

# Provisionar o Secure Firewall ASA para CSM

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurações](#)

[Configurar ASA para Gerenciamento HTTPS](#)

[Provisionar o Secure Firewall ASA para CSM](#)

[Verificar](#)

---

## Introdução

Este documento descreve o processo para provisionar o Secure Firewall Adaptive Security Appliance (ASA) para o Cisco Security Manager (CSM).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ASA com firewall seguro
- CSM

### Componentes Utilizados

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

- Secure Firewall ASA versão 9.18.3
- CSM versão 4.28

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

O CSM ajuda a permitir a aplicação consistente de políticas e a rápida solução de problemas de

eventos de segurança, oferecendo relatórios resumidos em toda a implantação de segurança. Usando sua interface centralizada, as organizações podem escalar com eficiência e gerenciar uma ampla variedade de dispositivos de segurança da Cisco com visibilidade aprimorada.

## Configurar

No próximo exemplo, um ASA virtual é provisionado para um CSM para gerenciamento centralizado.

### Configurações

#### Configurar ASA para Gerenciamento HTTPS

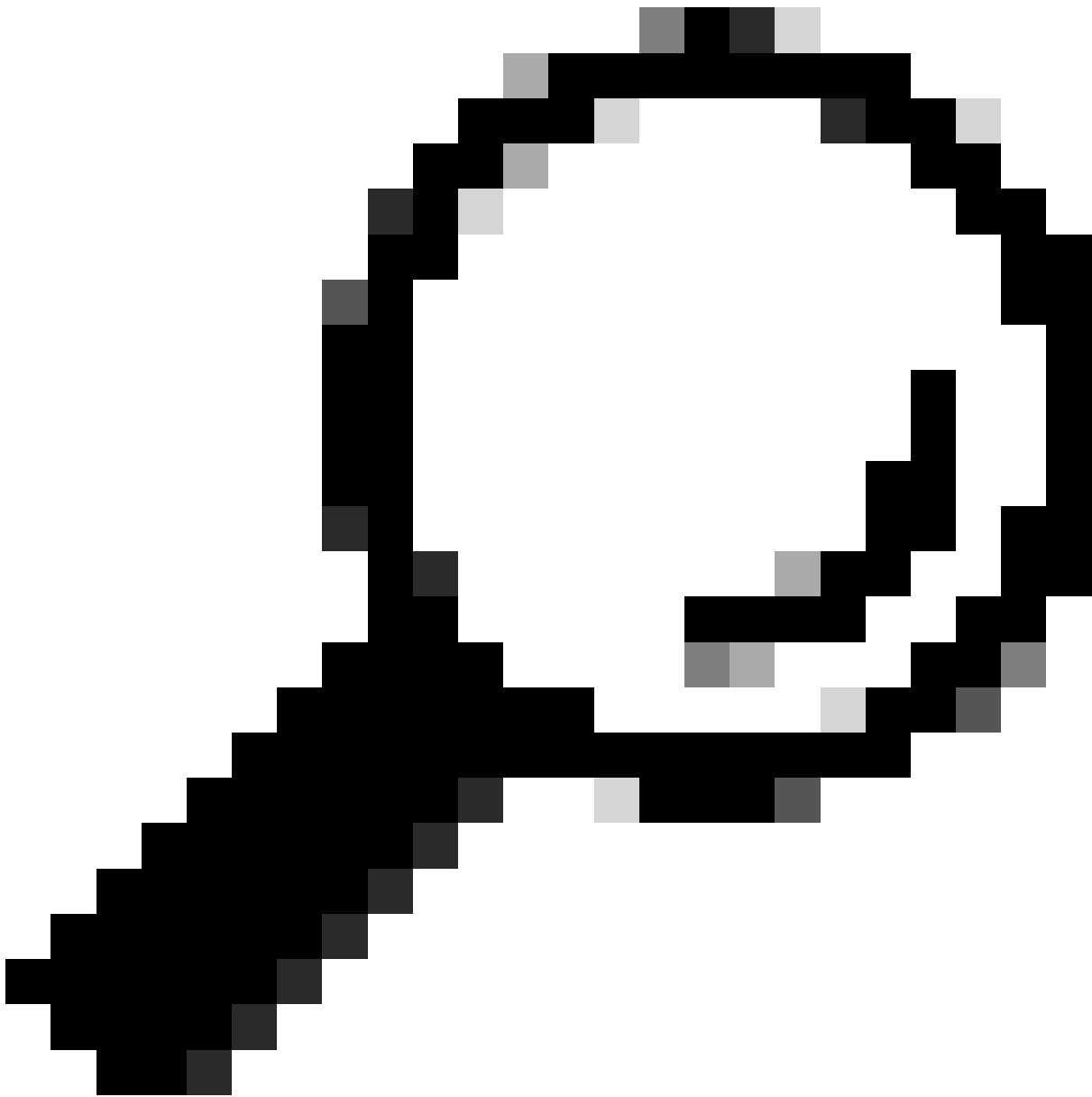
Etapa 1. Crie um usuário com todos os privilégios.

Sintaxe da linha de comando (CLI):

```
configure terminal  
username < user string > password < password > privilege < level number >
```

Isso se traduz no próximo exemplo de comando, que tem o usuário csm-user e a senha cisco123 da seguinte maneira:

```
ciscoasa# configure terminal  
ciscoasa(config)# username csm-user password cisco123 privilege 15
```



Dica: usuários autenticados externamente também são aceitos para essa integração.

---

Etapa 2. Habilite o servidor HTTP.

Sintaxe da linha de comando (CLI):

```
configure terminal  
http server enable
```

Etapa 3. Permitir acesso HTTPS para o endereço IP do servidor CSM.

Sintaxe da linha de comando (CLI):

```
configure terminal
http < hostname > < netmask > < interface name >
```

Isso se traduz no próximo exemplo de comando, que permite que qualquer rede acesse o ASA através de HTTPS na interface externa (GigabitEthernet0/0):

```
ciscoasa# configure terminal
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

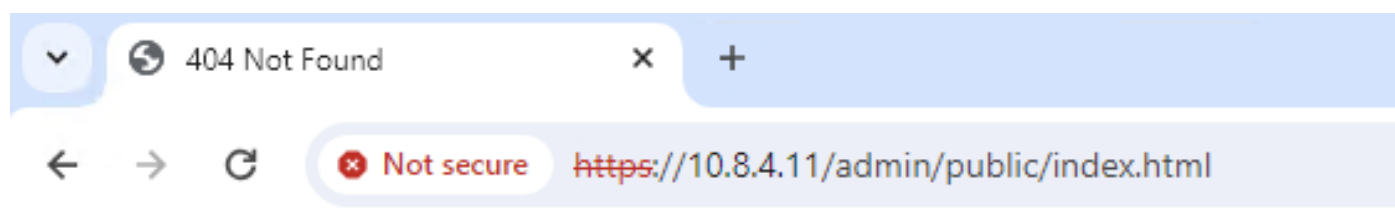
Etapa 4. Valide se o HTTPS pode ser acessado do servidor CSM.

Abra qualquer navegador da Web e digite a próxima sintaxe:

```
https://< ASA IP address >/
```

Isso se traduz no próximo exemplo para o endereço IP da interface externa que foi permitido para acesso HTTPS na etapa anterior:

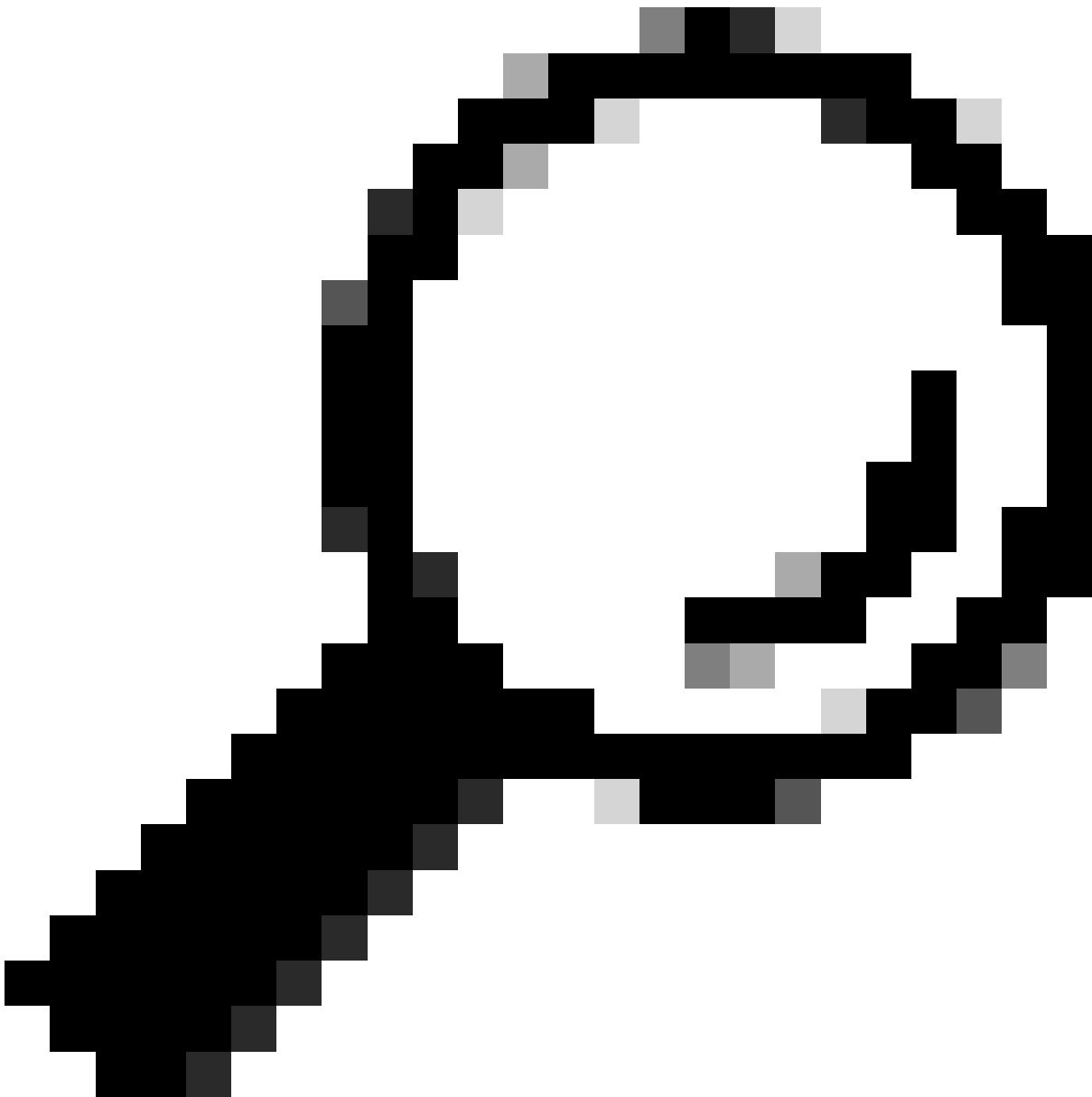
```
https://10.8.4.11/
```



## 404 Not Found

The requested URL `/admin/public/index.html` was not found on this server.

Resposta ASA HTTPS



Dica: o erro 404 não encontrado é esperado nesta etapa, pois este ASA não tem o Cisco Adaptive Security Device Manager (ASDM) instalado, mas a resposta HTTPS está lá quando a página redireciona para a URL `/admin/public/index.html`.

---

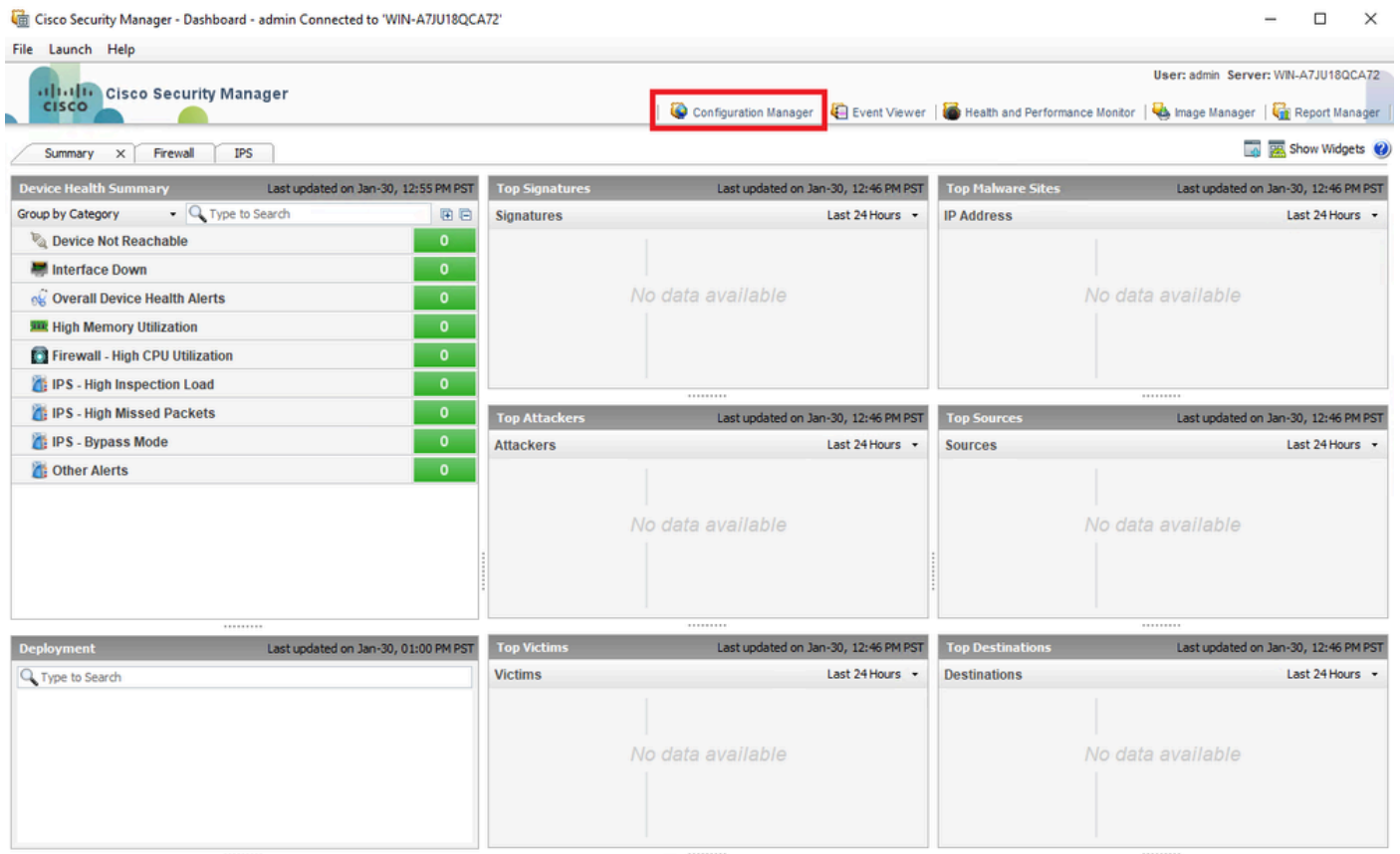
Provisionar o Secure Firewall ASA para CSM

Etapa 1. Abra e faça login no cliente CSM.

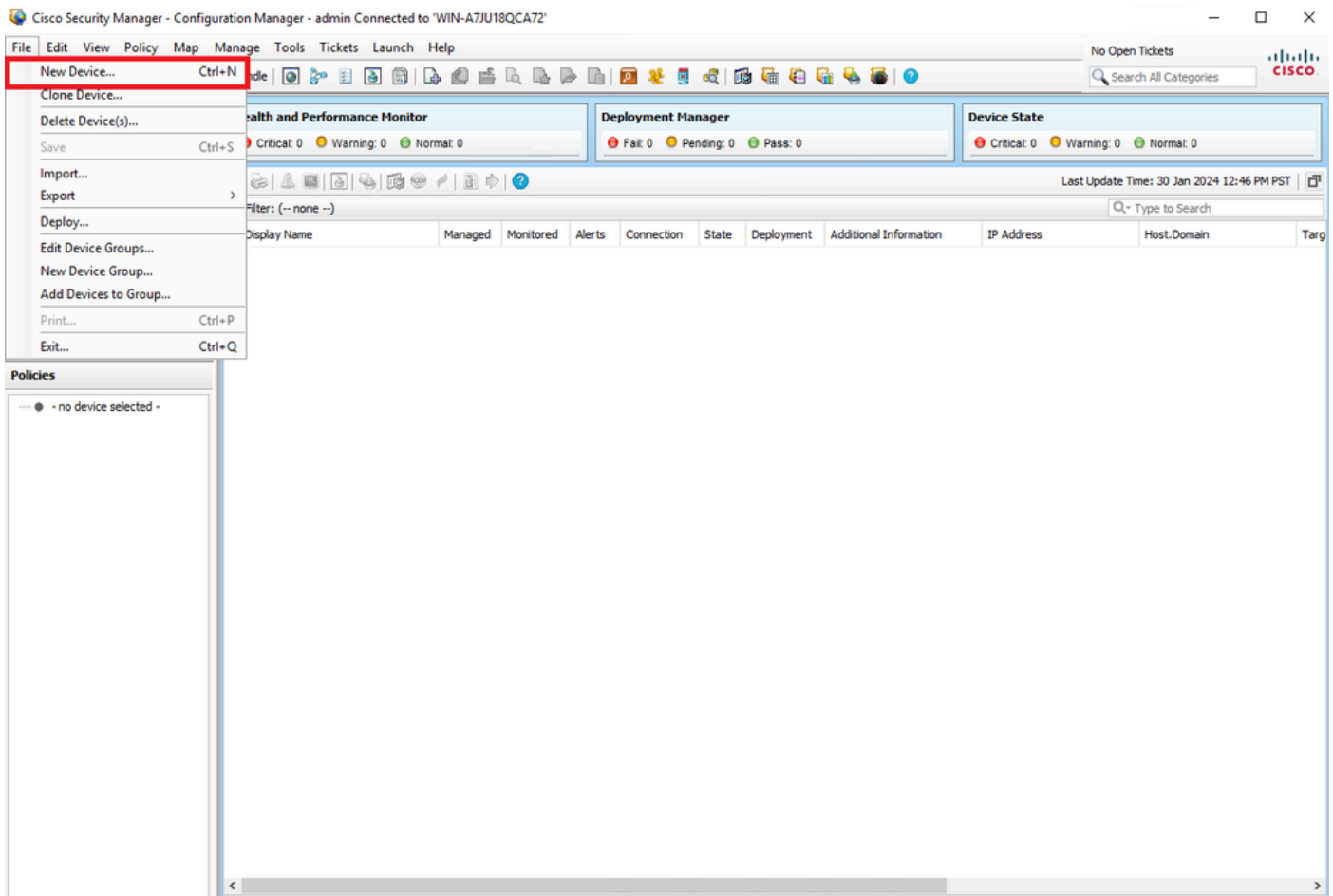


Logon do cliente CSM

Etapa 2. Abra o Gerenciador de configurações.



### Etapa 3. Navegue até Devices > New Device.



Gerenciador de configuração do CSM

Etapa 4. Selecione a opção de adição que preenche o requisito de acordo com o resultado desejado. Como o ASA configurado já está configurado na rede, a melhor opção para este exemplo é **Add Device From Network** e clique em **Next**.

Please choose how you would like to add the device:

Add Device From Network

When you add a device that is live on the network, Cisco Security Manager makes a secure connection with the device and discovers its identifying information and properties.

Add from Configuration File(s)

You can add one or more device configurations from multiple files. When you add a device using its configuration file, Cisco Security Manager discovers the device's identifying information, properties and policies from the file.

Add New Device

You can add a device that is not yet on the network by specifying the device's identifying information and credentials.

Add Device From File

You can add devices from an inventory file that is in the CSV (comma-separated values) format used by Cisco Security Manager, CiscoWorks Common Services DCR, or CS-MARS



Back

Next

Finish

Cancel

Help

### Método de Adição de Dispositivo

Etapa 5. Preencha os dados necessários de acordo com a configuração no Secure Firewall ASA e com as configurações de detecção. Em seguida, clique em **Next**.



**Identity**

IP Type: Static

Host Name: ciscoasa

Domain Name:

IP Address: 10.8.4.11

Display Name: \* ciscoasa

OS Type: \* ASA

Transport Protocol: HTTPS

System Context

**Discover Device Settings**

Perform Device Discovery

Discover: Policies and Inventory

Platform Settings

Firewall Policies

NAT Policies

IPS Policies

RA VPN Policies

Discover Policies for Security Contexts

Back Next Finish Cancel Help

*Configurações do ASA*

Etapa 6. Preencha as credenciais necessárias do usuário CSM configurado no ASA e da senha de **ativação**.

**Primary Credentials**

Username:

Password:\*  Confirm:\*

Enable Password:  Confirm:\*

**HTTP Credentials**

Use Primary Credentials

Username:

Password:

Confirm:

HTTP Port:

HTTPS Port:   Use Default

IPS RDEP Mode:  ▾

Certificate Common Name:  Confirm:

*Credenciais do ASA*

Passo 7. Selecione os grupos desejados ou ignore esta etapa se nenhum grupo for necessário e clique em **Finish**.

Select the groups that this device belongs to:

Department:

Location:

test:

Set Values as Default

*Seleção de grupo CSM*

Etapa 8. Uma solicitação de tíquete é gerada para fins de controle, clique em **OK**.

Select the groups that this device belongs to:

Department:

Location:

test:

Set Values as Default

Ticket Required ✕

You must have an editable ticket opened in order to perform this action. You may:  
Create a new ticket:

Ticket:

Description:



*Criação de tíquete CSM*







Etapa 9. Valide se a descoberta termina sem erros e clique em **Fechar**.

100%

Status: Discovery completed with warnings  
Devices to be discovered: 1  
Devices discovered successfully: 1  
Devices discovered with errors: 0

## Discovery Details

Type	Name	Severity	State	Discovered From
	ciscoasa		Discovery Completed with Warnings	Live Device

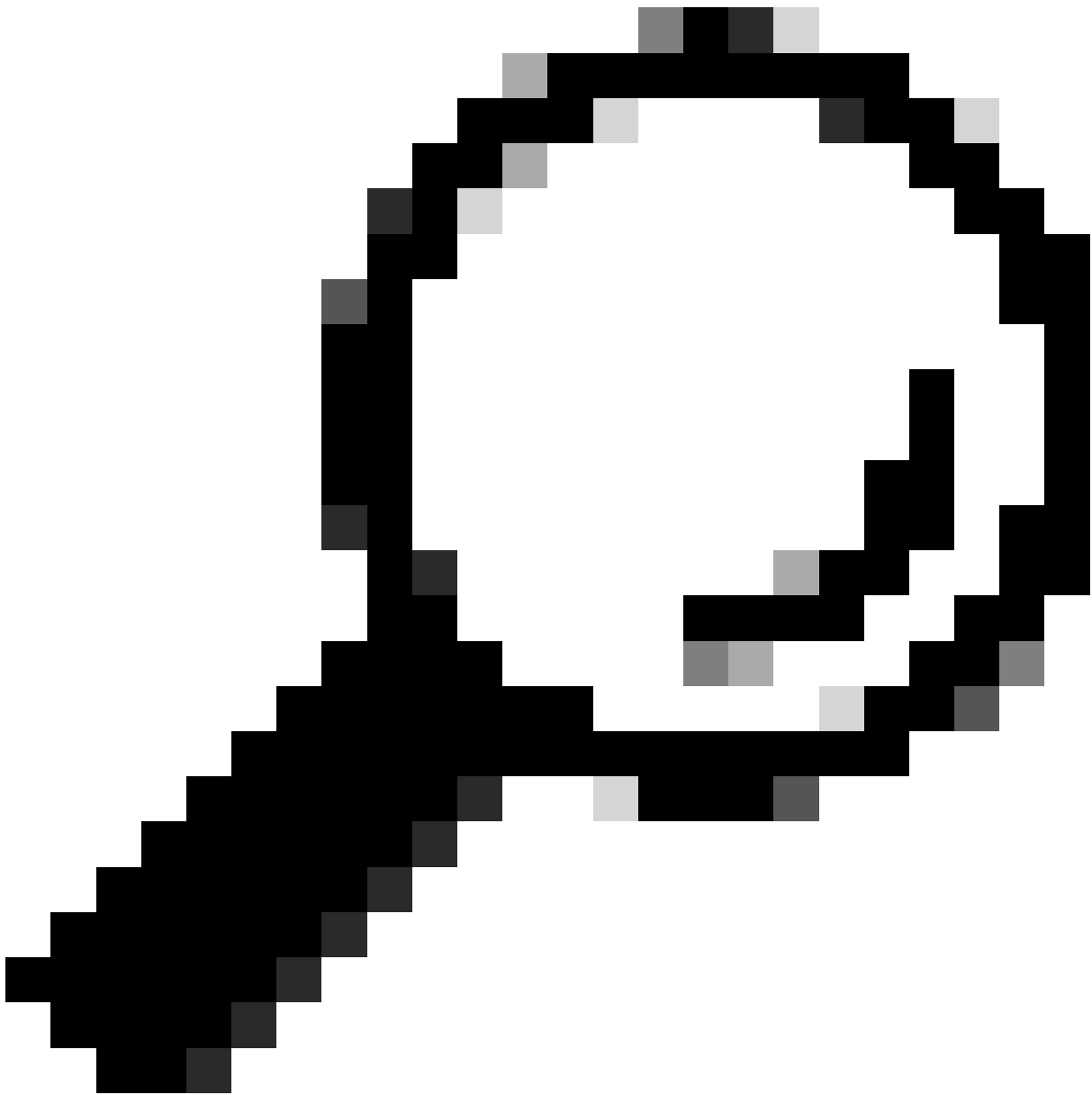
Messages	Severity	Description
CLI not discovered		Policy discovery does not support the following CLI in your configuration: Line 5:service-module 0 keepalive-timeout 4 Line 6:service-module 0 keepalive-counter 6 Line 8:license smart Line 12:no mac-address auto Line 50:no failover wait-disable Line 55:no asdm history enable Line 57:no arp permit-nonconnected
Policies discovered		
Existing policy objects reused		
Value overrides created for device		
Policies discovered		
Add Device Successful		Action If you wish to manage these commands in CS Manager, please use the "Flex Config" function

Generate Report

Abort

Close

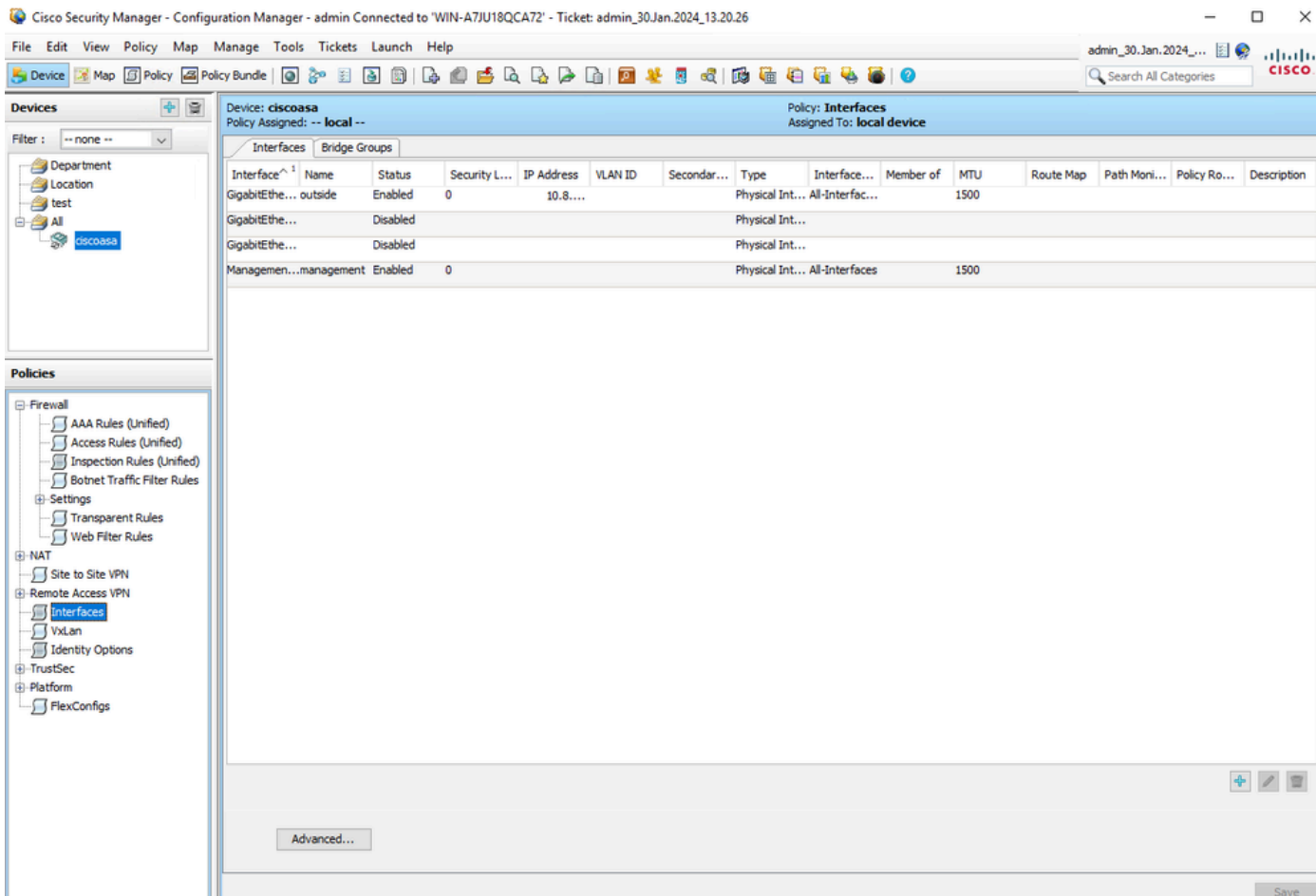
Help



**Dica:** os avisos são aceitos como uma saída bem-sucedida, pois nem todas as funcionalidades do ASA são suportadas pelo CSM.

---

Etapa 10. Valide se o ASA agora aparece como registrado no cliente CSM e exibe as informações corretas.



Informações do ASA registradas

Verificar

Uma depuração HTTPS está disponível no ASA para fins de solução de problemas. O próximo comando é usado:

`debug http`

Este é um exemplo de uma depuração de registro de CSM bem-sucedida:

```
ciscoasa# debug http debug http enabled at level 1. ciscoasa# HTTP: processing handoff to legacy admin
```

## 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.