

Atualização do Secure Firewall Threat Defense Fusing Firewall Device Manager

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Antes de Começar](#)

[Configurar](#)

[Validação](#)

Introdução

Este documento descreve um exemplo de atualização do Cisco Secure Firewall Threat Defense (FTD) usando o Gerenciador de Dispositivos de Firewall (FDM).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Não há requisitos específicos para este guia

Componentes Utilizados

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

- Cisco Firepower 4125 executando o FTD versão 7.2.3

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

Os requisitos específicos deste documento incluem:

- Conectividade com o IP de gerenciamento do FTD
- O pacote de atualização do FTD (**.REL.tar**) baixado anteriormente do Software Cisco Portal

Este procedimento de atualização é compatível com dispositivos:

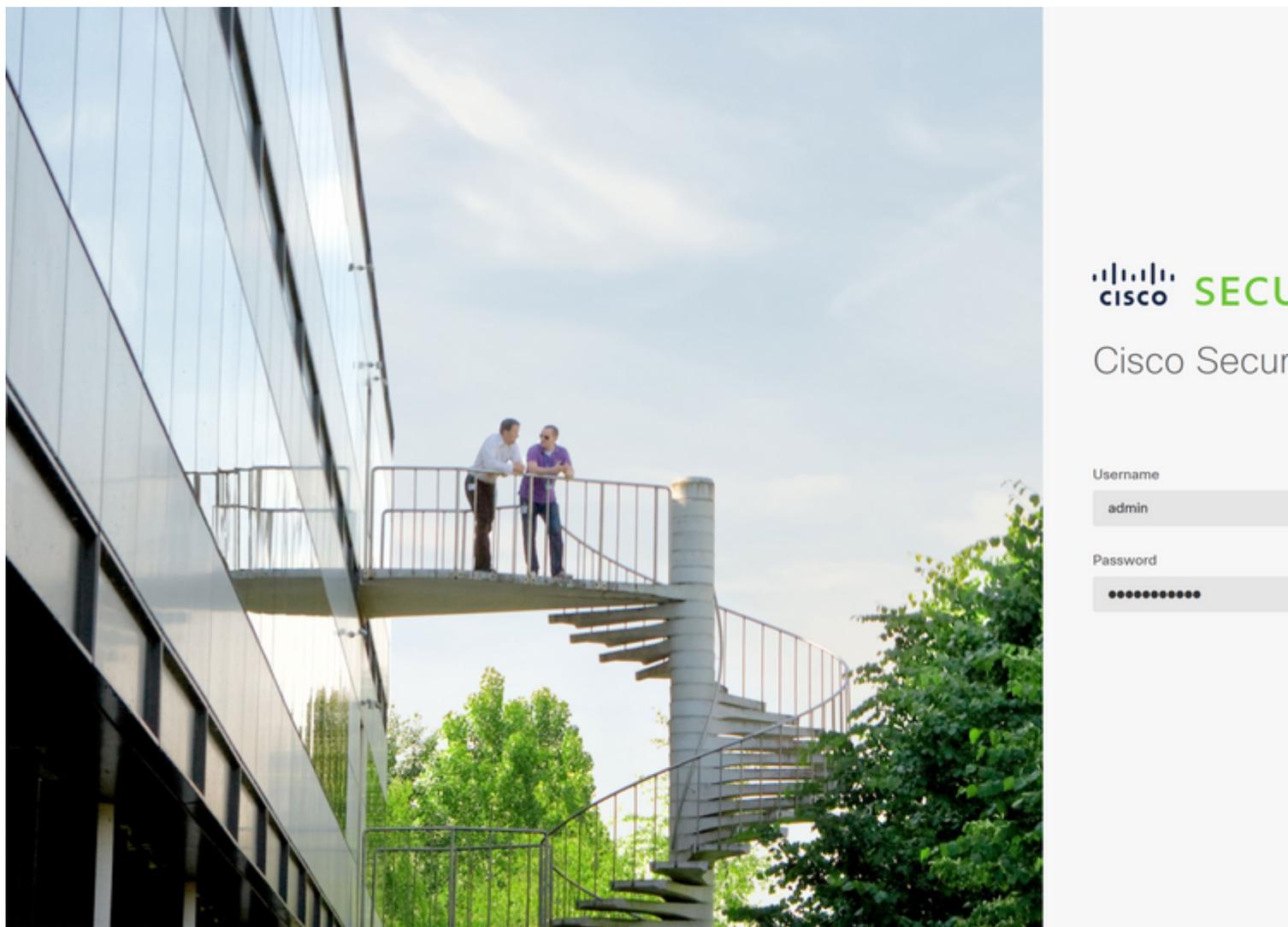
- Qualquer modelo do Cisco Firepower executando o software FTD configurado com gerenciamento local.

Antes de Começar

1. Crie e baixe um backup das Configurações de FTD.
2. Valide o [caminho de atualização](#) para a versão de destino.
3. Faça o download do pacote de atualização do [Cisco Software Central](#).
4. Não renomeie o arquivo de atualização. O sistema considera os arquivos renomeados como inválidos.
5. Programe uma janela de manutenção para o procedimento de atualização porque o tráfego é afetado.

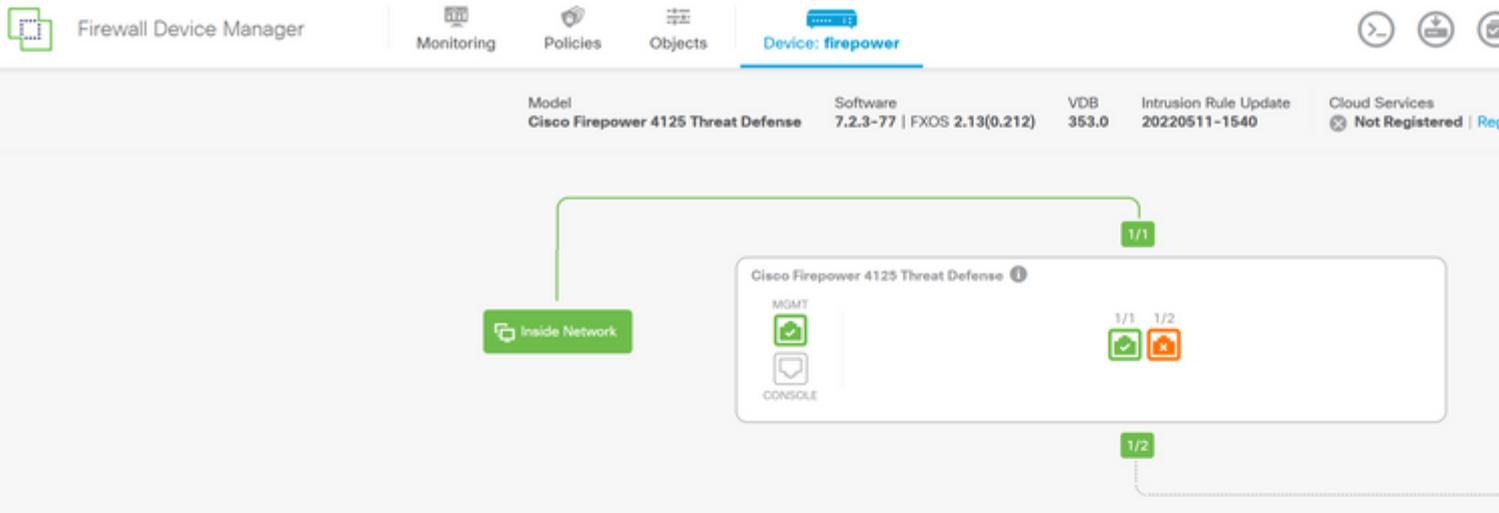
Configurar

Etapa 1. Faça login no Gerenciador de dispositivos de firewall usando o IP de gerenciamento do FTD:



© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions: 2.0 and 3.0". ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2.0 or later".

Etapa 2. Clique em **View Configuration** no painel do Gerenciador de dispositivos de firewall:



Interfaces Connected Enabled 3 of 3 View All Interfaces	Routing <i>There are no static routes yet</i> View Configuration	Updates Geolocation, Rule, VDB, System Up Security Intelligence Feeds View Configuration
Smart License Evaluation expires in 90 days View Configuration	Backup and Restore View Configuration	Troubleshoot <i>No files created yet</i> REQUEST FILE TO BE CREATED
Site-to-Site VPN <i>There are no connections yet</i> View Configuration	Remote Access VPN Requires RA VPN license No connections 1 Group Policy Configure	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration

Etapa 3. Clique no botão Procurar na seção Atualização do sistema para carregar o pacote de instalação:



Device Summary

Updates

Geolocation 2022-05-11-103

Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD



VDB 353.0

Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Security Intelligence Feeds

Configure
Set recurring updates

UPDATE FROM CLOUD

System Upgrade

Current version threat defense: 7.2.3-77 | Current version FXOS: 2.13(0.212)

ImportantMake sure the threat defense version is compatible with the FXOS version.
[Learn more](#)*There are no software upgrades available on the system.**Upload an upgrade file to install.*

BROWSE



Intrusion Rule 20220511-15

Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Cuidado: depois que você carregar o pacote de atualização, o **BROWSE** exibirá uma animação enquanto o arquivo ainda estiver sendo carregado. Não atualize a página da Web até que o carregamento seja concluído.

Exemplo de página de progresso de upload:

Firewall Device Manager

Monitoring Policies Objects Device: firepower

Device Summary Updates

Geolocation 2022-05-11-103
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

VDB 353.0
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Security Intelligence Feeds

Configure
Set recurring updates

UPDATE FROM CLOUD

System Upgrade
Current version threat defense: 7.2.3-77 | Current version FXOS: 2.13(0.212)

Important
Make sure the threat defense version is compatible with the FXOS version.
[Learn more](#)

There are no software upgrades available on the system.
Upload an upgrade file to install.

Cisco_FTD_SSP_Upgrade-7.2.4-165.REL.tar

Intrusion Rule 20220511-154
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Etapa 4. Quando o upload for concluído, uma janela pop-up será exibida solicitando confirmação:

Firewall Device Manager

Monitoring Policies Objects Device: fire

Device Summary Updates

Geolocation 2022-05-11-103
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

VDB 353.0
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Security Intelligence Feeds

Configure
Set recurring updates

UPDATE FROM CLOUD

System Upgrade
Current version threat defense: 7.2.3-77 | Current version FXOS: 2.13(0.212)

Important
Make sure the threat defense version is compatible with the FXOS version.
[Learn more](#)

File	Upload Date	Action
Cisco_FTD_SSP_Upgrade-7.2.4-165.s...	19 Jul 2023 11:49 AM	Replace file

Upgrade to: 7.2.4-165

Readiness Check: **Not Performed Yet** [Run Upgrade Readiness Check](#)

UPGRADE NOW **Reboot required**

Intrusion Rule 20220511-154
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Confirmation

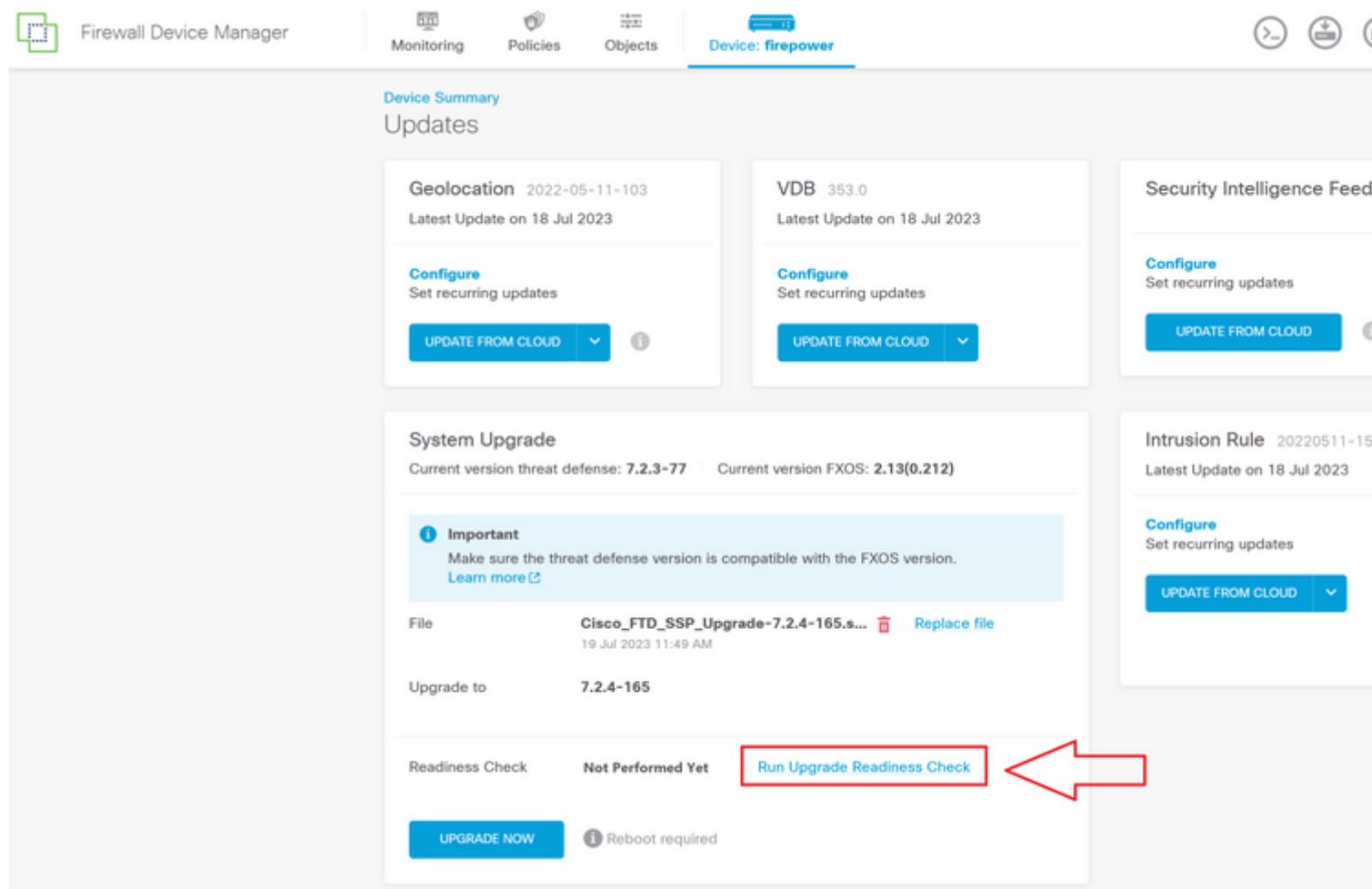
The uploaded file will be staged for later installation. If you want to run the upgrade immediately, select the option below.

Run Upgrade immediately on upload

CANCEL OK

Observação: você pode marcar a opção **Executar atualização imediatamente no upload** no caso de você desejar continuar diretamente com a atualização, no entanto, observe que isso vai ignorar a Verificação de preparação, que pode fornecer insights sobre conflitos na atualização evitando uma falha.

Etapa 5. Clique em **Executar Verificação de Preparação para Atualização** para executar uma pré-validação na atualização para evitar uma falha de atualização:



The screenshot displays the 'Firewall Device Manager' interface for a device named 'firepower'. The 'Updates' section is active, showing various update cards for Geolocation, VDB, Security Intelligence Feeds, and Intrusion Rules. The 'System Upgrade' section is the primary focus, displaying the current version (7.2.3-77) and the target version (7.2.4-165). An important message states: 'Make sure the threat defense version is compatible with the FXOS version.' Below this, a table shows the upgrade file: 'Cisco_FTD_SSP_Upgrade-7.2.4-165.s...' with a 'Replace file' option. The 'Readiness Check' status is 'Not Performed Yet', and a red box highlights the 'Run Upgrade Readiness Check' button, which is pointed to by a red arrow. An 'UPGRADE NOW' button is also visible, with a note that a 'Reboot required'.

Observação: você pode validar se a Verificação de preparação foi concluída com êxito na Lista de tarefas.

Exemplo de uma verificação de preparação bem-sucedida:

The screenshot shows the Firewall Device Manager interface. A 'Task List' modal window is open, displaying a table of tasks. The table has columns for Name, Start Time, End Time, and Status. One task, 'Upgrade Readiness', is listed with a start time of 19 Jul 2023 11:52 AM and an end time of 19 Jul 2023 11:54 AM. The status is 'Upgrade Readiness Check Completed Successfully'. The background shows the 'System Upgrade' section with a 'UPGRADE NOW' button and a 'Reboot required' notification.

Name	Start Time	End Time	Status
Upgrade Readiness	19 Jul 2023 11:52 AM	19 Jul 2023 11:54 AM	Upgrade Readiness Check Completed Successfully

Etapa 6. Clique no botão ATUALIZAR AGORA para continuar com a atualização do software:

Device Summary

Updates

Geolocation 2022-05-11-103
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

VDB 353.0
Latest Update on 18 Jul 2023

Configure
Set recurring updates

UPDATE FROM CLOUD

Security Intelligence Feed

Configure
Set recurring updates

UPDATE FROM CLOUD

System Upgrade

Current version threat defense: **7.2.3-77** Current version FXOS: **2.13(0.212)**

Important
Make sure the threat defense version is compatible with the FXOS version.
[Learn more](#)

File Cisco_FTD_SSP_Upgrade-7.2.4-165.s... [Replace file](#)
19 Jul 2023 11:49 AM

Upgrade to 7.2.4-165

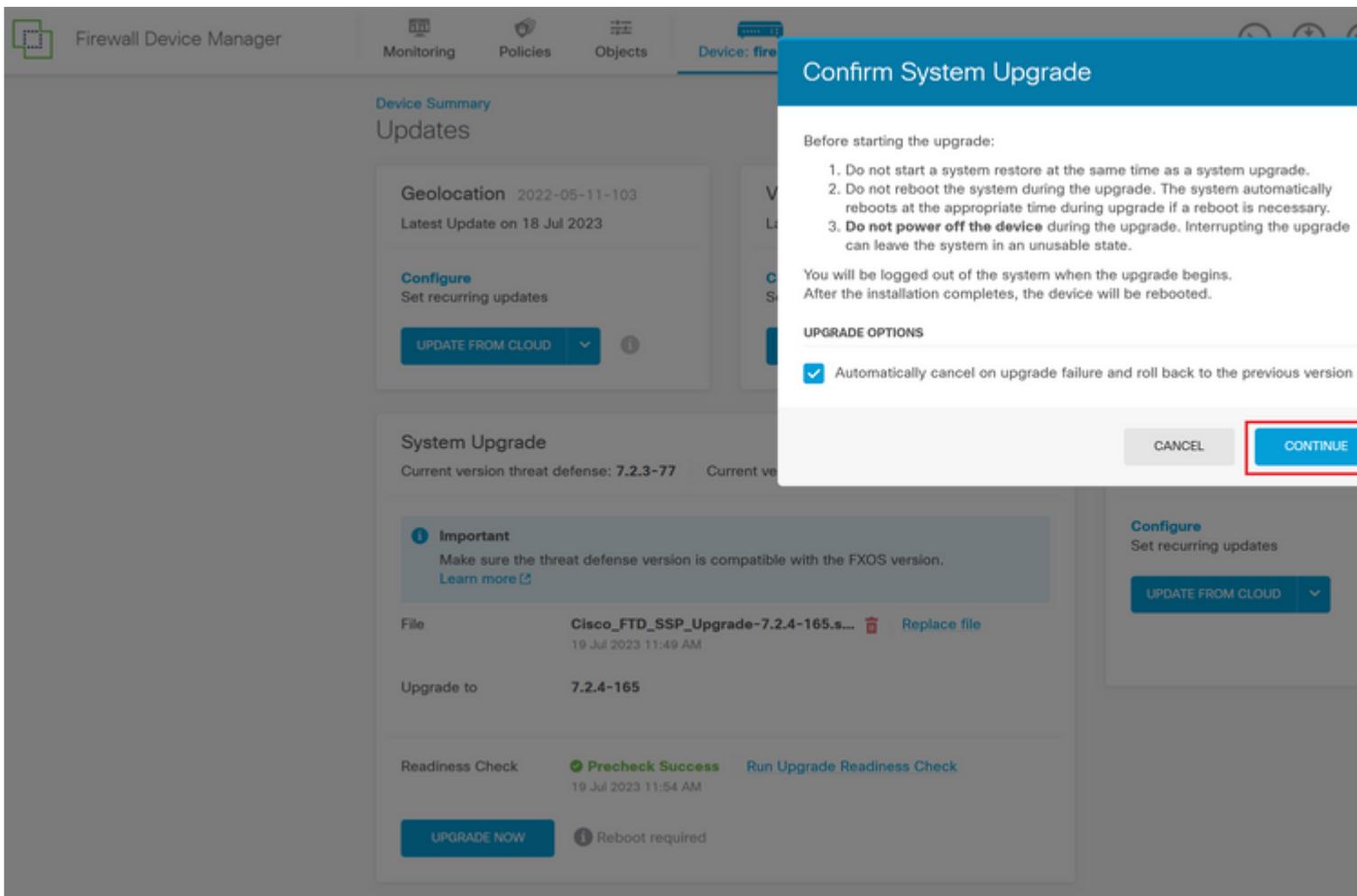
Readiness Check ✔ Precheck Success [Run Upgrade Readiness Check](#)
19 Jul 2023 11:54 AM



UPGRADE NOW

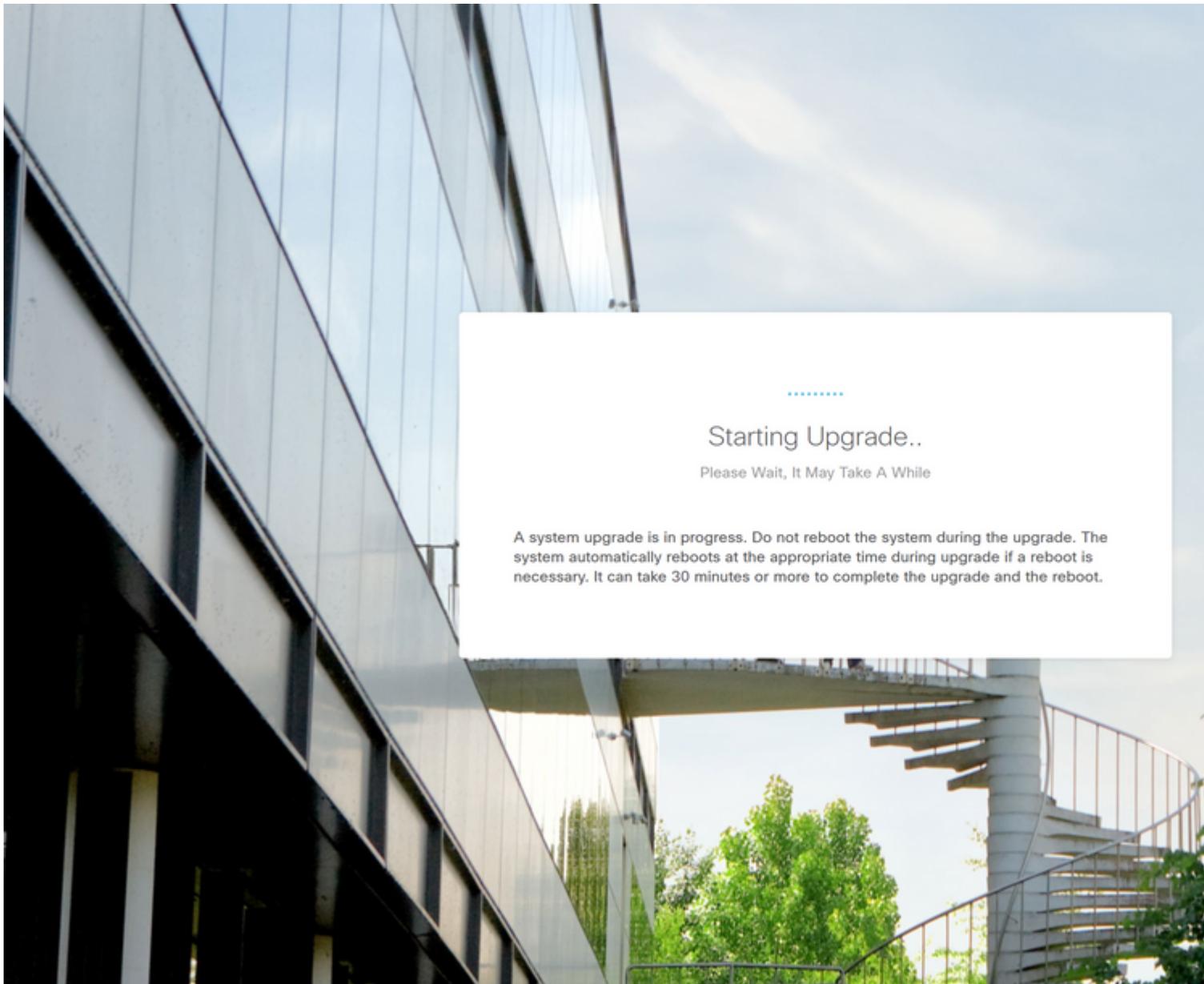
Reboot required

Passo 7. Na janela pop-up, selecione CONTINUAR para continuar a atualização:

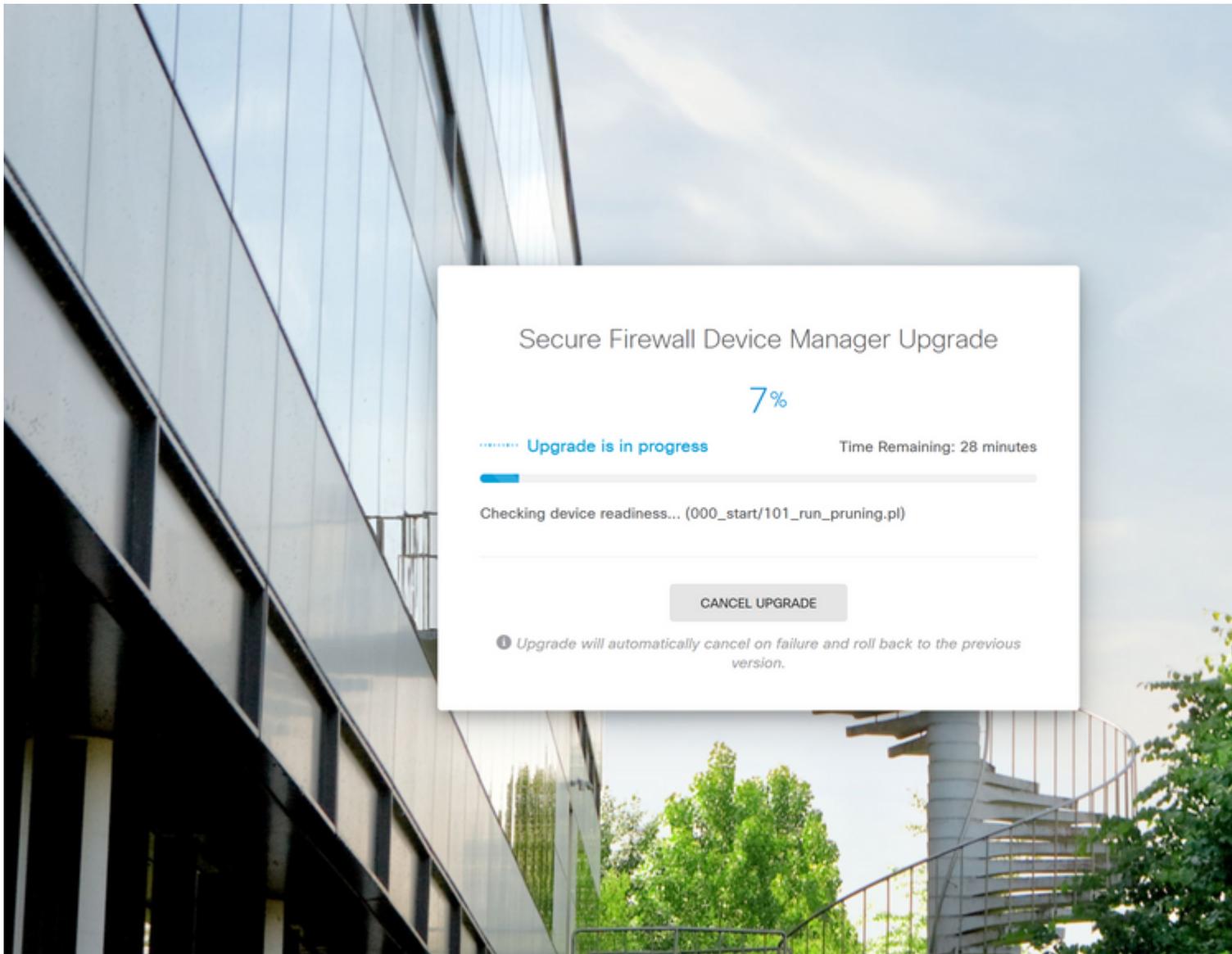


Observação: a opção de reversão está ativada por padrão, sugerimos que você mantenha essa opção para reverter qualquer configuração de atualização em caso de problema no upgrade.

Etapa 8. Você será redirecionado para uma página onde o progresso da atualização será exibido:

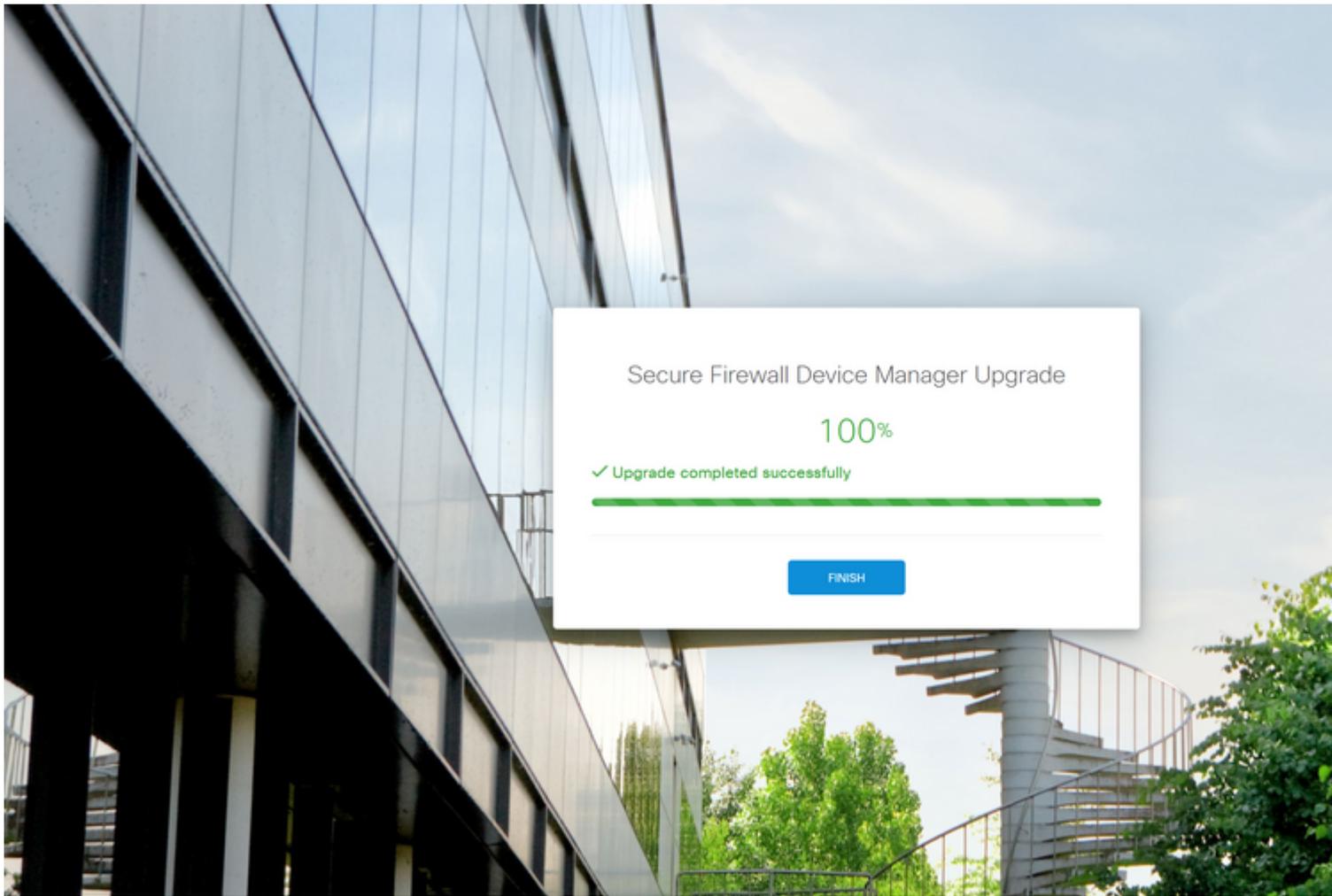


Exemplo da página de andamento:



© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc.
This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, [version 2](#), [version 2.1](#) and [version 3](#)".

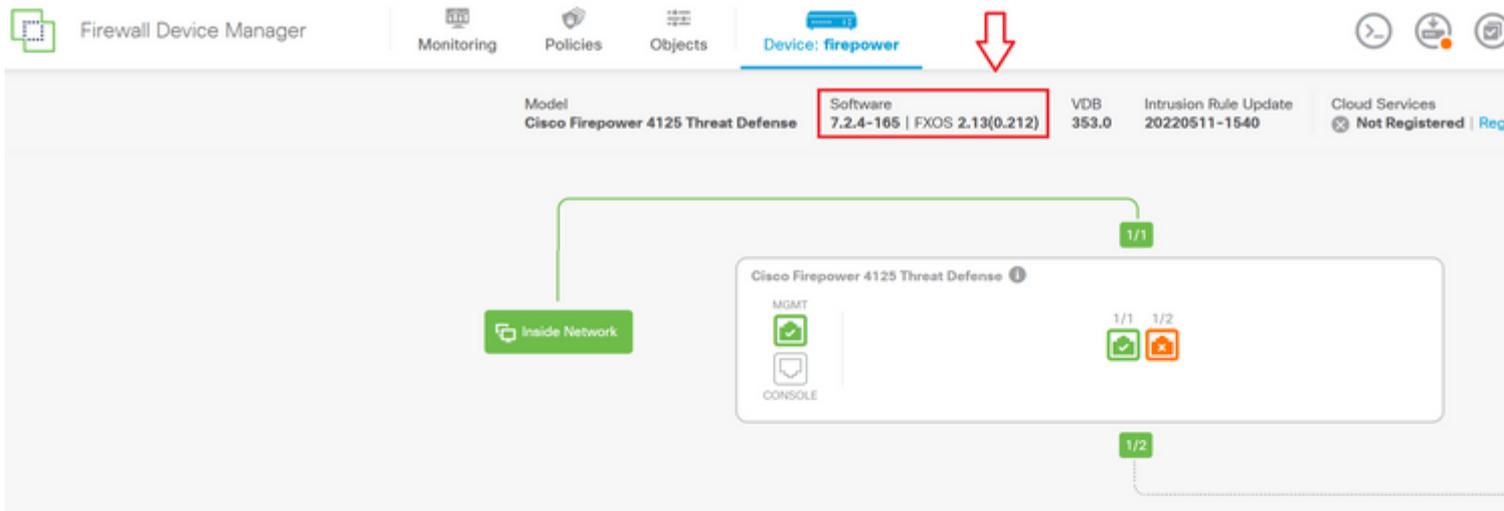
Etapa 9. Clique no botão FINISH após a conclusão bem-sucedida da atualização para retornar à tela de login:



© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, [version 2](#), [version 2.1](#) and [version 3](#)".

Validação

Quando a atualização for concluída, você poderá fazer login no Gerenciador de dispositivos do Firepower para validar a versão atual. Isso será exibido no painel Visão geral:



Interfaces Connected Enabled 3 of 3 View All Interfaces	Routing There are no static routes yet View Configuration	Updates Geolocation, Rule, VDB, System Upd Security Intelligence Feeds View Configuration
Smart License Evaluation expires in 90 days View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Requires RA VPN license No connections 1 Group Policy Configure	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration

Para executar uma validação de atualização via CLI, você pode usar estas etapas:

- I. Crie uma sessão SSH usando o IP de gerenciamento do FTD.
- II. Use o comando **show version** para validar a versão atual no seu chassi.

Exemplo do procedimento sugerido:

Copyright 2004-2023, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 499)
Cisco Firepower 4125 Threat Defense v7.2.4 (build 165)

> show version

```
-----[ firepower ]-----  
Model                : Cisco Firepower 4125 Threat Defense (76) Ve  
UUID                 : e55a326e-25cd-11ee-b261-8d0ffe6dde59  
LSP version          : lsp-rel-20220511-1540  
VDB version          : 353  
-----
```

> █

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.