Guía del usuario

Extensión de McAfee Security-as-a-Service

Para su uso con el software ePolicy Orchestrator® 4.6.0

INFORMACIÓN DE LICENCIA

Acuerdo de licencia
AVISO A TODOS LOS USUARIOS: LEA DETENIDAMENTE EL ACUERDO LEGAL CORRESPONDIENTE A LA LICENCIA QUE HA ADQUIRIDO, QUE ESTIPULA LOS TÉRMINOS Y CONDICIONES GENERALES PARA EL USO DEL SOFTWARE CON LICENCIA. SI NO SABE QUÉ TIPO DE LICENCIA HA ADQUIRIDO, CONSULTE LOS DOCUMENTOS DE VENTA Y OTROS DOCUMENTOS RELACIONADOS CON LA CONCESIÓN DE LA LICENCIA O CON LA ORDEN DE COMPRA QUE ACOMPAÑAN AL PAQUETE DE SOFTWARE, O QUE HAYA RECIBIDO POR SEPARADO COMO PARTE DE LA COMPRA (POR EJEMPLO, UN MANUAL, UN ARCHIVO DEL CD DEL PRODUCTO O UN ARCHIVO DISPONIBLE EN EL SITIO WEB DESDE EL QUE DESCARGÓ EL PAQUETE DE SOFTWARE). SI NO ACEPTA TODOS LOS TÉRMINOS DESCRITOS EN EL ACUERDO, NO INSTALE EL SOFTWARE. SI PROCEDE, PUEDE DEVOLVER EL PRODUCTO A MCAFEE O AL LUGAR DONDE LO ADQUIRIÓ CON EL FIN DE OBTENER SU REEMBOLSO ÍNTEGRO.

Contenido

Prefacio

En esta guía se proporciona la información necesaria para todas las fases de uso del producto, desde la instalación a la configuración y la solución de problemas.

Contenido

Acerca de esta guía

Esta información incluye los destinatarios de la guía, las convenciones tipográficas y los iconos utilizados, además de cómo está organizada.

Destinatarios

La documentación de McAfee se investiga y escribe cuidadosamente para sus destinatarios.

La información de esta guía va dirigida principalmente a:

- **Administradores**: personas que implementan y aplican el programa de seguridad de la empresa.

Convenciones

En esta guía se utilizan las convenciones tipográficas y los iconos siguientes.

Título de manual o *Énfasis*	Título de un manual, capítulo o tema; introducción de un nuevo término; énfasis.
Negrita	Texto que se enfatiza particularmente.
`Entrada de usuario` o `Ruta de acceso`	Comandos y otros tipos de texto que escribe el usuario; ruta de acceso a una carpeta o a un programa.
`Código`	Muestra de código.
Interfaz de usuario	Palabras de la interfaz de usuario, incluidos los nombres de opciones, menús, botones y cuadros de diálogo.
Hipertexto en azul	Vínculo activo a un tema o sitio web.
	**Nota**: información adicional, como un método alternativo de acceso a una opción.
	**Sugerencia**: sugerencias y recomendaciones.
	**Importante/Precaución**: consejo importante para proteger el sistema informático, la instalación del software, la red, la empresa o los datos.
	**Advertencia**: consejo crítico para evitar daños personales al utilizar un producto de hardware.

Búsqueda de documentación del producto

McAfee le proporciona la información que necesita en cada fase del proceso de implementación del producto, desde la instalación al uso diario y a la solución de problemas. Tras el lanzamiento de un producto, su información se introduce en la base de datos online KnowledgeBase de McAfee.

Procedimiento

1 Vaya a McAfee Technical Support ServicePortal en http://mysupport.mcafee.com.

2 En **Self Service** (Autoservicio) puede acceder al tipo de información que necesite:

Para acceder a...	Haga lo siguiente...
Documentación de usuario	1 Haga clic en **Product Documentation** (Documentación del producto). 2 Seleccione un producto, después seleccione una versión. 3 Seleccione un documento del producto.
KnowledgeBase	• Haga clic en **Search the KnowledgeBase** (Buscar en KnowledgeBase) para encontrar respuestas a sus preguntas sobre el producto. • Haga clic en **Browse the KnowledgeBase** (Examinar KnowledgeBase) para ver los artículos clasificados por producto y versión.

1 Introducción a la extensión de Security-as-a-Service

La extensión de generación de informes de McAfee® Security-as-a-Service le permite supervisar el estado de los equipos protegidos por los servicios de McAfee Security-as-a-Service (McAfee SaaS) y gestionados con el sitio web administrativo de McAfee® SecurityCenter.

La extensión es para su uso con el software McAfee® ePolicy Orchestrator (McAfee ePO™) versión 4.6 o posterior.

Contenido

Administración de los servicios de protección de McAfee SaaS

La extensión de generación de informes de Security-as-a-Service le permite utilizar la consola de ePolicy Orchestrator para supervisar el estado y la información de eventos correspondiente a los sistemas gestionados protegidos por los servicios de McAfee SaaS.

Su suscripción a los servicios de protección de McAfee SaaS incluye una cuenta para una herramienta de gestión basada en web llamada SecurityCenter, la cual incluye:

- **Servidor de base de datos**: mantiene la información sobre los servicios de protección de McAfee SaaS y los equipos protegidos por ellos.
- **Consola de SecurityCenter**: muestra información de la base de datos con objeto de administrar los sistemas donde estén instalados los servicios de McAfee SaaS (por ejemplo, mediante la creación de directivas e informes de detección detallados).

La extensión establece un vínculo de comunicación entre el servidor de ePolicy Orchestrator y una o varias cuentas de SecurityCenter. A continuación, extrae (o copia) los datos de la base de datos de SecurityCenter y los sincroniza con la base de datos de ePolicy Orchestrator. Puede utilizar las funciones de supervisión y generación de informes que proporciona la extensión para ver información básica de SaaS en la consola de ePolicy Orchestrator.

Componentes necesarios

La administración de los servicios de protección de McAfee SaaS con la extensión de Security-as-a-Service precisa que los siguientes componentes se encuentren configurados y en ejecución.

- **Servidor y base de datos de ePolicy Orchestrator 4.6 (o posterior)**: la herramienta de administración de seguridad para empresas que supervisa la actividad y crea informes sobre los sistemas gestionados que ejecutan productos de seguridad de McAfee.
- **McAfee SecurityCenter** : herramienta de administración basada en web para los servicios de McAfee SaaS. El administrador del sitio utiliza esta herramienta para instalar software cliente, desplegar directivas, supervisar actividades y detecciones, crear informes y administrar información de las cuentas.
- **Extensión de Security-as-a-Service**: software que proporciona la interfaz entre SecurityCenter y el servidor y la base de datos de ePolicy Orchestrator.
- **Servicios de protección de McAfee SaaS**: servicios de protección que supervisan la actividad, generan informes, detectan amenazas y responden a ellas, en sistemas informáticos cliente. Algunos servicios de protección incluyen la configuración de cuentas o la instalación de un componente de software cliente.

Configuración e integración de componentes

Una vez que el entorno de ePolicy Orchestrator está en ejecución, se requieren cuatro tareas para configurar adecuadamente la interacción entre los componentes de gestión y los servicios de protección de McAfee SaaS.

Si ya ha configurado una cuenta administrativa de SecurityCenter y llevado a cabo cualquier instalación, activación o configuración necesarias para los servicios de protección de McAfee SaaS, empiece con la tarea 3.

Descripción general del proceso

1. Configure una cuenta administrativa en SecurityCenter.

Cuando adquiera una suscripción a servicios de McAfee SaaS, McAfee o su proveedor de servicios:

- Crea una cuenta para usted.
- Configura una herramienta administrativa basada en web, SecurityCenter. SecurityCenter se usa para gestionar el estado de los equipos protegidos por los servicios de McAfee SaaS.
- Envía sus credenciales para iniciar sesión en la consola de SecurityCenter. Debe iniciar sesión en su cuenta y configurar los ajustes conforme sea necesario.

2. Instale el software cliente y active los servicios de protección que necesite.

Algunos servicios de protección requieren la instalación de software en los equipos cliente, su activación o su configuración para que comience la protección. Para obtener más información, consulte el mensaje de correo electrónico de bienvenida que recibió al suscribirse a los servicios de McAfee SaaS y la documentación disponible en la página **Ayuda y asistencia** de la consola de SecurityCenter.

Verifique que los datos de los sistemas gestionados de McAfee SaaS aparecen en la consola de SecurityCenter antes de actuar. Por ejemplo, compruebe la página **Equipos** para asegurarse de que aparecen los sistemas gestionados en la cuenta. Consulte los widgets en la página **Panel** para ver la información de estado y sobre detecciones de un vistazo. No es posible ver la información en la consola de ePolicy Orchestrator hasta que esté disponible en SecurityCenter.

3. Instale y configure la extensión.

Se proporcionan instrucciones en esta guía y en una guía de inicio rápido que está disponible desde la consola de SecurityCenter, en la ficha **Servidores de ePO** de la página **Utilidades**.

4. Gestione los equipos protegidos por los servicios de McAfee SaaS desde dos ubicaciones.

Una vez que se ha completado la instalación, puede acceder a la información de los sistemas gestionados desde dos consolas:

- **Consola de ePolicy Orchestrator**: supervise la información de estado y eventos. Cuando necesite instalar software cliente, configurar directivas o llevar a cabo otras tareas de administración, seleccione los vínculos en el monitor de **McAfee SecurityCenter**, en el panel de **Security-as-a-Service**, para abrir la consola de SecurityCenter.
- **Consola de SecurityCenter**: cree directivas personalizadas, instale software cliente y ejecute informes detallados. Para obtener más información, consulte la documentación de McAfee® SaaS Endpoint Protection, disponible en la página **Ayuda y asistencia** de la consola de SecurityCenter.

2 Instalación y configuración de la extensión

Estos temas explican cómo instalar y configurar las funciones de la extensión.

Contenido

Descripción general de la instalación y la configuración

Son precisas cuatro tareas generales para instalar y configurar la extensión.

Descripción general del proceso

1. **Descargue e instale la extensión.**

   Descargue el archivo .ZIP de la extensión de producto desde SecurityCenter o desde la consola de ePolicy Orchestrator y, después, instale la extensión desde la consola de ePolicy Orchestrator.

2. **Registre la cuenta de SecurityCenter con el software ePolicy Orchestrator.**

   Esto requiere credenciales de inicio de sesión para una cuenta de SecurityCenter administrativa. Si no dispone de ellas, cree una cuenta de administrador de sincronización antes de llevar a cabo esta tarea.

3. **Cree un contenedor (*punto de sincronización*) para los datos de McAfee SaaS en el árbol de sistemas.**

   Los datos sincronizados de los sistemas gestionados de McAfee SaaS se colocarán en este contenedor.

4. **Sincronice los datos de SaaS extraídos de SecurityCenter con la base de datos de ePolicy Orchestrator.**

   Esto hace que los datos actuales de McAfee SaaS sean accesible para las funciones de supervisión y generación de informes de la extensión y del software ePolicy Orchestrator.

Véase también

Instalación de la extensión de producto en la página 14
Creación o actualización de una cuenta de administrador de sincronización en la página 28
Registro de una cuenta de SecurityCenter en la página 17
Creación de un punto de sincronización en el árbol de sistemas en la página 21
Sincronización de datos desde SecurityCenter en la página 22

Funciones agregadas al entorno de ePolicy Orchestrator

La extensión agrega o utiliza estas funciones en el entorno de ePolicy Orchestrator para obtener datos de una cuenta de SecurityCenter y sincronizarlos con el servidor de ePolicy Orchestrator.

Tabla 2-1 Funciones agregadas para sincronizar datos de SaaS

Función	Detalles
Servidores registrados	Requiere un tipo de servidor de base de datos registrado: • **Cuenta de SecurityCenter**: el registro requiere credenciales de inicio de sesión administrativo para cada cuenta de SecurityCenter que desee registrar.
Tareas servidor	Agrega una tarea de extracción preconfigurada y planificada: • **Sincronización de datos de SaaS**: extrae datos de la cuenta de SecurityCenter registrada y los sincroniza con la base de datos de ePolicy Orchestrator. Esta tarea servidor se encuentra desactivada de manera predeterminada. Agrega una opción nueva en el menú **Acciones**: • **Sincronizar sistemas de SaaS**
Árbol de sistemas	Agrega dos opciones del menú **Acciones** a la ficha **Detalles del grupo**: • **Gestionar configuración de sincronización de grupos**: le permite asociar un grupo a una cuenta de SecurityCenter registrada. (El grupo se convierte en el *punto de sincronización* de la cuenta.) • **Presentar una lista de todos los puntos de sincronización de SaaS**: muestra en qué momento se sincronizaron por última vez los datos de SaaS para cada cuenta de SecurityCenter registrada.
Conjuntos de permisos	Agrega dos funciones de usuario preconfiguradas: • **Administrador de SaaS**: de forma predeterminada, el Administrador de SaaS puede crear, editar o eliminar servidores registrados de SaaS, tareas servidor y consultas. • **Revisor de SaaS**: de forma predeterminada, el Revisor de SaaS puede ver servidores registrados, ver datos sincronizados y ejecutar consultas.

La extensión agrega asimismo funciones que se emplean para supervisar los datos sincronizados. Estas funciones se describen en otra sección de este documento.

Véase también

Funciones para la supervisión de los servicios de protección en la página 30
Configuración de servidores registrados en la página 16
Sincronización de datos con SecurityCenter en la página 19
Configuración de conjuntos de permisos en la página 26

Descripción general de la configuración de funciones

Utilice la consola de ePolicy Orchestrator para configurar o modificar la forma en que trabajan las funciones básicas de la extensión.

Tabla 2-2 Tareas de configuración que son necesarias siempre

Para esto...	Realice estas tareas...
Servidores registrados	Para cada cuenta de SecurityCenter: • Registre la cuenta de SecurityCenter con el servidor de ePolicy Orchestrator como un servidor de base de datos externo. Esto requiere credenciales de inicio de sesión administrativo para la cuenta de SecurityCenter. Si no dispone de credenciales de inicio de sesión administrativo, cree una cuenta de administrador de sincronización antes de usar esta función.
Tarea servidor de sincronización de datos de SaaS	Para cada cuenta de SecurityCenter registrada: • Configure un punto de sincronización en el árbol de sistemas. Este punto es la ubicación para almacenar los datos de McAfee SaaS extraídos desde SecurityCenter. • Configure la tarea servidor y después ejecútela inmediatamente o actívela para que se ejecute automáticamente a intervalos regulares. Cuando se instala la extensión, se crea una tarea servidor. Cree otras tareas servidor conforme sea necesario para las cuentas adicionales de SecurityCenter registradas.

Tabla 2-3 Tareas de configuración que son necesarias a veces

Para esto...	Realice estas tareas...
Conjuntos de permisos para funciones de usuario	Para los administradores que trabajen con la extensión en el entorno de ePolicy Orchestrator: • Otorgue funciones de usuario de Security-as-a-Service a los conjuntos de permisos existentes o bien cree nuevos conjuntos de permisos y agréguelos allí. (Para obtener más información, consulte la documentación de ePolicy Orchestrator.) • Especifique los conjuntos de permisos de acceso (lectura o escritura) para cada función.
Cuenta de administrador de sincronización	Para los usuarios que no dispongan de credenciales para una cuenta administrativa de SecurityCenter: • Cree una cuenta de administrador de sincronización. Esto es necesario para configurar servidores registrados y tareas servidor. Si es necesaria una cuenta de administrador de sincronización, los vínculos para crear y editar la cuenta aparecen en SecurityCenter, en la ficha **Servidores de ePO** de la página **Utilidades**.

Véase también

Instalación de la extensión de producto en la página 14
Registro de una cuenta de SecurityCenter en la página 17
Creación de un punto de sincronización en el árbol de sistemas en la página 21
Sincronización de datos desde SecurityCenter en la página 22

Instalación de la extensión de producto

Para que los servicios de protección de McAfee SaaS puedan ser gestionados por el software ePolicy Orchestrator, primero debe descargar e instalar la extensión de Security-as-a-Service.

Antes de empezar

Si ha instalado y desinstalado la extensión anteriormente, debe eliminar algunos archivos remanentes de forma manual.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

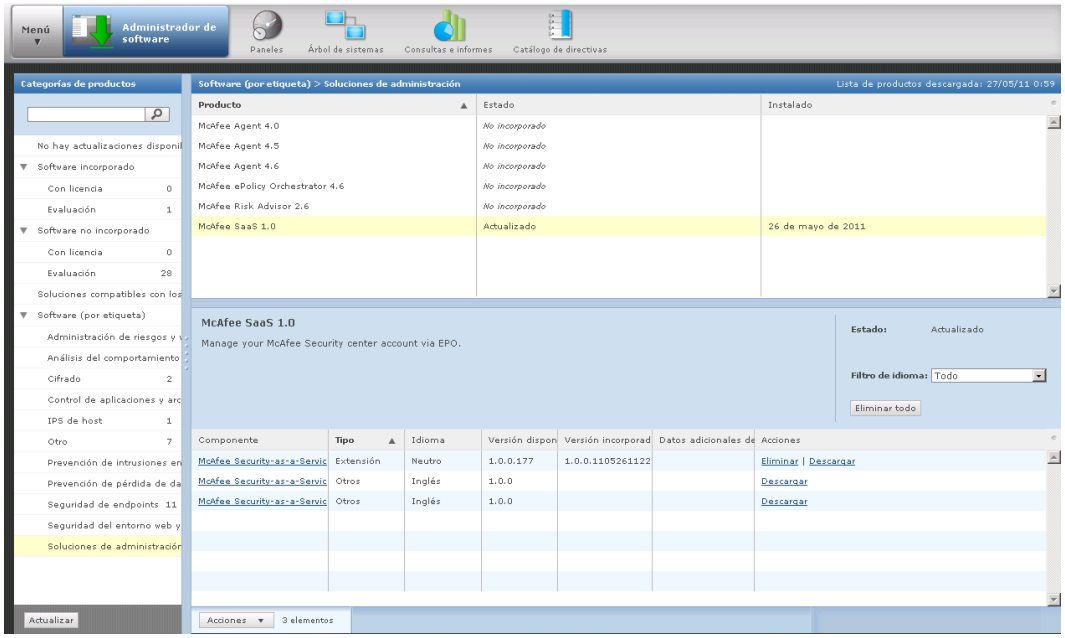
1 Descargue la extensión siguiendo uno de estos métodos:

Desde la consola de ePolicy Orchestrator

a Haga clic en **Menú** | **Software** | **Administrador de software** | **Extensiones**.

b En el panel **Categorías de productos**, haga clic en **Soluciones de administración**.

c En el panel derecho, en **Software**, haga clic en **McAfee SaaS <número de versión>**.



d En el panel derecho, en **Componentes**, localice la extensión y haga clic en **Descargar**.

e En el cuadro de diálogo **Descarga de archivos**, guarde el archivo McAfee Security-as-a-Service.zip en una carpeta local y haga clic en **Aceptar**.

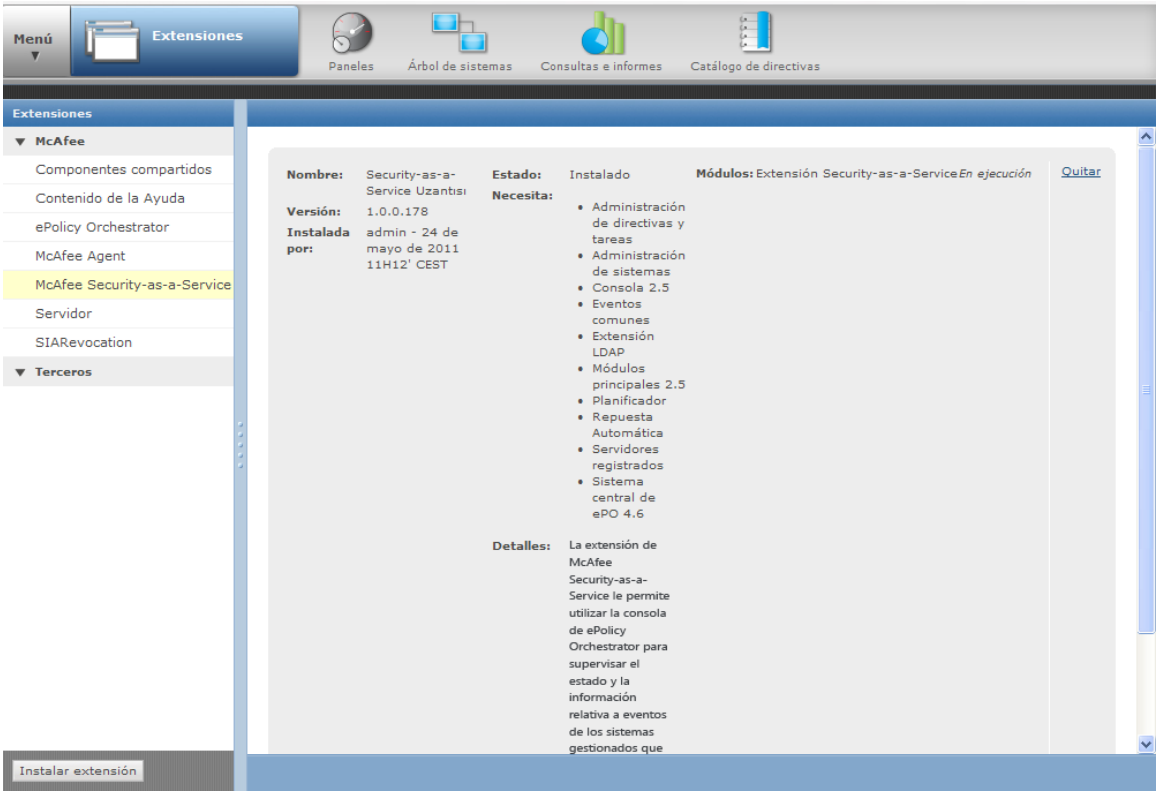
Desde la consola de SecurityCenter

a En la página **Utilidades**, haga clic en la ficha **Servidores de ePO**.

b Haga clic en el vínculo para descargar la extensión.

c En el cuadro de diálogo **Descarga de archivos**, guarde el archivo McAfee Security-as-a-Service.zip en una carpeta local y haga clic en **Aceptar**.

2 En la consola de ePolicy Orchestrator, haga clic en **Menú** | **Software** | **Extensiones**, después, en el panel **Extensiones**, seleccione **McAfee Security-as-a-Service** y, finalmente, en el panel derecho, haga clic en **Instalar extensión**.



Véase también

Eliminación manual de archivos y eventos en la página 42
Eliminación de datos manualmente en la página 43

Configuración de servidores registrados

Para posibilitar la comunicación entre la extensión y la base de datos de SecurityCenter, debe registrar cada cuenta de SecurityCenter con el servidor de ePolicy Orchestrator. Puede hacerlo desde la consola de ePolicy Orchestrator.

El registro requiere credenciales de inicio de sesión para cada cuenta administrativa de SecurityCenter que desee registrar.

Cuando se registra una cuenta de SecurityCenter, el servidor de ePolicy Orchestrator es reconocido por SecurityCenter como servidor registrado de ePolicy Orchestrator. Puede ver una lista de los servidores de ePolicy Orchestrator registrados desde la consola de SecurityCenter, en la ficha **Servidores de ePO** de la página **Utilidades**.

Tabla 2-4 Tareas para servidores registrados

Desde esta consola...	Puede...
ePolicy Orchestrator	• Registrar una cuenta. • Editar la información de registro. • Ver una lista de cuentas registradas. • Eliminar las cuentas registradas. Después de registrar o eliminar una cuenta en la consola de ePolicy Orchestrator, se muestra una alerta en la página **Panel** de la consola de SecurityCenter.
SecurityCenter	• Ver información sobre el servidor de ePolicy Orchestrator donde haya registrado la cuenta de SecurityCenter. • Eliminar el registro del servidor de ePolicy Orchestrator. Para obtener instrucciones, consulte la documentación de McAfee SaaS Endpoint Protection, disponible en la ficha **Ayuda y asistencia** de la consola de SecurityCenter.

Registro de una cuenta de SecurityCenter

Registre la cuenta de SecurityCenter con el software ePolicy Orchestrator, que permite que la extensión extraiga los datos de McAfee SaaS y los sincronice con la base de datos de ePolicy Orchestrator.

Antes de empezar

Si no dispone de credenciales de inicio de sesión para una cuenta administrativa de SecurityCenter, cree una cuenta de administrador de sincronización.

Se muestra una alerta en la página **Panel** de la consola de SecurityCenter siempre que se registra una cuenta.

Si dispone de varias cuentas de SecurityCenter, registre cada una de ellas por separado.

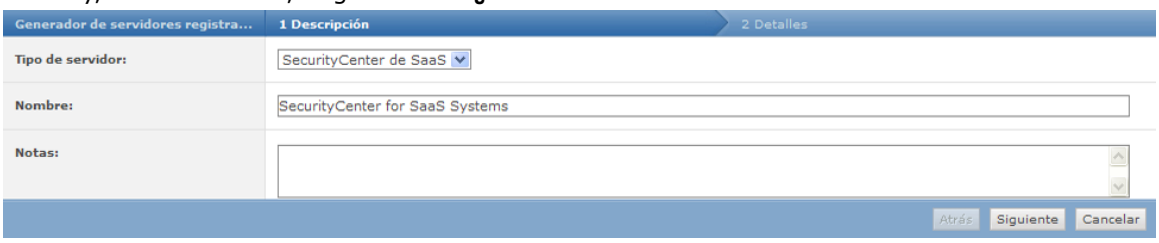
Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 En la consola de ePolicy Orchestrator, haga clic primero en **Menú** | **Configuración** | **Servidores registrados** y, después, en **Nuevo servidor**.

Se abre el asistente Generador de servidores registrados por la página **Descripción**.

2 En la lista **Tipo de servidor**, seleccione **SecurityCenter de SaaS**, especifique un nombre y las notas que desee y, a continuación, haga clic en **Siguiente**.



3 En la lista **Ubicación de SecurityCenter**, seleccione el centro de datos que albergue la cuenta.

El centro de datos se identifica mediante la porción del dominio de la URL utilizada para acceder a la consola de SecurityCenter (por ejemplo, www.mcafee.com o www.*suproveedordeservicios*.com). Si no está seguro de qué centro de datos seleccionar, consulte la URL proporcionada en el mensaje de correo electrónico de bienvenida que recibió al adquirir la suscripción a los servicios de protección de McAfee SaaS.

4 Introduzca sus credenciales para iniciar sesión en la cuenta de SecurityCenter.

Recibió estas credenciales en un mensaje de correo electrónico de bienvenida que le envió su proveedor de servicios cuando adquirió una suscripción a los servicios de protección de McAfee SaaS. Si McAfee o su proveedor de servicios no le enviaron credenciales, use las credenciales de una cuenta de administrador de sincronización.

5 Guarde la configuración haciendo clic en uno de estos botones:

- **Guardar configuración y registrar SecurityCenter**: guarda la información y registra el servidor.
- **Guardar** (esquina inferior derecha): guarda la información sin realizar el registro. Puede completar el registro más tarde sin necesidad de volver a introducir la información.

Cuando se completa el registro, la dirección de correo electrónico de la cuenta aparece en el monitor de **McAfee SecurityCenter** en el panel de **Security-as-a-Service** predeterminado, junto con vínculos a páginas en la consola de SecurityCenter.

Véase también

Purga de eventos de amenazas en la página 35
Creación o actualización de una cuenta de administrador de sincronización en la página 28

Visualización o edición de una lista de cuentas de SecurityCenter registradas

Vea una lista de las cuentas de SecurityCenter registradas en la consola de ePolicy Orchestrator y edite la configuración conforme sea necesario.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 Haga clic en **Menú** | **Configuración** | **Servidores registrados** para mostrar una lista de todos los servidores registrados.

2 Para ver la configuración de un servidor, seleccione el servidor registrado en la lista y haga clic en **Acciones** | **Editar**.

3 Modifique la configuración según sus preferencias y, a continuación, haga clic en **Guardar**.

Eliminación de una cuenta de SecurityCenter registrada

Elimine el registro de una cuenta de SecurityCenter que ya no usará más. Este procedimiento equivale a "anular el registro" de un servidor registrado.

Se muestra una alerta en la página **Panel** de la consola de SecurityCenter cuando se elimina un servidor registrado.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 Haga clic en **Menú** | **Configuración** | **Servidores registrados**.

2 Seleccione el servidor registrado en la lista y, a continuación, haga clic en **Acciones** | **Eliminar**.

3 Elimine el contenedor de grupos en el árbol de sistemas que actuó como punto de sincronización para la cuenta eliminada.

   a Haga clic en **Menú** | **Sistemas** | **Árbol de sistemas**.

   b En el panel **Árbol de sistemas**, seleccione el contenedor de grupos.

   c Haga clic en **Acciones en los sistemas** | **Eliminar grupo**.

4 Decida si purgar o no los eventos de amenazas correspondientes a la cuenta eliminada.

   - Si va a cancelar la cuenta de SecurityCenter, puede conservar los eventos de amenazas como referencia.
   - Si tiene la intención de volver a registrar la misma cuenta de SecurityCenter en el futuro, purgue todos los eventos de amenazas. En caso contrario, los datos históricos se extraerán cuando sincronice los datos correspondientes a la cuenta que se vuelva a registrar, lo que puede provocar que se creen entradas de eventos duplicadas.

Véase también

Purga de eventos de amenazas en la página 35

Sincronización de datos con SecurityCenter

Para poder ver los datos de McAfee SaaS en la consola de ePolicy Orchestrator, los datos deben extraerse antes de una cuenta de SecurityCenter registrada y sincronizarse con el servidor y la base de datos de ePolicy Orchestrator.

Cuando se instala la extensión, se crea una tarea servidor de sincronización de datos de SaaS y se preconfigura para que extraiga datos de una cuenta de SecurityCenter registrada.

Los datos sincronizados aparecen en el árbol de sistemas y en los monitores del panel de **Security-as-a-Service**, y es posible ejecutar consultas con respecto a los datos.

Durante las actualizaciones posteriores, los datos de SaaS se actualizan y sincronizan para reflejar los datos más recientes de la cuenta de SecurityCenter.

Dónde se colocan los datos: puntos de sincronización

Los datos correspondientes a los sistemas gestionados de McAfee SaaS se colocan en un contenedor del árbol de sistemas que se denomina *punto de sincronización*. Es necesario que cree este contenedor antes de ejecutar la tarea servidor por primera vez. Desde esta ubicación, puede ver los grupos y los equipos protegidos por los servicios de McAfee SaaS.

Si tiene varias cuentas de SecurityCenter, cree un punto de sincronización y una tarea servidor para cada una de las cuentas. Cree todos los puntos de sincronización en el nivel raíz en el árbol de sistemas; no anide un grupo dentro de otro.

Sincronización de datos completa e incremental

La primera vez que una tarea de sincronización de datos extrae datos de SaaS de una cuenta de SecurityCenter, extrae todos los datos relevantes de los últimos 30 días. El volumen de los datos, entre otras cosas, determina la cantidad de tiempo y recursos necesaria para realizar la tarea. La expectativa es que una tarea de sincronización de datos inicial usa los recursos del sistema de una forma más intensiva que las posteriores tareas de sincronización de datos para la misma cuenta de SecurityCenter.

Las posteriores tareas de sincronización de datos sólo extraen los datos que se han agregado o modificado desde la última sincronización. Esto suele afectar a un menor volumen de datos, por lo que estas actualizaciones requieren menos recursos de la red, del servidor de ePolicy Orchestrator y de la base de datos de ePolicy Orchestrator (que puede que se ejecute en un sistema distinto).

Sincronización de datos bajo demanda y planificada

Puede sincronizar los datos de SaaS en cualquier momento bajo demanda, y también puede planificar la sincronización de datos de SaaS para que se realice de forma automática a intervalos periódicos.

Puede planificar la sincronización para que se ejecute durante las horas de menor actividad en la red y de la consola de ePolicy Orchestrator. Esto puede ser especialmente importante a la hora de extraer datos de una cuenta de SecurityCenter por primera vez.

Acerca de los datos sincronizados

Puede especificar los tipos de datos que se deben recuperar para los servicios de protección de McAfee SaaS seleccionando opciones para la tarea servidor de sincronización de datos de SaaS.

La tarea servidor de sincronización de datos de SaaS puede recuperar estos tipos de datos:

- Endpoints (sistemas gestionados).
- Grupos en los que están organizados los sistemas gestionados.
- Eventos, como detecciones, comunicaciones bloqueadas o sitios web bloqueados.
- Estado de la protección.
- Información de resumen relacionada con servicios de protección específicos, como el número de mensajes de correo electrónico o sitios web analizados.

Cuando se completa la sincronización de datos de SaaS, puede acceder a los datos presentes en la consola de ePolicy Orchestrator utilizando las funciones de supervisión que proporcionan el software ePolicy Orchestrator y la extensión de Security-as-a-Service.

Véase también

Funciones para la supervisión de los servicios de protección en la página 30

Creación de un punto de sincronización en el árbol de sistemas

En el árbol de sistemas, cree un contenedor en el que se coloquen los datos de los servicios de protección de McAfee SaaS cuando se extraigan de la cuenta de SecurityCenter y se sincronicen con la base de datos de ePolicy Orchestrator. Este contenedor se denomina *punto de sincronización*.

Antes de empezar

Registre la cuenta de SecurityCenter con el software ePolicy Orchestrator. Debe tener los permisos correctos configurados para el árbol de sistemas y las tareas servidor. Para obtener información sobre la configuración de conjuntos de permisos, consulte la documentación de ePolicy Orchestrator.

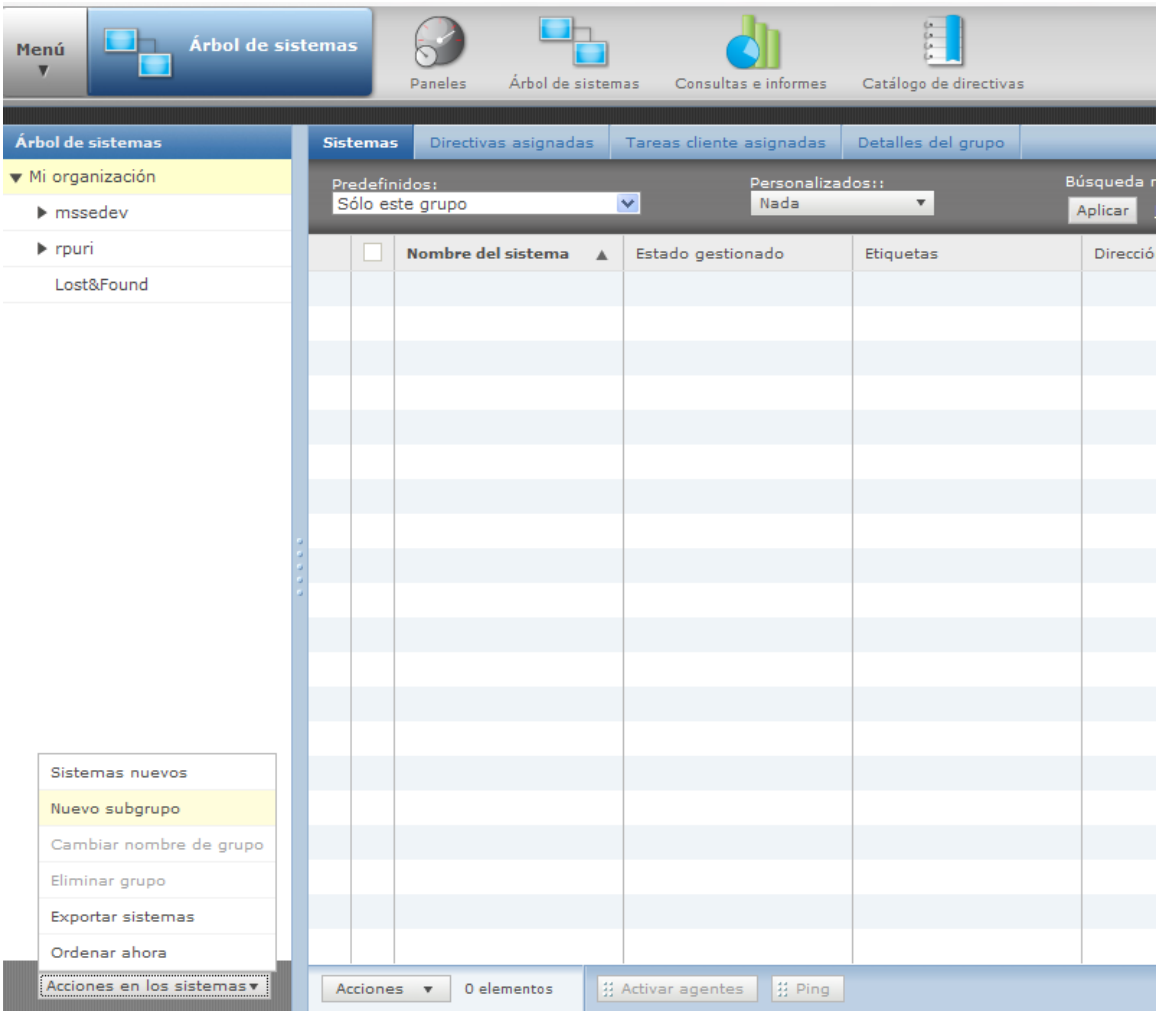
Si tiene varias cuentas de SecurityCenter, cree un punto de sincronización independiente en el nivel raíz del árbol de sistemas para cada una de las cuentas. No anide un contenedor de sincronización dentro de otro.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 En la consola de ePolicy Orchestrator, haga clic en **Menú** | **Sistemas** | **Árbol de sistemas**.

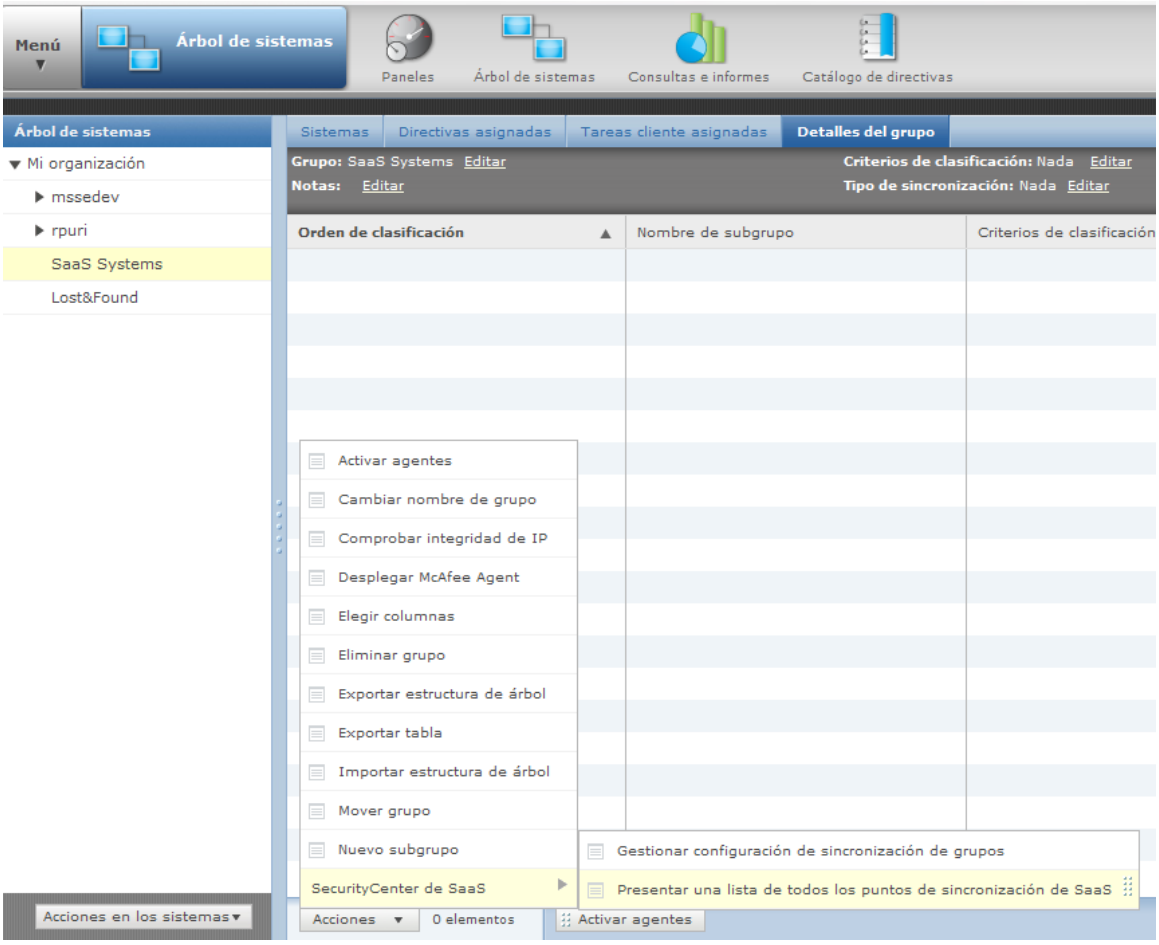
2 Haga clic en **Acciones en los sistemas** | **Nuevo subgrupo**.



3 Introduzca un nombre para el nuevo subgrupo.

4 En el panel del árbol de sistemas, seleccione el nuevo grupo y haga clic en la ficha **Detalles del grupo**.

5 Haga clic en **Acciones** | **SecurityCenter de SaaS** | **Gestionar configuración de sincronización de grupos**.



6 Seleccione una cuenta de SecurityCenter registrada.

7 Guarde la configuración haciendo clic en uno de estos botones:

- **Guardar configuración y sincronizar ahora**: guarda la configuración de sincronización y extrae los datos de forma inmediata.
- **Guardar** (esquina inferior derecha): guarda la configuración sin extraer los datos. Puede llevar a cabo la sincronización más tarde sin necesidad de volver a introducir la información.

Sincronización de datos desde SecurityCenter

Es posible extraer datos de McAfee SaaS de una cuenta de SecurityCenter registrada y sincronizarlos con la base de datos de ePolicy Orchestrator ejecutando una tarea servidor. La tarea puede ejecutarse

bajo demanda o automáticamente a intervalos regulares. Por ejemplo, se puede planificar la tarea para que extraiga datos a la misma hora cada noche durante las horas de menor actividad en la red.

Antes de empezar

Registre cada cuenta de SecurityCenter con el software ePolicy Orchestrator y cree su punto de sincronización en el árbol de sistemas. Debe disponer de los permisos correctos configurados para el conjunto de permisos de tareas servidor. Para obtener información sobre la configuración de conjuntos de permisos, consulte la documentación de ePolicy Orchestrator.

Tras sincronizar los datos de SaaS, los sistemas gestionados de McAfee SaaS aparecen en el árbol de sistemas y los datos de SaaS aparecen en monitores en el panel de **Security-as-a-Service**.

Si elimina un punto de sincronización existente, su tarea servidor asociada deja de ejecutarse. Si vuelve a crear el punto de sincronización, debe volver a configurar su tarea servidor o bien crear una tarea servidor que sincronice los datos. Volver a crear el punto de sincronización no hace que la tarea servidor asociada a la instancia anterior del punto de sincronización empiece automáticamente a sincronizar datos para la nueva instancia del punto de sincronización.

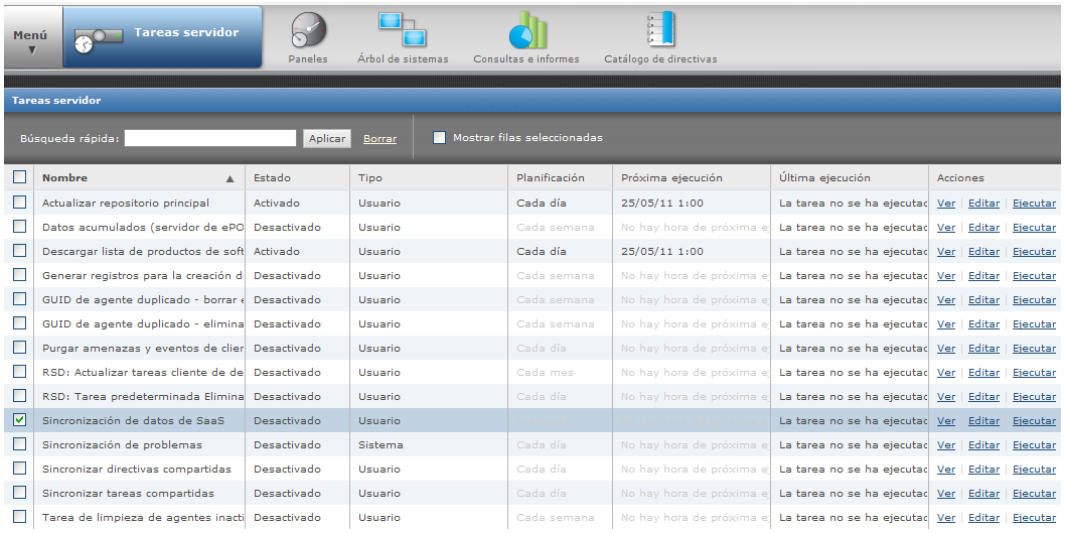
Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 En la consola de ePolicy Orchestrator, haga clic en **Menú** | **Automatización** | **Tareas servidor**.

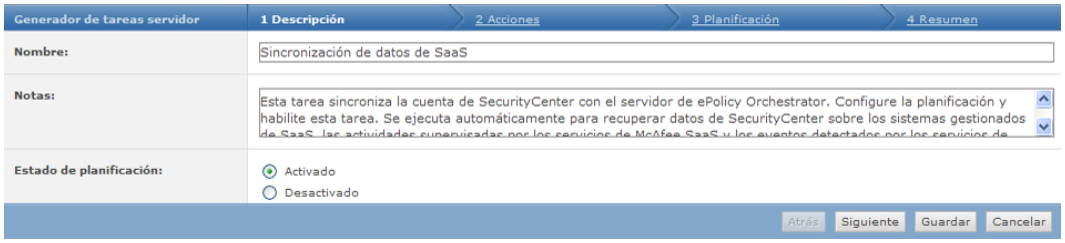
2 Si es la primera vez que utiliza esta tarea servidor para sincronizar datos, debe configurarla:

a Localice la tarea **Sincronización de datos de SaaS** en la lista y, a continuación, haga clic en **Editar**.



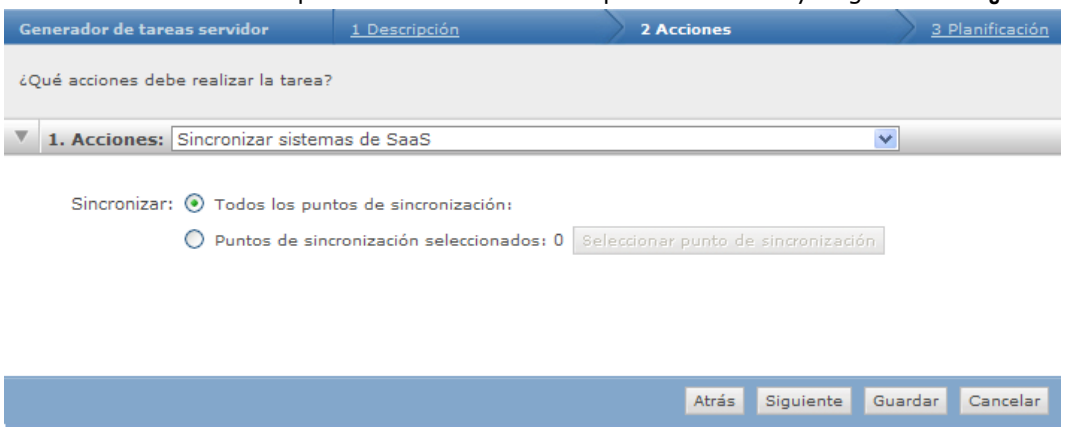
b En el asistente, escriba las notas que desee en la página **Descripción**, seleccione si desea activar la planificación y, a continuación, haga clic en **Siguiente**.

Si desea que la tarea servidor se ejecute automáticamente a intervalos regulares, seleccione **Activado** y, a continuación, configure las opciones de planificación para esta tarea. Puede configurar las opciones tanto si están activadas como desactivadas.



c En la lista **Acciones**, asegúrese de que esté seleccionado **Sincronizar sistemas de SaaS**.

d Seleccione uno o varios puntos de sincronización para esta tarea y haga clic en **Siguiente**.



Los tipos de datos que se deben sincronizar están previamente seleccionados.

e Seleccione las opciones de planificación y haga clic en **Siguiente**.

Se ignorarán estas selecciones a menos que active la planificación en uno de los pasos anteriores de este procedimiento. Puede configurar y guardar las opciones para activarlas o desactivarlas más tarde conforme sea necesario.

f Revise el resumen y haga clic en **Guardar**.

3 Para ejecutar la tarea en cualquier momento, haga clic en **Menú** | **Automatización** | **Tareas servidor**, localice la tarea en la lista y, a continuación, haga clic en **Ejecutar**.

Si ha activado la planificación, la tarea servidor se ejecuta automáticamente conforme a los intervalos planificados.

Véase también

Creación de un punto de sincronización en el árbol de sistemas en la página 21
Creación o actualización de una cuenta de administrador de sincronización en la página 28

Visualización del estado de los puntos de sincronización

Verifique que los datos de McAfee SaaS estén actualizados para todos los puntos de sincronización del árbol de sistemas.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 En la consola de ePolicy Orchestrator, haga clic en **Menú** | **Sistemas** | **Árbol de sistemas** y, a continuación, seleccione un grupo.

2 En la ficha **Detalles del grupo**, haga clic en **Acciones** | **SecurityCenter de SaaS** | **Presentar una lista de todos los puntos de sincronización de SaaS** y, a continuación, observe la **Hora de la última sincronización** y otra información que se presenta para cada punto de sincronización.

Configuración de conjuntos de permisos

Un conjunto de permisos es un grupo de derechos de acceso concedidos a una cuenta de usuario para funciones específicas de un producto. Los conjuntos de permisos sólo *otorgan* permisos, nunca los quitan.

Todos los permisos para todos los productos y funciones se asignan automáticamente a los administradores globales. Los permisos para los demás usuarios se asignan manualmente. Los administradores globales pueden asignar conjuntos de permisos existentes al crear o editar cuentas de usuario y conjuntos de permisos.

Para obtener información sobre los conjuntos de permisos, consulte la documentación de ePolicy Orchestrator.

Conjuntos de permisos de Security-as-a-Service

La extensión agrega una sección **Security-as-a-Service** a los conjuntos de permisos con dos funciones de usuario que están preconfiguradas. Éstas definen los derechos de acceso a las funciones de la extensión. Los administradores globales deben otorgar las funciones de usuario de Security-as-a-Service a los conjuntos de permisos existentes o bien crear conjuntos de permisos y agregarlos allí.

Tabla 2-5 Permisos para funciones de usuario de Security-as-a-Service

Funciones de usuario	Permisos predeterminados
Revisor de SaaS	Ver servidores registrados, ver datos sincronizados y ejecutar consultas.
Administrador de SaaS	Crear, editar o eliminar servidores registrados, tareas servidor y consultas.

Si es necesario, los administradores globales pueden cambiar los permisos definidos para estas funciones, o bien crear conjuntos de permisos para funciones nuevas.

Otros conjuntos de permisos necesarios

ePolicy Orchestrator necesita que los permisos otorguen acceso a otras funciones que funcionan con la extensión, como las consultas y los paneles. Por ejemplo, para gestionar la sincronización de datos de SaaS y los datos sincronizados, un usuario necesita permisos de visualización para el registro de eventos de amenazas, permisos de visualización para los sistemas, permisos de visualización para el acceso al árbol de sistemas y permisos de visualización y modificación para la tarea servidor de sincronización de datos de SaaS.

Tabla 2-6 Permisos requeridos por función

Funciones	Conjuntos de permisos requeridos
Paneles	Paneles, consultas
Consultas	Consultas

Tabla 2-6 Permisos requeridos por función *(continuación)*

Funciones	Conjuntos de permisos requeridos
Tareas servidor	Tareas servidor
Eventos en sistemas gestionados de SaaS	Sistemas, acceso al árbol de sistemas, registro de eventos de amenazas

Configuración de conjuntos de permisos para funciones de usuario

Actualice los permisos de lectura o escritura asignados a las funciones de usuario de Security-as-a-Service que hayan sido definidas para el entorno de ePolicy Orchestrator.

Antes de empezar

Determine las funciones de la extensión a las que desea dar acceso y los conjuntos de permisos adicionales que se deben asignar para acceder a todos los aspectos de esa función.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 En la consola de ePolicy Orchestrator, haga clic en **Menú** | **Administración de usuarios** | **Conjuntos de permisos**.

2 Seleccione una función de usuario.

- **Administrador de SaaS**: puede crear, editar o eliminar servidores registrados, tareas servidor y consultas.
- **Revisor de SaaS**: puede ver servidores registrados y datos sincronizados, así como ejecutar consultas.

3 En la lista **Acciones**, seleccione **Editar**.

4 Seleccione el permiso para cada función:

- **Ninguno**
- **Ver sólo la configuración**
- **Ver y cambiar configuración**

5 Haga clic en **Guardar**.

Para crear funciones adicionales, consulte la documentación de ePolicy Orchestrator.

Configuración de una cuenta de administrador de sincronización

Las tareas que incluyen alguna comunicación entre el servidor de SecurityCenter y otros servidores requieren credenciales de inicio de sesión para una cuenta de SecurityCenter administrativa.

Si aún no dispone de una cuenta administrativa de SecurityCenter, debe crear un una cuenta de administrador de sincronización antes de ejecutar estas tareas. Esta cuenta proporciona las credenciales necesarias para acceder a SecurityCenter únicamente para estas tareas. (Las credenciales de una cuenta administrativa son proporcionadas normalmente por McAfee, o bien por el proveedor a quien le haya adquirido los servicios de protección de McAfee SaaS.)

Utilice una cuenta de administrador de sincronización para:

- Registre una cuenta de SecurityCenter con el software ePolicy Orchestrator.
- Ejecutar o planificar la sincronización de datos entre el servidor de SecurityCenter y un servidor de Active Directory o ePolicy Orchestrator.
- Utilice la utilidad Push Install para desplegar el software cliente en los sistemas del dominio de Active Directory desde la consola de SecurityCenter.

Sólo se puede crear una cuenta de administrador de sincronización para una cuenta de SecurityCenter.

Si es necesaria una cuenta de administrador de sincronización, los vínculos para crear y editar la cuenta aparecen en SecurityCenter, en las fichas **Configuración de Active Directory** o **Servidores de ePO** de la página **Utilidades**.

Creación o actualización de una cuenta de administrador de sincronización

Si no dispone de una cuenta administrativa de SecurityCenter, debe crear una cuenta de administrador de sincronización para llevar a cabo tareas que precisen que el servidor de SecurityCenter se comunique con otros servidores.

Sólo se puede crear una cuenta de administrador de sincronización para una cuenta de SecurityCenter.

Si tiene una cuenta de SecurityCenter administrativa, los vínculos que se mencionan en esta tarea no aparecen. Sólo aparecen cuando se requiere una cuenta de administrador de sincronización.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 En la consola de SecurityCenter, haga clic en la ficha **Utilidades** y, a continuación, realice una de las siguientes acciones:
   - Haga clic en la ficha **Servidores de ePO**.
   - Haga clic en la ficha **Configuración de Active Directory**.

   Si debe crear una cuenta de administrador para realizar una tarea, aparece un mensaje, así como un vínculo **Crear**. Si ya existe una cuenta de administrador, aparecen una dirección de correo electrónico para la cuenta y un vínculo **Editar**.

2 Haga clic en el vínculo que corresponda.
   - **Crear**: introduzca la dirección de correo electrónico y la contraseña correspondientes a una nueva cuenta.
   - **Editar**: actualice la dirección de correo electrónico o la contraseña correspondientes a una cuenta existente.

3 Haga clic en **Guardar**.

3 Supervisión y gestión de la seguridad de McAfee SaaS

Con las funciones de la extensión, puede supervisar el estado de los sistemas gestionados y de los servicios de protección, así como utilizar la consola de ePolicy Orchestrator para identificar problemas.

Contenido

Descripción general del proceso de supervisión

Recomendamos utilizar una estrategia a dos bandas para supervisar y administrar los servicios de protección de McAfee SaaS en un entorno de ePolicy Orchestrator.

1 **Visualizar los datos sincronizados de SaaS desde la consola de ePolicy Orchestrator.**

Use las funciones de supervisión en la consola de ePolicy Orchestrator para comprobar los datos de SaaS e identificar problemas con los sistemas gestionados de McAfee SaaS.

Tabla 3-1 Dónde acceder a las funciones de supervisión

Tipo de datos	Dónde se ve
Información de resumen del estado y la actividad en tablas y gráficos	Panel y monitores de **Security-as-a-Service**
Tipos de información que se pueden seleccionar acerca del estado de sistemas gestionados de McAfee SaaS	Consultas e informes de **Security-as-a-Service**
Servicios de protección de McAfee SaaS y sus propiedades	En la página **Información del sistema**, la ficha **Productos de SaaS** y los detalles de los datos del monitor.
Detalles sobre los eventos de detección en sistemas gestionados de McAfee SaaS	Registro de eventos de amenazas; monitores, consultas e informes de Security-as-a-Service
Grupos y sistemas protegidos por los servicios de McAfee SaaS	En el árbol de sistemas, en la ficha **Sistemas**.
Estado de sincronización de cada punto de sincronización	En el árbol de sistemas, en la ficha **Detalles del grupo**, haga clic en **Acciones** | **SaaS SecurityCenter** | **Presentar una lista de todos los puntos de sincronización de SaaS**.

2 **Solucionar problemas desde la consola de SecurityCenter.**

Acceda a la consola de SecurityCenter para instalar software cliente en sistemas gestionados, configurar directivas y llevar a cabo otros pasos para corregir problemas. El panel predeterminado de **Security-as-a-Service** proporciona un acceso fácil a través del monitor de **McAfee SecurityCenter**, que a su vez ofrece vínculos directos a la consola de SecurityCenter para cada cuenta registrada.

Para obtener más información sobre la utilización de las funciones de SecurityCenter, consulte la documentación de McAfee SaaS Endpoint Protection, disponible en la página **Ayuda y asistencia** de la consola de SecurityCenter.

Consideraciones para supervisar la seguridad con otros productos de McAfee

Es importante comprobar y solucionar cualquier problema de compatibilidad entre la extensión y otro software de McAfee que se esté ejecutando en el entorno de ePolicy Orchestrator.

Véase también

Paneles y monitores de Security-as-a-Service en la página 31
Consultas e informes de Security-as-a-Service en la página 33
Página Información del sistema en la página 34
Registro de eventos de amenazas en la página 35
Apertura de SecurityCenter en la página 36
Compatibilidad con otros productos de McAfee en la página 36

Funciones para la supervisión de los servicios de protección

La extensión agrega funciones que se utilizan para visualizar y supervisar los datos sincronizados de los servicios de protección de McAfee SaaS.

Tabla 3-2 Funciones para supervisar datos de SaaS

Para esta función del software McAfee ePO...	La extensión agrega...
Paneles	Un panel preconfigurado: • **Security-as-a-Service**: muestra monitores correspondientes a los widgets que aparecen en la página **Panel** de la consola de SecurityCenter.
Consultas	Consultas preconfiguradas y opciones para crear consultas personalizadas: • Nuevo grupo de consultas compartidas, **Security-as-a-Service**, con un conjunto de consultas relacionadas con los datos de SaaS. • Nuevo grupo de tipos de resultado de consulta, **Security-as-a-Service**, en el Generador de consultas. El grupo contiene un conjunto de destinos de consulta relacionados con los datos de SaaS.

Tabla 3-2 Funciones para supervisar datos de SaaS *(continuación)*

Para esta función del software McAfee ePO...	La extensión agrega...
Árbol de sistemas	En la ficha **Detalles del grupo**, dos nuevas opciones del menú **Acciones**: • **SaaS SecurityCenter | Gestionar configuración de sincronización de grupos**: le permite asociar un contenedor de grupos en el árbol de sistemas a una cuenta de SecurityCenter registrada. (El contenedor se convierte en el punto de sincronización para la cuenta.) • **SaaS SecurityCenter | Presentar una lista de todos los puntos de sincronización de SaaS**: muestra en qué momento se sincronizaron por última vez los datos para cada cuenta registrada.
Página Información del sistema	• Nueva ficha **Productos de SaaS**. • Nuevo grupo de monitores de detalles personalizables.

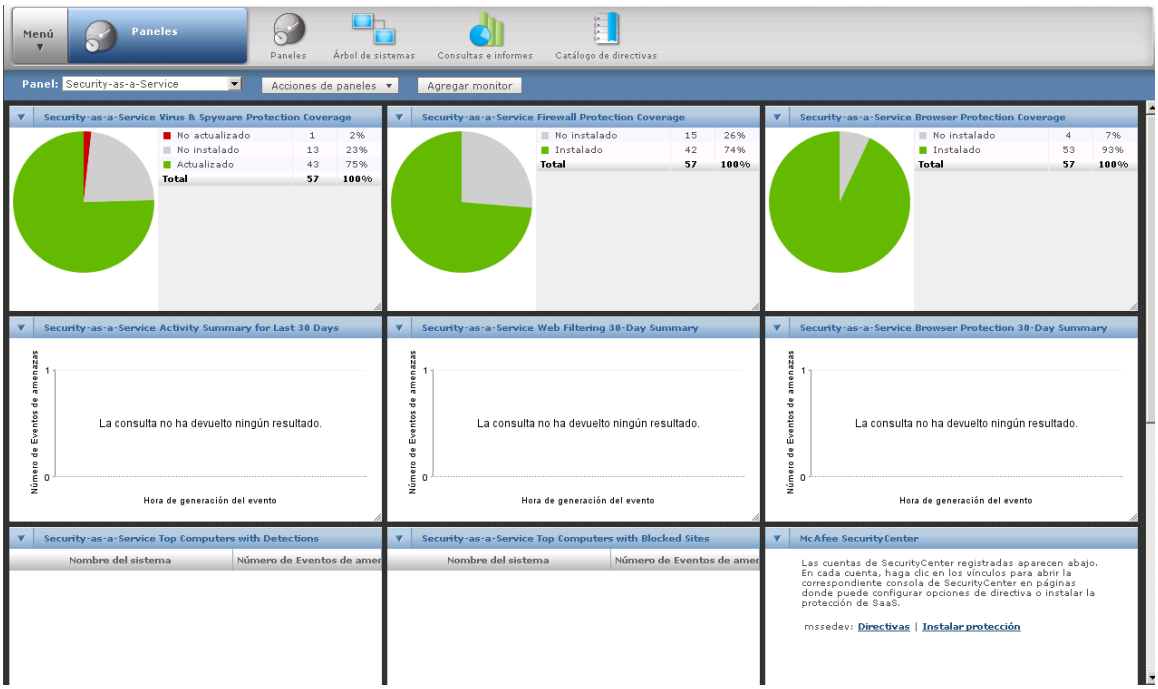
Paneles y monitores de Security-as-a-Service

Cuando se instala la extensión, se crea un panel **Security-as-a-Service** preconfigurado. Este panel muestra los monitores de **Security-as-a-Service**.

Los paneles son una recopilación de monitores que constituyen una herramienta esencial para la gestión del entorno. Puede crear y editar varios paneles si dispone de los permisos adecuados.

Panel de Security-as-a-Service predeterminado

La extensión proporciona un panel predeterminado con monitores que se corresponden con los widgets de la página **Panel** de SecurityCenter. *Los widgets* son pequeños informes interactivos que proporcionan información de resumen y general acerca de la cuenta.



Si registra y sincroniza datos para varias cuentas de SecurityCenter, los monitores muestran datos de resumen acerca de todas las cuentas.

Los monitores de datos de SaaS disponibles para el panel de **Security-as-a-Service** son los siguientes:

Tabla 3-3 Monitores de Security-as-a-Service

Este monitor...	Muestra...
McAfee SecurityCenter	Vínculos a cada cuenta de SecurityCenter registrada. Seleccione un vínculo para abrir una ventana del navegador y mostrar una página en la consola de SecurityCenter.
Cobertura de protección frente a spyware y virus de SaaS	Número de equipos en la cuenta en los que la protección está actualizada, no actualizada y no instalada. Los equipos actualizados han descargado los últimos archivos de definición de detección (DAT). Es necesario actualizar los archivos DAT de los equipos no actualizados. Haga clic en uno de los colores del gráfico de sectores del widget para que se muestre una lista de los equipos de una categoría concreta.
Cobertura de protección por firewall de SaaS	Número de equipos en la cuenta en los que la protección está instalada y no instalada. Haga clic en uno de los colores del gráfico de sectores del widget para que se muestre una lista de los equipos de una categoría concreta.
Cobertura de protección del navegador de SaaS	Número de equipos en la cuenta en los que la protección está instalada y no instalada. Haga clic en uno de los colores del gráfico de sectores del widget para que se muestre una lista de los equipos de una categoría concreta.
Principales equipos con detecciones de SaaS	Equipos con el mayor número de amenazas detectadas durante los últimos 7 días. Haga clic en un nombre de equipo o una cantidad de detecciones para mostrar los detalles.
Principales equipos con sitios bloqueados de SaaS	Equipos con el mayor número de sitios bloqueados durante los últimos 7 días por el servicio de protección del navegador. Haga clic en un nombre de equipo o una cantidad de detecciones para mostrar los detalles.
Resumen de actividad de los últimos 30 días de SaaS	Número de amenazas detectadas a diario durante el último mes.
Resumen de protección del navegador de SaaS de los últimos 30 días	Un historial de intentos de acceso durante los últimos 30 días a sitios web bloqueados, categorizados por las clasificaciones de seguridad de los sitios. Haga clic en una categoría para mostrar los detalles.
Resumen de filtrado web de SaaS de los últimos 30 días	Un historial de intentos de acceso durante los últimos 30 días a sitios web que el servicio de filtrado web bloquea o sobre los que advierte a los usuarios conforme a la configuración de directiva correspondiente al filtrado de contenido. Haga clic en una categoría para mostrar los detalles.
Tendencia durante 7 días de la protección de correo electrónico SaaS	Número y tipo de amenazas de correo electrónico detectadas a diario durante la última semana por el servicio de protección de correo electrónico SaaS. Haga clic en una categoría para mostrar los detalles.
Resumen de 7 días de la protección de correo electrónico SaaS	Número total de mensajes de correo electrónico enviados a su cuenta durante la última semana, número y tipo de amenazas detectadas por el servicio de protección de correo electrónico SaaS y número de mensajes que no contienen amenazas. Haga clic en una categoría para mostrar los detalles.
Análisis de vulnerabilidades y certificación PCI de SaaS	Número total de vulnerabilidades detectadas desde el último análisis. Clasifica el nivel de gravedad como bajo, medio, alto, crítico o urgente. Haga clic en una categoría para mostrar los detalles.

Paneles personalizados

Puede crear paneles personalizados y seleccionar los monitores y las consultas que desee mostrar.

Para obtener más información acerca de la creación y el uso de paneles, consulte la documentación de ePolicy Orchestrator.

Consultas e informes de Security-as-a-Service

La extensión incluye generación de consultas e informes a través del software ePolicy Orchestrator.

Puede crear consultas a partir de las propiedades almacenadas en la base de datos de ePolicy Orchestrator o bien utilizar consultas predefinidas. Para obtener más información, consulte la documentación de ePolicy Orchestrator.

La extensión agrega estas funciones de generación de informes al entorno de ePolicy Orchestrator:

- Varias consultas predefinidas que se pueden ejecutar con o sin edición previa.
- Un grupo de tipos de resultado de consulta, **Security-as-a-Service**, en el Generador de consultas. El grupo contiene un conjunto de destinos de consulta relacionados con los datos de SaaS que permiten crear consultas personalizadas.

Organice y mantenga consultas personalizadas conforme a sus necesidades y, después, úselas para ejecutar informes. Puede exportar informes en una gran variedad de formatos de archivo.

Consultas predefinidas

La extensión proporciona varas consultas predefinidas. Puede utilizarlas con su configuración predeterminada o editarlas para obtener sólo la información que necesita.

Los nombres de las consultas predefinidas coinciden exactamente con los nombres de los monitores de SaaS predefinidos para el panel de **Security-as-a-Service**.

Consultas e informes personalizados

Puede crear consultas e informes personalizados con el Generador de consultas. Los tipos de resultado seleccionados en el Generador de consultas identifican el tipo de datos que recupera la consulta.

La extensión agrega un nuevo grupo de tipos de resultado de consulta, **Security-as-a-Service**, en el Generador de consultas. El grupo contiene un conjunto de destinos de consulta relacionados con los datos de SaaS.

Tabla 3-4 Tipos de resultado de consulta de Security-as-a-Service

Tipo de resultado de consulta	Muestra esta información...
Propiedades de evento de SaaS	Eventos de detección
Sistemas gestionados de SaaS	Sistemas gestionados por SecurityCenter
Propiedades de producto de SaaS	Propiedades de los productos de McAfee SaaS instalados en sistemas gestionados
Productos de SaaS	Productos de McAfee SaaS que se encuentran en uso
Informes de resumen de SaaS	Datos de resumen de los servicios de protección de correo electrónico SaaS y de análisis de vulnerabilidades de SaaS

Para cada tipo de resultado, la extensión agrega diversas propiedades disponibles en el Generador de consultas para emplearlas en consultas personalizadas.

Para obtener más información sobre la creación y el uso de consultas e informes, consulte la documentación de ePolicy Orchestrator.

Página Información del sistema

La extensión agrega datos de consultas e información de producto a la página **Información del sistema** de la consola de ePolicy Orchestrator.

Acceda a la página **Información del sistema** haciendo clic en cualquier sistema gestionado en el árbol de sistemas.

Datos del monitor y de las consultas

La extensión agrega datos para el monitor de detalles personalizable que aparece en la esquina superior derecha de la página **Información del sistema**. Haga clic en **Personalizar** para mostrar y seleccionar un monitor.

Tabla 3-5 Consultas disponibles para el monitor de detalles

Categoría de consulta	Consultas
Grupos compartidos: Security-as-a-Service	• **Resumen de actividad de los últimos 30 días de Security-as-a-Service** • **Resumen de protección del navegador de los últimos 30 días de Security-as-a-Service** • **Resumen de filtrado web de los últimos 30 días de Security-as-a-Service**

La información de resumen sólo está disponible para los servicios de protección de McAfee SaaS que estén en uso para el sistema gestionado.

Ficha Productos de SaaS

La extensión crea una ficha **Productos de SaaS** que muestra cada servicio de protección de McAfee SaaS en uso para el sistema gestionado.

Utilice esta ficha para ver rápidamente las propiedades de cada servicio de protección. Las propiedades mostradas dependen del servicio.

Tabla 3-6 Información mostrada en la ficha Productos de SaaS

Propiedad	Muestra esta información...
Nombre del producto	Nombre del servicio de protección de McAfee SaaS.
Versión del producto	Número de la versión del producto.
Versión del motor del producto	Número del motor del producto. Sólo se muestra si es aplicable al producto y la información está disponible en la cuenta de SecurityCenter.
Versión del archivo DAT del producto	Número de versión del archivo de definición de amenazas (DAT) actualmente en uso. Sólo se muestra si es aplicable al producto y la información está disponible en la cuenta de SecurityCenter.
Fecha/hora del archivo DAT del producto	Fecha y hora en que se creó el archivo DAT. Sólo se muestra si es aplicable al producto y la información está disponible en la cuenta de SecurityCenter.

Registro de eventos de amenazas

Los eventos detectados en los sistemas gestionados protegidos por los servicios de McAfee SaaS aparecen en el Registro de eventos de amenazas de McAfee.

Acceda al Registro de eventos de amenazas haciendo clic en **Menú** | **Informes** | **Registro de eventos de amenazas** en la consola de ePolicy Orchestrator para ver detalles relativos a estos eventos y sus soluciones.

- Detecciones de virus y spyware
- Eventos entrantes bloqueados por el servicio de firewall
- eventos de filtrado web

La fecha y la hora mostradas indican la hora local del servidor de ePolicy Orchestrator en que se han producido los eventos. En cambio, la hora mostrada para los eventos en los informes de SecurityCenter es la hora local del sistema gestionado en el que se han producido los eventos.

Para obtener más información sobre el registro de eventos de amenazas, consulte la documentación de ePolicy Orchestrator.

Cuándo purgar los eventos de amenazas

A fin de evitar la aparición de datos duplicados u obsoletos en el registro de eventos de amenazas, recomendamos purgar manualmente los eventos de amenazas en estas situaciones:

- **Después de eliminar una cuenta de SecurityCenter registrada**: si elimina una cuenta registrada de la lista de servidores registrados de ePolicy Orchestrator, purgue los eventos de amenazas correspondientes a esa cuenta. (Si no tiene previsto volver a registrar la cuenta, puede conservar los eventos de amenazas como referencia.)
- **Antes de volver a instalar la extensión de Security-as-a-Service**: si ha instalado el software y sincronizado los datos de SaaS anteriormente, purgue los eventos de amenazas asociados.

Purga de eventos de amenazas

Al volver a instalar la extensión o registrar una cuenta de SecurityCenter que se ha registrado anteriormente, debe purgar el contenido del Registro de eventos de amenazas. Esto evita la aparición de datos antiguos o duplicados.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1. Haga clic en **Menú** | **Informes** | **Registro de eventos de amenazas**.
2. Haga clic en **Acciones** | **Purgar**.
3. En el cuadro de diálogo **Purgar** situado junto a **Purgar los registros con más de**, escriba un número y seleccione una unidad de tiempo.
4. Haga clic en **Aceptar**.

Los registros con una antigüedad mayor a la especificada se eliminan de forma permanente.

Apertura de SecurityCenter

Utilice la consola de SecurityCenter para solucionar problemas relacionados con los servicios de protección de McAfee SaaS. Acceda a la consola de SecurityCenter directamente desde la consola de ePolicy Orchestrator utilizando un monitor de panel que aparece en el panel de **Security-as-a-Service**.

> **Antes de empezar**
>
> Debe registrar la cuenta de SecurityCenter con el software ePolicy Orchestrator.

Para obtener más información sobre la utilización de las funciones de SecurityCenter, consulte la documentación de McAfee SaaS Endpoint Protection, disponible en la página **Ayuda y asistencia** de la consola de SecurityCenter.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1 Haga clic en **Menú** | **Informes** | **Paneles**.

2 En la lista **Paneles**, seleccione **Security-as-a-Service**.

3 En el monitor de **McAfee SecurityCenter**, seleccione uno de estos vínculos para abrir una ventana del navegador web y mostrar la consola de SecurityCenter:

- **Directivas**: abre la página **Directiva**, en la que puede editar directivas existentes o crear otras nuevas para los sistemas gestionados de McAfee SaaS.
- **Instalar protección**: abre la página **Instalar protección**, en la que puede instalar los servicios de protección de McAfee SaaS en equipos cliente.

Si dispone de varias cuentas de SecurityCenter, se muestran vínculos para todas ellas. Identifique la cuenta por el nombre especificado durante el registro.

Véase también

Registro de una cuenta de SecurityCenter en la página 17

Compatibilidad con otros productos de McAfee

La extensión es compatible con otros productos de McAfee presentes en el entorno de ePolicy Orchestrator.

Sin embargo, se requieren pasos de configuración adicionales cuando se utiliza con McAfee® Risk Advisor.

Consideraciones al utilizar McAfee Risk Advisor

Los análisis realizados por McAfee Risk Advisor, que analiza los sistemas gestionados e identifica vulnerabilidades, se deben configurar de una forma concreta cuando se ejecutan en un entorno de ePolicy Orchestrator que incluya sistemas gestionados de McAfee SaaS.

McAfee Risk Advisor extrae datos de amenazas actualizados de McAfee® Labs y después analiza los datos almacenados en la base de datos de ePolicy Orchestrator e identifica las vulnerabilidades de los sistemas gestionados.

En el caso de sistemas gestionados de McAfee SaaS, sólo se extrae de la cuenta de SecurityCenter un subconjunto de datos relevantes para calcular los riesgos que, seguidamente, se sincroniza con la base de datos de ePolicy Orchestrator. Por consiguiente, McAfee Risk Advisor no puede evaluar de forma precisa las vulnerabilidades de estos sistemas.

Para identificar con más precisión las vulnerabilidades en sistemas que no utilicen los servicios de McAfee SaaS, le recomendamos que excluya de los análisis los puntos de sincronización de Security-as-a-Service siguiendo uno de estos métodos:

- Seleccione manualmente todos los sistemas gestionados de McAfee SaaS en el árbol de sistemas y desactive su análisis.
- Cree una consulta de ePolicy Orchestrator para identificar los sistemas gestionados de McAfee SaaS y una tarea servidor para desactivar el análisis de estos sistemas.

Exclusión manualmente de sistemas gestionados de SaaS

Excluya manualmente sistemas gestionados de McAfee SaaS de los análisis que realiza McAfee Risk Advisor seleccionando los sistemas en el árbol de sistemas y desactivando su análisis.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1. Haga clic en **Menú** | **Sistemas** | **Árbol de sistemas**.
2. En el árbol de sistemas, seleccione el punto de sincronización que contiene los sistemas gestionados de McAfee SaaS.
3. En el panel derecho, haga clic en la ficha **Sistemas** y, a continuación, seleccione los sistemas que desea excluir.
4. Haga clic en **Acciones** | **Risk Advisor** | **Cambiar estado de análisis**.
5. Seleccione **Desactivar** y, a continuación, haga clic en **Aceptar**.
6. Compruebe el cambio.
   a. Haga clic en **Menú** | **Sistemas** | **Árbol de sistemas**.
   b. En el panel derecho, haga clic en la ficha **Sistemas** y, a continuación, en un nombre de equipo.
   c. En la página **Información del sistema**, haga clic en la ficha **Risk Advisor** y asegúrese de que **Estado de análisis** está **Desactivado**.

Exclusión de sistemas gestionados de SaaS con una tarea servidor

Para automatizar el proceso de exclusión de sistemas gestionados de McAfee SaaS de los análisis que realiza McAfee Risk Advisor, cree una consulta de ePolicy Orchestrator que identifique los sistemas gestionados de SaaS y una tarea servidor que desactive el análisis de esos sistemas.

La extensión agrega un tipo de administración, **Security-as-a-Service**, a la función de generación de informes de ePolicy Orchestrator. Este tipo de administración hace posible que las consultas localicen sistemas gestionados de SaaS automáticamente.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

1. Cree una consulta que identifique y seleccione todos los sistemas gestionados de McAfee SaaS.
   a. Haga clic en **Menú** | **Informes** | **Consultas e informes**.
   b. Haga clic en la ficha **Consulta** y, a continuación, haga clic en **Nueva**.
   c. Seleccione las opciones de la consulta.

En esta ficha...	Haga lo siguiente...
Tipo de resultado	1 En el panel **Grupo de funciones**, seleccione **Administración de sistemas**. 2 En el panel **Tipos de resultados**, haga clic en **Sistemas gestionados** y, a continuación, en **Siguiente**.
Gráfico	1 En el panel **Mostrar resultados como**, seleccione **Tabla**. 2 En el panel derecho, seleccione **Propiedades del equipo** | **Tipo de administración** en la lista **Ordenar por** y, a continuación, haga clic en **Siguiente**.
Columnas	• En el panel **Columnas disponibles**, en **Propiedades del equipo**, agregue el campo **Tipo de administración** y haga clic en **Siguiente**.
Filtros	1 En el panel **Propiedades disponibles** de **Propiedades del equipo**, agregue el campo **Tipo de administración**. 2 En el panel derecho, seleccione **Tipo de administración** | **Igual a** | **Security-as-a-Service** y, a continuación, haga clic en **Guardar**.

d Escriba un nombre para la consulta, especifique un grupo de consultas nuevo o existente y haga clic en **Guardar**.

2 Cree una tarea servidor que desactive el análisis de esos sistemas.

a Haga clic en **Menú** | **Automatización** | **Tareas servidor**.

b Haga clic en **Nueva tarea**.

c Escriba un nombre para la tarea, seleccione un estado de planificación de **Activado** y haga clic en **Siguiente**.

d En el menú **Acciones**, seleccione **Ejecutar consulta**.

e En el campo de consulta, haga clic en el icono de exploración, seleccione en la lista la consulta creada en el paso 1 y haga clic en **Aceptar**.

f En el campo **Subacciones**, haga clic en el icono de exploración, seleccione **Habilitar o deshabilitar amenaza(s) o activo(s)** en la lista y haga clic en **Aceptar**.

g En **Estado de análisis**, seleccione **Desactivar** y haga clic en **Siguiente**.

h Seleccione las opciones de planificación y haga clic en **Siguiente**.

i Haga clic en **Guardar**.

3 Ejecute la tarea servidor manualmente o espere a que se ejecute conforme a lo planificado.

La tarea servidor identifica cada uno de los sistemas gestionados de SaaS y establece su **Estado de análisis** como **Desactivado**. Estos sistemas no se incluirán en los análisis realizados por McAfee Risk Advisor.

4 Compruebe los resultados de la tarea servidor.

a Haga clic en **Menú** | **Sistemas** | **Árbol de sistemas**.

b En el panel derecho, haga clic en la ficha **Sistemas** y, a continuación, en un nombre de equipo.

c En la página **Información del sistema**, haga clic en la ficha **Risk Advisor** y compruebe que **Estado de análisis** esté **Desactivado**.

4 Solución de problemas

Estos temas proporcionan información adicional relacionada con la instalación y el uso de la extensión.

Contenido

Solución de problemas

Aquí tiene soluciones a problemas habituales.

Instalación de la extensión

La extensión no aparece en el Administrador de descargas de software del servidor de ePolicy Orchestrator

Descargue una copia de la extensión desde la consola de SecurityCenter. El vínculo está disponible en la ficha **Servidores de ePO** de la página **Utilidades**.

Volver a instalar la extensión después de haberla instalado y desinstalado

No todos los elementos asociados a la extensión se eliminan durante el proceso de desinstalación. Antes de volver a instalar la extensión, debe eliminar manualmente el panel de **Security-as-a-Service**, las consultas de **Security-as-a-Service**, la tarea servidor de sincronización de datos de SaaS predeterminada y los eventos de amenazas.

Conexión a SecurityCenter

No es posible crear un servidor registrado desde la consola de ePolicy Orchestrator

Realice una o varias de las siguientes acciones:

- **Compruebe que puede acceder a la consola de SecurityCenter desde el servidor de ePolicy Orchestrator.** En el equipo donde se esté ejecutando el servidor, abra una ventana del navegador, introduzca la dirección URL para acceder a SecurityCenter e intente realizar la conexión.
- **Compruebe que sus credenciales de SecurityCenter son correctas.** Abra una nueva ficha en el mismo navegador o abra una nueva ventana del navegador, introduzca sus credenciales e intente iniciar sesión.
- **Compruebe si el servidor de ePolicy Orchestrator aparece en la lista de servidores registrados de la consola de SecurityCenter.** En la página **Utilidades**, haga clic en la ficha **Servidores de ePO** y compruebe la lista **Servidores de ePolicy Orchestrator registrados**. Si la cuenta aparece en la lista, no puede volver a registrarla. Si no aparece en la lista, póngase en contacto con el servicio de soporte técnico.

Registro de un servidor

Se registra una cuenta de SecurityCenter y aparece un mensaje de error indicando que ya está registrada

Anule el registro de la cuenta y, después, vuelva a registrarla. Si el problema persiste, póngase en contacto con el servicio de soporte técnica.

Sincronización de los datos de SaaS

No es posible ver los datos después de registrar una cuenta de SecurityCenter

Los datos no aparecen hasta que se ejecuta correctamente una tarea de extracción del servidor de sincronización de datos de SaaS.

- **Compruebe el registro de tareas servidor para ver si la tarea se ha ejecutado o completado.** Si la tarea está planificada para ejecutarse a una hora concreta, es posible que aún no se haya ejecutado. Si es la primera vez que se ejecuta, podría durar algún tiempo debido a que extrae los datos de los últimos 30 días.
- **Espere tres minutos una vez completada la sincronización de datos, o bien actualice cada monitor de forma manual.** Haga clic en el icono del triángulo situado en la esquina superior izquierda de cada monitor y seleccione **Actualizar** en el menú.
- **Compruebe si la información aparece en los widgets de la página Panel de la consola de SecurityCenter.** Si ha configurado recientemente la cuenta de SecurityCenter y la información aún no ha tenido tiempo de aparecer en los widgets, no es posible sincronizarla con el software ePolicy Orchestrator. Si ha pasado tiempo suficiente y la información sigue sin aparecer en los widgets, entonces hay algún problema con la cuenta de SecurityCenter. Para obtener más información, consulte la documentación de McAfee SaaS Endpoint Protection, disponible en la ficha **Ayuda y asistencia** de la consola de SecurityCenter.

Se crea un punto de sincronización utilizando una cuenta de SecurityCenter que ya se ha registrado y sincronizado

La modificación del punto de sincronización para una cuenta registrada no hace que los monitores muestren automáticamente la información del nuevo punto de sincronización. Si modifica el punto de sincronización, realice una de las siguientes acciones:

- Cambie el nombre del punto de sincronización existente.
- Elimine los equipos gestionados de McAfee SaaS del punto de sincronización existente antes de configurar el nuevo punto de sincronización.

Aparecen datos duplicados de los sistemas gestionados de SaaS

Los datos duplicados pueden deberse a estas situaciones:

- **Ha eliminado una cuenta de SecurityCenter registrada y no eliminó manualmente el punto de sincronización asociado.** Elimine el punto de sincronización de la cuenta eliminada y, después, ejecute de nuevo la tarea de sincronización de datos de SaaS.
- **Ha eliminado una cuenta de SecurityCenter registrada y no ha eliminado manualmente los eventos de amenazas.** Esto ha provocado que los eventos de amenazas obsoletos del registro anterior hayan sido extraídos durante la sincronización de datos. Purgue los eventos de amenazas de la cuenta y, después, ejecute de nuevo la tarea de sincronización de datos.
- **Ha desinstalado y vuelto a instalar la extensión y no ha eliminado manualmente los eventos de amenazas.** Esto ha provocado que los eventos de amenazas obsoletos de la instalación anterior hayan sido extraídos durante la sincronización de datos. Purgue los eventos de amenazas de la cuenta y, después, ejecute de nuevo la tarea de sincronización de datos.

Se elimina un punto de sincronización y después se lo vuelve a crear

Si elimina un punto de sincronización existente, su tarea servidor asociada deja de ejecutarse. Si vuelve a crear el punto de sincronización, debe configurar su tarea servidor o bien una nueva tarea servidor que sincronice los datos. Volver a crear el punto de sincronización no hace que la tarea servidor asociada a la instancia anterior del punto de sincronización empiece automáticamente a sincronizar datos para la nueva instancia del punto de sincronización.

Los datos no se actualizan

Realice una o todas las acciones siguientes:

- En la consola de ePolicy Orchestrator, compruebe el estado de la tarea servidor de sincronización de datos de SaaS en el Registro de tareas servidor (haga clic en **Menú** | **Automatización** | **Registro de tareas servidor**).
- En la consola de SecurityCenter, observe el estado de sincronización (en la página **Utilidades**, haga clic en la ficha **Servidores de ePO** y, a continuación, observe la lista **Servidores de ePolicy Orchestrator [McAfee ePO]**).
- Si la tarea servidor de sincronización de datos de SaaS sigue sin funcionar, póngase en contacto con el servicio de soporte técnico (en la consola de SecurityCenter, haga clic en la ficha **Ayuda y asistencia** y, a continuación, en **Obtener soporte**).

Se ha anidado un punto de sincronización dentro de otro en el árbol de sistemas y el punto anidado ya no aparece

Cuando se sincronizan los datos para el punto de sincronización principal, todos los puntos de sincronización anidados dentro de él se eliminan (ya que esos sistemas no existen realmente en la misma cuenta registrada). Vuelva a crear el punto de sincronización eliminado en el nivel raíz del árbol de sistemas, vincúlelo a una tarea servidor de sincronización de datos de SaaS y ejecute esa tarea servidor para rellenar el punto de sincronización de sustitución con los sistemas gestionados de SaaS.

No aparecen todos los sistemas en el árbol de sistemas

Dentro de un único grupo de sistemas gestionados, sólo se puede sincronizar una instancia de un nombre de sistema. Si tiene varios sistemas que utilizan el mismo nombre dentro del mismo grupo, debe cambiarles el nombre por uno que sea exclusivo.

Visualización de datos con los monitores de panel

Se han sincronizado los datos, pero no aparecen en ningún monitor de panel de Security-as-a-Service

Cuando se completa la sincronización, la información de los monitores de panel se actualiza automáticamente después de tres minutos. Para ver los datos de forma inmediata, haga clic en el icono del triángulo situado en la esquina superior izquierda de cada monitor y seleccione **Actualizar** en el menú.

Hacer clic en el icono **Actualizar** situado en la esquina superior derecha de la consola no actualiza los monitores en este caso concreto.

Se han sincronizado los datos, pero la información que aparece en los monitores de Security-as-a-Service no coincide con lo que aparece en los widgets de SecurityCenter

La información que aparece en los monitores debe coincidir o ser muy similar a la que aparece en los widgets correspondientes de la página **Panel** de la consola de SecurityCenter. Si la información aparece en los widgets y no en los monitores, es posible que haya un problema con la configuración o la sincronización de la extensión. Póngase en contacto con el servicio de soporte técnico.

Se han sincronizado los datos, pero no aparecen en los monitores Principales equipos con detecciones o Principales equipos con sitios bloqueados

- Durante el periodo de tiempo especificado por el monitor, no se ha producido ninguna detección relevante.

  La cuenta de SecurityCenter no tiene que estar activa durante los 7 o 30 días completos para que aparezcan datos en un monitor. Los datos de la cuenta están disponibles para el número de días que haya estado activa la cuenta.

- La sincronización de datos no se ha completado correctamente o aún no se ha producido. Compruebe el estado en el Registro de tareas servidor (en la consola de ePolicy Orchestrator, haga clic en **Menú** | **Automatización** | **Registro de tareas servidor**).
- No han pasado tres minutos desde que se produjo la sincronización. Espere a que los monitores se actualicen automáticamente tras tres minutos, o actualice cada uno de ellos manualmente (haga clic en el icono del triángulo situado en la esquina superior izquierda de cada monitor y seleccione **Actualizar** en el menú).

Se han sincronizado los datos, pero no aparecen todos los datos de eventos de amenazas

Si los eventos de amenazas no aparecen en SecurityCenter después de ejecutar una tarea de sincronización de datos de SaaS, esto significa que la cantidad de información presente en la cuenta supera la cantidad máxima que se puede extraer durante una única ejecución de la tarea. Planifique la tarea para que se ejecute varias veces al día con el fin de asegurarse de que todos los eventos de amenazas se extraigan de SecurityCenter.

Realización de análisis de riesgos

Un análisis de riesgos de McAfee Risk Advisor indica que los sistemas gestionados de McAfee SaaS están en peligro

Sólo un subconjunto de información relevante para calcular los riesgos se extrae de la cuenta de SecurityCenter y se sincroniza con la base de datos de ePolicy Orchestrator. Por consiguiente, el análisis no puede evaluar de forma precisa las vulnerabilidades de estos sistemas. Para obtener resultados más precisos, le recomendamos que excluya de los análisis los sistemas gestionados de McAfee SaaS. Puede hacerlo manualmente en el árbol de sistemas, o bien crear una consulta y una tarea servidor que identifiquen y excluyan estos sistemas de forma automática.

Véase también

Exclusión manualmente de sistemas gestionados de SaaS en la página 37
Exclusión de sistemas gestionados de SaaS con una tarea servidor en la página 37
Eliminación de datos manualmente en la página 43
Purga de eventos de amenazas en la página 35

Eliminación manual de archivos y eventos

Algunos archivos no se eliminan automáticamente al quitar la extensión o sus componentes del entorno de ePolicy Orchestrator.

Debe eliminar los datos de forma manual en estas situaciones.

- **Después de eliminar una cuenta de SecurityCenter registrada.**
  - Elimine el grupo contenedor del árbol de sistemas donde estuvieran situados los grupos y sistemas sincronizados. (El grupo contenedor del árbol de sistemas deja de estar configurado como punto de sincronización, pero sigue conteniendo los grupos y los sistemas sincronizados anteriormente con la cuenta eliminada.)
  - Purgue los eventos de amenazas. (Si no tiene previsto volver a registrar la cuenta, puede conservar los eventos de amenazas como referencia.)

- **Antes de volver a instalar la extensión.**
  - Elimine estos elementos manualmente antes de volver a instalar la extensión:
    - La tarea **Sincronización de datos de SaaS** predeterminada.
    - El panel de **Security-as-a-Service**.
    - Las consultas de **Security-as-a-Service**.
    - Eventos de amenazas.
  - No elimine estos elementos. Se actualizan automáticamente durante la sincronización de datos de SaaS inicial correspondiente a la nueva instalación:
    - Las cuentas de SecurityCenter registradas.
    - Los equipos y los grupos sincronizados anteriormente con SecurityCenter.
  - No elimine estos elementos. Pueden volver a utilizarse o configurarse para la nueva instalación:
    - Las tareas de sincronización de datos de SaaS planificadas.

Eliminación de datos manualmente

Elimine o purgue los elementos que no se eliminen automáticamente al quitar la extensión o sus componentes del entorno de ePolicy Orchestrator.

Si tiene la intención de volver a instalar la extensión, sólo es necesario eliminar los eventos de amenazas y los puntos de sincronización.

Procedimiento

Para ver las definiciones de las opciones, haga clic en **?** en la interfaz.

- Elimine los elementos conforme sea necesario.

Para eliminar esto...	Siga estos pasos...
Eventos de amenazas	1 Haga clic en **Menú** | **Informes** | **Registro de eventos de amenazas**. 2 Haga clic en **Acciones** | **Purgar**. 3 En el cuadro de diálogo **Purgar** situado junto a **Purgar los registros con más de**, escriba un número y seleccione una unidad de tiempo. 4 Haga clic en **Aceptar**.
Puntos de sincronización	1 Haga clic en **Menú** | **Sistemas** | **Árbol de sistemas**. 2 En el panel **Árbol de sistemas**, seleccione el punto de sincronización. 3 Haga clic en **Acciones en los sistemas** | **Eliminar grupo**.
Panel predeterminado	1 Haga clic en **Menú** | **Informes** | **Paneles** y, a continuación, seleccione el panel que desea eliminar en la lista desplegable **Panel**. 2 En la lista **Paneles**, seleccione **Security-as-a-Service**. 3 Haga clic en **Acciones de paneles** | **Eliminar**. 4 Haga clic en **Aceptar**.

Para eliminar esto...	Siga estos pasos...
Tarea servidor predeterminada	1 Haga clic en **Menú** | **Automatización** | **Tareas servidor**. 2 Seleccione la tarea servidor **Sincronizar datos de SaaS** y, a continuación, haga clic en **Acciones** | **Eliminar**. 3 Haga clic en **Aceptar**.
Consultas	1 Haga clic en **Menú** | **Informes** | **Consultas e informes**. 2 Seleccione la consulta que desea eliminar y, a continuación, haga clic en **Acciones** | **Eliminar**. 3 Haga clic en **Sí**.

Véase también

Instalación de la extensión de producto en la página 14

Búsqueda de más información

Acceda a documentación adicional para obtener más información sobre el uso del software.

Procedimiento

- Realice cualquiera de las acciones que se indican a continuación.

Producto	Cómo acceder a documentación
Software ePolicy Orchestrator	Desde la consola de ePolicy Orchestrator: • Ver la ayuda online: Haga clic en el icono **?** situado en la esquina superior derecha de cualquier página. • Descargar la guía del usuario o las notas de la versión: **1** Haga clic en **Menú** | **Software** | **Administrador de software** | **Extensiones**. **2** En el panel **Categorías de productos**, haga clic en **Soluciones de administración**. **3** En el panel derecho, en **Software**, haga clic en **McAfee ePolicy Orchestrator**. **4** En el panel inferior derecho, localice el documento en la columna **Componente** y haga clic en **Descargar** en la columna **Acciones**. **5** En el cuadro de diálogo **Descarga de archivos**, guarde el archivo de documento en una carpeta local y haga clic en **Aceptar**.
Extensión de Security-as-a-Service	Desde la consola de ePolicy Orchestrator: • Ver la ayuda online: Haga clic en el icono **?** situado en la esquina superior derecha de cualquier página que incluya contenido específico de la extensión. • Descargar la guía del usuario o las notas de la versión: **1** Haga clic en **Menú** | **Software** | **Administrador de software** | **Extensiones**. **2** En el panel **Categorías de productos**, haga clic en **Soluciones de administración**. **3** En el panel derecho, en **Software**, haga clic en **McAfee SaaS <número de versión>**. **4** En el panel inferior derecho, localice el documento en la columna **Componente** y haga clic en **Descargar** en la columna **Acciones**. **5** En el cuadro de diálogo **Descarga de archivos**, guarde el archivo de documento en una carpeta local y haga clic en **Aceptar**.
Servicios de SecurityCenter, McAfee SaaS Endpoint Protection y McAfee SaaS	Desde la consola de SecurityCenter: • Ver la ayuda online: Haga clic en el icono **?** situado en la esquina superior derecha de cualquier página. • Ver la guía del producto o la guía de instalación de McAfee SaaS Endpoint Protection en formato PDF: Haga clic en la ficha **Ayuda y asistencia** y, a continuación, seleccione el vínculo de un documento. • Ver una guía de inicio rápido o de solución de problemas de la extensión: Seleccione uno de los enlaces de la ficha **Servidores de ePO** de la página **Utilidades**. • Ver documentación adicional de un servicio específico de McAfee SaaS: consulte el capítulo correspondiente de la guía del producto para obtener instrucciones. Por lo general, haga clic en un vínculo en el widget asociado al servicio para abrir el portal de administración de SaaS asociado y, después, haga clic en el vínculo **Ayuda** en el portal.

Índice

T

V