

將安全防火牆ASA調配到CSM

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[組態](#)

[為HTTPS管理配置ASA](#)

[將安全防火牆ASA調配到CSM](#)

[驗證](#)

簡介

本檔案介紹將Secure Firewall Adaptive Security Appliance (ASA)布建至Cisco Security Manager (CSM)的程式。

必要條件

需求

思科建議您瞭解以下主題：

- 安全防火牆ASA
- CSM

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全防火牆ASA版本9.18.3
- CSM版本4.28

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

CSM有助於實現一致的策略實施和安全事件快速故障排除，從而提供整個安全部署的摘要報告。藉助其集中式介面，組織可以高效地擴展和管理範圍廣泛的思科安全裝置，同時提高可視性。

設定

在下一個示例中，虛擬ASA調配到CSM以進行集中管理。

組態

為HTTPS管理配置ASA

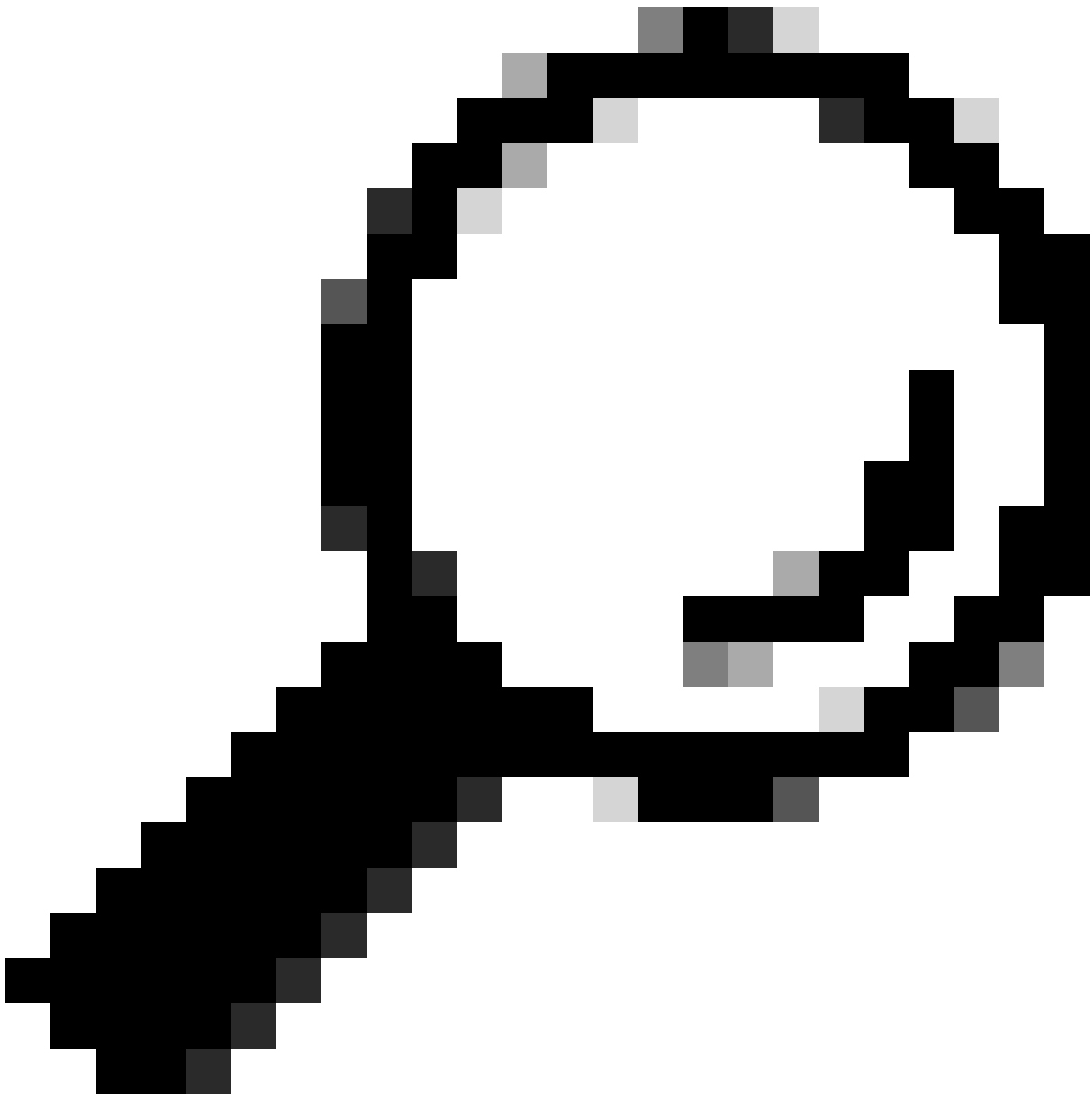
步驟 1. 建立具有所有許可權的使用者。

命令列(CLI)語法：

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

這將轉換為下一個命令示例，其中使用者csm-user和口令cisco123如下所示：

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



提示：外部身份驗證的使用者也接受此整合。

步驟 2. 啟用HTTP伺服器。

命令列(CLI)語法：

```
configure terminal  
http server enable
```

步驟 3. 允許CSM伺服器IP地址的HTTPS訪問。

命令列(CLI)語法：

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

這將轉換為下一個命令示例，該示例允許任何網路透過外部介面(GigabitEthernet0/0)上的HTTPS訪問ASA：

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

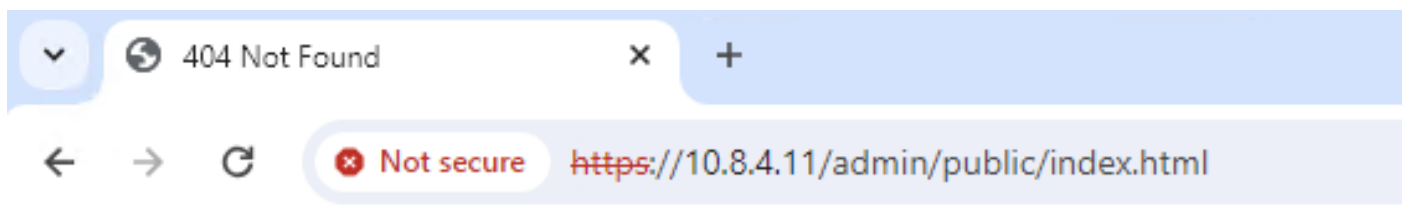
步驟 4. 驗證是否可從CSM伺服器訪問HTTPS。

開啟任何Web瀏覽器並鍵入下一個語法：

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

下面是上一步中允許HTTPS訪問的外部介面IP地址的示例：

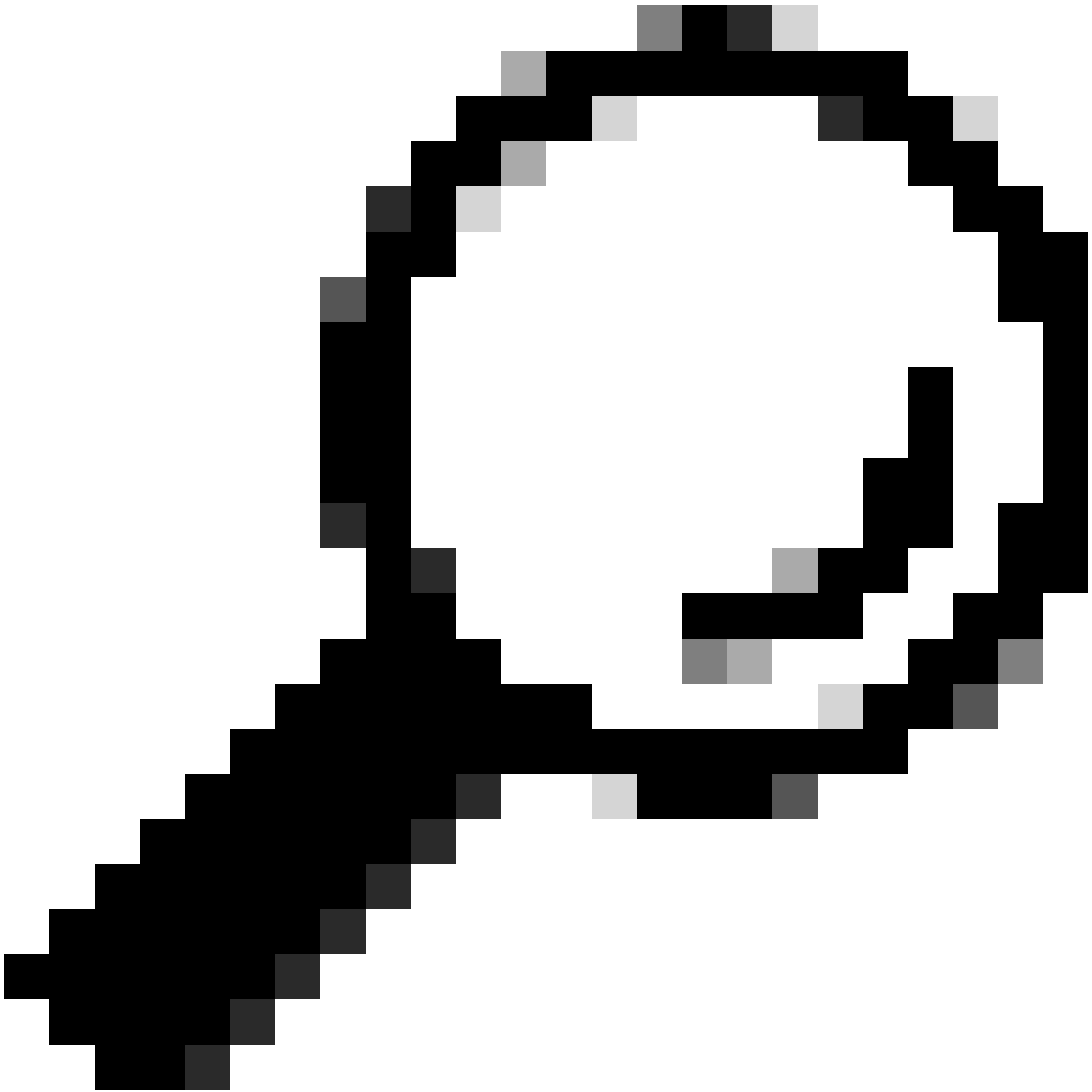
```
https://10.8.4.11/
```



404 Not Found

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

ASA HTTPS響應



提示：在此步驟中可能會出現Error 404 Not Found，因為此ASA未安裝思科自適應安全裝置管理器(ASDM)，但頁面重定向到URL /admin/public/index.html時存在HTTPS響應。

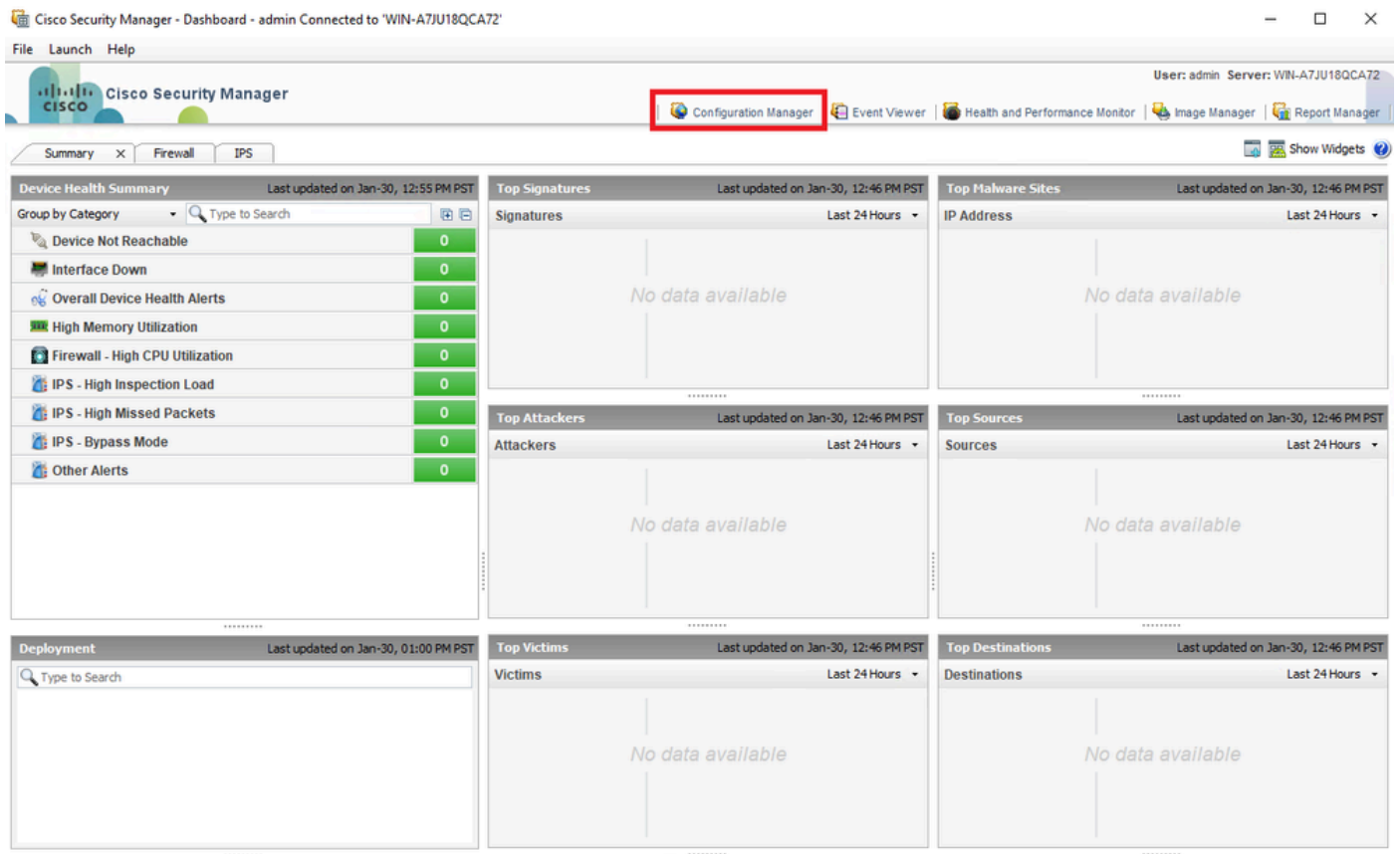
將安全防火牆ASA調配到CSM

步驟 1. 打開並登入到CSM客戶端。

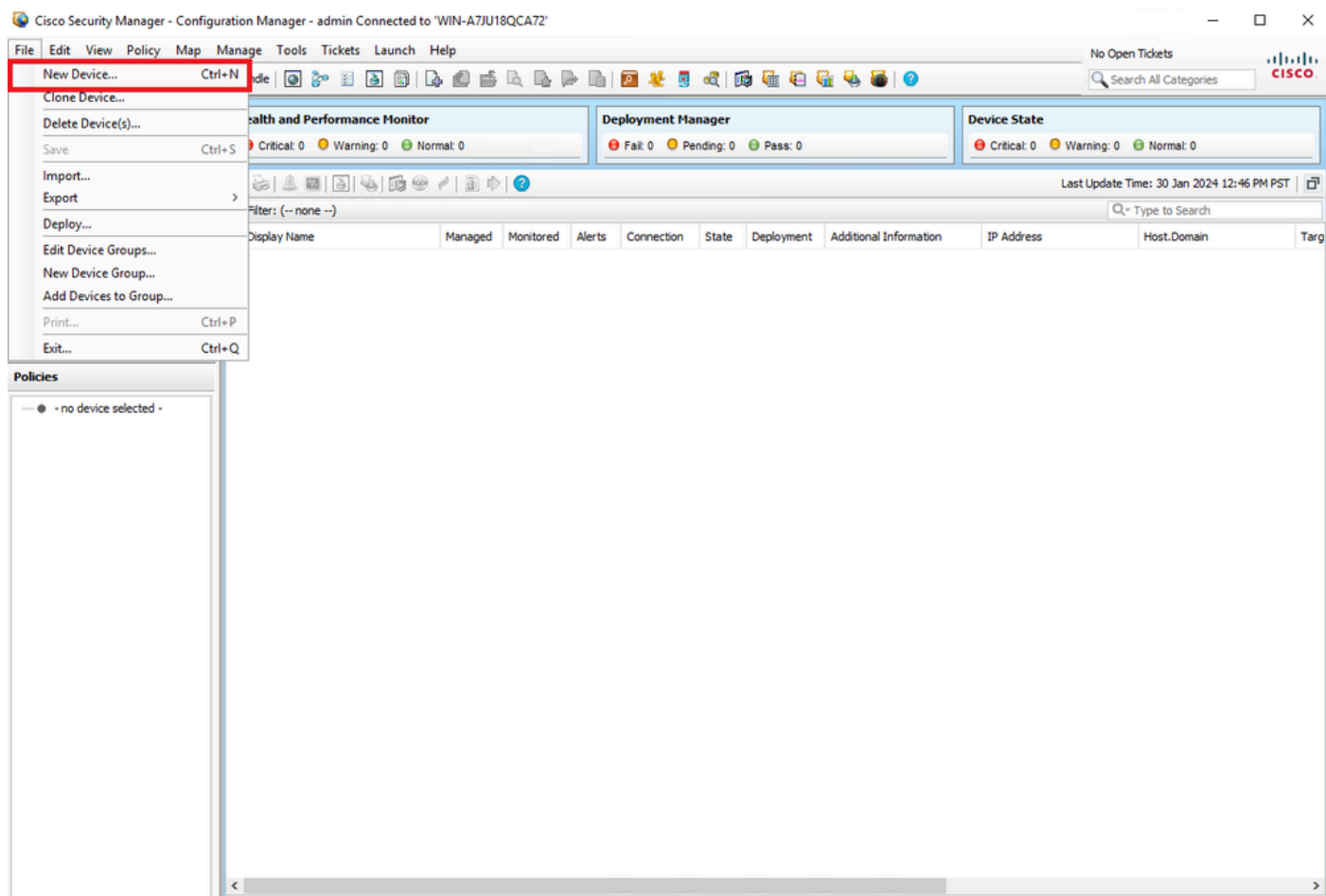


CSM客戶端登入

步驟 2. 開啟Configuration Manager。



步驟 3. 導航到裝置>新裝置。



步驟 4. 根據所需結果選擇滿足需求的增加選項。由於網路中已設定配置的ASA，因此本示例的最佳選項是Add Device From Network，然後按一下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

裝置增加方法

步驟 5. 根據安全防火牆ASA上的配置和發現設定，完成所需資料。然後按一下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

ASA設定

步驟 6. 從ASA上已配置的CSM使用者和enable密碼完成所需的憑據。

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憑證

步驟 7.選擇所需的組或在不需要的情況下跳過此步驟，然後按一下**Finish**。

Select the groups that this device belongs to:

Department:

Location:

test:

Set Values as Default

Back

Next

Finish

Cancel

Help

CSM組選擇

步驟 8.票證請求出於控制目的而生成，請點選**確定**。

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票證建立







步驟 9. 驗證發現是否完成並且沒有錯誤，然後按一下Close。

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

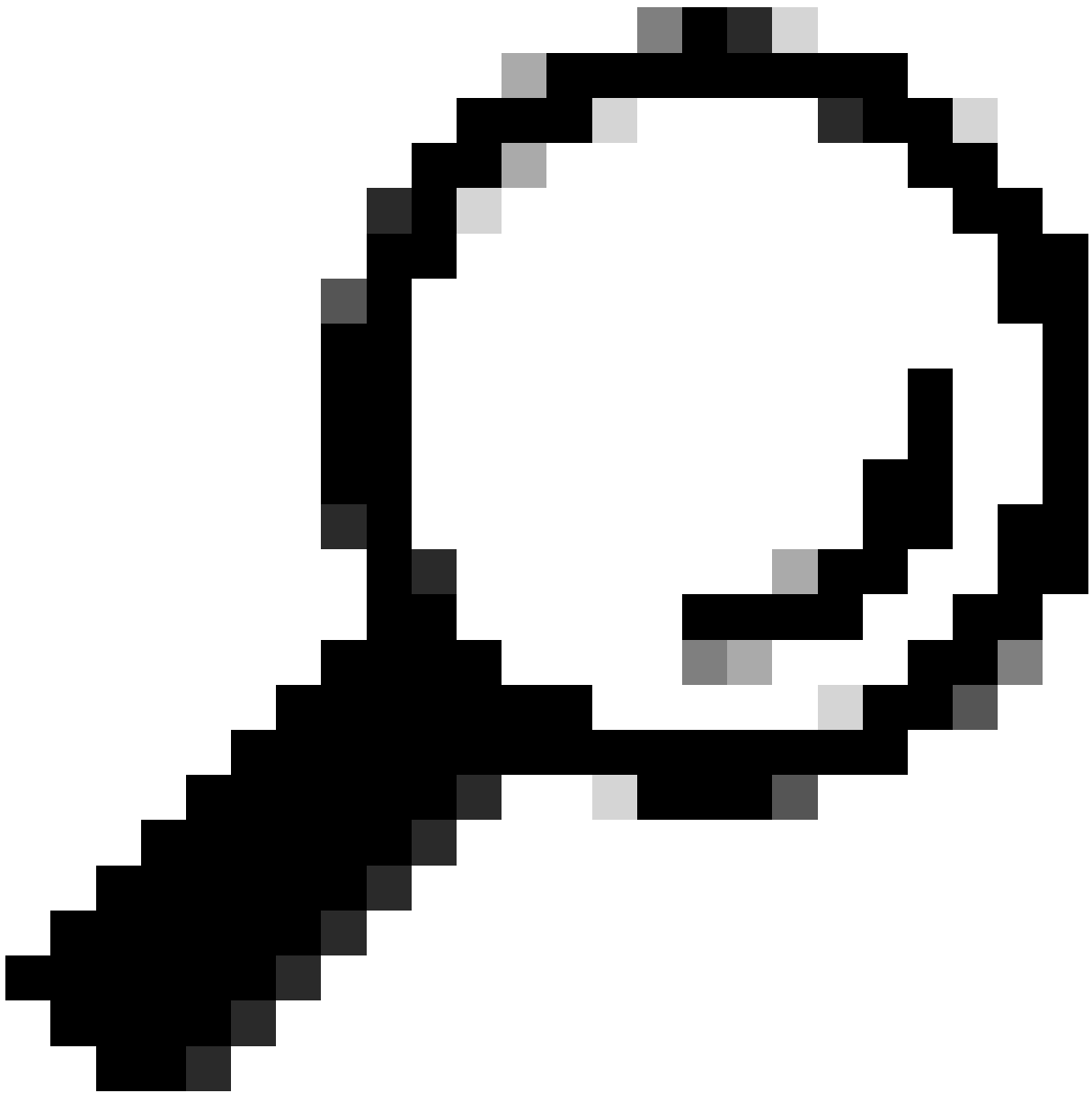
Messages	Severity	Description
CLI not discovered		Policy discovery does not support the following CLI in your configuration: Line 5:service-module 0 keepalive-timeout 4 Line 6:service-module 0 keepalive-counter 6 Line 8:license smart Line 12:no mac-address auto Line 50:no failover wait-disable Line 55:no 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

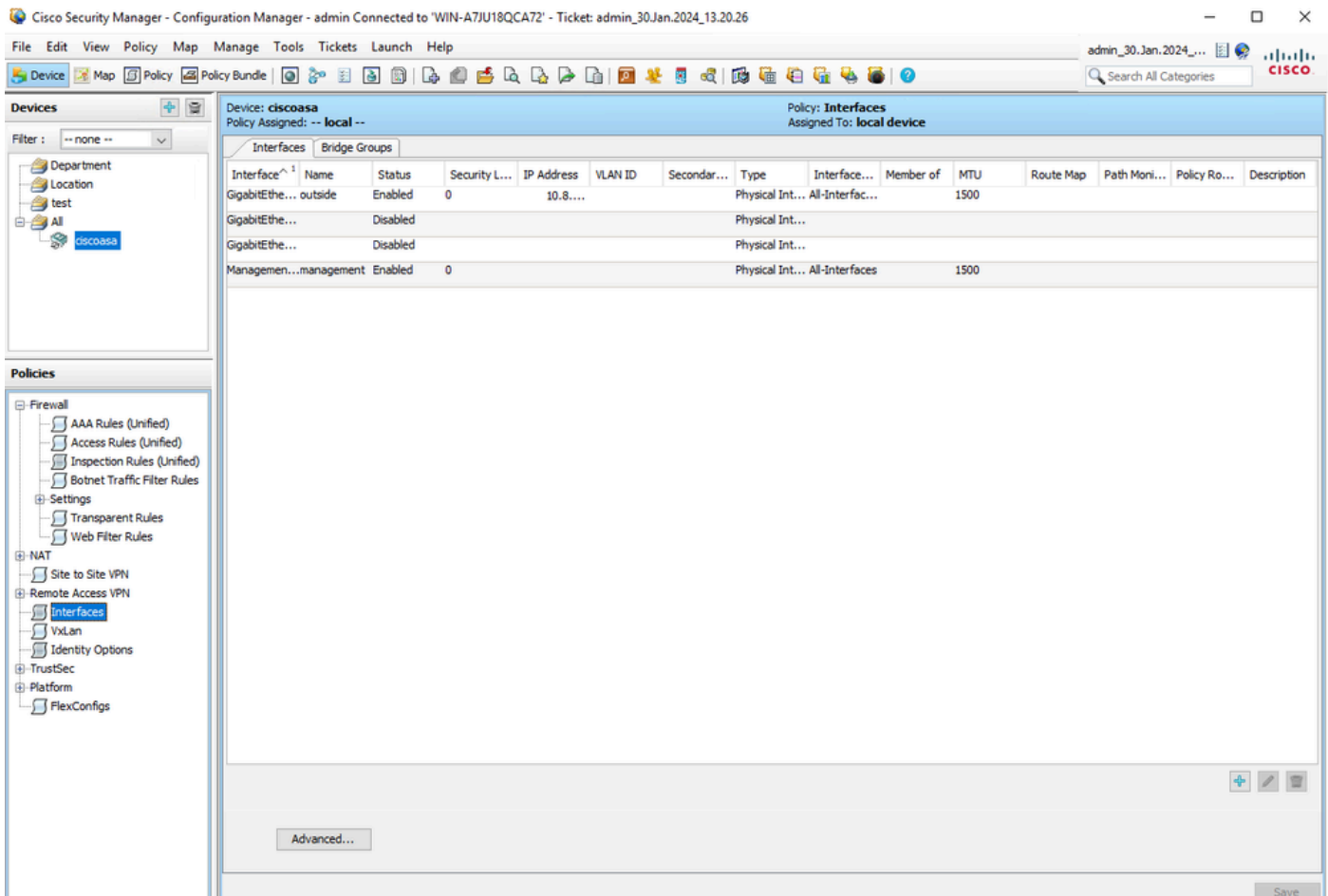
Close

Help



提示：由於CSM不支援所有ASA功能，因此警告被接受為成功輸出。

步驟 10. 驗證ASA現在在CSM客戶端上顯示為已註冊狀態，並顯示正確的資訊。



已註冊ASA資訊

驗證

ASA上提供HTTPS調試用於故障排除。使用下一個命令：

```
debug http
```

下面是成功的CSM註冊調試的示例：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。