

FMC 6.6.1+ - Dicas para antes e depois de uma atualização

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Principais coisas a serem feitas antes da atualização do FMC](#)

[Escolha a versão do software de destino do FMC](#)

[Verifique o modelo atual da FMC e a versão do software](#)

[Planejar o caminho de atualização](#)

[Carregar pacotes de atualização](#)

[Crie o backup do FMC](#)

[Verificar a sincronização do NTP](#)

[Verifique o espaço em disco](#)

[Implantar todas as alterações de política pendentes](#)

[Execute as verificações de prontidão do software Firepower](#)

[Principais coisas a serem feitas após a atualização do FMC](#)

[Implantar todas as alterações de política pendentes](#)

[Verifique se o banco de dados de vulnerabilidade e impressão digital mais recente está instalado](#)

[Verifique a versão atual da regra de Snort e do pacote de segurança leve](#)

[Verifique a versão atual da atualização da localização geográfica](#)

[Automatizar a atualização do banco de dados de filtragem de URL com tarefa agendada](#)

[Configurar backups periódicos](#)

[Verifique se a Smart License está registrada](#)

[Revisar a configuração dos conjuntos de variáveis](#)

[Verifique a ativação de serviços de nuvem](#)

[Filtragem de URL](#)

[AMP para redes](#)

[Região de nuvem da Cisco](#)

[Configuração do evento de nuvem da Cisco](#)

[Habilitar integração do SecureX](#)

[Integrar fita SecureX](#)

[Enviar eventos de conexão para SecureX](#)

[Integrar Endpoint Seguro \(AMP para Endpoints\)](#)

[Integre o Secure Malware Analytics \(Threat Grid\)](#)

Introduction

Este documento descreve as práticas recomendadas de verificação e configuração a serem concluídas antes e depois da atualização do Cisco Secure Firewall Management Center (FMC)

para a versão 6.6.1+.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Hardware: Cisco FMC 1000
- Software: Versão 7.0.0 (build 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Principais coisas a serem feitas antes da atualização do FMC

Escolha a versão do software de destino do FMC

Analise as [Notas de Versão do Firepower](#) para a Versão de Destino e conheça:

- Compatibilidade
- Recursos e funcionalidade
- Problemas resolvidos
- Problemas conhecidos

Verifique o modelo atual da FMC e a versão do software

Verifique o modelo atual da FMC e a versão do software:

1. Navegue até **Ajuda > Sobre**.
2. Verifique o **modelo** e a **versão do software**.

The screenshot shows the Cisco FMC 'About' page. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and a search icon. The main content area displays system information:

Model	Cisco Firepower Management Center 1000
Serial Number	WZP2326001X
Software Version	7.0.0 (build 94)
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.10.1 (build 174)
Snort Version	2.9.18 (Build 174)
Snort3 Version	3.1.0.1 (Build 174)
Rule Update Version	2021-09-15-001-vrt
Rulepack Version	2600
Module Pack Version	2961
LSP Version	lsp-rel-20210915-1507
Geolocation Update Version	2021-09-20-002
VDB Version	build 338 (2020-09-24 12:58:48)
Hostname	KSEC-FMC-1600-2

A help menu is open on the right, listing options such as 'Page-level Help', 'How-Tos', 'Documentation on Cisco.com', 'What's New in This Release', 'Software Download', 'Secure Firewall YouTube', 'Secure Firewall on Cisco.com', 'Firepower Migration Tool', 'Partner Ecosystem', 'Ask a Question', 'TAC Support Cases', and 'About'.

Planejar o caminho de atualização

Sujeito à versão atual e à versão do software FMC de destino, uma atualização temporária pode ser necessária. No [Guia de Atualização do Cisco Firepower Management Center](#), analise o **caminho de atualização**: Seção **Firepower Management Centers** e planeje o caminho de atualização.

Carregar pacotes de atualização

Para carregar o pacote de atualização no dispositivo, faça o seguinte:

1. Baixe o pacote de atualização da página [Download de software](#).
2. No FMC, navegue até **System > Updates (Sistema > Atualizações)**.
3. Escolha a **atualização do carregamento**.
4. Clique no botão de opção **Carregar pacote de atualização de software local**.
5. Clique em **Procurar** e escolha o pacote.
6. Clique em **Fazer upload**.

The screenshot shows the 'Product Updates' page in the Cisco FMC interface. The current software version is 7.0.0. The 'Updates' section is active, and the 'Action' is set to 'Upload local software update package'. The 'Package' field contains the file name 'Cisco_Firepower_Mgmt_Center_Patch-7.0.0.1-15.sh.REL.tar'. There are 'Cancel' and 'Upload' buttons at the bottom of the form.

Crie o backup do FMC

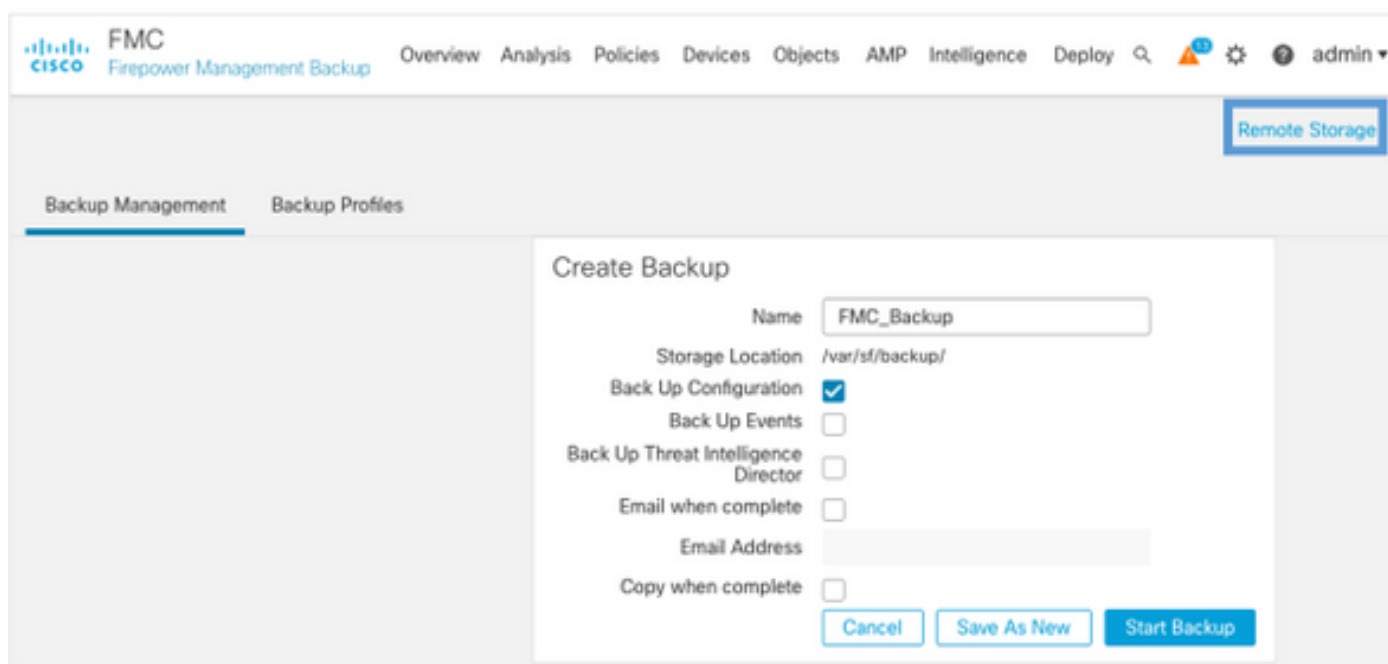
O backup é uma etapa importante de recuperação de desastres, que permite restaurar a configuração se uma atualização falhar catastróficamente.

1. Navegue até **System > Tools > Backup/Restore (Sistema > Ferramentas >**

Backup/Restauração).

2. Escolha o **Firepower Management Backup**.
3. No campo **Nome**, insira o nome de backup.
4. Escolha o local de armazenamento e as informações que devem ser incluídas no backup.
5. Clique em **Iniciar backup**.
6. Em **Notificação > Tarefas**, monitore o progresso da criação do Backup.

Tip: É altamente recomendável fazer o backup em um local remoto seguro e verificar se a transferência foi bem-sucedida. O armazenamento remoto pode ser configurado na página Gerenciamento de backup.



The screenshot displays the Cisco FMC Firepower Management Backup interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', and 'Deploy'. The main content area is titled 'Create Backup' and contains the following fields and options:

- Name:** FMC_Backup
- Storage Location:** /var/sf/backup/
- Back Up Configuration:**
- Back Up Events:**
- Back Up Threat Intelligence Director:**
- Email when complete:**
- Email Address:** (empty field)
- Copy when complete:**

At the bottom of the form are three buttons: 'Cancel', 'Save As New', and 'Start Backup'.

Para obter mais informações, consulte:

- [Guia de Configuração do Firepower Management Center, Versão 7.0 - Capítulo: Backup e restauração](#)
- [Guia de Configuração do Firepower Management Center, Versão 7.0 - Gerenciamento de Armazenamento Remoto](#)

Verificar a sincronização do NTP

Para uma atualização bem-sucedida do FMC, a sincronização do NTP é necessária. Para verificar a sincronização do NTP, faça o seguinte:

1. Navegue até **System > Configuration > Time**.
2. Verifique o **status do NTP**.

Note: Status: "Sendo usado" indica que o aplicativo está sincronizado com o 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 obter mais informações, consulte o [Guia de Configuração do Firepower Management Center, Versão 7.0 - Sincronização de Tempo e Hora](#).

Verifique o espaço em disco

Dependendo do modelo do FMC e da versão de destino, verifique se há espaço livre em disco suficiente disponível, caso contrário a atualização falhará. Para verificar o espaço em disco do FMC disponível, faça o seguinte:

1. Navegue até **System > Health > Monitor**.
2. Escolha o FMC.
3. Expanda o menu e procure **Disk Usage (Uso do disco)**.
4. Os requisitos de espaço em disco podem ser encontrados em [Testes de tempo e requisitos de espaço em disco](#).

The screenshot shows the Cisco FMC Monitor interface. The 'Health Status' section for the FMC device is active. Under 'Monitoring', 'Disk Usage' is selected, showing a warning icon and the text: 'Disk Usage / using 44%: 1.5G (2.0G Avail) of 3.7G see less'. Below this, a table titled 'Local Disk Partition Status' provides details:

Mount	Size	Free	Used	Percent
/	3.7G	2.0G	1.5G	44%
/Volume 1.1T 966G 70G 7%				

Other health items include 'FMC Access Configuration changes on device' which does not apply to this platform.

Implantar todas as alterações de política pendentes

Antes da atualização ou instalação de patches, é necessário implantar alterações nos sensores. Para garantir que todas as alterações pendentes sejam implantadas, faça o seguinte:

1. Navegue até **Implantar > Implantação**.
2. Escolha todos os dispositivos na lista e **Implantar**.

Caution: A coluna Inspeccionar interrupção indica interrupção de tráfego

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
FTD66	admin	Yes	FTD		Sep 13, 2021 1:33 PM		Pending

Traffic interruption needed Sensor with pending deployment

Execute as verificações de prontidão do software Firepower

As verificações de prontidão avaliam a preparação de um Firepower appliance para uma atualização de software.

Para executar as Verificações de prontidão do software, faça o seguinte:

1. Navegue até **System > Updates (Sistema > Atualizações)**.
2. Selecione o ícone **Instalar** ao lado da versão de destino.
3. Escolha o FMC e clique em **Verificar disponibilidade**.
4. Na janela pop-up, clique em **OK**.
5. Monitore o processo de verificação de prontidão em **Notificações > Tarefas**.

The screenshot shows the Cisco FMC 'Upload Update' interface. The 'Product Updates' tab is active, showing the 'Currently running software version: 7.0.0'. A 'Selected Update' box displays the following details:

Type	Cisco Firepower Mgmt Center Patch
Version	7.0.0.1-15
Date	Tue Jul 6 19:27:03 UTC 2021
Reboot	Yes

Below this, a table shows the results of the update check for a device group:

Device Group	Compatibility Check	Readiness Check Results	Readiness Check Completed	Estimated Upgrade Time
FTHC-NGFW-FMC1.proscloud.com 10.62.184.21 - Cisco Firepower Management Center 1000 v7.0.0	Compatibility check passed. Proceed			N/A

Buttons at the bottom include 'Back', 'Check Readiness', and 'Install'.

Para obter mais informações, consulte o [Guia de atualização do Cisco Firepower Management Center - Verificações de prontidão do software Firepower](#).

Principais coisas a serem feitas após a atualização do FMC

Implantar todas as alterações de política pendentes

Imediatamente após cada atualização ou instalação de patches, é necessário implantar alterações nos sensores. Para garantir que todas as alterações pendentes sejam implantadas, faça o seguinte:

1. Navegue até **Implantar > Implantação**.
2. Escolha todos os dispositivos na lista e clique em **Implantar**.

Caution: A coluna Inspeccionar interrupção indica interrupção de tráfego

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
FTD66	admin	Yes	FTD		Sep 13, 2021 1:33 PM		Pending

Traffic interruption needed Sensor with pending deployment

Verifique se o banco de dados de vulnerabilidade e impressão digital mais recente está instalado

Para verificar a versão atual da impressão digital (VDB), faça o seguinte:

1. Navegue até **Ajuda > Sobre**.
2. Verifique a **versão do VDB**.

Para fazer o download das atualizações de VDB diretamente do cisco.com, é necessário o acesso do FMC ao cisco.com.

1. Navegue até **System > Updates > Product Updates (Sistema > Atualizações > Atualizações de produtos)**.
2. Escolha **Baixar atualizações**.
3. Instale a versão mais recente disponível.
4. Você deve reimplantar os sensores depois.

Note: Se o FMC não tiver acesso à Internet, o pacote VDB poderá ser baixado diretamente do software.cisco.com.

É recomendável agendar tarefas para executar downloads e instalações automáticos de pacotes VDB.

Como uma boa prática, procure atualizações de VDB diariamente e instale-as no FMC durante os fins de semana.

Para verificar o VDB diariamente em www.cisco.com, faça o seguinte:

1. Navegue até **Sistema > Ferramentas > Agendamento**.
2. Clique em **Adicionar tarefa**.
3. Na lista suspensa **Tipo de tarefa**, escolha **Download da atualização mais recente**.
4. Para **executar a tarefa Agenda**, clique no botão de opção **Recorrente**.
5. Repita a tarefa todos os dias e execute-a às 3:00 da manhã ou fora do horário comercial.
6. Para **Atualizar itens**, marque a caixa de seleção **Banco de dados de vulnerabilidade**.

New Task

Job Type

Schedule task to run Once Recurring

Start On Europe/Warsaw

Repeat Every Hours Days Weeks Months

Run At

Job Name

Update Items Software Vulnerability Database

Comment

Email Status To

Para instalar o VDB mais recente no FMC, defina a tarefa periódica semanalmente:

1. Navegue até **Sistema > Ferramentas > Agendamento**.
2. Clique em **Adicionar tarefa**.
3. Na lista suspensa **Tipo de tarefa**, escolha **Instalar última atualização**.
4. Para **executar a tarefa de agendamento**, clique no botão de opção **Recorrente**.
5. Repita a tarefa a cada 1 semana e execute-a às 5:00 da manhã ou fora do horário comercial.
6. Para **Atualizar itens**, marque a caixa de seleção **Banco de dados de vulnerabilidades**.

New Task

Job Type

Schedule task to run Once Recurring

Start On Europe/Warsaw

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Update Items Software Vulnerability Database

Device

Comment

Email Status To

Para obter mais informações, consulte [Firepower Management Center Configuration Guide, Version 7.0 - Update the Vulnerability Database \(VDB\)](#)

Verifique a versão atual da regra de Snort e do pacote de segurança leve

Para verificar as versões atuais de SRU (Snort Rule, regra de Snort), Lightweight Security Package (LSP) e Geolocation, faça o seguinte:

1. Navegue até **Ajuda > Sobre**.
2. Verifique a **versão de atualização de regra** e a **versão LSP**.

Para baixar a SRU e o LSP diretamente de www.cisco.com, a acessibilidade do FMC para www.cisco.com é necessária.

1. Navegue até **System > Updates > Rule Updates**.
2. Na guia **One-Time Rule Update/Rules Import**, escolha **Download new rule update from the Support Site**.
3. Escolha **Importar**.
4. Implante a configuração para os sensores depois.

Note: Se o FMC não tiver acesso à Internet, os pacotes SRU e LSP podem ser baixados diretamente do software.cisco.com.

As atualizações da regra de intrusão são cumulativas e é recomendável sempre importar a atualização mais recente.

Para ativar o download e a implantação semanais de atualizações de regras de snort (SRU/LSP), faça o seguinte:

1. Navegue até **System > Updates > Rule Updates**.
2. Na guia **Importação de Atualização Recorrente de Regras**, marque a caixa de seleção **Ativar Importação de Atualização Recorrente de Regras do Site de Suporte**.
3. Escolha a frequência de importação como semanal, escolha um dia da semana e tarde para o download e a implantação de políticas.
4. Click **Save**.

Recurring Rule Update Imports

The scheduled rule update has not yet run.
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site

Import Frequency: Weekly on Monc at 10:00 PM Europe/Warsaw

Policy Deploy Deploy updated policies to targeted devices after rule update completes

Cancel Save

Para obter mais informações, consulte o [Guia de configuração do Firepower Management Center, Versão 7.0 - Atualizar regras de intrusão](#).

Verifique a versão atual da atualização da localização geográfica

Para verificar a versão atual da localização geográfica, faça o seguinte:

1. Navegue até **Ajuda > Sobre**.
2. Verifique a **versão da atualização da localização geográfica**.

Para fazer o download das atualizações da localização geográfica diretamente em www.cisco.com, é necessário o acesso do FMC a www.cisco.com.

1. Navegue até **System > Updates > Geolocation Updates**.
2. Na guia **One-Time Geolocation Update**, escolha **Download and install geolocation update from the Support Site**.
3. Clique em **Importar**.

Note: Se o FMC não tiver acesso à Internet, o pacote de atualizações de localização geográfica poderá ser baixado diretamente do software.cisco.com.

Para ativar as Atualizações automáticas de localização geográfica, faça o seguinte:

1. Navegue até **System > Updates > Geolocation Updates**.
2. Na seção **Atualizações de localização geográfica recorrentes**, marque a caixa de seleção **Ativar atualizações semanais recorrentes no site de suporte**.
3. Escolha a frequência de importação como semanal, escolha segunda-feira à meia-noite.
4. Click **Save**.

Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site

Update Start Time Europe/Warsaw

Para obter mais informações, consulte [Firepower Management Center Configuration Guide, Version 7.0 - Update the Geolocation Database \(GeoDB\)](#).

Automatizar a atualização do banco de dados de filtragem de URL com tarefa agendada

Para garantir que os dados de ameaças para filtragem de URL sejam atuais, o sistema deve obter atualizações de dados da nuvem Cisco Collective Security Intelligence (CSI). Para automatizar esse processo, siga estas etapas:

1. Navegue até **Sistema > Ferramentas > Agendamento**.
2. Clique em **Adicionar tarefa**.
3. Na lista suspensa **Tipo de tarefa**, escolha **Atualizar banco de dados de filtragem de URL**.
4. Para **executar a tarefa Programar**, clique no botão de opção **Recorrente**.
5. Repita a tarefa todas as semanas e execute-a às 20:00 horas aos domingos ou fora do horário comercial.
6. Click **Save**.

New Task

Job Type

Schedule task to run Once Recurring

Start On Europe/Warsaw

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Comment

Email Status To

Para obter mais informações, consulte o [Guia de Configuração do Firepower Management Center, Versão 7.0 - Automatização de Atualizações de Filtragem de URL com uma Tarefa Agendada](#).

Configurar backups periódicos

Como parte do plano de recuperação de desastres, recomenda-se executar backups periódicos.

1. Certifique-se de estar no **domínio global**.
2. Crie o perfil de backup do FMC. Para obter mais informações, consulte a seção **Criar o FMC Backup**.
3. Navegue até **Sistema > Ferramentas > Agendamento**.
4. Clique em **Adicionar tarefa**.
5. Na lista suspensa **Tipo de tarefa**, escolha **Backup**.
6. Para **executar a tarefa Programar**, clique no botão de opção **Recorrente**.
A frequência de backup deve ser ajustada de acordo com as necessidades da organização. Recomendamos criar backups durante uma janela de manutenção ou outro período de baixo uso.
7. Para **Tipo de backup**, clique no botão de opção **Centro de gerenciamento**.
8. Na lista suspensa **Perfil de backup**, escolha o Perfil de backup.
9. Click **Save**.

New Task

Job Type: Backup

Schedule task to run: Once Recurring

Start On: September 24, 2021 UTC

Repeat Every: 1 Hours Days Weeks Months

Run At: 11:00 Pm

Repeat On: Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name: FMC_weekly_backup

Backup Type: Management Center Device

Backup Profile: Backup_FMC

Comment: This tasks creates FMC weekly backup

Email Status To: admin@acme.com

Cancel Save

Para obter mais informações, consulte o [Guia de Configuração do Firepower Management Center, Versão 7.0 - Capítulo: Backup e restauração](#).

Verifique se a Smart License está registrada

Para registrar o Cisco Firewall Management Center com o Cisco Smart Software Manager, faça o

seguinte:

1. Em <https://software.cisco.com>, navegue para **Gerenciador Inteligente de Software > Gerenciar licenças**.
2. Navegue até **Inventário > guia Geral** e crie um **Novo token**.
3. Na IU da FMC, navegue até **System > Licenses > Smart Licenses (Sistema > Licenças > Licenças inteligentes)**.
4. Clique em **Registrar**.
5. Insira o token gerado no portal Cisco Smart Software Licensing.
6. Certifique-se de que a **Rede de Êxito da Cisco** esteja habilitada.
7. Clique em **Aplicar alterações**.
8. Verifique O Status Da Smart License.

Smart Licensing Product Registration

Product Instance Registration Token:

`MGI0ZGJhNTEtOTIxYy00ZGM2LWJjMTctNWE1ZTY5YWUxZGExLTE2NjQwMTUz%0AMDQ0OTZ8bTQxTWJDbmJJWVld3hQMGS4bytHdU4wVzNvRWRZM1pjbk.J4Nkcr%0A!`

If you do not have your ID token, you may copy it from your Smart Software manager under the assigned virtual account. [Cisco Smart Software Manager](#)

The Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco. Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the device from the cloud.

Cisco Success Network

The Cisco Success Network provides usage information and statistics to Cisco. This information 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.

Enable Cisco Success Network

Cisco Support Diagnostics

The Cisco Support Diagnostics capability provides entitled customers with an enhanced support experience by allowing Cisco TAC to collect essential information from your devices during the course of a TAC case. Additionally, Cisco will periodically collect configuration

Internet connection is required.

Cancel Apply Changes

Para obter mais informações, consulte o [Guia de Configuração do Firepower Management Center, Versão 7.0 - Registrar Licenças inteligentes](#).

Revisar a configuração dos conjuntos de variáveis

Certifique-se de que a variável HOME_NET contenha apenas as redes/sub-redes internas na organização. A definição incorreta do conjunto de variáveis afeta negativamente o desempenho do firewall.

1. Navegue até **Objetos > Conjunto de variáveis**.
2. Edite o conjunto de variáveis usado pela sua política de invasão. É permitido ter uma variável definida por política de intrusão com configurações diferentes.
3. Ajuste as variáveis de acordo com o ambiente e clique em **Salvar**.

Outras variáveis de interesse são DNS_SERVERS OU HTTP_SERVERS.

Para obter mais informações, consulte o [Guia de Configuração do Firepower Management Center, Versão 7.0 - Conjuntos de Variáveis](#).

Verifique a ativação de serviços de nuvem

Para aproveitar os diferentes serviços de nuvem, navegue até **System > Integration > Cloud Services**.

Filtragem de URL

1. Habilite a filtragem de URL e permita atualizações automáticas; ative a opção Consultar Cisco Cloud para URLs desconhecidas.
A expiração mais frequente de URL de cache requer mais consultas à nuvem, o que resulta em cargas da Web mais lentas.
2. **Salve as alterações.**

Tip: Para expiração de URL de cache, deixe o padrão **Nunca**. Se for necessária uma reclassificação mais rigorosa da Web, essa configuração poderá ser modificada de acordo.

AMP para redes

1. Verifique se ambas as configurações estão ativadas: **Ative as atualizações automáticas locais de detecção de malware e compartilhe URI de eventos de malware com a Cisco**.
2. No FMC 6.6.X, desative o uso da porta 32137 legada para AMP para redes, de modo que a porta TCP usada seja 443.
3. **Salve as alterações.**

Note: Essa configuração não está mais disponível no FMC 7.0+ e a porta é sempre 443.

Região de nuvem da Cisco

1. A região da nuvem precisa corresponder à região da empresa SecureX. Se a organização SecureX não for criada, escolha a região mais próxima à instalação da FMC: região da APJ, região da UE ou região dos EUA.
2. **Salve as alterações.**

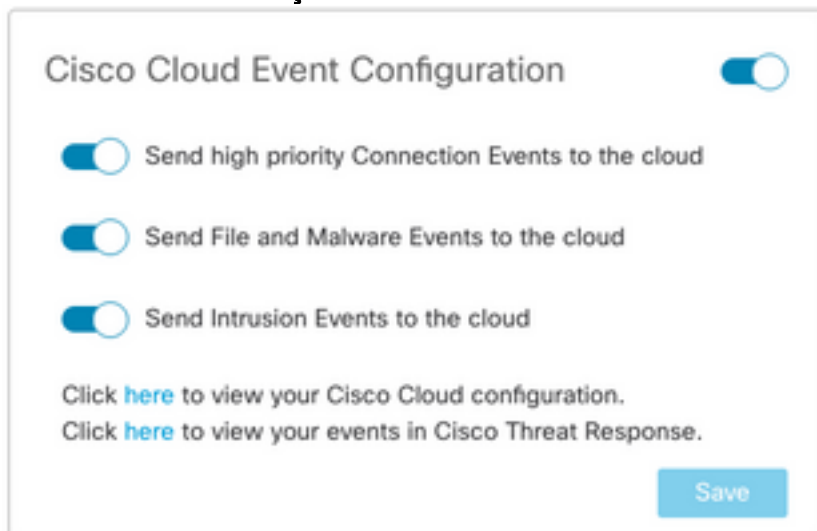
Configuração do evento de nuvem da Cisco

Para FMC 6.6.x

1. Verifique todas as três opções: **Envie eventos de conexão de alta prioridade para a nuvem**,

envie arquivos e eventos de malware para a nuvem e envie eventos de intrusão para a nuvem são escolhidos.

2. Salve as alterações.



Cisco Cloud Event Configuration

Send high priority Connection Events to the cloud

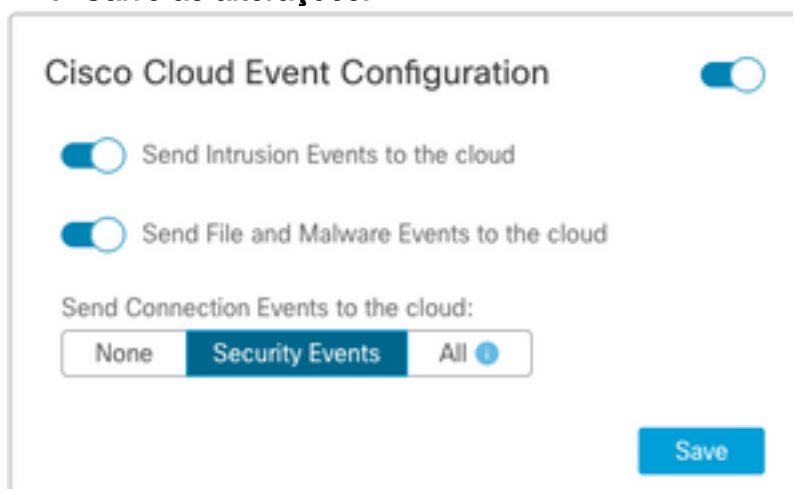
Send File and Malware Events to the cloud

Send Intrusion Events to the cloud

Click [here](#) to view your Cisco Cloud configuration.
Click [here](#) to view your events in Cisco Threat Response.

Para o FMC 7.0+

1. Verifique se ambas as opções foram escolhidas: **Envie eventos de invasão para a nuvem e envie arquivos e eventos de malware para a nuvem.**
2. Para o tipo de evento de conexão, escolha **All** se a solução Security Analytics and Logging estiver em uso. Para o SecureX, escolha apenas **Eventos de Segurança.**
3. **Salve as alterações.**



Cisco Cloud Event Configuration

Send Intrusion Events to the cloud

Send File and Malware Events to the cloud

Send Connection Events to the cloud:

Habilitar integração do SecureX

A integração do SecureX oferece visibilidade instantânea do cenário de ameaças em todos os seus produtos de segurança da Cisco. Para conectar o SecureX e ativar a fita, siga estas etapas:

Integrar fita SecureX

Note: Esta opção está disponível para o FMC versão 7.0+.

1. Efetue login no SecureX e crie um cliente API: No campo **Nome do cliente**, insira um nome descritivo do FMC. Por exemplo, FMC 7.0 API Client. Clique na guia **Oauth Code Clients**. Na

lista suspensa **Cliente predefinido**, escolha **Friso**. Ele escolhe os escopos: Casebook, Enrich:read, Global Intel:read, Inspect:read, Notification, Orbital, Private Intel, Profile, Response, Telemetry:write. Adicione os dois URLs de redirecionamento apresentados no FMC:

URL de redirecionamento: <FMC_URL>/securex/oauth/callback

Segundo URL de redirecionamento: <FMC_URL>/securex/testcallback

1. Na lista suspensa **Disponibilidade**, escolha **Organização**. Clique em **Adicionar novo cliente**.

Add New Client with 10 scopes ✕

Client Name*

Client Preset
 ✕ ▾

API Clients OAuth Code Clients

Scopes* [Select All](#)

🔍

<input checked="" type="checkbox"/> Response	List and execute response actions using configured modules
<input type="checkbox"/> SSE	SSE Integration. Manage your Devices.
<input checked="" type="checkbox"/> Telemetry:write	collect application data for analytics - Write Only
<input type="checkbox"/> Users	Manage users of your organisation
<input type="checkbox"/> Webhook	Manage your Webhooks

Redirect URL*

Redirect URL* Delete

Add another Redirect URL

Availability*
 ▾

Description

2. No FMC, navegue até **System > SecureX**.

3. Ative a alternância no canto superior direito e confirme se a região mostrada corresponde à empresa SecureX.


4. Copie o **ID do cliente** e a **senha do cliente** e cole-os no FMC.

5. Escolha **testar a configuração**.
6. Faça login no SecureX para autorizar o cliente API.
7. Salve as alterações e atualize o navegador para ver a faixa de opções exibida na parte inferior.
8. Expanda a faixa de opções e escolha **Get SecureX**. Insira as credenciais do SecureX, se solicitado.
9. A fita SecureX agora está totalmente funcional para o usuário do FMC.

SecureX Configuration

This feature allows FMC to integrate with other SecureX services via SecureX ribbon.

Follow these steps to configure SecureX

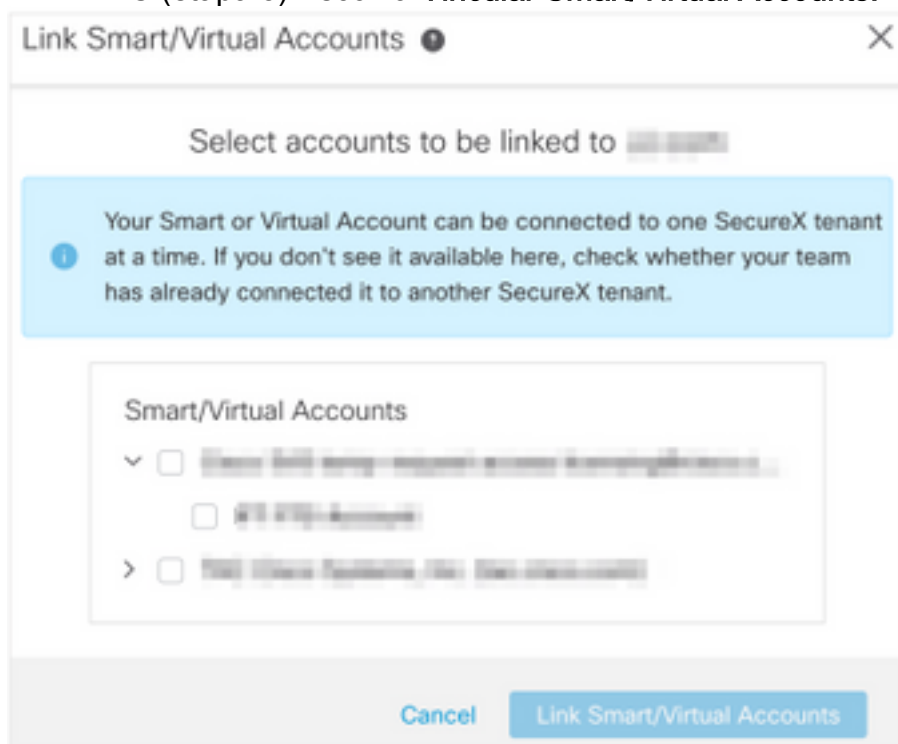
1. Confirm your cloud region
Currently selected region: `api-sse.cisco.com`
To change the cloud region, go to [System / Integration / Cloud Services](#).
2. [Create a SecureX API client](#) 
Copy and paste the URL below into the "Redirect URL" field:
[Copy to Clipboard](#)
`https://10.62.184.21/securex/oauth/callback`
Then click on "Add another Redirect URL" and copy and paste the URL below:
[Copied](#)
`https://10.62.184.21/securex/testcallback`
3. Enter the Client ID and password
Client ID
Client Password
 Show Password

5YVPsGdzrkX8q0yYI-tDitezO6p_17MtH6NATx68fUZ5u9T3qOEq

Note: Se qualquer outro usuário do FMC exigir acesso à faixa de opções, esse usuário precisará fazer login na faixa de opções com credenciais do SecureX.

Enviar eventos de conexão para SecureX

1. No FMC, navegue para **System > Integration > Cloud Services** e certifique-se de que a **Cisco Cloud Event Configuration** envie eventos de intrusão, arquivo e malware, conforme explicado na seção **Turn on Cloud Services**.
2. Verifique se o FMC está registrado com uma Smart License, conforme explicado na seção **Registrar as Smart Licenses**.
3. Anote o nome da **conta virtual atribuída**, conforme exibido na FMC em **System > Licenses > Smart Licenses**.
4. Registre o FMC no SecureX: No SecureX, navegue para **Administration > Devices**. Escolha **Gerenciar dispositivos**. Verifique se as janelas pop-up são permitidas no navegador. Faça login no Security Services Exchange (SSE). Navegue até o **menu Ferramentas > Vincular Smart/Virtual Accounts**. Escolha **Vincular mais contas**. Selecione a conta virtual atribuída ao FMC (etapa 3). Escolha **Vincular Smart/Virtual Accounts**.



- Verifique se o dispositivo FMC está listado nos Dispositivos.
 - Navegue até a guia **Cloud Services**, ative os recursos **de resposta a ameaças do Cisco SecureX e Eventos**.
 - Escolha as **configurações de serviço adicionais** (ícone da engrenagem) ao lado do recurso **Eventos**.
 - Na guia **Geral**, escolha **Compartilhar dados de eventos com Talos**.
 - Na guia **Promover automaticamente eventos**, na seção **Por tipo de evento**, escolha todos os tipos de eventos disponíveis e **Salvar**.
5. No portal SecureX principal, navegue para **Integration Modules > Firepower** e adicione o módulo de integração do Firepower.
 6. Crie um novo painel.
 7. Adicione os blocos relacionados ao Firepower.

Integrar Endpoint Seguro (AMP para Endpoints)

Para habilitar a integração do Secure Endpoint (AMP para endpoints) com a implantação do

Firepower, siga estas etapas:

1. Navegue até **AMP > AMP Management**.
2. Escolha **Add AMP Cloud Connection**.
3. Escolha a nuvem e **registre-se**.

Note: O status **Habilitado** significa que a conexão com a nuvem é estabelecida.

Integrar Secure Malware Analytics (Threat Grid)

Por padrão, o Firepower Management Center pode se conectar à nuvem pública do Cisco Threat Grid para envio de arquivos e recuperação de relatórios. Não é possível excluir esta conexão. No entanto, é recomendável escolher o mais próximo da nuvem de implantação:

1. Navegue até **AMP > Dynamic Analysis Connections**.
2. Clique em **Editar** (ícone do lápis) na seção **Ação**.
3. Escolha o nome de nuvem correto.
4. Para associar a conta do Threat Grid para relatórios detalhados e funcionalidades avançadas do sandbox, clique no ícone **Associar**.

Para obter mais informações, consulte o [Guia de Configuração do Firepower Management Center, Versão 7.0 - Habilitando o Acesso aos Resultados de Análise Dinâmica na Nuvem Pública](#).

Para a integração do dispositivo Threat Grid no local, consulte [Guia de Configuração do Firepower Management Center, Versão 7.0 - Dynamic Analysis On-Premises Appliance \(Cisco Threat Grid\)](#).