Provision Secure Firewall ASA to CSM

Contents

Introduction

This document describes the process to provision Secure Firewall Adaptive Security Appliance (ASA) to Cisco Security Manager (CSM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall ASA
- CSM

Components Used

The information in this document is based on these software and hardware versions:

- Secure Firewall ASA version 9.18.3
- CSM version 4.28

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

CSM helps to enable consistent policy enforcement and rapid troubleshooting of security events, offering summarized reports across the security deployment. Using its centralized interface, organizations can scale efficiently and manage a wide range of Cisco security devices with improved visibility.

Configure

In the next example, a virtual ASA is provisioned to a CSM for centralized management.

Configurations

Configure ASA for HTTPS Management

Step 1. Create a user with all privileges.

Command Line (CLI) syntax:

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

This translates into the next command example, which has the user **csm-user** and password **cisco123** as follows:

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

Tip: Externally authenticated users are accepted for this integration as well.

Step 2. Enable HTTP server.

Command Line (CLI) syntax:

```
configure terminal
http server enable
```

Step 3. Allow HTTPS access for the CSM server IP address.

Command Line (CLI) syntax:

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

This translates into the next command example, which allows any network to access the ASA through HTTPS on the **outside** interface (GigabitEthernet0/0):

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

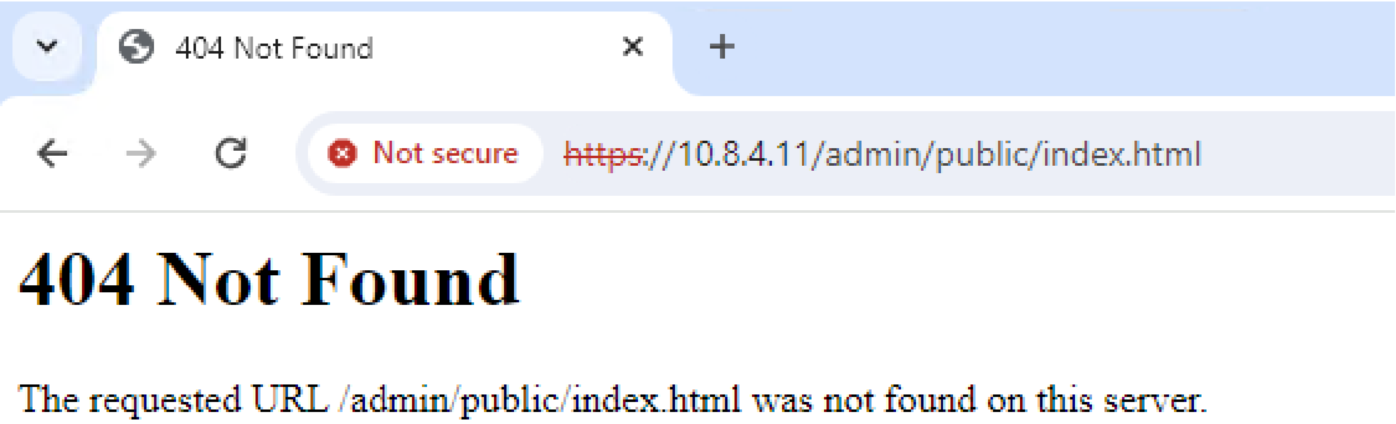
Step 4. Validate that HTTPS is reachable from the CSM server.

Open any web broser and type the next syntax:

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

This translates into the next example for the **outside** interface IP address that was allowed for HTTPS access on the previous step:

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



404 Not Found

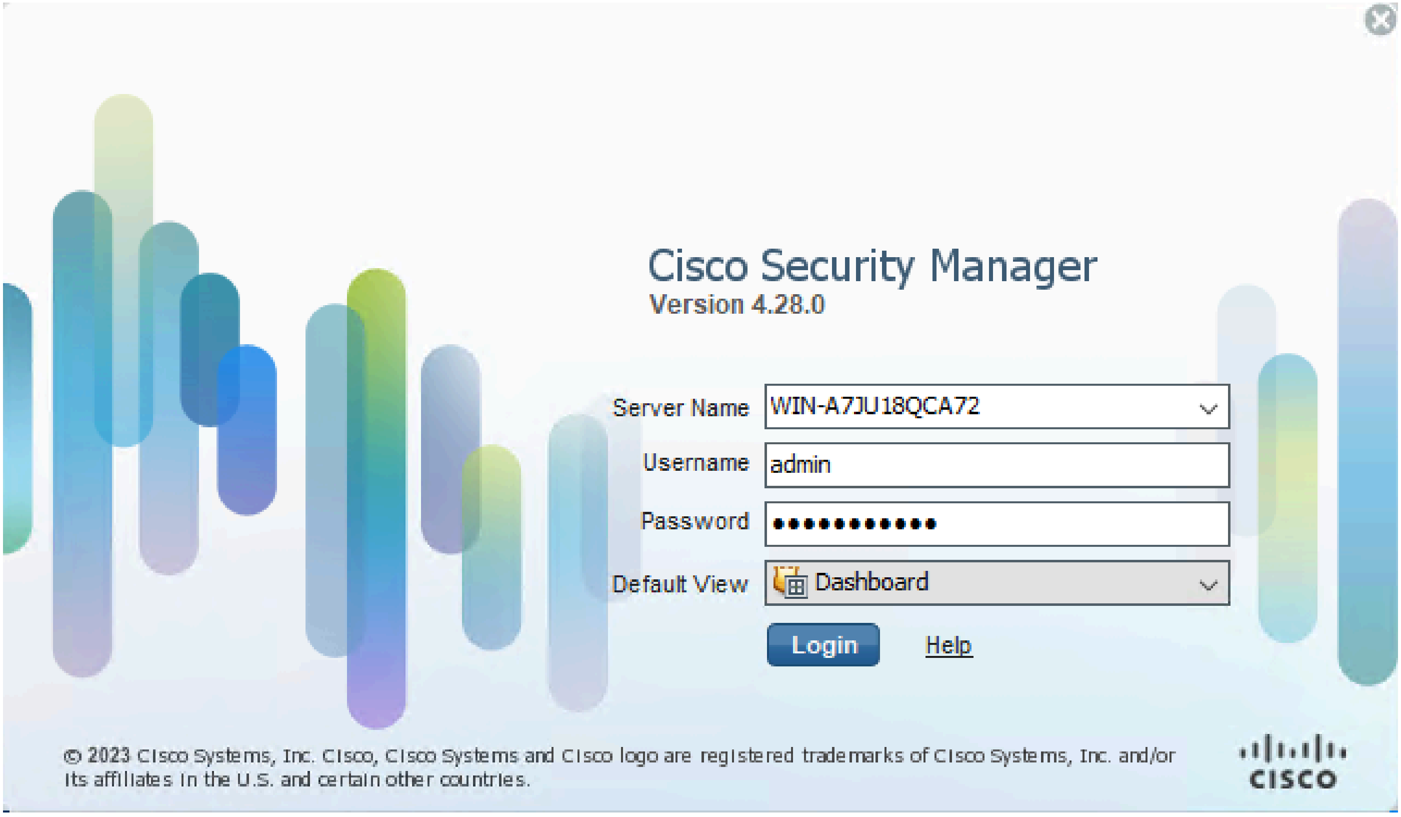
The requested URL /admin/public/index.html was not found on this server.

ASA HTTPS Response

Tip: Error **404 Not Found** is expected on this step as this ASA does not have the Cisco Adaptive Security Device Manager (ASDM) installed, but the HTTPS response is there as the page redirects to URL **/admin/public/index.html**.

Provision Secure Firewall ASA to CSM

Step 1. Open and Log into the CSM Client.



Cisco Security Manager
Version 4.28.0

Server Name: WIN-A7JU18QCA72

Username: admin

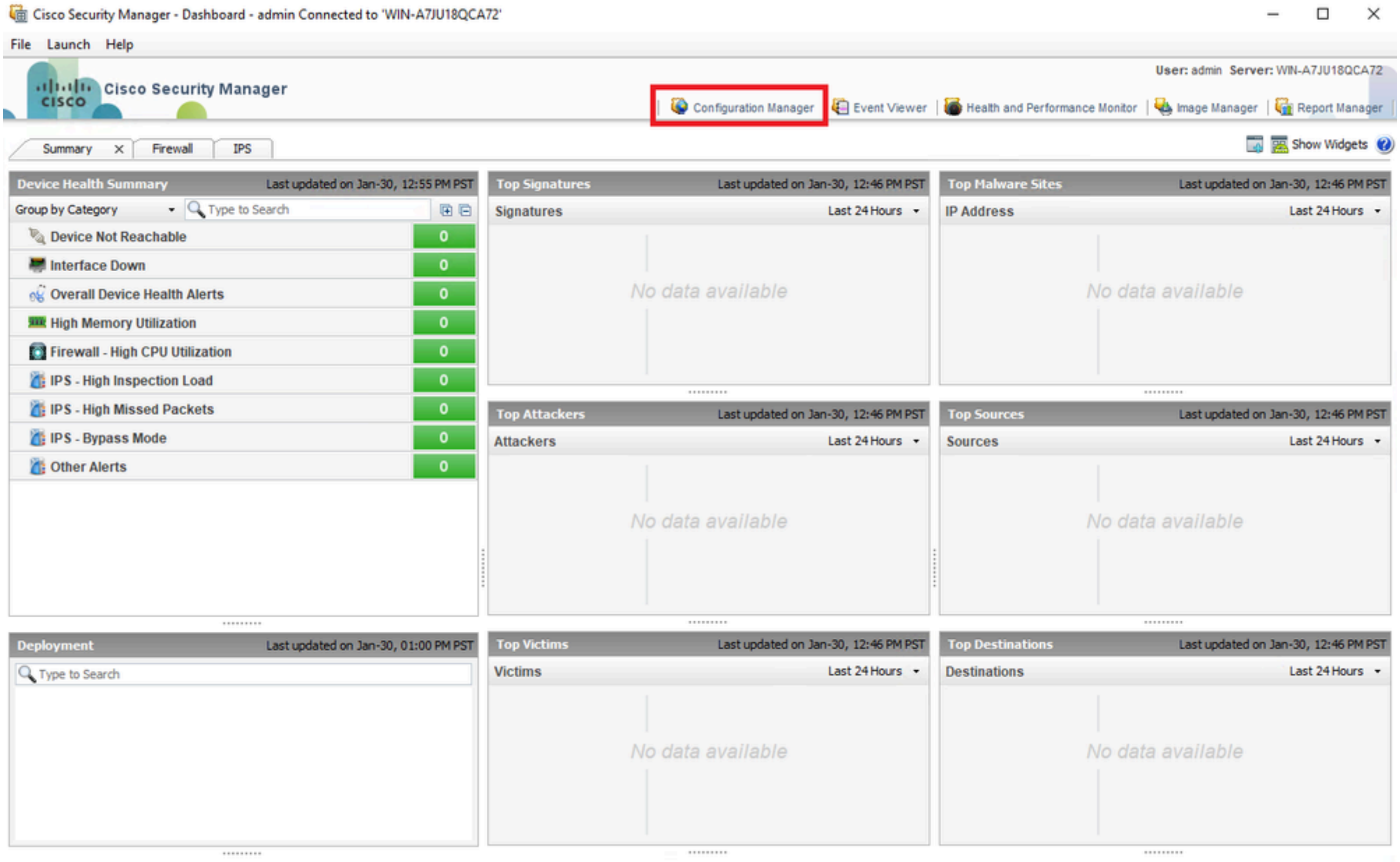
Password: ●●●●●●●●●●●

Default View: Dashboard

© 2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

CSM Client Log In

Step 2. Open the Configuration Manager.



Cisco Security Manager - Dashboard - admin Connected to 'WIN-A7JU18QCA72'

Device Health Summary — Last updated on Jan-30, 12:55 PM PST

Group by Category — Type to Search

Device Not Reachable	0
Interface Down	0
Overall Device Health Alerts	0
High Memory Utilization	0
Firewall - High CPU Utilization	0
IPS - High Inspection Load	0
IPS - High Missed Packets	0
IPS - Bypass Mode	0
Other Alerts	0

Top Signatures — Last updated on Jan-30, 12:46 PM PST — Signatures — Last 24 Hours — No data available

Top Malware Sites — Last updated on Jan-30, 12:46 PM PST — IP Address — Last 24 Hours — No data available

Top Attackers — Last updated on Jan-30, 12:46 PM PST — Attackers — Last 24 Hours — No data available

Top Sources — Last updated on Jan-30, 12:46 PM PST — Sources — Last 24 Hours — No data available

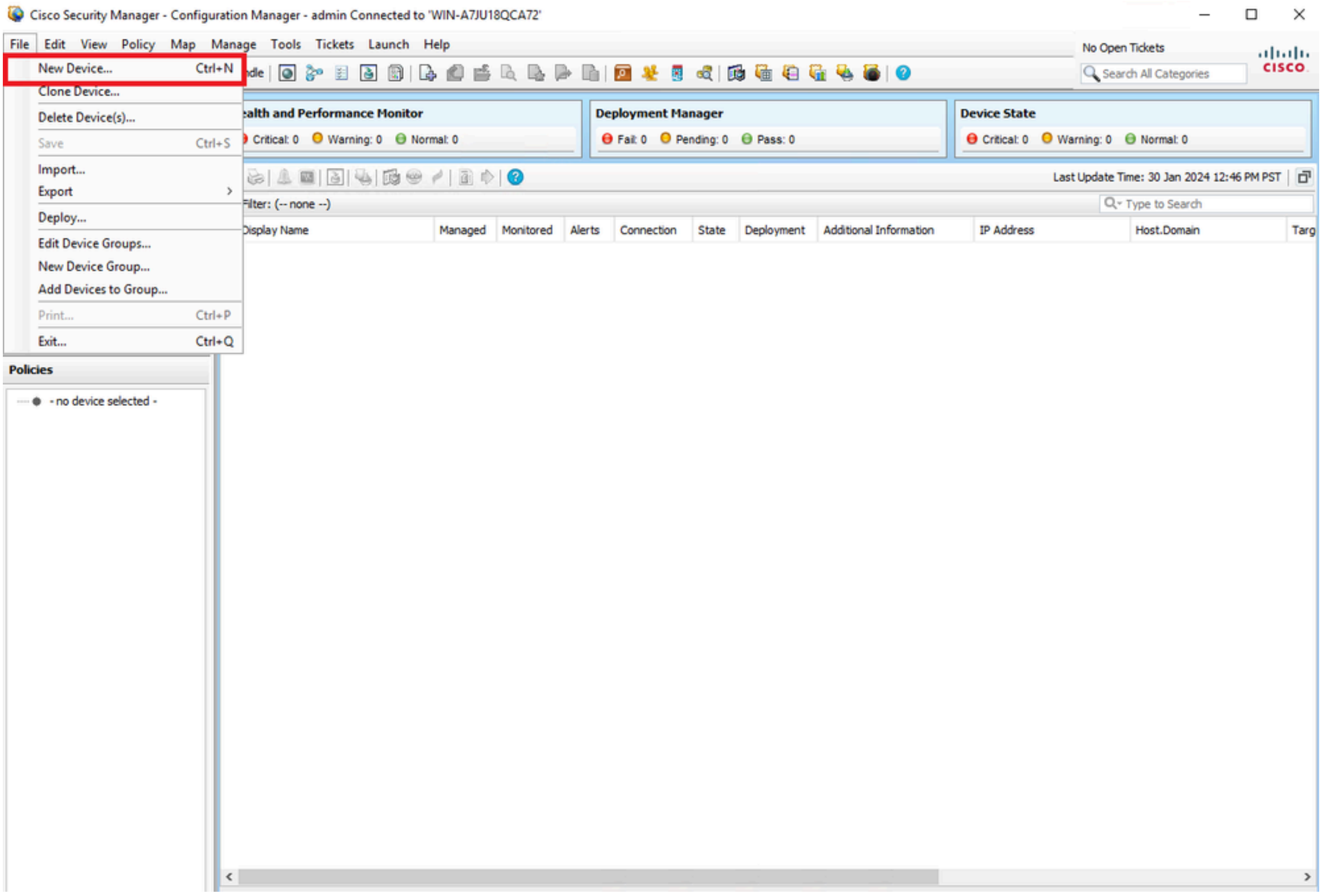
Deployment — Last updated on Jan-30, 01:00 PM PST — Type to Search

Top Victims — Last updated on Jan-30, 12:46 PM PST — Victims — Last 24 Hours — No data available

Top Destinations — Last updated on Jan-30, 12:46 PM PST — Destinations — Last 24 Hours — No data available

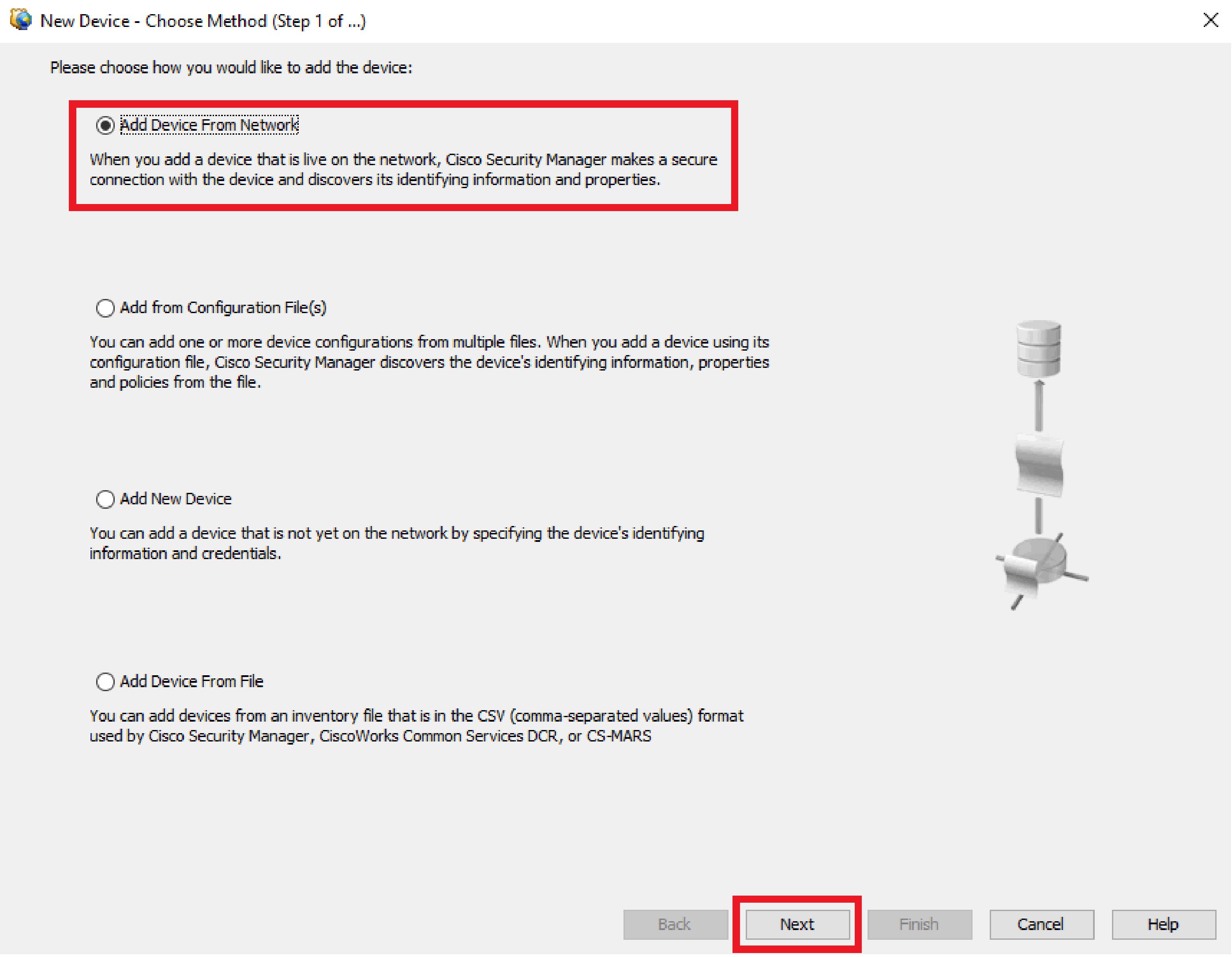
CSM Client Dashboard

Step 3. Navigate to **Devices** > **New Device**.



CSM Configuration Manager

Step 4. Select the adding option that fills the requirement according to the desired result. As the configured ASA is already setup in the network, the best option for this example is **Add Device From Network** and click on **Next**.



New Device - Choose Method (Step 1 of ...)

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

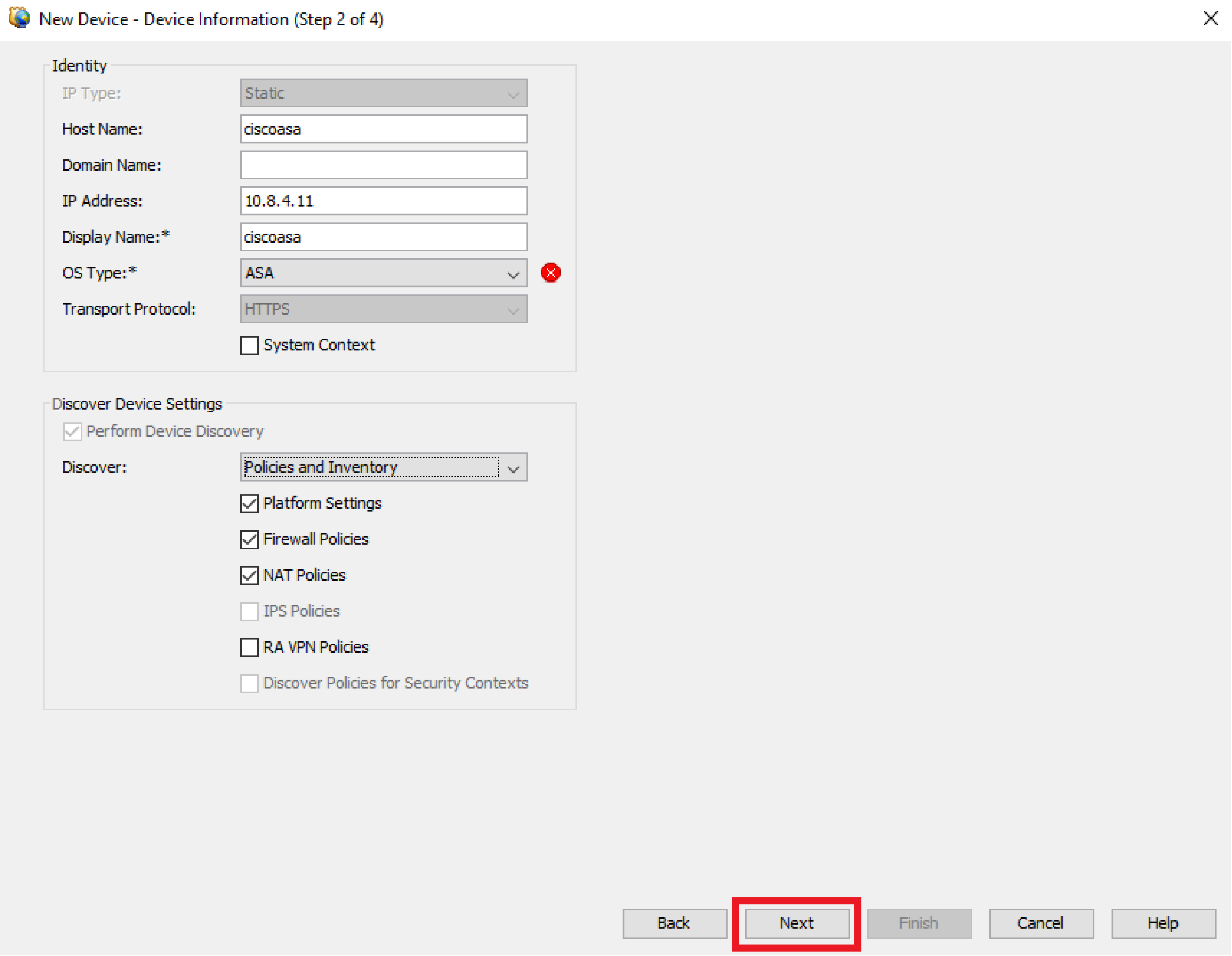
You can add a device that is not yet on the network by specifying the device's identifying information and credentials.

○ 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

Device Add Method

Step 5. Complete the required data according to the configuration on the Secure Firewall ASA, and the discovery settings. Then, click on **Next**.



New Device - Device Information (Step 2 of 4)

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

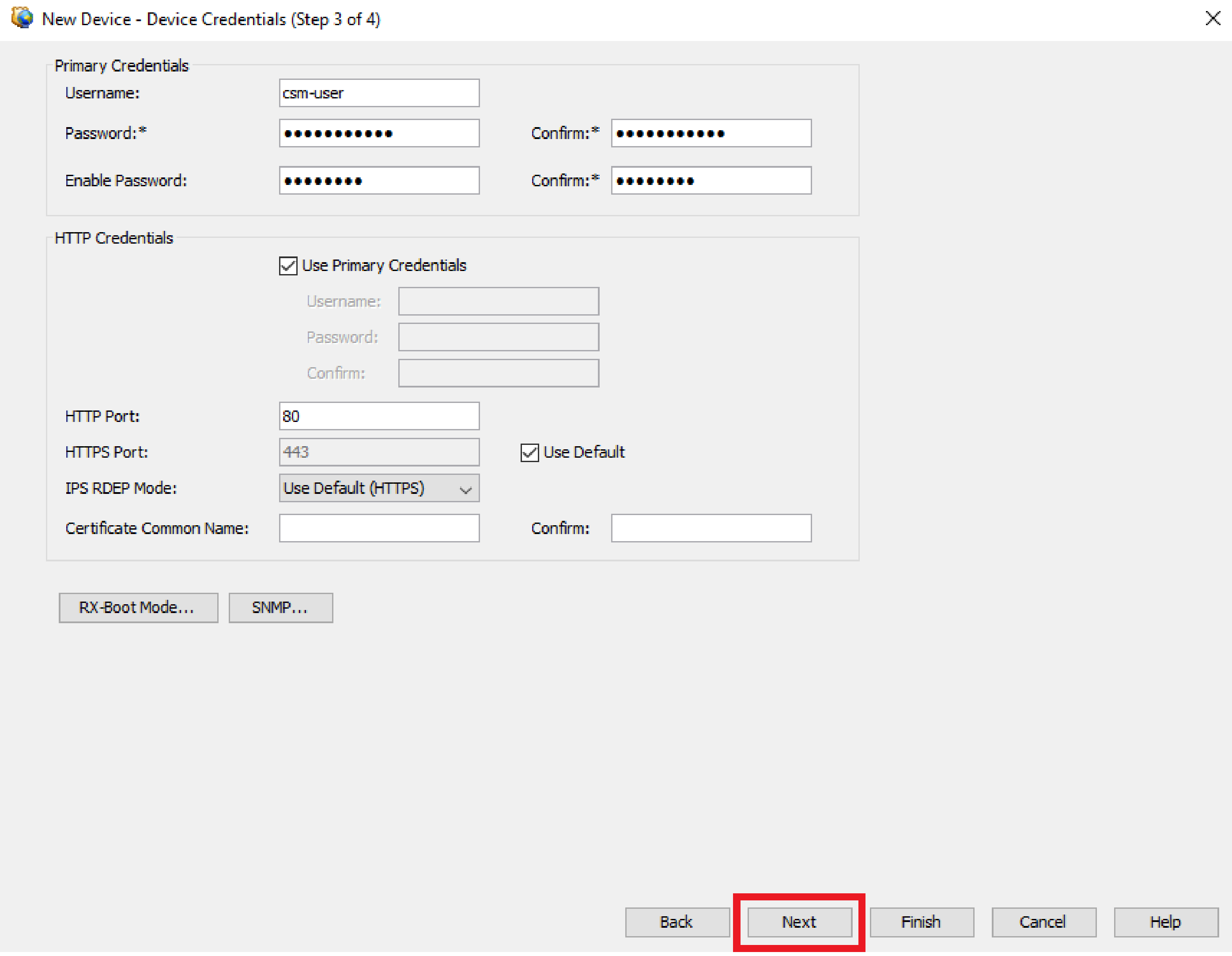
□ IPS Policies

□ RA VPN Policies

□ Discover Policies for Security Contexts

ASA Settings

Step 6. Complete the required credentials from both the configured CSM user on ASA and the **enable** password.



New Device - Device Credentials (Step 3 of 4)

Primary Credentials

Username: csm-user

Password:* ●●●●●●●●●●●● Confirm:* ●●●●●●●●●●●●

Enable Password: ●●●●●●●● Confirm:* ●●●●●●●●

HTTP Credentials

☑ Use Primary Credentials

Username:

Password:

Confirm:

HTTP Port: 80

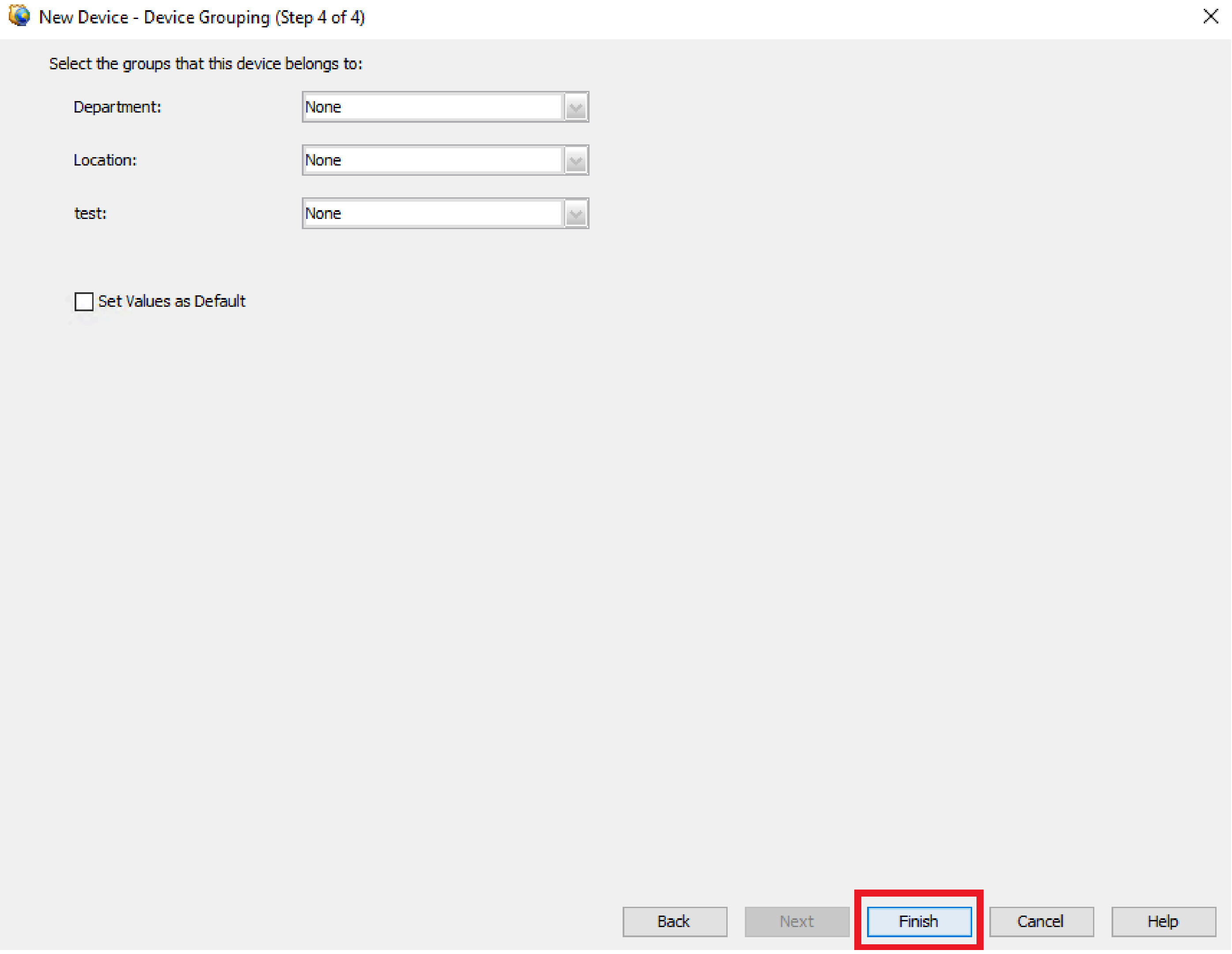
HTTPS Port: 443 ☑ Use Default

IPS RDEP Mode: Use Default (HTTPS)

Certificate Common Name: Confirm:

ASA Credentials

Step 7. Select the desired groups or skip this step if none is required and click on **Finish**.



New Device - Device Grouping (Step 4 of 4)

Select the groups that this device belongs to:

Department: None

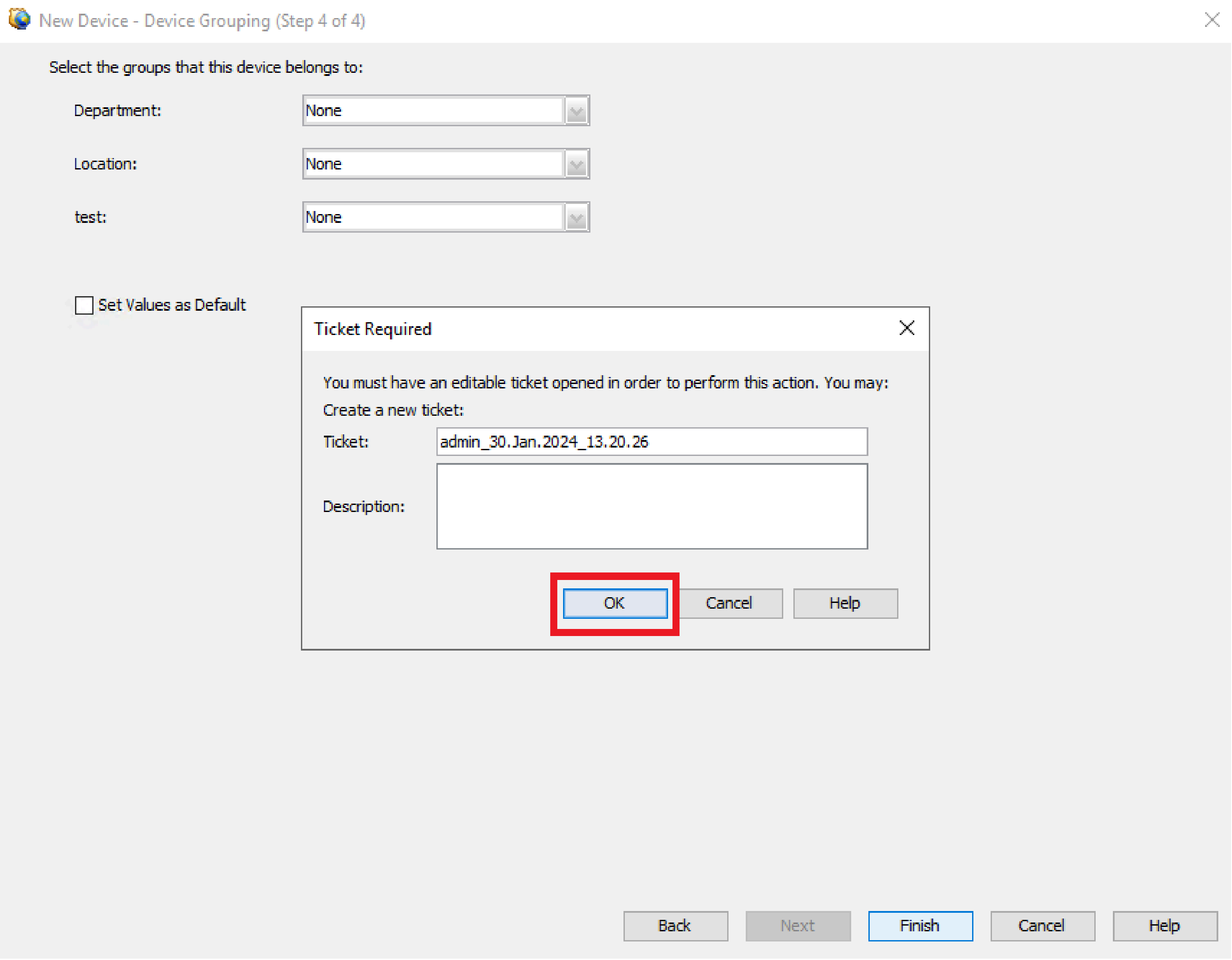
Location: None

test: None

□ Set Values as Default

CSM Group Selection

Step 8. A ticket request is generated for control purposes, click on **OK**.



Select the groups that this device belongs to:

Department: None

Location: None

test: None

□ Set Values as Default

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

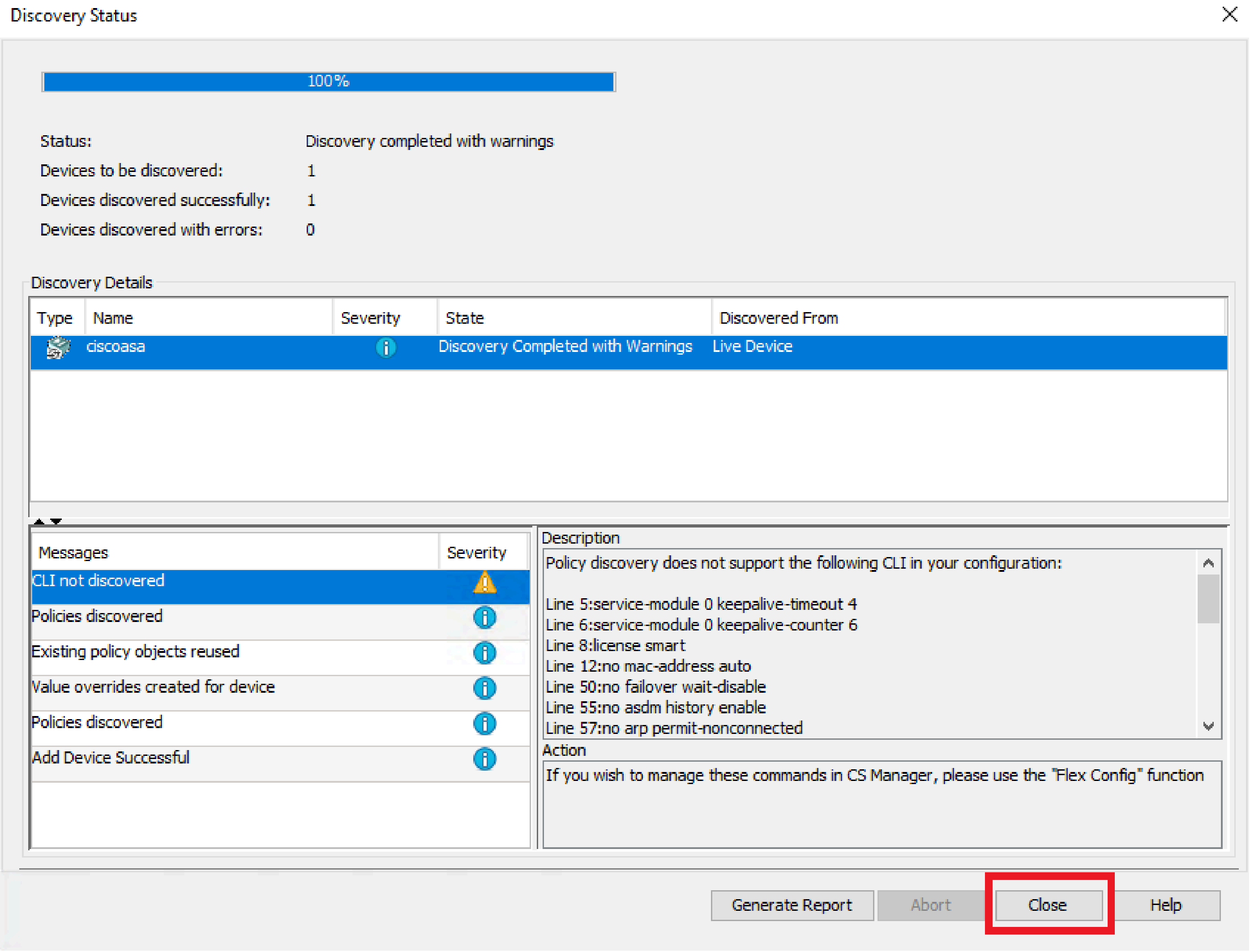
Create a new ticket:

Ticket: admin_30.Jan.2024_13.20.26

Description:

CSM Ticket Creation

Step 9. Validate that discovery finishes without errors and click on **Close**.



Discovery Status

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
CLI not discovered	⚠
Policies discovered	ⓘ
Existing policy objects reused	ⓘ
Value overrides created for device	ⓘ
Policies discovered	ⓘ
Add Device Successful	ⓘ

Description

```
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
```

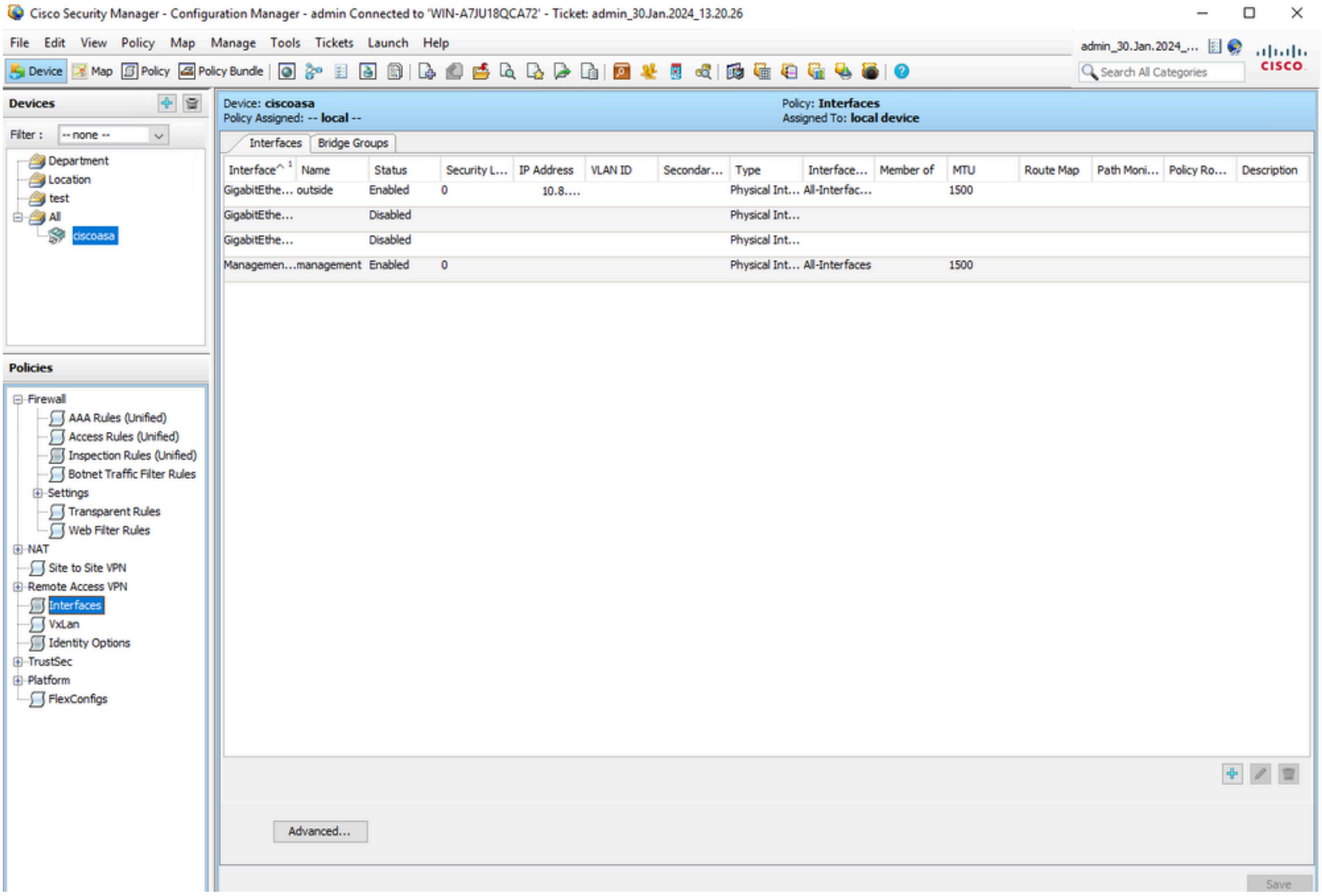
Action

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

ASA Discovery

Tip: Warnings are accepted as a successful output, as not all ASA functionalities are be supported by CSM.

Step 10. Validate that the ASA now appears as registered on the CSM client and displays the correct information.



Cisco Security Manager - Configuration Manager - admin Connected to 'WIN-A7JU18QCA72' - Ticket: admin_30.Jan.2024_13.20.26

Device: **ciscoasa**
Policy Assigned: -- **local** --

Policy: **Interfaces**
Assigned To: **local device**

Interface^ 1	Name	Status	Security L...	IP Address	VLAN ID	Secondar...	Type	Interface...	Member of	MTU	Route Map	Path Moni...	Policy Ro...	Description
GigabitEthe...	outside	Enabled	0	10.8....			Physical Int...	All-Interfac...		1500				
GigabitEthe...		Disabled					Physical Int...							
GigabitEthe...		Disabled					Physical Int...							
Managemen...	management	Enabled	0				Physical Int...	All-Interfaces		1500				

ASA Information Registered

Verify

A HTTPS debug is available on ASA for troubleshooting purposes. The next command is used:

```
debug http
```

This is an example of a successful CSM registration debug:

```
ciscoasa# debug http
debug http enabled at level 1.
ciscoasa# HTTP: processing handoff to legacy admin server [/admin/exec//show%20version]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20version HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

▒^^u

```
HTTP: processing GET URL '/admin/exec//show%20version' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/config]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/config HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒e
HTTP: processing GET URL '/admin/config' from host 10.8.4.12
HTTP: Authentication username = ''
HTTP: processing handoff to legacy admin server [/admin/exec//show%20version]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20version HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒^^u
HTTP: processing GET URL '/admin/exec//show%20version' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//sh%20module%20%7c%20in%20(CX%20Security%20
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//sh%20module%20%7c%20in%20(CX%20Security%20Services%20Processor-%7ccxsc%20ASA%
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒^2▒^aware_123▒
HTTP: processing GET URL '/admin/exec//sh%20module%20%7c%20in%20(CX%20Security%20Services%20Processor-%7
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//sh%20module%20%7c%20in%20(FirePOWER)]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//sh%20module%20%7c%20in%20(FirePOWER) HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒▒▒▒
```

```
HTTP: processing GET URL '/admin/exec//sh%20module%20%7c%20in%20(FirePOWER)' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//sh%20cluster%20info]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//sh%20cluster%20info HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒^
HTTP: processing GET URL '/admin/exec//sh%20cluster%20info' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//sh%20inventory]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//sh%20inventory HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒^^u
HTTP: processing GET URL '/admin/exec//sh%20inventory' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//sh%20vm]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//sh%20vm HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒

2▒^^^u
HTTP: processing GET URL '/admin/exec//sh%20vm' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/config]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/config HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

```
▒▒▒e
HTTP: processing GET URL '/admin/config' from host 10.8.4.12
HTTP: Authentication username = ''
HTTP: processing handoff to legacy admin server [/admin/exec//show%20version]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20version HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒^^u
HTTP: processing GET URL '/admin/exec//show%20version' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20inventory]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20inventory HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒u
HTTP: processing GET URL '/admin/exec//show%20inventory' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20password%20encryption]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20password%20encryption HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒^^
HTTP: processing GET URL '/admin/exec//show%20password%20encryption' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20running-config%20all%20tunnel-group
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20running-config%20all%20tunnel-group HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

```
▒▒▒2▒^▒^e
HTTP: processing GET URL '/admin/exec//show%20running-config%20all%20tunnel-group' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20running-config%20all%20group-policy
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20running-config%20all%20group-policy HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒2▒^▒^e
HTTP: processing GET URL '/admin/exec//show%20running-config%20all%20group-policy' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20crypto%20ca%20trustpool%20detail]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20crypto%20ca%20trustpool%20detail HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒2▒^2▒^▒^e
HTTP: processing GET URL '/admin/exec//show%20crypto%20ca%20trustpool%20detail' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20snmp-server%20engineID]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20snmp-server%20engineID HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒^P_▒
HTTP: processing GET URL '/admin/exec//show%20snmp-server%20engineID' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20version]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20version HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

```
▒▒▒▒^u
HTTP: processing GET URL '/admin/exec//show%20version' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20failover]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20failover HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒^u
HTTP: processing GET URL '/admin/exec//show%20failover' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//dir%20%2frecursive%20all-filesystems]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//dir%20%2frecursive%20all-filesystems HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒2▒^2▒^2▒^▒^e
HTTP: processing GET URL '/admin/exec//dir%20%2frecursive%20all-filesystems' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20asdm%20image]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20asdm%20image HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

▒▒▒^

2▒^^^
HTTP: processing GET URL '/admin/exec//show%20asdm%20image' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20running-config%20webvpn]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20running-config%20webvpn HTTP/1.1
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM
Cache-Control: no-cache
Pragma: no-cache
Host: 10.8.4.11
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
```

```
Connection: keep-alive

▒▒▒P_▒
HTTP: processing GET URL '/admin/exec//show%20running-config%20webvpn' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20vpn-sessiondb%20full%20webvpn]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20vpn-sessiondb%20full%20webvpn HTTP/1.1
Host: 10.8.4.1110.8.4.11
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM

▒▒▒^2▒^1
HTTP: processing GET URL '/admin/exec//show%20vpn-sessiondb%20full%20webvpn' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20vpn-sessiondb%20full%20ra-ikev1-ips
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20vpn-sessiondb%20full%20ra-ikev1-ipsec HTTP/1.1
Host: 10.8.4.1110.8.4.11
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM

▒▒▒
HTTP: processing GET URL '/admin/exec//show%20vpn-sessiondb%20full%20ra-ikev1-ipsec' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20vpn-sessiondb%20full%20ra-ikev2-ips
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20vpn-sessiondb%20full%20ra-ikev2-ipsec HTTP/1.1
Host: 10.8.4.1110.8.4.11
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM

▒▒▒
HTTP: processing GET URL '/admin/exec//show%20vpn-sessiondb%20full%20ra-ikev2-ipsec' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
HTTP: processing handoff to legacy admin server [/admin/exec//show%20vpn-sessiondb%20full%20anyconnect]
HTTP: admin session verified =  [0]
HTTP MSG: GET /admin/exec//show%20vpn-sessiondb%20full%20anyconnect HTTP/1.1
Host: 10.8.4.1110.8.4.11
Authorization: Basic OmNpc2NvMTIz
User-Agent: CSM

▒▒▒1
HTTP: processing GET URL '/admin/exec//show%20vpn-sessiondb%20full%20anyconnect' from host 10.8.4.12
HTTP: Authentication username = ''
Exited from HTTP Cli Exec
```