FMC 6.6.1+: consejos para la actualización antes y después

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Principales cosas que hacer antes de la actualización de FMC
Elija la versión de software de destino de FMC
Verifique el modelo FMC actual y la versión de software
Planificación de la ruta de actualización
Cargar paquetes de actualización
Creación de la copia de seguridad de FMC
Verificación de la Sincronización NTP
Verificar el espacio en disco
Implementar todos los cambios de política pendientes
Ejecute las comprobaciones de idoneidad del software Firepower
Principales cosas que hacer después de la actualización de FMC
Implementar todos los cambios de política pendientes
Verifique si se ha instalado la última base de datos de vulnerabilidades y huella dactilar
Verificar la versión actual de la regla Snort y del paquete de seguridad ligero
Verificar la versión actual de actualización de geolocalización
Automatizar la actualización de la base de datos de filtrado de URL con la tarea programada
Configurar copias de seguridad periódicas
Asegúrese de que la licencia inteligente esté registrada
Revisar la configuración de los conjuntos de variables
Verificar la habilitación de servicios en la nube
Filtrado de URL
AMP para redes
Región de nube de Cisco
Configuración de eventos en la nube de Cisco
Habilitar integración de SecureX
Integración de la cinta de opciones SecureX
Enviar eventos de conexión a SecureX
Integración de terminales seguros (AMP para terminales)
Integración de análisis de malware seguro (Threat Grid)

Introducción

Este documento describe las prácticas recomendadas de verificación y configuración para completar antes y después de la actualización de Cisco Secure Firewall Management Center

(FMC) a la versión 6.6.1+.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Hardware Cisco FMC 1000
- Software: Versión 7.0.0 (compilación 94)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Principales cosas que hacer antes de la actualización de FMC

Elija la versión de software de destino de FMC

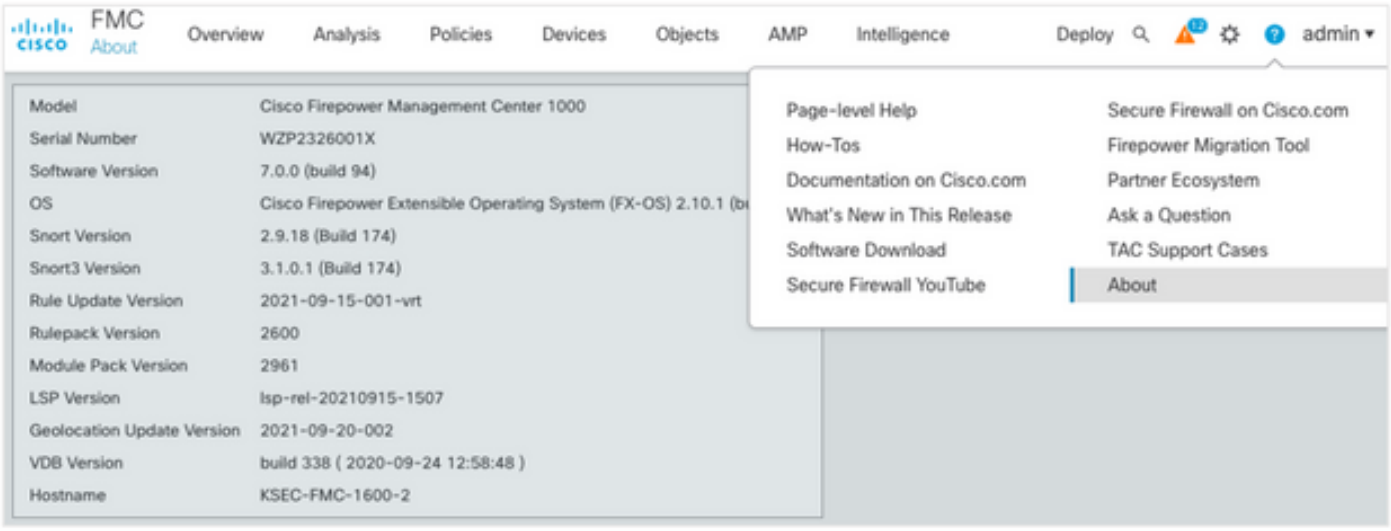
Revise las notas de la versión de Firepower para la versión de destino y conozca:

- Compatibilidad
- Funciones y funcionalidad
- Problemas resueltos
- Problemas conocidos

Verifique el modelo FMC actual y la versión de software

Verifique el modelo FMC actual y la versión de software:

1. Vaya a **Ayuda > Acerca de**.
2. Verifique la **versión de modelo** y **software**.



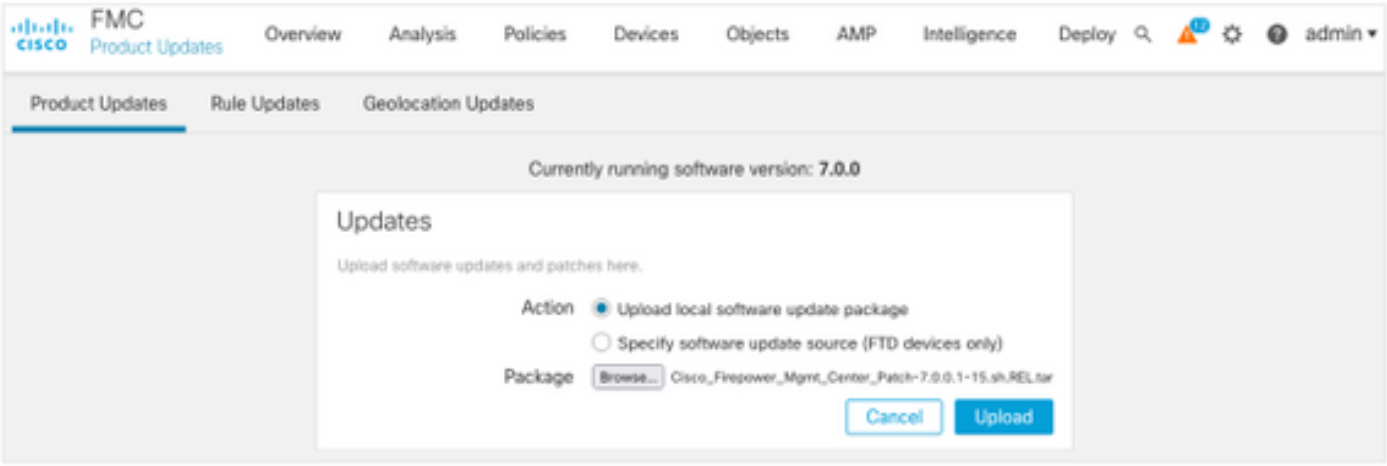
Planificación de la ruta de actualización

Sujeto a la versión de software FMC actual y de destino, puede que se requiera una actualización provisional. En la Guía de Actualización de Cisco Firepower Management Center, revise la **Trayectoria de Upgrade:** Sección **Firepower Management Centers** y planifique la ruta de actualización.

Cargar paquetes de actualización

Para cargar el paquete de actualización en el dispositivo, complete estos pasos:

1. Descargue el paquete de actualización desde la página Descarga de Software.
2. En el FMC navegue hasta **Sistema > Actualizaciones**.
3. Elija la **Cargar actualización**.
4. Haga clic en el botón de opción **Cargar paquete de actualización de software local**.
5. Haga clic en **Examinar** y elija el paquete.
6. Haga clic en **Cargar**.



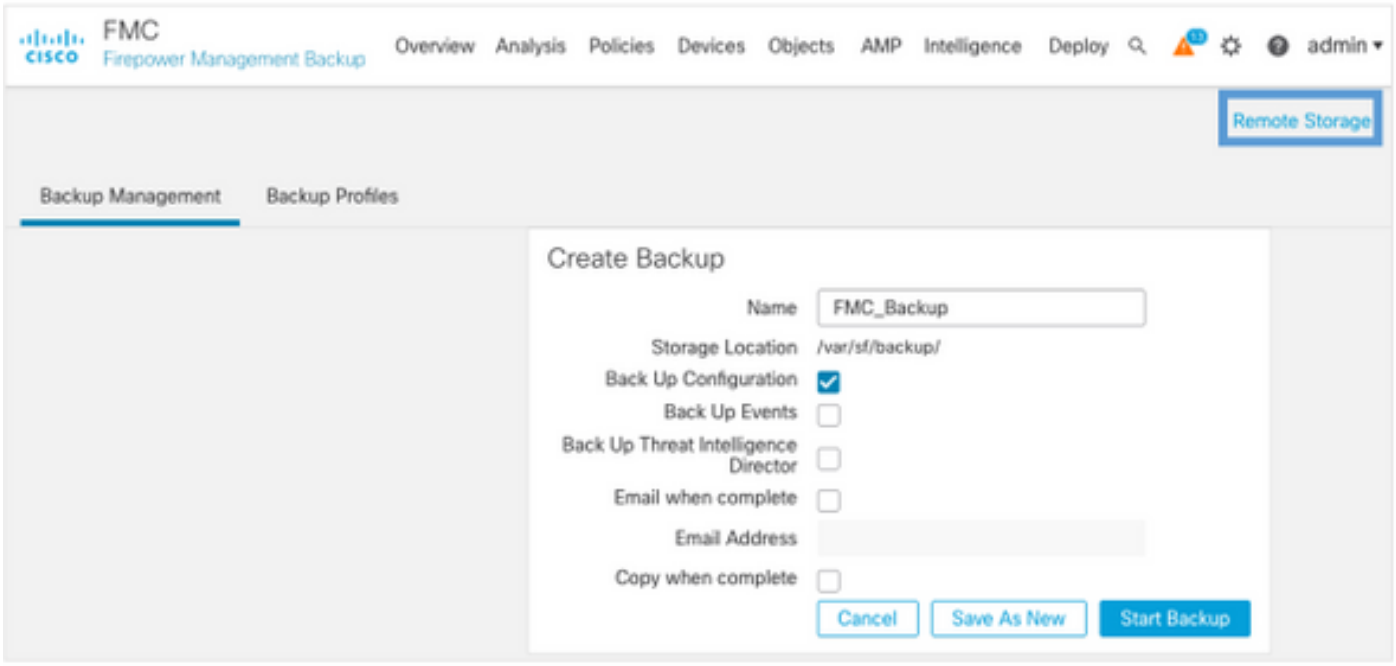
Creación de la copia de seguridad de FMC

La copia de seguridad es un paso importante en la recuperación ante desastres, que permite restaurar la configuración si una actualización falla catastróficamente.

1. Vaya a **System > Tools > Backup/Restore**.

2. Elija **Firepower Management Backup**.
3. En el campo **Name**, ingrese el nombre de la copia de seguridad.
4. Elija la ubicación de almacenamiento y la información que debe incluirse en la copia de seguridad.
5. Haga clic en **Iniciar copia de seguridad**.
6. En **Notification > Tasks**, supervise el progreso de creación de la copia de seguridad.

Consejo: Se recomienda encarecidamente realizar una copia de seguridad de una ubicación remota segura y verificar el éxito de la transferencia. El almacenamiento remoto se puede configurar desde la página Administración de copias de seguridad.



Para obtener más información, vea:

- Guía de Configuración de Firepower Management Center, Versión 7.0 - Capítulo: Copia de seguridad y restauración
- Guía de Configuración de Firepower Management Center, Versión 7.0 - Remote Storage Management

Verificación de la Sincronización NTP

Para una actualización correcta de FMC, se requiere sincronización NTP. Para verificar la sincronización NTP, complete estos pasos:

1. Vaya a **System > Configuration > Time**.
2. Verifique el **estado de NTP**.

Nota: Estado: "Se utiliza" indica que el dispositivo está sincronizado con el servidor NTP.

Current Setting Via NTP (based on System Configuration Time Synchronization)
Current Time 2021-09-21 13:50

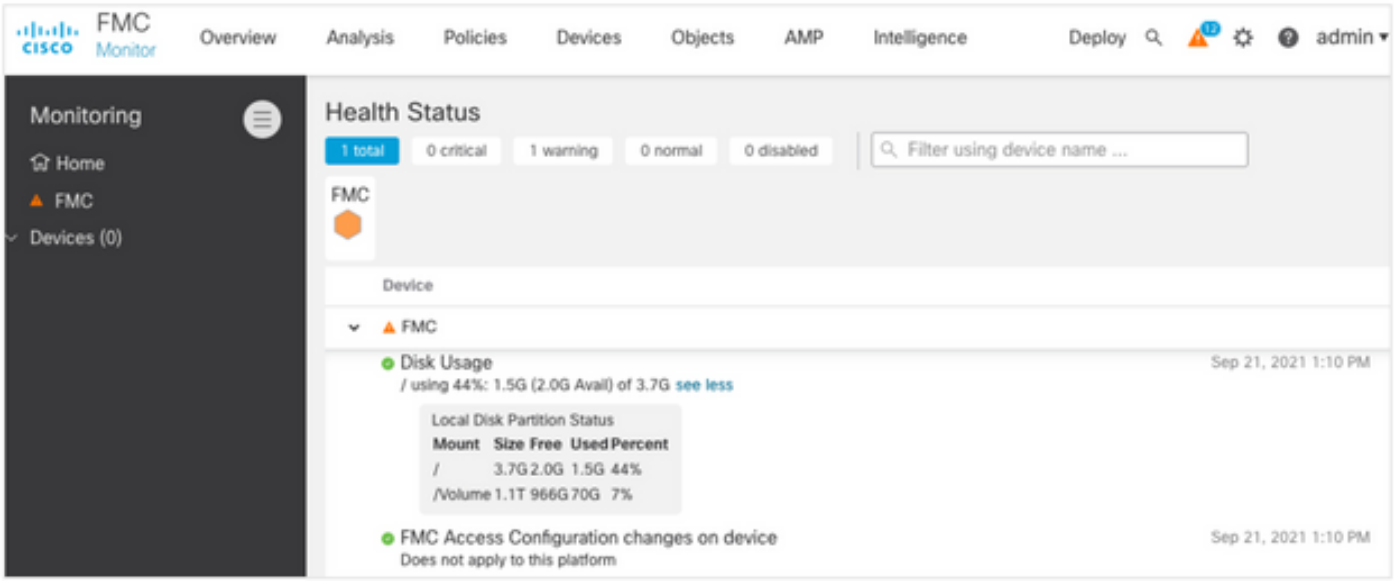
NTP Server	Status	Authentication	Offset	Last Update
173.38.201.115	Being Used	none	+0.011(milliseconds)	126(seconds)
173.38.201.67	Available	none	+0.042(milliseconds)	223(seconds)
127.127.1.1	Unknown	none	+0.000(milliseconds)	12d(seconds)

Para obtener más información, vea Firepower Management Center Configuration Guide, versión 7.0 - Sincronización de hora y hora.

Verificar el espacio en disco

Según el modelo FMC y la versión de destino, asegúrese de que haya suficiente espacio libre en disco disponible, de lo contrario la actualización falla. Para verificar el espacio disponible en disco de FMC, complete estos pasos:

1. Vaya a **System > Health > Monitor**.
2. Elija el FMC.
3. Expanda el menú y busque **Uso de disco**.
4. Los requisitos de espacio en disco se pueden encontrar en Pruebas de Tiempo y Requisitos de Espacio en Disco.

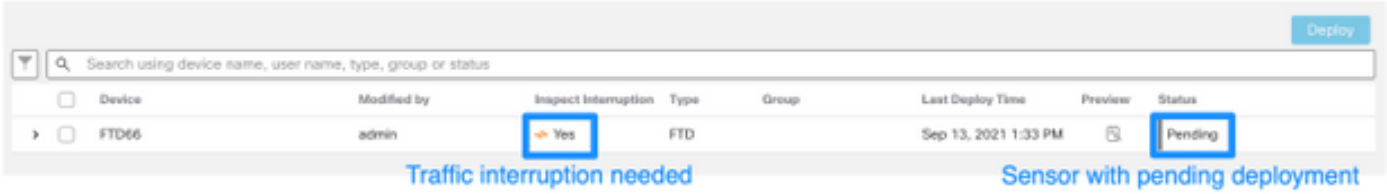


Implementar todos los cambios de política pendientes

Antes de la instalación de la actualización o del parche, es necesario implementar cambios en los sensores. Para asegurarse de que se implementan todos los cambios pendientes, complete estos pasos:

1. Navegue hasta **Implementar > Implementación**.
2. Elija todos los dispositivos de la lista e **implemente**.

Precaución: La columna Inspeccionar interrupción indica interrupción del tráfico

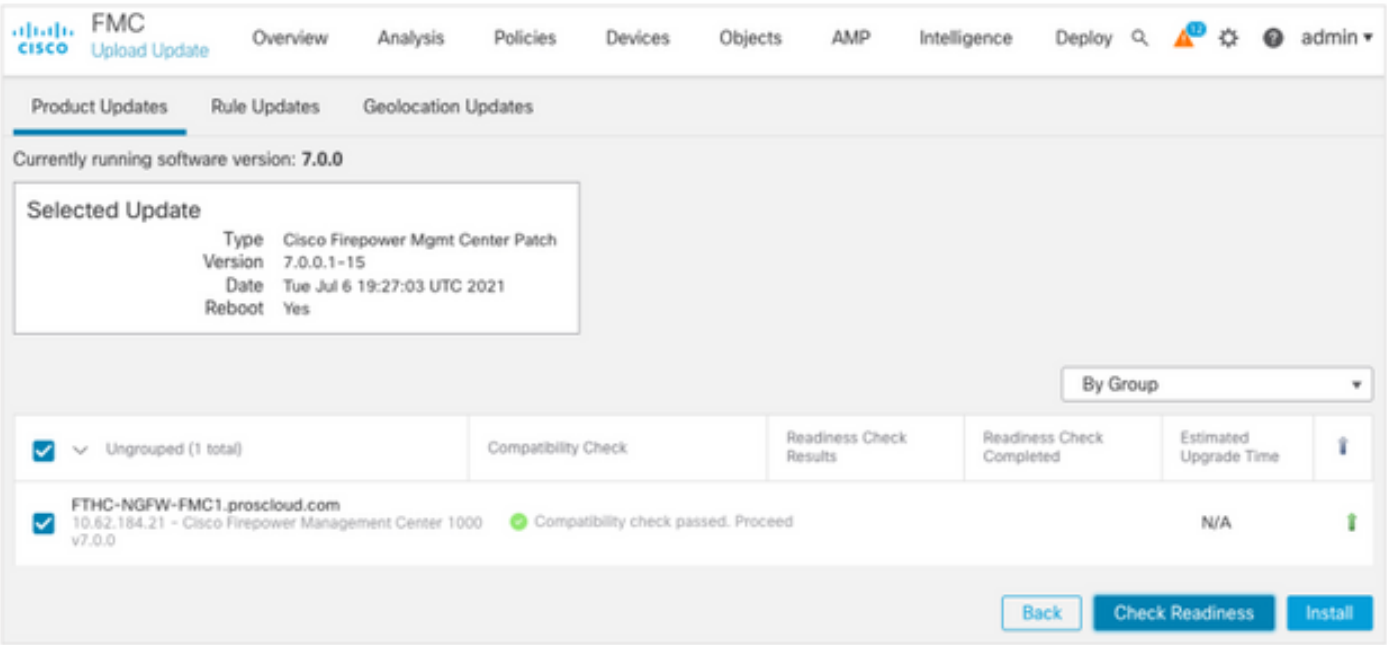


Ejecute las comprobaciones de idoneidad del software Firepower

Las comprobaciones de idoneidad evalúan la preparación de un dispositivo Firepower para una actualización de software.

Para realizar las Verificaciones de Preparación del Software, complete estos pasos:

1. Vaya a **Sistema > Actualizaciones**.
2. Seleccione el icono **Install** junto a la versión de destino.
3. Elija el FMC y haga clic en **Comprobar preparación**.
4. En la ventana emergente, haga clic en **Aceptar**.
5. Monitoree el proceso de Verificación de Preparación desde **Notifications > Tasks**.



Para obtener más información, consulte [Guía de actualización de Cisco Firepower Management Center - Verificaciones de preparación del software Firepower].

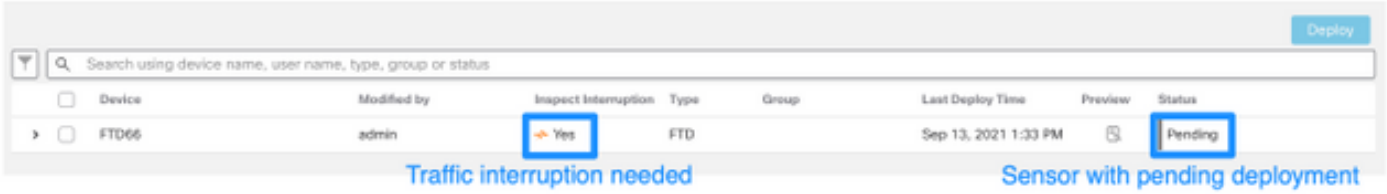
Principales cosas que hacer después de la actualización de FMC

Implementar todos los cambios de política pendientes

Inmediatamente después de cada actualización o instalación de parches, es necesario implementar cambios en los sensores. Para asegurarse de que se implementan todos los cambios pendientes, complete estos pasos:

1. Navegue hasta **Implementar > Implementación**.
2. Elija todos los dispositivos de la lista y haga clic en **Implementar**.

Precaución: La columna Inspeccionar interrupción indica interrupción del tráfico



Verifique si se ha instalado la última base de datos de vulnerabilidades y huella dactilar

Para verificar la versión actual de la huella dactilar (VDB), realice estos pasos:

1. Vaya a **Ayuda > Acerca de**.
2. Verifique la **versión de VDB**.

Para descargar las actualizaciones de VDB directamente desde cisco.com, se requiere disponibilidad de FMC a cisco.com.

1. Vaya a **Sistema > Actualizaciones > Actualizaciones de productos**.
2. Elija **Descargar actualizaciones**.
3. Instale la última versión disponible.
4. Debe volver a implementar los sensores después.

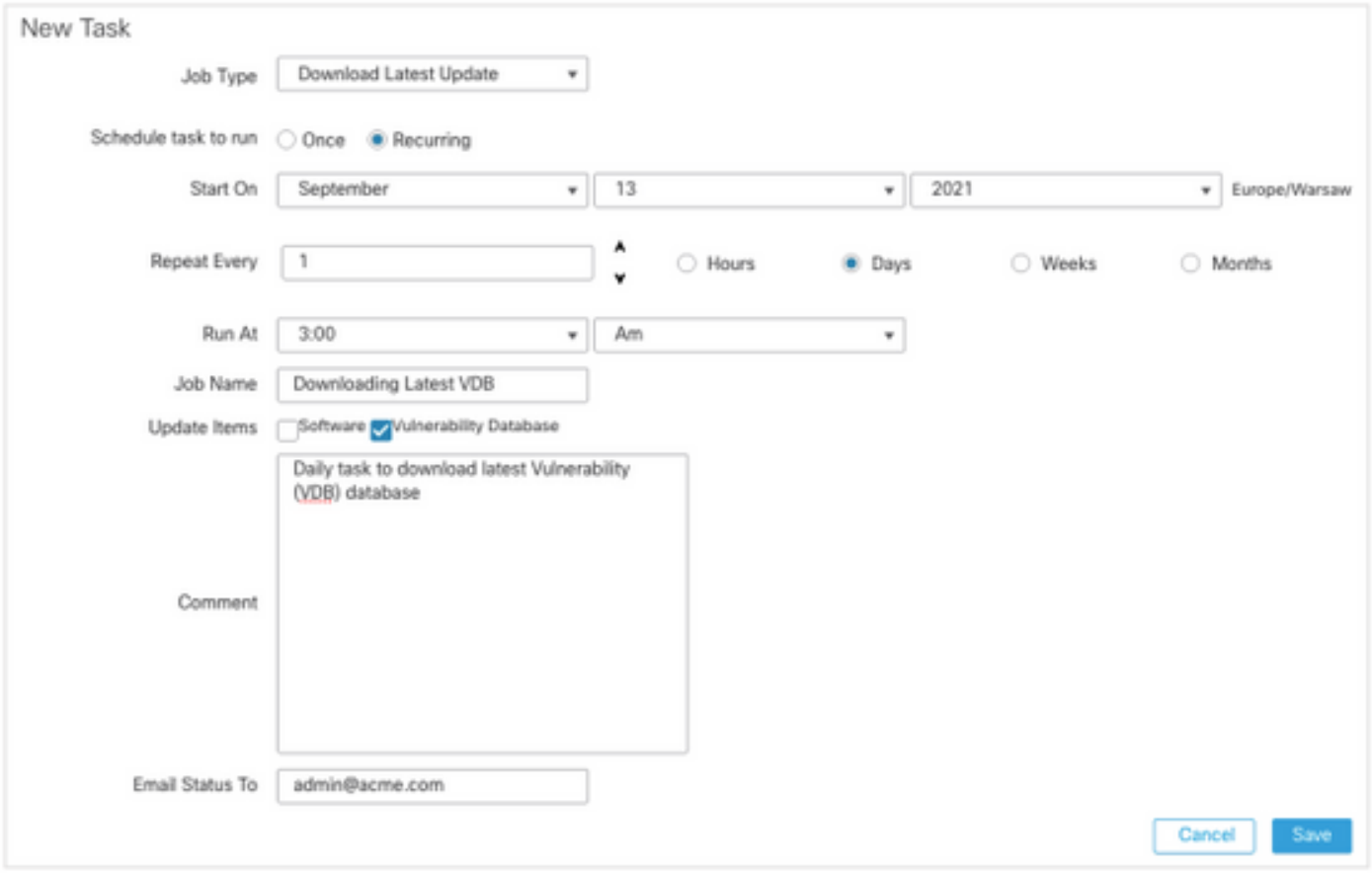
> **Nota:** Si FMC no tiene acceso a Internet, el paquete VDB se puede descargar directamente desde software.cisco.com.

Se recomienda programar tareas para realizar descargas e instalaciones automáticas de paquetes VDB.

Como buena práctica, verifique si VDB se actualiza diariamente e instálelas en el FMC durante los fines de semana.

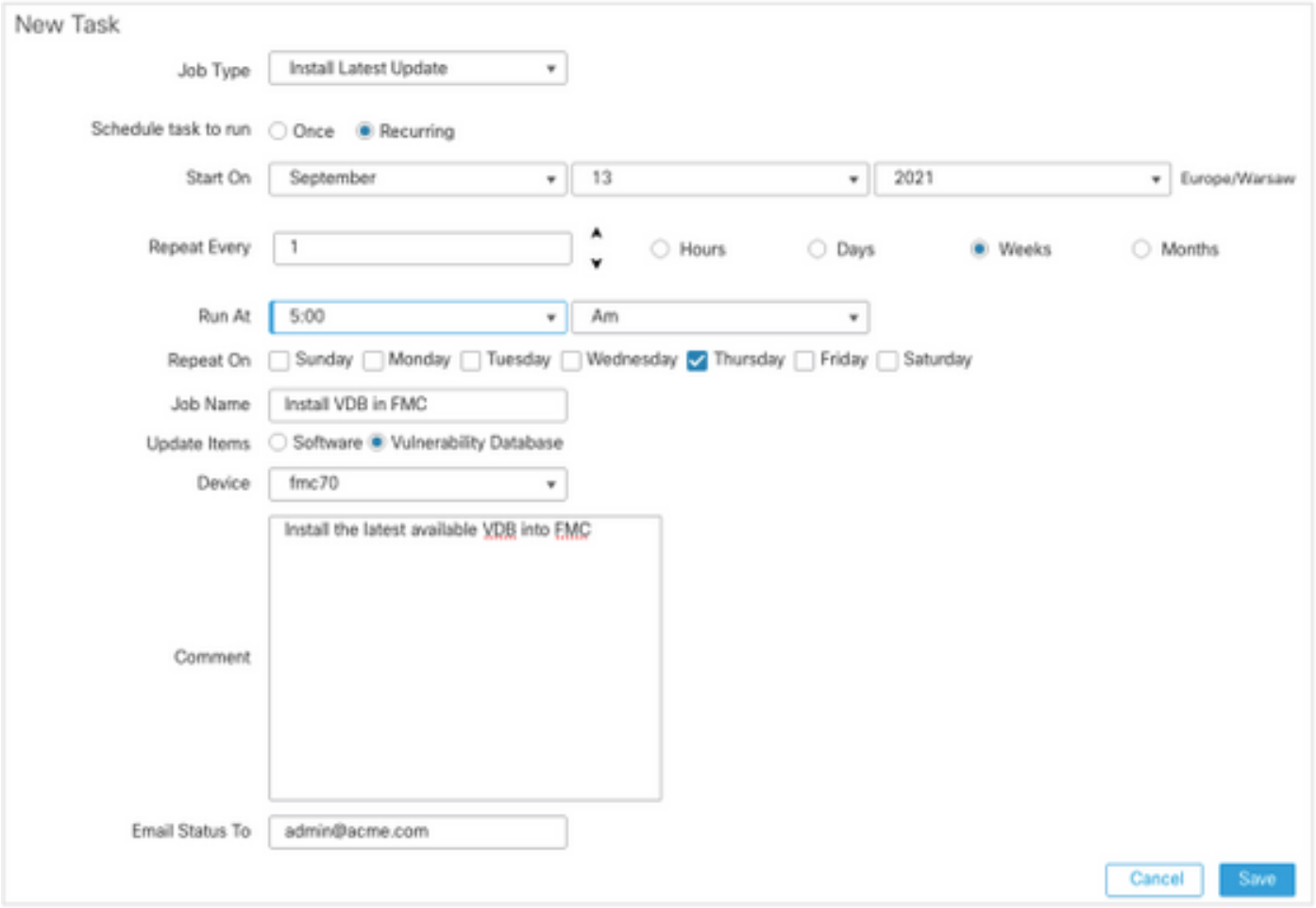
Para verificar el VDB diariamente desde www.cisco.com, complete estos pasos:

1. Vaya a **Sistema > Herramientas > Programación**.
2. Haga clic en **Agregar tarea**.
3. En la lista desplegable **Tipo de trabajo**, elija **Descargar última actualización.**
4. Para **ejecutar la tarea de programación**, haga clic en el botón de opción **Recurrente.**
5. Repita la tarea todos los días y ejecútela a las 3:00 AM o fuera del horario laboral.
6. Para **actualizar elementos**, marque la casilla de verificación **Base de datos de vulnerabilidades.**



Para instalar la última VDB en el FMC, configure la tarea periódica semanalmente:

1. Vaya a **Sistema > Herramientas > Programación**.
2. Haga clic en **Agregar tarea**.
3. En la lista desplegable **Tipo de trabajo**, elija **Instalar última actualización**.
4. Para **ejecutar la tarea de programación**, haga clic en el botón de opción **Recurrente**.
5. Repita la tarea cada 1 semana y ejecútela a las 5:00 AM o fuera del horario laboral.
6. Para **actualizar elementos**, active la **casilla de verificación Base de datos de vulnerabilidades.**



Para obtener más información, vea Firepower Management Center Configuration Guide, versión 7.0: actualización de la base de datos de vulnerabilidades (VDB)

Verificar la versión actual de la regla Snort y del paquete de seguridad ligero

Para verificar las versiones actuales de Regla de Snort (SRU), Paquete de seguridad ligero (LSP) y Geolocalización, complete estos pasos:

1. Vaya a **Ayuda > Acerca de**.
2. Verifique la **versión de actualización de reglas** y la **versión de LSP**.

Para descargar el SRU y el LSP directamente desde www.cisco.com, se requiere disponibilidad del FMC a www.cisco.com.

1. Vaya a **Sistema > Actualizaciones > Actualizaciones de reglas**.
2. En la pestaña **Actualización de reglas/Importación de reglas única**, elija **Descargar nueva actualización de reglas del sitio de soporte**.
3. Elija **Importar**.
4. Implemente la configuración en los sensores después.

Nota: Si FMC no tiene acceso a Internet, los paquetes SRU y LSP se pueden descargar directamente desde software.cisco.com.

Las actualizaciones de reglas de intrusión son acumulativas y se recomienda importar siempre la última actualización.

Para activar la descarga semanal y la implementación de las actualizaciones de reglas de sonda (SRU/LSP), complete estos pasos:

1. Vaya a **Sistema > Actualizaciones > Actualizaciones de reglas**.
2. En la ficha **Actualización periódica de importaciones de reglas**, active la **casilla de verificación Habilitar actualización periódica de reglas desde el sitio de soporte**.
3. Elija la frecuencia de importación como semanal, elija un día de la semana y tarde para la descarga e implementación de políticas.
4. Click **Save**.

Para obtener más información, vea Firepower Management Center Configuration Guide, versión 7.0 - Update Intrusion Rules.

Verificar la versión actual de actualización de geolocalización

Para verificar la versión actual de Geolocalización, complete estos pasos:

1. Vaya a **Ayuda > Acerca de**.
2. Verifique la **versión de actualización de geolocalización**.

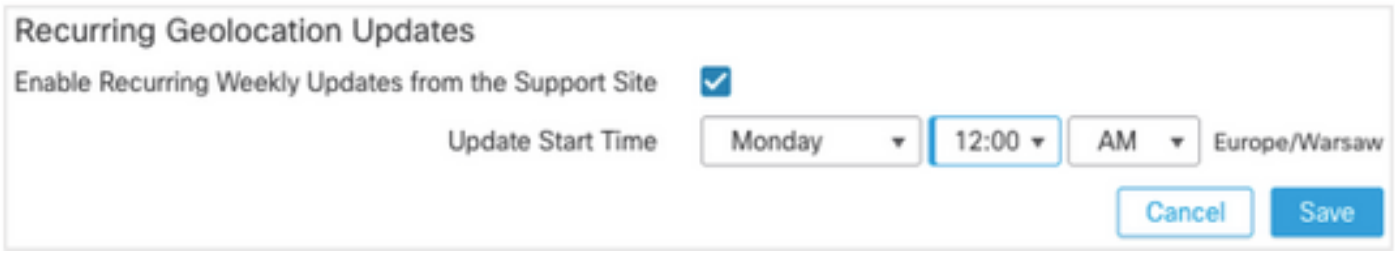
Para descargar las actualizaciones de geolocalización directamente desde www.cisco.com, se requiere disponibilidad desde el FMC a www.cisco.com.

1. Vaya a **Sistema > Actualizaciones > Actualizaciones de geolocalización**.
2. En la pestaña **Actualización de geolocalización única**, elija **Descargar e instalar actualización de geolocalización del sitio de soporte**.
3. Haga clic en **Importar**.

Nota: Si FMC no tiene acceso a Internet, el paquete de actualizaciones de geolocalización se puede descargar directamente desde software.cisco.com.

Para activar las Actualizaciones de geolocalización automáticas, complete estos pasos:

1. Vaya a **Sistema > Actualizaciones > Actualizaciones de geolocalización**.
2. En la sección Actualizaciones de geolocalización recurrentes, active la casilla de verificación **Habilitar actualizaciones semanales recurrentes desde el sitio de soporte**.
3. Elija la frecuencia de importación como semanal, elija Lunes a medianoche.
4. Click **Save**.

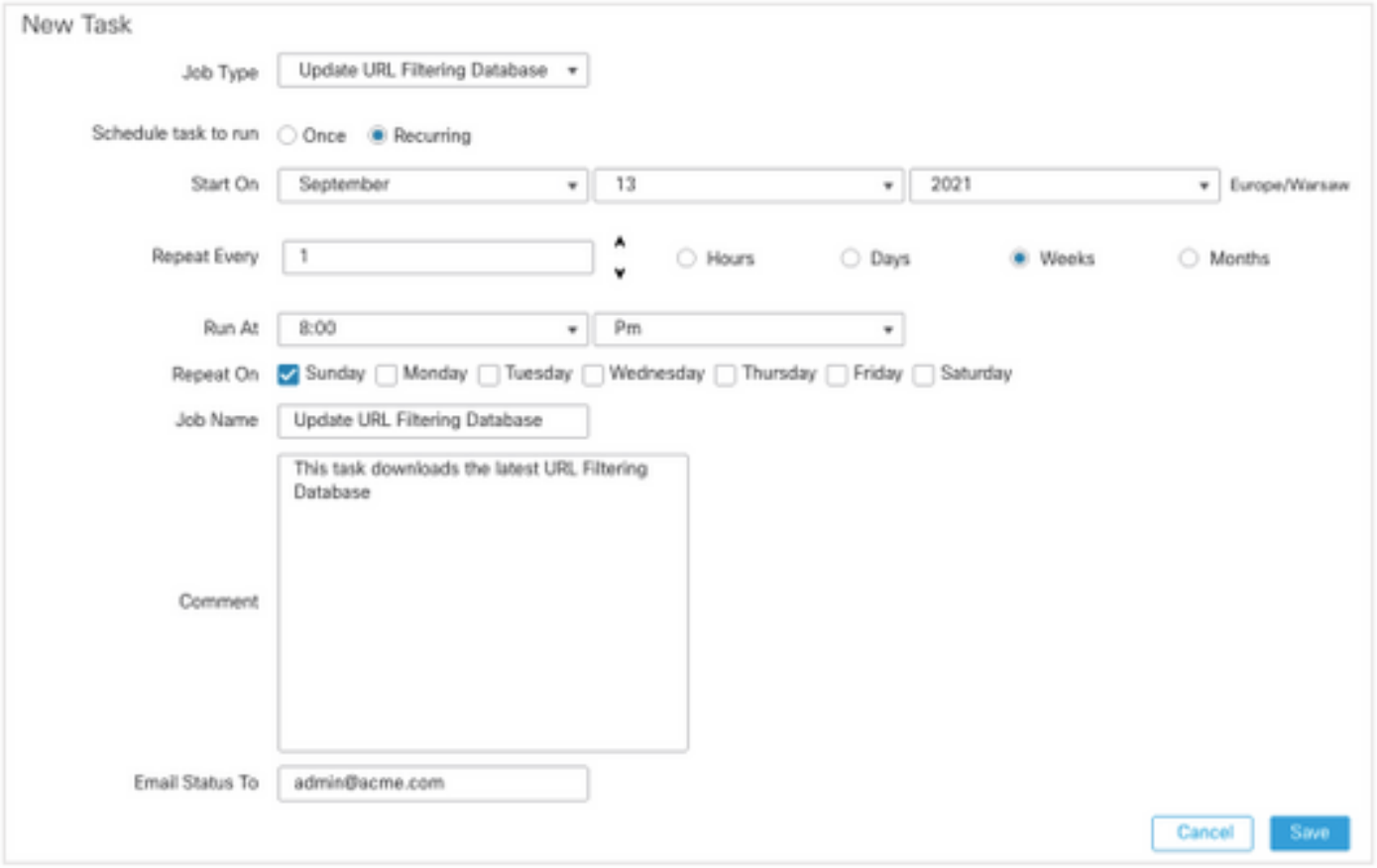


Para obtener más información, vea Firepower Management Center Configuration Guide, versión 7.0 - Update the Geolocation Database (GeoDB).

Automatizar la actualización de la base de datos de filtrado de URL con la tarea programada

Para asegurarse de que los datos de amenazas para el filtrado de URL están actualizados, el sistema debe obtener actualizaciones de datos de la nube de Cisco Collective Security Intelligence (CSI). Para automatizar este proceso, siga estos pasos:

1. Vaya a **Sistema > Herramientas > Programación**.
2. Haga clic en **Agregar tarea**.
3. En la lista desplegable **Tipo de trabajo**, elija **Actualizar base de datos de filtrado de URL.**
4. Para **ejecutar la tarea de programación**, haga clic en el botón de opción **Recurrente**.
5. Repita la tarea cada semana y ejecútela a las 8:00 pm los domingos o fuera del horario laboral.
6. Click **Save**.

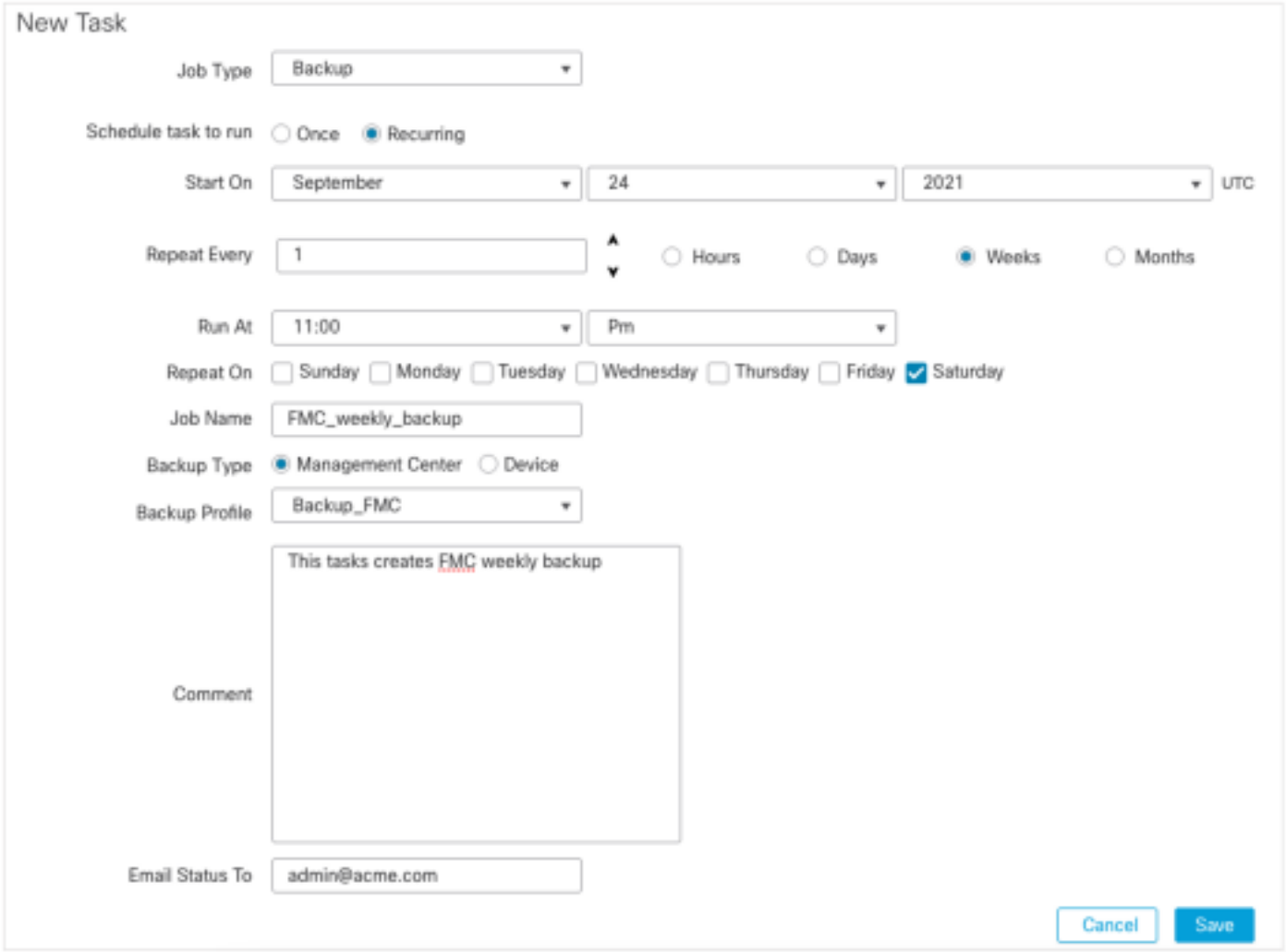


Para obtener más información, vea Firepower Management Center Configuration Guide, versión 7.0 - Automatización de actualizaciones de filtrado de URL mediante una tarea programada.

Configurar copias de seguridad periódicas

Como parte del plan de recuperación ante desastres, se recomienda realizar backups periódicos.

1. Asegúrese de estar en el **dominio global**.
2. Cree el perfil de copia de seguridad de FMC. Para obtener más información, vea la sección **Crear copia de seguridad de FMC**.
3. Vaya a **Sistema > Herramientas > Programación**.
4. Haga clic en **Agregar tarea**.
5. En la lista desplegable **Tipo de trabajo**, elija **Copia de seguridad.**
6. Para **ejecutar la tarea de programación**, haga clic en el botón de opción **Recurrente**. La frecuencia de backup debe ajustarse para adaptarse a las necesidades de la organización. Se recomienda crear copias de seguridad durante una ventana de mantenimiento u otro momento de uso bajo.
7. Para **Backup Type**, haga clic en el botón de opción **Management Center**.
8. En la lista desplegable **Perfil de copia de seguridad**, elija el Perfil de copia de seguridad.
9. Click **Save**.



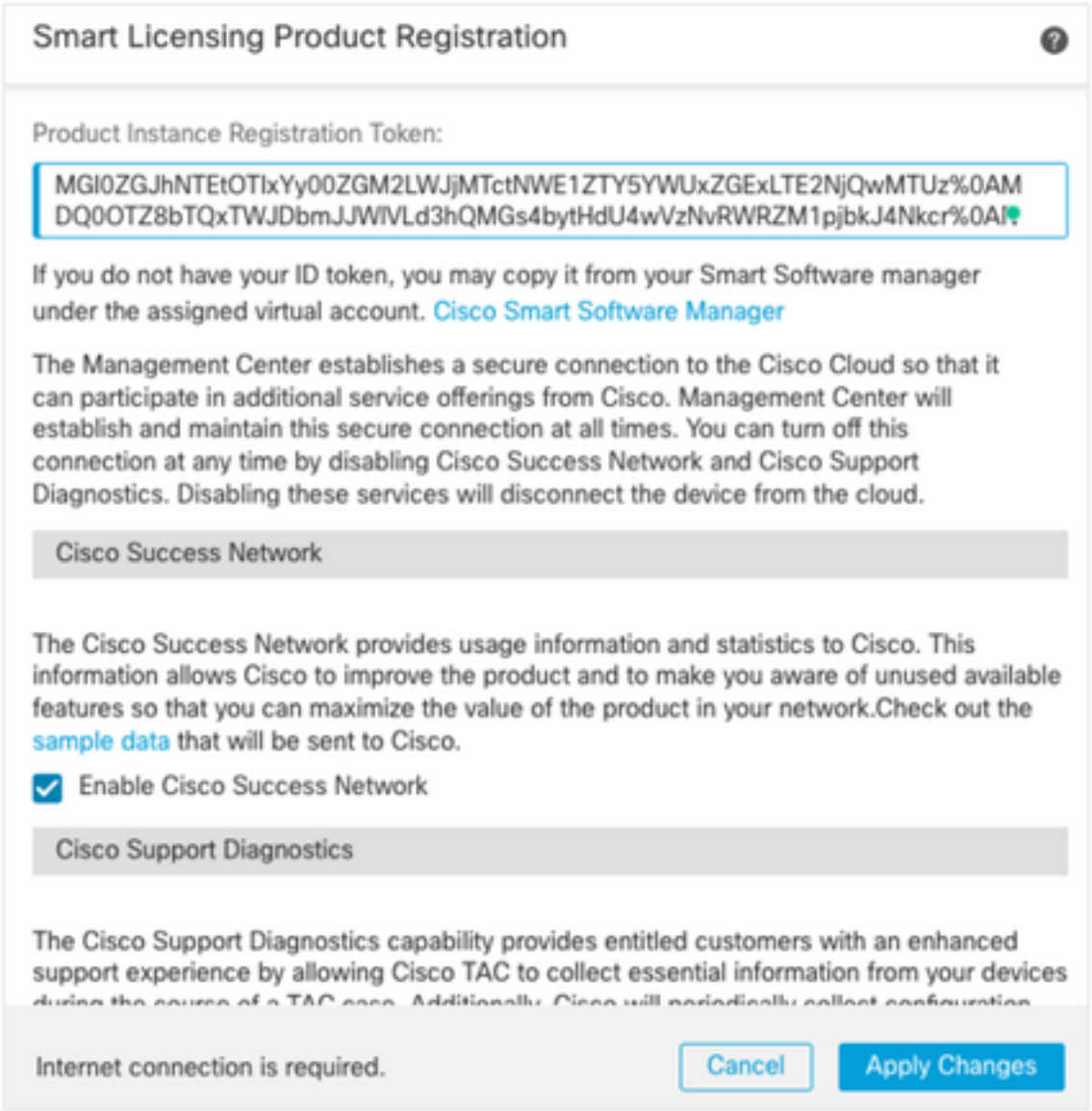
Para obtener más información, vea Firepower Management Center Configuration Guide, Versión 7.0 - Capítulo: Copia de seguridad y restauración.

Asegúrese de que la licencia inteligente esté registrada

Para registrar Cisco Firewall Management Center con Cisco Smart Software Manager, complete

estos pasos:

1. En https://software.cisco.com, navegue hasta **Smart Software Manager > Manage licenses**.
2. Navegue hasta la pestaña **Inventario > General** y cree un **Nuevo Token**.
3. En la interfaz de usuario de FMC, navegue hasta **System > Licenses > Smart Licenses**.
4. Haga clic en **Register**.
5. Inserte el token generado en el portal Cisco Smart Software Licensing.
6. Asegúrese de que **Cisco Success Network esté habilitado**.
7. Haga clic en **Aplicar cambios**.
8. Verifique El Estado De La Licencia Inteligente.



Para obtener más información, vea Firepower Management Center Configuration Guide, versión 7.0 - Registrar licencias inteligentes.

Revisar la configuración de los conjuntos de variables

Asegúrese de que la variable HOME_NET contiene sólo las redes internas/subredes de la organización. Una definición de conjunto de variables incorrecta afecta negativamente al rendimiento del firewall.

1. Vaya a **Objetos > Conjunto de variables**.

2. Edite la variable establecida por la política de intrusiones. Se permite tener una variable configurada por política de intrusión con diferentes configuraciones.
3. Ajuste las variables según su entorno y haga clic en **Guardar**.

Otras variables de interés son DNS_SERVERS O HTTP_SERVERS.

Para obtener más información, vea Firepower Management Center Configuration Guide, Versión 7.0 - Grupos de variables.

Verificar la habilitación de servicios en la nube

Para aprovechar los distintos servicios basados en la nube, navigate to **System > Integration > Cloud Services**.

Filtrado de URL

1. Active la opción Filtrado de URL y permita actualizaciones automáticas. Active la opción Consulta de Cisco Cloud para URL desconocidas.
   Un vencimiento más frecuente de la URL de caché requiere más consultas a la nube, lo que se traduce en cargas web más lentas.
2. **Guarde los cambios.**

Consejo: Para vencimiento de URL de caché, deje el valor predeterminado **Never**. Si se necesita una reclasificación web más estricta, esta configuración se puede modificar en consecuencia.

AMP para redes

1. Asegúrese de que ambas configuraciones estén activadas: **Habilite las actualizaciones automáticas de detección de malware local** y **comparta URI de eventos de malware con Cisco**.
2. En FMC 6.6.X, inhabilite el uso del puerto heredado 32137 para AMP para redes de modo que el puerto TCP utilizado en su lugar sea 443.
3. **Guarde los cambios.**

Nota: Esta configuración ya no está disponible en FMC 7.0+ y el puerto siempre es 443.

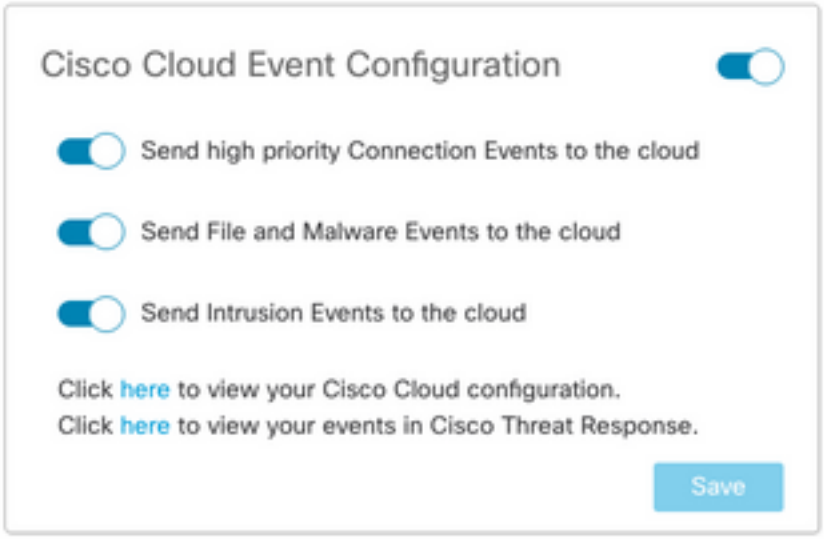
Región de nube de Cisco

1. La región de la nube debe coincidir con la región de la organización SecureX. Si no se crea la organización SecureX, elija la región más cercana a la instalación de FMC: región APJ, región de la UE o región de EE. UU.
2. **Guarde los cambios.**

Configuración de eventos en la nube de Cisco

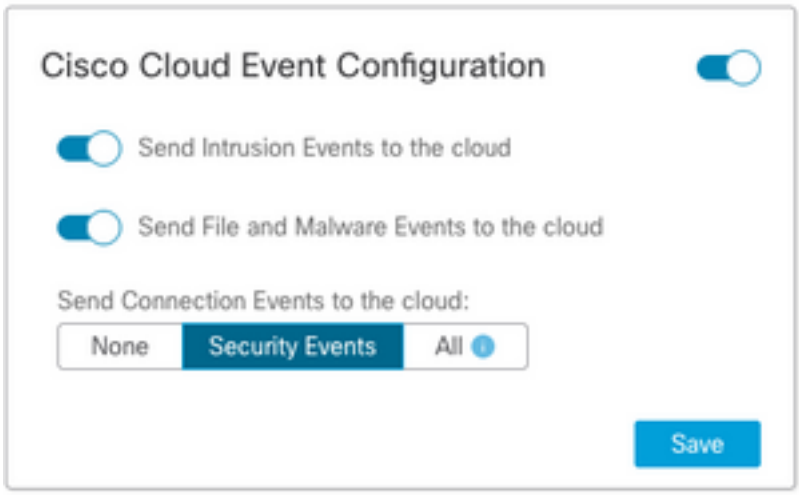
Para FMC 6.6.x

1. Asegúrese de las tres opciones: Se seleccionan **Enviar eventos de conexión de alta prioridad a la nube**, **Enviar eventos de archivo y malware a la nube** y **Enviar eventos de intrusión a la nube**.
2. **Guarde los cambios.**



Para FMC 7.0+

1. Asegúrese de que se han elegido ambas opciones: **Enviar eventos de intrusiones a la nube** y **Enviar eventos de archivos y malware a la nube**.
2. Para el tipo de eventos de conexión, elija **All** si la solución Security Analytics and Logging está en uso. Para SecureX, elija sólo **Eventos de seguridad**.
3. **Guarde los cambios.**



Habilitar integración de SecureX

La integración de SecureX proporciona una visibilidad instantánea del panorama de amenazas en sus productos de seguridad de Cisco. Para conectar SecureX y habilitar la cinta, siga estos pasos:

Integración de la cinta de opciones SecureX

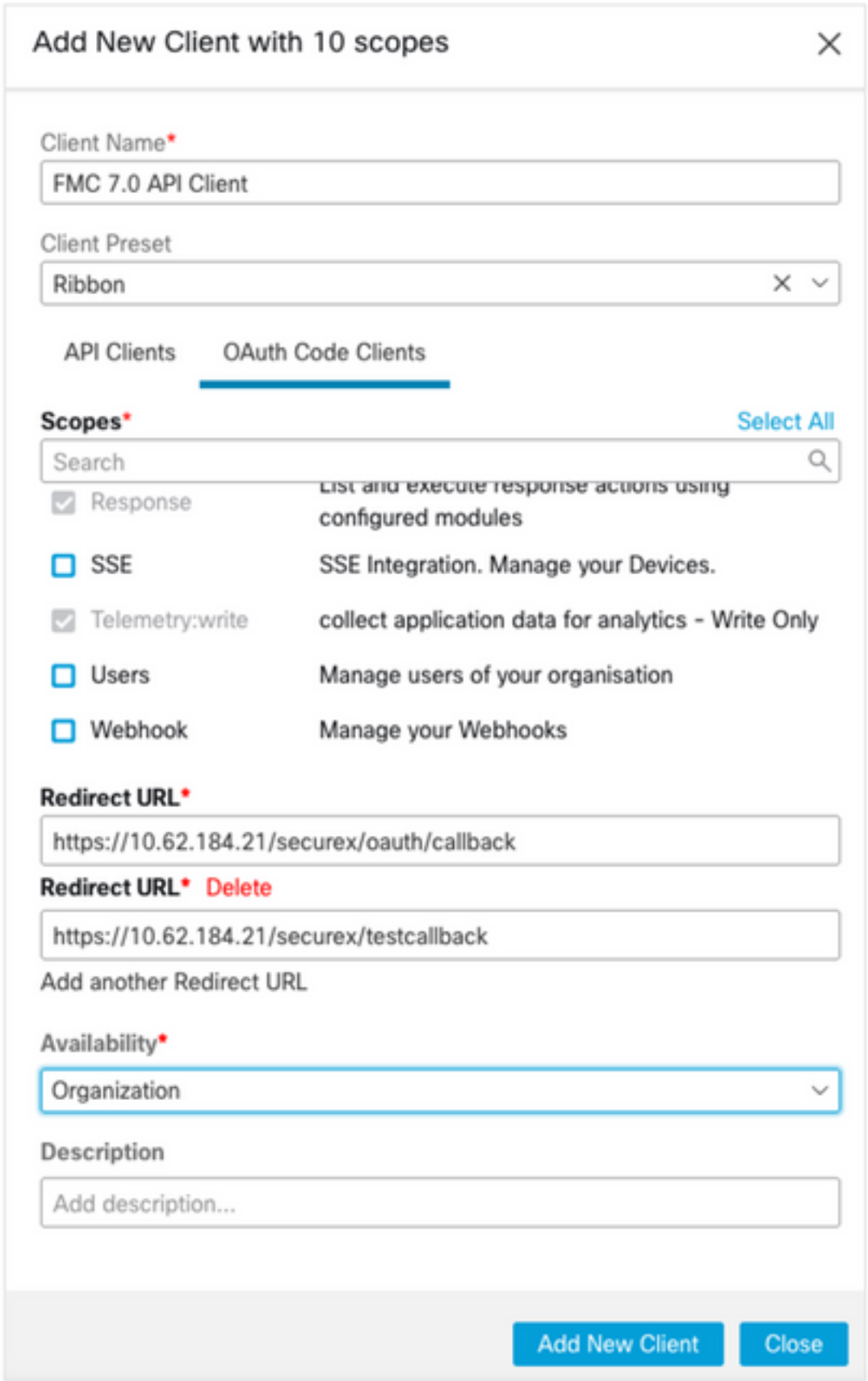
Nota: Esta opción está disponible para FMC versión 7.0+.

1. Inicie sesión en SecureX y cree un cliente API: En el campo **Client Name**, ingrese un nombre descriptivo del FMC. Por ejemplo, FMC 7.0 API Client.Haga clic en la ficha **Oauth Code Clients**.En la lista desplegable **Client Preset**, elija **Ribbon**. Elige los alcances: Casebook, Enrich:read, Global Intel:read, Inspect:read, Notification, Orbital, Private Intel, Profile, Response, Telemetry:write.Agregue las dos URL de redirección presentadas en el FMC:

Redirigir URL: <FMC_URL>/securex/oauth/callback

Segunda URL de redirección: <FMC_URL>/securex/testcallback

1. En la lista desplegable **Disponibilidad**, elija **Organización**.Haga clic en **Agregar nuevo cliente**.



2. Desde el FMC, navegue hasta **System > SecureX**.

3. Active la tecla de alternancia en la esquina superior derecha y confirme que la región mostrada coincide con la organización SecureX.

4. Copie la **ID del cliente** y la **contraseña del cliente** y péguelas en el FMC.

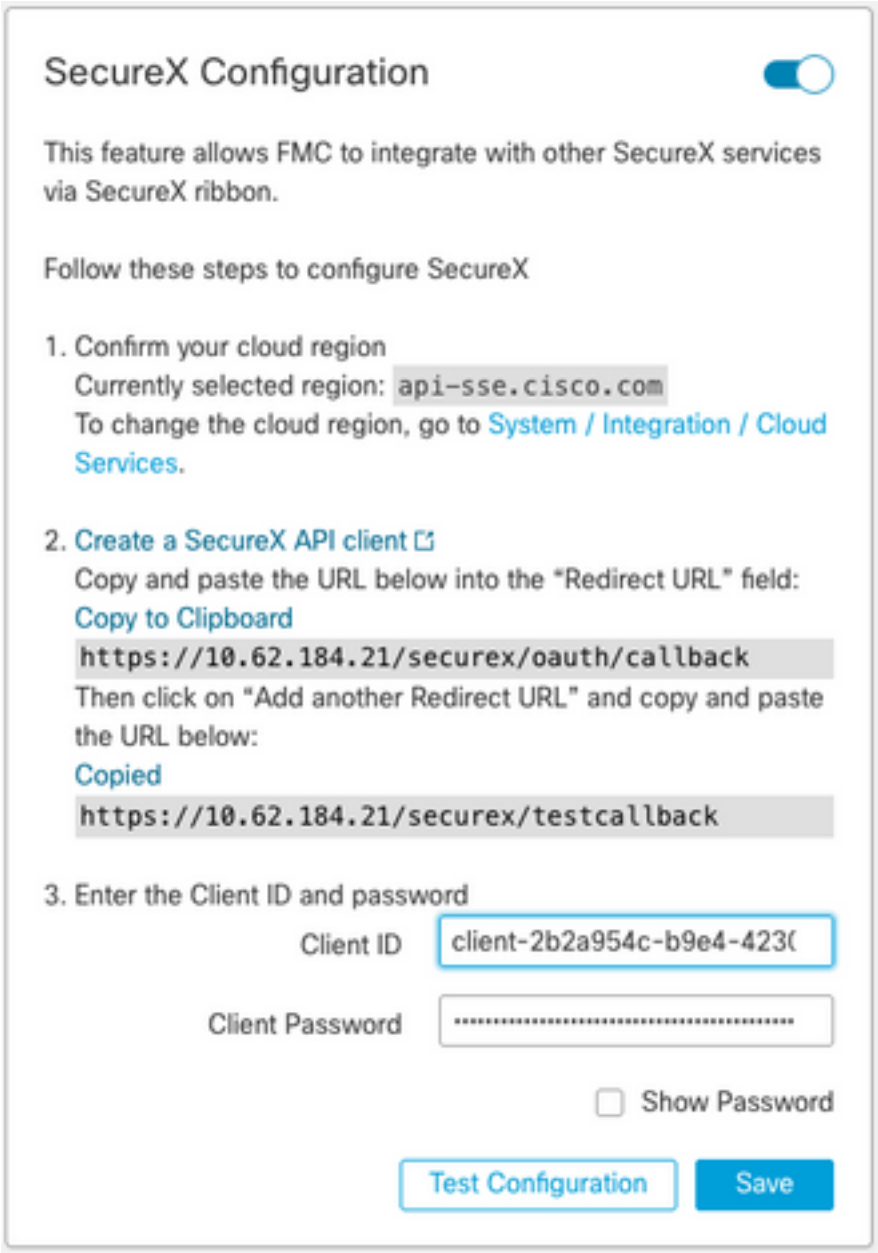
5. Elija **probar la configuración**.

6. Inicie sesión en SecureX para autorizar el cliente API.

7. Guarde los cambios y actualice el explorador para ver la cinta que se muestra en la parte inferior.

8. Expanda la cinta de opciones y elija **Get SecureX**. Introduzca las credenciales de SecureX si se le solicita.

9. La cinta SecureX ya funciona completamente para el usuario de FMC.

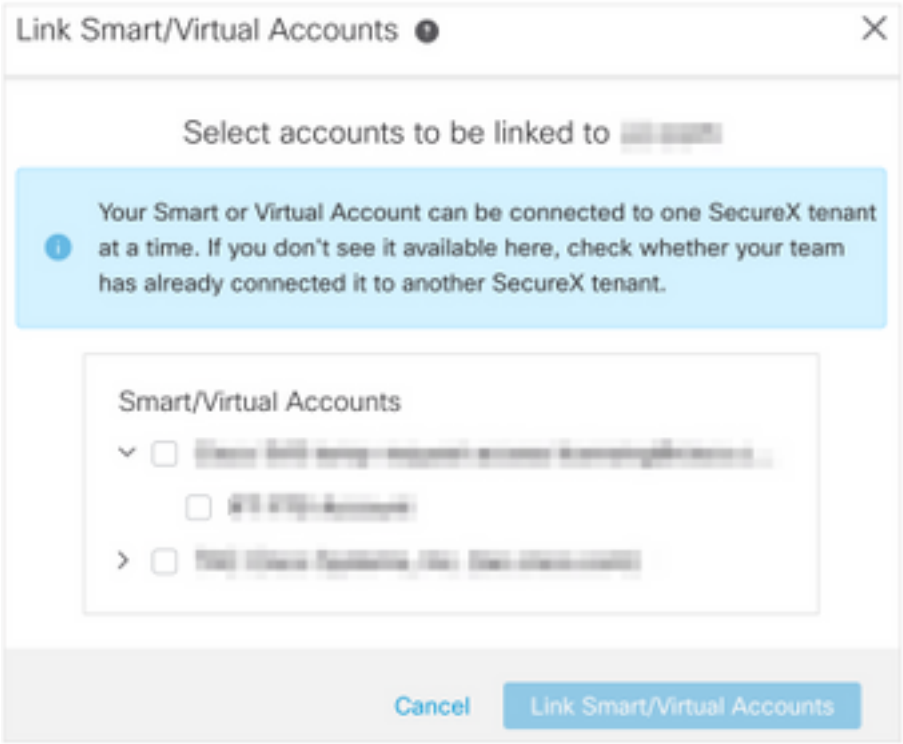


5YVPsGdzrkX8q8q0yYl-tDitezO6p_17MtH6NATx68fUZ5u9T3qOEQ

> **Nota:** Si cualquier otro usuario de FMC requiere acceso a la cinta, ese usuario debe iniciar sesión en la cinta con las credenciales de SecureX.

Enviar eventos de conexión a SecureX

1. En el FMC, navegue hasta **System > Integration > Cloud Services** y asegúrese de que la **configuración de eventos en la nube de Cisco** envíe eventos de intrusión, archivos y malware como se explica en la sección **Activar servicios en la nube**.
2. Asegúrese de que el FMC esté registrado con una licencia inteligente como se explica en la sección **Registro de las Licencias Inteligentes**.
3. Tome nota del nombre de **cuenta virtual asignada** tal como se muestra en FMC en **System > Licenses > Smart Licenses**.
4. Registre el FMC en SecureX: En SecureX, navegue hasta **Administration > Devices**.Elija **Administrar dispositivos**.Asegúrese de que las ventanas emergentes están permitidas en el explorador.Inicie sesión en Security Services Exchange (SSE).Vaya al **menú Herramientas > Enlazar cuentas inteligentes/virtuales**.Elija **Enlazar más cuentas**.Seleccione la cuenta virtual asignada al FMC (paso 3).Elija **Link Smart/Virtual Accounts.**



- Asegúrese de que el dispositivo FMC aparezca en los dispositivos.
- Vaya a la pestaña **Servicios en la nube**, active **Cisco SecureX Threat Response** y **Eventing** .
- Elija la **configuración de servicio adicional** (icono de engranaje) junto a la función de eventos.
- En la ficha General, elija **Compartir datos de eventos con Talos**.
- En la ficha Promocionar automáticamente eventos, en la sección Por tipo de evento elija todos los tipos de eventos disponibles y **Guardar**.

5. En el portal principal de SecureX, navegue hasta **Módulos de integración > Firepower** y agregue el módulo de integración de Firepower.

6. Cree un nuevo panel.

7. Agregue las fichas relacionadas con Firepower.

Integración de terminales seguros (AMP para terminales)

Para habilitar la integración de terminales seguros (AMP para terminales) con la implementación de Firepower, siga estos pasos:

1. Vaya a **AMP > AMP Management**.
2. Elija **Add AMP Cloud Connection**.
3. Elija la nube y **regístrese**.

Nota: El estado **Habilitado** significa que se establece la conexión a la nube.

Integrar Análisis de malware seguro (Threat Grid)

De forma predeterminada, Firepower Management Center puede conectarse a la nube pública de Cisco Threat Grid para el envío de archivos y la recuperación de informes. No es posible eliminar esta conexión. No obstante, se recomienda elegir el que más se aproxime a su nube de implementación:

1. Vaya a **AMP > Conexiones de análisis dinámico**.
2. Haga clic en **Editar** (icono del lápiz) en la sección Acción.
3. Elija el nombre de nube correcto.
4. Para asociar la cuenta Threat Grid a funciones de informes detallados y de sandbox avanzadas, haga clic en el icono **Asociar**.

Para obtener más información, consulte Firepower Management Center Configuration Guide, versión 7.0: habilitación del acceso a los resultados de análisis dinámicos en la nube pública.

Para obtener información sobre la integración de dispositivos Thread Grid en las instalaciones, consulte Firepower Management Center Configuration Guide, versión 7.0: Dynamic Analysis On-In-situ Appliance (Cisco Threat Grid) .