

Provision Secure Firewall ASA naar CSM

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuraties](#)

[ASA voor HTTPS-beheer configureren](#)

[Provision Secure Firewall ASA naar CSM](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft het proces om een beveiligde firewall adaptieve security applicatie (ASA) te provisioneren voor Cisco Security Manager (CSM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Secure-firewall ASA
- CSM

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Firewall ASA versie 9.18.3
- CSM versie 4.28

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

CSM helpt om consistente beleidshandhaving en snelle probleemoplossing van security

gebeurtenissen mogelijk te maken, met samengevatte rapporten over de security implementaties. Door gebruik te maken van de gecentraliseerde interface kunnen organisaties een brede reeks Cisco-beveiligingsapparaten efficiënt schalen en beheren met verbeterde zichtbaarheid.

Configureren

In het volgende voorbeeld wordt een virtuele ASA toegewezen aan een CSM voor gecentraliseerd beheer.

Configuraties

ASA voor HTTPS-beheer configureren

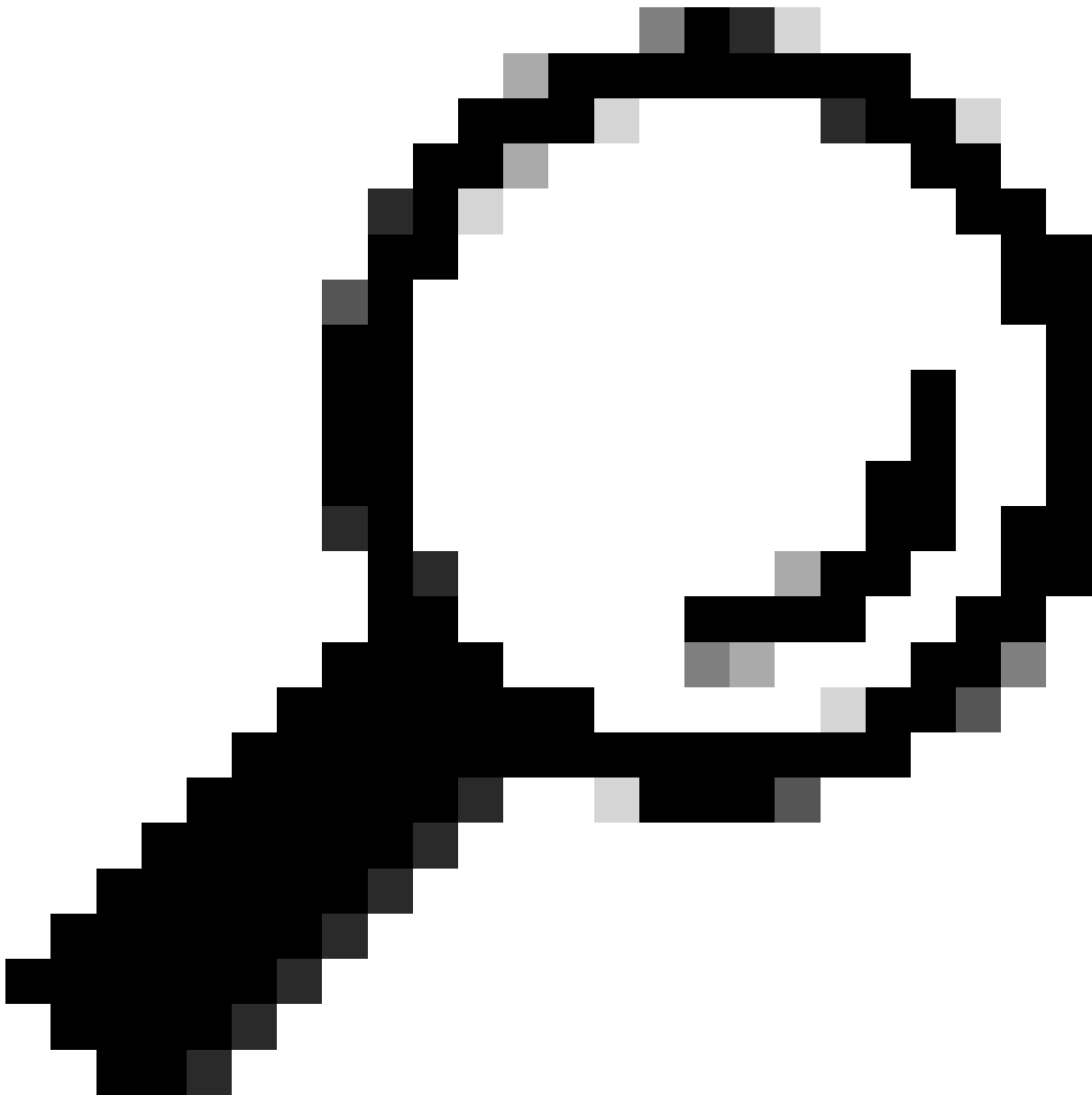
Stap 1. Een gebruiker met alle rechten maken.

CLI-syntaxis (Command Line):

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

Dit vertaalt zich in het volgende opdrachtvoorbeeld, dat de gebruiker csm-user en het wachtwoord cisco123 heeft als volgt:

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



Tip: Extern geverifieerde gebruikers worden ook voor deze integratie geaccepteerd.

Stap 2. HTTP-server inschakelen.

CLI-syntaxis (Command Line):

```
configure terminal  
http server enable
```

Stap 3. Verleen HTTPS-toegang voor het IP-adres van de CSM-server.

CLI-syntaxis (Command Line):

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

Dit vertaalt zich in het volgende opdrachtvoorbeeld, waarmee elk netwerk toegang tot de ASA kan krijgen via HTTPS op de buiteninterface (Gigabit Ethernet0/0):

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

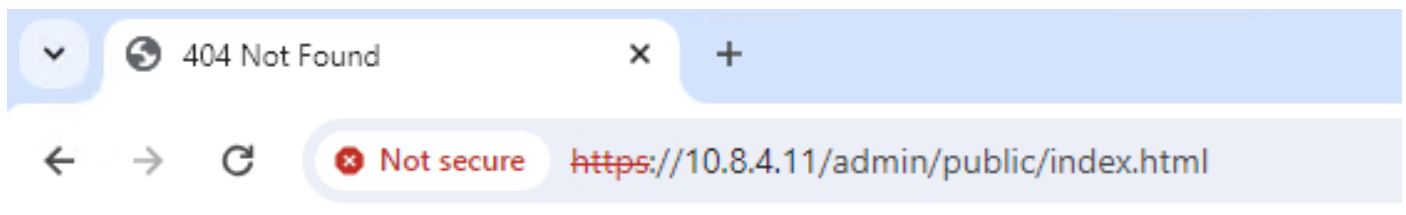
Stap 4. Controleer of HTTPS bereikbaar is vanaf de CSM-server.

Open een webbrowser en typ de volgende syntaxis:

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

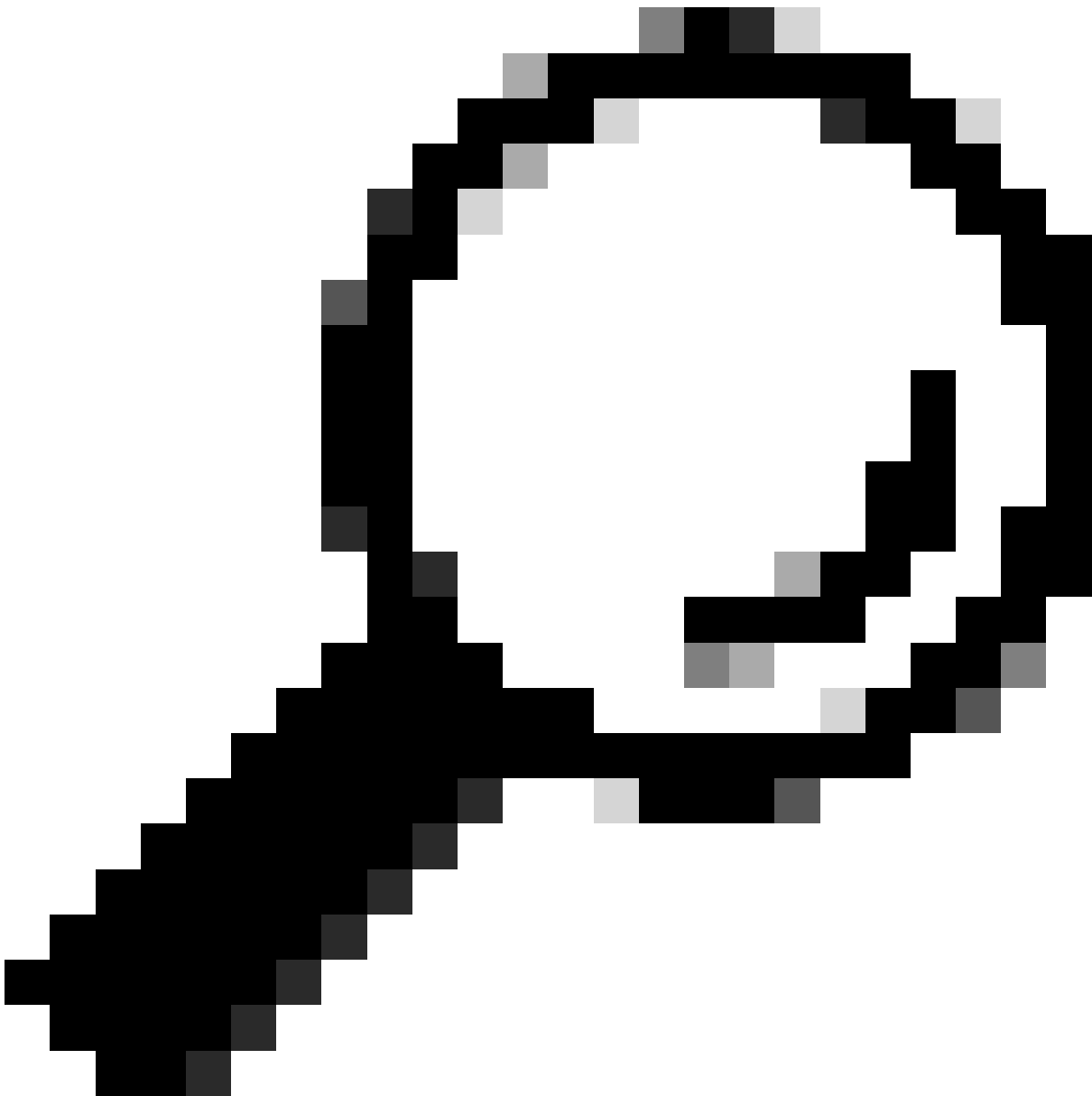
Dit vertaalt zich in het volgende voorbeeld voor het IP-adres van de externe interface dat bij de vorige stap voor HTTPS-toegang was toegestaan:

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



404 Not Found

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



Tip: fout 404 niet gevonden wordt verwacht in deze stap omdat bij deze ASA Cisco Adaptive Security Device Manager (ASDM) niet is geïnstalleerd, maar de HTTPS-respons is aanwezig als de pagina wordt omgeleid naar URL `/admin/public/index.html`.

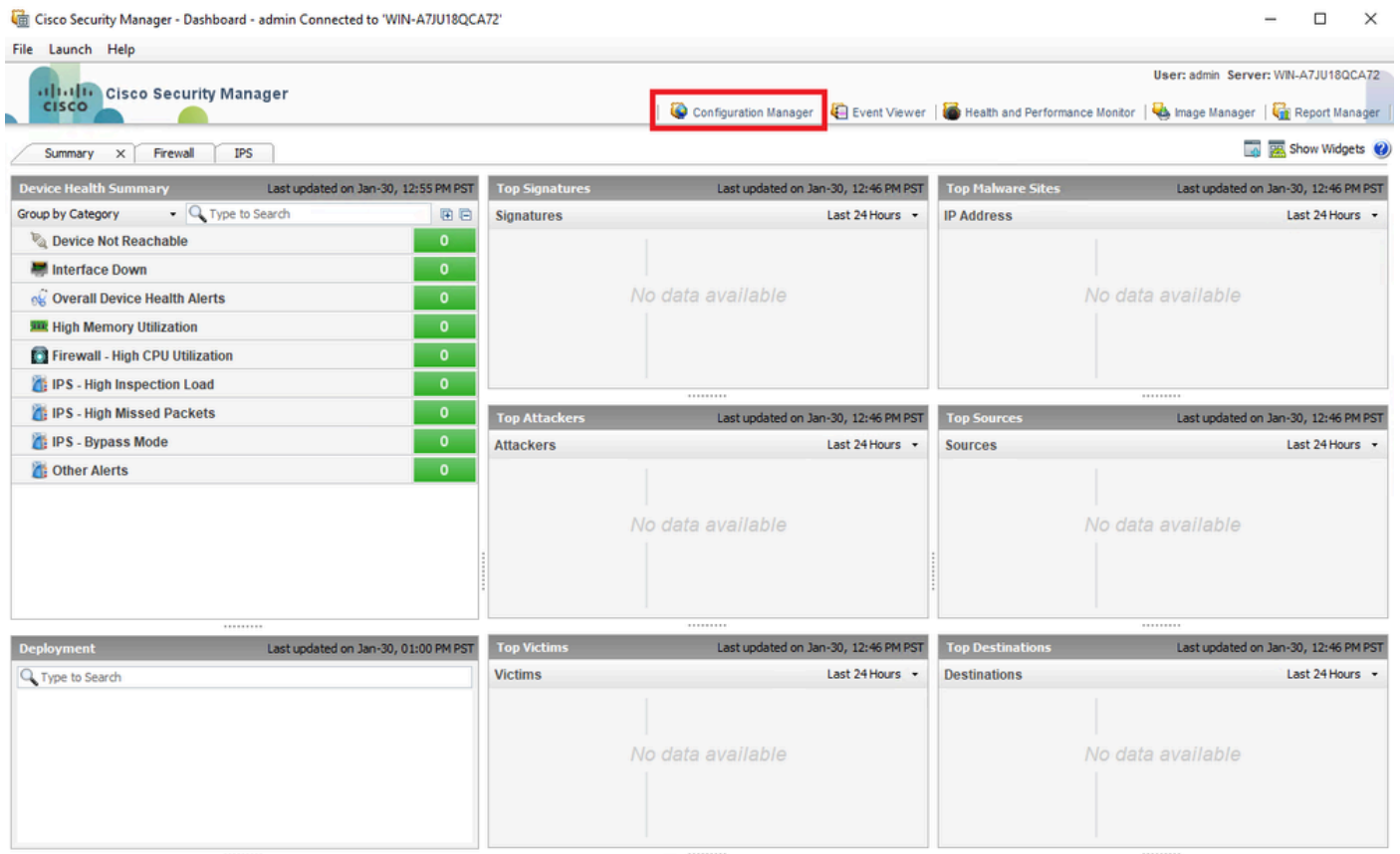
Provision Secure Firewall ASA naar CSM

Stap 1. Open de CSM-client en log in.

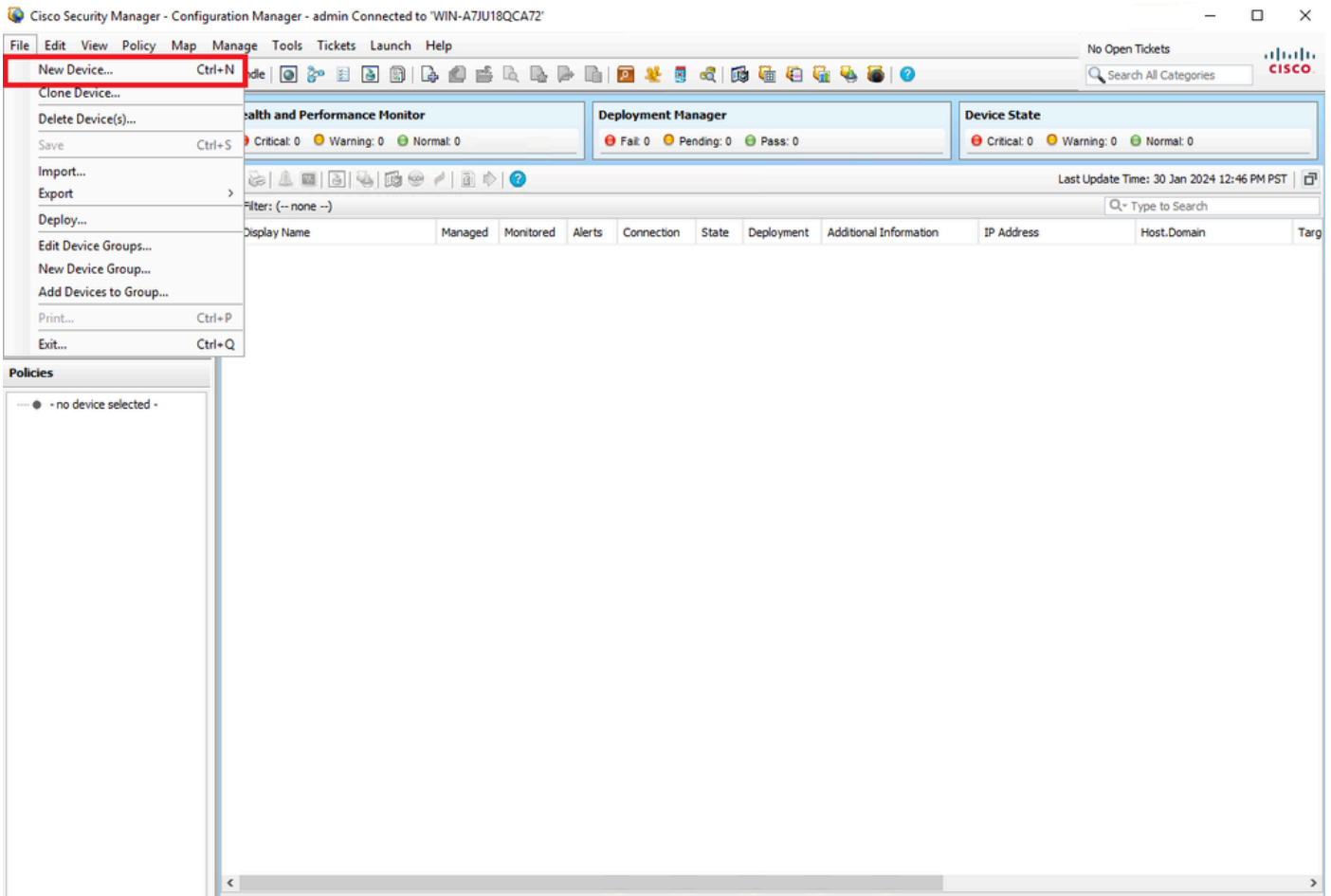


CSM-clientaanmelding

Step 2. Open Configuration Manager.



Stap 3. Ga naar Apparaten > Nieuw apparaat.



CSM Configuration Manager

Stap 4. Selecteer de toevoeging optie die voldoet aan het vereiste op basis van het gewenste resultaat. Aangezien de geconfigureerde ASA al in het netwerk is ingesteld, is de beste optie voor dit voorbeeld **Add Device From Network** en klik op **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

Methode voor toevoegen van apparaat

Stap 5. Vul de vereiste gegevens in volgens de configuratie op de Secure Firewall ASA en de instellingen voor detectie. Klik vervolgens op **Volgende**.

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

ASA-instellingen

Stap 6. Voltooi de vereiste referenties van zowel de geconfigureerde CSM-gebruiker op ASA als van het wachtwoord **Enable**.

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:

ASA-referenties

Stap 7. Selecteer de gewenste groepen of sla deze stap over als er geen groepen nodig zijn en klik op **Voltooien**.

Select the groups that this device belongs to:

Department:

Location:

test:

Set Values as Default

Back

Next

Finish

Cancel

Help

CSM-groepsselectie

Stap 8. Een kaartaanvraag wordt gegenereerd voor controledoelinden, klik op **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:



CSM-ticketontwikkeling







Stap 9. Bevestig dat de ontdekking zonder fouten eindigt en klik op **Sluiten**.

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		

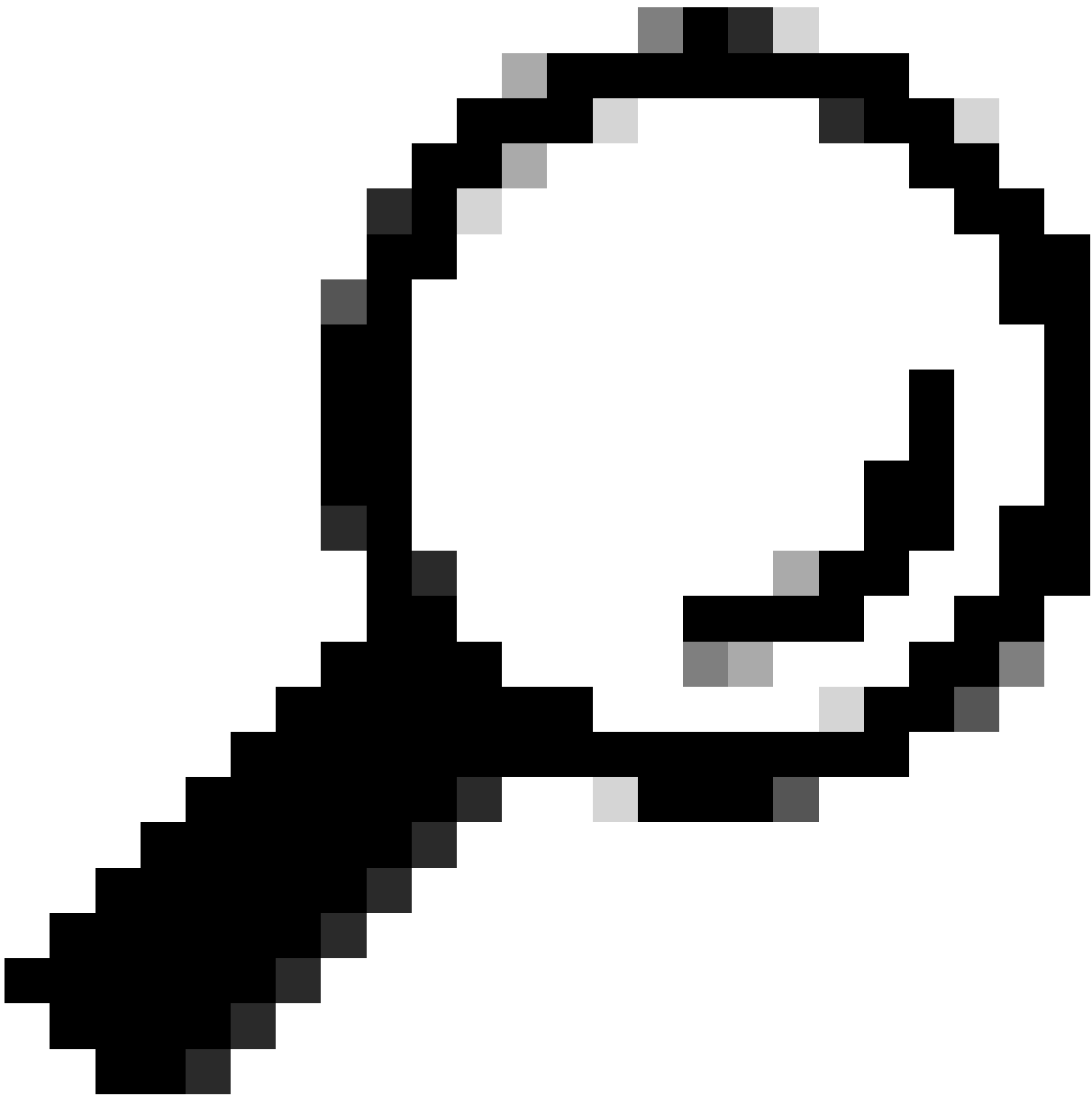
Action
If you wish to manage these commands in CS Manager, please use the "Flex Config" function

Generate Report

Abort

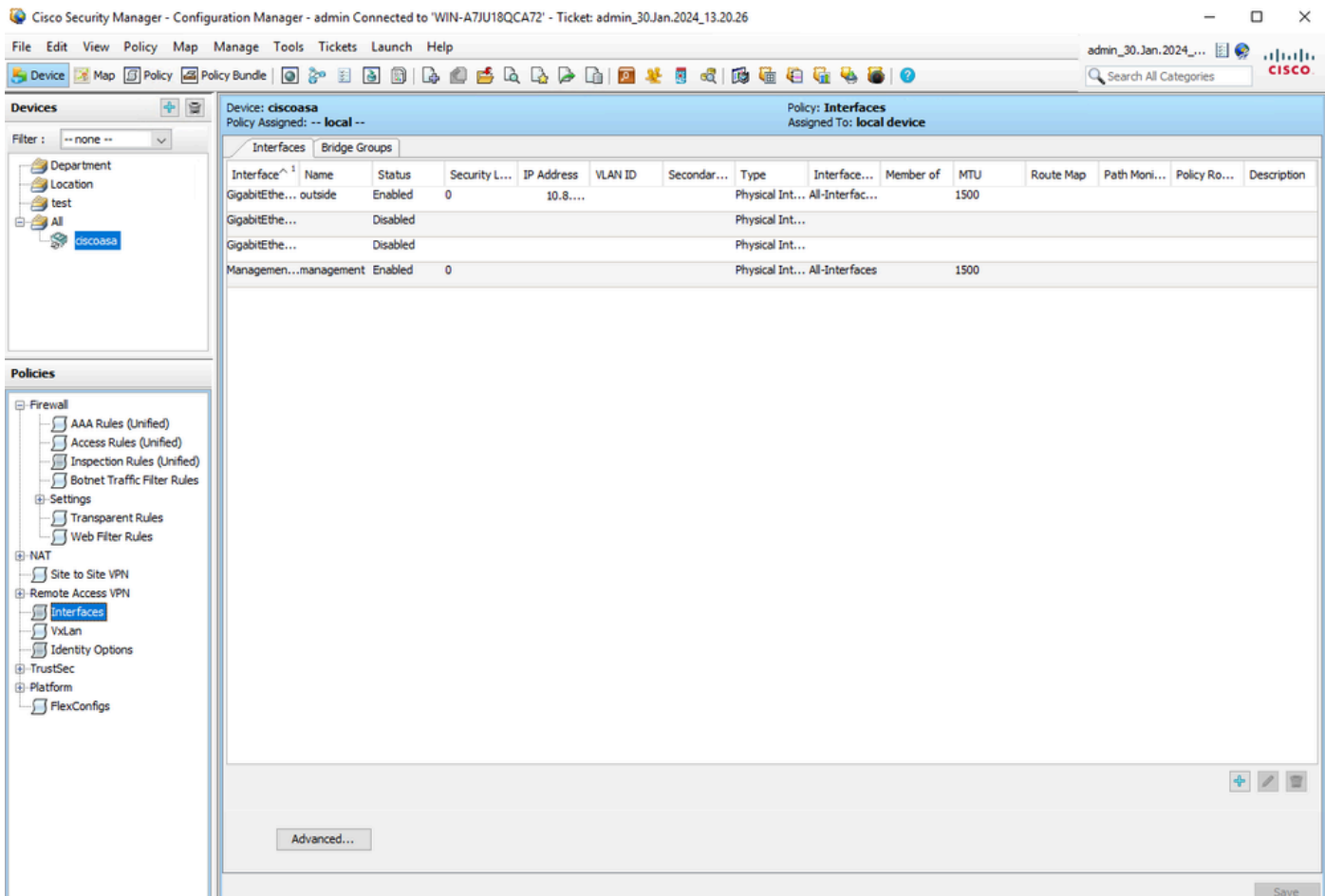
Close

Help



Tip: waarschuwingen worden geaccepteerd als een succesvolle uitvoer, omdat niet alle ASA-functies door CSM worden ondersteund.

Stap 10. Controleer of de ASA nu op de CSM-client is geregistreerd en geeft de juiste informatie weer.



ASA-informatie geregistreerd

Verifiëren

Er is een HTTPS-debug beschikbaar op ASA voor probleemoplossing. De volgende opdracht wordt gebruikt:

```
debug http
```

Dit is een voorbeeld van een succesvolle CSM-registratiebug:

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.