

FDM integrado ao Defense Orchestrator

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como integrar um dispositivo gerenciado pelo Firepower Device Manager (FDM) ao Cisco Defense Orchestrator (CDO) usando a chave de registro.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Device Manager (FDM)
- Cisco Defense Orchestrator (CDO)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Device Manager (FDM) Azure executando a versão 7.4.1

Para obter uma lista abrangente de versões e produtos compatíveis, consulte o [Secure Firewall Threat Defense Compatibility](#) Guide para obter detalhes adicionais.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

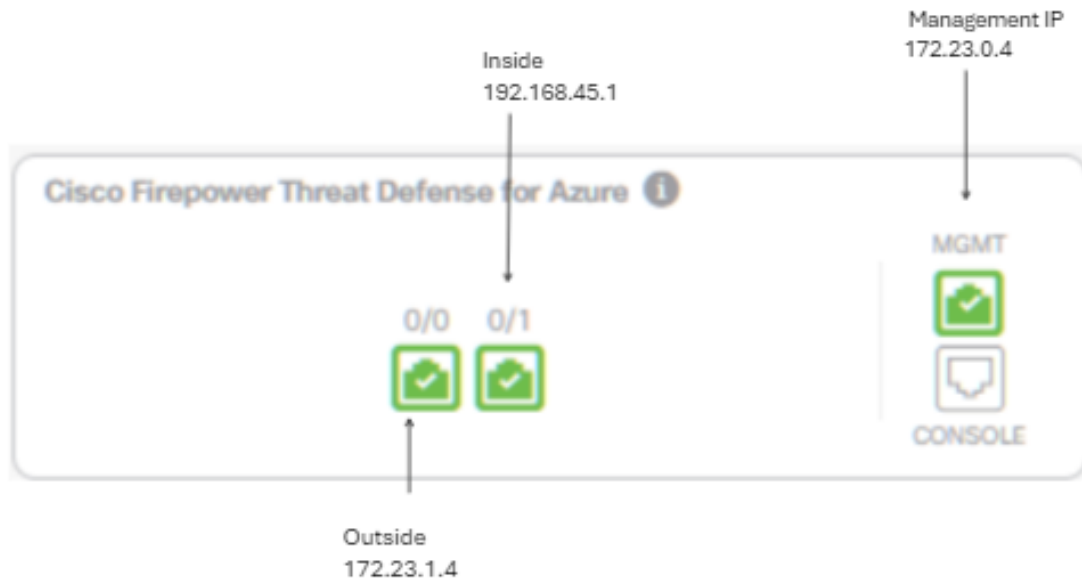
Antes de iniciar o processo de integração de um dispositivo gerenciado pelo FDM para o Cisco Defense Orchestrator (CDO) usando uma chave de registro, certifique-se de atender aos seguintes pré-requisitos:

1. Versão Compatível: seu dispositivo deve estar executando a versão 6.6 ou superior.
2. Requisitos de rede: [Conecte o Cisco Defense Orchestrator aos seus dispositivos gerenciados](#)
3. Software de Gerenciamento: o dispositivo deve ser gerenciado através do Gerenciador de Dispositivos de Firewall Seguro (FDM).
4. Licenciamento: seu dispositivo pode usar uma licença de avaliação de 90 dias ou uma licença inteligente.
5. Registros existentes: certifique-se de que o dispositivo ainda não esteja registrado no Cisco Cloud Services para evitar conflitos durante o processo de integração.
6. Alterações pendentes: verifique se não há alterações pendentes no dispositivo.
7. Configuração DNS: as configurações DNS devem ser definidas corretamente no dispositivo gerenciado pelo FDM.
8. Serviços de tempo: os serviços de tempo no dispositivo podem ser configurados com precisão para garantir a sincronização com os protocolos de tempo da rede.
9. Requisito para Ativação do Suporte do FDM. O suporte ao Gerenciador de Dispositivos de Firewall (FDM) e sua funcionalidade são concedidos exclusivamente mediante solicitação. Os usuários sem suporte do FDM habilitado em seus locatários não podem gerenciar ou implantar configurações em dispositivos gerenciados pelo FDM. Para ativar essa plataforma, os usuários devem [enviar uma solicitação à equipe de suporte](#) para habilitação de suporte do FDM.

Configurar

Diagrama de Rede

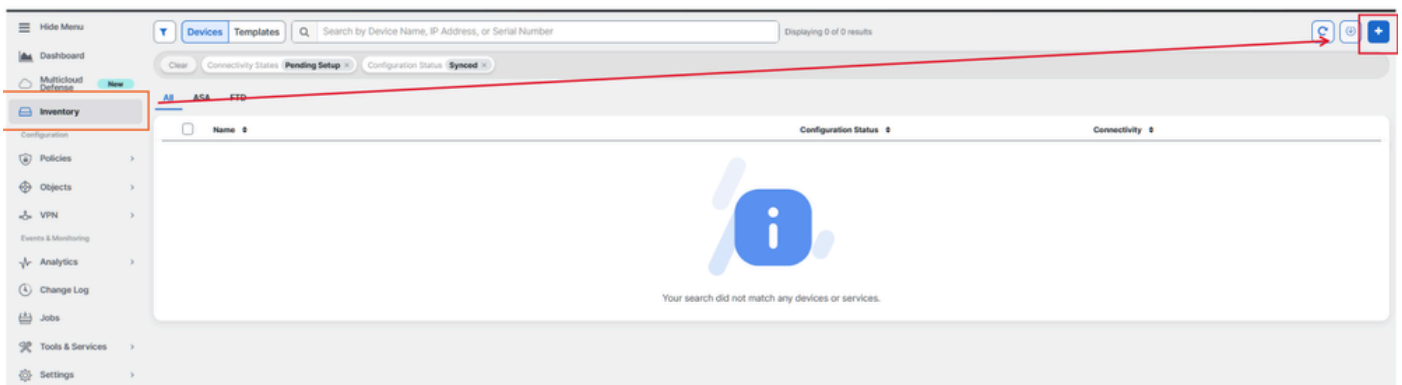
Este artigo se concentra em um dispositivo FDM (Firepower Device Manager), que é controlado por meio de sua interface de gerenciamento. Essa interface tem acesso à Internet, que é essencial para registrar o dispositivo com o Cisco Defense Orchestrator (CDO).



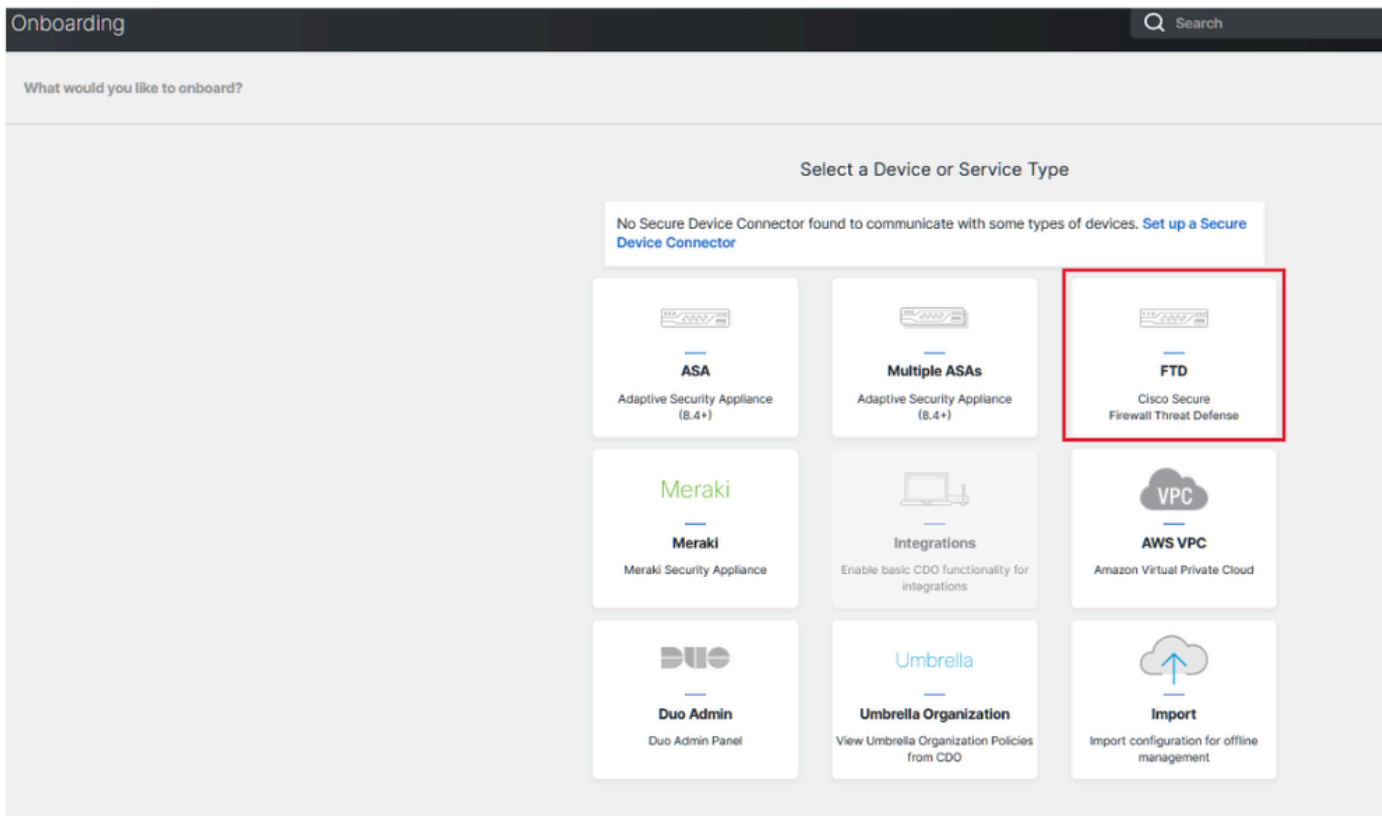
Configurações

Etapa 1. Faça login no [Cisco Defense Orchestrator](#) (CDO).

Etapa 2. Navegue até o painel Inventário e selecione o botão de adição azul para integrar um dispositivo.



Etapa 3. Escolha a opção FTD.




Etapa 4 Vá para a seção 'Onboard FTD Device' (Dispositivo FTD integrado) para iniciar o processo de registro. É importante observar os métodos disponíveis para integrar um dispositivo de defesa contra ameaças:


- Por número de série: esse método se aplica a dispositivos físicos como o Firepower 1000, Firepower 2100 ou Secure Firewall 3100 Series com versões de software suportadas. É necessário o número de série do chassis ou PCA e uma conexão de rede à Internet.
- Por chave de registro: este é o método preferido para integração, particularmente vantajoso para dispositivos que recebem endereços IP via DHCP, pois ajuda a manter a conectividade com CDO, mesmo que haja uma alteração no endereço IP do dispositivo.
- Uso de credenciais: essa alternativa envolve inserir as credenciais do dispositivo e o endereço IP de sua interface externa, interna ou de gerenciamento, adaptada à configuração do dispositivo na rede.


Para esse processo, selecione a opção FDM e, em seguida, a opção Usar Chave de Registro para garantir conectividade consistente com CDO, independentemente de alterações potenciais no endereço IP do dispositivo.


Follow the steps below Cancel

 **Important:** This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. [Learn more](#)

Firewall Threat Defense
Management Mode:
 FTD FDM
(Recommended)



Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.


Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000, 2100 and 3100 series only)



Use Credentials (Basic)
Onboard a device using its IP address, or host name, and a username and password.


Etapa 5. Insira o nome do dispositivo desejado no campo Device Name (Nome do dispositivo) e especifique a Policy Assignment (Atribuição de política). Além disso, escolha a licença de assinatura que deve ser associada ao dispositivo.


Follow the steps below Cancel

 **Important:** This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. [Learn more](#)

Firewall Threat Defense
Management Mode:
 FTD FDM
(Recommended)


Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.


Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000, 2100 and 3100 series only)


Use Credentials (Basic)
Onboard a device using its IP address, or host name, and a username and password.

1 Device Name

Device Name

Next

! **Important:** If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your CDO tenant and SecureX/CTR account in order for your devices to be registered with SecureX. You can do so through the SecureX portal. See [Merge Your CDO and SecureX Accounts](#) for instructions. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features.

2 Database Updates

Etapa 6. A seção Atualizações do Banco de Dados é configurada por padrão para executar atualizações de segurança imediatamente e configurar atualizações recorrentes. A alteração dessa configuração não altera nenhum agendamento de atualização existente estabelecido por meio do gerenciador de dispositivos do Firewall Seguro.

1 Device Name **FDM_Onboarding**

2 Database Updates Immediately perform security updates, and enable recurring updates.

Databases **Geolocation, Intrusion Rule, VDB, Security Intelligence Feeds**

Schedule **Weekly on Mo at 02:00 AM** [Set Schedule](#)

Next

3 Create Registration Key

4 Smart License

5 Done


Passo 7. Na seção Chave de registro da CLI, o CDO gera automaticamente uma chave de registro. Sair da interface de integração antes da conclusão resulta na criação de um espaço reservado para o dispositivo no Inventário. A chave de registro pode ser recuperada deste local posteriormente, se necessário.

1 Device Name **FDM_Onboarding**

2 Database Updates **Enabled**

3 Create Registration Key

1 Copy registration key

`8M8l6awbQ2s7c864R54e47789702f5fa` 

2 Paste the registration key copied above in the Cloud Services management in FDM. [Learn more](#)

Next

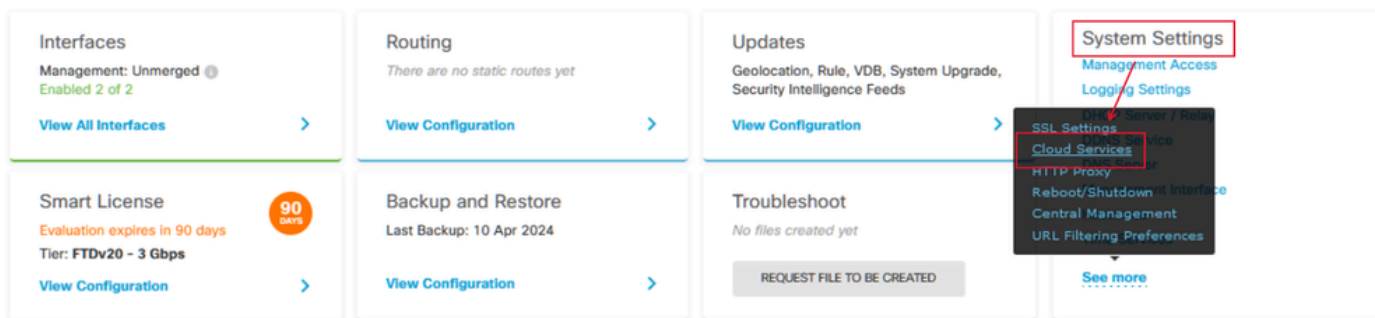
4 Smart License

5 Done

Etapa 8. Utilize o ícone Copiar para copiar a chave de registro gerada.

Etapa 9. Acesse o dispositivo Secure Firewall Device Manager destinado à integração com o CDO.

Etapa 10. Selecione Serviços em nuvem no menu Configurações do sistema.




Etapa 11. Designar a região de nuvem da Cisco correta no menu suspenso Região, alinhando-a com a localização geográfica do locatário:

- Para defensorchestrator.com, selecione US.
- Para defensorchestrator.eu, selecione EU.
- Para apj.cdo.cisco.com, selecione 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? 

Etapa 12. Na seção Tipo de Inscrição, opte pela Conta de Segurança.

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? [?](#)

Etapa 13. Cole a chave de registro no campo Registration Key (Chave 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?

Etapa 14. Para dispositivos na versão 6.7 ou posterior, verifique se o Cisco Defense Orchestrator está habilitado na seção Registro de serviço.

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?

Etapa 15. (Opcional) Revise os detalhes do Cisco Success Network Enrollment. Se não quiser participar, desmarque a caixa de seleção Registrar rede Cisco bem-sucedida.

Etapa 16. Selecione Registrar e aceite o Cisco Disclosure. O Gerenciador de dispositivos do Secure Firewall envia o registro para o 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
85038aebd2b7c06d454e4778972df6fa

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 a Cisco 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**

Etapa 17. De volta ao CDO, na área de criação da chave de registro, escolha Próximo.

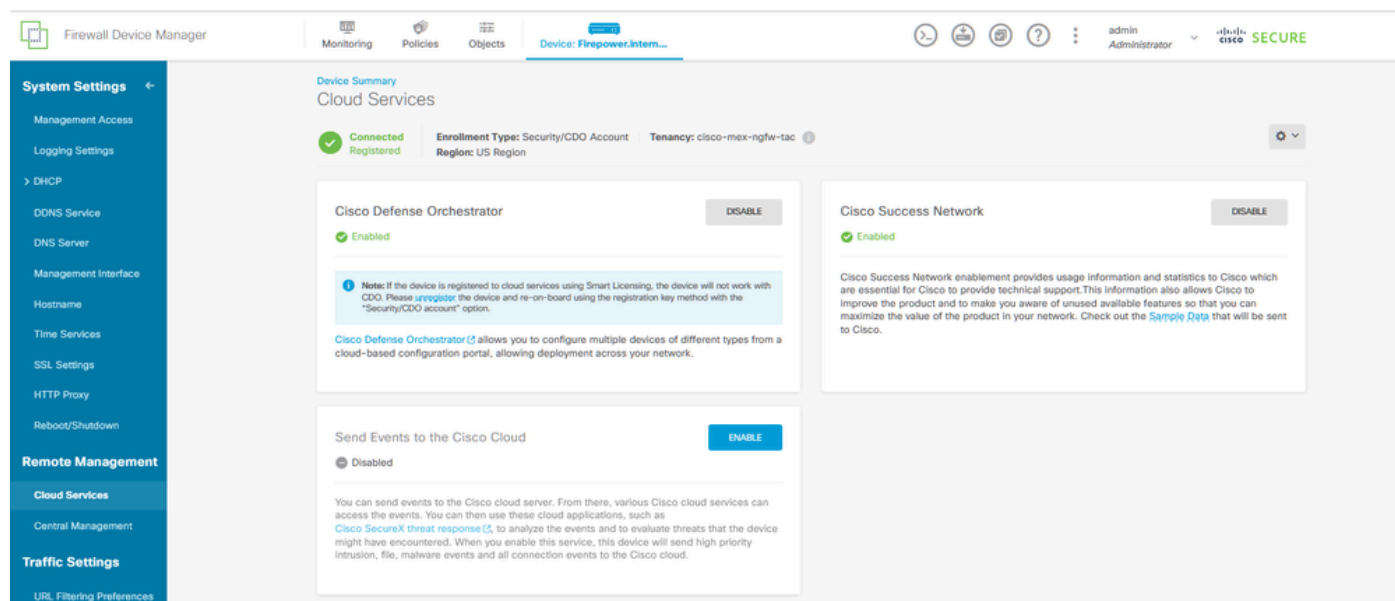
Etapa 18. (Opcional) Identifique e selecione as licenças destinadas ao dispositivo e, em seguida, continue selecionando Avançar.

Etapa 19. Observe o status do dispositivo na transição do Inventário de CDO de Não Provisionado para Localização, depois para Sincronização e, finalmente, para Sincronizado.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Navegue até o portal do CDO e verifique o status do dispositivo, que indica Online e Synced. Além disso, a verificação do status pode ser conduzida por meio da GUI do FDM. Navegue até System > Cloud Services para observar o status da conexão do Cisco Defense Orchestrator e da Cisco Success Network. A interface exibe um status Connected, confirmando a integração bem-sucedida com os serviços.



Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

- Resolução de Falha de FQDN de Serviço de Nuvem

Se o registro do dispositivo falhar devido a uma incapacidade de resolver o FQDN do serviço de nuvem, verifique a conectividade de rede ou a configuração DNS e tente a integração do dispositivo novamente.

- Erro de chave de registro inválida

Quando o registro do dispositivo não for concluído devido à entrada de uma chave de registro inválida no Gerenciador de dispositivos do firewall, continue copiando a chave de registro correta do Cisco Defense Orchestrator e repita o processo de registro. Se o dispositivo já tiver uma smart license, remova-a antes de digitar a chave de registro no Gerenciador de dispositivos de firewall.

- Problema de licença insuficiente

Nos casos em que o status de conectividade do dispositivo indicar "Licença insuficiente", vá para:

1. Aguarde algum tempo para que o dispositivo obtenha a licença, pois o Cisco Smart Software Manager pode exigir um período para aplicar uma nova licença ao dispositivo.
2. Se o status do dispositivo permanecer inalterado, atualize o portal CDO desconectando-se e, em seguida, conectando-se novamente para resolver possíveis problemas de comunicação de rede entre o servidor de licenças e o dispositivo.
3. Se a atualização do portal não atualizar o status do dispositivo, execute estas ações:
 - Gere uma nova chave de registro do [Cisco Smart Software Manager](#) e copie-a. Consulte o vídeo [Gerar Smart Licensing](#) para obter orientação.
 - Na barra de navegação do CDO, selecione a página Inventário.
 - Escolha o dispositivo listado com o estado Licença insuficiente.
 - No painel Device Details (Detalhes do dispositivo), clique em Manage Licenses (Gerenciar licenças) no alerta Insuf Licenses (Licenças insuficientes). A janela Gerenciar licenças é exibida.
 - No campo Ativar, cole a nova chave de registro e selecione Registrar dispositivo.

Depois que a nova chave de registro for aplicada com êxito, o estado de conectividade do dispositivo deverá ser alterado para 'Online'.

Para obter orientação abrangente sobre como registrar o Firepower Device Manager (FDM) usando métodos alternativos à Chave de Registro, consulte a documentação detalhada fornecida no link: [Solução de problemas de dispositivos gerenciados pelo FDM](#).

Este recurso oferece instruções passo a passo e dicas de solução de problemas para diferentes técnicas de registro que podem ser empregadas para integrar com êxito o FDM ao Cisco Defense Orchestrator (CDO).

Informações Relacionadas

- [Identificar e Solucionar Problemas de Dispositivos Gerenciados pelo FDM](#)
- [Gerenciamento de Dispositivos FDM com o Cisco Defense Orchestrator](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.