

Bereitstellung einer sicheren Firewall-ASA für CSM

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurationen](#)

[ASA für HTTPS-Management konfigurieren](#)

[Bereitstellung einer sicheren Firewall-ASA für CSM](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird der Prozess zur Bereitstellung der Secure Firewall Adaptive Security Appliance (ASA) für den Cisco Security Manager (CSM) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sichere Firewall ASA
- CSM

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Secure Firewall ASA Version 9.18.3
- CSM Version 4.28

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

CSM unterstützt die konsistente Durchsetzung von Richtlinien und die schnelle Behebung von Sicherheitsereignissen und bietet für die gesamte Sicherheitsinfrastruktur zusammengefasste Berichte. Die zentrale Benutzeroberfläche ermöglicht eine effiziente Skalierung und Verwaltung einer Vielzahl von Cisco Sicherheitsgeräten bei erhöhter Transparenz.

Konfigurieren

Im nächsten Beispiel wird eine virtuelle ASA für ein zentrales Management auf einem CSM bereitgestellt.

Konfigurationen

ASA für HTTPS-Management konfigurieren

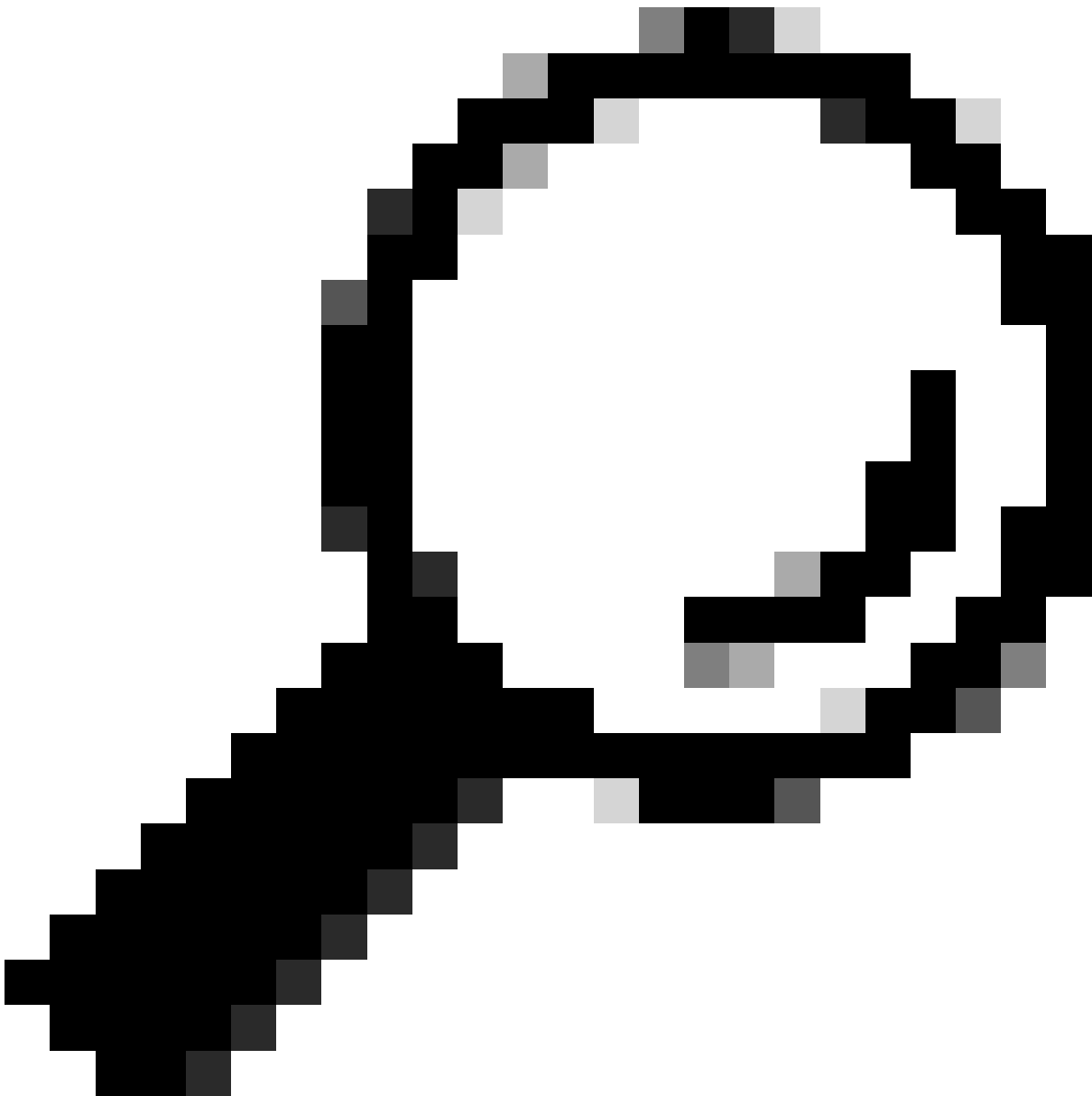
Schritt 1: Erstellen Sie einen Benutzer mit allen Berechtigungen.

Befehlszeilen-Syntax (CLI):

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

Dies wird in das nächste Befehlsbeispiel übersetzt, das den Benutzer csm-user und das Kennwort cisco123 wie folgt enthält:

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



Tipp: Auch extern authentifizierte Benutzer werden für diese Integration akzeptiert.

Schritt 2: HTTP-Server aktivieren.

Befehlszeilen-Syntax (CLI):

```
configure terminal  
http server enable
```

Schritt 3: HTTPS-Zugriff für die IP-Adresse des CSM-Servers zulassen.

Befehlszeilen-Syntax (CLI):

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

Dies wird in das nächste Befehlsbeispiel übersetzt, das jedem Netzwerk den Zugriff auf die ASA über HTTPS an der externen Schnittstelle (GigabitEthernet0/0) ermöglicht:

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

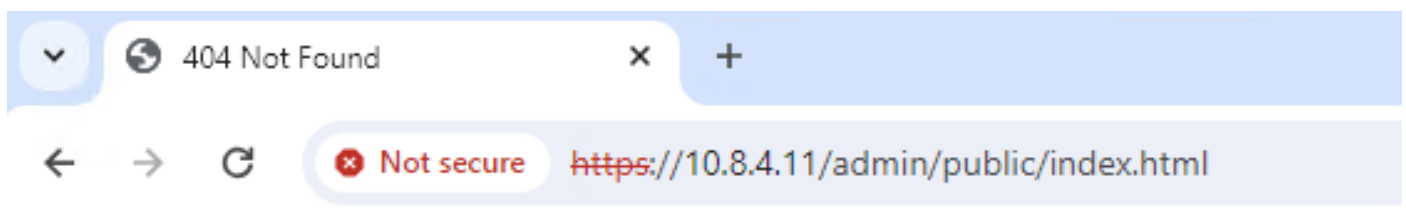
Schritt 4: Überprüfen Sie, ob HTTPS vom CSM-Server aus erreichbar ist.

Öffnen Sie einen beliebigen Webbrowser, und geben Sie die nächste Syntax ein:

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

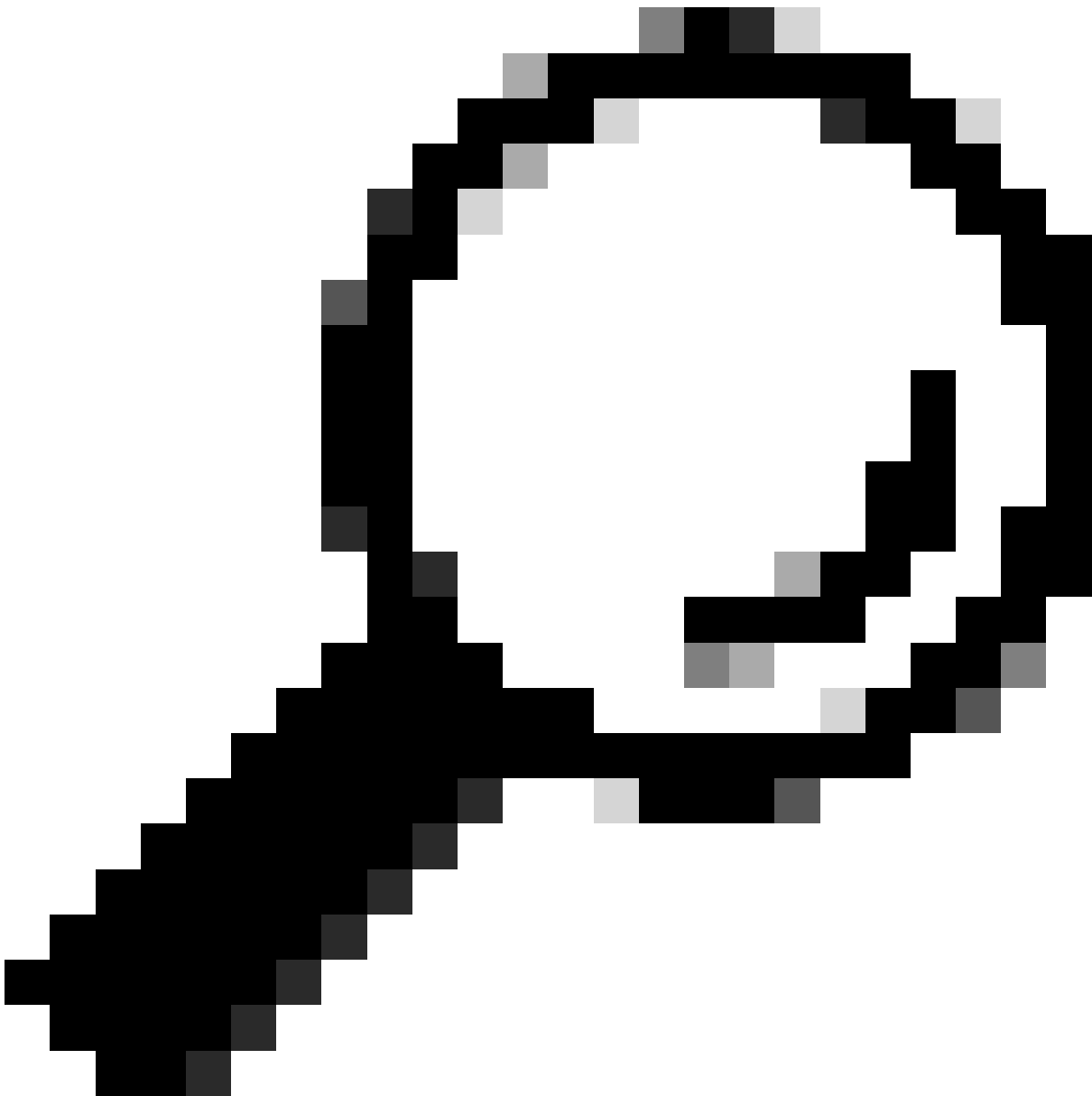
Dies wird in das nächste Beispiel für die externe Schnittstellen-IP-Adresse übersetzt, die im vorherigen Schritt für den HTTPS-Zugriff zugelassen wurde:

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



404 Not Found

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



Tipp: Fehler 404 Not Found (Nicht gefunden) wird für diesen Schritt erwartet, da auf dieser ASA der Cisco Adaptive Security Device Manager (ASDM) nicht installiert ist. Die HTTPS-Antwort wird jedoch angezeigt, wenn die Seite zu URL `/admin/public/index.html` umgeleitet wird.

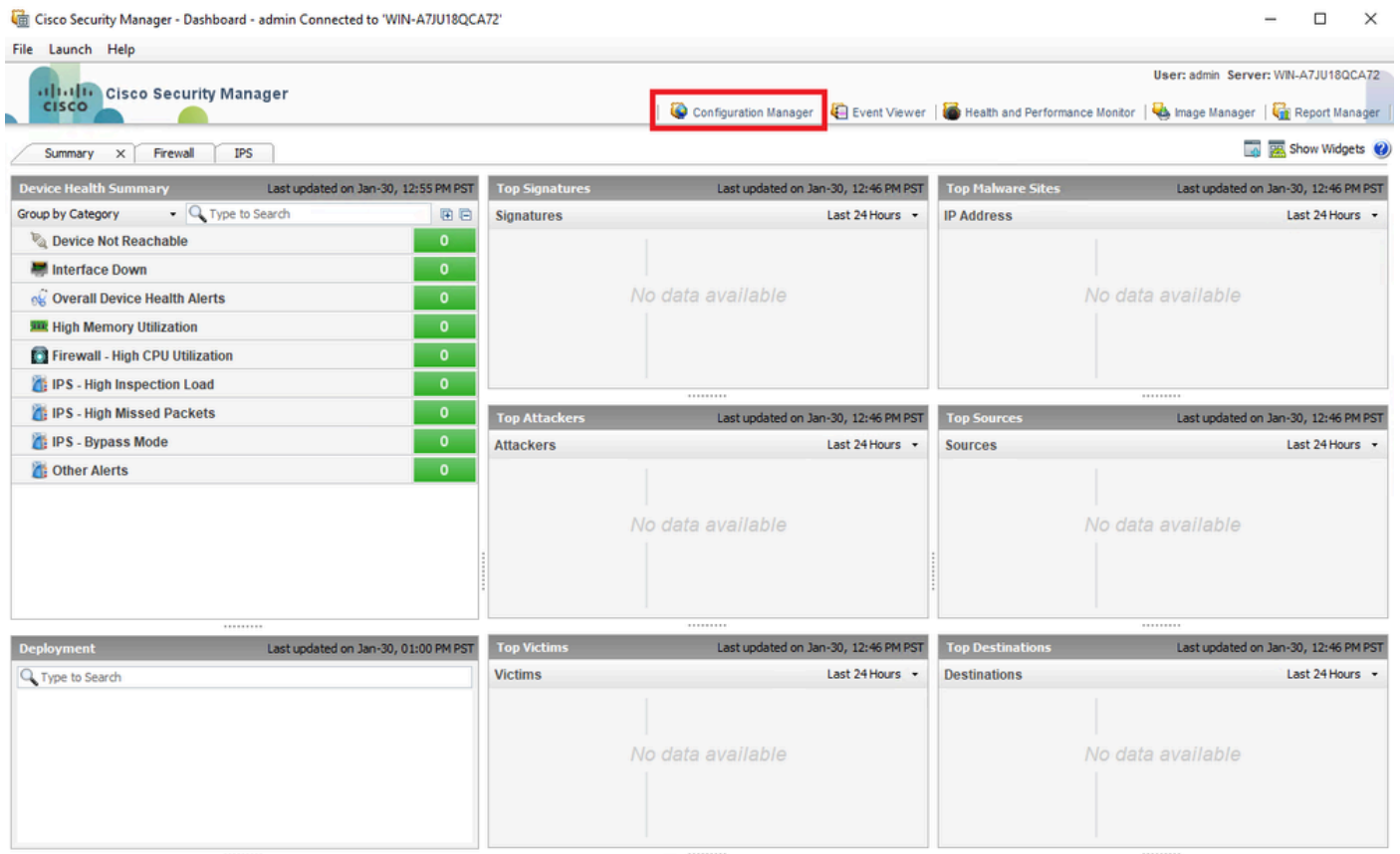
Bereitstellung einer sicheren Firewall-ASA für CSM

Schritt 1: Öffnen und beim CSM-Client anmelden

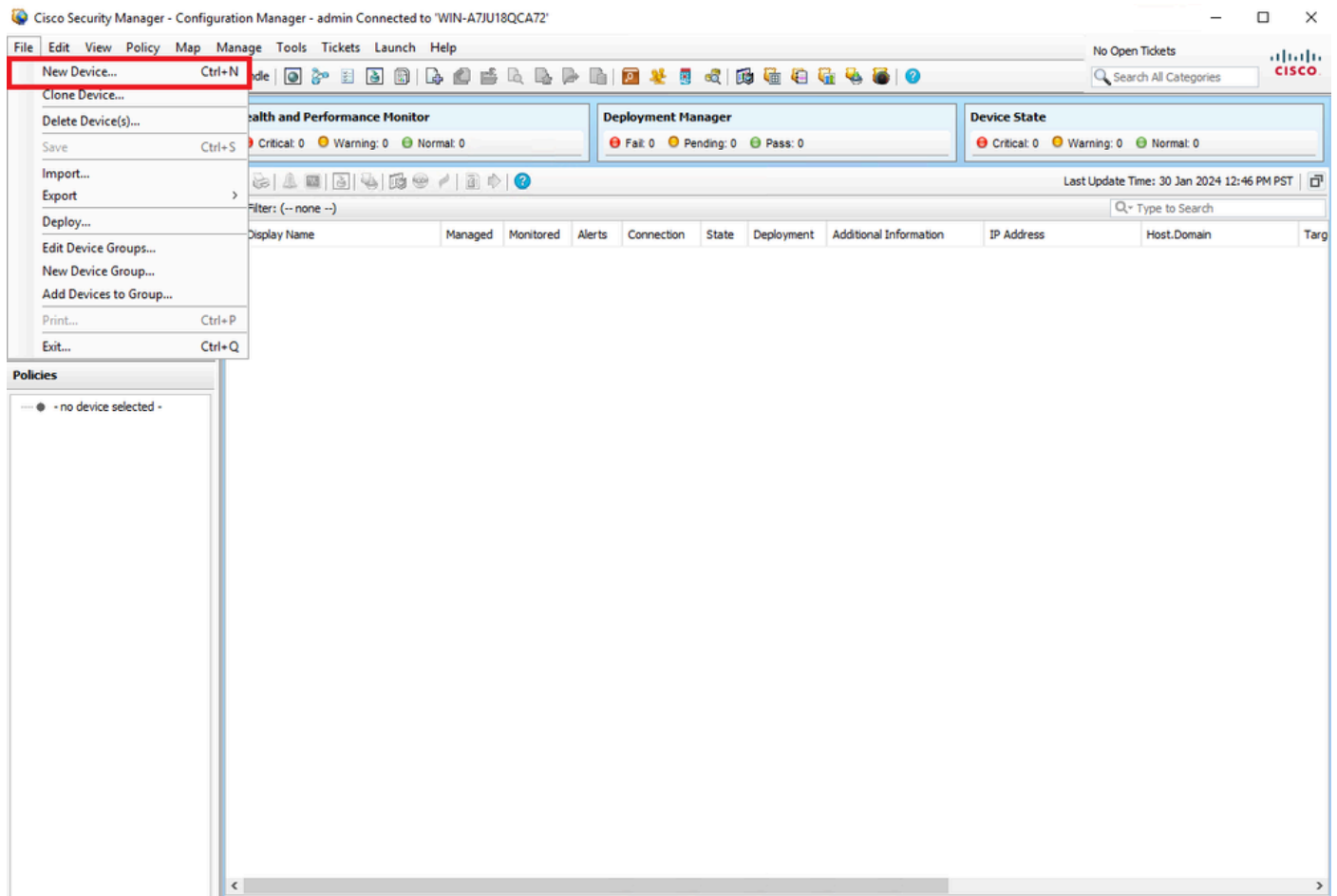


Anmeldung beim CSM-Client

Schritt 2: Öffnen Sie den Configuration Manager.



Schritt 3: Navigieren Sie zu Geräte > Neues Gerät.



CSM-Konfigurationsmanager

Schritt 4: Wählen Sie die Hinzufügungsoption aus, die die Anforderung gemäß dem gewünschten Ergebnis erfüllt. Da die konfigurierte ASA bereits im Netzwerk eingerichtet ist, ist die beste Option für dieses Beispiel **"Gerät vom Netzwerk hinzufügen"** und klicken auf **"Weiter"**.

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 zum Hinzufügen von Geräten

Schritt 5: Füllen Sie die erforderlichen Daten entsprechend der Konfiguration auf der Secure Firewall ASA und den Erkennungseinstellungen aus. Klicken Sie dann auf **Weiter**.

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-Einstellungen

Schritt 6: Geben Sie die erforderlichen Anmeldeinformationen des konfigurierten CSM-Benutzers auf der ASA und des **aktivierten** Kennworts ein.

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-Anmeldedaten

Schritt 7. Wählen Sie die gewünschten Gruppen aus oder überspringen Sie diesen Schritt, falls keine erforderlich ist, und klicken Sie auf **Fertig stellen**.

Select the groups that this device belongs to:

Department:

Location:

test:

Set Values as Default

Back

Next

Finish

Cancel

Help

CSM-Gruppenauswahl

Schritt 8: Eine Ticketanfrage wird zu Kontrollzwecken generiert, klicken Sie auf **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:



Erstellung von CSM-Tickets







Schritt 9. Überprüfen Sie, ob die Erkennung fehlerfrei abgeschlossen wurde, und klicken Sie auf **Schließen**.

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		

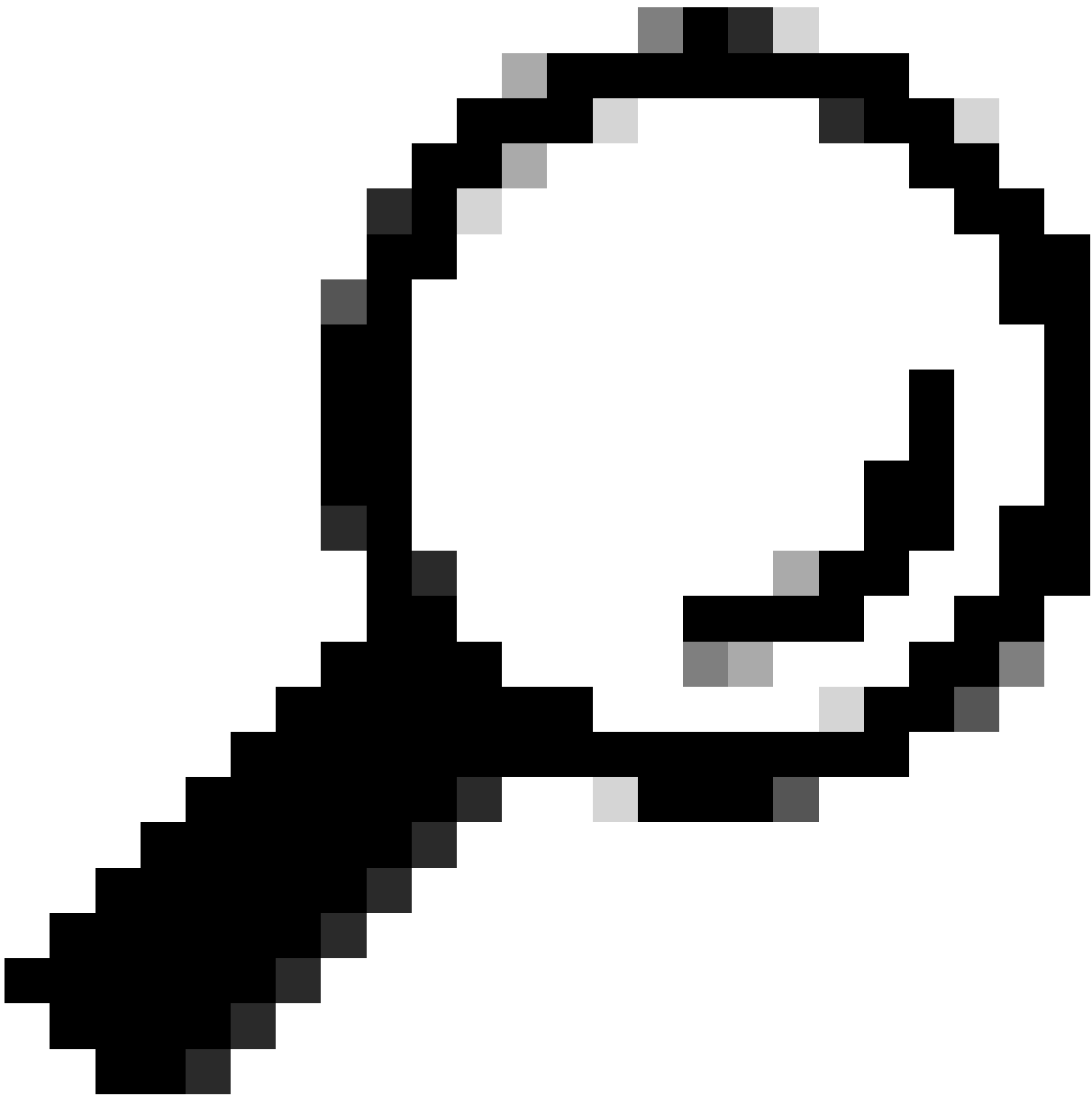
Action
If you wish to manage these commands in CS Manager, please use the "Flex Config" function

Generate Report

Abort

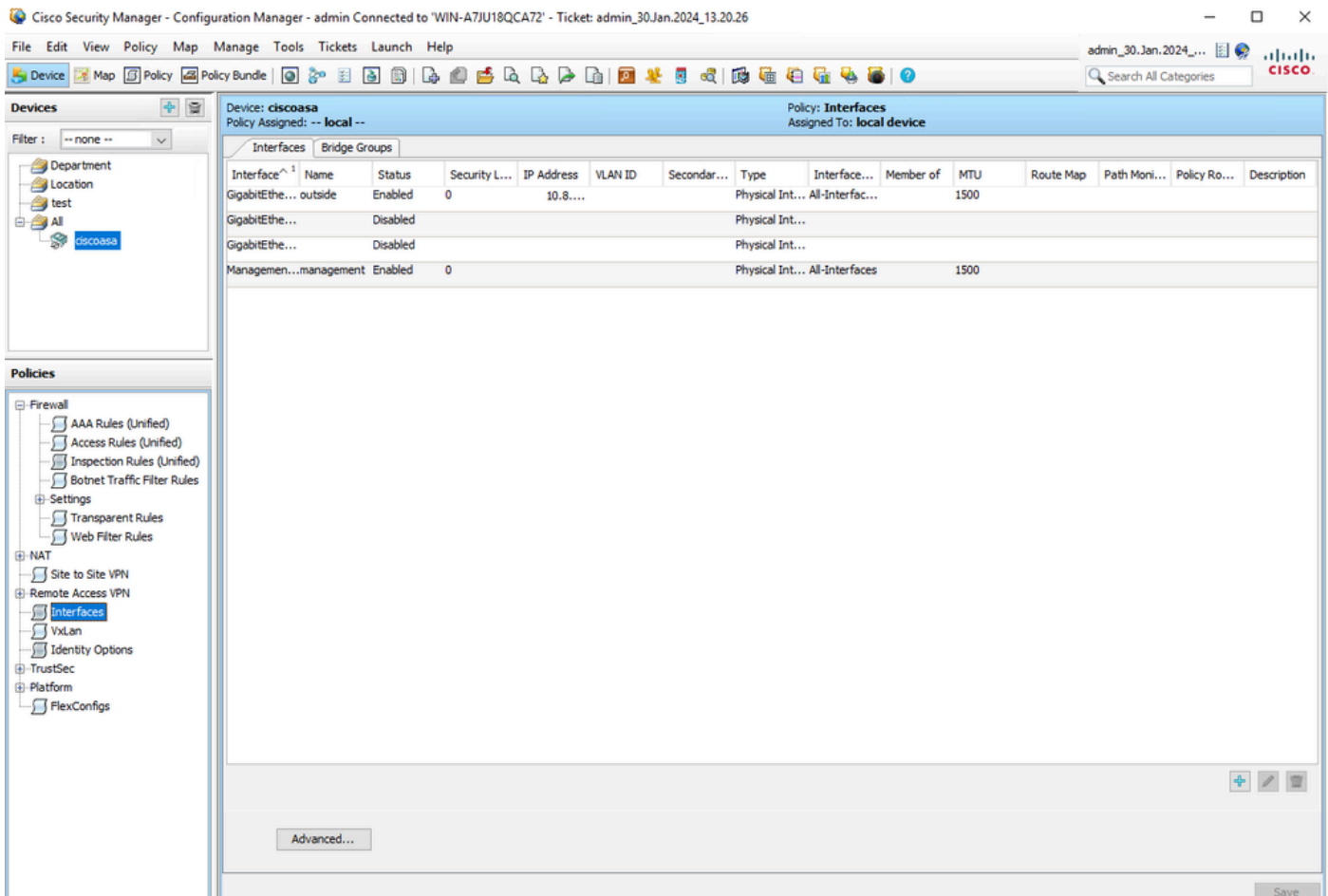
Close

Help



Tipp: Warnungen werden als erfolgreiche Ausgabe akzeptiert, da nicht alle ASA-Funktionen von CSM unterstützt werden.

Schritt 10. Überprüfen Sie, ob die ASA jetzt als auf dem CSM-Client registriert angezeigt wird, und zeigen Sie die richtigen Informationen an.



Registrierte ASA-Informationen

Überprüfung

Zur Fehlerbehebung steht auf ASA ein HTTPS-Debugging zur Verfügung. Der nächste Befehl wird verwendet:

```
debug http
```

Dies ist ein Beispiel für ein erfolgreiches CSM-Registrierungsdebug:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.