Demonstrate Different Ways to Add Security Firewall Devices to CSM

Contents

Introduction	
Prerequisites	
Requirements	
Components Used	
Background Information	
Demonstration Methodology	
How to Navigate to Add Device	
Ways to Add Device to CSM	
Add a Device From Network	
Step 1:	
<u>Step 2:</u>	
<u>Step 3:</u>	
<u>Step 4:</u>	
Add a New Device	
<u>Step 1:</u>	
<u>Step 2:</u>	
<u>Step 3:</u>	
Step 4:	

Introduction

This document describes different methods to add security firewall devices to Cisco Security Manager (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 focuses on 2 ways to add the device to CSM.

- Add device from network
- Add a new device

How to Navigate to Add Device

You can navigate to add device in 2 ways.

- 1. Navigate to **File > New device**.
- 2. Right click from device pane or use the plus icon in the device pane.





Ways to Add Device to CSM

Add a Device From Network

Security Manager establishes a direct and secure connection to active devices on the network to retrieve their identifying information and properties.

Step 1:

Once you click **new device**, the pop window appears. Choose the first option, **Add device from network**.



Step 2:

New Device - Device Info	ormation (Step 2 of 4)					×
Sdentity IP Types Host Name: Domain Name: IP Address: Display Name:* OS Type:* Transport Photocol:	Static					
Discover Device Settings	Policies and Inventory Platform Settings Previal Policies NAT Policies RA VPN Policies Discover Policies for Security Contexts					
		Back	Next	Frish	Cancel	Нер

Step 3:

New Device - Device Credent	tials (Step 3 of 4)		×
Primary Credentials Username: Password:*		Confirm:*	
Enable Password:		Confirm	
HTTP Credentials			
	Usernames Password: Confirm:		
HTTP Port:	80		
HTTPS Part:	643	Use Default	
Certificate Common Name:	Use Denant (milling)	Confirm:	
RX doot Mode 5	284		
		Back Next	Finish Cancel Help

\

Step 4:

If you need to add the department or location to group the device, you can choose the **Edit groups** options.

New Device - Device Grouping ()	(kep 4 of 4)			\times
Select the groups that this device	belongs to:			
Department	Nove			
Locations	Nors			
🗌 Set Volues as Default				
		lack Next	Finish Cancel	Help

Once the edit device group pop up window opens, you can add group or types based on the requirement.

New Device - Device Grouping	(Step 4 of 4) X
Select the groups that this devi	ot belongs to:
Departments	E Freval 20
Location:	Edit Device Groups X
. 🔲 Set Wakses as Default	Grape: Copartment Costantion
	OK Cancel Help
	Back Next Presh Cancel Help

Once you click **finish**, the device is registered. You see a window similar to the example shown.

	2005			
Status	Discovery compl	leted with warrings		
Devices to be docovered:	1			
Devices discovered successfully:	1			
Devices discovered with errors:	•			
Discovery Cetals				
Type Name	Severity	State	Discovered Prom	
8		Docovery Completed with	Namings Live Device	
-				
		Severity Description		
• •		Severity Description Policy deco	ery does not support the following CLI in your configuration:	~
Messages CLI not docovered Folicies docovered		Sevenity A Une Strom	ery does not support the following CLI in your configuration:	~
• • • Messages Foldes decovered Policies decovered Existing policy sbjects reused		Severity Severity Policy deco Line Sizona Line Sizona Line Sizona	ery does not support the following CLI in your configuration: sc-address auto sdm history enable rp permit -nanconnected	^
Messages Tolices docovered Notices docovered Existing policy objects neused Noticy objects oreated		Severity Severity Cescription Policy deco Line Strong Line Strong Line Strong Line Strong Line Strong Line Strong Line Strong	ery does not support the following CLI in your configuration: ac-address auto edm history enable rp permit nanconnected vate-limit 8102 out pat-skiete 0:00:30	A
Messages Reliant docovered Rolices docovered Existing policy objects neused Rolicy objects created Rolices docovered		Severity Description Policy deco Une Strong / Une Stro	ery does not support the following CLI in your configuration: scheddress auto adm history enable rp permit nonconnected rate-limit 8192 out pat-slate 0.100:30 out hat-proxy-reasenbly 0.01.00 out hat-proxy-reasenbly 0.01.00 out factors com 0.000.00	
		Sevenity Policy deco Line Sizes Une Sizes Une Sizes Line Sizes	ery does not support the following CLI in your configuration: screddress auto edm history enable rp permit noncommected rate limit 8192 out spin-printy-reassembly 0:01:00 out fige-printy-reassembly 0:01:00 out fige-printy-reassembly 0:01:00	1
Messages Reliance docovered Policies docovered Existing policy objects neused Policies docovered Policies docovered Add Device Successful		Severity Severity Severity Severity Policy deco Line Sino in Line	ery does not support the following CLI in your configuration: c-address auto adm history enable rp permit-nonconnected vate-limit 6192 out pat-slate 0:00:30 out pat-slate 0:00:30 out top-priory-reassenbly 0:01:00 out floating-conn 0:00:00 to manage these commands in CS Manager, please use the "Hex Config" funct	A v

The device is added to both department and location groups as created earlier. In this example, you created the location group as India and Department group as Firewall.



Add a New Device

To incorporate a device that is not currently part of the network, enable pre-provisioning in Security Manager. You have the option to create the device within the system. This allows you to assign policies to the device and generate configuration files prior to installing the device hardware.

Step 1:

Once you click new device, the pop up window appears. Choose the option Add device from network.



Step 2:

Select the **device type** from left pane, and enter the **device details** in the right pane.



Device Type		Liferation .	
Geco Interface Cards	-	R Tuter	Carbo Carbo
E Cisco Network Modules		as a library	
E Coco Security Modules for Security Appliances		Host Name:	
③ Coco Services Modules		Domain Names	
🛞 🧮 Rovters		The Address of	
Security and 1991		P ACCESS:	
E Ceco 7100 Series VPN Routers		Display Name: *	
Cisco ASA Series Adaptive Security Appliances			
 Osco ASA Adaptive Security Virtual Appliance 		Operating System	
 Security Applance 		OS Type:	ASA
 Second ASA-5506 Adaptive Security Appliance 		Target OS Version:	9.12(2)
CISOS ASA-5309H Adaptive Security Applance			
Cisco ASA-5506W Adaptive Security Appliance		Contexts:	STALE
- get Caco ASA-5508 Adaptive Security Applance		Operational Mode:	ROUTER
Caco ADA-DOU Adaptive Security Appende			
Caco AGA-0512 Adaptive Security Appliance		Auto Update	
Cons Kit SUS Adaptive Security Applied of Cons Mit SUS Adaptive Security Applied of		Server:	None
Constanting Security Anglance		Desire Meethy	
- S Case AtA-5125 Adaptive Security Anniance		TOTAL PROPERTY.	
- S Coro 454-5540 Adaptive Security Applance		Research Core Security	v Manadar
Osco A5A-5545 Adaptive Security Applance		2	
- Deco ASA-5550 Adaptive Security Applance		Security Context of Unit	sanaged Device
Coco ASA-5555 Adaptive Security Applance		Clicense Supports Palove	·
- Deco ASA-5580 Adaptive Security Appliance			Add the device details
Coco ASA-5585 Adaptive Security Appliance	÷.		and versions to register
			and versions to registe
Selected Device Type:* Adaptive Security Virtual Applance			
System Object ID: 1.3.6.1.4.1.9.1.1902 v			

Step 3:

Enter the **device username** and **credential details**.

New Device - Device Credent	tials (Step 3 of 4)						×
Primary Credentials Username: Password: Enable Password:		Confirm: Confirm:					
HTTP Credentials	Use Primary Credentials						
HTTP: Facts	Password:						
HTTPS Port IPS RDEP Mode:	HIS Use Default (HTTPS) v	Use Defa	R.				
RX-Boot Mode	2017	Contract					
Test Connectivity							
			Back.	Next	Finish	Cancel	Heb

Step 4:

Add the **device** to the groups.

New Device - Device Grouping ()	kep 4 of 4)			×
Select the groups that the device	belongs to:			
Department	Note		•	
Locations	Sono			
Set Values as Default				
		Beck Fil	ext Frish	Cancel Help

Once you click **finish**, the device is registered and it shows as depicted in the example.

