

Configura sincronizzazione da dispositivi a Security Manager

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Metodologia dimostrativa](#)

[Individuazione singola periferica](#)

[Passaggi per eseguire il rilevamento di un singolo dispositivo:](#)

[Passaggi per eseguire il rilevamento di un singolo dispositivo:](#)

[Passaggio 1:](#)

[Passaggio 2:](#)

[Bulk Device Discovery](#)

[Procedura per eseguire l'individuazione di massa dei dispositivi:](#)

[Passaggio 1:](#)

[Passaggio 2:](#)

[Passaggio 3:](#)

Introduzione

In questo documento vengono descritti diversi modi per sincronizzare la configurazione da ASA a CSM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Security Manager
- Dispositivo di sicurezza adattivo

Componenti usati

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

- Cisco Security Manager 4.25
- Appliance di sicurezza adattiva

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

Cisco Security Manager offre servizi di gestione e monitoraggio centralizzati per i dispositivi Cisco ASA.

Metodologia dimostrativa

In questo documento vengono descritti due metodi o opzioni distinti per la sincronizzazione della configurazione da ASA a CSM.

- Individuazione di un singolo dispositivo
- Rilevamento in blocco dei dispositivi

Individuazione singola periferica

È possibile eseguire un'individuazione singola solo se il dispositivo è stato aggiunto all'inventario. Può essere eseguita solo se il dispositivo

- Configurazioni del contesto di sicurezza per dispositivi ASA, PIX e FWSM in esecuzione in modalità a più contesti.
- Configurazioni dei sensori virtuali per dispositivi IPS.
- Informazioni sul modulo di servizio per i dispositivi Catalyst.

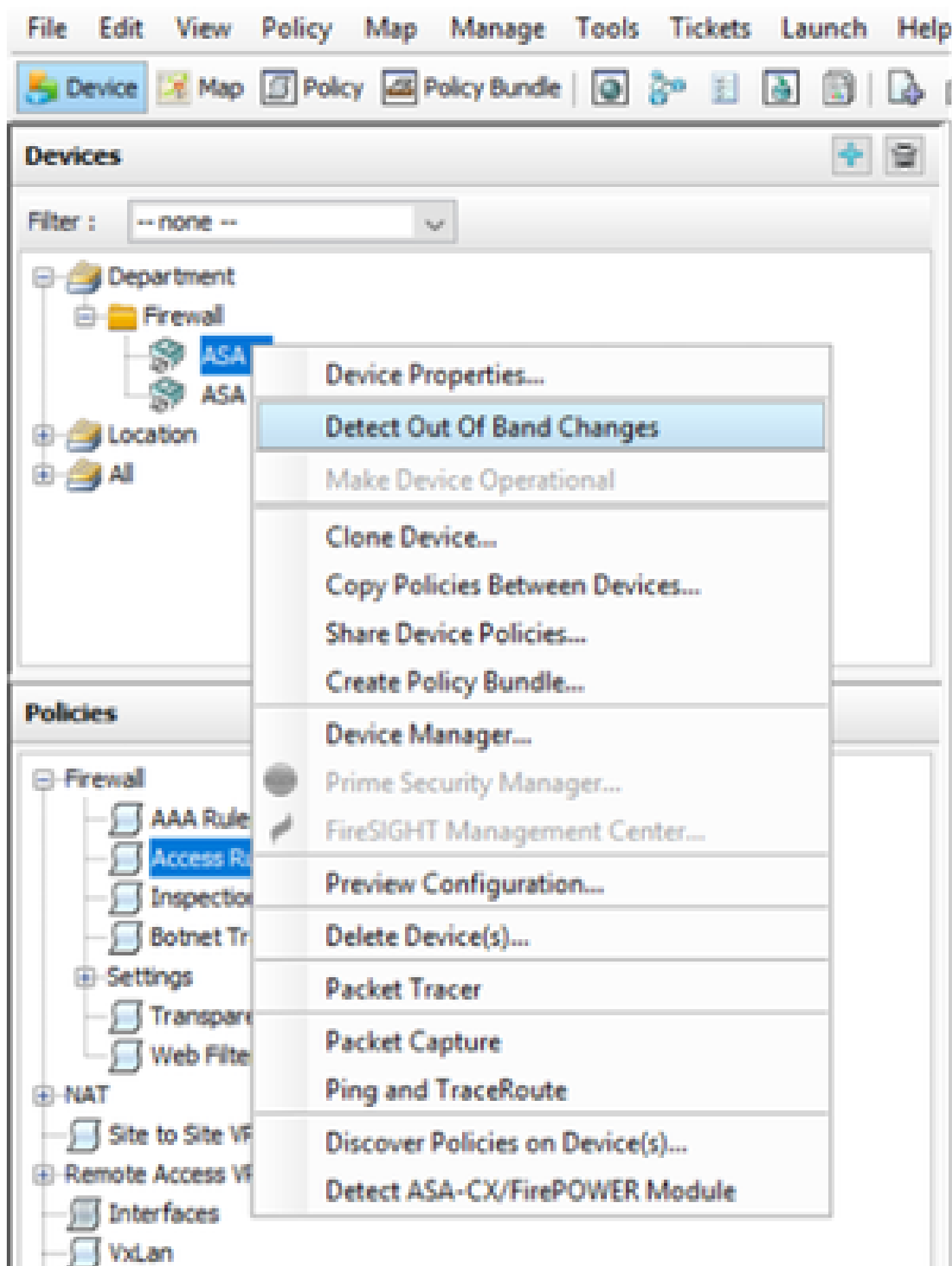
Passaggi per eseguire il rilevamento di un singolo dispositivo:

È possibile eseguire il rilevamento dei dispositivi dopo aver apportato modifiche alla CLI dei dispositivi o se il dispositivo è stato rimosso e riaggiunto.

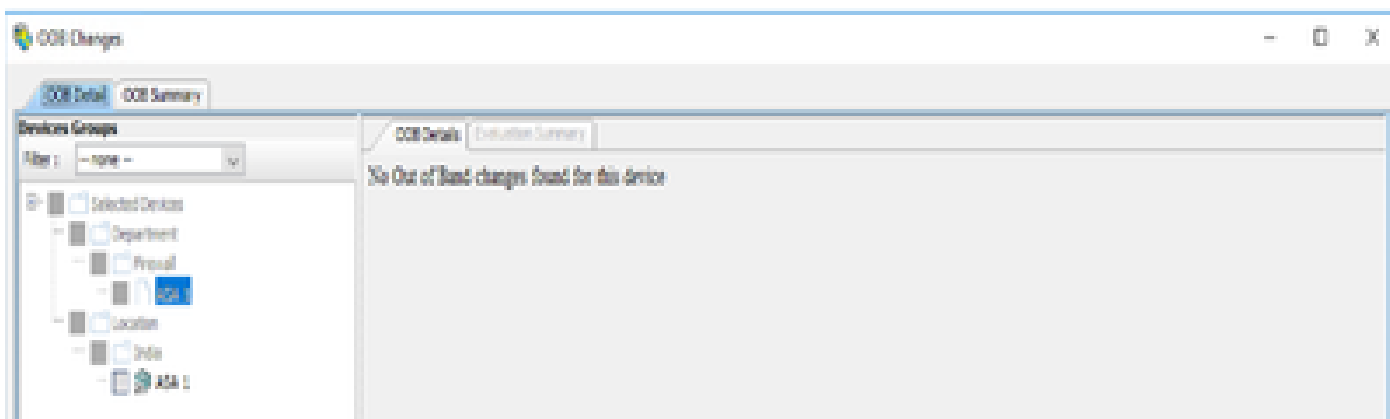
Per verificare se le modifiche in sospeso devono ancora essere sincronizzate, osservare l'esempio citato.

Fare clic con il pulsante destro del mouse sul dispositivo corrispondente nel riquadro dei dispositivi

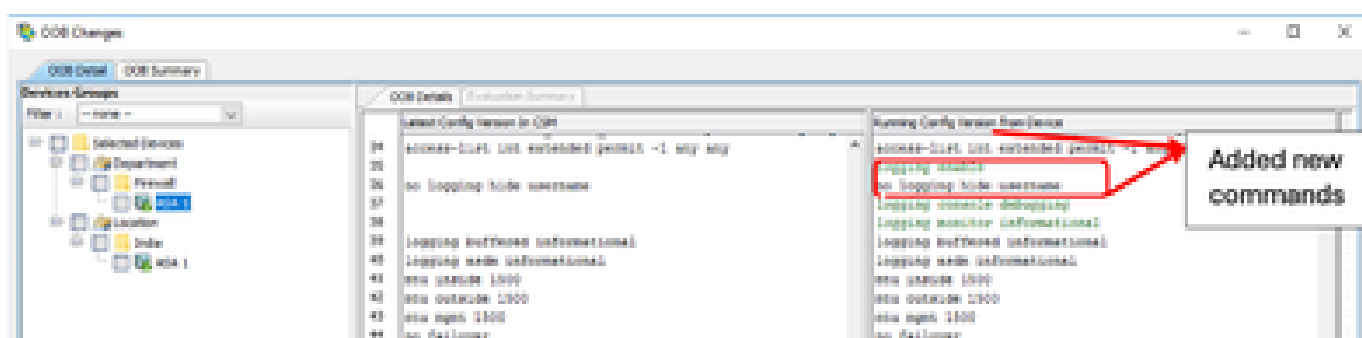
e selezionare l'opzione Rileva modifiche fuori banda.



Se non sono state rilevate modifiche, la pagina viene visualizzata come nessuna modifica non associata trovata per il dispositivo.



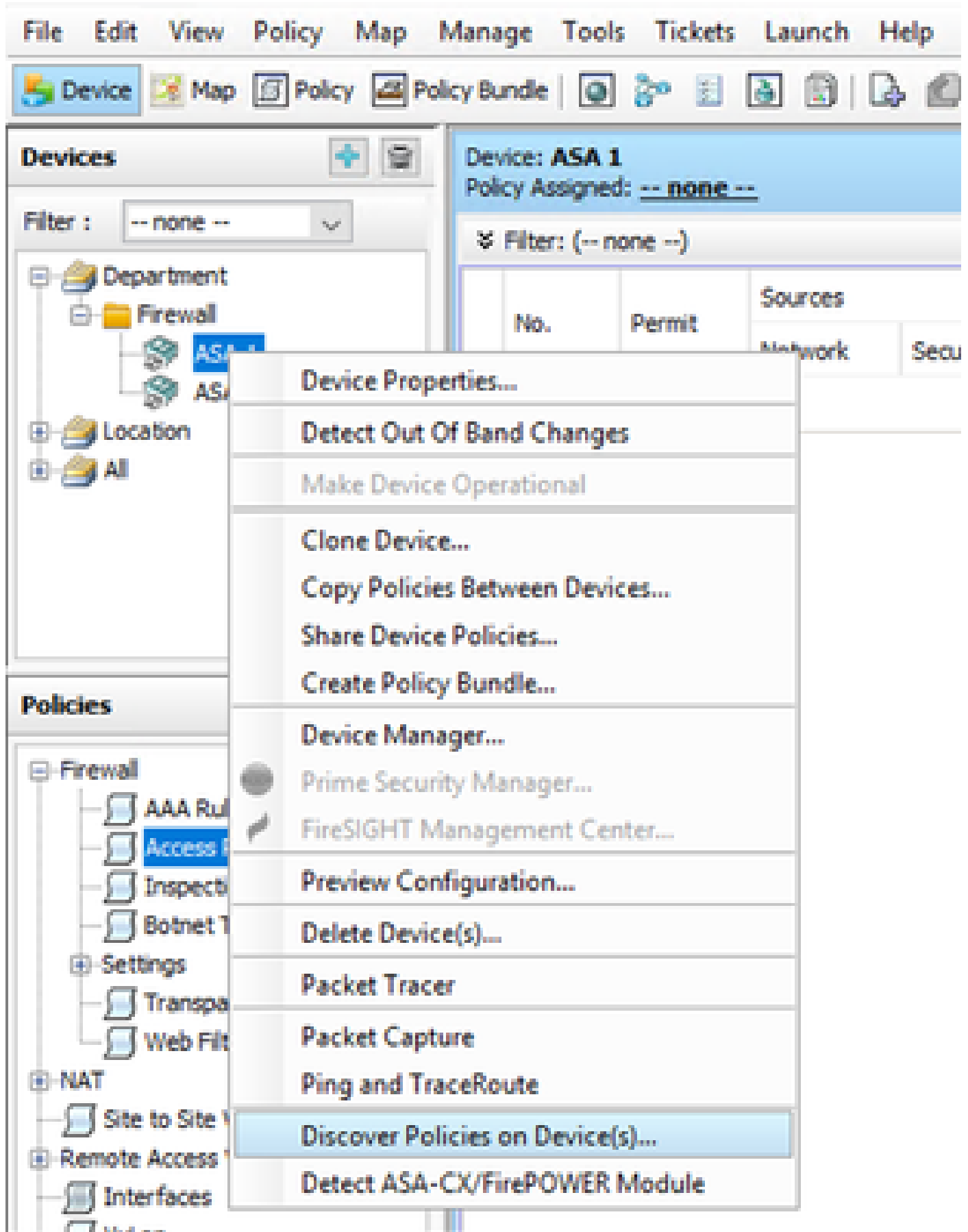
Se sono state apportate modifiche, le righe vengono evidenziate in base alla legenda.



Passaggi per eseguire il rilevamento di un singolo dispositivo:

Passaggio 1:

Fare clic con il pulsante destro del mouse sul nome del dispositivo nel riquadro del dispositivo e scegliere l'opzione Individua criteri su dispositivo/i.



Passaggio 2:

Per il metodo di recupero con un solo dispositivo è possibile visualizzare solo la finestra di dialogo Crea attività di rilevamento. Se viene visualizzata una finestra di dialogo per l'individuazione in blocco, chiuderla e riaprirla.

Sono disponibili 3 opzioni per eseguire il rilevamento.

- Live Device - Recupera la configurazione dal Live Device che si trova nella rete.
- File di configurazione - È possibile scegliere il file di configurazione e procedere con l'individuazione.
- Configurazione predefinita di fabbrica - Ripristina le configurazioni predefinite del dispositivo. Questo metodo può essere utilizzato per i dispositivi che eseguono solo la modalità a contesto singolo o con singoli contesti di protezione.

Create Discovery Task [X]

Discovery Task Name:

Discover From:

- Live Device
- Config File
- Factory Default Configuration

Config File:

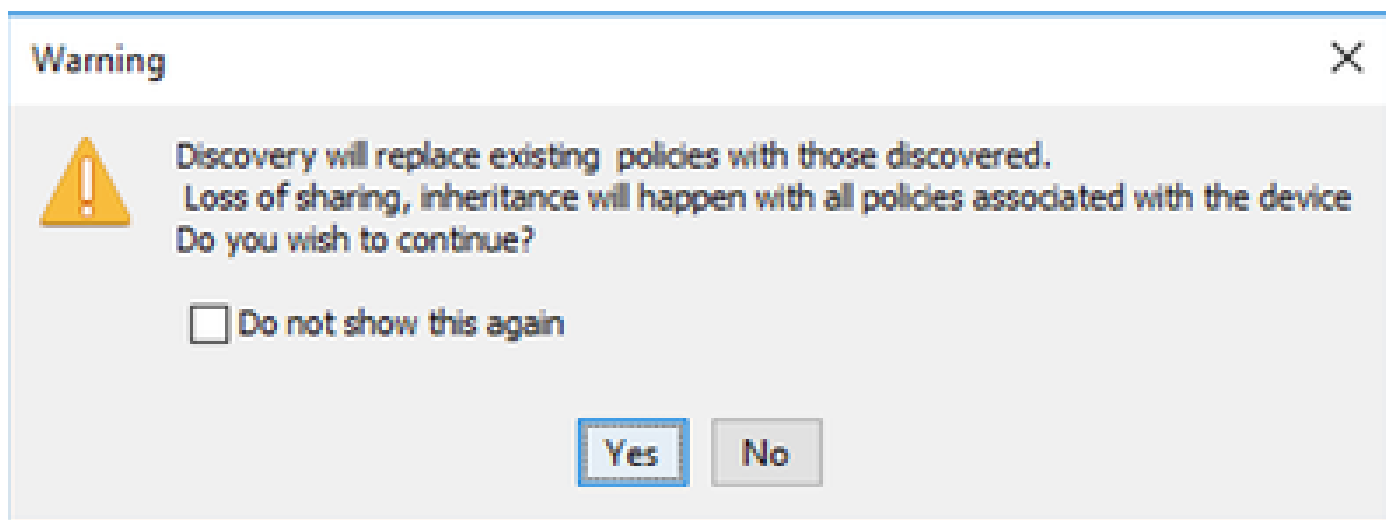
Discover Policies for Security Contexts

Policies To Discover

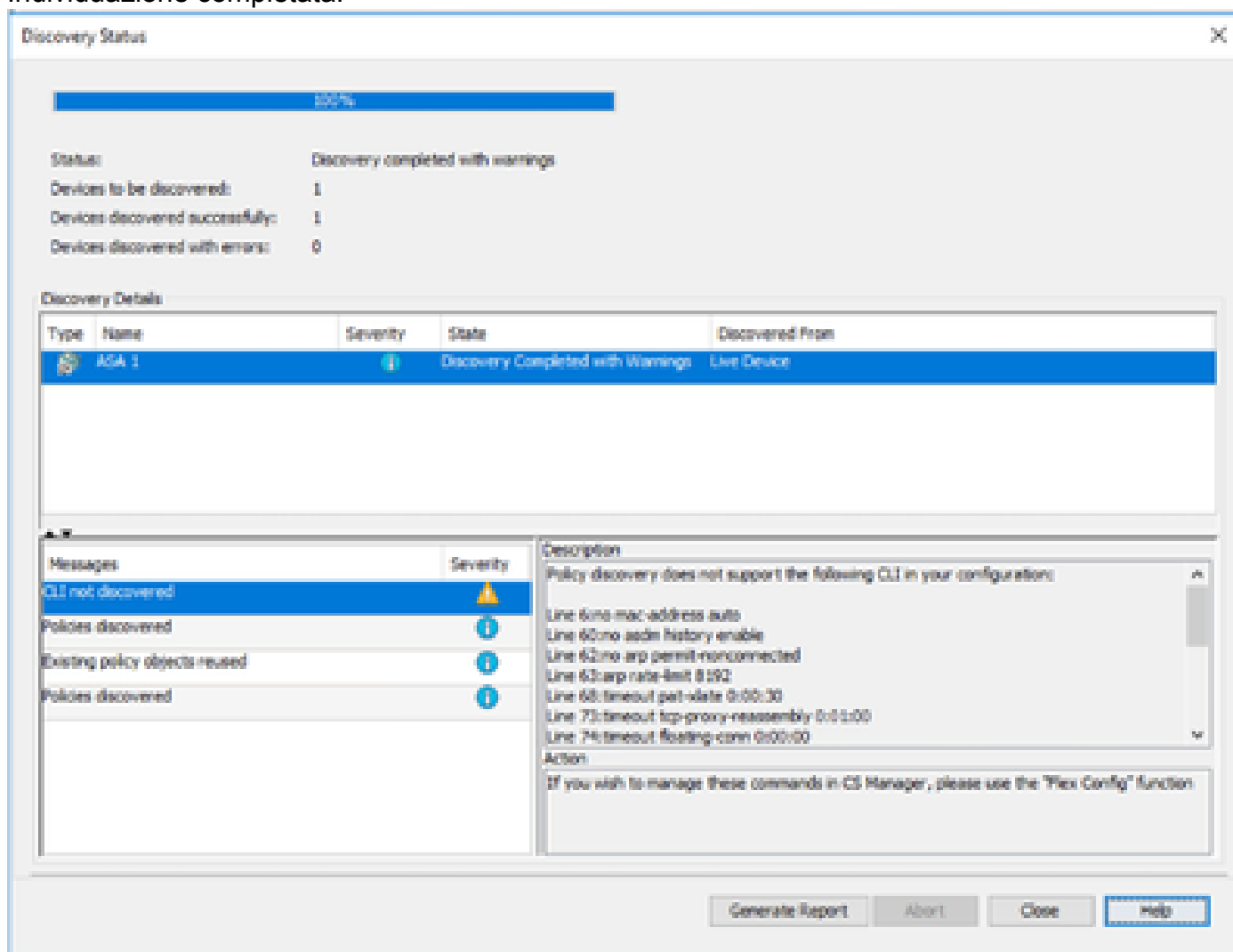
Select the policies to discover

- Detect ASA-CX/FirePOWER Module
- Inventory
- Platform Settings
- Firewall Services
- NAT Policies
- Routing Policies
- SSL Policy
- RA VPN Policies
- IPS

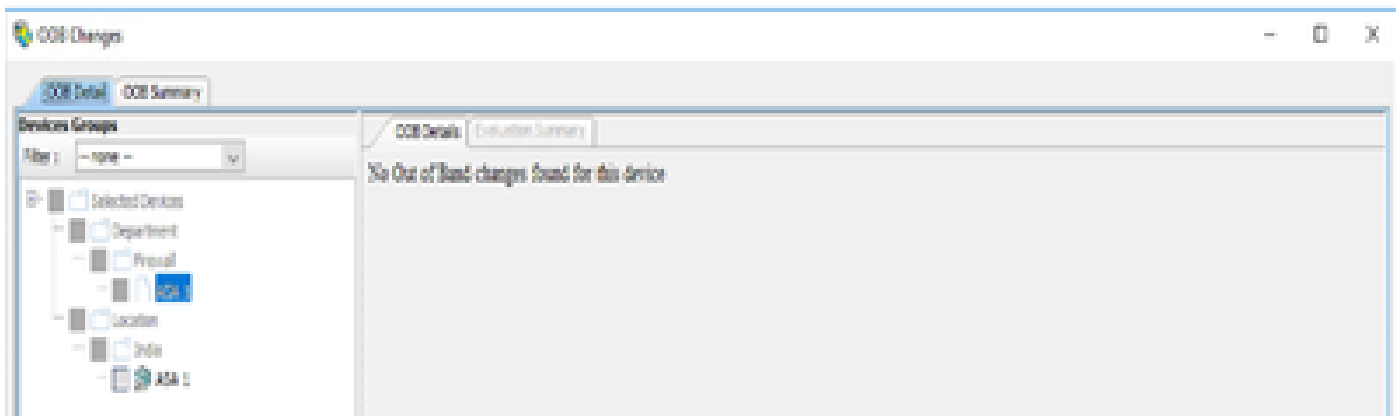
Prima di procedere con l'individuazione, verificare di conoscere la topologia di rete e le modifiche che possono verificarsi nella rete.



Al termine dell'individuazione, è possibile visualizzare la schermata pop con lo stato Individuazione completata.



Inoltre, dai cambiamenti fuori banda non può avere alcun cambiamento.



Bulk Device Discovery

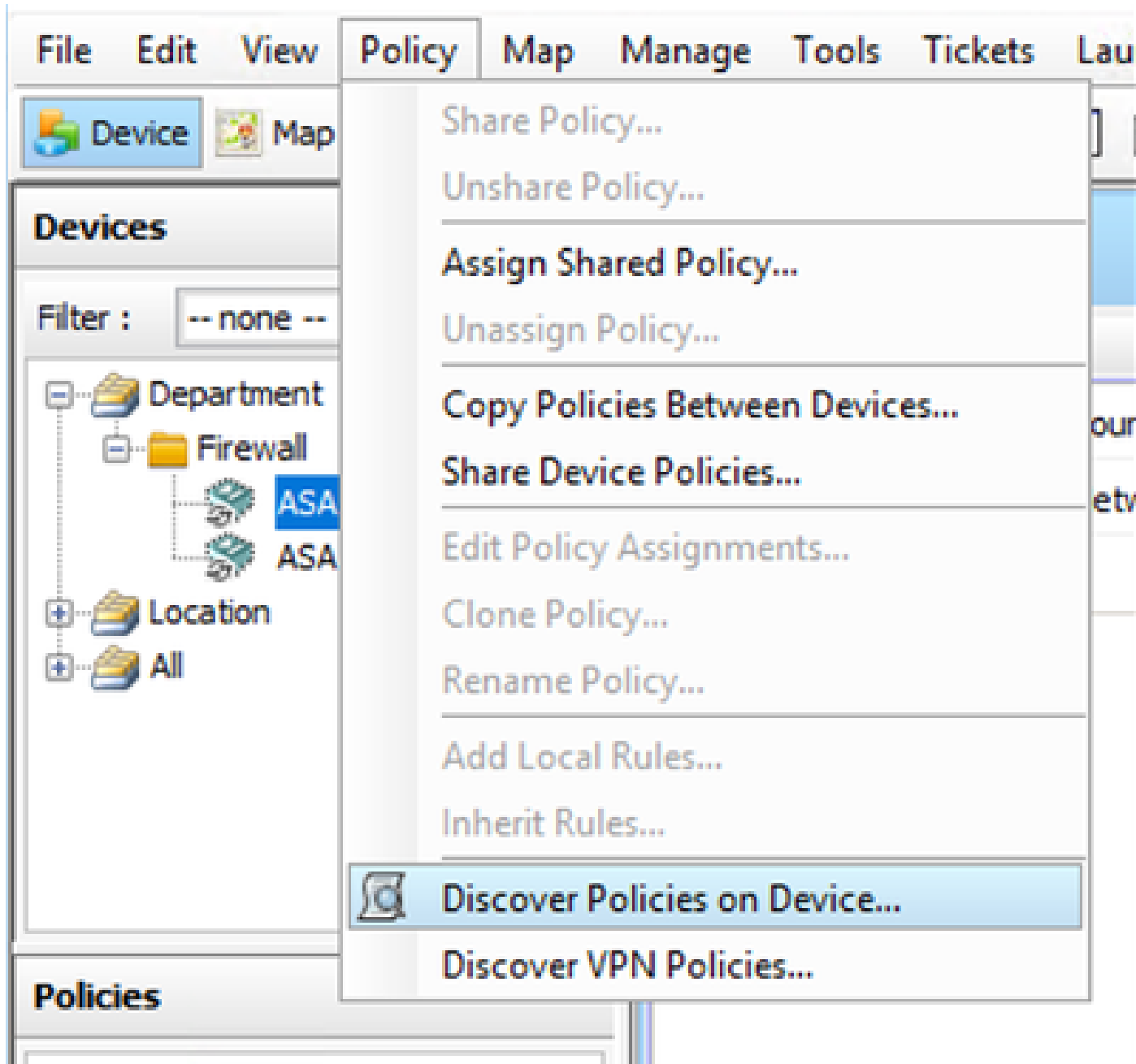
Per individuare le regole per più dispositivi, è possibile eseguire una nuova ricerca globale. È importante notare che la ricerca in blocco è limitata ai dispositivi attivi, quelli attualmente operativi e accessibili all'interno della rete.

Non è possibile eseguire l'individuazione in blocco sui sensori virtuali, ovvero il contesto di sicurezza. I moduli di assistenza possono essere individuati e selezionati separatamente.

Procedura per eseguire l'individuazione di massa dei dispositivi:

Passaggio 1:

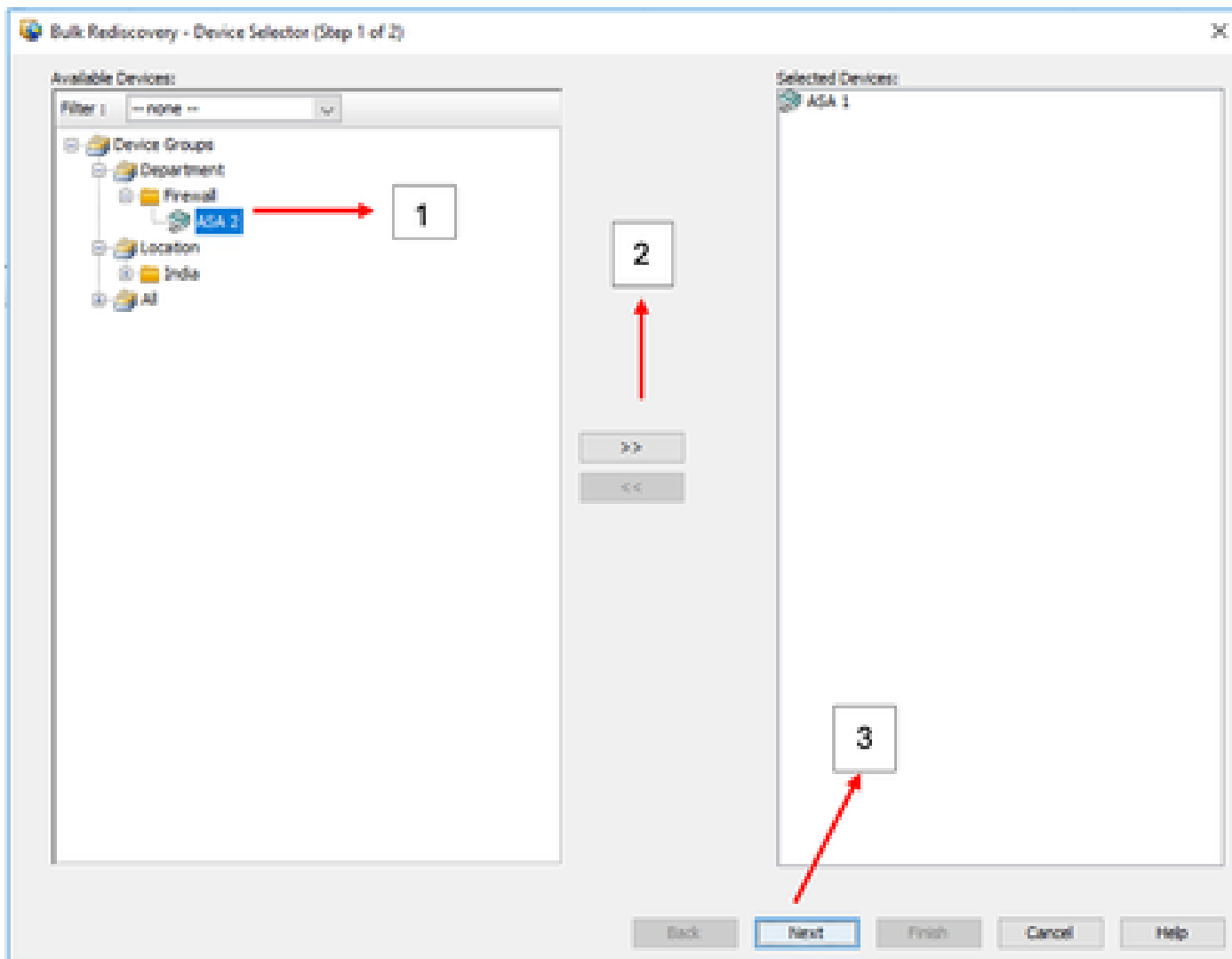
Passa a Criterio > Individua criteri sul dispositivo



Passaggio 2:

Se si sta eseguendo la ricerca di massa, è possibile visualizzare solo la finestra di dialogo per la nuova ricerca di massa.

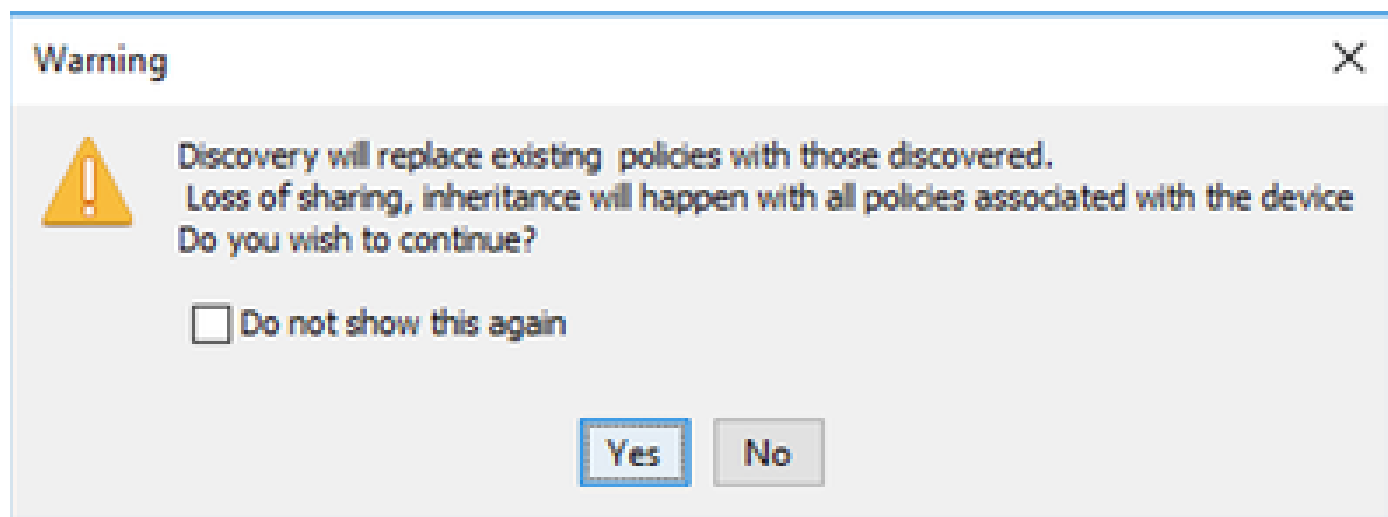
Da Periferiche disponibili nel riquadro di sinistra, scegliere l'elenco di periferiche per le quali si desidera individuare le policy e spostarlo sul lato destro.



Passaggio 3:


Verificare che tutti i dispositivi selezionati siano elencati e fare clic su Fine per continuare con la ricerca di massa.

Prima di procedere con l'individuazione, verificare di conoscere la topologia di rete e le modifiche che possono verificarsi nella rete.



Una volta completato il rilevamento, sar  possibile visualizzare l'esempio come

Warning



Changes that you make to Remote Access VPN policies might not be deployed if you have not performed a prior deployment.
Action: Please select File > Deploy immediately after discovery, before making any change to RA VPN policies.
We recommend that you perform this initial deployment to a file rather than directly to the device.
To change the deployment method, click the Edit Deploy Method button in the Deploy Saved Changes dialog box.

Do not show this again

OK

Individuazione di entrambi i dispositivi completata.

Discovery Status

100%

Status: Discovery completed with warnings

Devices to be discovered: 2

Devices discovered successfully: 2

Devices discovered with errors: 0

Discovery Details

Type	Name	Severity	State	Discovered From
ASA	ASA 1	Information	Discovery Completed with Warnings	Live Device
ASA	ASA 2	Information	Discovery Completed with Warnings	Live Device

Messages

Messages	Severity
DAP xml configuration was not discovered.	Information
CSD xml configuration was not discovered.	Information
Hostscan package file is not found on device or not ...	Information
Incomplete Remote Access VPN Configuration	Warning
CLI not discovered	Warning
Policies discovered	Information
Existing policy objects reused	Information
Value overrides created for device	Information

Description: No DAP xml configuration file found on device.

Action: No action is required.

Generate Report Abort Close Help

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).