

Konfiguration der Synchronisierung von Geräten mit dem Security Manager

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Demo-Methodik](#)

[Erkennung einzelner Geräte](#)

[Schritte zur Einzelgeräteerkennung:](#)

[Schritte zur Einzelgeräteerkennung:](#)

[Schritt 1:](#)

[Phase 2:](#)

[Große Geräteerkennung](#)

[Schritte zur Massengeräteerkennung:](#)

[Schritt 1:](#)

[Phase 2:](#)

[Schritt 3:](#)

Einleitung

In diesem Dokument werden verschiedene Möglichkeiten zur Konfigurations-Synchronisierung von ASA zu CSM beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Security Manager
- Adaptives Sicherheitsgerät

Verwendete Komponenten

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

- Cisco Security Manager 4.25
- Adaptive Security Appliance

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

Der Cisco Security Manager bietet zentralisierte Management- und Überwachungsservices für Cisco ASA-Geräte.

Demo-Methodik

In diesem Dokument werden zwei verschiedene Methoden oder Optionen zum Synchronisieren der Konfiguration von ASA mit CSM beschrieben.

- Erkennung einzelner Geräte
- Neuermittlung großer Gerätemengen

Erkennung einzelner Geräte

Eine einzige Erkennung kann nur durchgeführt werden, wenn das Gerät dem Bestand hinzugefügt wird. Dies ist nur möglich, wenn das Gerät

- Sicherheitskontextkonfigurationen für ASA-, PIX- und FWSM-Geräte, die im Mehrfachkontextmodus ausgeführt werden.
- Virtuelle Sensorkonfigurationen für IPS-Geräte
- Servicemodul-Informationen für Catalyst-Geräte

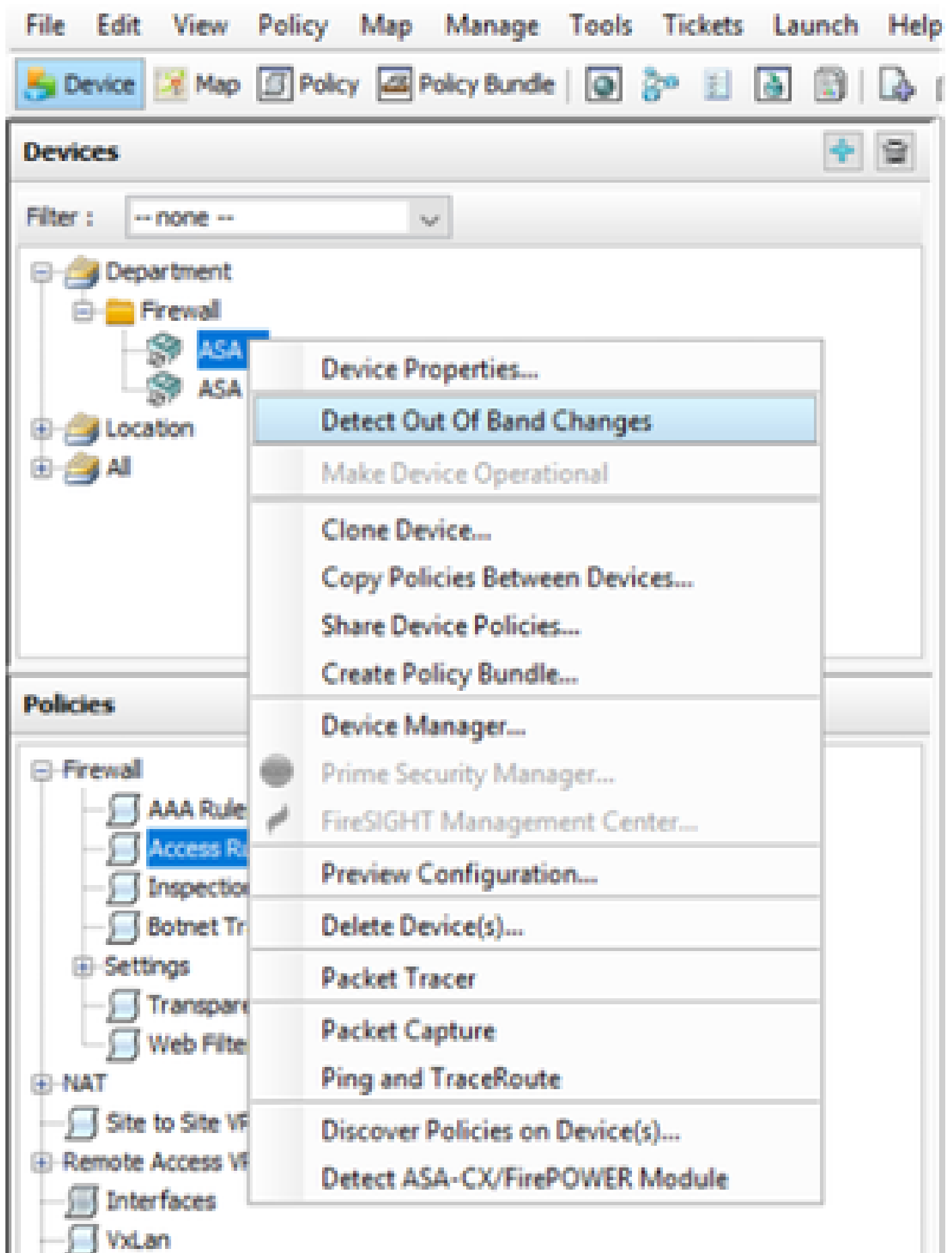
Schritte zur Einzelgeräteerkennung:

Sie können die Geräteerkennung durchführen, wenn Sie Änderungen an der Geräte-CLI vorgenommen haben oder wenn das Gerät entfernt und wieder hinzugefügt wurde.

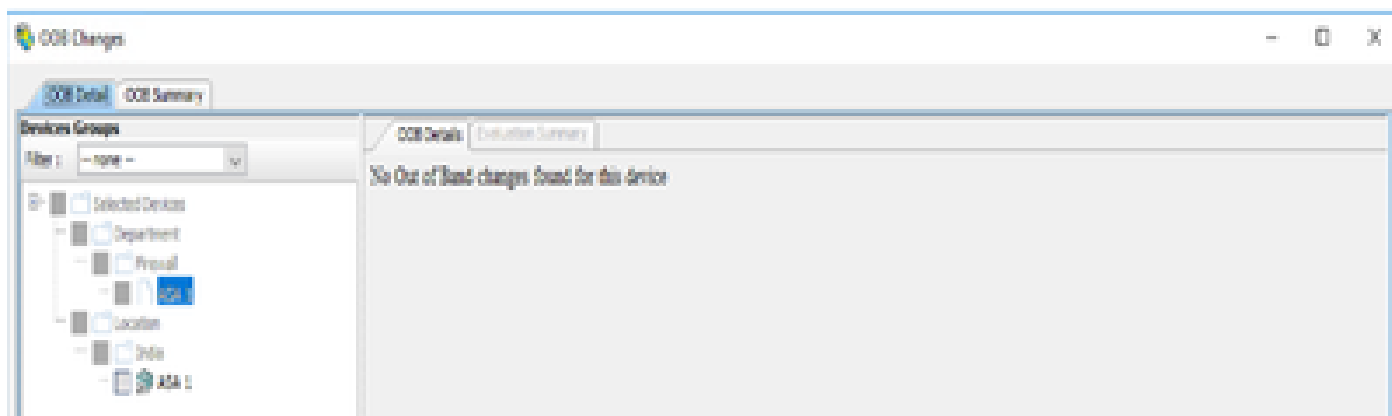
Um zu überprüfen, ob ausstehende Änderungen noch synchronisiert werden müssen, befolgen Sie das genannte Beispiel.

Klicken Sie mit der rechten Maustaste im Gerätebereich auf das entsprechende Gerät, und

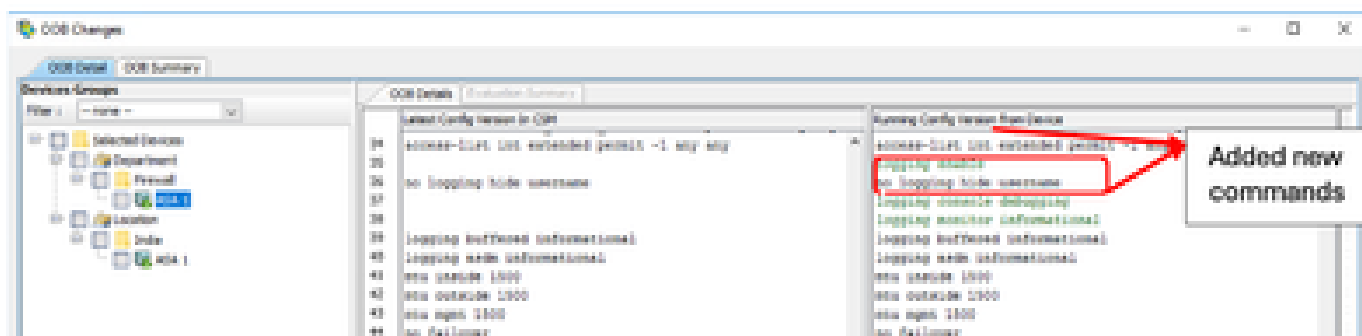
wählen Sie die Option Out-of-Band-Änderungen erkennen aus.



Wenn keine Änderungen vorgenommen wurden, wird die Seite als keine ausgehenden Änderungen für dieses Gerät angezeigt.



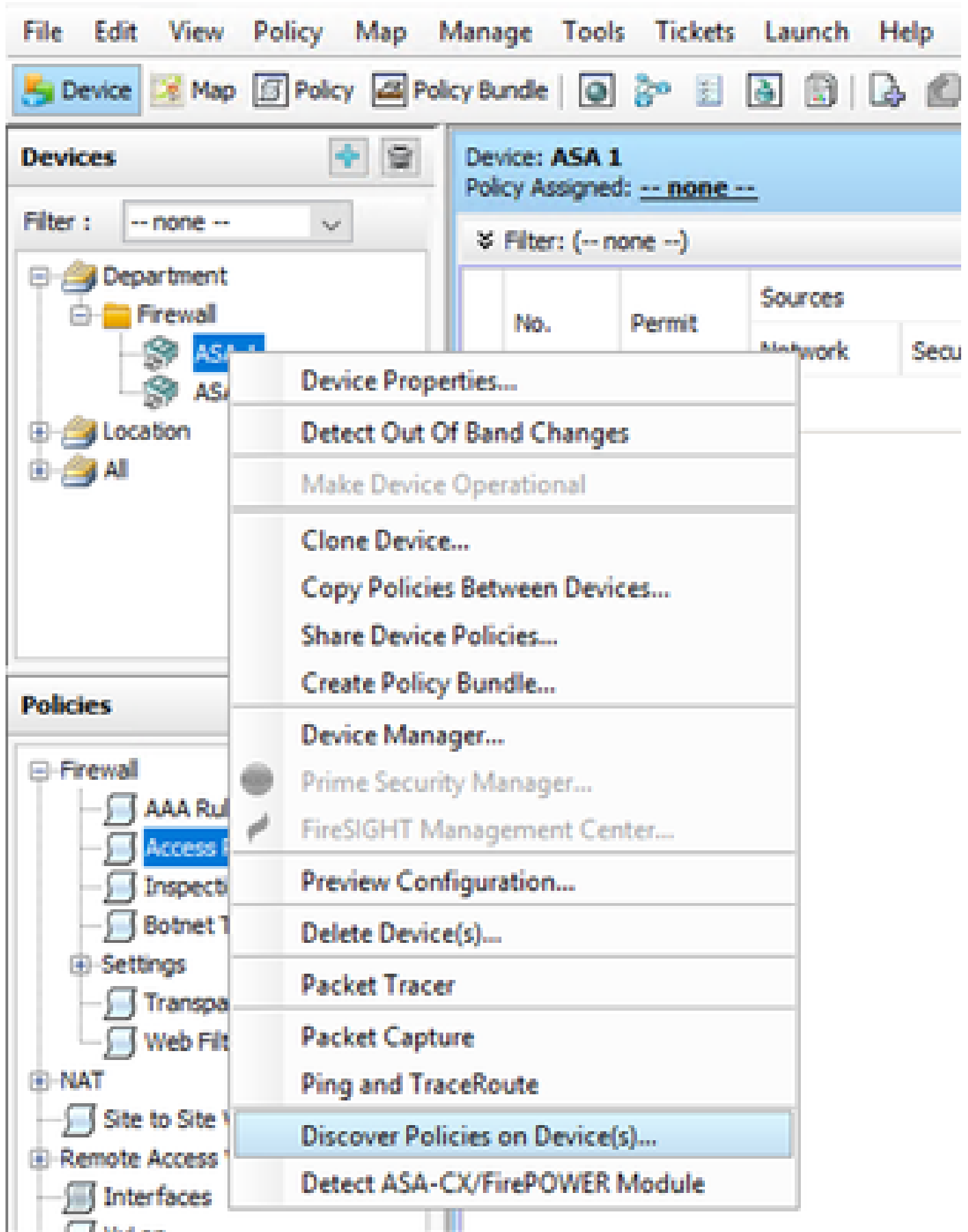
Wenn Änderungen vorgenommen wurden, werden die Linien entsprechend der Legende hervorgehoben.



Schritte zur Einzelgeräteerkennung:

Schritt 1:

Klicken Sie mit der rechten Maustaste auf den entsprechenden Gerätenamen im Gerätebereich, und wählen Sie die Option Richtlinien auf Geräten erkennen aus.



Phase 2:

Für die Einzelgeräte-Wiederherstellungsmethode wird nur das Dialogfeld Discovery Task erstellen angezeigt. Falls Sie ein Bulk Discovery-Dialogfeld erhalten, schließen Sie es, und öffnen Sie es erneut.

Sie haben drei Optionen, um die Erkennung durchzuführen.

- Live-Gerät - Es ruft die Konfiguration vom Live-Gerät ab, das sich im Netzwerk befindet.
- Konfigurationsdatei - Sie können die Konfigurationsdatei auswählen und mit der Erkennung fortfahren.
- Werksseitige Standardkonfiguration - Das Gerät wird auf die Standardkonfigurationen zurückgesetzt. Diese Methode kann für Geräte verwendet werden, die nur den Einzelkontextmodus ausführen, oder für Geräte mit individuellen Sicherheitskontexten.

Create Discovery Task [X]

Discovery Task Name:

Discover From:

- Live Device
- Config File
- Factory Default Configuration

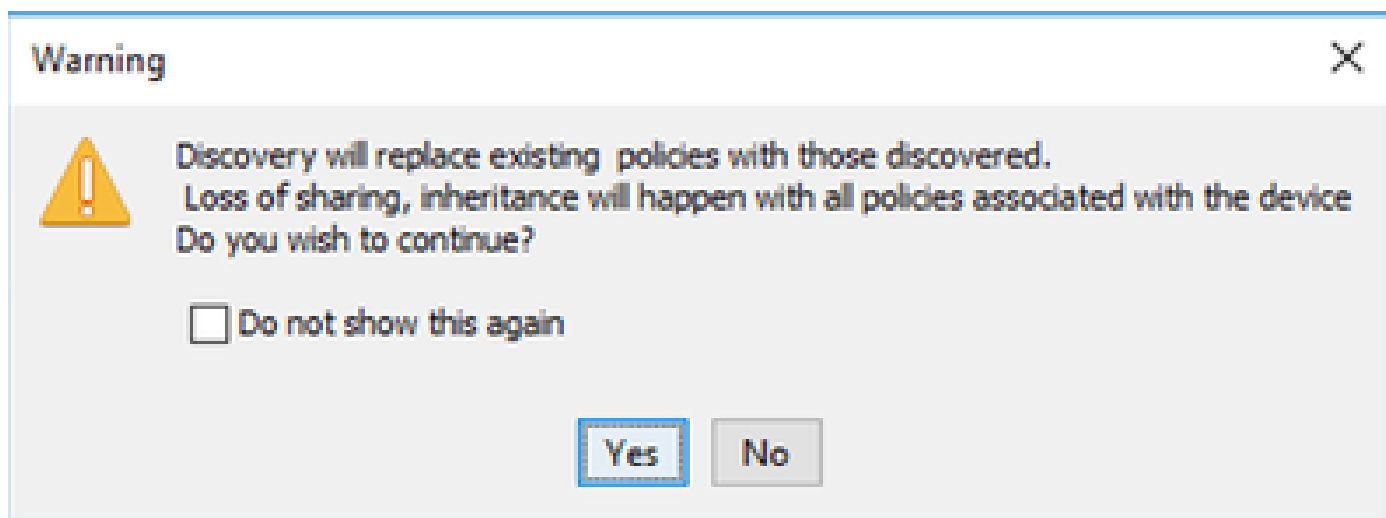
Config File:

Discover Policies for Security Contexts

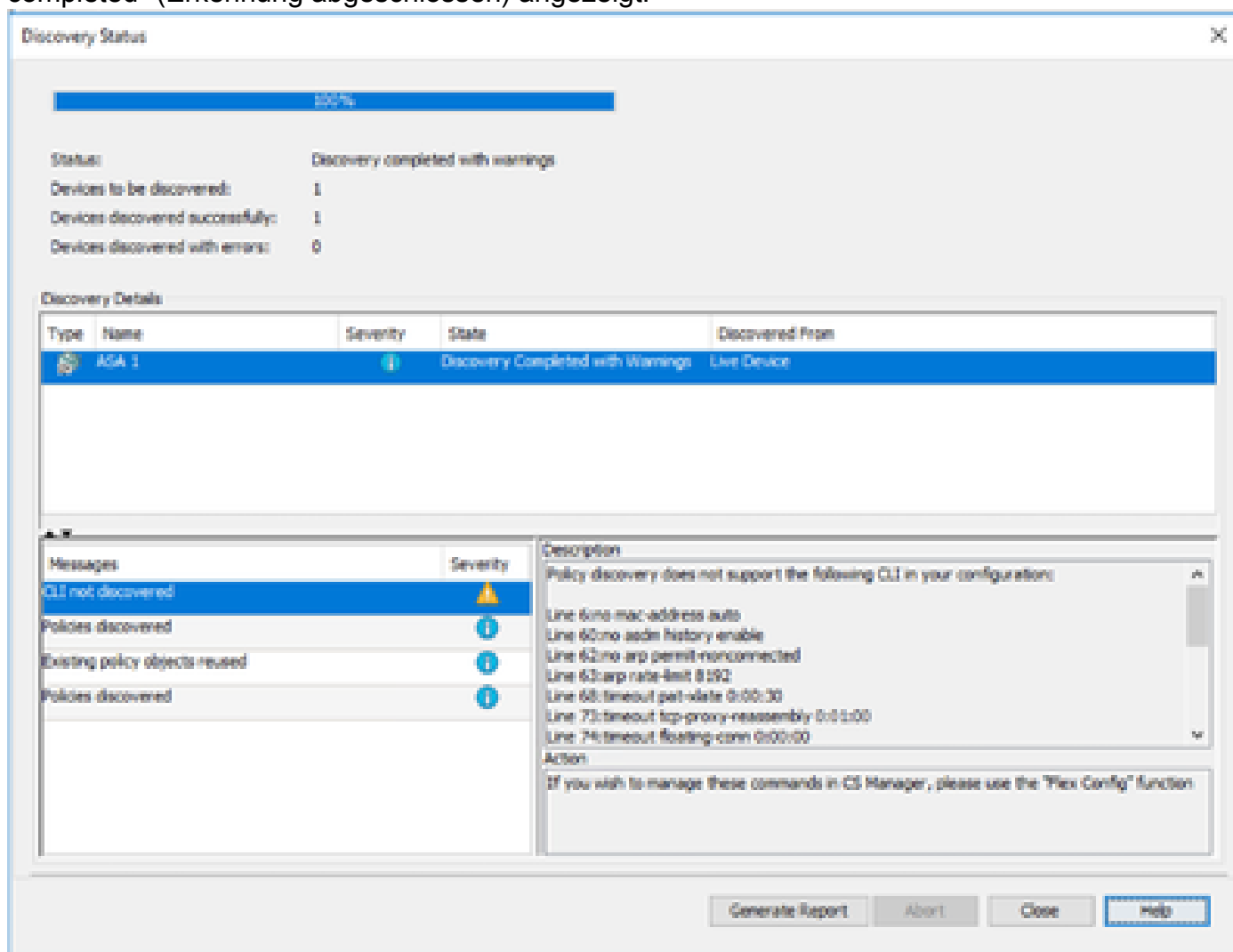
Policies To Discover
Select the policies to discover

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

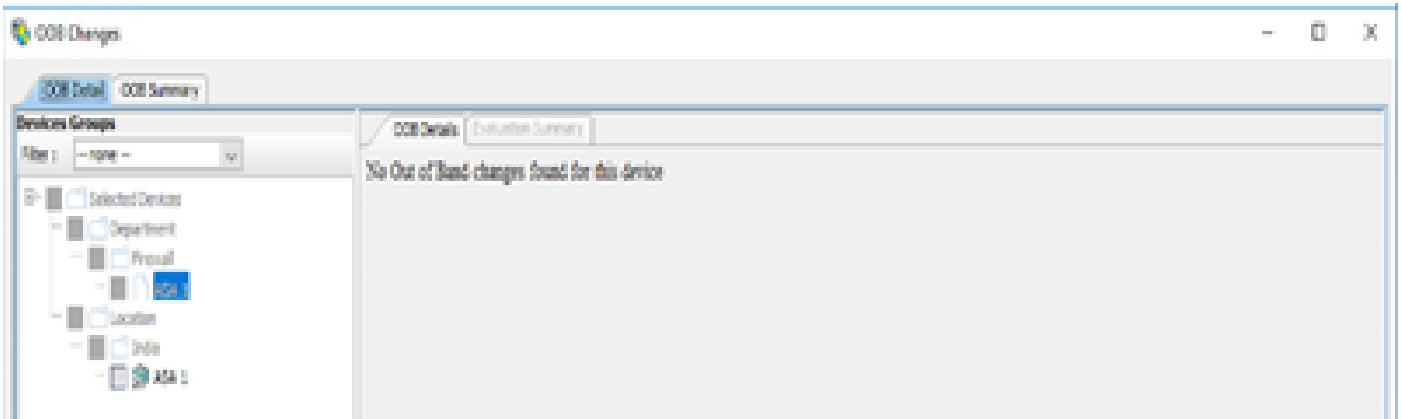
Vergewissern Sie sich, dass Sie die Netzwerktopologie und die möglichen Änderungen in Ihrem Netzwerk kennen, bevor Sie mit der Erkennung fortfahren.



Sobald die Erkennung abgeschlossen ist, wird der Popup-Bildschirm mit dem Status "Discovery completed" (Erkennung abgeschlossen) angezeigt.



Und von Out-of-Band-Änderungen kann es auch keine Änderungen geben.



Große Geräteerkennung

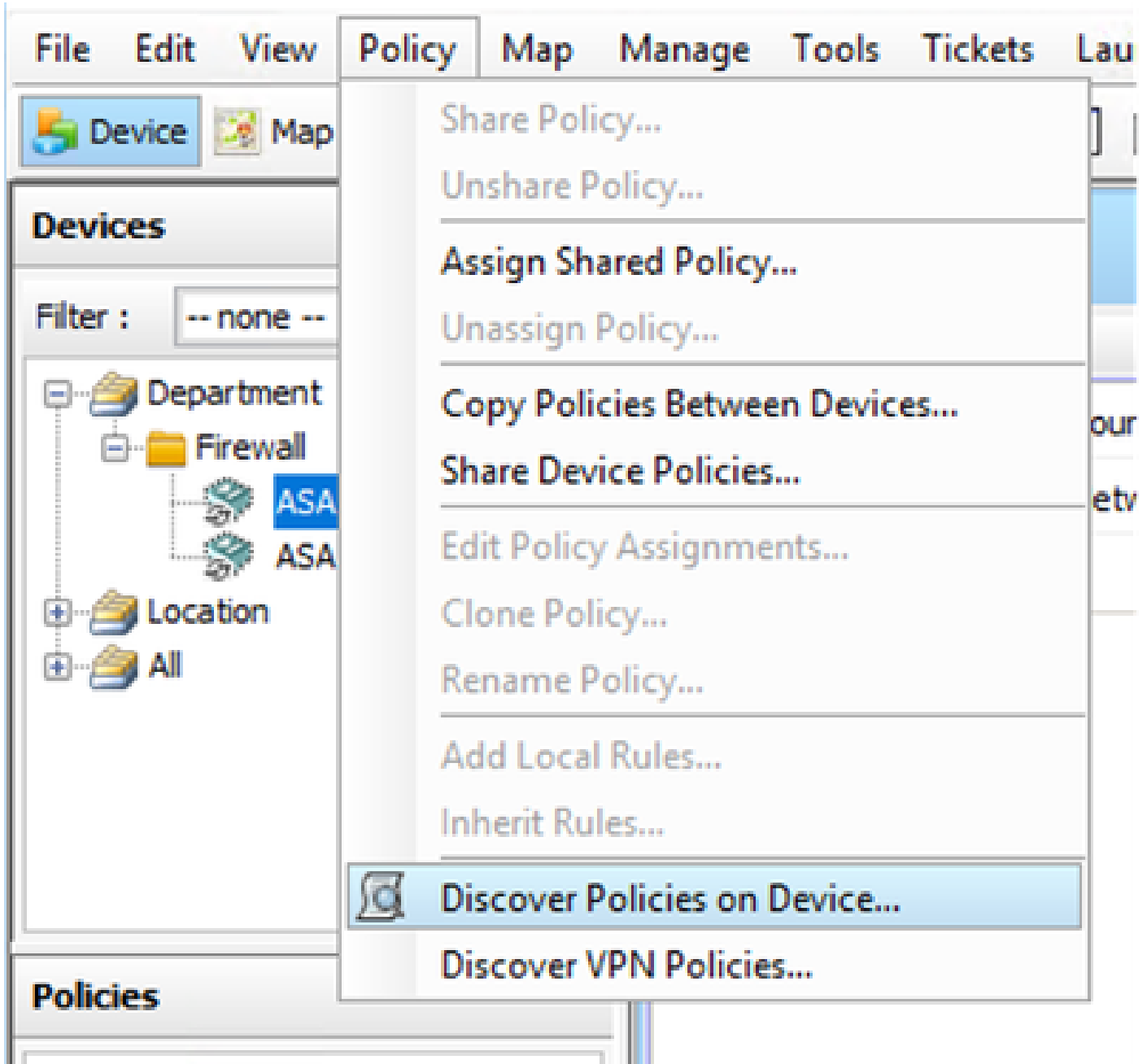
Um Richtlinien für mehrere Geräte zu ermitteln, können Sie eine erneute Erkennung mehrerer Geräte durchführen. Beachten Sie, dass die Wiedererkennung von Massen auf Live-Geräte beschränkt ist, die derzeit in Ihrem Netzwerk betriebsbereit und zugänglich sind.

Sie können die Bulk Discovery nicht für Sicherheitskontext und virtuelle Sensoren durchführen. Servicemodule können erkannt werden, wenn sie separat ausgewählt werden.

Schritte zur Massengeräteerkennung:

Schritt 1:

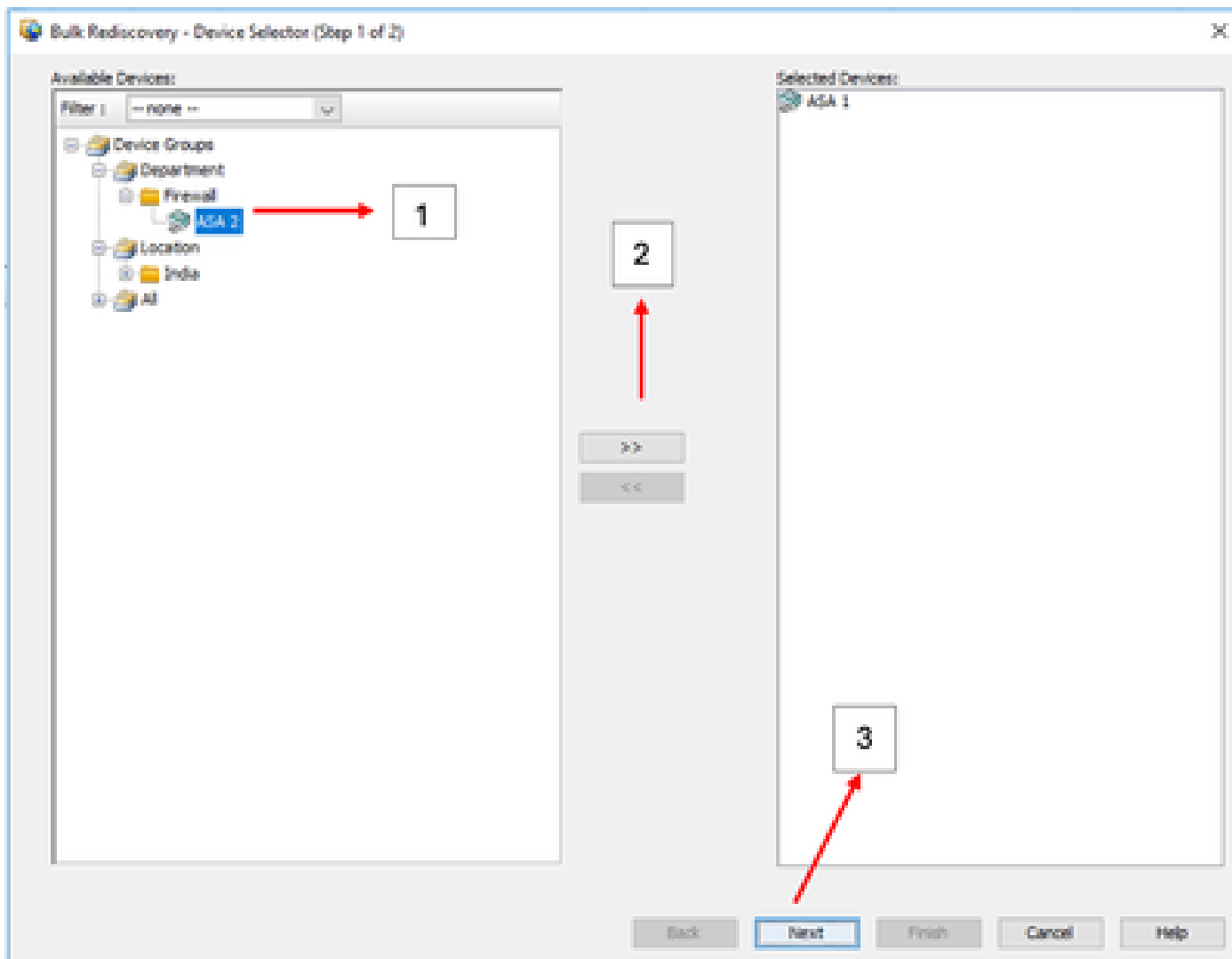
Navigieren Sie zu Richtlinie > Richtlinien auf Gerät erkennen



Phase 2:

Wenn Sie die Massenerkennung durchführen, kann nur das Dialogfeld zur Massenerkennung angezeigt werden.

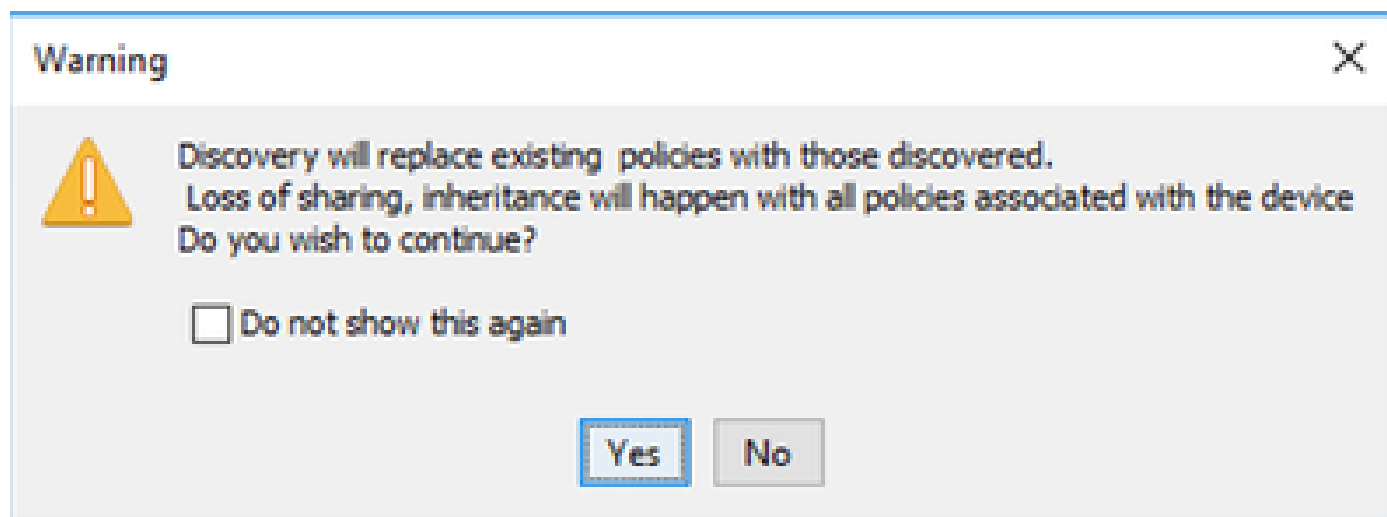
Wählen Sie aus der Liste der verfügbaren Geräte im linken Bereich die Geräte aus, für die Sie Richtlinien ermitteln möchten, und verschieben Sie sie auf die rechte Seite.



Schritt 3:


Überprüfen Sie, ob alle ausgewählten Geräte aufgelistet sind, und klicken Sie auf "Beenden", um die erneute Erkennung der Massen fortzusetzen.

Vergewissern Sie sich, dass Sie die Netzwerktopologie und die möglichen Änderungen in Ihrem Netzwerk kennen, bevor Sie mit der Erkennung fortfahren.



Sobald die Erkennung abgeschlossen ist, können Sie das Beispiel

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

Beide Geräte werden erfolgreich erkannt.

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

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.