Configure Synchronization from Devices to Security Manager

Contents

Introduction

This document describes different ways of configuration synchronization from ASA to CSM.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Security Manager
- Adaptive security device

Components Used

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

- Cisco Security Manager 4.25
- Adaptive security appliance

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

The Cisco security manager delivers centralized management and monitoring services for Cisco ASA device.

Demonstration Methodology

This document describes two distinct methods or options for synchronizing the configuration from ASA to CSM.

- Single device discovery
- Bulk device rediscovery

Single Device Discovery

Single discovery can only be performed if the device is added to the inventory. It can be performed only when the device has

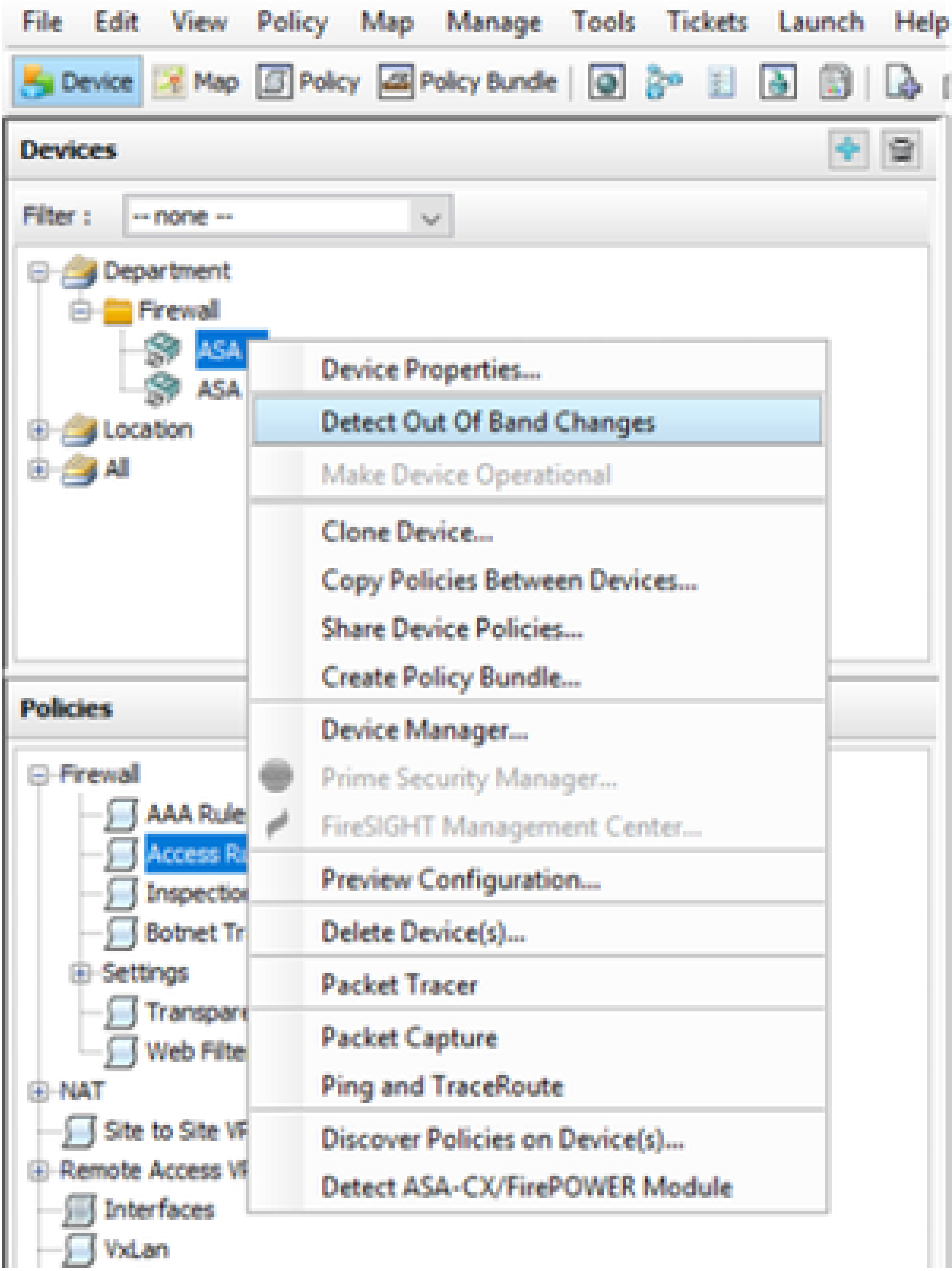
- Security context configurations for ASA, PIX, and FWSM devices running in multiple context mode.
- Virtual sensor configurations for IPS devices.
- Service module information for Catalyst devices.

Steps to Perform Single Device Discovery:

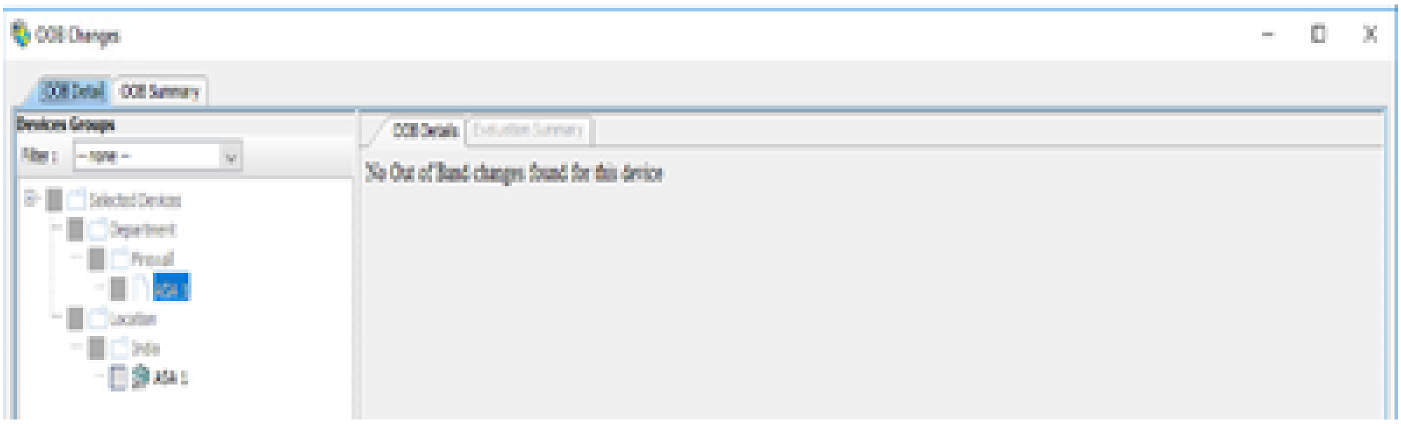
You can perform the device discovery when you have performed any changes on device CLI or if the device was removed and added back.

To check if any pending changes are yet to be synchronized , obeserve the example mentioned.

Right click on the respective device from the device pane and select the option **Detect out of band changes.**

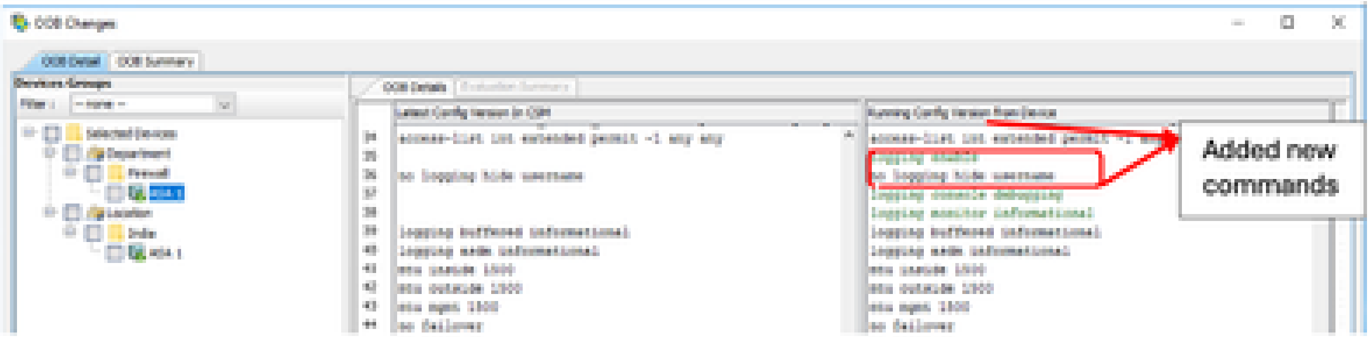


If there are no changes , then the page displays as no out of bound changes found for this device.



No Out of Band changes found for this device

If there were any changes done , then the lines are highlighted as per the legend.



Latest Config Version In CSM

```
access-list 101 extended permit ip any any

no logging hide username


logging buffered informational
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu mgmt 1500
no failover
```

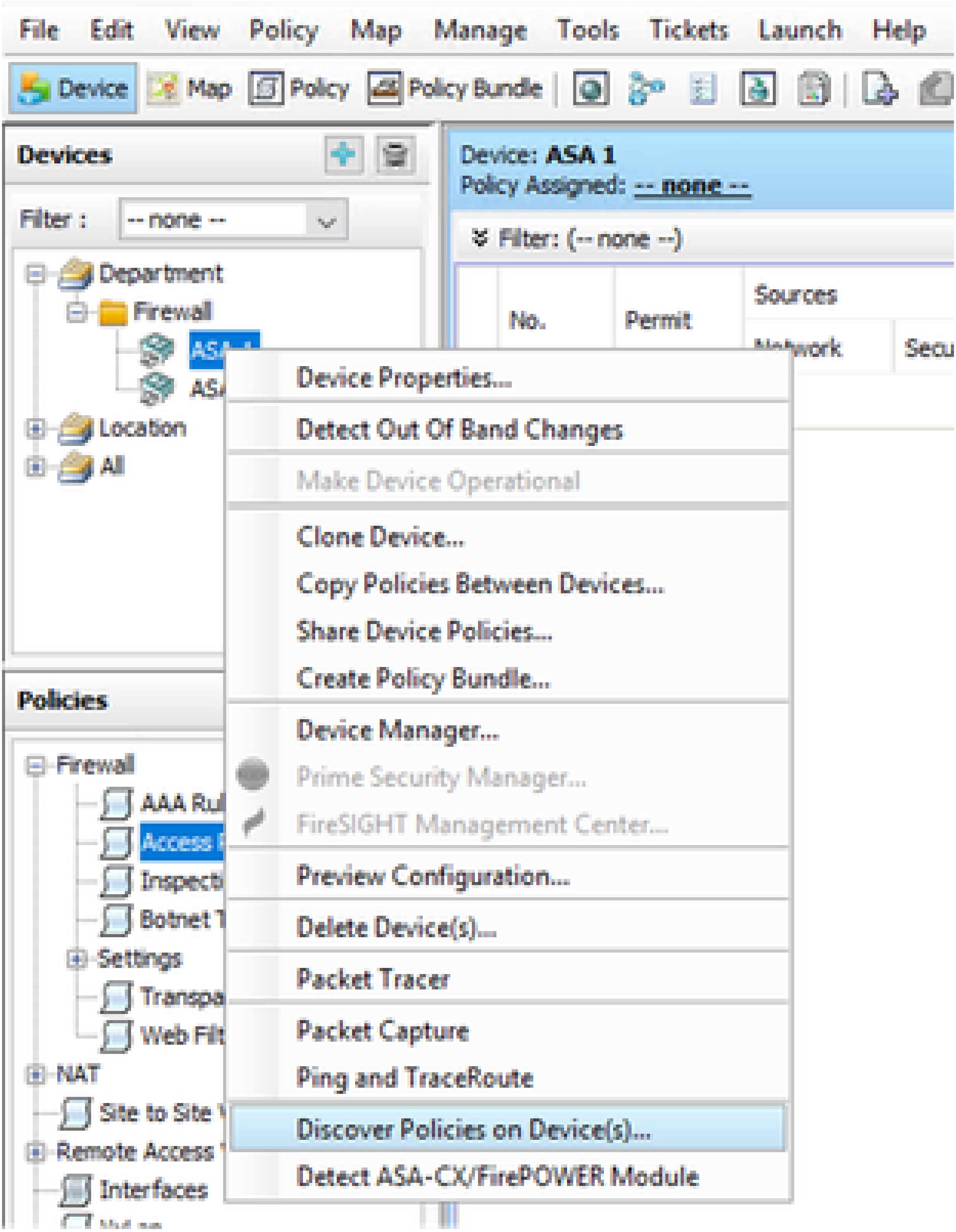
Running Config Version from Device

```
access-list 101 extended permit ip any any
logging enable
no logging hide username
logging console debugging
logging monitor informational
logging buffered informational
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu mgmt 1500
no failover
```

Steps to Perform Single Device Discovery:

Step 1:

Right click on respective device name from **device pane and choose the option Discover policies on Device(s).**



Device: **ASA 1**

Policy Assigned: -- none --

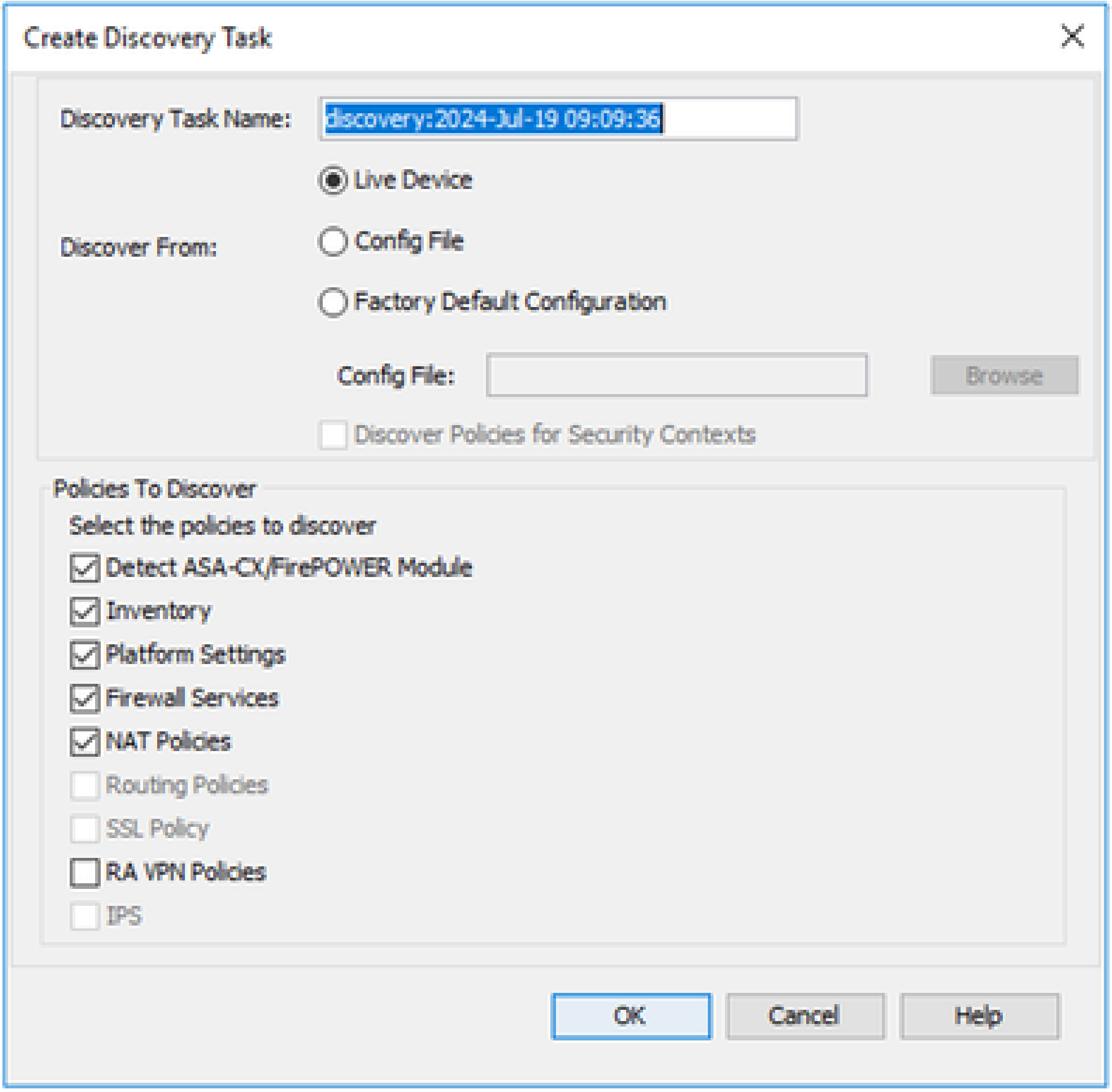
Filter: (-- none --)

Step 2:

For single device recovery method you can only see the **Create Discovery Task** dialogue box. Incase if you are getting a bulk discovery dialogue box , kindly close and open it again.

You have 3 options to perform the discovery.

- **Live Device** – It fetchs the configuration from live device , which is in network.
- **Configuration File** – You can choose the configuration file and proceed with the discovery.
- **Factory Default Configuration** – It resets the device to the default configurations. This method can be used for devices that only run single-context mode or for with individual security contexts.



Create Discovery Task

Discovery Task Name: discovery:2024-Jul-19 09:09:36

Discover From: ● Live Device ○ Config File ○ Factory Default Configuration

Config File:

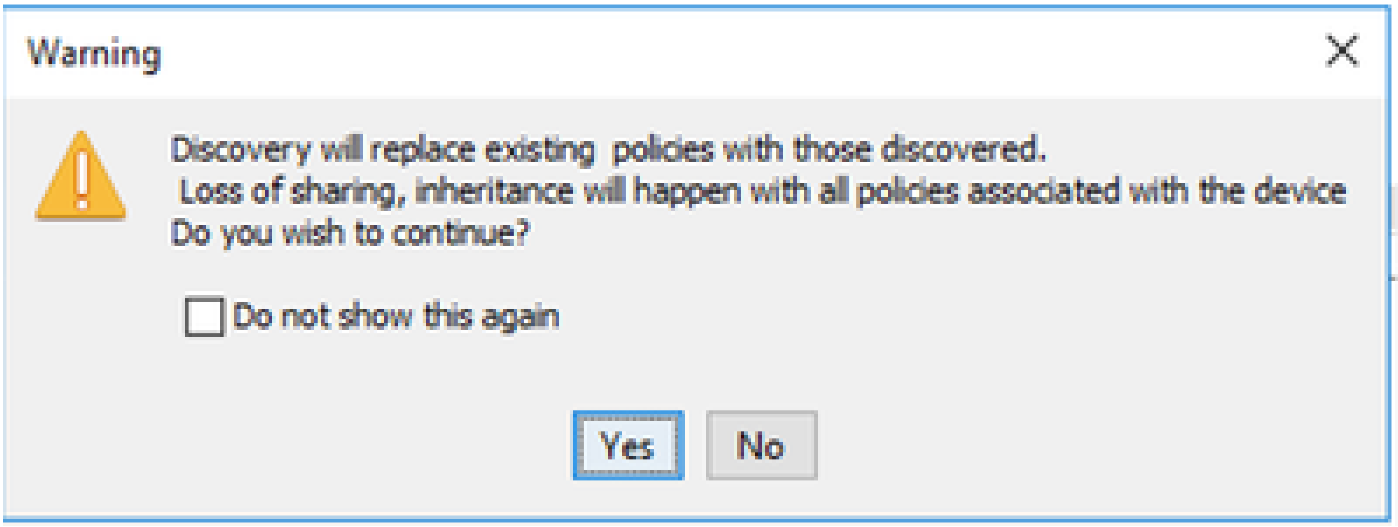
□ Discover Policies for Security Contexts

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

Make sure you are aware of the network topology and the changes that can happen in your network before you proceed with the discovery.

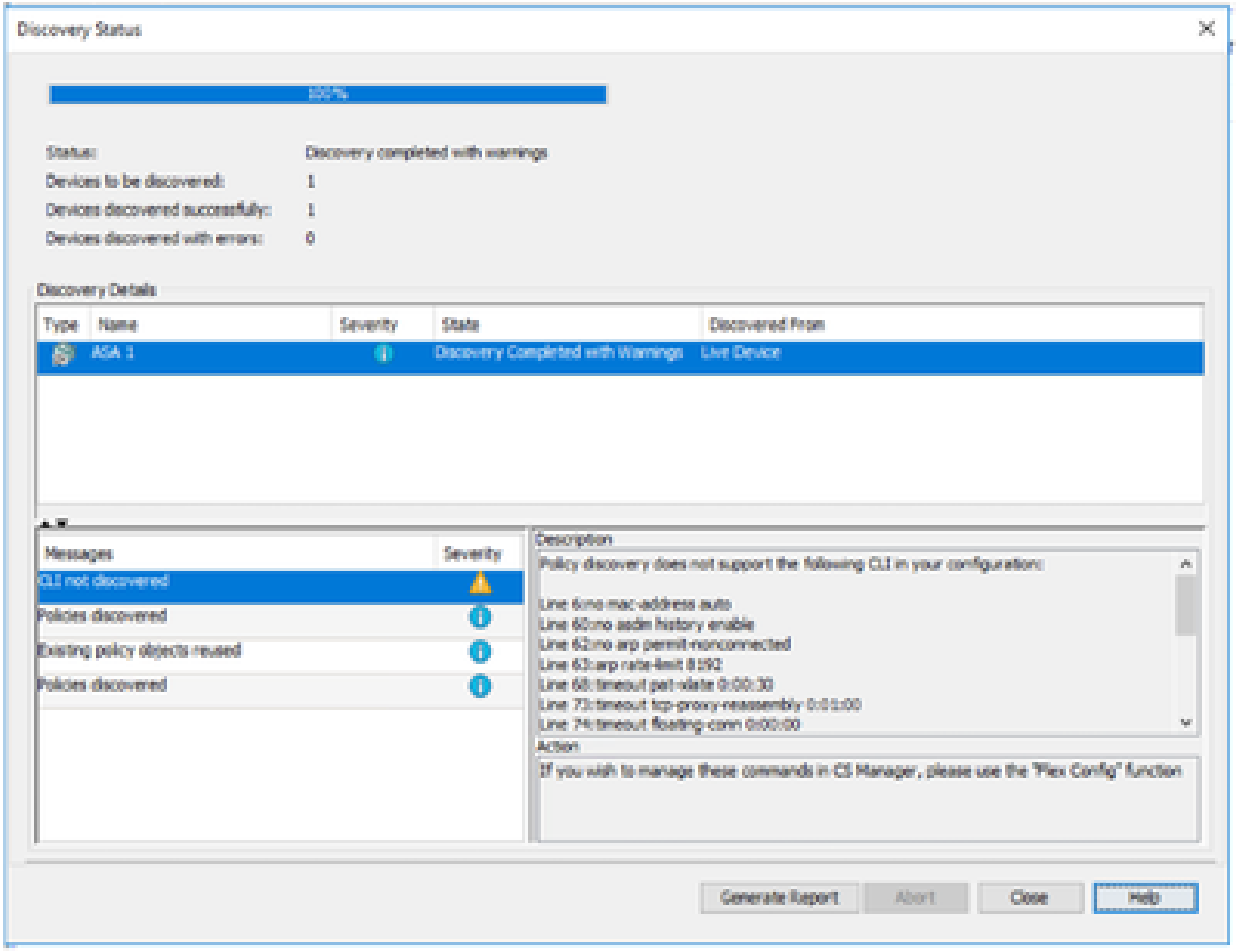


Warning

Discovery will replace existing policies with those discovered.
 Loss of sharing, inheritance will happen with all policies associated with the device
Do you wish to continue?

□ Do not show this again

Once the discover is completed , you can see the pop screen with the status as Discovery completed.



Discovery Status

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
	ASA 1	ⓘ	Discovery Completed with Warnings	Live Device

Messages	Severity
CLI not discovered	⚠
Policies discovered	ⓘ
Existing policy objects reused	ⓘ
Policies discovered	ⓘ

Description

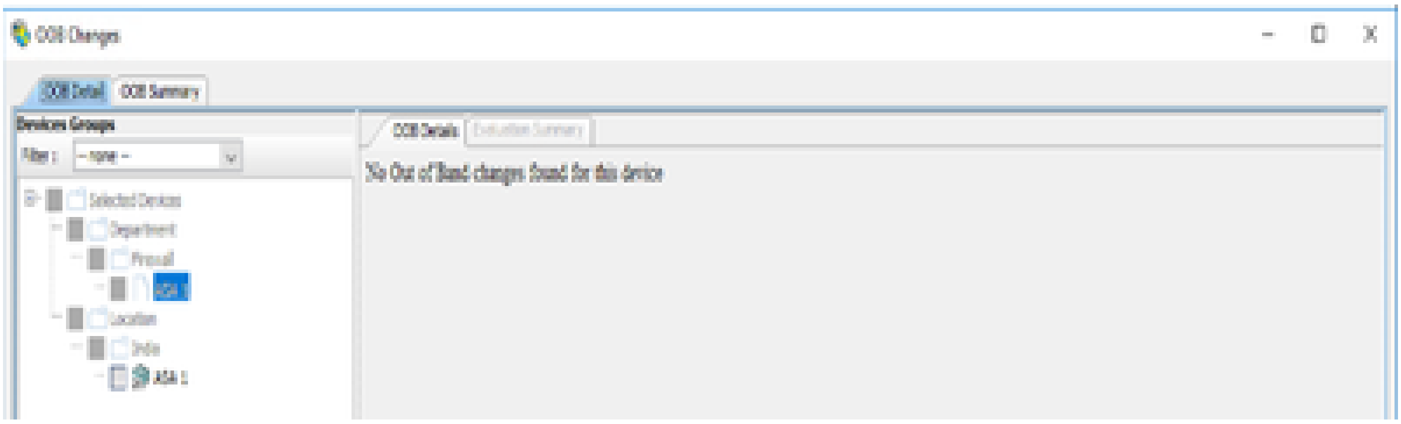
```
Policy discovery does not support the following CLI in your configuration:

Line 6:no mac-address auto
Line 60:no asdm history enable
Line 62:no arp permit-nonconnected
Line 63:arp rate-limit 8192
Line 68:timeout pat-xlate 0:00:30
Line 73:timeout tcp-proxy-reassembly 0:01:00
Line 74:timeout floating-conn 0:00:00
```

Action

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

And from out of band changes also it cannot have any changes.



No Out of Band changes found for this device

Bulk Device Discovery

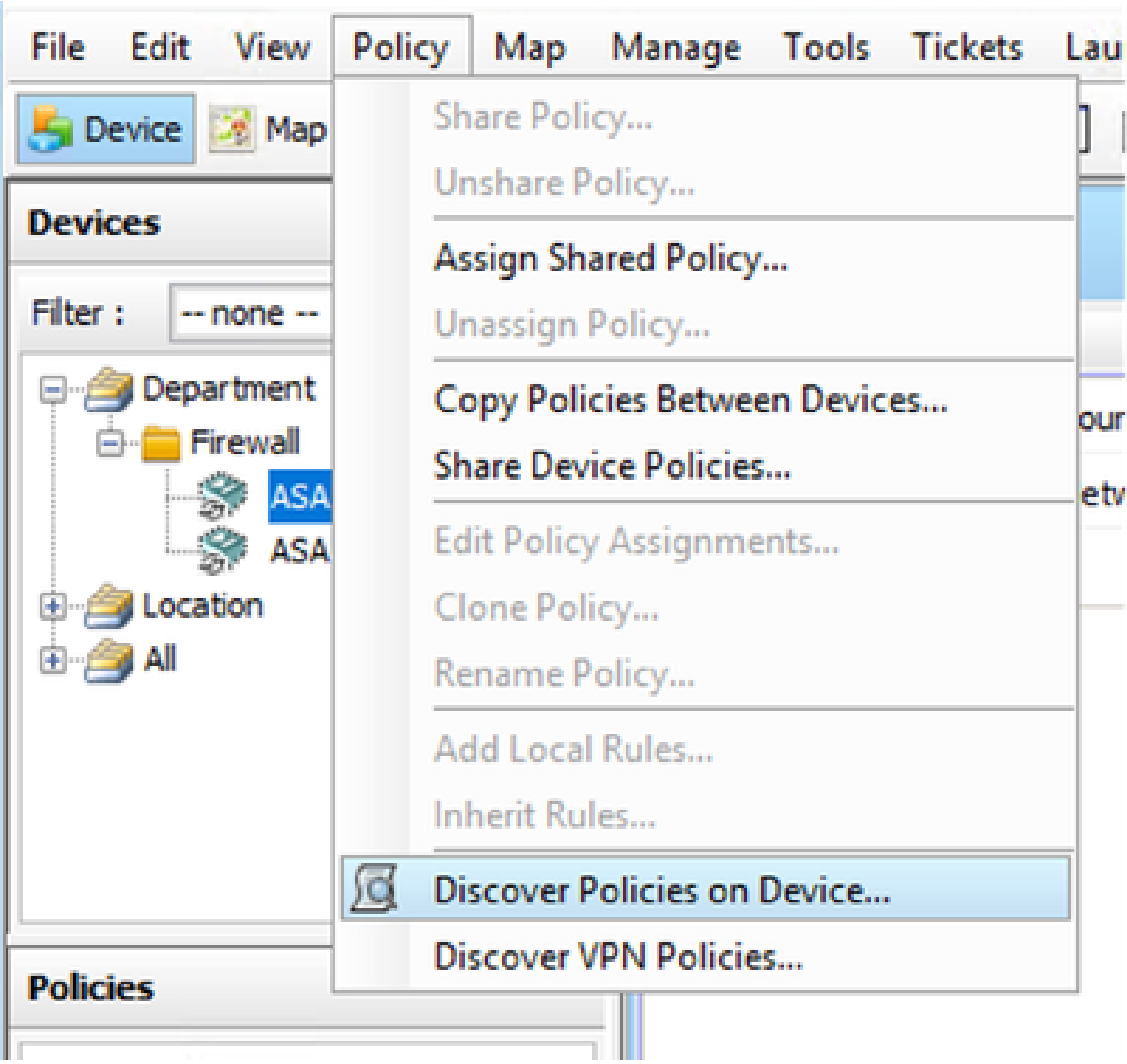
To discover policies for multiple devices, you can conduct bulk rediscovery. It is important to note that bulk rediscovery is limited to live devices , those currently operational and accessible within your network.

You cannot perform the bulk discovery on security context, virtual sensors. Service modules can be discovered it selected separately.

Steps to Perform Bulk Device Discovery:

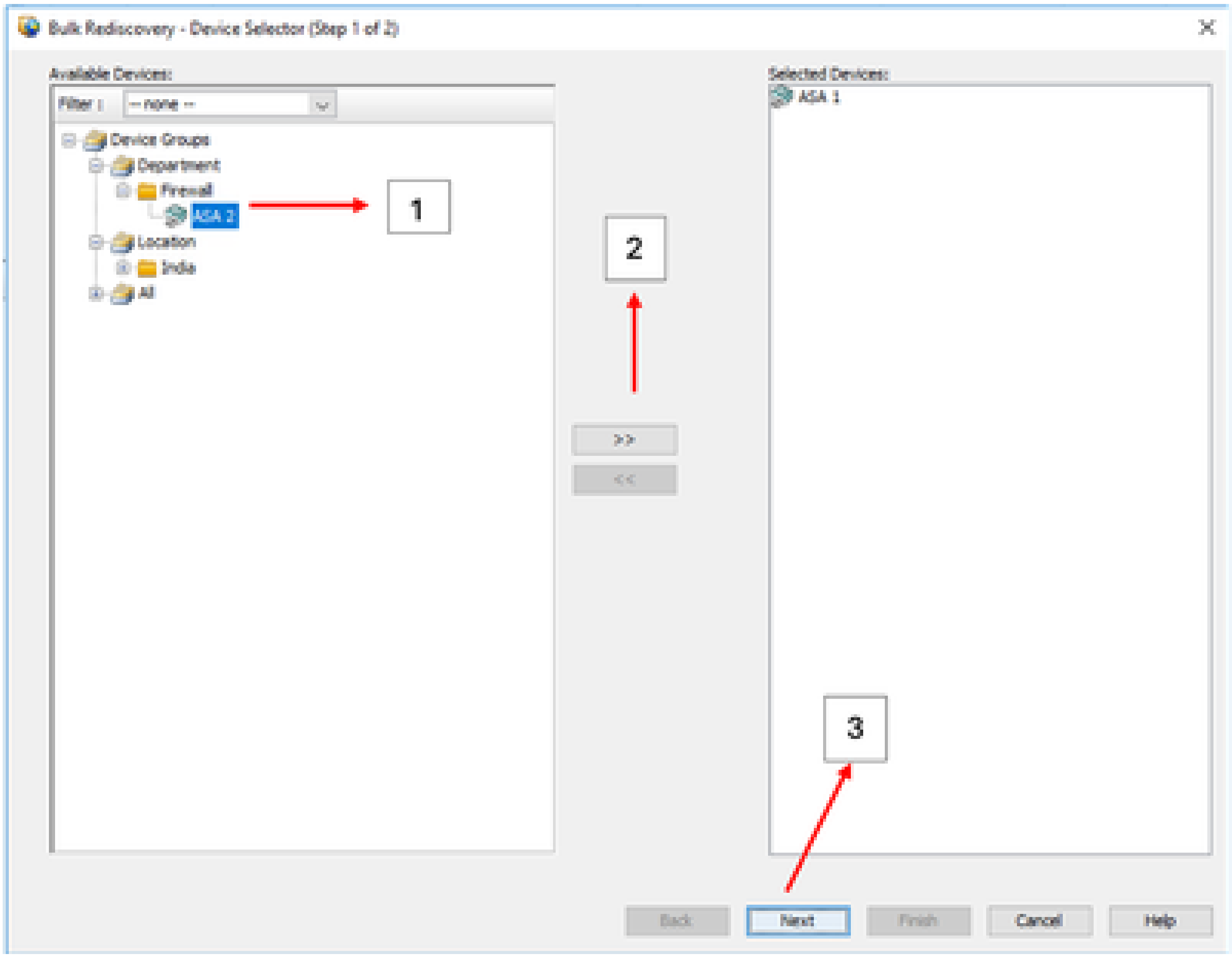
Step 1:

Navigate to **Policy > Discover Policies** on device



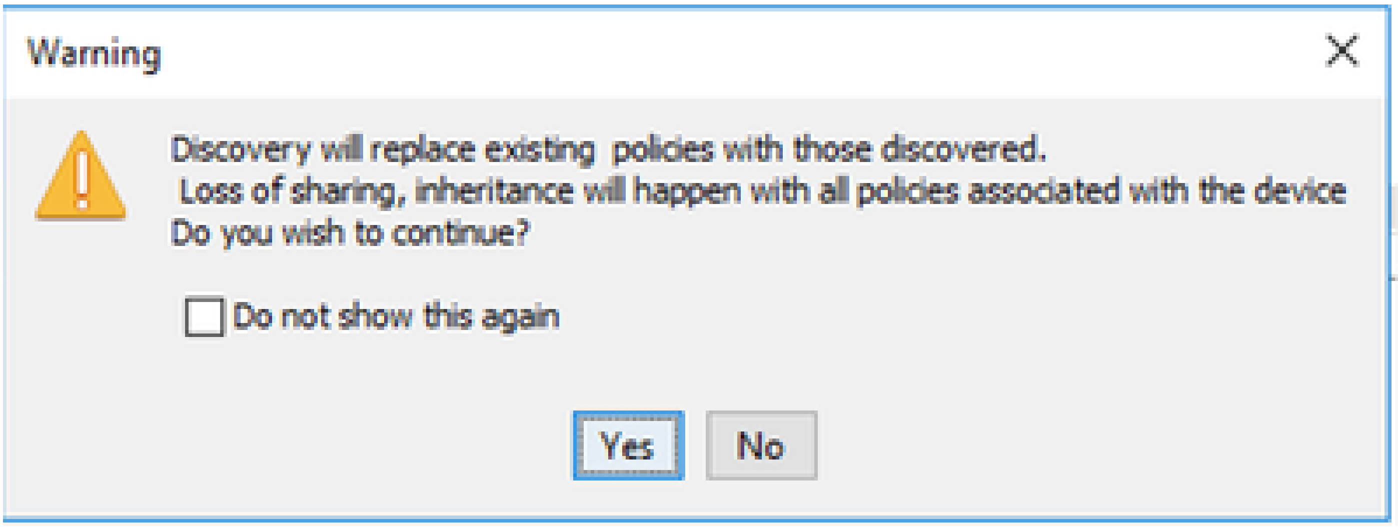
Step 2:

If you are performing Bulk rediscovery , only the bulk rediscovery dialogue box can appear.
From available devices in the left pane , choose the list of devices for which you want to discover policies and move it to the right side.



Step 3:

Verify if all the selected devices are listed and click on Finish to proceed further with the bulk rediscovery. Make sure you are aware of the network topology and the changes that can happen in your network before you proceed with the discovery.

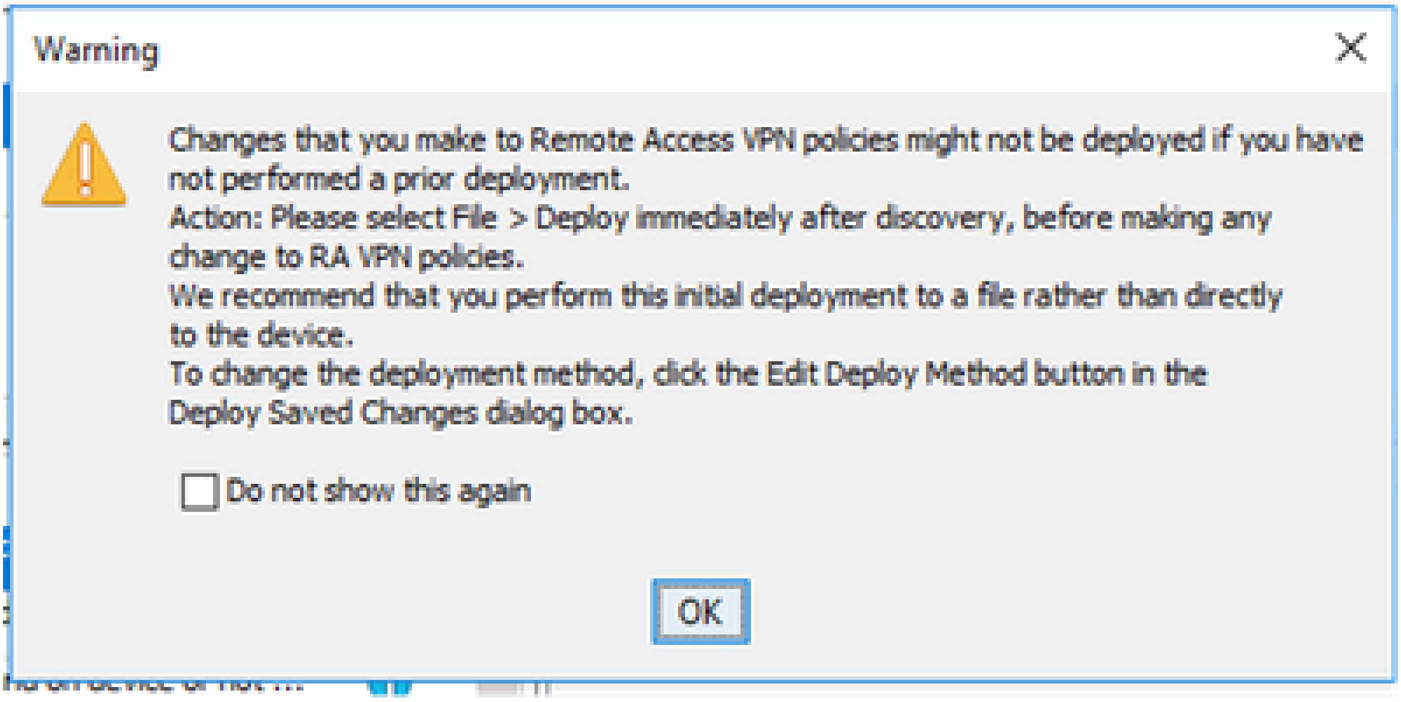


Warning

Discovery will replace existing policies with those discovered.
Loss of sharing, inheritance will happen with all policies associated with the device
Do you wish to continue?

□ Do not show this again

Once the discovery is completed you can see the example like

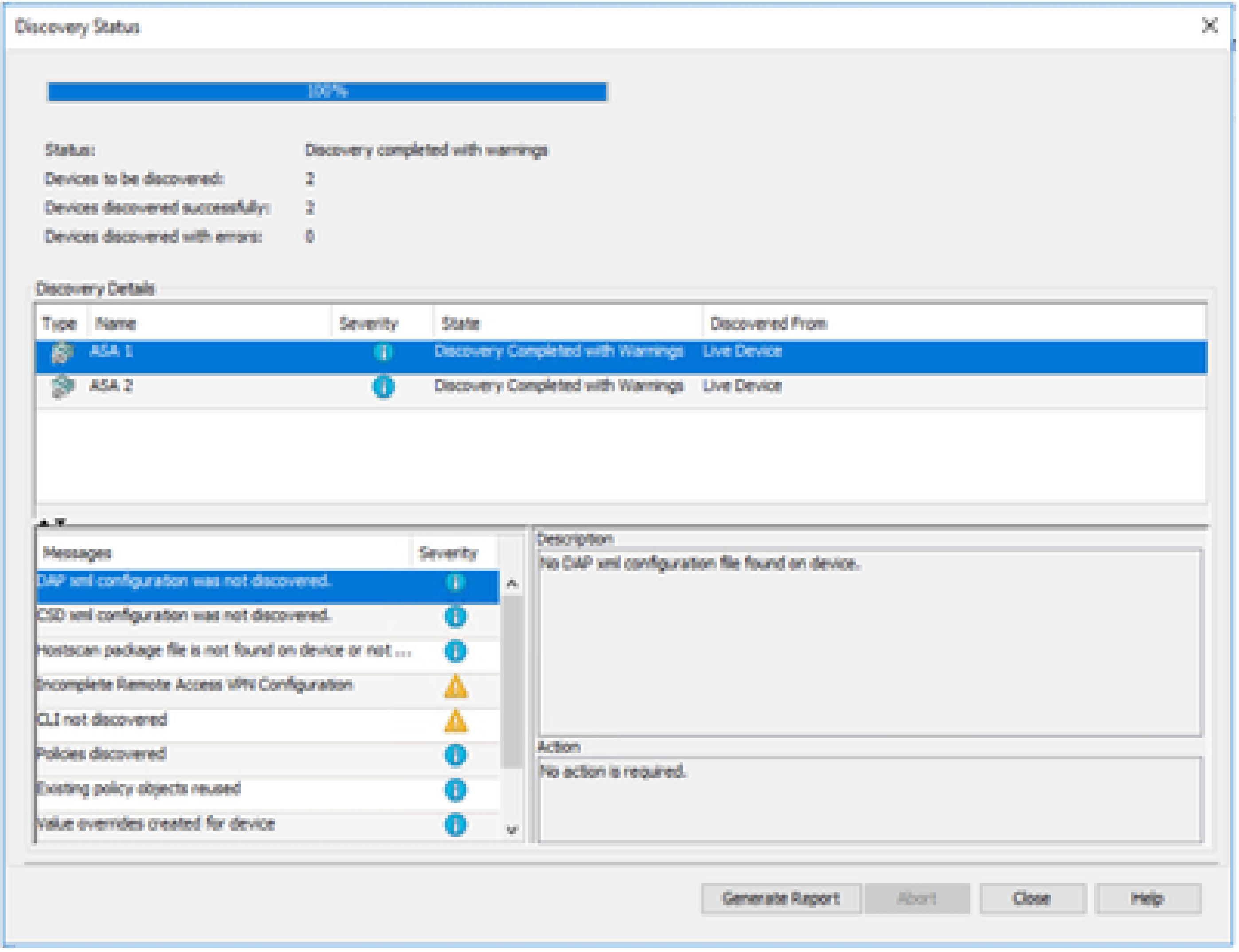


Warning

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

Both the devices are discovered successfully.



Discovery Status

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 1	ⓘ	Discovery Completed with Warnings	Live Device
	ASA 2	ⓘ	Discovery Completed with Warnings	Live Device

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

Description
No DAP xml configuration file found on device.

Action
No action is required.