

Provisioning di ASA Secure Firewall per CSM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazioni](#)

[Configurazione di ASA per la gestione HTTPS](#)

[Provisioning di ASA Secure Firewall per CSM](#)

[Verifica](#)

Introduzione

In questo documento viene descritto il processo di provisioning di ASA (Secure Firewall Adaptive Security Appliance) in Cisco Security Manager (CSM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Firewall ASA
- CSM

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Firewall ASA versione 9.18.3
- CSM versione 4.28

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il modulo CSM consente l'applicazione coerente delle policy e la rapida risoluzione dei problemi relativi agli eventi di sicurezza, offrendo report riepilogativi su tutta l'implementazione della sicurezza. Grazie all'interfaccia centralizzata, le organizzazioni possono scalare in modo efficiente e gestire un'ampia gamma di dispositivi di sicurezza Cisco con una maggiore visibilità.

Configurazione

Nell'esempio successivo, un'ASA virtuale viene fornita a un CSM per la gestione centralizzata.

Configurazioni

Configurazione di ASA per la gestione HTTPS

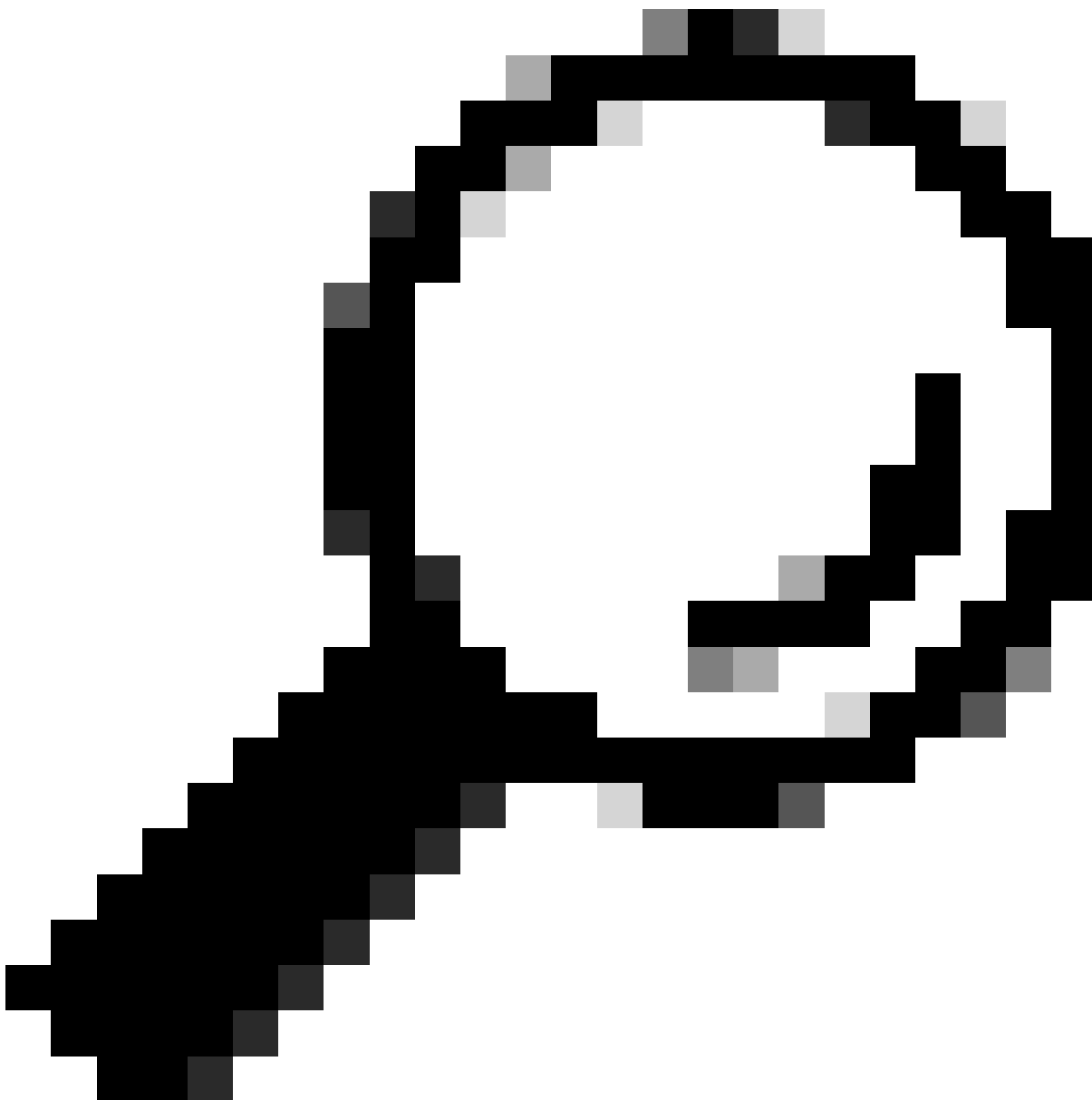
Passaggio 1. Creare un utente con tutti i privilegi.

Sintassi della riga di comando (CLI):

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

La traduzione si traduce nell'esempio di comando successivo, in cui l'utente csm-user e la password cisco123 sono i seguenti:

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



Suggerimento: Anche per questa integrazione sono accettati utenti autenticati esternamente.

Passaggio 2. Abilitare il server HTTP.

Sintassi della riga di comando (CLI):

```
configure terminal  
http server enable
```

Passaggio 3. Consentire l'accesso HTTPS per l'indirizzo IP del server CSM.

Sintassi della riga di comando (CLI):

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

Questo si traduce nell'esempio di comando successivo, che permette a qualsiasi rete di accedere all'ASA tramite HTTPS sull'interfaccia esterna (Gigabit Ethernet0/0):

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

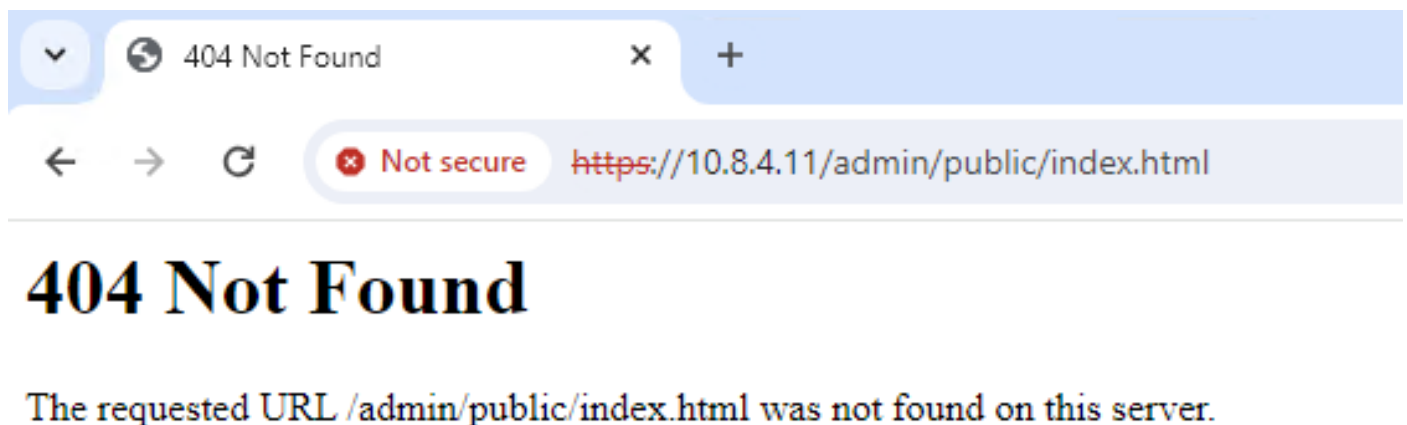
Passaggio 4. Verificare che HTTPS sia raggiungibile dal server CSM.

Aprire un browser Web e digitare la sintassi successiva:

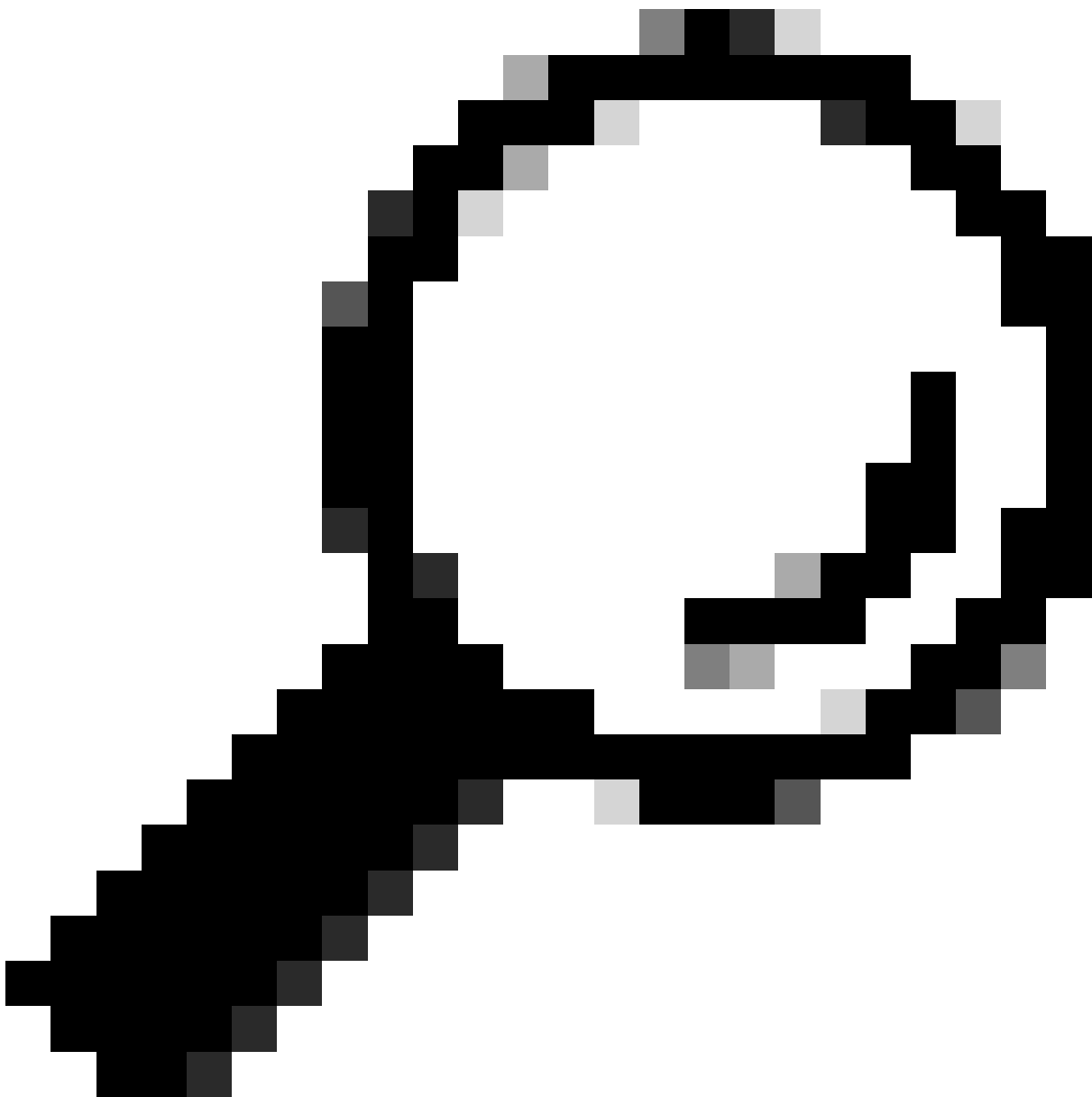
```
https://< ASA IP address >/
```

Questo si traduce nell'esempio successivo per l'indirizzo IP dell'interfaccia esterna che è stato consentito per l'accesso HTTPS nel passaggio precedente:

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



Risposta HTTPS ASA



Suggerimento: In questo passaggio è previsto l'errore 404 - Non trovato, perché sull'appliance ASA non è installato Cisco Adaptive Security Device Manager (ASDM), ma è presente la risposta HTTPS quando la pagina viene reindirizzata all'URL `/admin/public/index.html`.

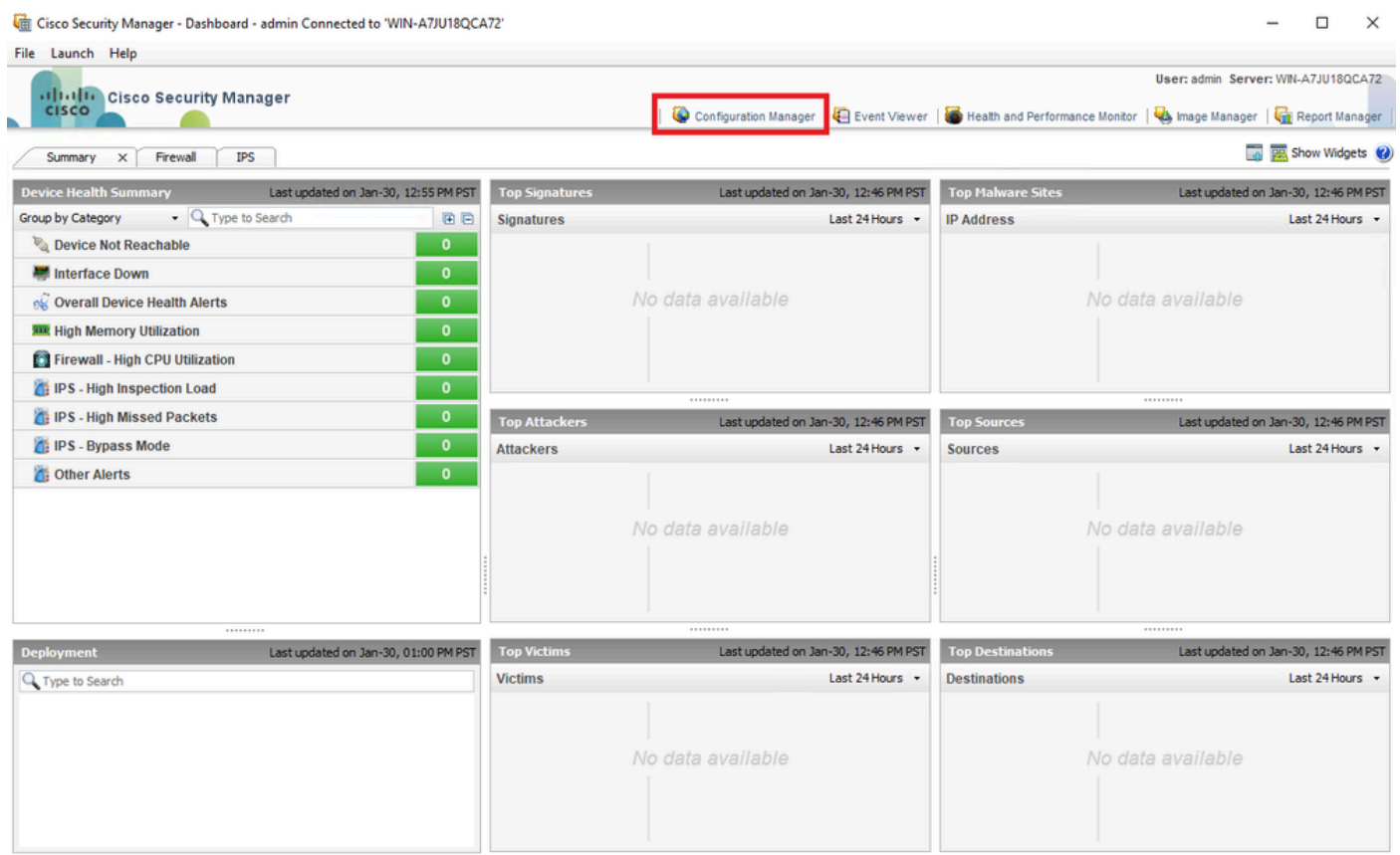
Provisioning di ASA Secure Firewall per CSM

Passaggio 1. Aprire e accedere al client CSM.

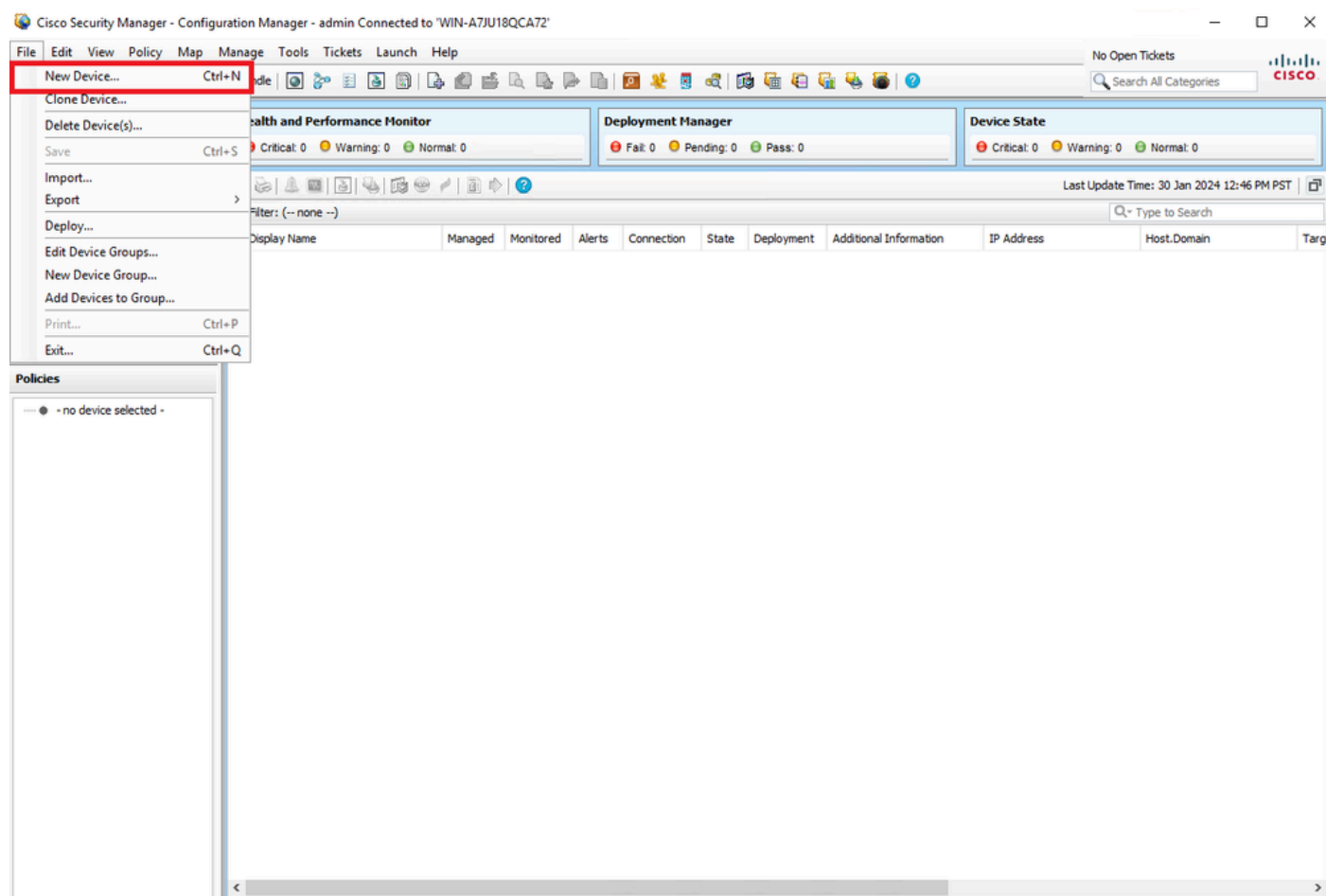


Accesso client CSM

Passaggio 2. Aprire Gestione configurazione.



Passaggio 3. Passare a Dispositivi > Nuovo dispositivo.



CSM Configuration Manager

Passaggio 4. Selezionare l'opzione di aggiunta che soddisfa il fabbisogno in base al risultato desiderato. Poiché l'ASA configurata è già configurata nella rete, l'opzione migliore per questo esempio è Add Device From Network (Aggiungi dispositivo dalla rete) e fare clic su Next (Avanti).

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

Metodo Add Dispositivo

Passaggio 5. Completare i dati richiesti in base alla configurazione sull'appliance ASA Secure Firewall e alle impostazioni di rilevamento. Quindi fai clic su Avanti.

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

Impostazioni ASA

Passaggio 6. Completare le credenziali richieste dall'utente CSM configurato sull'appliance ASA e la password di abilitazione.

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:

RX-Boot Mode...

SNMP...

Back

Next

Finish

Cancel

Help

Credenziali ASA

Passaggio 7. Selezionare i gruppi desiderati o saltare questo passaggio se non ne è richiesto alcuno e fare clic su Fine.

Select the groups that this device belongs to:

Department:

Location:

test:

☐ Set Values as Default

Selezione gruppo CSM

Passaggio 8. Una richiesta di ticket viene generata a scopo di controllo, fare clic su 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:

OK

Cancel

Help

Back

Next

Finish

Cancel

Help

Creazione ticket CSM

Passaggio 9. Verificare che il rilevamento termini senza errori e fare clic su Chiudi.

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

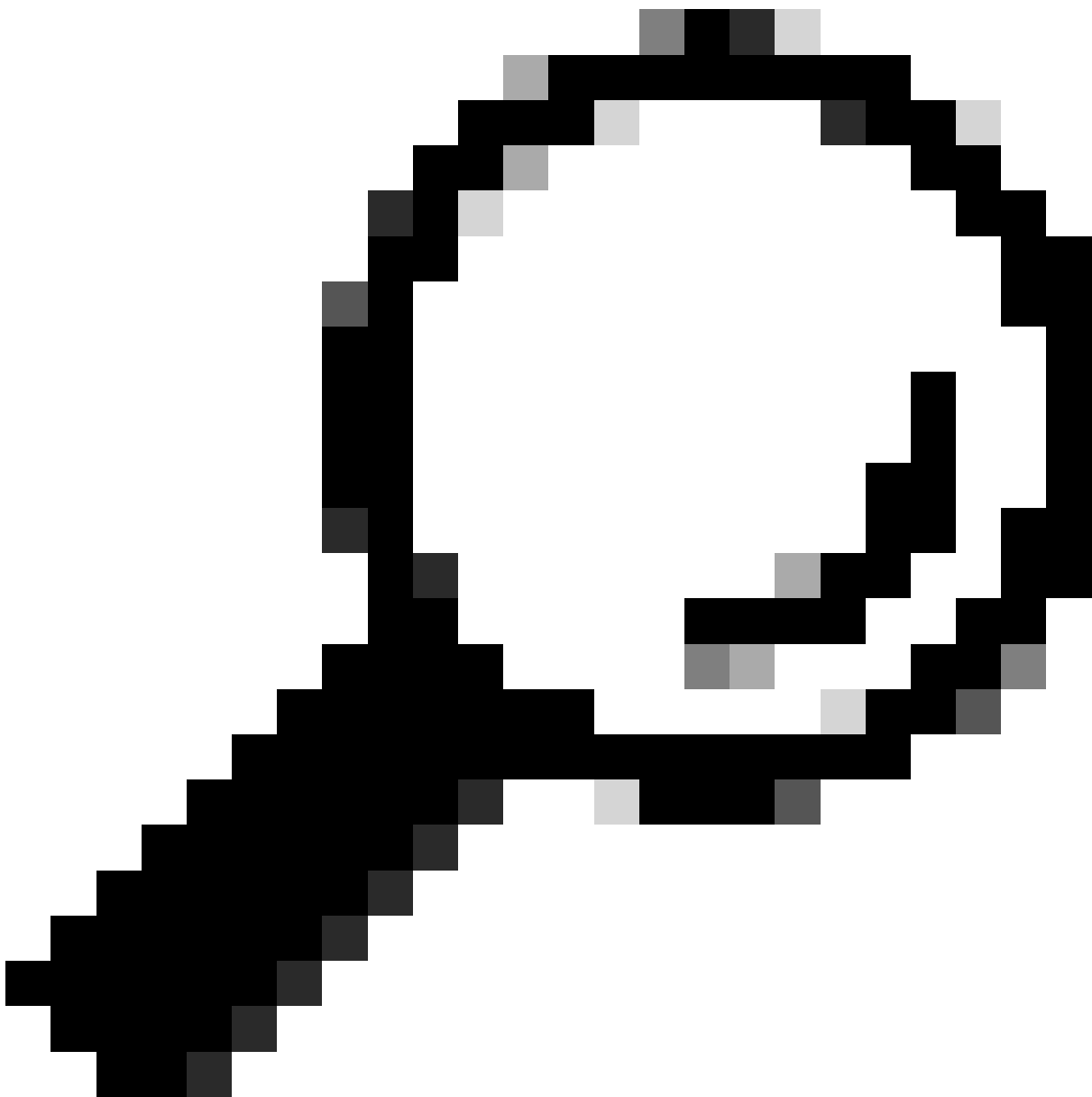
Messages	Severity	Description
CLI not discovered		Policy discovery does not support the following CLI in your configuration: Line 5:service-module 0 keepalive-timeout 4 Line 6:service-module 0 keepalive-counter 6 Line 8:license smart Line 12:no mac-address auto Line 50:no failover wait-disable Line 55:no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

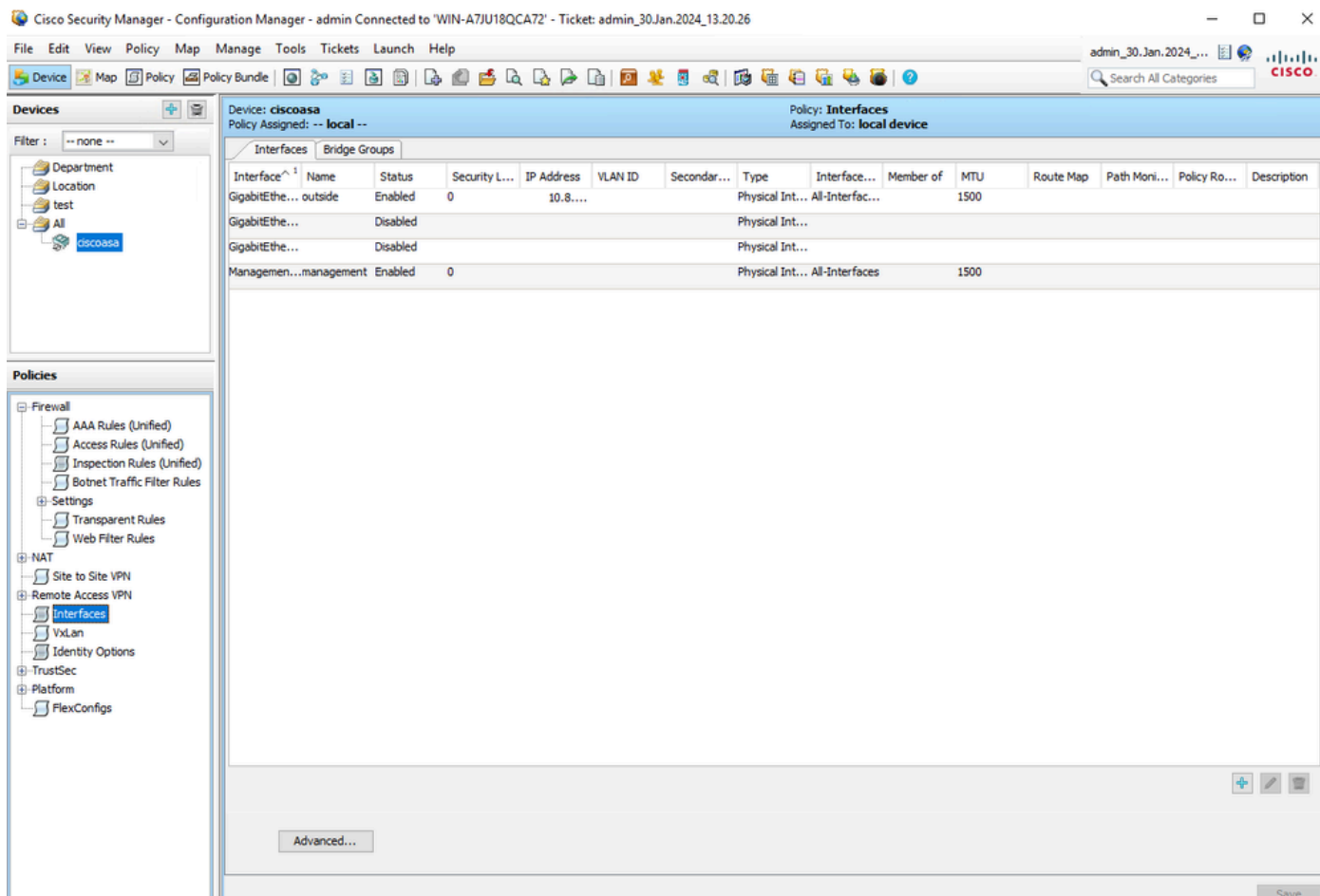
Close

Help



Suggerimento: Gli avvisi sono accettati come output positivo, in quanto non tutte le funzionalità ASA sono supportate da CSM.

Passaggio 10. Verificare che l'ASA appaia come registrata sul client CSM e visualizzi le informazioni corrette.



Informazioni ASA registrate

Verifica

Un debug HTTPS è disponibile sull'appliance ASA per la risoluzione dei problemi. Viene utilizzato il comando successivo:

```
debug http
```

Questo è un esempio di debug riuscito della registrazione del modulo CSM:

```
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%20Services%20Processor-%7ccxsc%20ASA%20CX5) HTTP/1.1
HTTP: admin session verified = [0]
HTTP MSG: GET /admin/exec//sh%20module%20%7c%20in%20(CX%20Security%20Services%20Processor-%7ccxsc%20ASA%20CX5) 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^aware_123

HTTP: processing GET URL '/admin/exec//sh%20module%20%7c%20in%20(CX%20Security%20Services%20Processor-%7ccxsc%20ASA%20CX5) HTTP/1.1
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%20recursive%20all-file systems]
HTTP: admin session verified = [0]
HTTP MSG: GET /admin/exec//dir%20%20recursive%20all-file systems 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//dir%20%20recursive%20all-file systems' 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-ipsec]
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-ipsec]
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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).