

FDM integrado a orquestador de defensa

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo incorporar un dispositivo administrado por Firepower Device Manager (FDM) a Cisco Defense Orchestrator (CDO) mediante la clave de registro.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de dispositivos Firepower (FDM)
- Cisco Defense Orchestrator (CDO)

Componentes Utilizados

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

- Firepower Device Manager (FDM) Azure que ejecuta la versión 7.4.1

Para obtener una lista completa de versiones y productos compatibles, consulte la Guía de compatibilidad de [Secure Firewall Threat Defence](#) para obtener más información.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

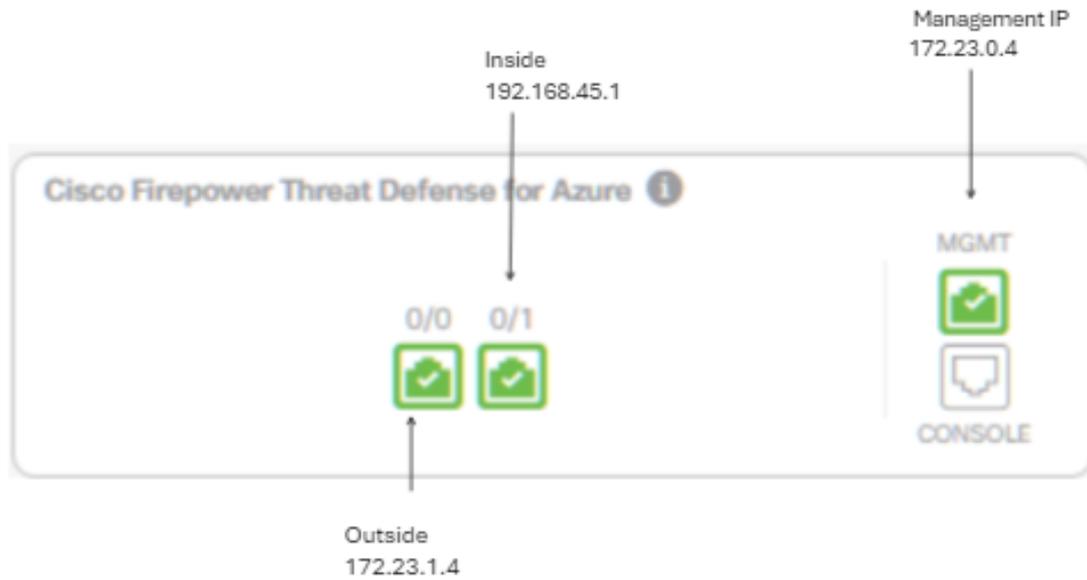
Antes de comenzar el proceso de incorporación de un dispositivo gestionado por FDM a Cisco Defense Orchestrator (CDO) mediante una clave de registro, asegúrese de que cumple estos requisitos previos:

1. Versión compatible: el dispositivo debe ejecutar la versión 6.6 o superior.
2. Requisitos de red: [Conecte Cisco Defense Orchestrator a sus dispositivos gestionados](#)
3. Software de administración: el dispositivo debe administrarse a través del administrador de dispositivos de firewall seguro (FDM).
4. Licencias: el dispositivo puede usar una licencia de evaluación de 90 días o una licencia inteligente.
5. Registros existentes: asegúrese de que el dispositivo no esté registrado aún con los servicios en la nube de Cisco para evitar conflictos durante el proceso de incorporación.
6. Cambios pendientes: compruebe que no hay cambios pendientes en el dispositivo.
7. Configuración de DNS: los parámetros de DNS deben configurarse correctamente en el dispositivo administrado por FDM.
8. Servicios de hora: los servicios de hora del dispositivo se pueden configurar con precisión para garantizar la sincronización con los protocolos de tiempo de la red.
9. Requisito para la activación de la compatibilidad con FDM. La compatibilidad con el administrador de dispositivos de firewall (FDM) y su funcionalidad se concede exclusivamente previa solicitud. Los usuarios sin la compatibilidad con FDM habilitada en su arrendatario no pueden administrar ni implementar configuraciones en los dispositivos administrados con FDM. Para activar esta plataforma, los usuarios deben [enviar una solicitud al equipo de soporte](#) para la habilitación de soporte de FDM.

Configurar

Diagrama de la red

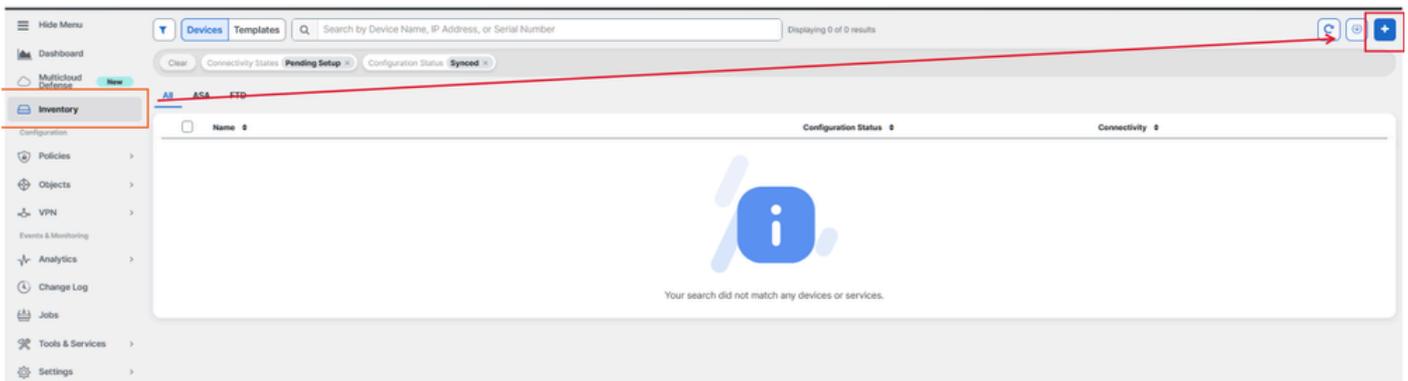
Este artículo se centra en un dispositivo FDM (Firepower Device Manager), que se controla a través de su interfaz de gestión. Esta interfaz dispone de acceso a Internet que es esencial para registrar el dispositivo con Cisco Defense Orchestrator (CDO).



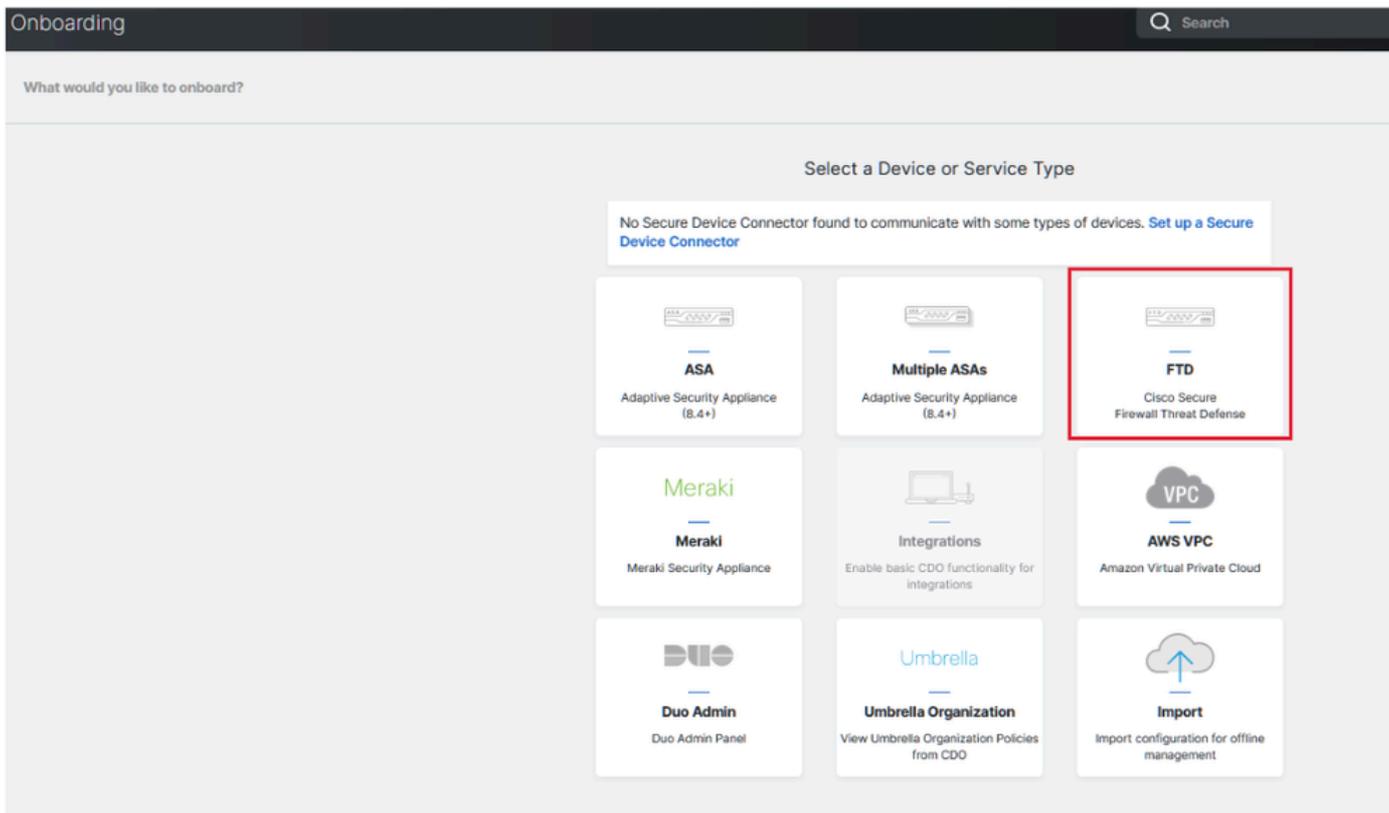
Configuraciones

Paso 1. Inicie sesión en [Cisco Defense Orchestrator](#) (CDO).

Paso 2. Vaya al panel Inventario y seleccione el botón azul más para incorporar un dispositivo.



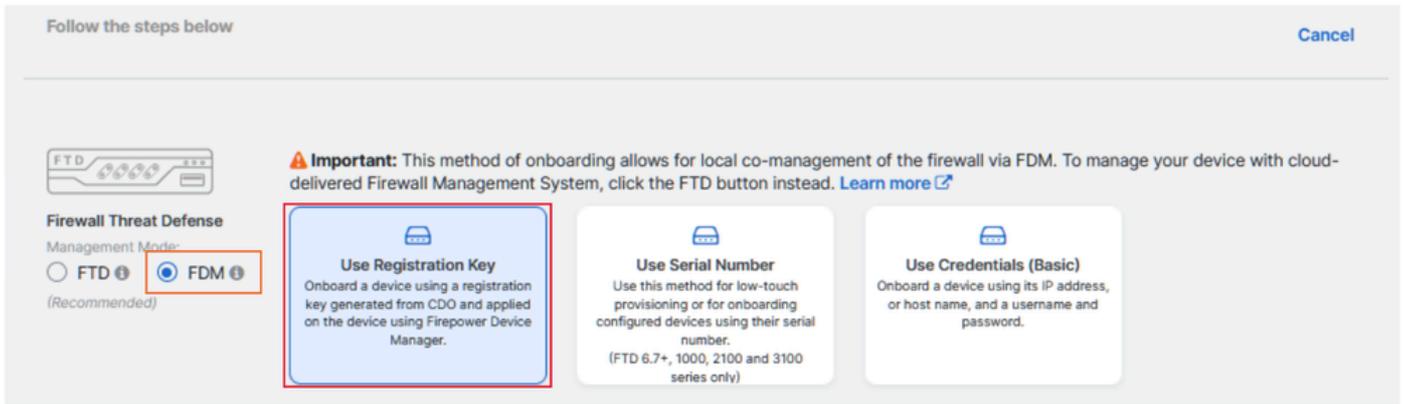
Paso 3. Seleccione la opción FTD.



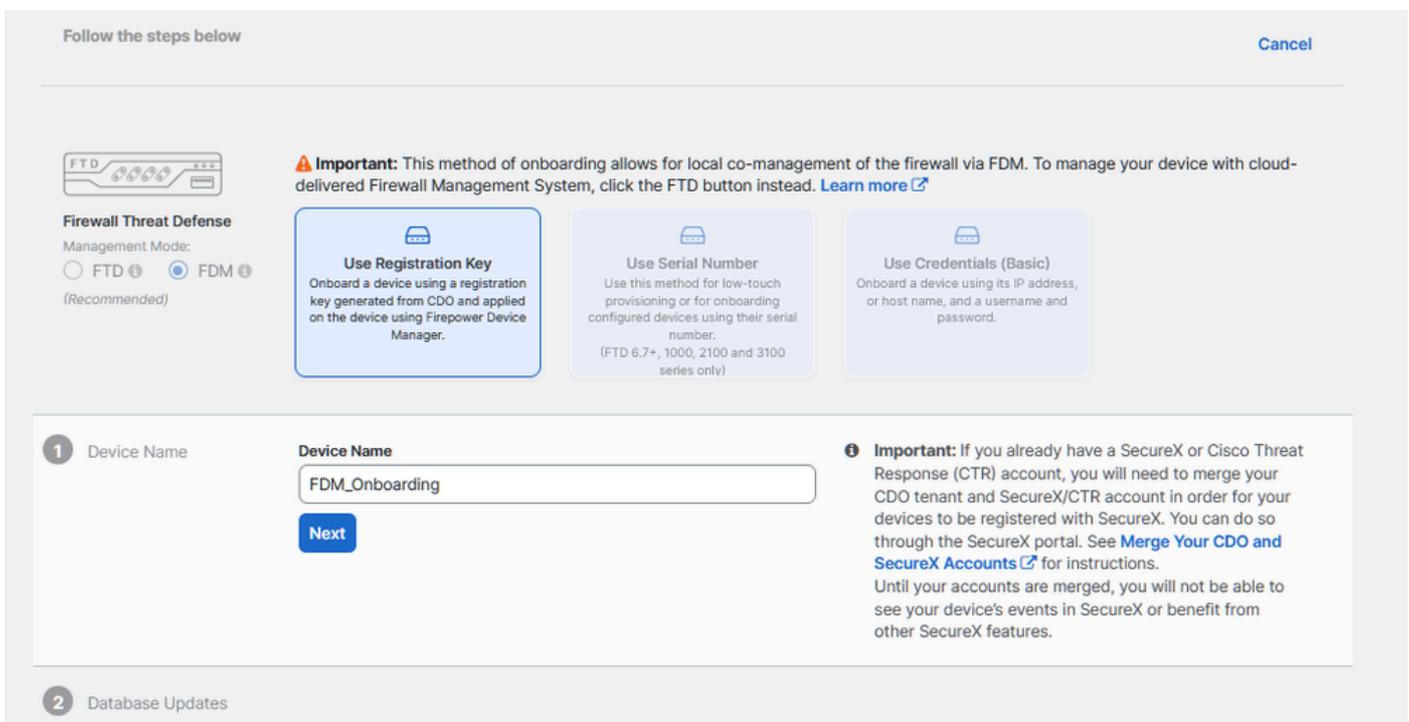
Paso 4 Vaya a la sección "Onboard FTD Device" (Dispositivo FTD incorporado) para iniciar el proceso de registro. Es importante tener en cuenta los métodos disponibles para incorporar un dispositivo Threat Defence:

- Por número de serie: este método se aplica a dispositivos físicos como Firepower serie 1000, Firepower serie 2100 o Secure Firewall serie 3100 con versiones de software compatibles. Necesita el número de serie del chasis o PCA y una conexión de red a Internet.
- By Registration Key: Este es el método preferido para la incorporación, especialmente ventajoso para los dispositivos que reciben direcciones IP a través de DHCP, ya que ayuda a mantener la conectividad con CDO incluso si hay un cambio en la dirección IP del dispositivo.
- Uso de credenciales: esta alternativa implica la introducción de las credenciales del dispositivo y la dirección IP de su interfaz externa, interna o de gestión, adaptada a la configuración del dispositivo dentro de la red.

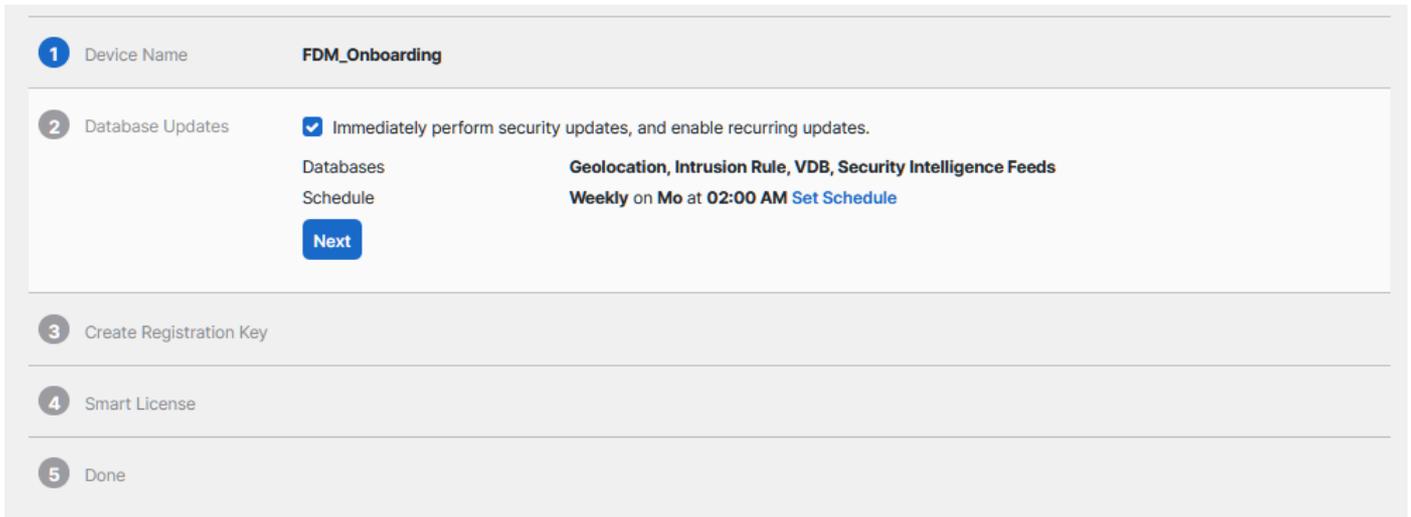
Para este proceso, seleccione la opción FDM y, a continuación, la opción Use Registration Key para garantizar una conectividad uniforme con CDO, independientemente de los posibles cambios en la dirección IP del dispositivo.



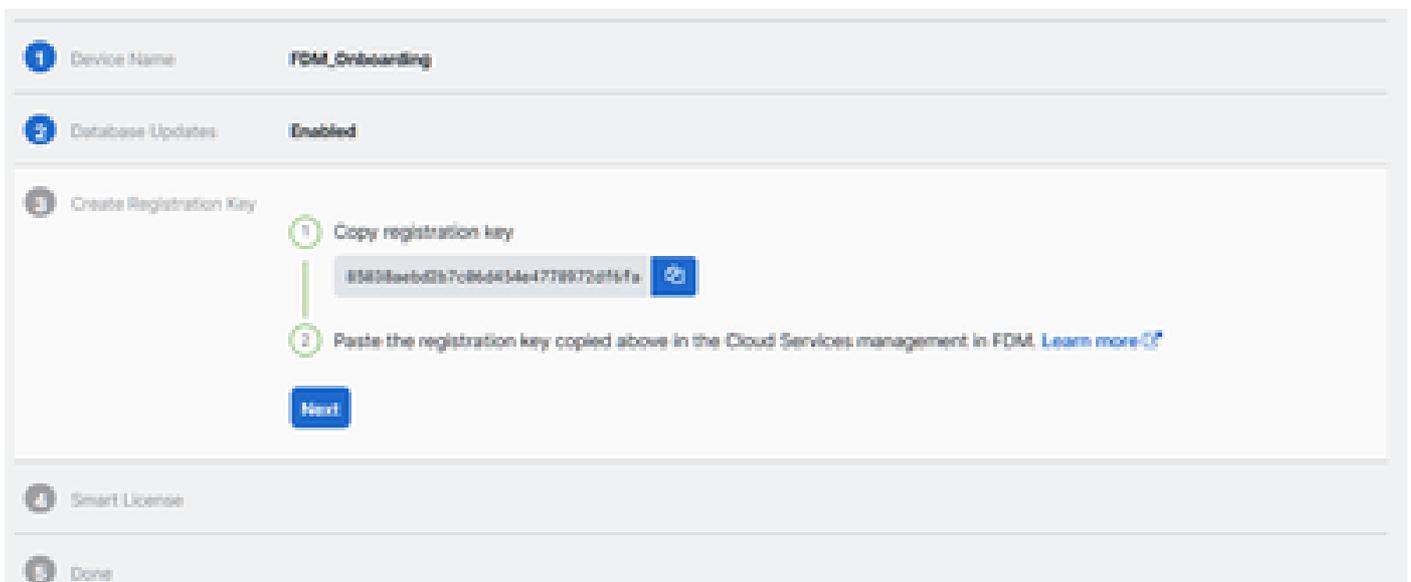
Paso 5. Introduzca el nombre de dispositivo deseado en el campo Device Name (Nombre de dispositivo) y especifique la asignación de directiva. Además, elija la licencia de suscripción que debe asociarse con el dispositivo.



Paso 6. La sección Actualizaciones de la base de datos está configurada de forma predeterminada para ejecutar actualizaciones de seguridad inmediatamente y configurar actualizaciones periódicas. El cambio de esta configuración no modifica ninguna programación de actualización existente establecida a través del administrador de dispositivos de Secure Firewall.



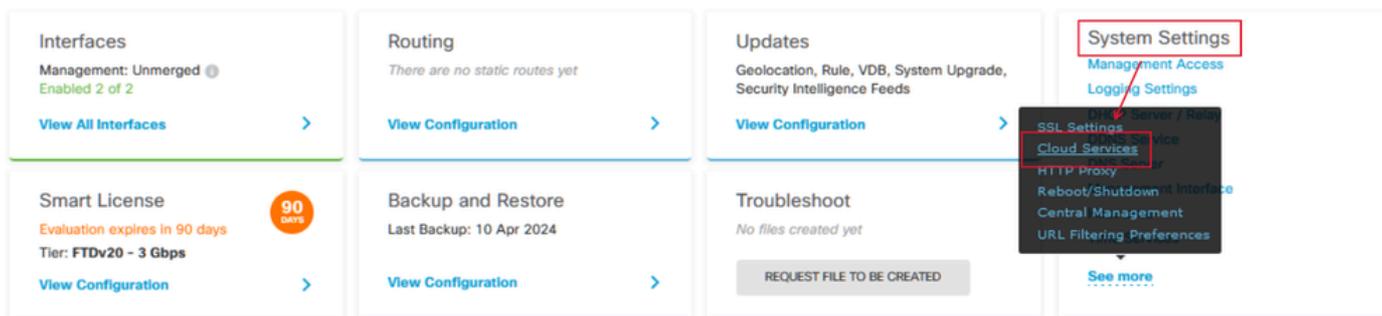
Paso 7. En la sección CLI Registration Key (Clave de registro de CLI), CDO genera automáticamente una clave de registro. Al salir de la interfaz de onboarding antes de la finalización, se crea un marcador de posición para el dispositivo dentro del Inventario. La clave de registro se puede recuperar de esta ubicación más adelante si es necesario.



Paso 8. Utilice el icono Copiar para copiar la clave de registro generada.

Paso 9. Acceda al dispositivo Secure Firewall Device Manager destinado a la incorporación a CDO.

Paso 10. Seleccione Servicios en la nube en el menú Configuración del sistema.



Paso 11. Designe la región de nube de Cisco correcta en el menú desplegable Región, alineada con la ubicación geográfica del arrendatario:

- En defenseorchestrator.com, seleccione US (EE. UU.).
- Para defenseorchestrator.eu, seleccione EU.
- Para apj.cdo.cisco.com, seleccione APJ.

Device Summary

Cloud Services

 **Not Registered**

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

85038aebd2b7c06d454e4778972df6fa

Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) 

Enroll Cisco Success Network

REGISTER

Need help? 

Paso 12. En la sección Tipo de inscripción, elija la cuenta de seguridad.

Device Summary

Cloud Services



Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

85038aebd2b7c06d454e4778972df6a

Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▾

Enroll Cisco Success Network

REGISTER

Need help?

Paso 13. Pegue la clave de registro en el campo Clave de registro.

Device Summary

Cloud Services



Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

85038aebd2b7c06d454e4778972d96fa



Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▼

Enroll Cisco Success Network

REGISTER

Need help?

Paso 14. En el caso de los dispositivos de la versión 6.7 o posterior, compruebe que Cisco Defense Orchestrator está activado en la sección Inscripción de servicios.

Device Summary

Cloud Services



Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

65038aebd2b7c06d454e4778973d9fa

Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▾

Enroll Cisco Success Network

REGISTER

Need help? [?](#)

Paso 15. (Opcional) Revise los detalles de Cisco Success Network Enrollment. Si no desea participar, desactive la casilla de verificación Inscribir a Cisco Success Network.

Paso 16. Seleccione Registrar y acepte la divulgación de información de Cisco. El administrador de dispositivos de firewall seguro envía el registro a CDO.

Device Summary
Cloud Services

Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type
Security/CDO Account Smart Licensing

Region
US Region

Registration Key
85038aebd2b7c06d454e4778972d6fa

Service Enrollment

Cisco Defense Orchestrator
Cisco Defense Orchestrator is a cloud-based management solution for Cisco Secure Firewall devices. Select this option if you want to register with an account.

Enable Cisco Defense Orchestrator

Cisco Success Network
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#)

Enroll Cisco Success Network

REGISTER Need help?

Cisco Disclosure

Your device establishes a secure connection to the Cisco Cloud so that your device can participate in additional service offerings from Cisco such as technical support services, cloud management and monitoring services. Your device will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network, Cisco SecureX threat response and Cisco Defense Orchestrator. Disabling all will disconnect the device from the cloud.

Disconnection of Cisco Success Network, Cisco SecureX threat response and Cisco Defense Orchestrator will not impact the receipt of updates or operation of the Smart Licensing capabilities; such functions will continue to operate normally.

DECLINE ACCEPT

Paso 17. De nuevo en CDO, en el área de creación de claves de registro, seleccione Siguiente.

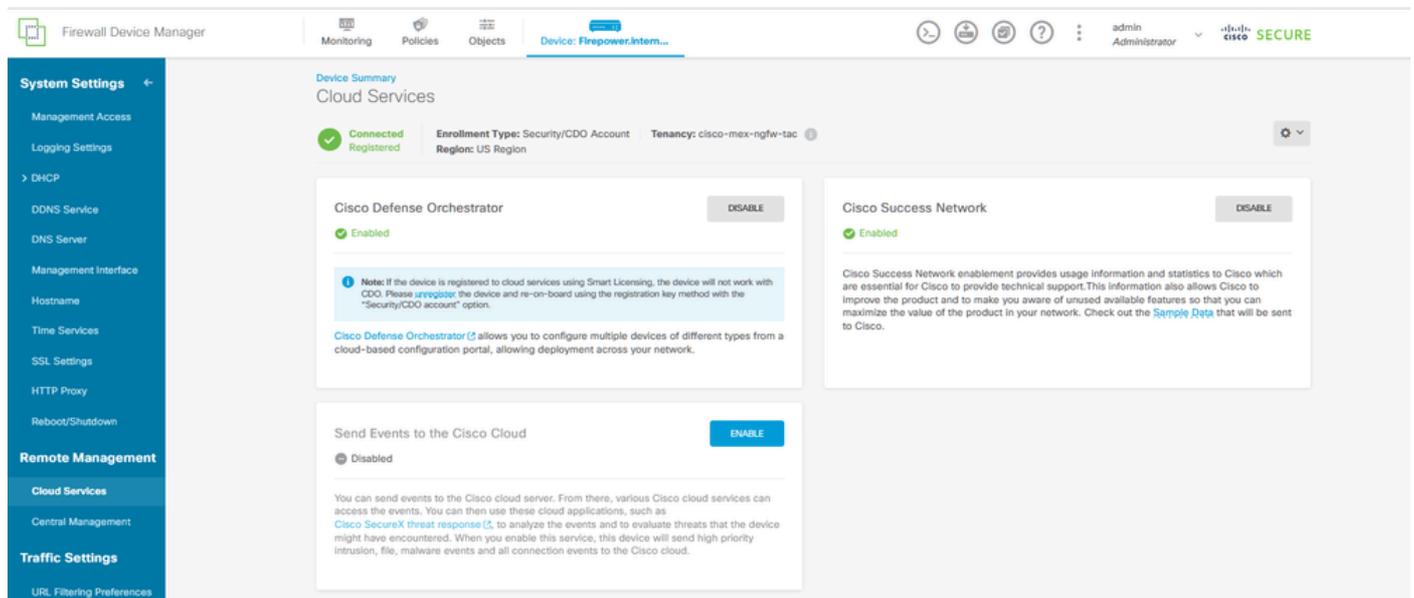
Paso 18. (Opcional) Identifique y seleccione las licencias previstas para el dispositivo y, a continuación, seleccione Next (Siguiente).

Paso 19. Observe el estado del dispositivo en la transición del inventario de CDO de No provisionado a Localizando, luego a Sincronizando y, finalmente, a Sincronizado.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Navigue hasta el portal CDO y verifique el estado del dispositivo, que indica Online y Synced. Además, la verificación del estado se puede llevar a cabo mediante la GUI de FDM. Vaya a Sistema > Servicios en la nube para observar el estado de conexión de Cisco Defense Orchestrator y Cisco Success Network. La interfaz muestra el estado Conectado, lo que confirma la integración correcta con los servicios.



The screenshot shows the Firewall Device Manager (FDM) interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: Firepower.Intem...'. The left sidebar lists various settings categories. The main content area is titled 'Cloud Services' and shows the following configuration:

- Connected Registered** (Status: Green checkmark)
- Enrollment Type:** Security/CDO Account
- Tenancy:** cisco-mex-ngfw-tac
- Region:** US Region

Three service cards are visible:

- Cisco Defense Orchestrator:** Status: Enabled (Green checkmark). Includes a note about Smart Licensing and a link to the CDO portal.
- Cisco Success Network:** Status: Enabled (Green checkmark). Includes a note about usage information and statistics.
- Send Events to the Cisco Cloud:** Status: Disabled (Grey circle). Includes a note about sending events to the Cisco cloud server.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

- Resolución del fallo del FQDN del servicio en la nube

Si el registro del dispositivo falla debido a una incapacidad para resolver el FQDN del servicio en la nube, verifique la conectividad de red o la configuración DNS e intente volver a incorporar el dispositivo.

- Error de clave de registro no válida

Cuando el registro del dispositivo no se completa debido a la entrada de una clave de registro no válida en el Administrador de dispositivos de firewall, copie la clave de registro correcta de Cisco Defense Orchestrator y vuelva a intentar el proceso de registro. Si el dispositivo ya tiene una licencia inteligente, quite la licencia inteligente antes de introducir la clave de registro en el Administrador de dispositivos de firewall.

- Problema de licencia insuficiente

En los casos en los que el estado de la conectividad del dispositivo indique "Licencia insuficiente", vaya a:

1. Espere a que el dispositivo obtenga la licencia, ya que Cisco Smart Software Manager puede requerir un período para aplicar una nueva licencia al dispositivo.
2. Si el estado del dispositivo no cambia, actualice el portal CDO cerrando sesión y volviendo a iniciarla para resolver posibles problemas de comunicación de red entre el servidor de licencias y el dispositivo.
3. Si la actualización del portal no actualiza el estado del dispositivo, realice estas acciones:
 - Genere una nueva clave de registro de [Cisco Smart Software Manager](#) y cópiela. Refiérase al video [Generación de Licencias Inteligentes](#) para obtener orientación.
 - En la barra de navegación de CDO, seleccione la página Inventario.
 - Elija el dispositivo enumerado con el estado Licencia insuficiente.
 - En el panel Detalles del dispositivo, haga clic en Administrar licencias bajo la alerta Licencias insuficientes. Mensajes de la ventana Administrar licencias.
 - En el campo Activar, pegue la nueva clave de registro y seleccione Registrar dispositivo.

Una vez que la nueva clave de registro se haya aplicado correctamente, el estado de conectividad del dispositivo debe cambiar a 'En línea'.

Para obtener una guía completa sobre el registro de Firepower Device Manager (FDM) mediante métodos alternativos a la clave de registro, consulte la documentación detallada que se proporciona en el enlace: [Troubleshooting de dispositivos gestionados por FDM](#).

Este recurso ofrece instrucciones paso a paso y consejos para la resolución de problemas relacionados con las diferentes técnicas de registro que se pueden emplear para incorporar correctamente FDM a Cisco Defense Orchestrator (CDO).

Información Relacionada

- [Solucionar problemas de dispositivos administrados por FDM](#)
- [Gestión de dispositivos FDM con Cisco Defense Orchestrator](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).