pequeñas y medianas empresas

Vea el siguiente vídeo para obtener más información sobre Defender para empresas:

Qué se incluye con Defender para empresas



Con Defender para empresas, puede ayudar a proteger los dispositivos y los datos que usa su empresa con:

- **Enterprise nivel de seguridad**. Defender for Business ofrece eficaces funcionalidades de seguridad de puntos de conexión de nuestra solución de Microsoft Defender para punto de conexión líder del sector y optimiza esas funcionalidades para que los administradores de TI admitan pequeñas y medianas empresas.
- **Una solución de seguridad fácil de usar**. Defender for Business ofrece experiencias simplificadas que le guían a la acción con recomendaciones e información sobre la seguridad de los puntos de conexión. No se requiere ningún conocimiento especializado, ya que Defender for Business ofrece directivas de seguridad predeterminadas y de configuración basadas en asistentes diseñadas para ayudar a proteger los dispositivos de su empresa desde el primer día.

- **Flexibilidad para su entorno**. Defender for Business puede trabajar con su entorno empresarial, tanto si usa Microsoft Intune como si es nuevo en Microsoft Cloud. Defender para empresas funciona con componentes integrados en Windows y con aplicaciones para dispositivos macOS, iOS y Android.
- **Integración con Microsoft 365 Lighthouse**. Si es un proveedor de servicios administrados (MSP) que usa Microsoft 365 Lighthouse, hay más funcionalidades disponibles. Si los clientes usan Microsoft 365 Empresa Premium junto con Defender para empresas, puede ver incidentes de seguridad y alertas entre los inquilinos de clientes que se incorporan a Microsoft 365 Lighthouse.

Uso de esta guía

Esta guía está pensada para:

- **Proporcione información general de Defender para empresas para** que sepa lo que se incluye y cómo funciona.
  - Use este artículo como punto de partida
  - Comparación de las características de seguridad de Microsoft Defender para Empresas con otros planes
  - Obtenga información sobre cómo obtener Microsoft Defender para Empresas
- **Tutorial sobre la configuración y configuración de las funcionalidades de protección contra amenazas**
  - Use el cuaderno de estrategias de prueba: Microsoft Defender para Empresas
  - Más información sobre el proceso de configuración simplificado
  - Vea cómo configurar Defender para empresas
- **Ayuda para empezar a usar Defender para empresas**, empezando por el portal de Microsoft 365 Defender
  - Navegar por el portal de Microsoft 365 Defender
  - Probar escenarios, tutoriales y simulaciones
- **Proporcionar instrucciones sobre la administración de dispositivos y directivas de seguridad**
  - Monitorear o administrar dispositivos
  - Ver o editar las directivas de seguridad

Pasos siguientes

- Pruebe la guía interactiva: Comenzar con Defender para empresas
- Obtenga más información sobre el proceso de configuración simplificado en Microsoft Defender para Empresas
- Obtenga información sobre cómo obtener Microsoft Defender para Empresas

Proceso de configuración simplificado en Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

Microsoft Defender para Empresas cuenta con un proceso de configuración simplificado, diseñado especialmente para pequeñas y medianas empresas. Esta experiencia elimina las conjeturas de la incorporación y administración de dispositivos, con una experiencia similar a un asistente y directivas predeterminadas diseñadas para proteger los dispositivos de la empresa desde el primer día. **Se recomienda usar el proceso de configuración simplificado; sin embargo, no se limita a esta opción**.

Cuando se trata de incorporar dispositivos y configurar opciones de seguridad para los dispositivos de su empresa, puede elegir entre varias experiencias:

- Proceso de configuración simplificado en Microsoft Defender para Empresas (*recomendado*)
- Microsoft Intune (incluido en Microsoft 365 Empresa Premium)

Qué hacer

1. Revise las opciones de configuración y configuración
2. Más información sobre el proceso de configuración simplificado en Defender para empresas
3. Continúe con los pasos siguientes.

Revise las opciones de configuración y configuración

En la tabla siguiente se describe cada experiencia:

EXPERIENCIA DEL PORTAL	DESCRIPCIÓN
La experiencia de configuración simplificada en el portal de Microsoft 365 Defender (https://security.microsoft.com) (*Esta es la opción recomendada para la mayoría de los clientes*)	La experiencia de configuración simplificada incluye una experiencia similar a un asistente para ayudarle a configurar Defender for Business. Para más información, consulte Uso del asistente para configurar Microsoft Defender para Empresas. La configuración simplificada también incluye directivas y opciones de seguridad predeterminadas para ayudarle a proteger los dispositivos de su empresa en cuanto se incorporan a Defender for Business. Puede ver las directivas predeterminadas y, si es necesario, editarlas para satisfacer sus necesidades empresariales. Para más información, consulte Visualización o edición de directivas de dispositivo en Microsoft Defender para Empresas. Con la experiencia simplificada, el equipo de seguridad usa el portal de Microsoft 365 Defender como tienda integral para: - Configuración y configuración de Defender para empresas - Visualización y administración de incidentes - Respuesta y mitigación de amenazas - Visualización de informes - Revisar acciones pendientes o completadas

EXPERIENCIA DEL PORTAL	DESCRIPCIÓN
Centro de administración de Microsoft Endpoint Manager (https://endpoint.microsoft.com)	Microsoft Intune es un proveedor de administración de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM) basado en la nube para aplicaciones y dispositivos. Intune no se incluye en la versión independiente de Defender for Business; sin embargo, Microsoft 365 Empresa Premium incluye Intune. Si ya usa Intune, puede usar el centro de administración de Endpoint Manager para administrar dispositivos, como teléfonos móviles, tabletas y portátiles. Consulte Microsoft Intune: Administración de dispositivos.

Por qué se recomienda usar el proceso de configuración simplificado

Se recomienda usar el proceso de configuración simplificado en Microsoft Defender para Empresas para la mayoría de los clientes.

- El proceso de configuración simplificado se simplifica especialmente para pequeñas y medianas empresas.
- Defender for Business no requiere conocimientos técnicos ni conocimientos especiales profundos.
- Con las directivas y la configuración de seguridad predeterminadas, los dispositivos se protegen en cuanto se incorporan.
- La experiencia simplificada en el portal de Microsoft 365 Defender facilita la incorporación de dispositivos y su administración.
- Las directivas predeterminadas se incluyen para que los dispositivos de la empresa estén protegidos en cuanto se incorporen.
- Puede mantener la configuración predeterminada tal y como están o realizar cambios para satisfacer sus necesidades empresariales.
- Puede agregar directivas nuevas y personalizadas para satisfacer sus necesidades empresariales.

Pasos siguientes

- Configuración y configuración de Microsoft Defender para Empresas
- Comenzar mediante Microsoft Defender para Empresas

Comparación de características de seguridad en planes de Microsoft 365 para pequeñas y medianas empresas

21/06/2022 • 4 minutes to read

Microsoft ofrece una amplia variedad de soluciones y servicios en la nube, incluidos varios planes diferentes para pequeñas y medianas empresas. Por ejemplo, Microsoft 365 Empresa Premium incluye funcionalidades de administración de dispositivos y seguridad, junto con características de productividad, como Office aplicaciones. Este artículo está diseñado para ayudar a aclarar qué características de seguridad, como la protección de dispositivos, se incluyen en Microsoft 365 Empresa Premium, Microsoft Defender para Empresas y Microsoft Defender para punto de conexión.

Use este artículo para:

- Comparar Microsoft Defender para Empresas (independiente) con Microsoft 365 Empresa Premium
- Comparación de Defender para empresas (independiente) con Microsoft Defender para punto de conexión ofertas empresariales

No es necesario tener una suscripción Microsoft 365 para comprar y usar Microsoft Defender para Empresas. Microsoft Defender para Empresas se incluye en Microsoft 365 Empresa Premium y está disponible como una solución de seguridad independiente para pequeñas y medianas empresas. Si ya tiene Microsoft 365 Empresa Básico o Estándar, considere la posibilidad de agregar actualizaciones a Microsoft 365 Empresa Premium o agregar Microsoft Defender para Empresas para obtener más funcionalidades de protección contra amenazas.

Compare las características de seguridad de Microsoft Defender para Empresas con Microsoft 365 Empresa Premium

> **NOTE**
> Este artículo está diseñado para proporcionar información general de alto nivel sobre las características de protección contra amenazas incluidas en Microsoft Defender para Empresas (como un plan independiente) y Microsoft 365 Empresa Premium (que incluye Defender para empresas). Este artículo no está pensado para servir como descripción del servicio o documento de contrato de licencia. Para obtener más información, consulte la guía de licencias de Microsoft 365 para la seguridad & cumplimiento.

A partir del 1 de marzo de 2022, Defender for Business se incluye en Microsoft 365 Empresa Premium. Defender para empresas también está disponible como una suscripción independiente. En la tabla siguiente se comparan las características y funcionalidades de seguridad de Defender para empresas (independiente) con Microsoft 365 Empresa Premium.

CARACTERÍSTICA O FUNCIONALIDAD	MICROSOFT DEFENDER PARA EMPRESAS (INDEPENDIENTE)	MICROSOFT 365 EMPRESA PREMIUM (INCLUYE DEFENDER PARA EMPRESAS)

CARACTERÍSTICA O FUNCIONALIDAD	MICROSOFT DEFENDER PARA EMPRESAS (INDEPENDIENTE)	MICROSOFT 365 EMPRESA PREMIUM (INCLUYE DEFENDER PARA EMPRESAS)
Protección por correo electrónico	Sí - Examen por correo electrónico con Antivirus de Microsoft Defender	Sí - Exchange Online Protection - Examen por correo electrónico con Antivirus de Microsoft Defender
Protección contra correo no deseado	Sí - Para dispositivos	Sí - Para dispositivos : para Microsoft 365 contenido de correo electrónico, como mensajes y datos adjuntos
Protección antimalware	Sí - Para dispositivos	Sí - Para dispositivos : para Microsoft 365 contenido de correo electrónico, como mensajes y datos adjuntos
Protección de última generación (protección antivirus y antimalware)	Sí - Antivirus de Microsoft Defender se incluye en Windows 10 y versiones posteriores	Sí - Antivirus de Microsoft Defender se incluye en Windows 10 y versiones posteriores - Directivas de protección de última generación para dispositivos incorporados
Reducción de la superficie expuesta a ataques (Reglas de ASR en Windows 10 o versiones posteriores y protección del firewall)	Sí	Sí
EDR (detección basada en comportamiento y acciones de respuesta manual)	Sí	Sí
Investigación y respuesta automatizadas	Sí	Sí
Administración de vulnerabilidades y amenazas	Sí	Sí
Administración centralizada e informes	Sí	Sí
API (para la integración con aplicaciones personalizadas o soluciones de informes)	Sí	Sí

Comparar Microsoft Defender para Empresas con los planes 1 y 2 de Microsoft Defender para punto de conexión

Defender for Business ofrece funcionalidades de nivel empresarial de Defender para punto de conexión a pequeñas y medianas empresas. En la tabla siguiente se comparan las características y funcionalidades de seguridad de Defender para empresas con las ofertas empresariales, Microsoft Defender para punto de

conexión los planes 1 y 2.

CARACTERÍSTICA O FUNCIONALIDAD	DEFENDER PARA EMPRESAS (INDEPENDIENTE)	PLAN 1 DE DEFENDER PARA PUNTO DE CONEXIÓN (PARA CLIENTES EMPRESARIALES)	PLAN 2 DE DEFENDER PARA PUNTO DE CONEXIÓN (PARA CLIENTES EMPRESARIALES)
Administración centralizada	Sí [1]	Sí	Sí
Configuración de cliente simplificada	Sí	No	No
Administración de vulnerabilidades y amenazas	Sí	No	Sí
Capacidades de reducción de superficie expuesta a ataques	Sí	Sí	Sí
Protección de última generación	Sí	Sí	Sí
EDR	Sí [2]	No	Sí
Investigación y respuesta automatizadas	Sí [3]	No	Sí
Búsqueda de amenazas y seis meses de retención de datos	No [4]	No	Sí
Análisis de amenazas	Sí [5]	No	Sí
Compatibilidad multiplataforma. (sistema operativo Windows, macOS, iOS y Android)	Sí [6]	Sí	Sí
Expertos en amenazas de Microsoft	No	No	Sí
API de asociados	Sí	Sí	Sí
integración Microsoft 365 Lighthouse (Para ver los incidentes de seguridad entre los inquilinos del cliente)	Sí	Sí [7]	Sí [7]

(
1) Incorporación y administración de dispositivos en el portal de Microsoft 365 Defender (https://security.microsoft.com) o con Microsoft Intune, administrados en el centro de administración de Microsoft Endpoint Manager (https://endpoint.microsoft.com).

(
2) Las funcionalidades de detección y respuesta de puntos de conexión (EDR) en Defender for Business incluyen

la detección basada en comportamiento y los cuatro tipos siguientes de acciones de respuesta manual:

- Ejecutar examen de antivirus
- Aislar el dispositivo
- Detener y poner en cuarentena un archivo
- Adición de un indicador para bloquear o permitir un archivo

(
3) En Defender para empresas, la investigación y la respuesta automatizadas están activadas de forma predeterminada, en todo el inquilino. Si desactiva la investigación y la respuesta automatizadas, afectará a la protección en tiempo real. Consulte Revisión de la configuración de las características avanzadas.

(
4) No hay ninguna vista de escala de tiempo en Defender para empresas.

(
5) En Defender para empresas, el análisis de amenazas está optimizado para pequeñas y medianas empresas.

(
6) Consulte Incorporación de dispositivos para Microsoft Defender para Empresas.

(
7) La capacidad de ver incidentes entre inquilinos mediante Defender para punto de conexión es nueva.

Pasos siguientes

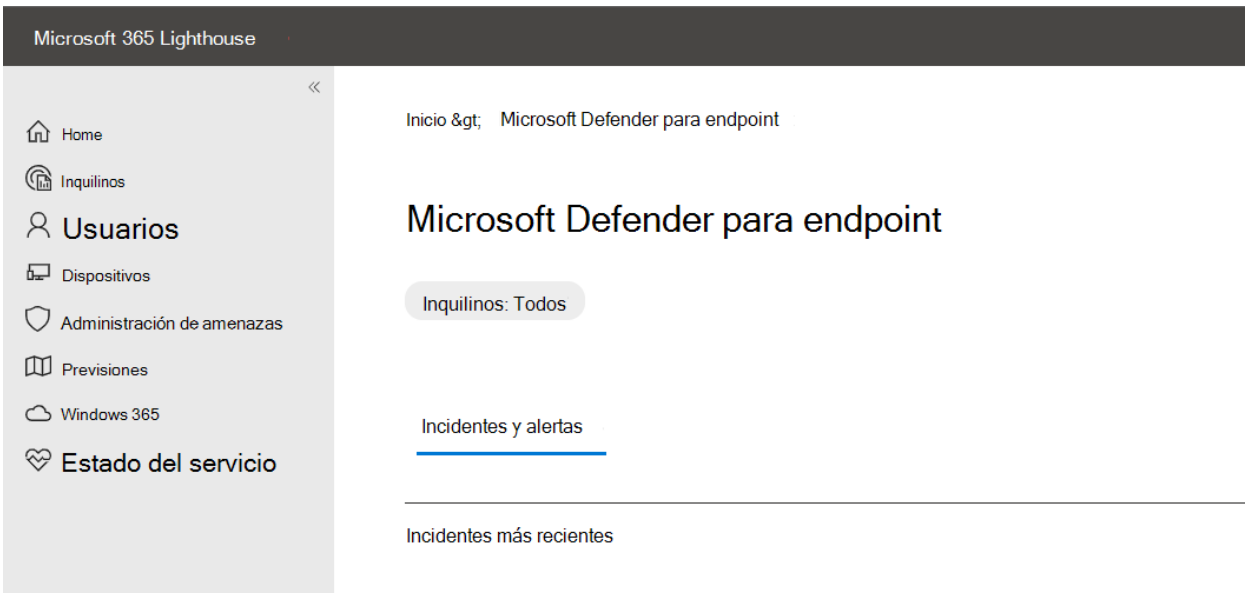
- Consulte los requisitos de Microsoft Defender para Empresas
- Obtener Microsoft Defender para Empresas
- Aprenda a configurar y configurar Microsoft Defender para Empresas

Microsoft 365 Lighthouse y Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

Microsoft Defender para Empresas se integra con Microsoft 365 Lighthouse

Si es un Proveedor de soluciones en la nube de Microsoft (CSP) y tiene Microsoft 365 Lighthouse, puede administrar la seguridad de los clientes (pequeñas y medianas empresas). Microsoft Defender para Empresas está diseñado para integrarse con Microsoft 365 Lighthouse, de modo que pueda ver incidentes de seguridad entre inquilinos en el portal de Microsoft 365 Lighthouse (https://lighthouse.microsoft.com).



Para acceder a la lista de incidentes, en Microsoft 365 Lighthouse, en la página principal, busque la tarjeta Incidentes de **seguridad** y, a continuación, seleccione **Ver todos los incidentes**.

Más información sobre Microsoft 365 Lighthouse

Microsoft 365 Lighthouse permite a los proveedores de Microsoft Cloud Service proteger y administrar dispositivos, datos y usuarios a escala para clientes empresariales pequeños y medianos que usan una de las siguientes suscripciones:

- Microsoft Defender para Empresas
- Microsoft 365 Empresa Premium
- Microsoft 365 E3 (que ahora incluye Microsoft Defender para punto de conexión plan 1)

Para más información, consulte Introducción a Microsoft 365 Lighthouse.

Obtener Microsoft Defender para Empresas

21/06/2022 • 4 minutes to read

Si aún no tiene Microsoft Defender para Empresas, puede elegir entre varias opciones:

- Pruebe o compre la versión independiente de Defender para empresas.
- Obtener Microsoft 365 Empresa Premium, que ahora incluye Defender para empresas
- Trabaje con un proveedor de soluciones de Microsoft que pueda ayudarle a configurar y configurar todo.

Si se ha registrado para obtener una evaluación, después de recibir el correo electrónico de aceptación, puede activar la prueba y asignar licencias de usuario y, a continuación, continuar con los pasos siguientes.

Pruebe o compre Microsoft Defender para Empresas

1. Vaya a la página web Microsoft Defender para Empresas y seleccione la opción para probar o comprar Defender para empresas.
2. Cuando reciba su correo electrónico con la información de su cuenta y suscripción, inicie sesión con el vínculo de su correo electrónico.
3. Vaya a Agregar usuarios y asigne licencias.

> **TIP**
> Consulte el cuaderno de estrategias de prueba para Defender para empresas.

Obtención de Microsoft 365 Empresa Premium

A partir del 1 de marzo de 2022, Defender for Business se incluye en Microsoft 365 Empresa Premium.

1. Visite la página del producto Microsoft 365 Empresa Premium.
2. Elige probar o comprar tu suscripción. Consulte Probar o comprar una suscripción a Microsoft 365 para Empresas En el sitio Microsoft 365 Products, elige **Microsoft 365 Empresa Premium**.
3. Después de registrarse en Microsoft 365 Empresa Premium, recibirá un correo electrónico con un vínculo para iniciar sesión y empezar. Procede a Configurar Microsoft 365 Empresa Premium.

Trabajar con un proveedor de soluciones de Microsoft

Microsoft tiene una lista de proveedores de soluciones autorizados para vender ofertas, incluidos Microsoft 365 Empresa Premium y Microsoft Defender para Empresas. Para buscar un proveedor de soluciones en su área, siga estos pasos:

1. Ve a la página de **Microsoft Solution Providers**. (https://www.microsoft.com/solution-providers)
2. En el cuadro de búsqueda, rellene la ubicación y el tamaño de la empresa.
3. En el cuadro de **Búsqueda de productos, servicios, aptitudes, sectores**, coloque `Microsoft 365` y, a continuación, seleccione **Go**.
4. Revise la lista de resultados. Seleccione un proveedor para obtener más información sobre su experiencia y los servicios que proporcionan. Su proveedor puede ayudarle a registrarse en Defender para empresas.

Activación de la prueba

Cuando reciba el correo electrónico de aceptación, aquí le mostremos cómo activar la suscripción de prueba:

1. En el correo electrónico de aceptación, selecciona el vínculo que incluye tu código promocional.
2. Si ya tiene una suscripción Microsoft 365, inicie sesión con su cuenta. Si aún no tiene una suscripción, siga las indicaciones para crear una nueva cuenta.
3. Cuando inicie sesión por primera vez, irá al Centro de administración de Microsoft 365 (https://admin.microsoft.com/). Consulte Información general de la Centro de administración de Microsoft 365.
4. Utilice uno de los procedimientos siguientes:

ESCENARIO	PROCEDURE
Está configurando una suscripción de Microsoft 365 por primera vez.	Seleccione **Ir a la configuración guiada** y complete los pasos siguientes: 1. Instale las aplicaciones de Office ahora o elija **Continuar** para omitir este paso. (Puede instalar las aplicaciones de Office más adelante). 2. Si su empresa tiene un dominio, puede agregarlo ahora (se recomienda esta opción). Como alternativa, podría optar por usar el dominio predeterminado `.onmicrosoft.com` por ahora. 3. Agregue usuarios y asigne licencias. A cada usuario que enumere se le asignará automáticamente una licencia. Consulte Agregar usuarios y asignar licencias al mismo tiempo.
Va a agregar una prueba a un inquilino de Microsoft 365 existente.	1. Vaya al Centro de administración de Microsoft 365 (https://admin.microsoft.com/) e inicie sesión. 2. En el panel de navegación, elija **Usuarios** > **usuarios activos**. Revise la lista de usuarios. 3. Para asignar licencias, siga las instrucciones de Asignación de licencias a los usuarios.

Dos portales para la instalación

Cuando esté listo para empezar, trabajará con dos portales principales: el Centro de administración de Microsoft 365 y el portal de Microsoft 365 Defender.

PORTAL	DESCRIPCIÓN
El Centro de administración de Microsoft 365 (https://admin.microsoft.com/)	Use el Centro de administración de Microsoft 365 para activar la prueba e iniciar sesión por primera vez. También usará el Centro de administración de Microsoft 365 para: • Agregar o quitar usuarios. • Asignar licencias de usuario. • Vea sus productos y servicios. • Complete las tareas de configuración de la suscripción de Microsoft 365. Para obtener más información, consulte Información general de la Centro de administración de Microsoft 365.

PORTAL	DESCRIPCIÓN
El portal de Microsoft 365 Defender (https://security.microsoft.com)	Use el portal de Microsoft 365 Defender para configurar Defender para empresas. Usará el portal de Microsoft 365 Defender para: • Vea los dispositivos y las directivas de protección de dispositivos. • Vea las amenazas detectadas y tome medidas. • Vea las recomendaciones de seguridad y administre la configuración de seguridad. Para obtener más información, consulte Comenzar mediante el portal de Microsoft 365 Defender.

TIP

Si tiene Microsoft 365 Empresa Premium, también tiene Microsoft Intune. Puede usar el centro de administración de Microsoft Endpoint Manager (https://endpoint.microsoft.com/) para administrar dispositivos y configurar las opciones de seguridad. Para obtener más información sobre Intune, consulte Microsoft Intune es un proveedor de MDM y MAM para los dispositivos.

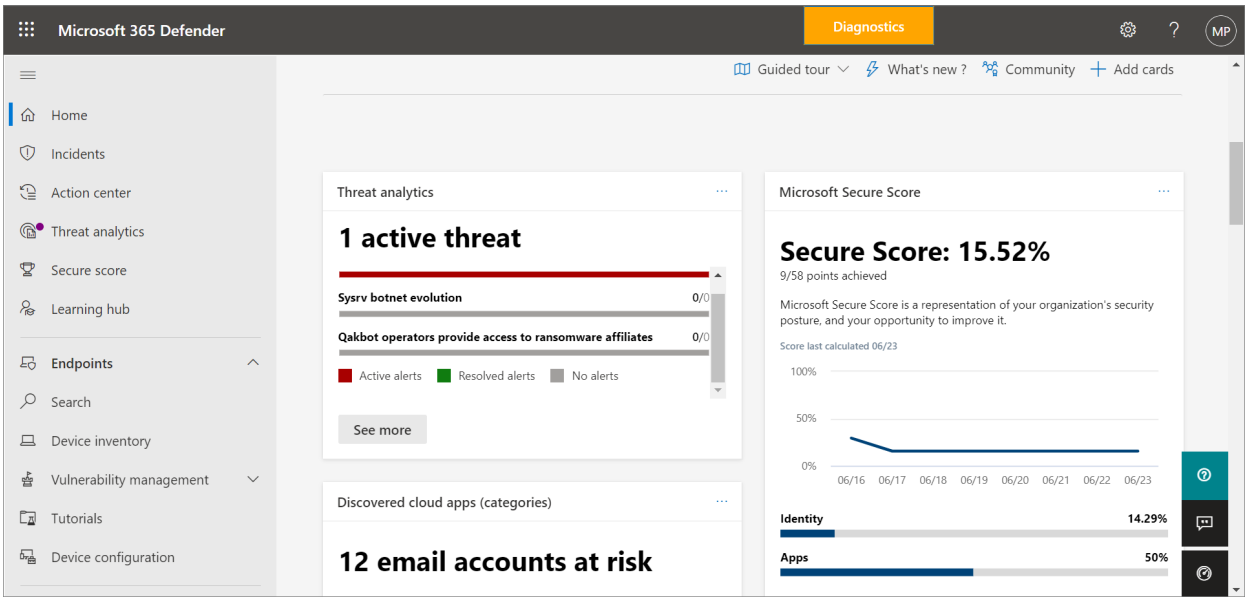
Pasos siguientes

- Consulte el cuaderno de estrategias de prueba: Microsoft Defender para Empresas.
- Use el asistente de instalación en Microsoft Defender para Empresas.
- Consulte el proceso de configuración y configuración de Defender para empresas.
- Vea cómo obtener ayuda y soporte técnico para Defender para empresas (por si necesita ayuda).

Visitar el portal de Microsoft 365 Defender

21/06/2022 • 4 minutes to read

El portal de Microsoft 365 Defender (https://security.microsoft.com) es tu tienda integral para usar y administrar Microsoft Defender para Empresas. Incluye un banner de bienvenida y llamadas que te ayudarán a empezar, tarjetas que exponen información relevante y una barra de navegación para que puedas acceder fácilmente a las distintas características y funcionalidades.



Barra de navegación

Use la barra de navegación del lado izquierdo de la pantalla para acceder a los incidentes, ver informes y administrar las directivas de seguridad. En la tabla siguiente se describen los elementos que verá en la barra de navegación.

ITEM	DESCRIPCIÓN
Inicio	Le lleva a la página principal en Microsoft 365 Defender. La página principal incluye tarjetas que resaltan las amenazas activas que se detectaron, junto con recomendaciones para ayudar a proteger los datos y los dispositivos de su empresa. Recomendaciones se incluyen en Defender for Business puede ahorrar tiempo y esfuerzo al equipo de seguridad. Recomendaciones se basan en los procedimientos recomendados del sector. Para obtener más información sobre las recomendaciones, consulte Recomendaciones de seguridad: Administración de amenazas y vulnerabilidades.
Incidentes	Le lleva a la lista de incidentes recientes. A medida que se desencadenan alertas, se crean incidentes. Un incidente puede incluir varias alertas. Asegúrese de revisar los incidentes con regularidad. Para más información sobre los incidentes, consulte Visualización y administración de incidentes en Microsoft Defender para Empresas.

ITEM	DESCRIPCIÓN
Centro de actividades	Le lleva a la lista de acciones de respuesta, incluidas las acciones completadas o pendientes. - Seleccione la pestaña **Historial** para ver las acciones realizadas. Algunas acciones se realizan automáticamente; otros se toman manualmente o se completan después de que se aprueben. - Seleccione la pestaña **Pendiente** para ver las acciones que requieren aprobación para continuar. Para obtener más información sobre el Centro de acciones, consulte Revisar las acciones de corrección en el Centro de acciones.
Análisis de amenazas	Le lleva a una vista de las amenazas actuales y le proporciona una vista general del panorama de las amenazas. El análisis de amenazas también incluye informes e información de investigadores de seguridad de Microsoft. Para más información sobre el análisis de amenazas, consulte Seguimiento y respuesta a amenazas emergentes a través del análisis de amenazas.
Puntuación de seguridad	Proporciona una representación de la posición de seguridad de su empresa y ofrece sugerencias para mejorarla. Para obtener más información sobre la puntuación de seguridad, consulte Puntuación de seguridad de Microsoft para dispositivos.
centro de Learning	Proporciona acceso al entrenamiento de seguridad y a otros recursos a través de rutas de aprendizaje que se incluyen con la suscripción. Puede filtrar por producto, nivel de aptitud, rol y mucho más. El centro de Learning puede ayudar al equipo de seguridad a aumentar las características de seguridad & funcionalidades de Defender para empresas y más ofertas de Microsoft, como Microsoft Defender para punto de conexión y Microsoft Defender para Office 365.
Extremos > Búsqueda	Permite buscar uno o varios dispositivos que se incorporaron a Microsoft Defender para Empresas.
Extremos > Inventario de dispositivos	Permite buscar uno o varios dispositivos que se incorporaron a Microsoft Defender para Empresas.
Extremos > Administración de vulnerabilidades	Proporciona un panel, recomendaciones, actividades de corrección, un inventario de software y una lista de posibles debilidades dentro de la empresa.
Extremos > Tutoriales	Proporciona acceso a tutoriales y simulaciones para ayudarle a obtener más información sobre cómo funcionan las características de protección contra amenazas. Seleccione el vínculo **Leer el tutorial** antes de intentar obtener el archivo de simulación para cada tutorial. Algunas simulaciones requieren Office aplicaciones, como Microsoft Word, para leer el tutorial.

ITEM	DESCRIPCIÓN
Extremos > **Configuración del dispositivo**	Enumera las directivas de seguridad por sistema operativo y por tipo. Para obtener más información sobre las directivas de seguridad, consulte Ver o editar directivas en Microsoft Defender para Empresas.
Informes	Enumera los informes de seguridad disponibles. Estos informes le permiten ver las tendencias de seguridad, ver detalles sobre las detecciones y alertas de amenazas y obtener más información sobre los dispositivos vulnerables de su empresa.
Estado	Permite ver el estado de mantenimiento del servicio y planear los próximos cambios. - Seleccione **Estado del servicio** para ver el estado de mantenimiento de los servicios de Microsoft 365 que se incluyen en la suscripción de su empresa. - Seleccione **Centro de** mensajes para obtener información sobre los cambios planeados y lo que se espera.
Permisos & roles	Permite asignar permisos a las personas de la empresa que administrarán la seguridad y verán los incidentes e informes en el portal de Microsoft 365 Defender. También le permite configurar y administrar grupos de dispositivos para incorporar los dispositivos de su empresa y asignar las directivas de protección contra amenazas.
Configuración	Permite editar la configuración del portal de Microsoft 365 Defender y Microsoft Defender para Empresas. Por ejemplo, puede incorporar (o offboard) y los dispositivos de su empresa (también conocidos como puntos de conexión). También puede definir reglas, como las reglas de supresión de alertas, y configurar indicadores para bloquear o permitir determinados archivos o procesos.
Más recursos	Vaya a otros portales, como Azure Active Directory. Tenga en cuenta que el portal de Microsoft 365 Defender debe satisfacer sus necesidades sin necesidad de navegar a otros portales.

Pasos siguientes

- Uso del asistente para la instalación en Microsoft Defender para Empresas
- Consulte el proceso de configuración y configuración.

Uso del asistente para la instalación en Microsoft Defender para Empresas

21/06/2022 • 5 minutes to read

Microsoft Defender para Empresas se diseñó para ahorrar tiempo y esfuerzo a las pequeñas y medianas empresas. Por ejemplo, puede realizar la configuración y la configuración iniciales con un asistente para la instalación. El asistente para la configuración le guía a través de la concesión de acceso al equipo de seguridad, la configuración de notificaciones por correo electrónico para el equipo de seguridad y la incorporación de los dispositivos de Windows de su empresa.

TIP

El uso del asistente para la instalación es opcional. Puede optar por trabajar manualmente en el proceso de configuración y configuración. Para más información, vea:

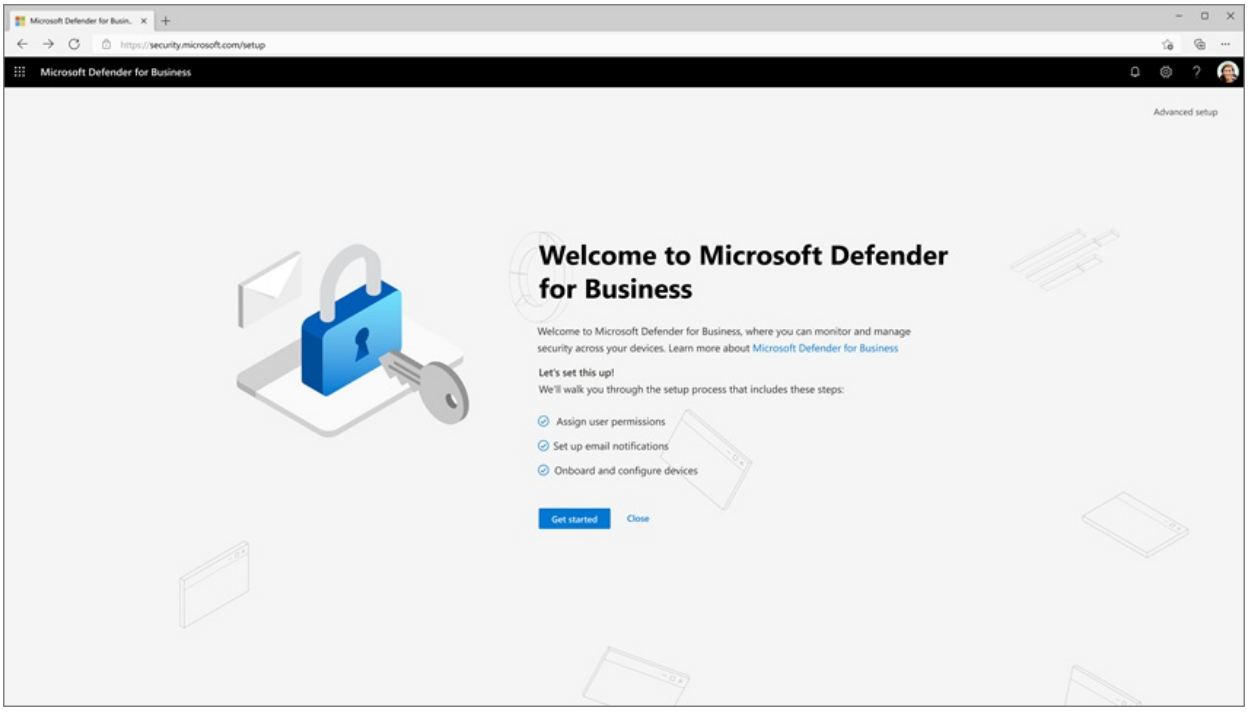
- ¿Qué ocurre si no uso el asistente?
- Configuración y configuración de Microsoft Defender para Empresas

Cómo iniciar el asistente para la instalación

El asistente para la instalación está diseñado para ejecutarse la primera vez que alguien de la empresa inicia sesión en el portal de Microsoft 365 Defender (https://security.microsoft.com).

Si su empresa ha estado usando Microsoft 365 Empresa Premium, el Asistente para la configuración de Defender para empresas se ejecutará la primera vez que alguien vaya al **inventario de dispositivos de puntos de conexión** > .

La pantalla de inicio del asistente para la instalación es similar a la siguiente imagen:



Flujo del asistente de instalación

> **IMPORTANT**
> Debe ser administrador global para ejecutar el asistente de instalación. La persona que registró su empresa para Microsoft 365 o para Microsoft Defender para Empresas es un administrador global de forma predeterminada.

El asistente para la instalación está diseñado para ayudarle a configurar Defender for Business de forma rápida y eficaz. El asistente le guiará por los pasos siguientes:

1. **Asignar permisos de usuario**. En este paso, concederá acceso al equipo de seguridad al portal de Microsoft 365 Defender (https://security.microsoft.com). En este portal, usted y su equipo de seguridad administrarán sus funcionalidades de seguridad, verán alertas y realizarán las acciones necesarias en las amenazas detectadas. El acceso al portal se concede a través de roles que implican ciertos permisos.

   En Defender para empresas, a los miembros del equipo de seguridad se les puede asignar uno de los tres roles siguientes:

   - **Administración global**: un administrador global puede ver y editar toda la configuración en el inquilino de Microsoft 365. El administrador global realiza la configuración y configuración iniciales de la suscripción de Microsoft 365 de la empresa.
   - **Administrador de** seguridad: un administrador de seguridad puede ver y editar la configuración de seguridad y tomar medidas cuando se detectan amenazas.
   - **Lector de** seguridad: un lector de seguridad puede ver información en los informes, pero no puede cambiar ninguna configuración de seguridad.

   Obtenga más información sobre los roles y permisos.

2. **Configurar notificaciones por correo electrónico**. En este paso, puede configurar notificaciones por correo electrónico para el equipo de seguridad. A continuación, cuando se genera una alerta o se detecta una nueva vulnerabilidad, el equipo de seguridad no la perderá aunque esté fuera de su escritorio. Obtenga más información sobre las notificaciones por correo electrónico.

3. **Incorporación y configuración de dispositivos Windows**. En este paso, puede incorporar rápidamente los dispositivos Windows de su empresa a Defender for Business. La incorporación de dispositivos de inmediato ayuda a proteger esos dispositivos desde el primer día.

   - **Si ya usa Microsoft Intune** y su empresa tiene dispositivos inscritos en Intune, se le preguntará si desea usar la incorporación automática para algunos o todos los dispositivos Windows inscritos. La incorporación automática configura una conexión entre Intune y Defender for Business y, a continuación, incorpora Windows dispositivos a Defender for Business sin problemas.
   - **Si aún no usa Intune**, puede incorporar dispositivos a Defender for Business.

   Obtenga más información sobre la incorporación de dispositivos a Microsoft Defender para Empresas.

4. **Configure las directivas de seguridad**. Defender for Business incluye directivas de seguridad predeterminadas para la protección de próxima generación y la protección de firewall que se pueden aplicar a los dispositivos de la empresa. Estas directivas predeterminadas usan la configuración recomendada y están diseñadas para proporcionar una protección segura para los dispositivos. También puede crear sus propias directivas de seguridad. Además, si ya usa Intune, puede seguir usando el centro de administración de Microsoft Endpoint Manager para administrar las directivas de seguridad.

   Vea y edite las directivas de seguridad y la configuración.

¿Qué es la incorporación automática?

La incorporación automática es una manera simplificada de incorporar dispositivos Windows a Defender for Business. La incorporación automática solo está disponible para dispositivos Windows que ya están inscritos en

Microsoft Intune.

Mientras usa el asistente para la instalación, el sistema detectará si Windows dispositivos ya están inscritos en Intune. Se le preguntará si desea usar la incorporación automática para todos o algunos de esos dispositivos. Puede incorporar todos los dispositivos Windows a la vez o seleccionar dispositivos específicos con los que empezar y, a continuación, agregar más dispositivos más adelante.

Para incorporar otros dispositivos, consulte Incorporación de dispositivos a Microsoft Defender para Empresas.

TIP

- Se recomienda seleccionar los "todos los dispositivos inscritos". Opción. De este modo, cuando Windows dispositivos se inscriban en Intune más adelante, se incorporarán automáticamente a Defender for Business.
- Si ha estado administrando directivas y configuraciones de seguridad en el centro de administración de Endpoint Manager, se recomienda cambiar al portal de Microsoft 365 Defender para administrar los dispositivos, las directivas y la configuración. Para más información, consulte Elegir dónde administrar directivas y dispositivos de seguridad.

¿Qué ocurre si no uso el asistente?

El uso del asistente para la instalación es opcional. Si decide no usar el asistente o si el asistente se cierra antes de que se complete el proceso de instalación, puede completar el proceso de instalación y configuración por su cuenta.

Consulte Configuración y configuración de Microsoft Defender para Empresas para seguir estos pasos:

1. **Asigne roles y permisos** para que el equipo de seguridad pueda acceder y usar el portal de Microsoft 365 Defender (https://security.microsoft.com).
2. **Configure las notificaciones por correo electrónico para el equipo de seguridad para** que estén en el bucle sobre nuevas alertas o vulnerabilidades.
3. **Incorpore dispositivos** para que estén protegidos por Defender para empresas.
4. **Administre las directivas de seguridad**, que incluyen protección de última generación, protección contra firewalls y filtrado de contenido web.

Pasos siguientes

- Incorporación de más dispositivos a Microsoft Defender para Empresas
- Ver y editar las directivas de seguridad y la configuración en Microsoft Defender para Empresas

Tutoriales y simulaciones en Microsoft Defender para Empresas

21/06/2022 • 3 minutes to read

Si acaba de terminar de configurar Microsoft Defender para Empresas, es posible que se pregunte dónde empezar a aprender sobre cómo funciona Defender para empresas. En este artículo se describen algunos escenarios que probar y varios tutoriales y simulaciones que están disponibles para Defender para empresas. Estos recursos están diseñados para ayudarle a ver cómo Defender for Business puede funcionar para su empresa.

Pruebe estos escenarios

En la tabla siguiente se resumen varios escenarios para probar con Defender para empresas:

ESCENARIO	DESCRIPCIÓN
Incorporar dispositivos con un script local	En Defender para empresas, puede incorporar Windows y macOS dispositivos mediante un script que descargue y ejecute en cada dispositivo. El script crea una confianza con Azure Active Directory (Azure AD) (si esa confianza aún no existe), inscribe el dispositivo con Microsoft Intune (si tiene Intune) e incorpora el dispositivo a Defender for Business. Para más información, consulte Incorporación de dispositivos para Microsoft Defender para Empresas.
Incorporación de dispositivos mediante el centro de administración de Microsoft Endpoint Manager	Si ya usaba Intune antes de obtener Defender for Business, puede seguir usando Endpoint Manager centro de administración para incorporar dispositivos. Pruebe a incorporar los dispositivos Windows, macOS, iOS y Android con Microsoft Intune. Para más información, consulte Inscripción de dispositivos en Microsoft Intune.
Edición de directivas de seguridad	Si va a administrar las directivas de seguridad en Defender para empresas, use la página **Configuración del dispositivo** para ver y, si es necesario, editar las directivas. Defender for Business incluye directivas predeterminadas que usan la configuración recomendada para proteger los dispositivos de su empresa en cuanto se incorporan. Puede mantener las directivas predeterminadas, editarlas y definir las suyas propias para satisfacer sus necesidades empresariales. Para obtener más información, consulte Ver o editar directivas en Microsoft Defender para Empresas.
Ejecución de un ataque simulado	Hay varios tutoriales y simulaciones disponibles en Defender para empresas. Estos tutoriales y simulaciones están diseñados para mostrar de primera mano cómo pueden funcionar las características de protección contra amenazas de Defender for Business para su empresa. También puede usar un ataque simulado como ejercicio de entrenamiento para el equipo. Para probar uno o varios de los tutoriales, consulte Tutoriales recomendados para Microsoft Defender para Empresas.

ESCENARIO	DESCRIPCIÓN
Visualización de incidentes en Microsoft 365 Lighthouse	Si es un Proveedor de soluciones en la nube de Microsoft que usa Microsoft 365 Lighthouse, podrá ver los incidentes entre los inquilinos de los clientes en el portal de Microsoft 365 Lighthouse. Para más información, consulte Microsoft 365 Lighthouse y Microsoft Defender para Empresas.

Tutoriales recomendados para Defender para empresas

En la tabla siguiente se describen los tutoriales recomendados para clientes de Defender for Business:

TUTORIAL	DESCRIPCIÓN
El documento quita la puerta trasera	Simular un ataque que introduce malware basado en archivos en un dispositivo de prueba. En el tutorial se describe cómo obtener y usar el archivo de simulación y qué se debe observar en el portal de Microsoft 365 Defender. Este tutorial requiere que Microsoft Word se instale en el dispositivo de prueba.
Tutorial de respuesta dinámica	Obtenga información sobre cómo usar comandos básicos y avanzados con Live Response. Obtenga información sobre cómo buscar un archivo sospechoso, corregirlo y recopilar información en un dispositivo.
Administración de vulnerabilidades de & amenazas (escenarios principales)	Obtenga información sobre Administración de amenazas y vulnerabilidades a través de tres escenarios: 1. Reduzca la exposición a amenazas y vulnerabilidades de su empresa. 2. Solicitar una corrección. 3. Cree una excepción para las recomendaciones de seguridad. Amenazas y administración de vulnerabilidades usa un enfoque basado en riesgos para la detección, priorización y corrección de vulnerabilidades de punto de conexión y configuraciones incorrectas.

Cada tutorial incluye un documento de tutorial que explica el escenario, cómo funciona y qué hacer.

> **TIP**
> Verá referencias a Microsoft Defender para punto de conexión en los documentos del tutorial. Los tutoriales enumerados en este artículo se pueden usar con Defender para punto de conexión o Defender para empresas.

Acceso a los tutoriales

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. En el panel de navegación, en **Puntos de conexión**, elija **Tutoriales**.
3. Elija uno de los siguientes tutoriales:
   - **El documento quita la puerta trasera**
   - **Tutorial de respuesta dinámica**

- **Administración de vulnerabilidades de & amenazas (escenarios principales)**

Pasos siguientes

- Administración de dispositivos en Microsoft Defender para Empresas
- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Revisión de las acciones de corrección en el Centro de acciones

Configuración y configuración de Microsoft Defender para Empresas

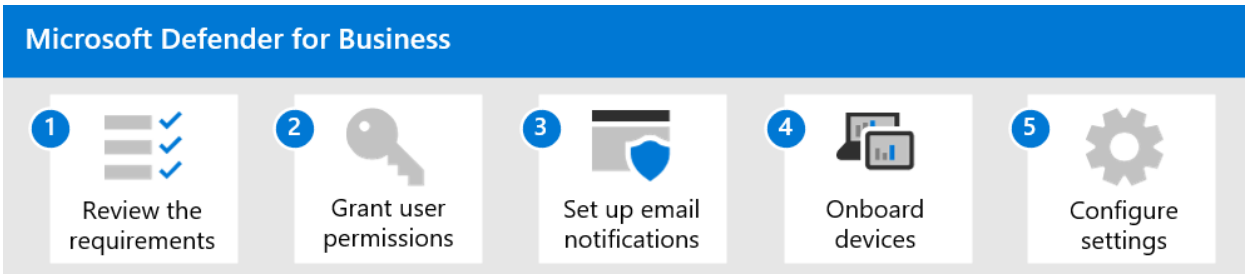
21/06/2022 • 2 minutes to read

Microsoft Defender para Empresas proporciona una experiencia de configuración y configuración simplificada, diseñada especialmente para las pequeñas y medianas empresas. Use este artículo como guía para el proceso general.

> **TIP**
>
> Si usó el asistente para la instalación, ya ha completado varios pasos del proceso de instalación básico. En este caso, puede:
>
> - Incorporación de más dispositivos
> - Configuración de directivas y opciones de seguridad
> - Visite el panel de administración de vulnerabilidades

Proceso de instalación y configuración

En el diagrama siguiente se muestra el proceso de configuración y configuración general de Defender para empresas. Si usó el asistente para la instalación, es probable que ya haya completado los pasos 1 a 3 y posiblemente el paso 4.



PASO	ARTÍCULO	DESCRIPCIÓN
1	Revisar los requisitos	Revise los requisitos, incluidos los sistemas operativos compatibles, para Microsoft Defender para Empresas. Consulte requisitos de Microsoft Defender para Empresas.
2	Asignación de roles y permisos	Los usuarios del equipo de seguridad necesitan permisos para realizar tareas, como revisar las amenazas detectadas & acciones de corrección, ver & directivas de edición, incorporar dispositivos y usar informes. Puede conceder estos permisos a través de determinados roles. Consulte Asignación de roles y permisos.

PASO	ARTÍCULO	DESCRIPCIÓN
3	Configuración de notificaciones por correo electrónico	Puede especificar quién debe recibir notificaciones por correo electrónico cuando se desencadenen alertas o se detecten nuevas vulnerabilidades. Consulte Configuración de notificaciones por correo electrónico.
4	Incorporar dispositivos	Microsoft Defender para Empresas está configurado para que pueda elegir entre varias opciones para incorporar los dispositivos de su empresa. Consulte Incorporación de dispositivos para Microsoft Defender para Empresas.
5	Configuración de las directivas y las opciones de seguridad	Puede elegir entre varias opciones para configurar las directivas y las opciones de seguridad, incluido un proceso de configuración simplificado en Defender para empresas o mediante el centro de administración de Microsoft Endpoint Manager. Consulte Configuración de las directivas y las opciones de seguridad.

Pasos siguientes

Continúe con el paso 1: Revisar los requisitos de Microsoft Defender para Empresas.

requisitos de Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

En este artículo se describen los requisitos de Microsoft Defender para Empresas.

Qué hacer

1. Revise los requisitos y asegúrese de cumplirlos.
2. Continúe con los pasos siguientes.

Revisar los requisitos

En la tabla siguiente se enumeran los requisitos básicos para configurar y usar Microsoft Defender para Empresas.

REQUISITO	DESCRIPCIÓN
Suscripción	Microsoft 365 Empresa Premium o Microsoft Defender para Empresas (independiente). Consulte Cómo obtener Microsoft Defender para Empresas. Tenga en cuenta que si tiene varias suscripciones, la suscripción más alta tiene prioridad. Por ejemplo, si tiene Microsoft Defender para punto de conexión Plan 2 (suscripción comprada o de prueba) y obtiene Microsoft Defender para Empresas, El plan 2 de Defender para punto de conexión tiene prioridad. En este caso, no verá la experiencia de Defender para empresas.
Datacenter	Una de las siguientes ubicaciones del centro de datos: - Unión Europea - Reino Unido - Estados Unidos
Cuentas de usuario	- Las cuentas de usuario se crean en el Centro de administración de Microsoft 365 (https://admin.microsoft.com) : las licencias de Microsoft Defender para Empresas se asignan en el Centro de administración de Microsoft 365 Para obtener ayuda con esta tarea, consulte Agregar usuarios y asignar licencias.
Permisos	Para registrarse en Microsoft Defender para Empresas, debe ser un Administración global. Para acceder al portal de Microsoft 365 Defender, los usuarios deben tener asignado uno de los siguientes roles en Azure AD: - Lector de seguridad - Administración de seguridad - Administración global Para más información, consulte Roles y permisos en Microsoft Defender para Empresas.

REQUISITO	DESCRIPCIÓN
Requisitos de los exploradores	Microsoft Edge o Google Chrome
Sistema operativo	Para administrar dispositivos en el portal de Microsoft 365 Defender, los dispositivos deben ejecutar uno de los siguientes sistemas operativos: - Windows 10 Business o posterior - Windows 10 Professional o posterior - Windows 10 Enterprise o posterior - macOS (se admiten las tres versiones más actuales) Asegúrese de que KB5006738 está instalado en Windows dispositivos. Si ya está administrando dispositivos en Microsoft Intune, puede seguir usando el centro de administración de Microsoft Endpoint Manager.

NOTE

Azure Active Directory (Azure AD) se usa para administrar los permisos de usuario y los grupos de dispositivos. Azure AD se incluye en la suscripción de Defender para empresas.

- Si no tiene una suscripción Microsoft 365 antes de iniciar la prueba, Azure AD se aprovisionará automáticamente durante el proceso de activación.
- Si tiene otra suscripción Microsoft 365 al iniciar la prueba de Defender para empresas, puede usar el servicio de Azure AD existente.
- Si usa Microsoft 365 Empresa Premium al iniciar la prueba de Defender para empresas, tendrá la opción de administrar los dispositivos mediante Intune.

Pasos siguientes

Vaya al paso 2: Asignación de roles y permisos en Microsoft Defender para Empresas.

Asignación de roles y permisos en Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

Para realizar tareas en el portal de Microsoft 365 Defender, como configurar Microsoft Defender para Empresas, ver informes o realizar acciones de respuesta sobre amenazas detectadas, se deben asignar permisos adecuados al equipo de seguridad. Los permisos se conceden a través de roles asignados en el portal de Microsoft 365 Defender (https://security.microsoft.com) o en Azure Active Directory.

Qué hacer

1. Obtenga información sobre los roles en Defender para empresas.
2. Vea o edite las asignaciones de roles para el equipo de seguridad.
3. Continúe con los pasos siguientes.

Roles en Defender para empresas

En la tabla siguiente se describen los tres roles que se pueden asignar en Defender para empresas. Obtenga más información acerca de los roles de administrador.

NIVEL DE PERMISOS	DESCRIPCIÓN
Administradores globales (también conocidos como administradores globales) *Como procedimiento recomendado, limite el número de administradores globales.*	Los administradores globales pueden realizar todo tipo de tareas. La persona que registró su empresa para Microsoft 365 o para Microsoft Defender para Empresas es un administrador global de forma predeterminada. Los administradores globales pueden acceder o cambiar la configuración en todos los portales de Microsoft 365, como: - El Centro de administración de Microsoft 365 (https://admin.microsoft.com) - Microsoft 365 Defender portal (https://security.microsoft.com)
Administradores de seguridad (también conocidos como administradores de seguridad)	Los administradores de seguridad pueden realizar las siguientes tareas: - Visualización y administración de directivas de seguridad - Ver y administrar alertas y amenazas de seguridad (estas actividades incluyen la realización de acciones de respuesta en puntos de conexión) - Visualización de información de seguridad e informes
Lector de seguridad	Los lectores de seguridad pueden realizar las siguientes tareas: - Visualización de directivas de seguridad - Visualización de amenazas y alertas de seguridad - Visualización de información de seguridad e informes

Visualización o edición de asignaciones de roles

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.

2. En el panel de navegación, elija **Permisos & roles** y, en **Azure AD**, seleccione **Roles**.
3. Seleccione uno de los siguientes roles para abrir su panel lateral:
   - Administrador global
   - Administrador de seguridad
   - Lector de seguridad

   > **IMPORTANT**
   > Microsoft recomienda conceder a las personas acceso solo a lo que necesitan para realizar sus tareas. A este concepto se le llama *privilegio mínimo* para los permisos. Para obtener más información, consulte Procedimientos recomendados para el acceso con privilegios mínimos para las aplicaciones.

4. En el panel lateral, seleccione el vínculo **Administrar miembros en Azure AD** . Esta acción le lleva a Azure Active Directory (Azure AD) donde puede ver y administrar las asignaciones de roles.
5. Seleccione un usuario para abrir su perfil y, a continuación, elija **Roles asignados**.
   - Para agregar un rol, elija **+ Agregar asignaciones**.
   - Para quitar un rol, elija **X Quitar asignaciones**.

¿Necesita agregar usuarios?

Si aún no ha agregado usuarios a su suscripción, consulte Agregar usuarios y asignar licencias al mismo tiempo.

Pasos siguientes

Continúe con:

- Paso 3: Configurar notificaciones por correo electrónico
- Paso 4: Incorporación de dispositivos a Microsoft Defender para Empresas

Configuración de notificaciones por correo electrónico

21/06/2022 • 2 minutes to read

Puede configurar notificaciones por correo electrónico para el equipo de seguridad. A continuación, a medida que se generan alertas o se detectan nuevas vulnerabilidades, se notificará automáticamente a las personas del equipo de seguridad.

Qué hacer

1. Obtenga información sobre los tipos de notificaciones por correo electrónico.
2. Ver y editar la configuración de notificaciones por correo electrónico.
3. Continúe con los pasos siguientes.

Tipos de notificaciones por correo electrónico

Al configurar notificaciones por correo electrónico, puede elegir entre dos tipos, como se describe en la tabla siguiente:

TIPO DE NOTIFICACIÓN	DESCRIPCIÓN
Vulnerabilidades	Cada vez que se detectan nuevas vulnerabilidades de seguridad o eventos de vulnerabilidad, los destinatarios reciben un correo electrónico.
Alertas & vulnerabilidades	Cuando se generan alertas porque se detectan amenazas en los dispositivos o cuando se detectan nuevas vulnerabilidades o eventos de vulnerabilidad, los destinatarios reciben un correo electrónico.

TIP

Las notificaciones por correo electrónico no son la única manera en que el equipo de seguridad puede averiguar sobre nuevas alertas o vulnerabilidades.

Las notificaciones por correo electrónico son una manera cómoda de ayudar a mantener informado a su equipo de seguridad, en tiempo real. ¡Pero hay otros! Por ejemplo, cada vez que el equipo de seguridad inicie sesión en el portal de Microsoft 365 Defender (https://security.microsoft.com), verá tarjetas que resaltan nuevas amenazas, alertas y vulnerabilidades. Defender for Business está diseñado para resaltar la información importante que le importa al equipo de seguridad en cuanto inician sesión.

El equipo de seguridad también puede elegir **Incidentes** en el panel de navegación para ver información. Para más información, consulte Visualización y administración de incidentes en Microsoft Defender para Empresas.

Visualización y edición de notificaciones por correo electrónico

Para ver o editar la configuración de notificaciones por correo electrónico de su empresa, siga estos pasos:

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. En el panel de navegación, seleccione **Configuración** y, a continuación, seleccione **Puntos de**

conexión. A continuación, en **General**, seleccione **Notificaciones por correo electrónico**.

3. Revise la información de las pestañas **Alertas** y **vulnerabilidades** .

   - Si no ve ningún elemento en la pestaña **Alertas** , puede crear una regla para que los usuarios reciban una notificación cuando se generen alertas. Para obtener ayuda con esta tarea, consulte Creación de reglas para notificaciones de alertas.
   - Si no ve ningún elemento en la pestaña **Vulnerabilidades** , puede crear una regla para que las personas reciban notificaciones cada vez que se detecte una nueva vulnerabilidad. Para obtener ayuda con esta tarea, consulte Creación de reglas para eventos de vulnerabilidad.
   - Si tiene reglas creadas, seleccione una regla para editarla. También puede eliminar una regla.

> **IMPORTANT**
> Al configurar notificaciones por correo electrónico en Defender para empresas, debe asignar las reglas de notificación a usuarios específicos. Defender for Business no usa el control de acceso basado en rol, como hace Defender para punto de conexión. Además, las notificaciones por correo electrónico no se pueden aplicar a grupos de dispositivos en Defender para empresas.

Pasos siguientes

Continúe con:

- Paso 4: Incorporación de dispositivos a Microsoft Defender para Empresas

Incorporación de dispositivos a Microsoft Defender para Empresas

21/06/2022 • 10 minutes to read

Con Microsoft Defender para Empresas, tiene varias opciones entre las que elegir para incorporar los dispositivos de su empresa. Este artículo le guiará por las opciones e incluye información general sobre cómo funciona la incorporación.

Qué hacer

1. Seleccione la pestaña del sistema operativo: **Windows clientes**, **equipos macOS** o **dispositivos móviles**.
2. Vea las opciones de incorporación y siga las instrucciones de la pestaña seleccionada.
3. Continúe con los pasos siguientes.

- **clientes Windows**
- **macOS**
- **dispositivos móviles**

clientes Windows

Elija una de las siguientes opciones para incorporar Windows dispositivos cliente a Defender for Business:

- Script local (para la incorporación manual de dispositivos en el portal de Microsoft 365 Defender)
- directiva de grupo (si ya usa directiva de grupo en su organización)
- Microsoft Intune (incluido en Microsoft 365 Empresa Premium)

Script local para clientes Windows

Puede usar un script local para incorporar Windows dispositivos cliente. Al ejecutar el script de incorporación en un dispositivo, crea una confianza con Azure Active Directory (si esa confianza no existe aún), inscribe el dispositivo en Microsoft Intune (si aún no está inscrito) y, a continuación, incorpora el dispositivo a Defender for Business. El método de script local funciona incluso si actualmente no tiene Intune. Se recomienda incorporar hasta 10 dispositivos a la vez mediante este método.

> **TIP**
> Se recomienda incorporar hasta 10 dispositivos a la vez cuando se usa el método de script local.

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. En el panel de navegación, elija **Settings** > **Endpoints**, y, a continuación, en **Management**, elige **Incorporación**.
3. Seleccione un sistema operativo, como **Windows 10 y 11**, y, a continuación, en la sección **Método de implementación**, elija **Script local**.
4. Seleccione **Descargar el paquete de incorporación** Se recomienda guardar el paquete de incorporación en una unidad extraíble.
5. En un dispositivo Windows, extraiga el contenido del paquete de configuración en una ubicación, como la

carpeta Escritorio. Debe tener un archivo denominado `WindowsDefenderATPLocalOnboardingScript.cmd`.

6. Abra una ventana de Símbolo de sistema como administrador.
7. Escriba la ubicación del archivo de script. Por ejemplo, si copió el archivo en la carpeta Escritorio, escriba `%userprofile%\Desktop\WindowsDefenderATPLocalOnboardingScript.cmd` y, a continuación, presione la tecla Entrar (o seleccione **Aceptar**).
8. Después de ejecutar el script, vaya a Ejecutar una prueba de detección.

directiva de grupo para clientes Windows

Si prefiere usar directiva de grupo para incorporar clientes Windows, siga las instrucciones de Incorporación de dispositivos Windows mediante directiva de grupo. En este artículo se describen los pasos para la incorporación a Microsoft Defender para punto de conexión; sin embargo, los pasos para la incorporación a Defender for Business son similares.

Microsoft Intune para clientes Windows

Si la suscripción incluye Intune, puede incorporar Windows clientes y otros dispositivos en el centro de administración de Microsoft Endpoint Manager (https://endpoint.microsoft.com). Por ejemplo, si tiene Microsoft 365 Empresa Premium, ha Intune como parte de la suscripción.

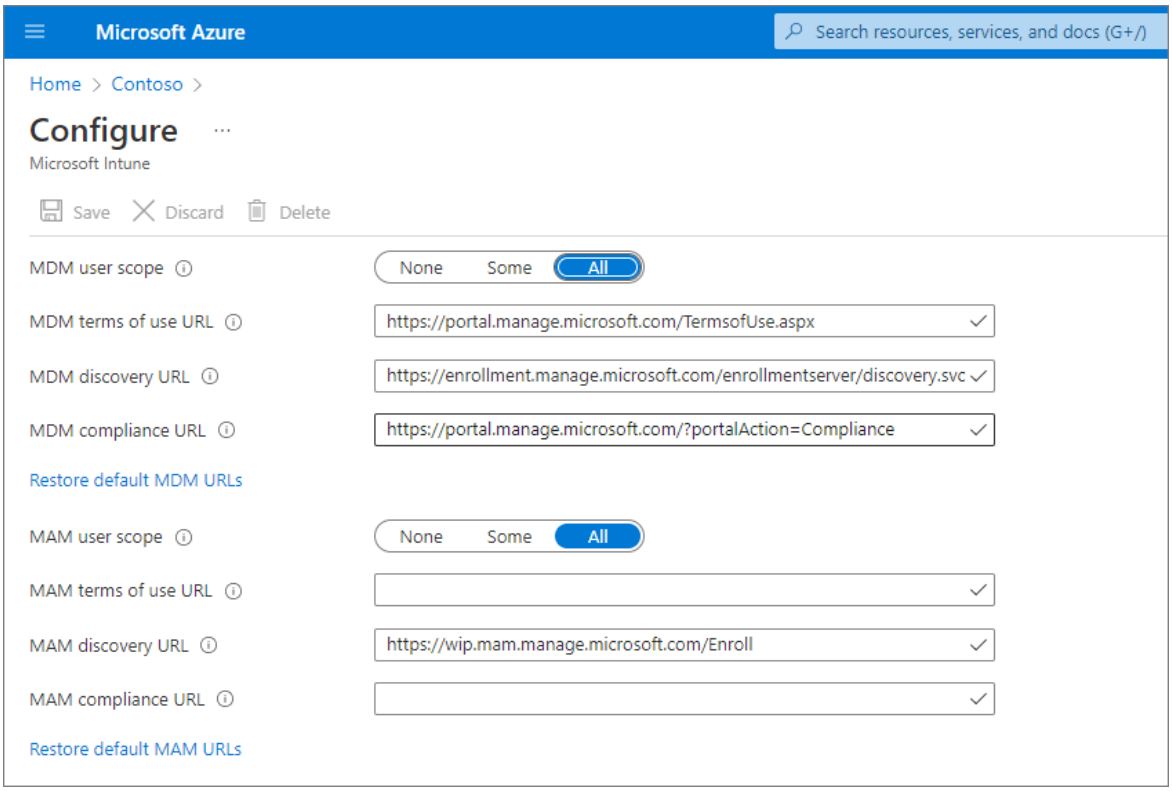
Hay varios métodos disponibles para inscribir dispositivos en Intune. Se recomienda empezar por uno de los métodos siguientes:

- Habilitación Windows inscripción automática para dispositivos propiedad de la empresa o administrados por la empresa
- Pida a los usuarios que inscriban sus propios dispositivos Windows 10/11 en Intune

Para habilitar la inscripción automática para dispositivos Windows

Al configurar la inscripción automática, los usuarios agregan su cuenta profesional al dispositivo. En segundo plano, el dispositivo se registra y se une a Azure Active Directory (Azure AD) y se inscribe en Intune.

1. Vaya a la Azure Portal (https://portal.azure.com/) e inicie sesión.
2. Seleccione **Azure Active Directory** > **Mobility (MDM y MAM)** > **Microsoft Intune**.
3. Configure el **ámbito de usuario mdm** y el **ámbito de usuario mam**.



- En ámbito de usuario de MDM, se recomienda seleccionar **Todo** para que todos los usuarios puedan inscribir automáticamente sus dispositivos Windows.
- En la sección Ámbito de usuario mam, se recomienda usar los siguientes valores predeterminados para las direcciones URL:
  - **URL de los términos de uso de MDM**
  - **URL de detección de MDM**
  - **URL de cumplimiento de MDM**

4. Seleccione **Guardar**.
5. Después de inscribir un dispositivo en Intune, puede agregarlo a un grupo de dispositivos. Obtenga más información sobre los grupos de dispositivos en Microsoft Defender para Empresas.

> **TIP**
> Para más información sobre la inscripción automática, consulte Habilitación Windows inscripción automática.

Para que los usuarios inscriban sus propios dispositivos Windows

1. Vea el siguiente vídeo para ver cómo funciona la inscripción:

2. Comparta este artículo con los usuarios de su organización: Inscriba dispositivos Windows 10/11 en Intune.
3. Después de inscribir un dispositivo en Intune, puede agregarlo a un grupo de dispositivos. Obtenga más información sobre los grupos de dispositivos en Microsoft Defender para Empresas.

Ejecución de una prueba de detección en un cliente de Windows

Después de incorporar dispositivos Windows a Defender para empresas, puedes ejecutar una prueba de detección en un dispositivo Windows para asegurarte de que todo funciona correctamente.

1. En el dispositivo Windows, cree una carpeta: `C:\test-MDATP-test`.

2. Abra una ventana de Símbolo de sistema como administrador.
3. En la ventana símbolo del sistema, ejecute el siguiente comando de PowerShell:

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference =
'silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe',
'C:\\test-MDATP-test\\invoice.exe');Start-Process 'C:\\test-MDATP-test\\invoice.exe'
```

Una vez ejecutado el comando, la ventana del símbolo del sistema se cerrará automáticamente. Si se realiza correctamente, la prueba de detección se marcará como completada y aparecerá una nueva alerta en el portal de Microsoft 365 Defender (https://security.microsoft.com) para el dispositivo recién incorporado en unos 10 minutos.

Ver una lista de dispositivos incorporados

Para ver la lista de dispositivos que se incorporan a Defender for Business, en el portal de Microsoft 365 Defender (https://security.microsoft.com), en el panel de navegación, en **Puntos de conexión**, elija **Inventario de dispositivos**.

Pasos siguientes

- Si tiene otros dispositivos que incorporar, seleccione la pestaña correspondiente al sistema operativo de los dispositivos (Windows clientes, Windows Server, macOS o dispositivos móviles) y siga las instrucciones de esa pestaña.
- Si ha terminado de incorporar dispositivos, vaya al Paso 5: Configurar las directivas y las opciones de seguridad en Microsoft Defender para Empresas
- Consulte Comenzar con Microsoft Defender para Empresas.

Ver y editar las directivas de seguridad y la configuración en Microsoft Defender para Empresas

21/06/2022 • 14 minutes to read

Después de incorporar los dispositivos de la empresa a Microsoft Defender para Empresas, el siguiente paso es revisar las directivas de seguridad. Si es necesario, puede editar las directivas de seguridad y la configuración.

> **TIP**
> Defender for Business incluye directivas de seguridad preconfiguradas que usan la configuración recomendada. Sin embargo, puede editar la configuración para satisfacer sus necesidades empresariales.

Las directivas de seguridad que se van a revisar y configurar incluyen:

- **Directivas de protección de última generación**, que determinan la protección antivirus y antimalware para los dispositivos de la empresa
- **Protección y reglas de firewall**, que determinan qué tráfico de red puede fluir hacia o desde los dispositivos de la empresa
- **Filtrado de contenido web**, que impide que las personas visiten determinados sitios web (URL) en función de categorías, como contenido para adultos o responsabilidad legal.
- **Características avanzadas**, como investigación y respuesta automatizadas, y detección y respuesta de puntos de conexión (EDR) en modo de bloque.

En Defender para empresas, las directivas de seguridad se aplican a los dispositivos a través de grupos de dispositivos.

Además de las directivas de seguridad, puede ver y editar la configuración, como la zona horaria que se va a usar en el portal de Microsoft 365 Defender (https://security.microsoft.com) y si se van a recibir características en versión preliminar a medida que estén disponibles.

Use este artículo como guía para administrar las directivas de seguridad y la configuración.

Qué hacer

1. Elija dónde administrar las directivas de seguridad y los dispositivos.
2. Revise las directivas de protección de próxima generación.
3. Revise las directivas de firewall y las reglas personalizadas.
4. Configurar el filtrado de contenido web.
5. Revise la configuración de las características avanzadas.
6. Vea otras opciones de configuración en el portal de Microsoft 365 Defender.
7. Continúe con los pasos siguientes.

Elección de dónde administrar directivas y dispositivos de seguridad

Defender for Business ofrece un proceso de configuración simplificado que ayuda a simplificar el proceso de configuración y configuración. Si selecciona el proceso de configuración simplificado, puede ver y administrar las directivas de seguridad en el portal de Microsoft 365 Defender (https://security.microsoft.com/). Sin embargo, no se limita a esta opción. Si ha estado usando Microsoft Intune, puede seguir usando el centro de administración de Microsoft Endpoint Manager.

La tabla siguiente puede ayudarle a elegir dónde administrar las directivas de seguridad y los dispositivos.

OPCIÓN	DESCRIPCIÓN
Uso del portal de Microsoft 365 Defender (*recomendado*)	El portal de Microsoft 365 Defender (https://security.microsoft.com/) puede ser tu tienda integral para administrar los dispositivos, las directivas de seguridad y la configuración de seguridad de tu empresa. Puede acceder a las directivas de seguridad y la configuración, usar el panel de administración de vulnerabilidades de Threat & y ver y administrar incidentes en un solo lugar. Si usa Intune, los dispositivos que incorpore a Defender for Business y las directivas de seguridad estarán visibles en el centro de administración de Endpoint Manager. Para más información, consulte los artículos siguientes: - Configuración predeterminada de Defender for Business y Microsoft Intune - Firewall en Microsoft Defender para Empresas
Uso del centro de administración de Microsoft Endpoint Manager	Si su empresa ya usa Intune para administrar directivas de seguridad, puede seguir usando el centro de administración de Endpoint Manager para administrar los dispositivos y las directivas de seguridad. Para más información, consulte Administración de la seguridad de dispositivos con directivas de seguridad de punto de conexión en Microsoft Intune. Si decide cambiar al proceso de configuración simplificado en Defender for Business, se le pedirá que elimine las directivas de seguridad existentes en Intune para evitar conflictos de directivas más adelante.

IMPORTANT

Si está administrando directivas de seguridad en el portal de Microsoft 365 Defender, puede *ver* esas directivas en el centro de administración de Endpoint Manager (https://endpoint.microsoft.com), que aparece como **directivas antivirus** o **de firewall**. Cuando vea las directivas de firewall en el centro de administración de Endpoint Manager, verá dos directivas en la lista: una directiva para la protección del firewall y otra para reglas personalizadas.

Visualización o edición de las directivas de protección de próxima generación

En función de si usa el portal de Microsoft 365 Defender o el centro de administración de Microsoft Endpoint Manager para administrar las directivas de protección de próxima generación, use uno de los procedimientos de la tabla siguiente:

PORTAL	PROCEDURE

PORTAL	PROCEDURE
portal de Microsoft 365 Defender (https://security.microsoft.com)	1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión. 2. En el panel de navegación, elija **Configuración del dispositivo**. Las directivas se organizan por sistema operativo y tipo de directiva. 3. Seleccione una pestaña del sistema operativo (por ejemplo **, Windows clientes**). 4. Expanda **Protección de próxima generación** para ver la lista de directivas. 5. Seleccione una directiva para ver más detalles sobre la directiva. Para realizar cambios o obtener más información sobre la configuración de directivas, consulte los artículos siguientes: - Visualización o edición de directivas de dispositivo - Descripción de la configuración de próxima generación
Microsoft Endpoint Manager centro de administración (https://endpoint.microsoft.com)	1. Vaya a https://endpoint.microsoft.com e inicie sesión. Ahora está en el centro de administración de Endpoint Manager. 2. Seleccione **Seguridad del punto de conexión**. 3. Seleccione **Antivirus** para ver las directivas en esa categoría. Para obtener ayuda para administrar la configuración de seguridad en Intune, comience con Administrar la seguridad de los puntos de conexión en Microsoft Intune.

Visualización o edición de directivas de firewall y reglas personalizadas

En función de si usa el portal de Microsoft 365 Defender o el centro de administración de Microsoft Endpoint Manager para administrar la protección del firewall, use uno de los procedimientos de la tabla siguiente:

PORTAL	PROCEDURE

PORTAL	PROCEDURE
portal de Microsoft 365 Defender (https://security.microsoft.com)	1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión. 2. En el panel de navegación, elija **Configuración del dispositivo**. Las directivas se organizan por sistema operativo y tipo de directiva. 3. Seleccione una pestaña del sistema operativo (por ejemplo **, Windows clientes**). 4. Expanda **Firewall** para ver la lista de directivas. 5. Seleccione una directiva para ver más detalles sobre la directiva. Para realizar cambios o obtener más información sobre la configuración de directivas, consulte los artículos siguientes: - Visualización o edición de directivas de dispositivo - Configuración del firewall - Administración de reglas personalizadas para directivas de firewall
Microsoft Endpoint Manager centro de administración (https://endpoint.microsoft.com)	1. Vaya a https://endpoint.microsoft.com e inicie sesión. Ahora está en el centro de administración de Endpoint Manager. 2. Seleccione **Seguridad del punto de conexión**. 3. Seleccione **Firewall** para ver las directivas en esa categoría. Las reglas personalizadas que se definen para la protección del firewall se enumeran como directivas independientes. Para obtener ayuda para administrar la configuración de seguridad en Intune, comience con Administrar la seguridad de los puntos de conexión en Microsoft Intune.

Configuración del filtrado de contenido web

El filtrado de contenido web permite al equipo de seguridad realizar un seguimiento y regular el acceso a sitios web en función de sus categorías de contenido, como:

- Contenido para adultos: Sitios relacionados con cultos, juegos de azar, desnudez, pornografía, material sexualmente explícito o violencia
- Ancho de banda alto: descarga de sitios, sitios de uso compartido de imágenes o hosts punto a punto
- Responsabilidad legal: Sitios que incluyen imágenes de abuso infantil, promueven actividades ilegales, fomentan plagios o engaños escolares, o que promueven actividades dañinas
- Ocio: sitios que proporcionan salas de chat basadas en web, juegos en línea, correo electrónico basado en web o redes sociales
- Sin categoría: sitios que no tienen contenido o que recién están registrados

No todos los sitios web de estas categorías son malintencionados, pero podrían ser problemáticos para su empresa debido a las regulaciones de cumplimiento, el uso de ancho de banda u otros problemas. Además, puede crear una directiva de solo auditoría para comprender mejor si el equipo de seguridad debe bloquear las categorías de sitios web.

El filtrado de contenido web está disponible en los principales exploradores web, con bloques realizados por Windows Defender SmartScreen (Microsoft Edge) y Network Protection (Chrome, Firefox, Brave y Opera). Para

obtener más información, consulte Requisitos previos para el filtrado de contenido web.

Para configurar el filtrado de contenido web

1. En el portal de Microsoft 365 Defender (https://security.microsoft.com), elija **Configuración** > **Filtro de** > contenido web **+ Agregar directiva**.
2. Especifique un nombre y una descripción para la directiva.
3. Seleccione las categorías que desea bloquear. Use el icono expandir para expandir por completo cada categoría primaria y seleccionar categorías de contenido web específicas. Para configurar una directiva de solo auditoría que no bloquee ningún sitio web, no seleccione ninguna categoría.

   No seleccione **Sin categoría**.
4. Especifique el ámbito de la directiva seleccionando grupos de dispositivos para aplicar la directiva. Solo se impedirá que los dispositivos de los grupos de dispositivos seleccionados accedan a sitios web de las categorías seleccionadas.
5. Revise el resumen y guarde la directiva. La actualización de la directiva puede tardar hasta 2 horas en aplicarse a los dispositivos seleccionados.

> **TIP**
> Para más información sobre el filtrado de contenido web, consulte Filtrado de contenido web.

Revisar la configuración de las características avanzadas

Además de las directivas de filtrado de contenido web, firewall y protección de última generación, Defender for Business incluye características de seguridad avanzadas. Estas características se preconfigura mediante la configuración recomendada; sin embargo, puede revisarlos y, si es necesario, editar la configuración para satisfacer sus necesidades empresariales.

Para acceder a la configuración de las características avanzadas, en el portal de Microsoft 365 Defender (https://security.microsoft.com), vaya a **Configuración** > Características **avanzadas generales** > **deEndpoints** > .

En la tabla siguiente se describe la configuración de las características avanzadas:

CONFIGURACIÓN	DESCRIPCIÓN

CONFIGURACIÓN	DESCRIPCIÓN
Investigación automatizada (activado de forma predeterminada)	A medida que se generan alertas, pueden producirse investigaciones automatizadas. Cada investigación automatizada determina si una amenaza detectada requiere acción y, a continuación, realiza (o recomienda) acciones de corrección (como enviar un archivo a cuarentena, detener un proceso, aislar un dispositivo o bloquear una dirección URL). Durante la ejecución de una investigación, todas las demás alertas relacionadas que puedan surgir se agregarán a la investigación hasta que se finalice. Si ve una entidad afectada en otro lugar, la investigación automatizada expande su ámbito para incluir esa entidad, y el proceso de investigación se repite. Puede ver las investigaciones en la página **Incidentes** . Seleccione un incidente y, a continuación, seleccione la pestaña **Investigaciones** . De forma predeterminada, las funcionalidades automatizadas de investigación y respuesta están activadas, en todo el inquilino. **Se recomienda mantener activada la investigación automatizada**. Si la desactiva, la protección en tiempo real en Antivirus de Microsoft Defender se verá afectada y su nivel general de protección se reducirá. Obtenga más información sobre las investigaciones automatizadas.
Respuesta dinámica	Defender for Business incluye los siguientes tipos de acciones de respuesta manual: - Ejecutar examen de antivirus - Aislar el dispositivo - Detener y poner en cuarentena un archivo - Agregar un indicador para bloquear o permitir un archivo Obtenga más información sobre las acciones de respuesta.
Respuesta dinámica para servidores	(Esta configuración no está disponible actualmente en Defender para empresas)
Ejecución de script sin firmar de Respuesta dinámica	(Esta configuración no está disponible actualmente en Defender para empresas)
Habilitar EDR en modo de bloque (activado de forma predeterminada)	Proporciona protección adicional contra artefactos malintencionados cuando Antivirus de Microsoft Defender no es el producto antivirus principal y se ejecuta en modo pasivo en un dispositivo. La detección y respuesta de puntos de conexión (EDR) en modo de bloque funciona en segundo plano para corregir artefactos malintencionados detectados por EDR funcionalidades. Es posible que el producto antivirus principal que no es de Microsoft haya perdido estos artefactos. Obtenga más información sobre EDR en modo de bloque.

CONFIGURACIÓN	DESCRIPCIÓN
Permitir o bloquear un archivo (activado de forma predeterminada)	Permite permitir o bloquear un archivo mediante indicadores. Esta funcionalidad requiere que Antivirus de Microsoft Defender esté en modo activo y que se active la protección en la nube. El bloqueo de un archivo impedirá que se lea, escriba o ejecute en dispositivos de la organización. Obtenga más información sobre los indicadores de los archivos.
Indicadores de red personalizados (activado de forma predeterminada)	Permite permitir o bloquear una dirección IP, una dirección URL o un dominio mediante indicadores de red. Esta funcionalidad requiere que Antivirus de Microsoft Defender esté en modo activo y que se active la protección de red. Puede permitir o bloquear direcciones IP, direcciones URL o dominios en función de su propia inteligencia sobre amenazas. También puede advertir a los usuarios con un mensaje si abren una aplicación de riesgo. El símbolo del sistema no les impedirá usar la aplicación, pero puede proporcionar una advertencia para los usuarios. Obtenga más información sobre la protección de red.
Protección contra alteraciones (se recomienda activar esta configuración)	La protección contra alteraciones evita que las aplicaciones malintencionadas realicen acciones como: - Deshabilitación de la protección contra amenazas y virus - Deshabilitación de la protección en tiempo real - Desactivar la supervisión del comportamiento - Deshabilitación de la protección en la nube - Eliminación de actualizaciones de inteligencia de seguridad - Deshabilitación de acciones automáticas en las amenazas detectadas La protección contra alteraciones básicamente bloquea Antivirus de Microsoft Defender a sus valores seguros y predeterminados e impide que las aplicaciones y los métodos no autorizados cambien la configuración de seguridad. Obtenga más información sobre la protección contra alteraciones.
Mostrar los detalles del usuario (activado de forma predeterminada)	Permite a los usuarios de su organización ver detalles, como la imagen, el nombre, el título y el departamento de los empleados. Estos detalles se almacenan en Azure Active Directory (Azure AD). Obtenga más información sobre los perfiles de usuario en Azure AD.
integración Skype Empresarial (activado de forma predeterminada)	Skype Empresarial se retiró en julio de 2021. Si aún no se ha movido a Microsoft Teams, consulte Configuración de Microsoft Teams en su pequeña empresa. La integración con Microsoft Teams (o el Skype Empresarial anterior) permite la comunicación con un solo clic entre las personas de su empresa.

CONFIGURACIÓN	DESCRIPCIÓN
Filtrado de contenido web (activado de forma predeterminada)	Bloquear el acceso a sitios web que contienen contenido no deseado y realizar un seguimiento de la actividad web en todos los dominios. Consulte Configuración del filtrado de contenido web.
conexión Microsoft Intune (Se recomienda activar esta configuración si tiene Intune)	Si la suscripción de su organización incluye Microsoft Intune (incluida en Microsoft 365 Empresa Premium), esta configuración permite a Defender for Business compartir información sobre los dispositivos con Intune.
Detección de dispositivo (activado de forma predeterminada)	Permite al equipo de seguridad encontrar dispositivos no administrados conectados a la red de la empresa. Los dispositivos desconocidos y no administrados presentan riesgos significativos para la red, ya sea una impresora sin revisiones, dispositivos de red con configuraciones de seguridad débiles o un servidor sin controles de seguridad. La detección de dispositivos usa dispositivos incorporados para detectar dispositivos no administrados, de modo que el equipo de seguridad pueda incorporar los dispositivos no administrados y reducir la vulnerabilidad. Obtenga más información sobre la detección de dispositivos.
Versión preliminar de las características	Microsoft actualiza continuamente servicios, como Defender para empresas, para incluir nuevas mejoras y funcionalidades de características. Si opta por recibir características en versión preliminar, será uno de los primeros en probar las próximas características en la experiencia en versión preliminar. Obtenga más información sobre las características en versión preliminar.

Visualización y edición de otras configuraciones en el portal de Microsoft 365 Defender

Además de las directivas de seguridad que se aplican a los dispositivos, hay otras configuraciones que puede ver y editar en Defender para empresas. Por ejemplo, especifica la zona horaria que se va a usar y puede incorporar (o fuera del panel) dispositivos.

> **NOTE**
> Es posible que vea más opciones de configuración en el inquilino de las que se enumeran en este artículo. En este artículo se resalta la configuración más importante que debe revisar en Defender para empresas.

Configuración revisar para Defender para empresas

En la tabla siguiente se describe la configuración que se va a ver (y, si es necesario, editar) en Defender for Business:

CATEGORÍA	CONFIGURACIÓN	DESCRIPCIÓN

CATEGORÍA	CONFIGURACIÓN	DESCRIPCIÓN
Security Center	**Zona horaria**	Seleccione la zona horaria que se usará para las fechas y horas que se muestran en incidentes, amenazas detectadas e investigación automatizada & corrección. Puede usar UTC o la zona horaria local (*recomendado*).
Microsoft 365 Defender	**Account**	Vea los detalles, como dónde se almacenan los datos, el identificador de inquilino y el identificador de la organización (organización).
Microsoft 365 Defender	**Versión preliminar de las características**	Active las características en versión preliminar para probar las próximas características y nuevas funcionalidades. Puede estar entre las primeras en obtener una vista previa de las nuevas características y proporcionar comentarios.
Puntos de conexión	**Notificaciones de correo electrónico**	Configure o edite las reglas de notificación por correo electrónico. Cuando se detectan vulnerabilidades o se crea una alerta, los destinatarios especificados en las reglas de notificación por correo electrónico recibirán un correo electrónico. Obtenga más información sobre las notificaciones por correo electrónico.
Puntos de conexión	**Administración de dispositivos > Incorporación**	Incorporación de dispositivos a Defender for Business mediante un script descargable. Para más información, consulte Incorporación de dispositivos para Microsoft Defender para Empresas.
Puntos de conexión	**Administración de dispositivos > Offboarding**	Dispositivos offboard (quitar) de Defender for Business. Al desconectar un dispositivo, ya no envía datos a Defender for Business, pero se conservan los datos recibidos antes de la retirada. Para obtener más información, consulte Offboarding a device (Offboarding a device).

Acceso a la configuración en el portal de Microsoft 365 Defender

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com/) e inicie sesión.
2. Seleccione **Configuración** y, a continuación, seleccione una categoría (como **Security Center**, **Microsoft 365 Defender** o **Puntos de conexión**).
3. En la lista de configuraciones, seleccione un elemento para ver o editar.

Pasos siguientes

Continúe con una o varias de las siguientes tareas:

- Comenzar mediante Microsoft Defender para Empresas
- Administración de dispositivos en Microsoft Defender para Empresas
- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Ver o editar directivas en Microsoft Defender para Empresas

Use el panel de administración de vulnerabilidades de Threat & en Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

Microsoft Defender para Empresas incluye un panel de administración de vulnerabilidades & amenazas que está diseñado para ahorrar tiempo y esfuerzo al equipo de seguridad. Además de proporcionar una puntuación de exposición, también puede ver información sobre los dispositivos expuestos y las recomendaciones de seguridad. Puede usar el panel de administración de vulnerabilidades de Threat & para:

- Visualización de la puntuación de exposición, que está asociada a los dispositivos de la empresa
- Vea las principales recomendaciones de seguridad, como abordar las comunicaciones con dispositivos con problemas, activar la protección del firewall o actualizar las definiciones de Antivirus de Microsoft Defender
- Ver las actividades de corrección, como los archivos que se enviaron a la cuarentena o las vulnerabilidades encontradas en los dispositivos

¿Quieres ver cómo funciona? Vea este vídeo, que describe Administración de vulnerabilidades de Microsoft Defender.

Más información sobre Administración de vulnerabilidades de Microsoft Defender.

Pasos siguientes

- Tutoriales y simulaciones en Microsoft Defender para Empresas
- Incorporación de dispositivos a Microsoft Defender para Empresas
- Ver o editar directivas en Microsoft Defender para Empresas

Visualización y administración de incidentes en Microsoft Defender para Empresas

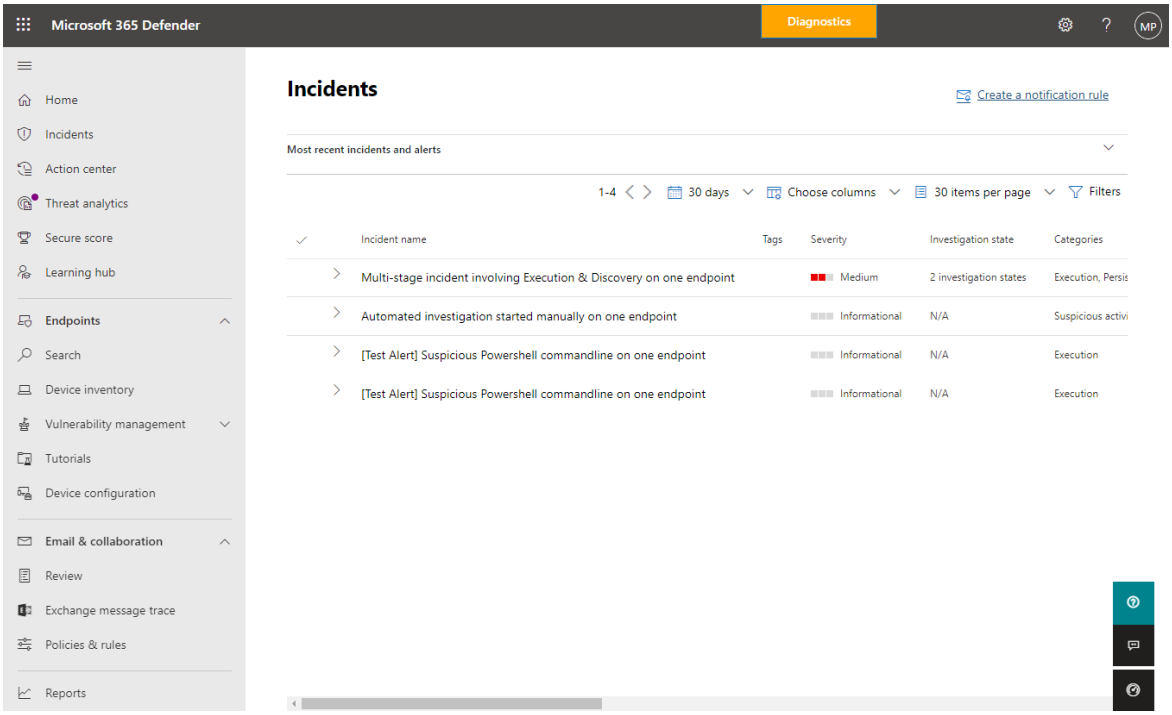
21/06/2022 • 2 minutes to read

A medida que se detectan amenazas y se desencadenan alertas, se crean incidentes. El equipo de seguridad de la empresa puede ver y administrar incidentes en el portal de Microsoft 365 Defender.

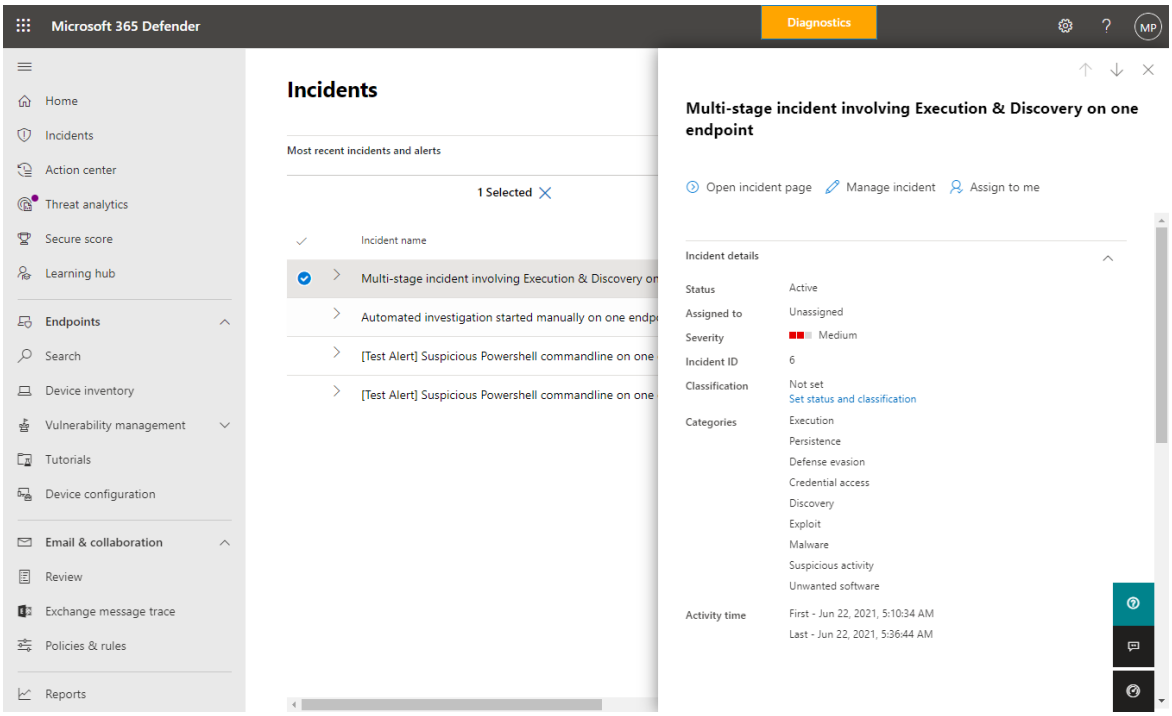
En este artículo se incluyen:

Supervisión de los incidentes & alertas

1. En el portal de Microsoft 365 Defender (https://security.microsoft.com), en el panel de navegación, seleccione **Incidentes**. Los incidentes que se crearon aparecen en la página.



2. Seleccione una alerta para abrir su panel flotante, donde puede obtener más información sobre la alerta.



3. En el panel flotante, puede ver el título de la alerta, ver una lista de recursos (como puntos de conexión o cuentas de usuario) que se vieron afectados, realizar acciones disponibles y usar vínculos para ver más información e incluso abrir la página de detalles de la alerta seleccionada.

> **TIP**
> Microsoft Defender para Empresas está diseñado para ayudarle a abordar las amenazas detectadas mediante la oferta de acciones recomendadas. Cuando vea una alerta, busque las acciones recomendadas que debe realizar. Tome nota también de la gravedad de la alerta, que se determina no solo en función de la gravedad de la amenaza, sino también del nivel de riesgo para su empresa.

Gravedad de la alerta

Cuando Antivirus de Microsoft Defender asigna una gravedad de alerta basada en la gravedad absoluta de una amenaza detectada (malware) y el riesgo potencial para un punto de conexión individual (si está infectado). Microsoft Defender para Empresas asigna una gravedad de alerta en función de la gravedad del comportamiento detectado, el riesgo real para un punto de conexión (dispositivo) y, lo que es más importante, el riesgo potencial para la empresa. En la tabla siguiente se enumeran algunos ejemplos:

ESCENARIO	GRAVEDAD DE LA ALERTA	REASON
Antivirus de Microsoft Defender detecta y detiene una amenaza antes de que se produzcan daños.	Informativo	La amenaza se detuvo antes de que se realizara cualquier daño.
Antivirus de Microsoft Defender detecta el malware que se estaba ejecutando dentro de la empresa. El malware se detiene y se corrige.	Bajo	Aunque es posible que se haya producido algún daño en un punto de conexión individual, el malware no supone ninguna amenaza para su empresa.
Microsoft Defender para Empresas detecta el malware que se está ejecutando. El malware se bloquea casi inmediatamente.	Medio o alto	El malware supone una amenaza para puntos de conexión individuales y para su empresa.

ESCENARIO	GRAVEDAD DE LA ALERTA	REASON
Se detecta un comportamiento sospechoso, pero aún no se realizan acciones correctivas.	Bajo, Medio o Alto	La gravedad depende del grado en que el comportamiento supone una amenaza para la empresa.

Pasos siguientes

- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Revisión de las acciones de corrección en el Centro de acciones
- Ver o editar directivas de dispositivo en Microsoft Defender para Empresas

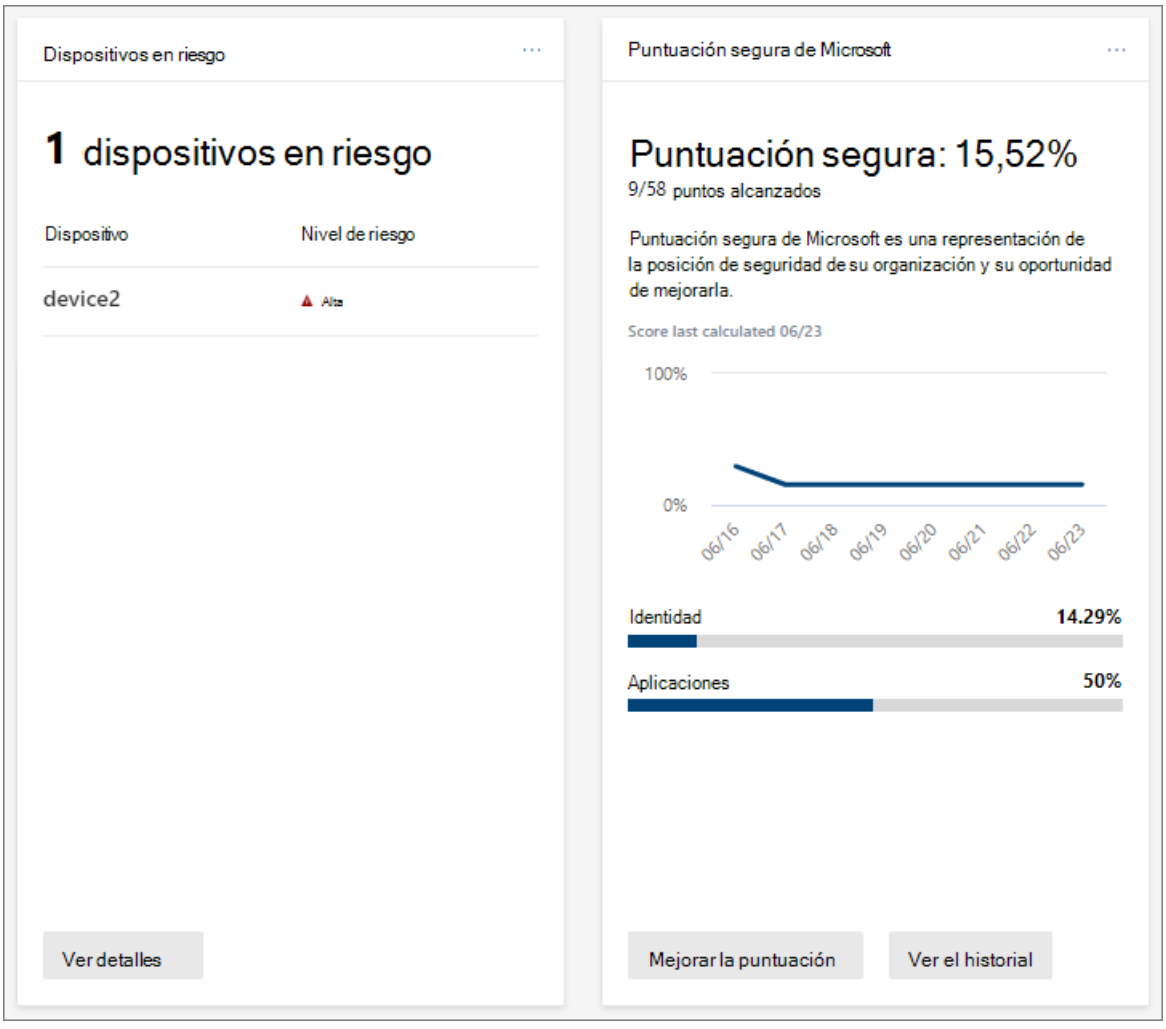
Respuesta y mitigación de amenazas en Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

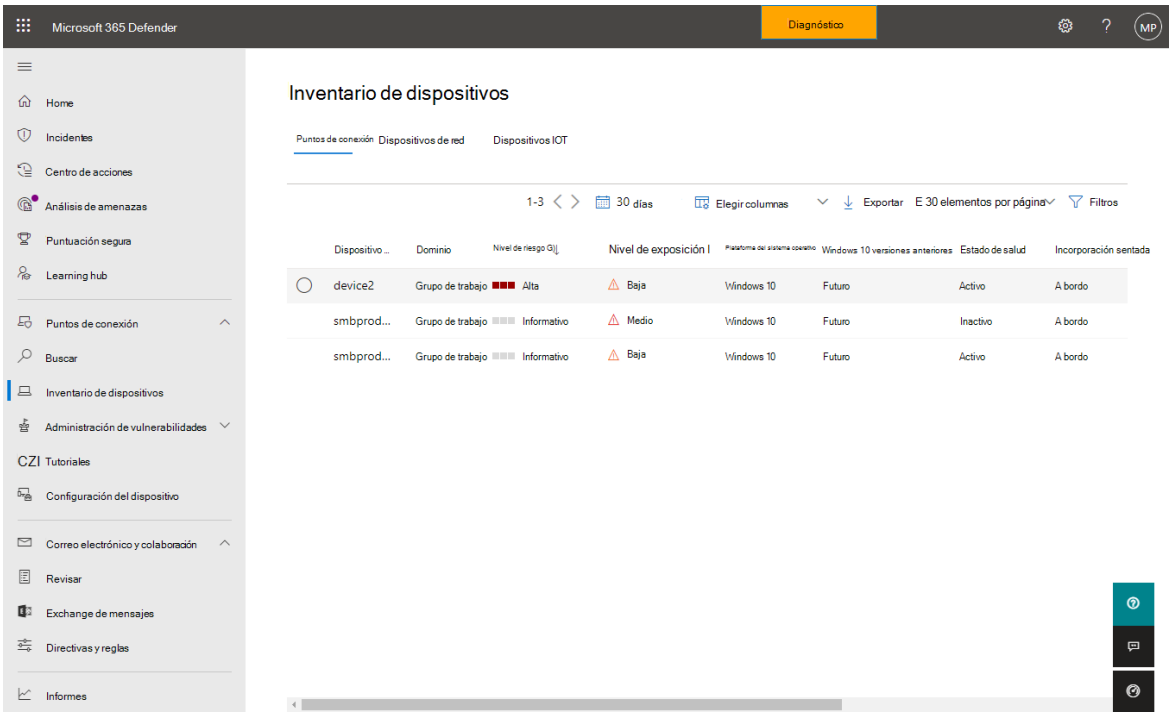
El portal de Microsoft 365 Defender permite al equipo de seguridad responder y mitigar las amenazas detectadas. Este artículo le guiará a través de un ejemplo de cómo puede usar Defender para empresas.

Visualización de las amenazas detectadas

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. Observe las tarjetas en la página principal. Las tarjetas le indican de un vistazo cuántas amenazas se detectaron, junto con cuántas cuentas de usuario, puntos de conexión (dispositivos) y otros recursos se vieron afectados. La siguiente imagen es un ejemplo de tarjetas que puede ver:

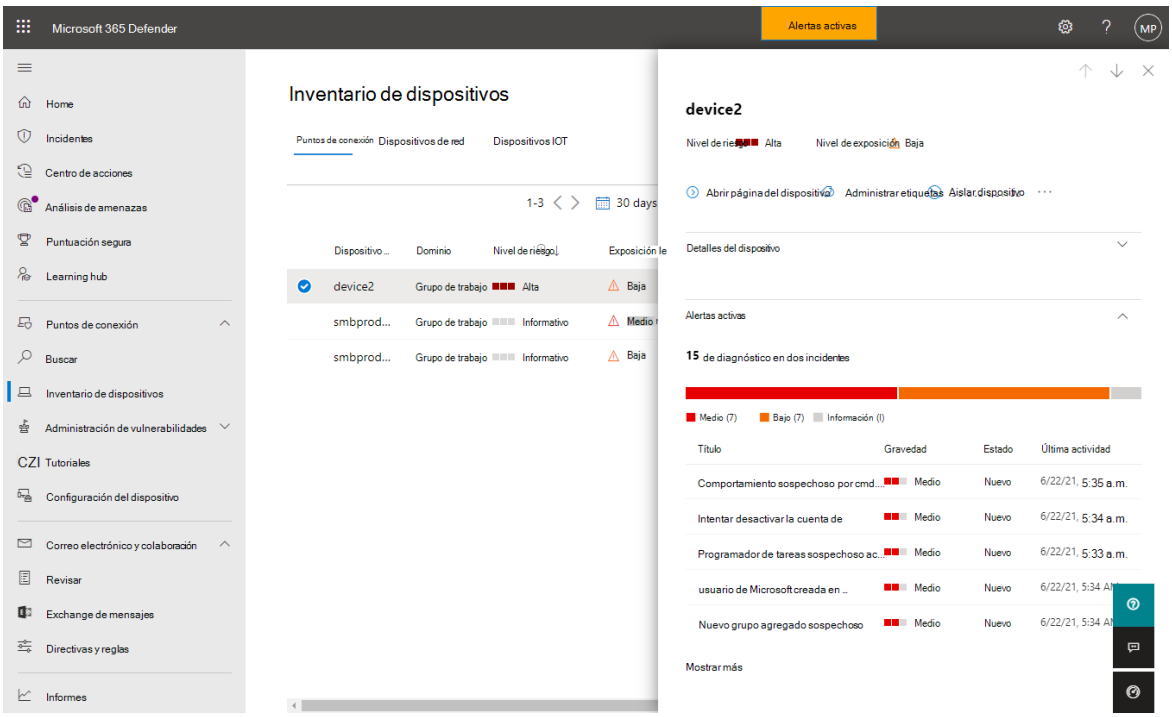


3. Seleccione un botón o vínculo en la tarjeta para ver más información y tomar medidas. Por ejemplo, nuestra tarjeta **Dispositivos en riesgo** incluye un botón **Ver detalles** . Al seleccionar ese botón, se nos lleva a la página **Inventario** de dispositivos, como se muestra en la siguiente imagen:

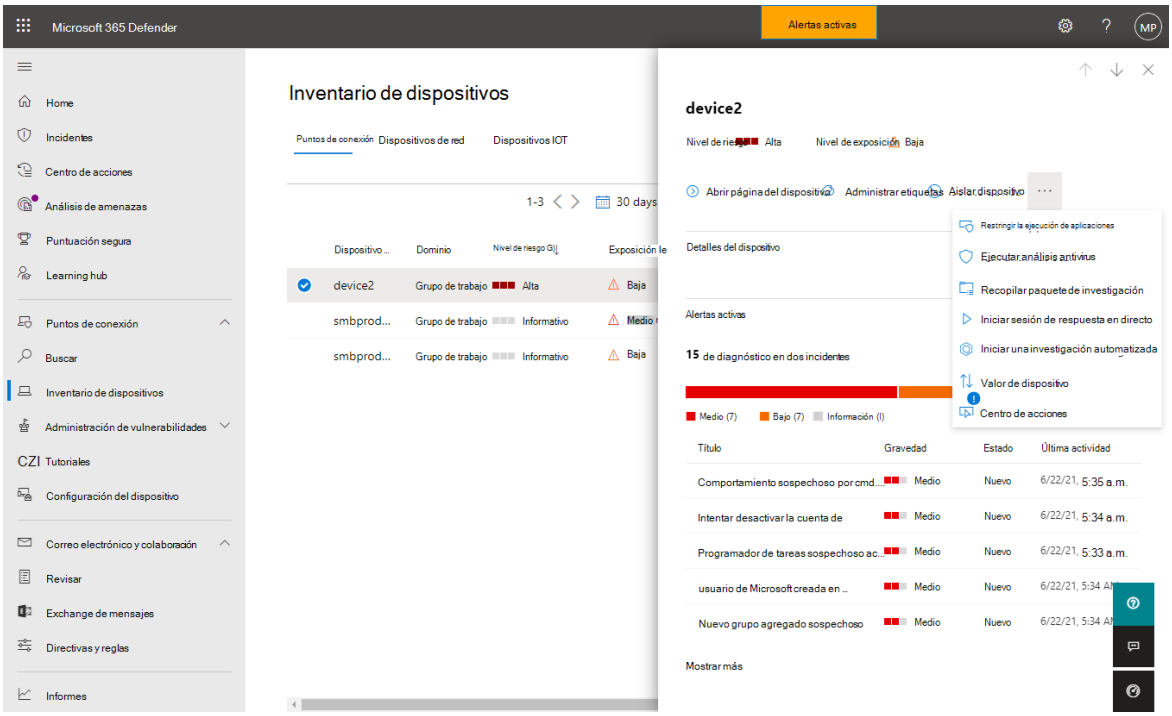


En la página **Inventario de** dispositivos se enumeran los dispositivos de la empresa, junto con su nivel de riesgo y nivel de exposición.

4. Seleccione un elemento, como un dispositivo. Se abre un panel flotante y muestra más información sobre las alertas y los incidentes generados para ese elemento, como se muestra en la siguiente imagen:



5. En el control flotante, vea la información que se muestra. Seleccione los puntos suspensivos (...) para abrir un menú que enumera las acciones disponibles, como se muestra en la siguiente imagen:



6. Seleccione una acción disponible. Por ejemplo, puede elegir **Ejecutar examen antivirus**, lo que hará que Antivirus de Microsoft Defender inicie un examen rápido en el dispositivo. O bien, podría seleccionar **Iniciar investigación automatizada** para desencadenar una investigación automatizada en el dispositivo.

Pasos siguientes

- Revisión de las acciones de corrección en el Centro de acciones
- Administración de dispositivos en Microsoft Defender para Empresas
- Visualización y administración de incidentes en Microsoft Defender para Empresas

Revisión de las acciones de corrección en el Centro de acciones

21/06/2022 • 2 minutes to read

A medida que se detectan amenazas, entran en juego las acciones de corrección. En función de la amenaza en particular y de cómo se configure la configuración de seguridad, es posible que las acciones de corrección se realicen automáticamente o solo tras la aprobación. Entre los ejemplos de acciones de corrección se incluyen el envío de un archivo a la cuarentena, la detención de la ejecución de un proceso y la eliminación de una tarea programada. Todas las acciones de corrección se realizan en el Centro de acciones.

En este artículo se describe:

- Uso del Centro de acción
- Acciones de corrección

Uso del Centro de acción

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. En el panel de navegación, elija **Centro de actividades**.
3. Seleccione la pestaña **Pendiente** para ver y aprobar (o rechazar) las acciones pendientes. Estas acciones pueden surgir de la protección antivirus/antimalware, las investigaciones automatizadas, las actividades de contestación manual o las sesiones de respuesta inmediata.
4. Seleccione la pestaña **Historial** para ver una lista de las acciones completadas.

Acciones de corrección

Microsoft Defender para Empresas incluye varias acciones de corrección. Estas acciones incluyen acciones de contestación manual, acciones después de la investigación automatizada y acciones de respuesta inmediata.

En la tabla siguiente se enumeran las acciones de corrección que están disponibles:

ORIGEN	ACCIONES

ORIGEN	ACCIONES
Investigaciones automatizadas	- Poner en cuarentena un archivo - Quitar una clave del registro - Eliminación de un proceso - Detener un servicio - Deshabilitar un controlador - Quitar una tarea programada
Acciones de contestación manual	- Ejecutar examen de antivirus - Aislar el dispositivo - Detener y poner en cuarentena - Agregar un indicador para bloquear o permitir un archivo
Respuesta inmediata	- Recopilación de datos forenses - Análisis de un archivo - Ejecutar un script - Envío de una entidad sospechosa a Microsoft para su análisis - Corrección de un archivo - Buscar amenazas de forma proactiva

Pasos siguientes

- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Administración de dispositivos en Microsoft Defender para Empresas

Informes en Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

Hay varios informes disponibles en el portal de Microsoft 365 Defender (https://security.microsoft.com). En este artículo se describen estos informes, cómo puede usarlos y cómo encontrarlos.

Informes en Defender para empresas

INFORME	DESCRIPCIÓN
Informe de seguridad	El informe de seguridad proporciona información sobre las identidades, los dispositivos y las aplicaciones de la empresa. Para acceder a este informe, en el panel de navegación, elija Informe de seguridad **general** > **de informes** > . **PROPINA** Puede ver información similar en la página principal del portal de Microsoft 365 Defender (https://security.microsoft.com).
Protección contra amenazas	El informe de protección contra amenazas proporciona información sobre alertas y tendencias de alertas. Use la columna **Tendencias de alertas** para ver información sobre las alertas que se desencadenaron en los últimos 30 días. Use la columna **Estado de alerta** para ver la información de instantáneas actual sobre alertas, como categorías de alertas sin resolver y su clasificación. Para acceder a este informe, en el panel de navegación, elija **Informes** > **puntos de conexión** > **Protección contra amenazas**. **SUGERENCIA**: También puede usar la lista **Incidentes** para ver información sobre las alertas. En el panel de navegación, elija **Incidentes** para ver y administrar los incidentes actuales. Para más información, consulte Visualización y administración de incidentes en Microsoft Defender para Empresas.
Cumplimiento y mantenimiento del dispositivo	El informe de estado y cumplimiento del dispositivo proporciona información sobre el estado y las tendencias del dispositivo. Puede usar este informe para determinar si los sensores de Defender for Business funcionan correctamente en los dispositivos y el estado actual de Antivirus de Microsoft Defender. Para acceder a este informe, en el panel de navegación, elija **Informes** > de estado **y cumplimiento del dispositivo** de **puntos** > de conexión. **SUGERENCIA**: Puede usar la lista **Inventario** de dispositivos para ver información sobre los dispositivos de su empresa. En el panel de navegación, elija **Inventario de dispositivos**. Para más información, consulte Administración de dispositivos en Microsoft Defender para Empresas.

INFORME	DESCRIPCIÓN
Dispositivos vulnerables	El informe de dispositivos vulnerables proporciona información sobre los dispositivos y las tendencias. Use la columna **Tendencias** para ver información sobre los dispositivos que han tenido alertas en los últimos 30 días. Use la columna **Estado** para ver la información de instantáneas actual sobre los dispositivos que tienen alertas. Para acceder a este informe, en el panel de navegación, elija Dispositivos **vulnerables** de **puntos** > de conexión de **informes** > . **SUGERENCIA**: Puede usar la lista **Inventario** de dispositivos para ver información sobre los dispositivos de su empresa. En el panel de navegación, elija **Inventario de dispositivos**. Para más información, consulte Administración de dispositivos en Microsoft Defender para Empresas.
Protección web	El informe de protección web muestra los intentos de acceder a sitios de phishing, vectores de malware, sitios de vulnerabilidades de seguridad, sitios que no son de confianza o de baja reputación y sitios que están bloqueados explícitamente. Las categorías de sitios bloqueados incluyen contenido para adultos, sitios de ocio, sitios de responsabilidad legal, etc. Para acceder a este informe, en el panel de navegación, elija Protección **web** de **puntos** > de conexión **de informes** > . **SUGERENCIA**: Si aún no ha configurado la protección web para su empresa, elija el botón **Configuración** en una vista de informe. A continuación, en **Reglas**, elija **Filtrado de contenido web**. Para más información sobre el filtrado de contenido web, consulte Filtrado de contenido web.

Consulte también

- Comenzar mediante Microsoft Defender para Empresas
- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Administración de dispositivos en Microsoft Defender para Empresas

Ver o editar directivas en Microsoft Defender para Empresas

21/06/2022 • 4 minutes to read

En Microsoft Defender para Empresas, la configuración de seguridad se configura mediante directivas que se aplican a los dispositivos. Para simplificar la experiencia de configuración y configuración, Defender for Business incluye directivas preconfiguradas para ayudar a proteger los dispositivos de su empresa en cuanto se incorporan. Puede usar las directivas predeterminadas, editar directivas o crear sus propias directivas.

En este artículo se describe cómo:

Directivas predeterminadas en Defender para empresas

En Defender para empresas, hay dos tipos principales de directivas para proteger los dispositivos de su empresa:

- **Directivas de protección de última generación**, que determinan la configuración de Antivirus de Microsoft Defender y otras características de protección contra amenazas
- **Directivas de firewall**, que determinan qué tráfico de red puede fluir hacia y desde los dispositivos de la empresa

Ver las directivas existentes

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. En el panel de navegación, elija **Configuración del dispositivo**. Las directivas se organizan por sistema operativo (como **Cliente de Windows**) y por tipo de directiva (como **Protección de última generación** y **Firewall**).
3. Seleccione una pestaña del sistema operativo (por ejemplo, **clientes de Windows**) y, a continuación, revise la lista de directivas en las categorías **Protección de última generación** y **Firewall**.
4. Para ver más detalles sobre una directiva, seleccione su nombre. Se abre un panel lateral que proporciona más información sobre la directiva, por ejemplo, qué dispositivos están protegidos por esa directiva.

Editar una directiva existente

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. En el panel de navegación, elija **Configuración del dispositivo**. Las directivas se organizan por sistema operativo (como **Cliente de Windows**) y por tipo de directiva (como **Protección de última generación** y **Firewall**).
3. Seleccione una pestaña del sistema operativo (por ejemplo, **clientes de Windows**) y, a continuación, revise la lista de directivas en las categorías **Protección de última generación** y **Firewall**.
4. Para editar una directiva, seleccione su nombre y, a continuación, elija **Editar**.

5. En la pestaña **Información general**, revise la información. Si es necesario, puede editar la descripción. A continuación, elija **Siguiente**.

6. En la pestaña **Grupos de dispositivos**, determine qué grupos de dispositivos deben recibir esta directiva.

   - Para dejar el grupo de dispositivos seleccionado tal y como está, elija **Siguiente**.
   - Para quitar un grupo de dispositivos de la directiva, seleccione **Quitar**.
   - Para configurar un nuevo grupo de dispositivos, seleccione **Crear nuevo grupo** y, a continuación, configure el grupo de dispositivos. (Para obtener ayuda con esta tarea, consulte Grupos de dispositivos en Microsoft Defender para Empresas).
   - Para aplicar la directiva a otro grupo de dispositivos, seleccione **Usar grupo existente**.

   Después de especificar qué grupos de dispositivos deben recibir la directiva, elija **Siguiente**.

7. En la pestaña **Opciones de configuración**, revise la configuración. Si es necesario, puede editar la configuración de la directiva. Para obtener ayuda con esta tarea, consulte los artículos siguientes:

   - Comprender las opciones de configuración de última generación
   - Configuración de firewall

   Una vez que haya especificado las opciones de configuración de protección de última generación, elija **Siguiente**.

8. En la pestaña **Revisar la directiva**, revise la información general, los dispositivos de destino y las opciones de configuración.

   - Si necesita realizar cambios, seleccione **Editar**.
   - Cuando esté listo para continuar, elija **Actualizar directiva**.

Crear una nueva directiva

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.

2. En el panel de navegación, elija **Configuración del dispositivo**. Las directivas se organizan por sistema operativo (como **Cliente de Windows**) y por tipo de directiva (como **Protección de última generación** y **Firewall**).

3. Seleccione una pestaña del sistema operativo (por ejemplo, **clientes de Windows**) y, a continuación, revise la lista de directivas de **Protección de última generación**.

4. En **Protección de última generación** o **Firewall**, seleccione **+ Agregar**.

5. En la pestaña **Información general**, siga estos pasos:

   a. Especifique un nombre y una descripción. Esta información le ayudará a usted y a los miembros de su equipo a identificarla más adelante.
   b. Revise el orden de la directiva y edítelo si fuera necesario. (Para obtener más información, consulte Orden de directiva).
   c. Elija **Siguiente**.

6. En la pestaña **Grupos de dispositivos**, cree un nuevo grupo de dispositivos o use un grupo existente. Las directivas se asignan a los dispositivos a través de grupos de dispositivos. Estos son algunos aspectos que debe tener en cuenta:

   - Inicialmente, es posible que solo tenga el grupo de dispositivos predeterminado, que incluye los dispositivos que usan los usuarios de su empresa para acceder a los datos y el correo electrónico de la empresa. Puede conservar y usar el grupo de dispositivos predeterminado.
   - Cree un nuevo grupo de dispositivos para aplicar una directiva con una configuración específica que

sea diferente de la directiva predeterminada.

- Al configurar el grupo de dispositivos, se especifican determinados criterios, como la versión del sistema operativo. Los dispositivos que cumplen los criterios se incluyen en ese grupo de dispositivos, a menos que se excluyan.
- Todos los grupos de dispositivos, incluidos los grupos de dispositivos predeterminados y personalizados que defina, se almacenan en Azure Active Directory (Azure AD).

Para más información sobre los grupos de dispositivos, consulte Grupos de dispositivos en Defender para empresas.

7. En la pestaña **Opciones de configuración**, especifique la configuración de la directiva y, a continuación, elija **Siguiente**. Para obtener más información sobre la configuración individual, consulte Configuración para Microsoft Defender para Empresas.

8. En la pestaña **Revisar la directiva**, revise la información general, los dispositivos de destino y las opciones de configuración.

   - Si necesita realizar cambios, seleccione **Editar**.
   - Cuando esté listo para continuar, elija **Crear directiva**.

Pasos siguientes

Elija una o varias de las siguientes tareas:

- Administrar dispositivos
- Creación de una nueva directiva en Microsoft Defender para Empresas
- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Revisión de las acciones de corrección en el Centro de acciones

Descripción del orden de la directiva en Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

Orden de la directiva en Microsoft Defender para Empresas

Microsoft Defender para Empresas incluye directivas predefinidas para ayudar a garantizar que los dispositivos que usan los empleados estén protegidos. El equipo de seguridad también puede agregar nuevas directivas. Por ejemplo, supongamos que desea aplicar ciertas configuraciones a algunos dispositivos y configuraciones diferentes a otros dispositivos. Para ello, agregue directivas, como directivas de protección de próxima generación o directivas de firewall.

A medida que se agregan directivas, observará que se asigna un orden de prioridad. Puede editar el orden de prioridad de las directivas que defina, pero no puede cambiar el orden de prioridad de las directivas predeterminadas. Por ejemplo, supongamos que, para los dispositivos cliente Windows, tiene tres directivas de protección de próxima generación. En este caso, la directiva predeterminada es el número 3 en prioridad. Puede cambiar el orden de las directivas numeradas 1 y 2, pero la directiva predeterminada seguirá siendo el número 3 de la lista.

Lo importante que hay que recordar sobre varias directivas es que los dispositivos solo recibirán la primera directiva aplicada. En referencia a nuestro ejemplo anterior de tres directivas de próxima generación, supongamos que tiene dispositivos destinados a las tres directivas. En este caso, esos dispositivos recibirán el número de directiva 1, pero no recibirán las directivas numeradas 2 y 3.

Puntos clave para recordar sobre el orden de la directiva

- A las directivas se les asigna un orden de prioridad.
- Los dispositivos solo reciben la primera directiva aplicada.
- Puede cambiar el orden de prioridad de las directivas.
- Las directivas predeterminadas tienen el orden de prioridad más bajo.

Pasos siguientes

- Comenzar mediante Defender para empresas
- Administrar dispositivos
- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Revisión de las acciones de corrección en el Centro de acciones

Descripción de la configuración de próxima generación en Microsoft Defender para Empresas

21/06/2022 • 8 minutes to read

La protección de última generación en Defender for Business incluye antivirus sólidos y protección antimalware. Las directivas predeterminadas están diseñadas para proteger los dispositivos y los usuarios sin obstaculizar la productividad; sin embargo, también puede personalizar las directivas para satisfacer sus necesidades empresariales. Además, si usa Microsoft Intune, puede usar el centro de administración de Microsoft Endpoint Manager para administrar las directivas de seguridad.

En este artículo se describe:

Configuración y opciones de protección de última generación

En la tabla siguiente se enumeran la configuración y las opciones:

CONFIGURACIÓN	DESCRIPCIÓN
Protección en tiempo real	
Activar la protección en tiempo real	Habilitada de forma predeterminada, la protección en tiempo real busca y evita que el malware se ejecute en los dispositivos. *Se recomienda mantener activada la protección en tiempo real.* Cuando se activa la protección en tiempo real, configura los siguientes valores: - La supervisión del comportamiento está activada (AllowBehaviorMonitoring) - Se examinan todos los archivos y datos adjuntos descargados (AllowIOAVProtection) - Los scripts que se usan en exploradores de Microsoft se examinan (AllowScriptScanning)

CONFIGURACIÓN	DESCRIPCIÓN
Bloqueo a primera vista	Habilitado de forma predeterminada, bloquear a primera vista bloquea el malware en segundos después de la detección, aumenta el tiempo (en segundos) permitido para enviar archivos de ejemplo para su análisis y establece el nivel de detección en Alto. *Se recomienda mantener activado el bloqueo a primera vista.* Cuando el bloqueo a primera vista está activado, configura los siguientes valores para Antivirus de Microsoft Defender: - El bloqueo y el examen de archivos sospechosos se establece en el nivel de bloqueo alto (CloudBlockLevel) - El número de segundos para que un archivo se bloquee y compruebe se establece en 50 segundos (CloudExtendedTimeout) **IMPORTANTE**: Si el bloqueo a primera vista está desactivado, afecta a `CloudBlockLevel` y `CloudExtendedTimeout` para Antivirus de Microsoft Defender.
Habilitar protección de red	Cuando está activada, la protección de red ayuda a protegerse frente a estafas de suplantación de identidad (phishing), sitios de hospedaje de vulnerabilidades de seguridad y contenido malintencionado en Internet. También impide que los usuarios desactiven la protección de red. La protección de red se puede establecer en uno de los modos siguientes: - **Modo de bloque** (esta configuración es la predeterminada), lo que impide que los usuarios visiten sitios que se consideran no seguros. *Se recomienda mantener la protección de red establecida en modo de bloqueo.* - **Modo de auditoría**, que permite a los usuarios visitar sitios que podrían no ser seguros y realizar un seguimiento de la actividad de red hacia y desde dichos sitios - **Modo deshabilitado**, que impide a los usuarios visitar sitios que podrían no ser seguros ni realizar un seguimiento de la actividad de red hacia y desde dichos sitios
Remediación	
Acción para realizar aplicaciones potencialmente no deseadas (PUA)	PUA puede incluir software de publicidad, software de agrupación que ofrece para instalar otro software sin firmar y software de evasión que intenta eludir las características de seguridad. Aunque PUA no es necesariamente un virus, malware u otro tipo de amenazas, PUA puede afectar al rendimiento del dispositivo. La protección pua bloquea los elementos que se detectan como PUA. Puede establecer la protección pua en una de las siguientes opciones: - **Habilitado** (esta configuración es la predeterminada), que bloquea los elementos detectados como PUA en los dispositivos. *Se recomienda mantener habilitada la protección de PUA.* - **Modo de auditoría**, que no realiza ninguna acción en los elementos detectados como PUA - **Deshabilitado**, que no detecta ni toma medidas en elementos que podrían ser PUA

CONFIGURACIÓN	DESCRIPCIÓN
Escanear	
Tipo de examen programado	Considere la posibilidad de ejecutar un examen antivirus semanal en los dispositivos. Puede elegir entre las siguientes opciones de tipo de examen: - **Quickscan** comprueba las ubicaciones, como las claves del Registro y las carpetas de inicio, donde se podría registrar malware para empezar con un dispositivo. *Se recomienda usar la opción quickscan.* - **Fullscan** comprueba todos los archivos y carpetas de un dispositivo - **Deshabilitado** significa que no se realizará ningún examen programado. Los usuarios todavía pueden ejecutar exámenes en sus propios dispositivos. (En general, no se recomienda deshabilitar los exámenes programados). Obtenga más información sobre los tipos de examen.
Día de la semana para ejecutar un examen programado	Seleccione un día para que se ejecuten los exámenes antivirus normales y semanales.
Hora del día para ejecutar un examen programado	Seleccione una hora para ejecutar los exámenes antivirus programados periódicamente para ejecutarse.
Uso de bajo rendimiento	Esta configuración está desactivada de forma predeterminada. *Se recomienda mantener esta configuración desactivada.* Sin embargo, puede activar esta configuración para limitar la memoria del dispositivo y los recursos que se usan durante los exámenes programados. **IMPORTANTE** Si activa **Usar bajo rendimiento**, configura los siguientes valores para Antivirus de Microsoft Defender: - No se examinan los archivos de archivo (AllowArchiveScanning) - A los exámenes se les asigna una prioridad de CPU baja (EnableLowCPUPriority) - Si se pierde un examen antivirus completo, no se ejecutará ningún examen de puesta al día (DisableCatchupFullScan) - Si se pierde un examen rápido del antivirus, no se ejecutará ningún examen de puesta al día (DisableCatchupQuickScan) - Reduce el factor de carga promedio de CPU durante un examen antivirus del 50 % al 20 % (AvgCPULoadFactor)
Experiencia del usuario	
Permitir que los usuarios accedan a la aplicación Seguridad de Windows	Active esta opción para permitir que los usuarios abran la aplicación Seguridad de Windows en sus dispositivos. Los usuarios no podrán invalidar la configuración que configure en Microsoft Defender para Empresas, pero podrán ejecutar un examen rápido si es necesario o ver las amenazas detectadas.

CONFIGURACIÓN	DESCRIPCIÓN
Exclusiones de antivirus	Las exclusiones son procesos, archivos o carpetas omitidos por Antivirus de Microsoft Defender exámenes. *En general, no es necesario definir exclusiones.* Antivirus de Microsoft Defender incluye muchas exclusiones automáticas basadas en comportamientos conocidos del sistema operativo y archivos de administración típicos. Más información sobre las exclusiones
Exclusiones de procesos	Las exclusiones de procesos impiden que Antivirus de Microsoft Defender analicen los archivos abiertos por procesos específicos. Más información sobre las exclusiones de procesos
Exclusiones de extensiones de archivo	Las exclusiones de extensiones de archivo impiden que Antivirus de Microsoft Defender analicen los archivos con extensiones específicas. Más información sobre las exclusiones de extensiones de archivo
Exclusiones de archivos y carpetas	Las exclusiones de archivos y carpetas impiden que Antivirus de Microsoft Defender analicen los archivos que se encuentran en carpetas específicas. Más información sobre las exclusiones de archivos y carpetas

Otras configuraciones preconfiguradas en Defender para empresas

La siguiente configuración de seguridad está preconfigurada en Defender para empresas:

- El examen de unidades extraíbles está activado (AllowFullScanRemovableDriveScanning)
- Los exámenes rápidos diarios no tienen una hora preestablecida (ScheduleQuickScanTime)
- Las actualizaciones de inteligencia de seguridad se comprueban antes de que se ejecute un examen antivirus (CheckForSignaturesBeforeRunningScan)
- Las comprobaciones de inteligencia de seguridad se producen cada cuatro horas (SignatureUpdateInterval)

Configuración predeterminada de Defender for Business y Microsoft Intune

En la tabla siguiente se describen los valores preconfigurados para Defender para empresas y cómo se corresponden con lo que puede ver en Intune (administrado en el centro de administración de Microsoft Endpoint Manager). Si usa el proceso de configuración simplificado en Defender for Business, no es necesario editar esta configuración.

CONFIGURACIÓN	DESCRIPCIÓN

CONFIGURACIÓN	DESCRIPCIÓN
Protección en la nube	A veces denominada protección entregada en la nube o Servicio de protección avanzada de Microsoft (MAPS), la protección en la nube funciona con Antivirus de Microsoft Defender y la nube de Microsoft para identificar nuevas amenazas, a veces incluso antes de que un solo dispositivo se vea afectado. De forma predeterminada, AllowCloudProtection está activado. Más información sobre la protección en la nube.
Supervisión de archivos entrantes y salientes	Para supervisar los archivos entrantes y salientes, RealTimeScanDirection está establecido para supervisar todos los archivos.
Examen de archivos de red	De forma predeterminada, AllowScanningNetworkFiles no está habilitado y los archivos de red no se examinan.
Examen de mensajes de correo electrónico	De forma predeterminada, AllowEmailScanning no está habilitado y los mensajes de correo electrónico no se examinan.
Número de días (0-90) para mantener el malware en cuarentena	De forma predeterminada, DaysToRetainCleanedMalware esta configuración se establece en cero (0) días. Artifacts que en cuarentena no se quitan automáticamente.
Enviar el consentimiento de ejemplos	De forma predeterminada, SubmitSamplesConsent está establecido para enviar muestras seguras automáticamente. Algunos ejemplos de ejemplos seguros son `.bat`, `.scr`, `.dll` y `.exe` archivos que no contienen información de identificación personal (PII). Si un archivo contiene PII, el usuario recibe una solicitud para permitir que continúe el envío de ejemplo. Más información sobre la protección en la nube y el envío de ejemplos
Examen de unidades extraíbles	De forma predeterminada, AllowFullScanRemovableDriveScanning está configurado para examinar unidades extraíbles, como unidades usb en dispositivos. Más información sobre la configuración de directivas antimalware
Ejecución del tiempo de examen rápido diario	De forma predeterminada, ScheduleQuickScanTime se establece en 2:00 AM. Obtenga más información sobre la configuración del examen.

CONFIGURACIÓN	DESCRIPCIÓN
Comprobación de actualizaciones de firmas antes de ejecutar el examen	De forma predeterminada, CheckForSignaturesBeforeRunningScan está configurado para comprobar si hay actualizaciones de inteligencia de seguridad antes de ejecutar exámenes antivirus o antimalware. Obtenga más información sobre la configuración de examen y las actualizaciones de inteligencia de seguridad.
Frecuencia (0-24 horas) para comprobar si hay actualizaciones de inteligencia de seguridad	De forma predeterminada, SignatureUpdateInterval está configurado para comprobar si hay actualizaciones de inteligencia de seguridad cada cuatro horas. Obtenga más información sobre la configuración de examen y las actualizaciones de inteligencia de seguridad.

Siguientes pasos

- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Revisión de las acciones de corrección en el Centro de acciones

Consulte también

- Visitar el portal de Microsoft 365 Defender
- Administración de la configuración del firewall en Microsoft Defender para Empresas
- CSP de directiva: Defender

Firewall en Microsoft Defender para Empresas

21/06/2022 • 3 minutes to read

Microsoft Defender para Empresas incluye funcionalidades de firewall con Firewall de Windows Defender. La protección del firewall ayuda a proteger los dispositivos con reglas que determinan qué tráfico de red puede entrar o fluir desde los dispositivos.

Puede usar la protección de firewall para especificar si desea permitir o bloquear conexiones en dispositivos en varias ubicaciones. Por ejemplo, la configuración del firewall puede permitir conexiones entrantes en dispositivos que están conectados a la red interna de la empresa, pero evitar esas conexiones cuando el dispositivo está en una red con dispositivos que no son de confianza.

En este artículo se describe:

Configuración predeterminada del firewall en Defender para empresas

Microsoft Defender para Empresas incluye directivas de firewall y configuración predeterminadas para ayudar a proteger los dispositivos de la empresa desde el primer día. En cuanto los dispositivos de su empresa se incorpore a Microsoft Defender para Empresas, la directiva de firewall predeterminada funciona de la siguiente manera:

- Las conexiones salientes desde dispositivos se permiten de forma predeterminada, independientemente de la ubicación.
- Cuando los dispositivos están conectados a la red de la empresa, todas las conexiones entrantes se bloquean de forma predeterminada.
- Cuando los dispositivos están conectados a una red pública o a una red privada, todas las conexiones entrantes se bloquean de forma predeterminada.

En Microsoft Defender para Empresas, puede definir excepciones para bloquear o permitir conexiones entrantes. Estas excepciones se definen mediante la creación de reglas personalizadas. Consulte Administración de reglas personalizadas para directivas de firewall.

Configuración de firewall que puede configurar en Defender para empresas

Microsoft Defender para Empresas incluye protección contra firewalls a través de Firewall de Windows Defender. En la tabla siguiente se enumeran los valores que se pueden configurar para la protección del firewall en Microsoft Defender para Empresas.

CONFIGURACIÓN	DESCRIPCIÓN
Red de dominio	El perfil de red de dominio se aplica a la red de su empresa. La configuración de firewall de la red de dominio se aplica a las conexiones entrantes que se inician en otros dispositivos que se encuentran en la misma red. De forma predeterminada, las conexiones entrantes se establecen en **Bloquear todo**.

CONFIGURACIÓN	DESCRIPCIÓN
Red pública	El perfil de red pública se aplica a una red que se puede usar en una ubicación pública, como una cafetería o un aeropuerto. La configuración de firewall de las redes públicas se aplica a las conexiones entrantes que se inician en otros dispositivos que se encuentran en la misma red. Dado que una red pública puede incluir dispositivos que no conoce o en los que no confía, las conexiones entrantes se establecen en **Bloquear todo** de forma predeterminada.
Red privada	El perfil de red privada se aplica a una red en una ubicación privada, como su hogar. La configuración de firewall de las redes privadas se aplica a las conexiones entrantes que se inician en otros dispositivos que se encuentran en la misma red. En general, en una red privada, se supone que todos los demás dispositivos de la misma red son dispositivos de confianza. Sin embargo, de forma predeterminada, las conexiones entrantes se establecen en **Bloquear todo**.
Reglas personalizadas	Las reglas personalizadas permiten bloquear o permitir conexiones específicas. Por ejemplo, supongamos que desea bloquear todas las conexiones entrantes en dispositivos conectados a una red privada, excepto las conexiones a través de una aplicación específica en un dispositivo. En este caso, establecería **Red privada** para bloquear todas las conexiones entrantes y, a continuación, agregaría una regla personalizada para definir la excepción. Puede usar reglas personalizadas para definir excepciones para archivos o aplicaciones específicos, una dirección de protocolo de Internet (IP) o un intervalo de direcciones IP. En función del tipo de regla personalizada que esté creando, estos son algunos valores de ejemplo que puede usar: Ruta de acceso del archivo de aplicación: `C:\Windows\System\Notepad.exe or %WINDIR%\Notepad.exe` IP: una dirección IPv4/IPv6 válida, como `192.168.11.0` o `192.168.1.0/24` IP: intervalo de direcciones IPv4/IPv6 válido, con formato similar `192.168.1.0-192.168.1.9` (sin espacios incluidos)

Pasos siguientes

- Administración de la configuración del firewall en Microsoft Defender para Empresas
- Más información sobre Firewall de Windows Defender
- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Revisión de las acciones de corrección en el Centro de acciones

Administrar las reglas personalizadas para directivas de firewall en Microsoft Defender para Empresas

21/06/2022 • 3 minutes to read

Microsoft Defender para Empresas incluye directivas de firewall que ayudan a proteger los dispositivos del tráfico de red no deseado. Puede usar reglas personalizadas para definir excepciones para las directivas de firewall. Es decir, puede usar reglas personalizadas para bloquear o permitir conexiones específicas.

Para más información sobre las directivas y la configuración del firewall, consulte Firewall en Microsoft Defender para Empresas.

En este artículo se describe cómo:

- Creación de una regla personalizada para una directiva de firewall
- Edición de una regla personalizada para una directiva de firewall
- Eliminación de una regla personalizada

Creación de una regla personalizada para una directiva de firewall

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. Vaya a **Configuración del dispositivo de puntos** > de conexión y revise la lista de directivas.
3. En la sección **Firewall** , seleccione una directiva existente o agregue una nueva.
4. En el paso **Configuración** , revise la configuración. Realice los cambios necesarios en **Red de dominio**, **Red pública** y **Red privada**.
5. Para crear una regla personalizada, siga estos pasos:
   a. En **Reglas personalizadas**, elija **+ Agregar regla**. (Puede tener hasta 150 reglas personalizadas).
   b. En el control flotante **Crear nueva regla** , especifique un nombre y una descripción para la regla.
   c. Seleccione un perfil. (Las opciones incluyen **Red de dominio**, **Red pública** o **Red privada**).
   d. En la lista **Tipo de dirección remota** , seleccione **IP** o **Ruta de acceso del archivo de aplicación**.
   e. En el cuadro **Valor** , especifique un valor adecuado. En función de lo que haya seleccionado en el paso 6d, puede especificar una dirección IP, un intervalo de direcciones IP o una ruta de acceso del archivo de aplicación. (Consulte Configuración del firewall).
   f. En el control flotante **Crear nueva regla** , seleccione **Crear regla**.
6. En la pantalla **Configuración** , elija **Siguiente**.
7. En la pantalla **Revisar la directiva** , revise los cambios realizados en la configuración de la directiva de firewall. Realice los cambios necesarios y, a continuación, elija **Crear directiva**.

Edición de una regla personalizada para una directiva de firewall

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. Vaya a **Configuración del dispositivo de puntos** > de conexión y revise la lista de directivas.
3. En la sección **Firewall** , seleccione una directiva existente o agregue una nueva.
4. En **Reglas personalizadas**, revise la lista de reglas.

5. Seleccione una regla y, a continuación, elija **Editar**. Se abre el control flotante.
6. Para editar la regla personalizada, siga estos pasos:
   a. En el control flotante **Editar regla** , revise y edite el nombre y la descripción de la regla.
   b. Revise y, si es necesario, edite el perfil de la regla. (Las opciones incluyen **Red de dominio**, **Red pública** o **Red privada**).
   c. En la lista **Tipo de dirección remota** , seleccione **IP** o **Ruta de acceso del archivo de aplicación**.
   d. En el cuadro **Valor** , especifique un valor adecuado. En función de lo que haya seleccionado en el paso 6c, puede especificar una dirección IP, un intervalo de direcciones IP o una ruta de acceso del archivo de aplicación. (Consulte Configuración del firewall).
   e. Establezca **Habilitar regla en Activado** para que la regla esté activa. O bien, para deshabilitar la regla, establezca el modificador en **Desactivado**.
   f. En el control flotante **Editar regla** , seleccione **Actualizar regla**.
7. En la pantalla **Configuración** , elija **Siguiente**.
8. En la pantalla **Revisar la directiva** , revise los cambios realizados en la configuración de la directiva de firewall. Realice los cambios necesarios y, a continuación, elija **Crear directiva**.

Eliminación de una regla personalizada

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. Vaya a **Configuración del dispositivo de puntos** > de conexión y revise la lista de directivas.
3. En la sección **Firewall** , seleccione una directiva existente o agregue una nueva.
4. En **Reglas personalizadas**, revise la lista de reglas.
5. Seleccione una regla y, a continuación, elija **Eliminar**. Se abre el control flotante.
6. En la pantalla de confirmación, elija **Eliminar**.

Pasos siguientes

- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Revisión de las acciones de corrección en el Centro de acciones

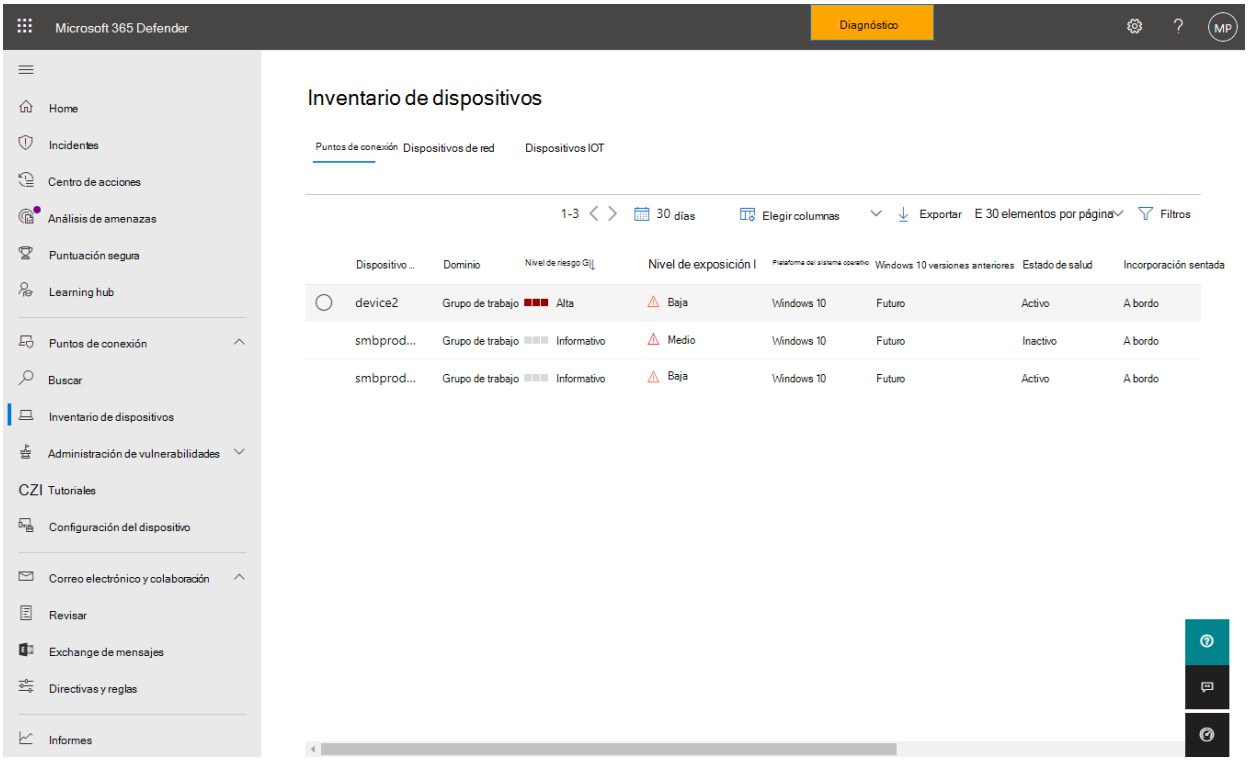
Administración de dispositivos en Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

En Microsoft Defender para Empresas, puede administrar los dispositivos de la siguiente manera:

- Ver una lista de dispositivos incorporados para ver su nivel de riesgo, nivel de exposición y estado de mantenimiento
- Realizar acciones en un dispositivo que tenga detecciones de amenazas
- Incorporación de un dispositivo a Defender for Business
- Desconectar un dispositivo de Defender para empresas

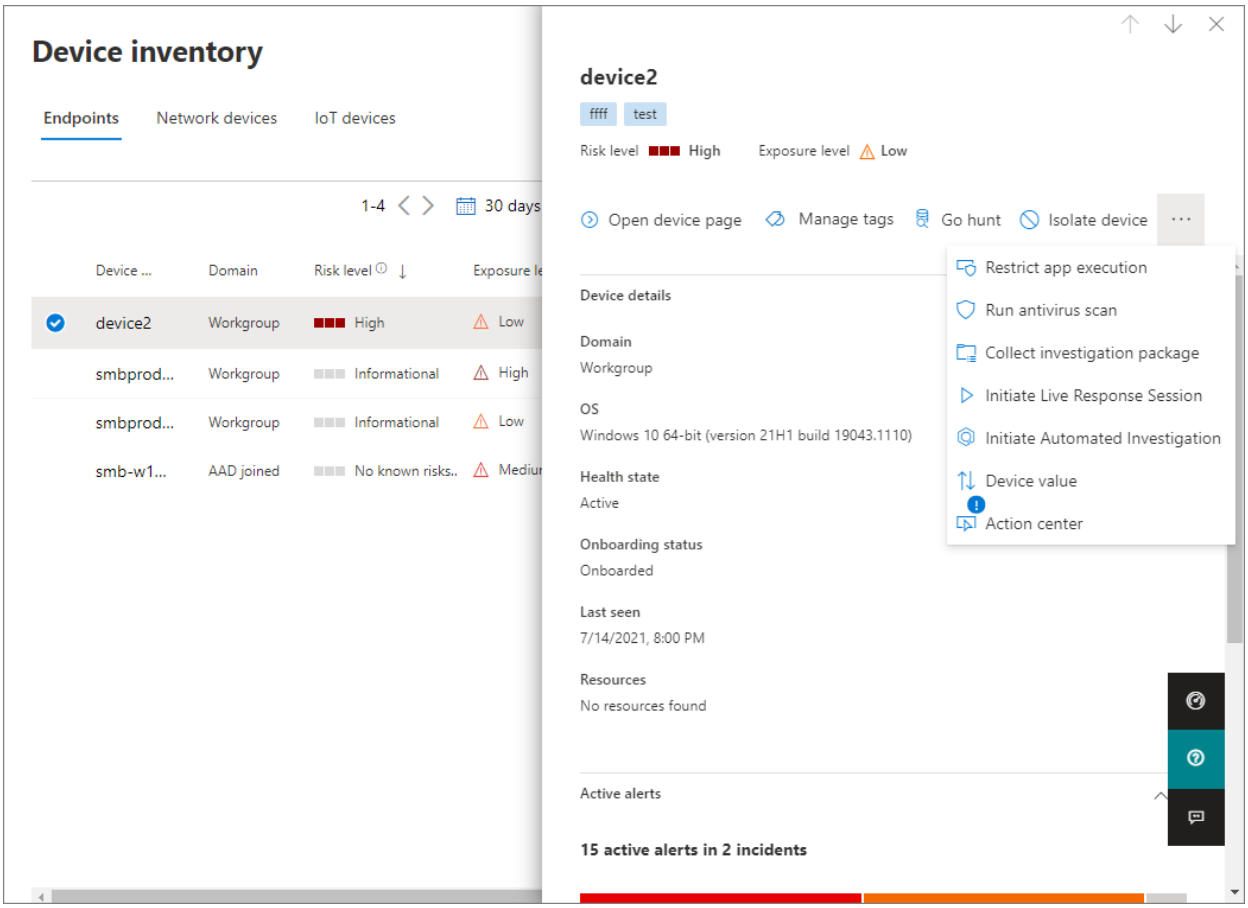
Ver la lista de dispositivos incorporados



1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. En el panel de navegación, elija **Inventario de dispositivos**.
3. Seleccione un dispositivo para abrir su panel flotante, donde puede obtener más información sobre su estado y tomar medidas.

   Si aún no aparece ningún dispositivo, incorpore dispositivos para Microsoft Defender para Empresas

Realizar acciones en un dispositivo que tenga detecciones de amenazas



1. En el portal de Microsoft 365 Defender (https://security.microsoft.com), en el panel de navegación, elija **Inventario de dispositivos**.
2. Seleccione un dispositivo para abrir su panel flotante y revise la información que se muestra.
3. Seleccione los puntos suspensivos (...) para abrir el menú acciones.
4. Seleccione una acción, como **Ejecutar examen antivirus** o **Iniciar investigación automatizada**.

Incorporación de un dispositivo

Consulte Incorporación de dispositivos para Microsoft Defender para Empresas.

Retirar un dispositivo

Consulte Offboarding a device (Offboarding a device).

Pasos siguientes

- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Revisión de las acciones de corrección en el Centro de acciones
- Creación o edición de grupos de dispositivos

Grupos de dispositivos en Microsoft Defender para Empresas

21/06/2022 • 3 minutes to read

En Microsoft Defender para Empresas, las directivas se aplican a los dispositivos a través de ciertas colecciones que se denominan grupos de dispositivos.

En este artículo se describe:

- Qué son los grupos de dispositivos
- Creación de grupos de dispositivos en Defender para empresas
- Visualización de un grupo de dispositivos existente
- Qué hace la opción Agregar todos los dispositivos

¿Qué es un grupo de dispositivos?

Un grupo de dispositivos es una colección de dispositivos que se agrupan por determinados criterios especificados, como la versión del sistema operativo. Los dispositivos que cumplen los criterios se incluyen en ese grupo de dispositivos, a menos que se excluyan. En Microsoft Defender para Empresas, las directivas se aplican a los dispositivos mediante grupos de dispositivos.

Defender for Business incluye grupos de dispositivos predeterminados que puede usar. Los grupos de dispositivos predeterminados incluyen todos los dispositivos que se incorporan a Defender para Empresas. Por ejemplo, hay un grupo de dispositivos predeterminado para Windows dispositivos. Cada vez que incorpore Windows dispositivos, se agregan automáticamente al grupo de dispositivos predeterminado.

También puede crear nuevos grupos de dispositivos para asignar directivas con una configuración específica a determinados dispositivos. Por ejemplo, puede tener una directiva de firewall asignada a un conjunto de dispositivos Windows y una directiva de firewall diferente asignada a otro conjunto de dispositivos Windows. Puede definir grupos de dispositivos específicos para usarlos con las directivas.

> **NOTE**
> Al crear directivas en Defender para empresas, se asigna un orden de prioridad. Si aplica varias directivas a un conjunto determinado de dispositivos, estos solo recibirán la primera directiva aplicada. Para obtener más información, consulte Descripción del orden de la directiva en Microsoft Defender para Empresas.

Todos los grupos de dispositivos, incluidos los grupos de dispositivos predeterminados y los grupos de dispositivos personalizados que defina, se almacenan en Azure Active Directory (Azure AD).

Creación de un nuevo grupo de dispositivos

Actualmente, en Defender para empresas, puede crear un nuevo grupo de dispositivos mientras está en proceso de crear o editar una directiva, como se describe en el procedimiento siguiente:

1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. En el panel de navegación, elija **Configuración del dispositivo**.
3. Realice una de las acciones siguientes:

a. Seleccione una directiva existente y, a continuación, elija **Editar**.
b. Elija **+ Agregar** para crear una nueva directiva.

> **TIP**
> Para obtener ayuda para crear o editar una directiva, vea Ver o editar directivas en Microsoft Defender para Empresas.

4. En el paso **Información general**, revise la información, edítela si es necesario y, a continuación, elija **Siguiente**.
5. Elija **+ Crear nuevo grupo**.
6. Especifique un nombre y una descripción para el grupo de dispositivos y, a continuación, elija **Siguiente**.
7. Seleccione los dispositivos que desea incluir en el grupo y, a continuación, elija **Crear grupo**.
8. En el paso **Grupos de dispositivos**, revise la lista de grupos de dispositivos de la directiva. Si es necesario, quite un grupo de la lista. A continuación, elija **Siguiente**.
9. En la página **Opciones de configuración**, revise y edite la configuración según sea necesario y, a continuación, elija **Siguiente**. Para obtener más información sobre estas opciones, consulte Configuración.
10. En el paso **Revisar la directiva**, revise toda la configuración, realice las modificaciones necesarias y, a continuación, elija **Crear directiva** o **Actualizar directiva**.

Visualización de un grupo de dispositivos existente

Actualmente, en Defender para empresas, puede ver los grupos de dispositivos existentes mientras está en proceso de crear o editar una directiva, como se describe en el procedimiento siguiente:

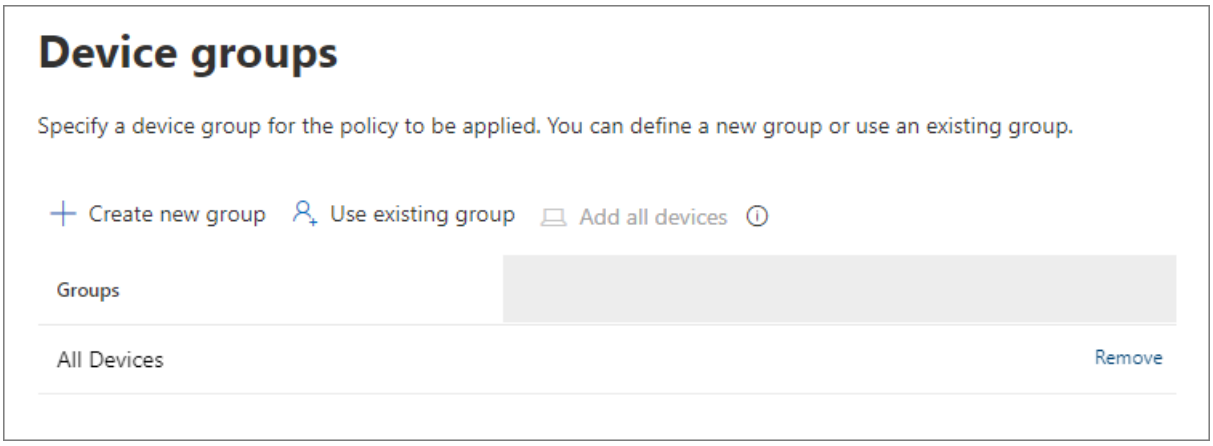
1. Vaya al portal de Microsoft 365 Defender (https://security.microsoft.com) e inicie sesión.
2. En el panel de navegación, elija **Configuración del dispositivo**.
3. Realice una de las acciones siguientes:
   a. Seleccione una directiva existente y, a continuación, elija **Editar**.
   b. Elija **+ Agregar** para crear una nueva directiva.

> **TIP**
> Para obtener ayuda para crear o editar una directiva, vea Ver o editar directivas en Microsoft Defender para Empresas.

4. En el paso **Información general**, revise la información, edítela si es necesario y, a continuación, elija **Siguiente**.
5. Elija **Usar grupo existente**. Se abre un control flotante y muestra los grupos de dispositivos. Si aún no tiene ningún grupo de dispositivos, se le pedirá que cree un nuevo grupo de dispositivos.

¿Qué hace la opción Agregar todos los dispositivos?

Al crear o editar una directiva, es posible que vea la opción **Agregar todos los dispositivos** .



Si selecciona esta opción, todos los dispositivos inscritos en Microsoft Intune recibirán la directiva que está creando o editando de forma predeterminada.

Pasos siguientes

Elija una o varias de las siguientes tareas:

- Ver o editar directivas
- Crear una nueva directiva
- Visualización y administración de incidentes en Microsoft Defender para Empresas
- Respuesta y mitigación de amenazas en Microsoft Defender para Empresas
- Revisión de las acciones de corrección en el Centro de acciones

Obtener ayuda y soporte técnico para Microsoft Defender para Empresas

21/06/2022 • 2 minutes to read

Obtener ayuda y soporte técnico

Si necesita ayuda con Microsoft Defender para Empresas, seleccione el icono ayuda (?) en la esquina superior derecha de la pantalla. Escriba su pregunta o problema. Se mostrarán varias opciones, como respuestas rápidas o artículos de ayuda.

Si no ve la respuesta a su pregunta, puede abrir una incidencia de soporte técnico. Consulte Obtención de soporte técnico

Consulte también

- Microsoft Defender para Empresas: preguntas y respuestas más frecuentes
- solución de problemas de Microsoft Defender para Empresas
- Introducción a Microsoft 365 Empresa Premium

Acceso de asociados a través de api de Microsoft Defender para punto de conexión

21/06/2022 • 6 minutes to read

Se aplica a:

- Microsoft Defender para punto de conexión Plan 2
- Microsoft Defender para Empresas

IMPORTANT

Las funcionalidades avanzadas de búsqueda no se incluyen en Defender para empresas. Consulte Comparar Microsoft Defender para Empresas con los planes 1 y 2 de Microsoft Defender para punto de conexión.

¿Quiere experimentar Microsoft Defender para punto de conexión? Regístrese para obtener una prueba gratuita.

NOTE

Si es un cliente del Gobierno de Estados Unidos, use los URI que aparecen en Microsoft Defender para endpoints para clientes de US Government.

TIP

Para mejorar el rendimiento, puede usar el servidor más cercano a la ubicación geográfica:

- api-us.securitycenter.microsoft.com
- api-eu.securitycenter.microsoft.com
- api-uk.securitycenter.microsoft.com

En esta página se describe cómo crear una aplicación de Azure Active Directory (Azure AD) para obtener acceso mediante programación a Microsoft Defender para punto de conexión en nombre de los clientes.

Microsoft Defender para punto de conexión expone gran parte de sus datos y acciones a través de un conjunto de API mediante programación. Esas API le ayudarán a automatizar los flujos de trabajo e innovar en función de Microsoft Defender para punto de conexión funcionalidades. El acceso a la API requiere la autenticación de OAuth2.0. Para obtener más información, vea Flujo de código de autorización de OAuth 2.0.

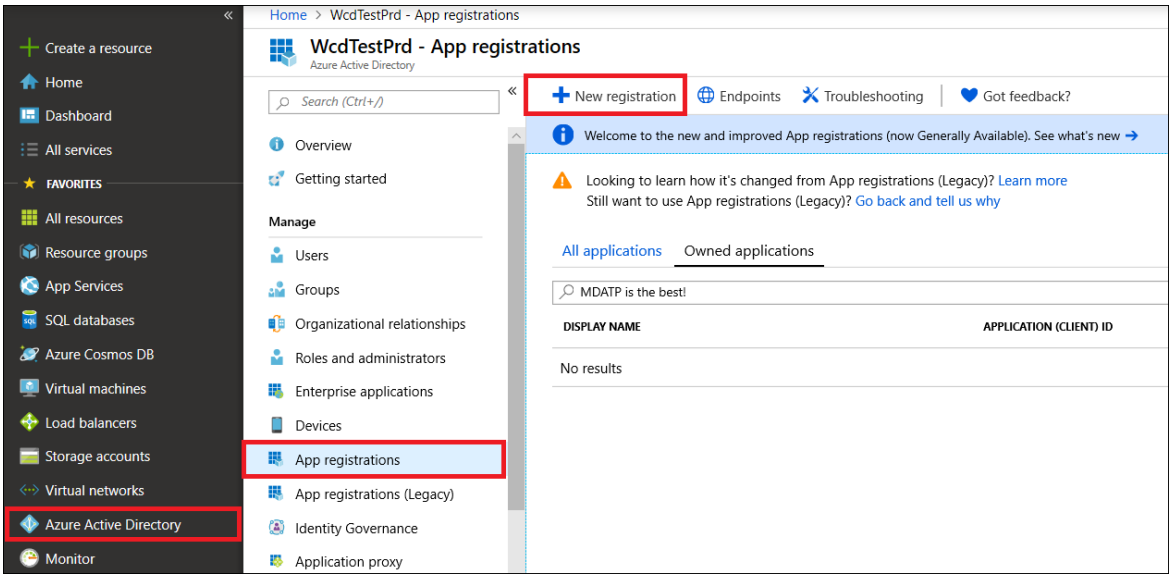
En general, deberá realizar los pasos siguientes para usar las API:

- Cree una aplicación de Azure AD **multiinquilino** .
- Obtenga autorización (consentimiento) por parte del administrador del cliente para que la aplicación acceda a los recursos de Defender para punto de conexión que necesita.
- Obtenga un token de acceso mediante esta aplicación.
- Use el token para acceder a Microsoft Defender para punto de conexión API.

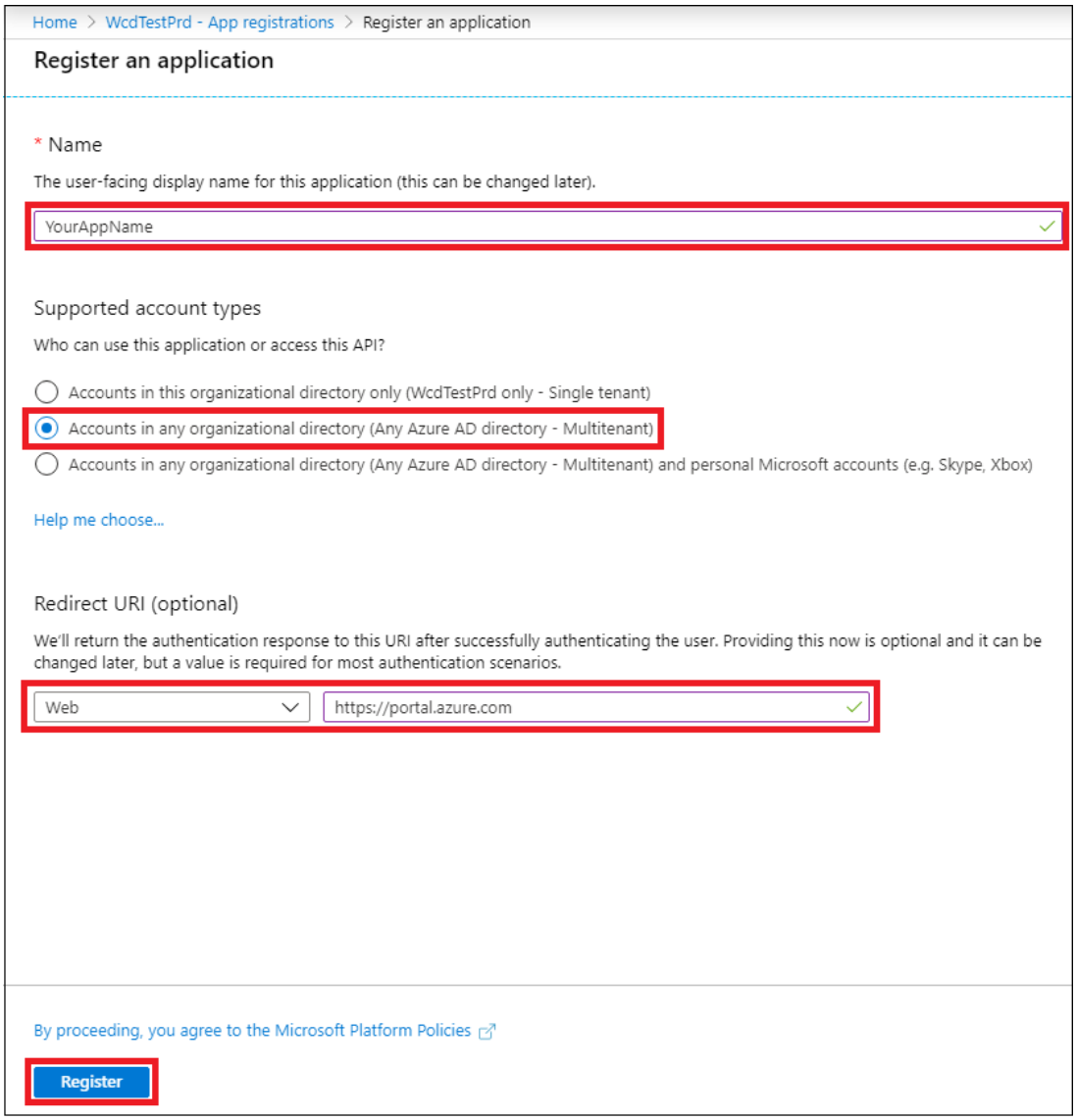
Los pasos siguientes le guiarán para crear una aplicación de Azure AD, obtener un token de acceso para Microsoft Defender para punto de conexión y validar el token.

Creación de la aplicación multiinquilino

1. Inicie sesión en el inquilino de Azure con un usuario que tenga el rol **de administrador global** .
2. Vaya a **Azure Active Directory** > **Registros de aplicaciones** > **Nuevo registro**.



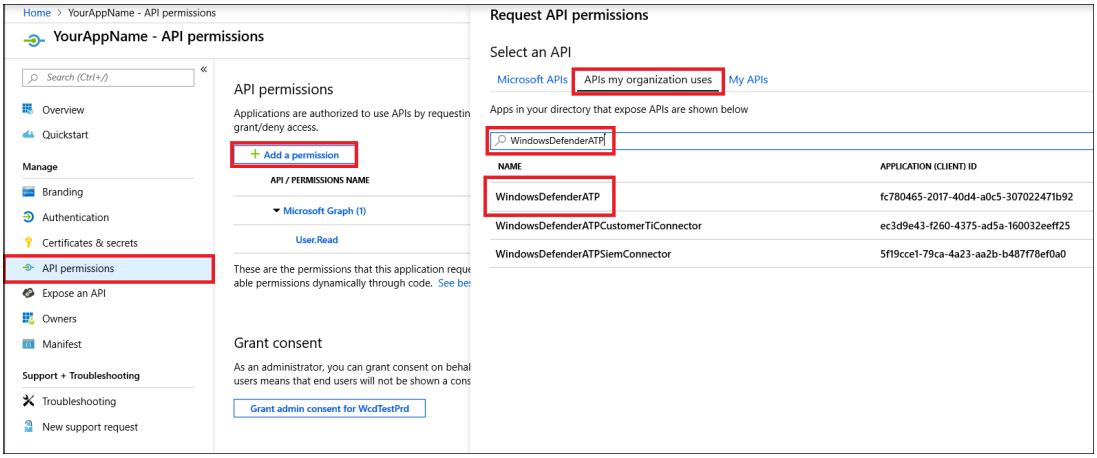
3. En el formulario de registro:
   - Elija un nombre para la aplicación.
   - Tipos de cuenta admitidos: cuentas en cualquier directorio organizativo.
   - URI de redirección: tipo: Web, URI: https://portal.azure.com



4. Permita que la aplicación acceda a Microsoft Defender para punto de conexión y asígnela con el conjunto mínimo de permisos necesarios para completar la integración.

   - En la página de la aplicación, seleccione **Permisos** > de API **Agregar API de permisos** > **Que mi organización usa** > escriba **WindowsDefenderATP** y seleccione en **WindowsDefenderATP**.

   - **Nota**: *WindowsDefenderATP* no aparece en la lista original. Empiece a escribir su nombre en el cuadro de texto para verlo aparecer.



Solicitar permisos de API

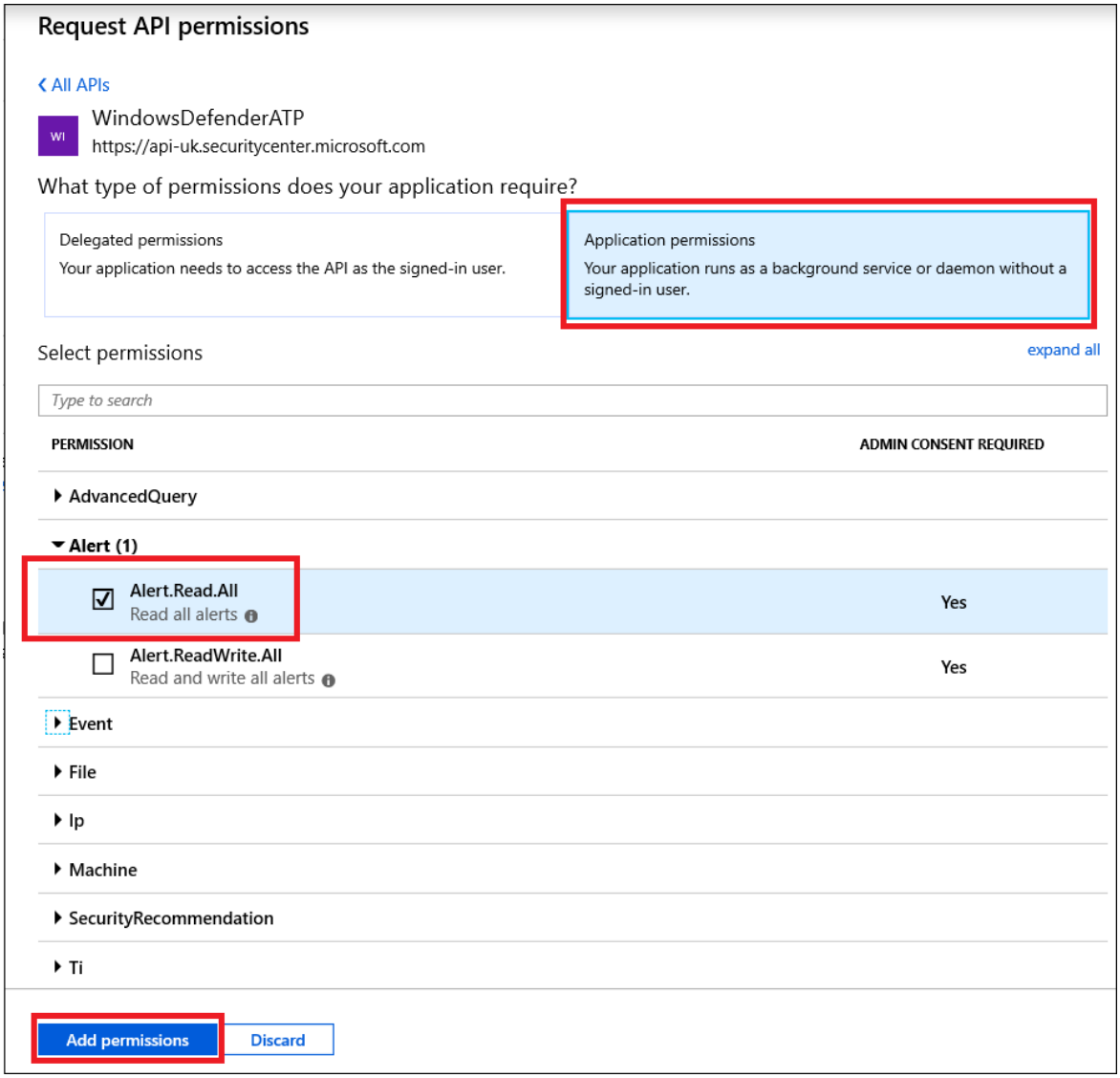
Para determinar qué permiso necesita, revise la sección **Permisos** de la API a la que está interesado llamar. Por

ejemplo:

- Para ejecutar consultas avanzadas, seleccione el permiso "Ejecutar consultas avanzadas".
- Para aislar un dispositivo, seleccione el permiso "Aislar máquina".

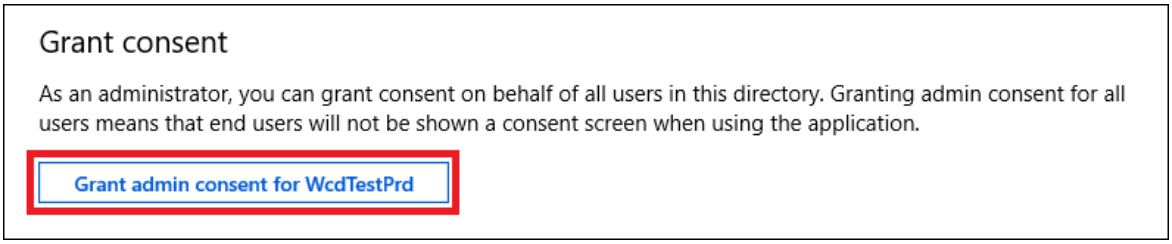
En el ejemplo siguiente usaremos el permiso **"Leer todas las alertas"** :

1. Elija **Permisos** > de aplicación **Alert.Read.All** > seleccione Agregar **permisos**.



2. Seleccione **Conceder consentimiento**

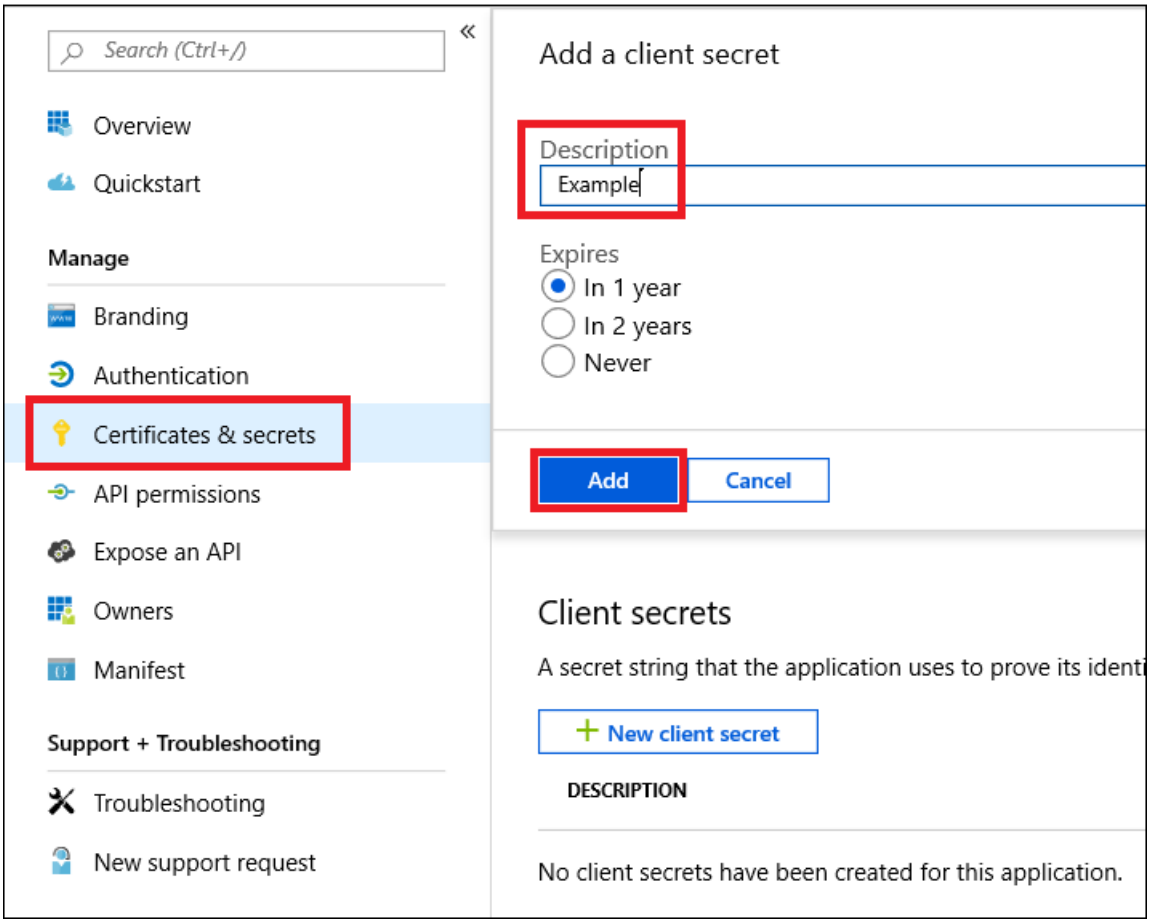
   - **Nota**: Cada vez que agregue permiso, debe seleccionar en **Conceder consentimiento** para que el nuevo permiso surta efecto.



3. Agregue un secreto a la aplicación.

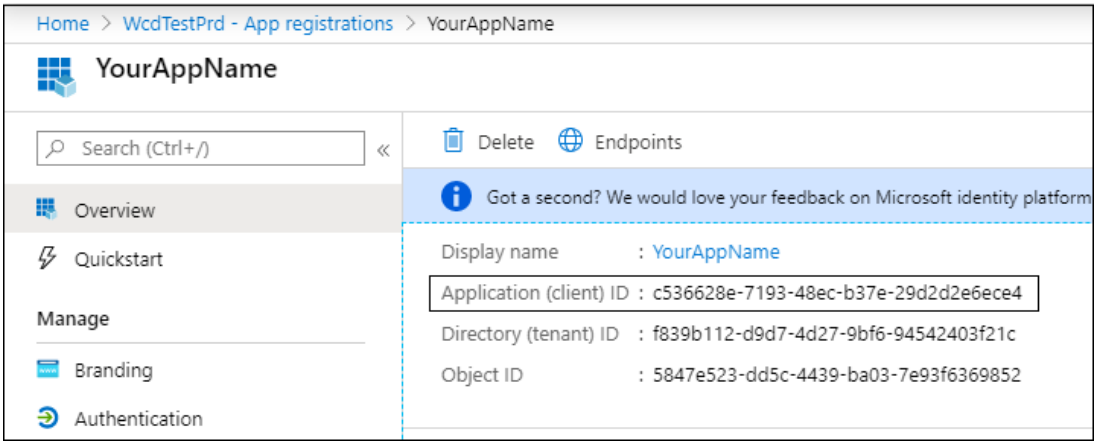
   - Seleccione **Certificados & secretos**, agregue la descripción al secreto y seleccione **Agregar**.

   Importante: Después de hacer clic en Agregar, **copie el valor de secreto generado**. ¡No podrás recuperarlo después de irte!



4. Anote el identificador de la aplicación:

   - En la página de la aplicación, vaya a **Información general** y copie la siguiente información:



5. Agregue la aplicación al inquilino del cliente.

   Necesita que la aplicación se apruebe en cada inquilino de cliente en el que quiera usarlo. Esto se debe a que la aplicación interactúa con Microsoft Defender para punto de conexión aplicación en nombre del cliente.

   Un usuario con **administrador global** del inquilino del cliente debe seleccionar el vínculo de consentimiento y aprobar la aplicación.

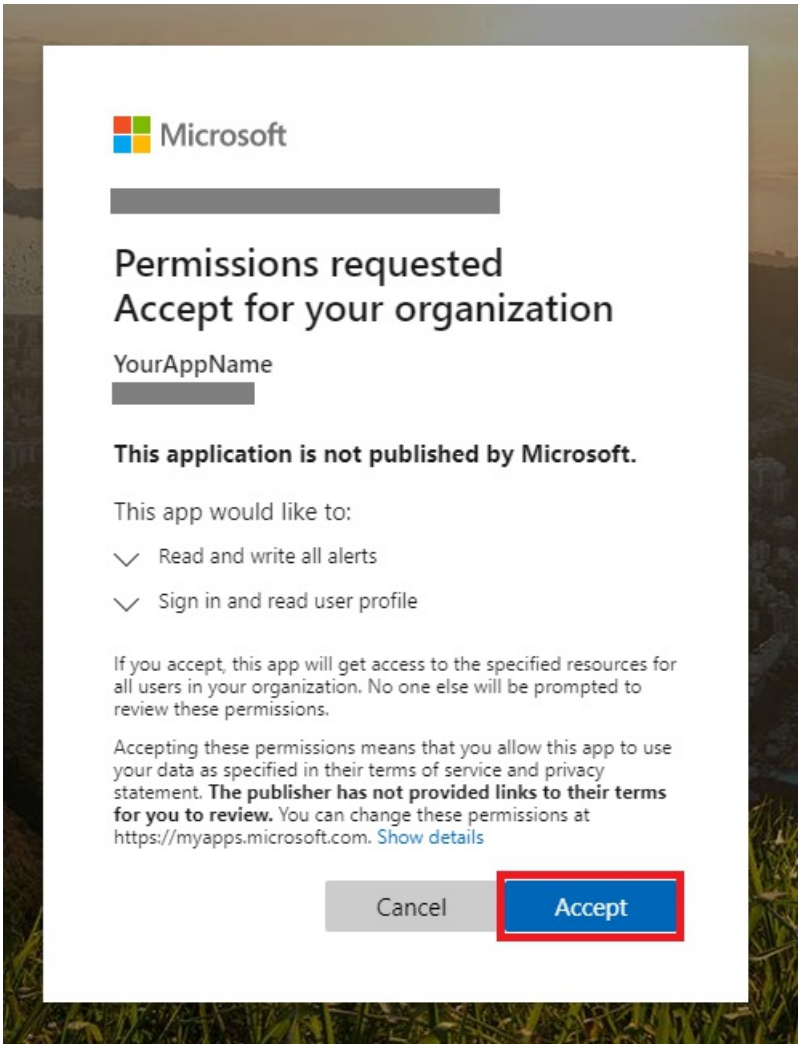
   El vínculo de consentimiento tiene el siguiente formato:

```
https://login.microsoftonline.com/common/oauth2/authorize?prompt=consent&client_id=00000000-0000-0000-0000-000000000000&response_type=code&sso_reload=true
```

   Donde 0000000000-0000-0000-0000-0000000000000 debe reemplazarse por el identificador de

aplicación

Después de hacer clic en el vínculo de consentimiento, inicie sesión con el administrador global del inquilino del cliente y dé su consentimiento a la aplicación.



Además, tendrá que pedir al cliente su identificador de inquilino y guardarlo para su uso futuro al adquirir el token.

6. **¡Hecho!** Ha registrado correctamente una aplicación. Consulte los ejemplos siguientes para la adquisición y validación de tokens.

Obtener un ejemplo de token de acceso

Nota: Para obtener el token de acceso en nombre del cliente, use el identificador de inquilino del cliente en las siguientes adquisiciones de tokens.

Para obtener más información sobre el token de AAD, consulte el tutorial de AAD.

Con PowerShell

```
# That code gets the App Context Token and save it to a file named "Latest-token.txt" under the current
directory
# Paste below your Tenant ID, App ID and App Secret (App key).

$tenantId = '' ### Paste your tenant ID here
$appId = '' ### Paste your Application ID here
$appSecret = '' ### Paste your Application key here

$resourceAppIdUri = 'https://api.securitycenter.microsoft.com'
$oAuthUri = "https://login.microsoftonline.com/$TenantId/oauth2/token"
$authBody = [Ordered] @{
    resource = "$resourceAppIdUri"
    client_id = "$appId"
    client_secret = "$appSecret"
    grant_type = 'client_credentials'
}
$authResponse = Invoke-RestMethod -Method Post -Uri $oAuthUri -Body $authBody -ErrorAction Stop
$token = $authResponse.access_token
Out-File -FilePath "./Latest-token.txt" -InputObject $token
return $token
```

Uso de C

> El código siguiente se ha probado con Nuget Microsoft.Identity.Client.

IMPORTANT

El paquete NuGet Microsoft.IdentityModel.Clients.ActiveDirectory y la Biblioteca de autenticación de Azure AD (ADAL) han quedado en desuso. No se han agregado nuevas características desde el 30 de junio de 2020. Le recomendamos encarecidamente que actualice, consulte la guía de migración para obtener más detalles.

- Creación de una nueva aplicación de consola
- Instalación de NuGet Microsoft.Identity.Client
- Agregue lo siguiente mediante

  ```
  using Microsoft.Identity.Client;
  ```

- Copie o pegue el código siguiente en la aplicación (no olvide actualizar las tres variables: `tenantId`, `appId` y `appSecret`)

```
string tenantId = "00000000-0000-0000-0000-000000000000"; // Paste your own tenant ID here
string appId = "11111111-1111-1111-1111-111111111111"; // Paste your own app ID here
string appSecret = "22222222-2222-2222-2222-222222222222"; // Paste your own app secret here for a
test, and then store it in a safe place!
const string authority = https://login.microsoftonline.com;
const string audience = https://api.securitycenter.microsoft.com;

IConfidentialClientApplication myApp =
ConfidentialClientApplicationBuilder.Create(appId).WithClientSecret(appSecret).WithAuthority($"
{authority}/{tenantId}").Build();

List<string> scopes = new List<string>() { $"{audience}/.default" };

AuthenticationResult authResult =
myApp.AcquireTokenForClient(scopes).ExecuteAsync().GetAwaiter().GetResult();

string token = authResult.AccessToken;
```

Uso de Python

Consulte Obtención de un token mediante Python.

Uso de Curl

> **NOTE**
> El procedimiento siguiente supone que Curl para Windows ya está instalado en el equipo.

- Abrir una ventana de comandos
- Establecimiento de CLIENT_ID en el identificador de aplicación de Azure
- Establecimiento de CLIENT_SECRET en el secreto de aplicación de Azure
- Establezca TENANT_ID en el identificador de inquilino de Azure del cliente que quiere usar la aplicación para acceder a Microsoft Defender para punto de conexión aplicación.
- Ejecute el siguiente comando:

```
curl -i -X POST -H "Content-Type:application/x-www-form-urlencoded" -d "grant_type=client_credentials" -d
"client_id=%CLIENT_ID%" -d "scope=https://securitycenter.onmicrosoft.com/windowsatpservice/.default" -d
"client_secret=%CLIENT_SECRET%" "https://login.microsoftonline.com/%TENANT_ID%/oauth2/v2.0/token" -k
```

Obtendrá una respuesta del formulario:

```
{"token_type":"Bearer","expires_in":3599,"ext_expires_in":0,"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1
NiIsIn <truncated> aWReH7P0s0tjTBX8wGWqJUdDA"}
```

Validar el token

Comprobación de integridad para asegurarse de que tiene un token correcto:

- Copie o pegue en JWT el token que obtiene en el paso anterior para descodificarlo.
- Validar que obtiene una notificación de "roles" con los permisos deseados
- En la captura de pantalla siguiente, puede ver un token descodificado adquirido de una aplicación con varios permisos para Microsoft Defender para punto de conexión:
- La notificación "tid" es el identificador de inquilino al que pertenece el token.

Uso del token para acceder a Microsoft Defender para punto de conexión API

- Elija la API que desea usar. Para obtener más información, consulte Api de Microsoft Defender para punto de conexión compatibles.
- Establezca el encabezado Authorization en la solicitud Http que envíe a "Bearer {token}" (Bearer es el esquema de autorización)
- La hora de expiración del token es de 1 hora (puede enviar más de una solicitud con el mismo token)
- Ejemplo de envío de una solicitud para obtener una lista de alertas **mediante C#**

```
var httpClient = new HttpClient();

var request = new HttpRequestMessage(HttpMethod.Get,
"https://api.securitycenter.microsoft.com/api/alerts");

request.Headers.Authorization = new AuthenticationHeaderValue("Bearer", token);

var response = httpClient.SendAsync(request).GetAwaiter().GetResult();

// Do something useful with the response
```

Consulte también

- API compatibles de Microsoft Defender para punto de conexión
- Acceso a Microsoft Defender para punto de conexión en nombre de un usuario