Synchronisatie van apparaten naar Security Manager configureren

Inhoud

Inleiding

Dit document beschrijft verschillende manieren van configuratiesynchronisatie van ASA naar CSM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Security Manager
- Adaptief beveiligingsapparaat

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Security Manager 4.25
- Adaptieve security applicatie

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De Cisco security manager levert gecentraliseerde beheer- en bewakingsservices voor Cisco ASA-apparaat.

Demonstratiemethode

Dit document beschrijft twee verschillende methoden of opties om de configuratie van ASA naar CSM te synchroniseren.

- Detectie van één apparaat
- Herontdekking van bulkapparaten

Detectie van één apparaat

Een enkele ontdekking kan alleen worden uitgevoerd als het apparaat wordt toegevoegd aan de inventaris. Het kan alleen worden uitgevoerd als het apparaat

- Security contextconfiguraties voor ASA-, PIX- en FWSM-apparaten die in meerdere contextmodi werken.
- Virtuele sensor configuraties voor IPS apparaten.
- Informatie over servicemodule voor Catalyst-apparaten.

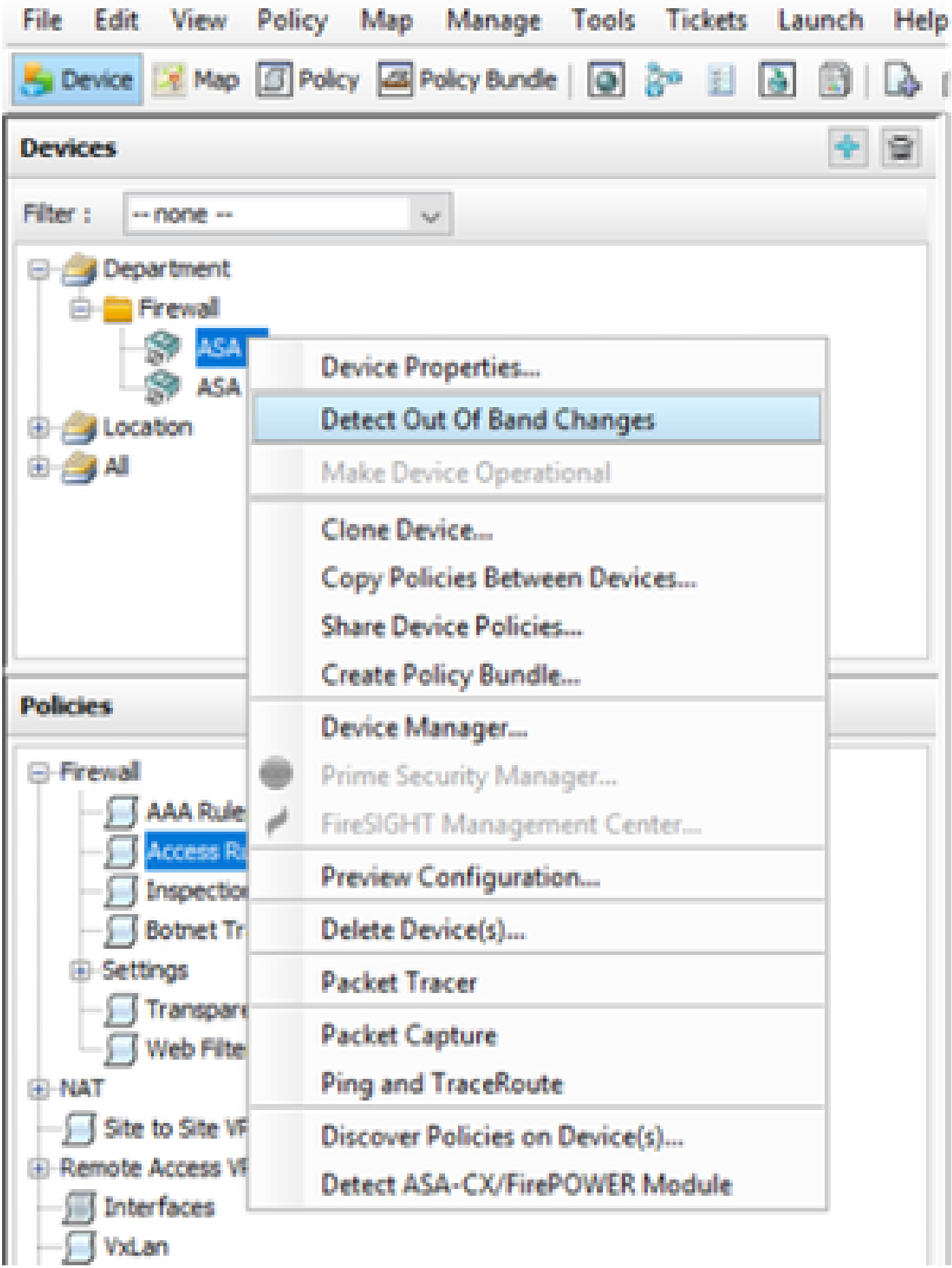
Stappen om detectie van één apparaat uit te voeren:

U kunt de apparaatdetectie uitvoeren wanneer u wijzigingen op apparaat CLI hebt uitgevoerd of als het apparaat is verwijderd en opnieuw is toegevoegd.

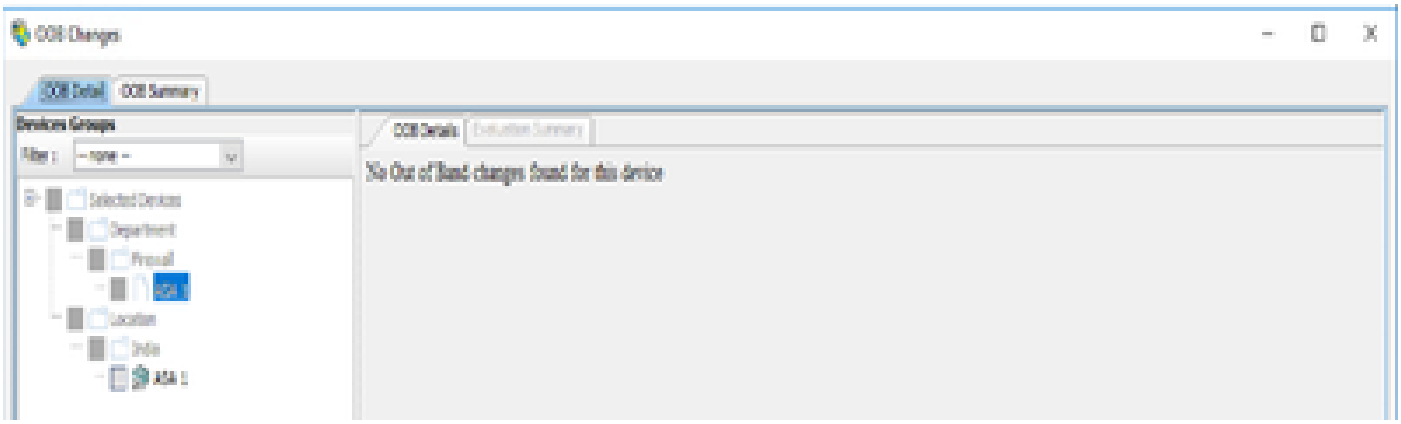
Om te controleren of wijzigingen die nog in behandeling zijn nog moeten worden gesynchroniseerd , gaat u verder met het genoemde voorbeeld.

Klik met de rechtermuisknop op het betreffende apparaat in het apparaatvenster en selecteer de

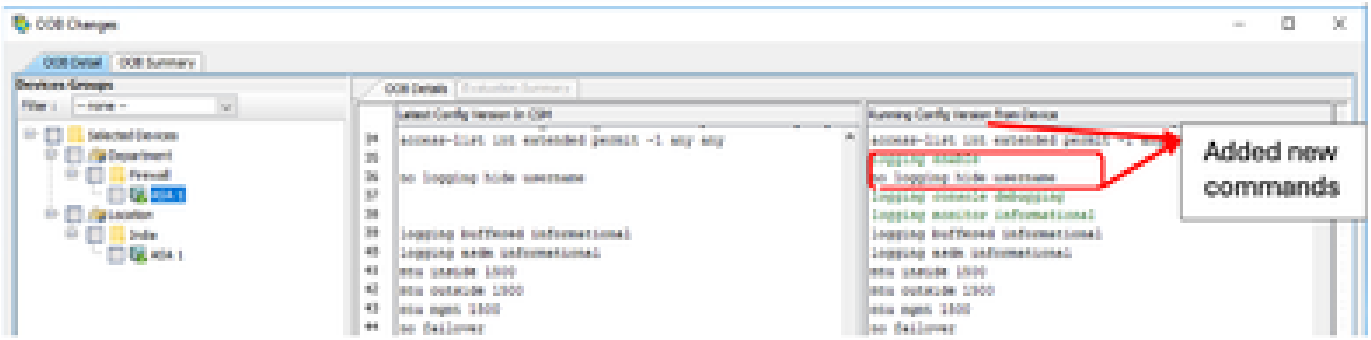
optie Uitgaande bandwijzigingen detecteren.



Als er geen wijzigingen zijn, wordt de pagina weergegeven als geen uitgaande wijzigingen gevonden voor dit apparaat.



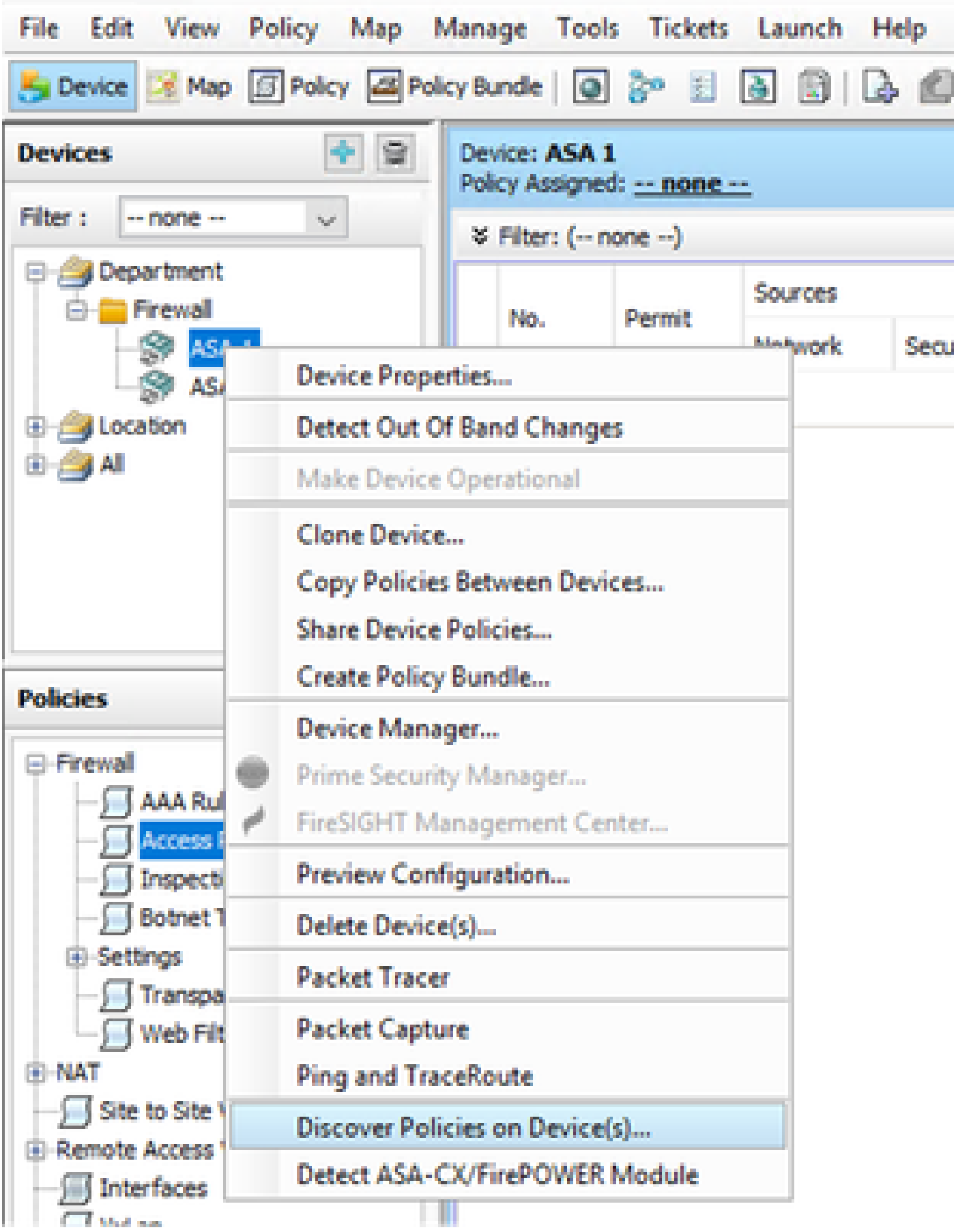
Als er veranderingen zijn aangebracht, worden de lijnen gemarkeerd zoals in de legende.



Stappen om detectie van één apparaat uit te voeren:

Stap 1:

Klik met de rechtermuisknop op de betreffende apparaatnaam in het apparaatvenster en kies de optie Beleid inzake apparaat(en) detecteren.

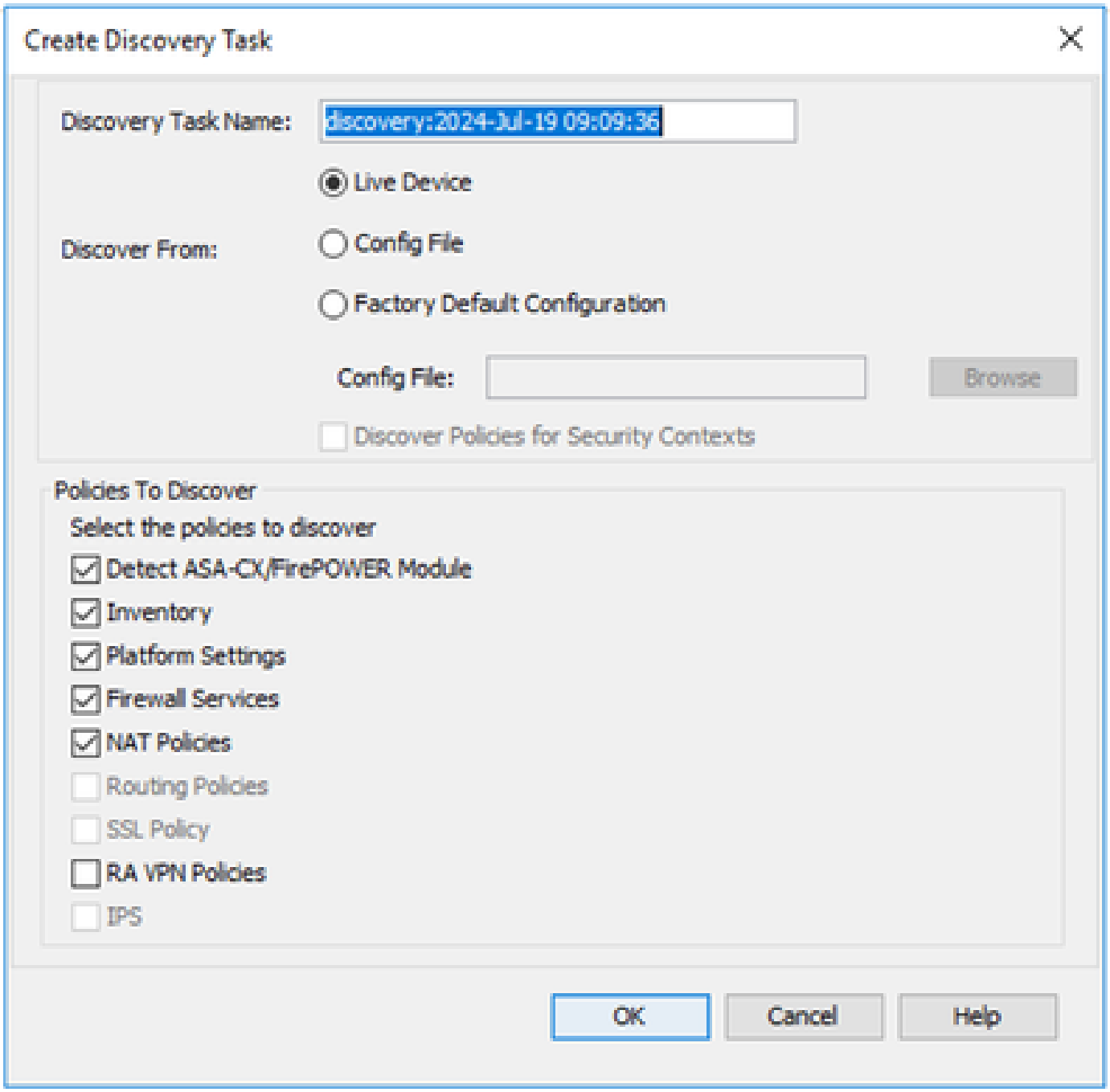

File Edit View Policy Map Manage Tools Tickets Launch Help
Device Map Policy Policy Bundle
Devices
Filter : -- none --
Department
Firewall
Location
All
Device: ASA 1
Policy Assigned: -- none --
Filter: (-- none --)
No.
Permit
Sources
Device Properties...
Detect Out Of Band Changes
Make Device Operational
Clone Device...
Copy Policies Between Devices...
Share Device Policies...
Create Policy Bundle...
Device Manager...
Prime Security Manager...
FireSIGHT Management Center...
Preview Configuration...
Delete Device(s)...
Packet Tracer
Packet Capture
Ping and TraceRoute
Discover Policies on Device(s)...
Detect ASA-CX/FirePOWER Module
Policies
Firewall
Settings
NAT
Interfaces

Stap 2:

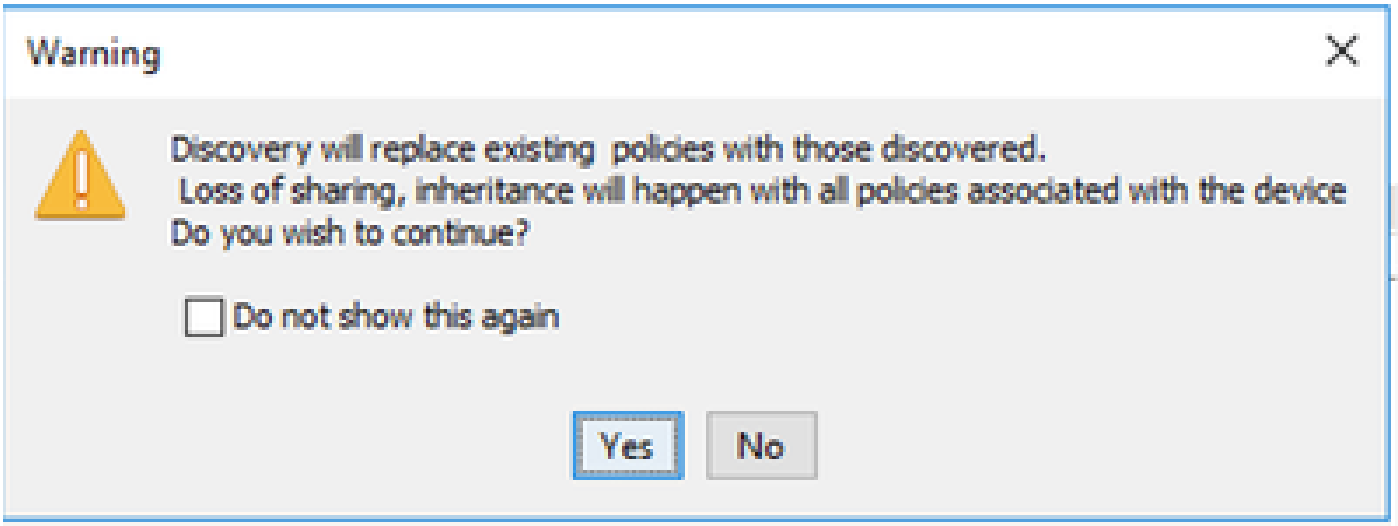
Voor de herstelmethode met één apparaat kunt u alleen het dialoogvenster Detectietaak maken zien. Ingeval als u een bulk ontdekkings dialoogvenster krijgt, sluit u dit vriendelijk en opent u het opnieuw.

U hebt 3 opties om de ontdekking uit te voeren.

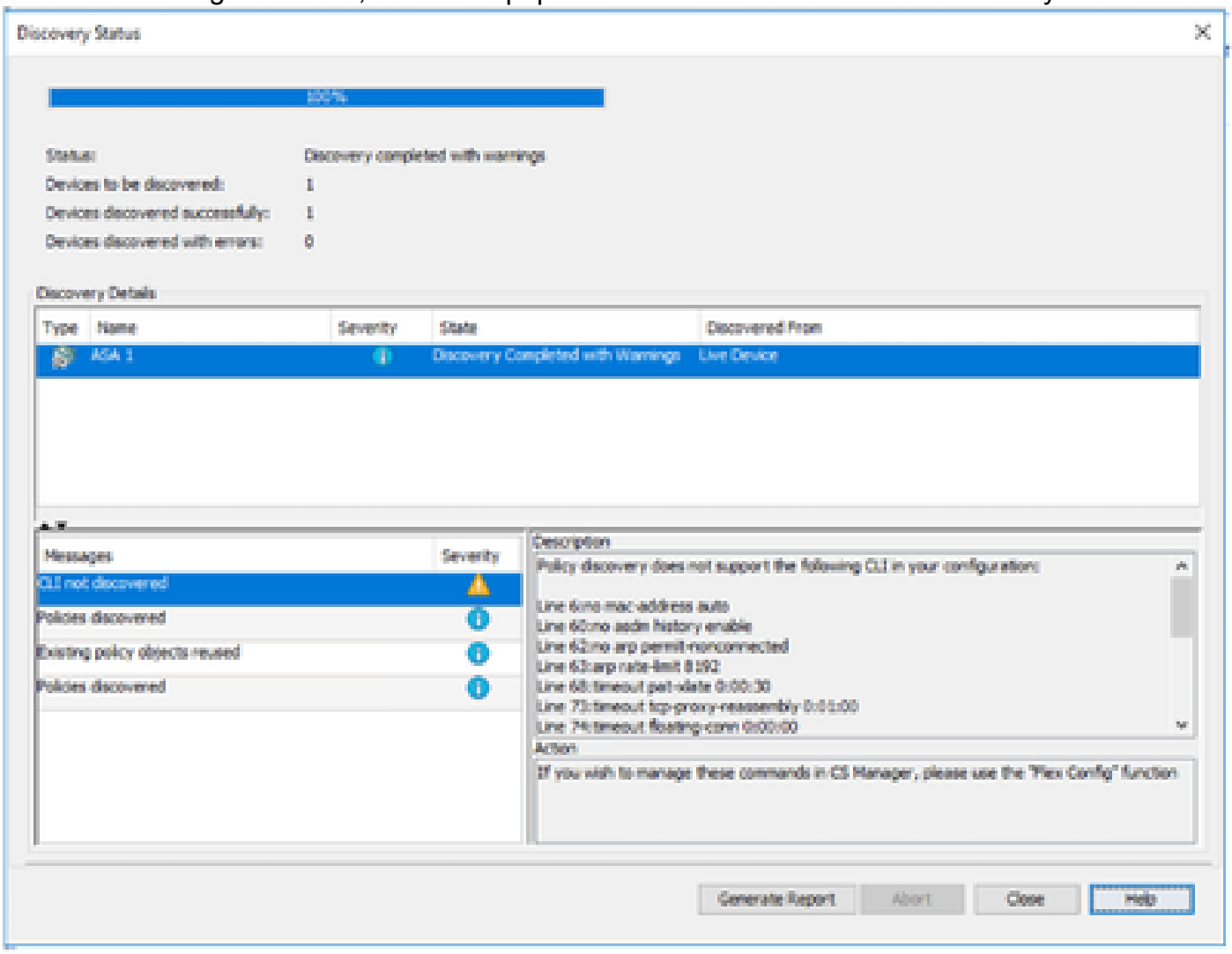
- Levend apparaat - Het haalt de configuratie van levend apparaat, dat in netwerk is.
- Configuration File - U kunt het configuratiebestand kiezen en doorgaan met de detectie.
- Standaard fabriekskonfiguratie - de standaardconfiguraties van het apparaat worden hersteld. Deze methode kan worden gebruikt voor apparaten die alleen met één contextmodus werken of voor apparaten met afzonderlijke beveiligingscontexten.



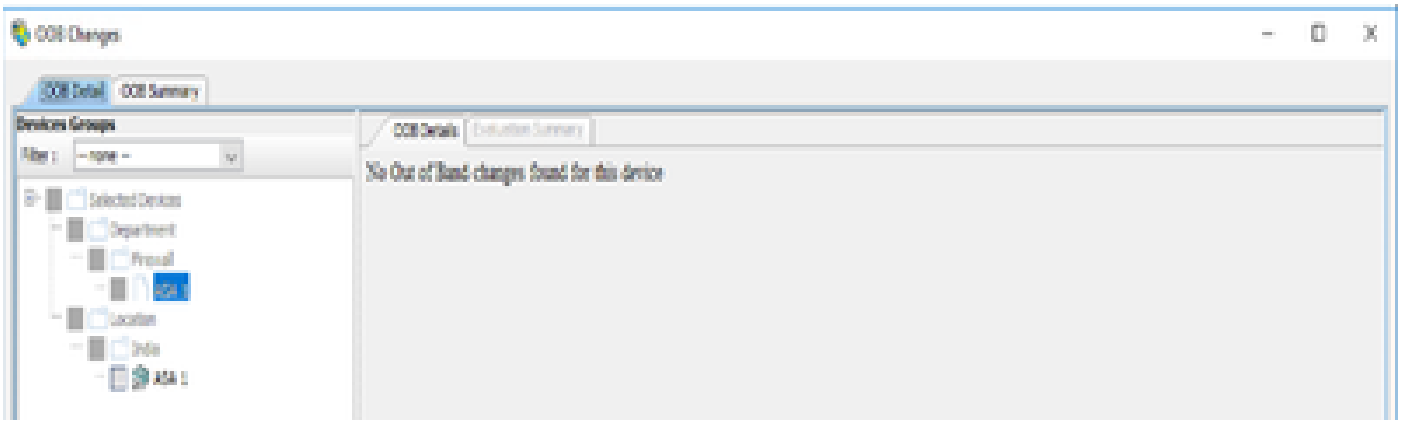
Zorg ervoor dat u zich bewust bent van de netwerktopologie en de veranderingen die in uw netwerk kunnen gebeuren voordat u doorgaat met de ontdekking.



Als de ontdekking is voltooid, kunt u het popscherm zien met de status als Discovery is voltooid.



En van buiten-band veranderingen kan het ook geen veranderingen hebben.



Detectie van bulkapparaten

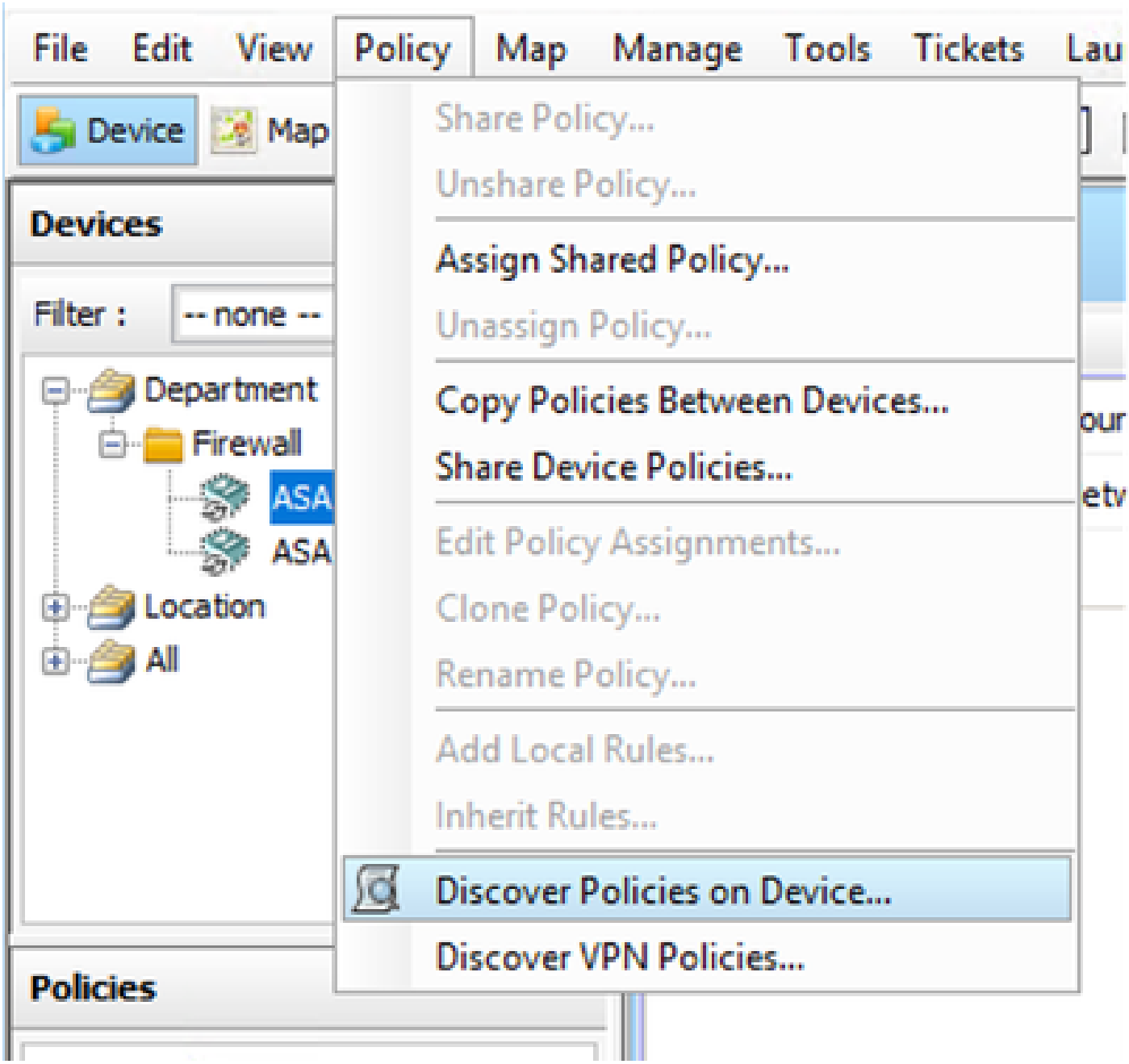
Om beleid voor meerdere apparaten te ontdekken, kunt u bulk herontdekken. Het is belangrijk om op te merken dat bulk herontdekking is beperkt tot live apparaten , die momenteel operationeel en toegankelijk zijn binnen uw netwerk.

U kunt de bulkdetectie niet uitvoeren op beveiligingscontext, virtuele sensoren. Servicemodules kunnen afzonderlijk worden ontdekt.

Stappen om bulk apparaat detectie uit te voeren:

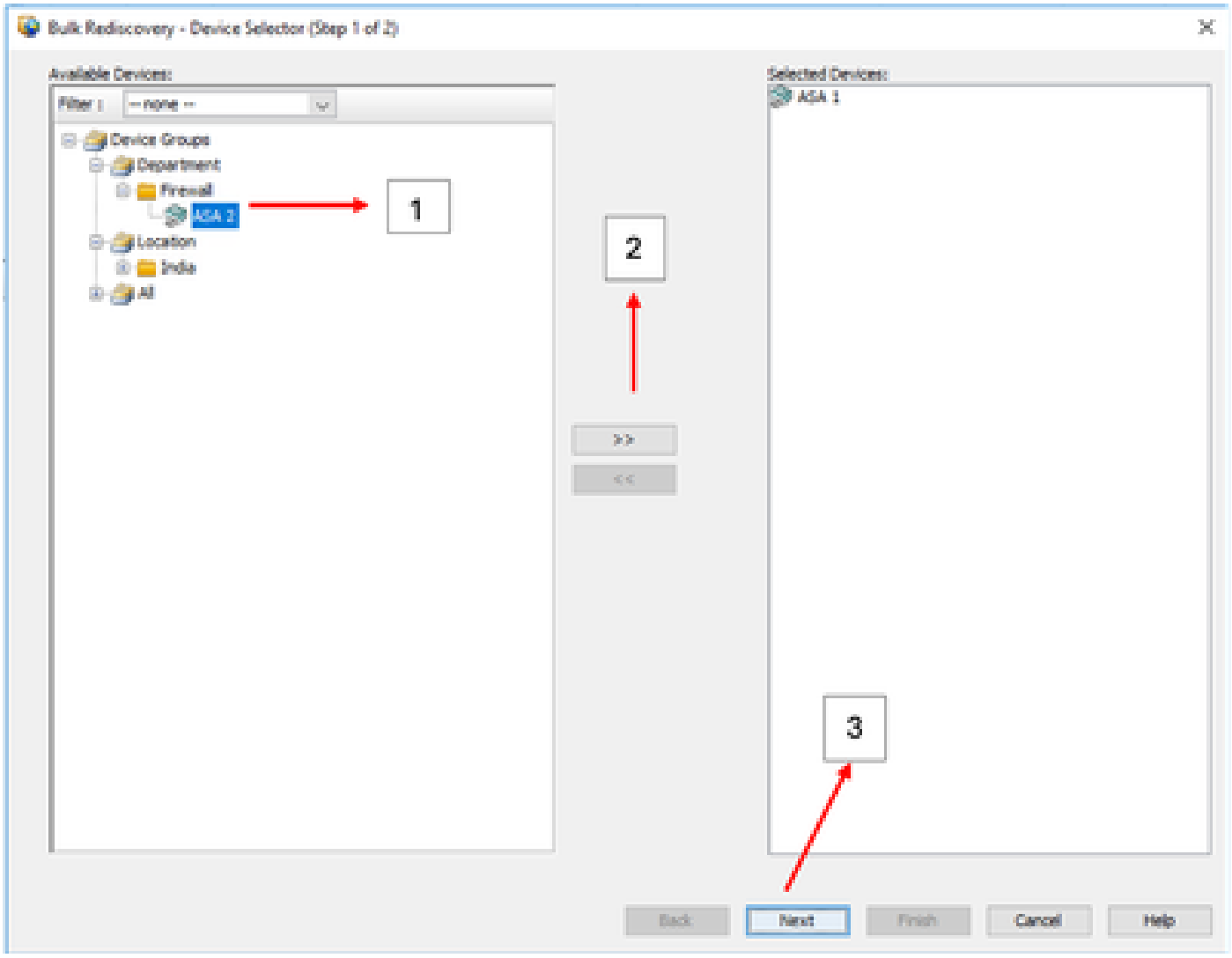
Stap 1:

Navigeren naar beleid > Ontdek beleid op apparaat



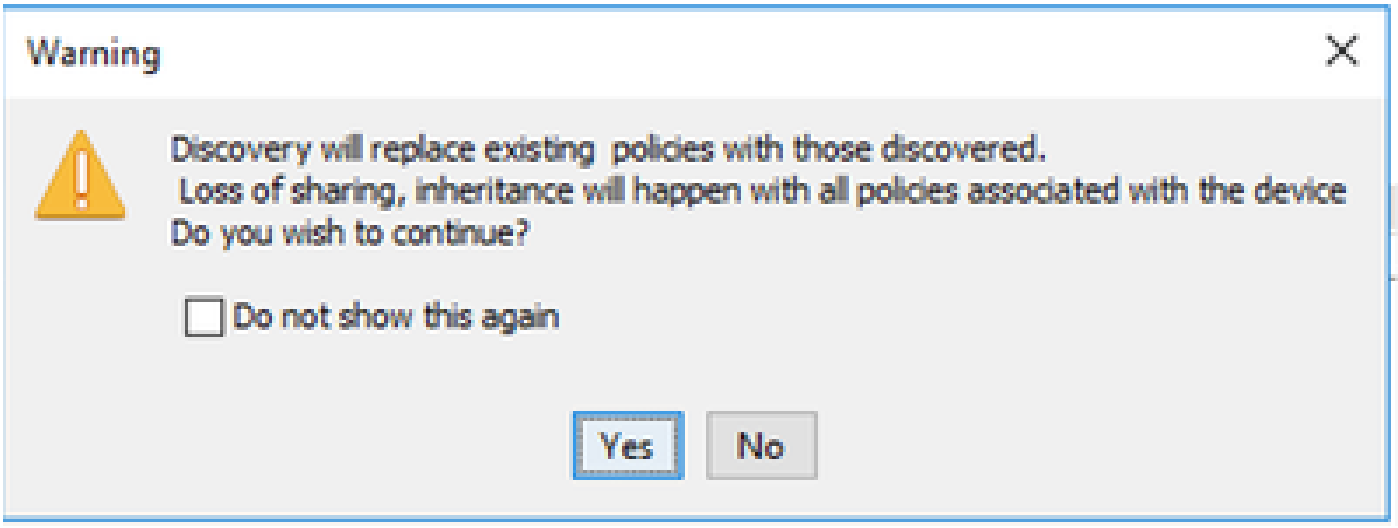
Stap 2:

Als u Bulkherontdekking uitvoert, kan slechts het de dialoogvakje van de bulkherontdekking verschijnen.
Kies vanuit de beschikbare apparaten in het linker deelvenster de lijst met apparaten waarvoor u beleid wilt ontdekken en naar de rechterkant wilt verplaatsen.

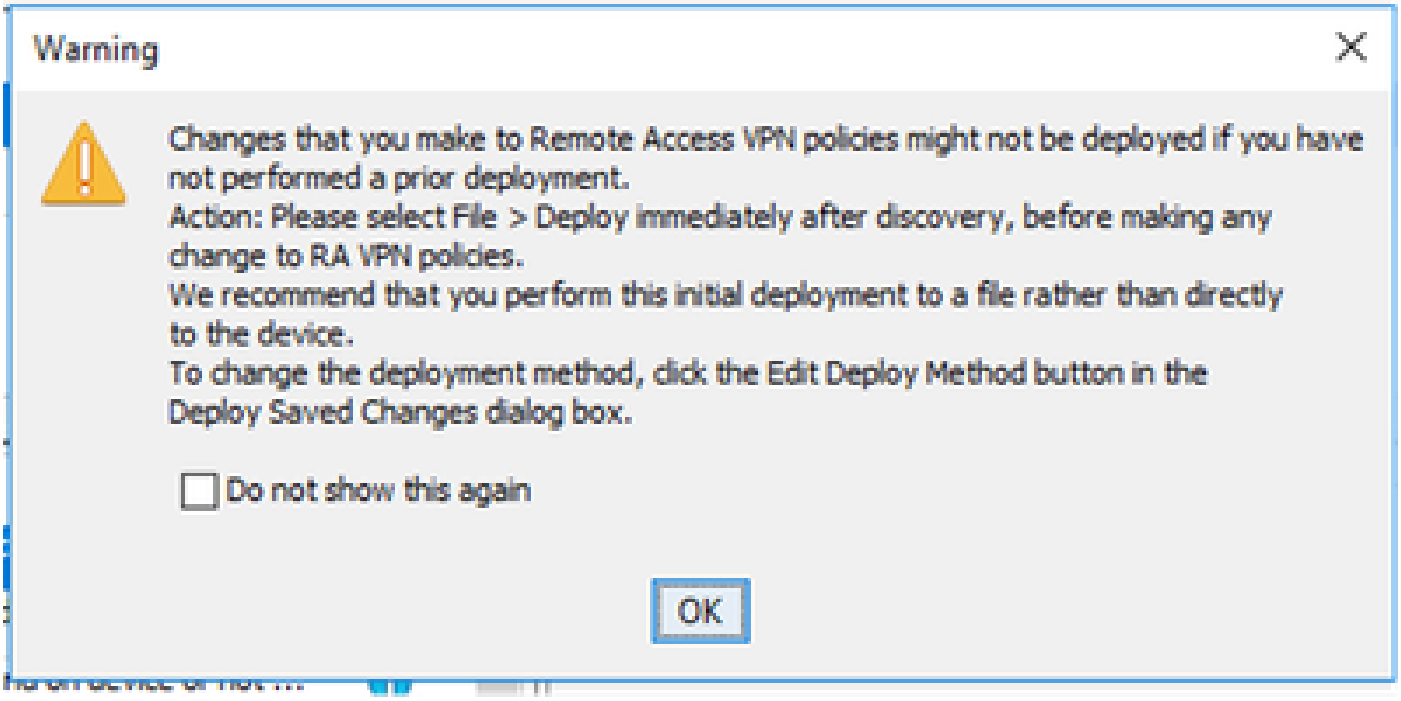


Stap 3:

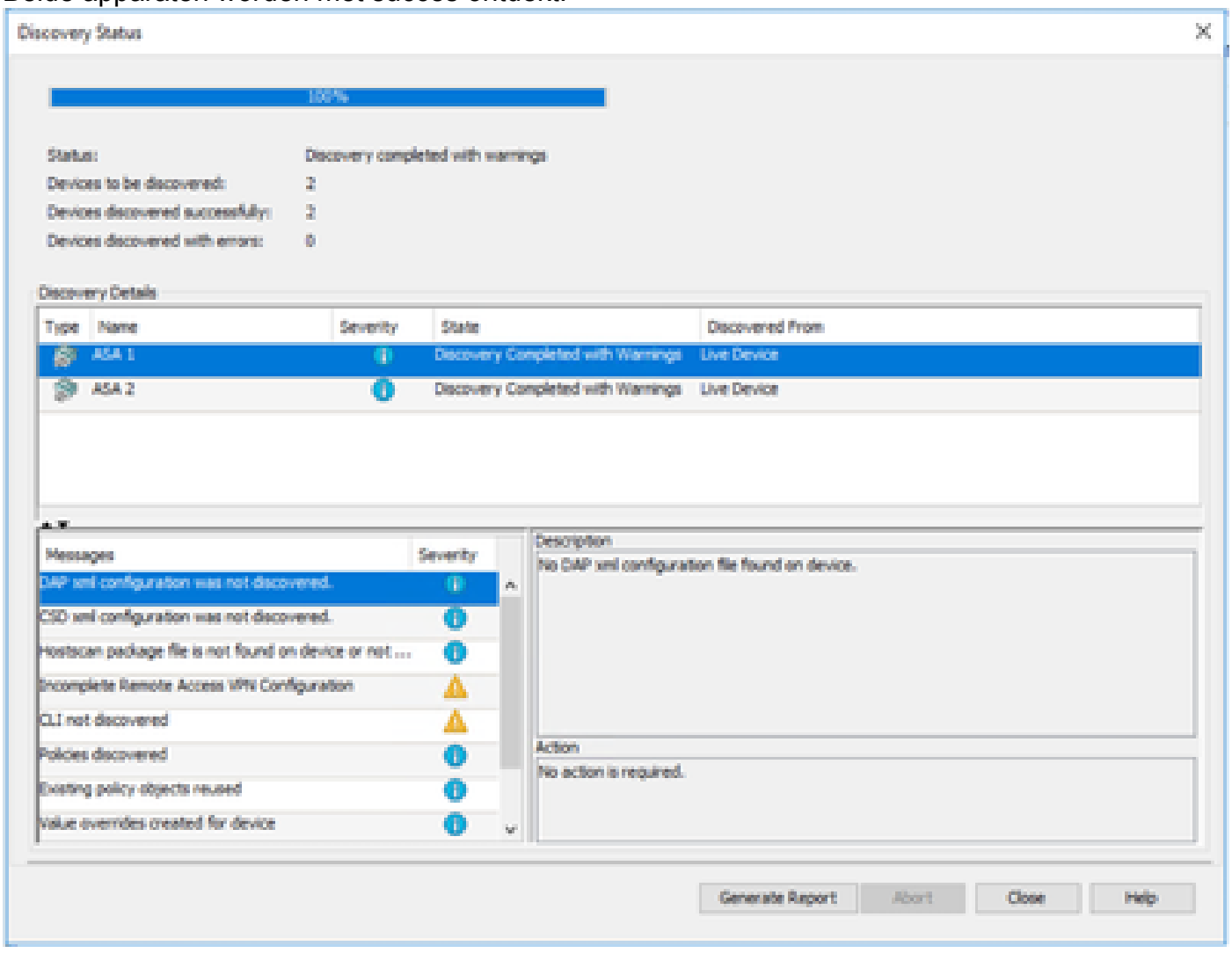
Controleer of alle geselecteerde apparaten worden vermeld en klik op Voltooien om verder te gaan met de bulkherontdekking.
Zorg ervoor dat u zich bewust bent van de netwerktopologie en de veranderingen die in uw netwerk kunnen gebeuren voordat u doorgaat met de ontdekking.



Als de ontdekking is voltooid, kunt u het voorbeeld zien zoals



Beide apparaten worden met succes ontdekt.



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.