

Recupere a senha do dispositivo lógico a partir do Gerenciador de chassis

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Procedimento](#)

[Configurações](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como recuperar a senha de um dispositivo lógico do Gerenciador de chassis de firewall seguro (FCM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Sistema operacional extensível (FXOS) com firewall seguro
- Cisco Adaptive Secure Appliance (ASA)
- Defesa contra ameaças de firewall (FTD) segura

Componentes Utilizados

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

- Dispositivos Secure Firewall 4100/9300.
- Dispositivo lógico, ASA ou FTD, já criado e no estado online.

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

A senha de um dispositivo lógico é configurada quando criada, e isso também pode ser alterado após a configuração de bootstrap ter sido implantada a partir da CLI.

Procedimento

Este procedimento descreve como alterar a senha da GUI do Gerenciador de chassis depois que um dispositivo lógico já tiver sido criado. Isso se aplica aos dispositivos lógicos ASA e FTD.



Aviso: o procedimento para recuperar a senha substitui a configuração de bootstrap do FCM. Isso significa que todas as alterações no IP de gerenciamento executadas a partir da CLI do dispositivo lógico após a criação do dispositivo também são restauradas.

Configurações

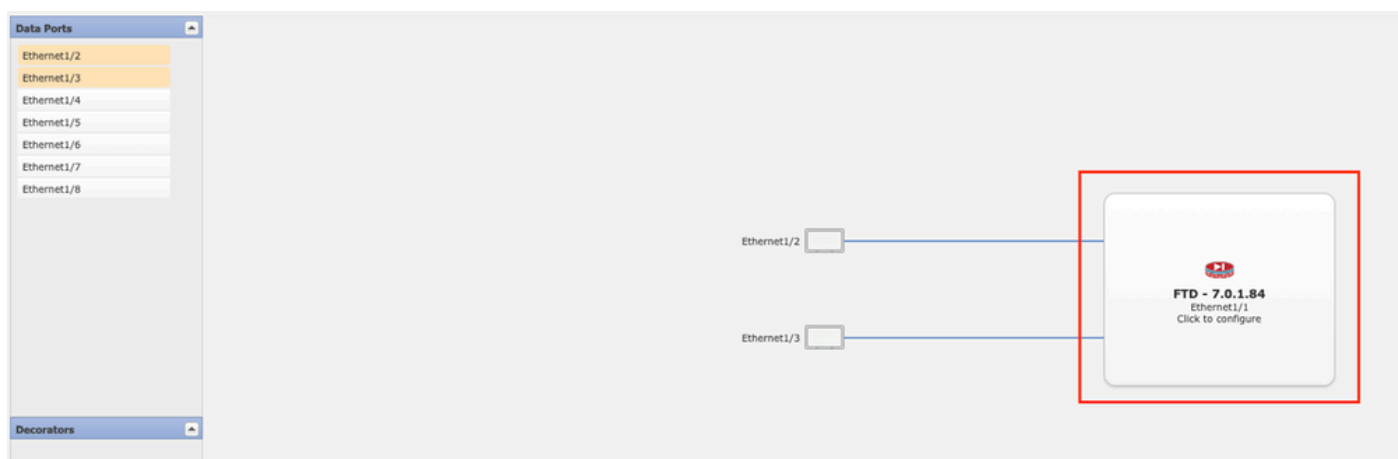
1. Faça login no Gerenciador de chassis do Secure Firewall.

2. Para alterar a senha do dispositivo lógico, navegue até Logical Device > Edit.



Menu de dispositivo lógico

3. Entre na configuração de bootstrap clicando no botão do dispositivo.



Configuração de bootstrap

4. Clique em Configurações. Observe que Password já está definido. Digite sua nova senha e confirme-a.

Esta ação altera a senha, mas é necessário reinicializar para executar as alterações.

Cisco Firepower Threat Defense - Bootstrap Configuration



General Information Settings Agreement

Management type of application instance:	<input type="text" value="FMC"/>	
Search domains:	<input type="text"/>	
Firewall Mode:	<input type="text" value="Routed"/>	
DNS Servers:	<input type="text"/>	
Fully Qualified Hostname:	<input type="text"/>	
Password:	<input type="text"/>	Set: Yes
Confirm Password:	<input type="text"/>	
Registration Key:	<input type="text"/>	Set: Yes
Confirm Registration Key:	<input type="text"/>	
Firepower Management Center IP:	<input type="text" value="10.88.243.23"/>	
Firepower Management Center NAT ID:	<input type="text"/>	
Eventing Interface:	<input type="text"/>	

OK Cancel

Campo Senha

5. Quando você salva as alterações, uma mensagem de confirmação é exibida. Você pode optar por reiniciar o dispositivo agora ou mais tarde em Dispositivos lógicos > Reiniciar.

Bootstrap Settings Update Confirmation



Updating the bootstrap settings from the Firepower Chassis Manager is for disaster recovery only; we recommend that you instead change bootstrap settings in the application. To update the bootstrap settings from the Firepower Chassis Manager, click **Restart Now**: the old bootstrap configuration will be overwritten, and the application will restart. Or click **Restart Later** so you can manually restart the application at a time of your choosing and apply the new bootstrap settings (**Logical Devices > Restart**).

Note: For FTD, if you change the management IP address, be sure to change the device IP address in **FMC (Devices > Device Management > Device tab > Management area)**. This task is not required if you specified the NAT ID instead of the device IP address in FMC.

Restart Now

Restart Later

Cancel

Aviso de Salvar Alterações

6. Quando o dispositivo lógico voltar, você poderá executar SSH para o dispositivo e acessar o modo especialista com as novas credenciais.

Informações Relacionadas

- [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.