Deploy Example on CSM to ASA

Contents

- Introduction
- Prerequisites
  - Requirements
  - Components Used
- Background Information
- Configure
  - Non-Workflow Mode without Ticket Management
  - Non-Workflow Mode with Ticket Management
    - Enable Ticket Management
    - Deployment with Non-Workflow Mode with Ticket Management
- Troubleshoot

Introduction

This document describes a deployment on Cisco Security Manager (CSM) using workflow and ticket base.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Adaptive Security Appliance (ASA)
- Knowledge of Firewall configuration

Components Used

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

- Windows Server 2012
- CSM v4.22
- ASA v9.12.5

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

Specific requirements for this document include:

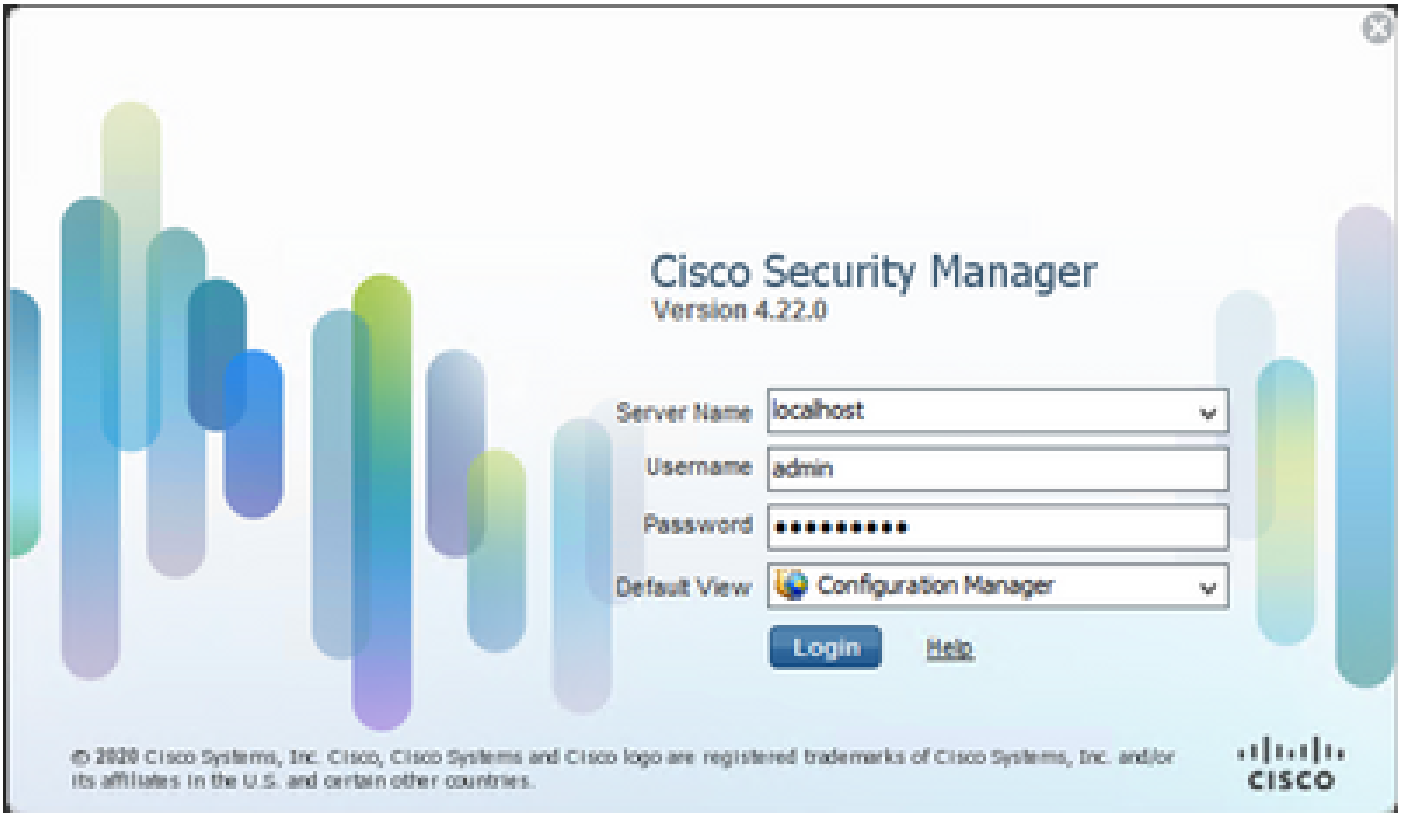
- Ensure you have enough privileges to make the necessary changes
- Ensure that you understand the changes you are going to make with each deployment

- Choose the appropriate guide depending on your current configuration

Configure

Non-Workflow Mode without Ticket Management

Step 1. Log in to Cisco Security Manager Client. From the dropdown, choose Configuration Manager.

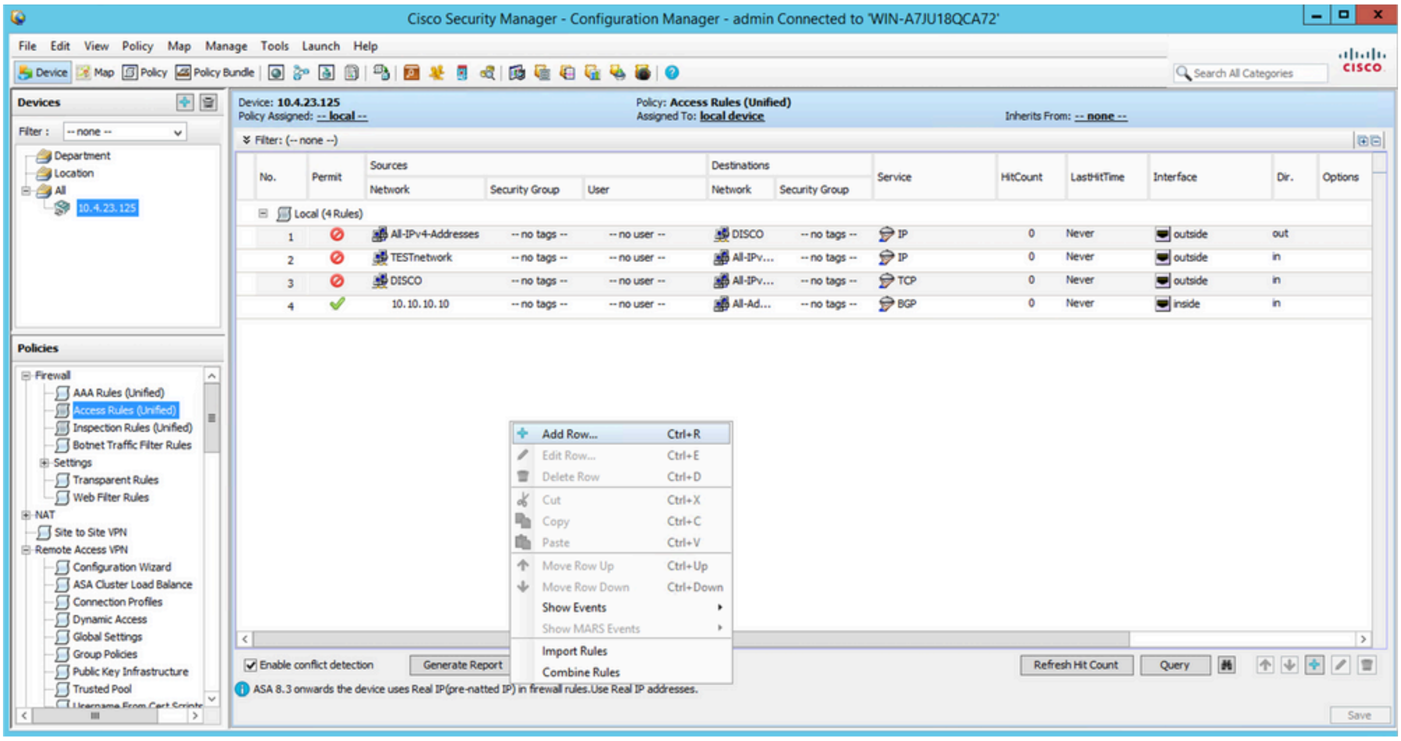


Cisco Security Manager
Version 4.22.0

Server Name: localhost
Username: admin
Password: **********
Default View: Configuration Manager

© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Step 2. Make changes that you like to deploy.



Cisco Security Manager - Configuration Manager - admin Connected to 'WIN-A7JU18QCA72'

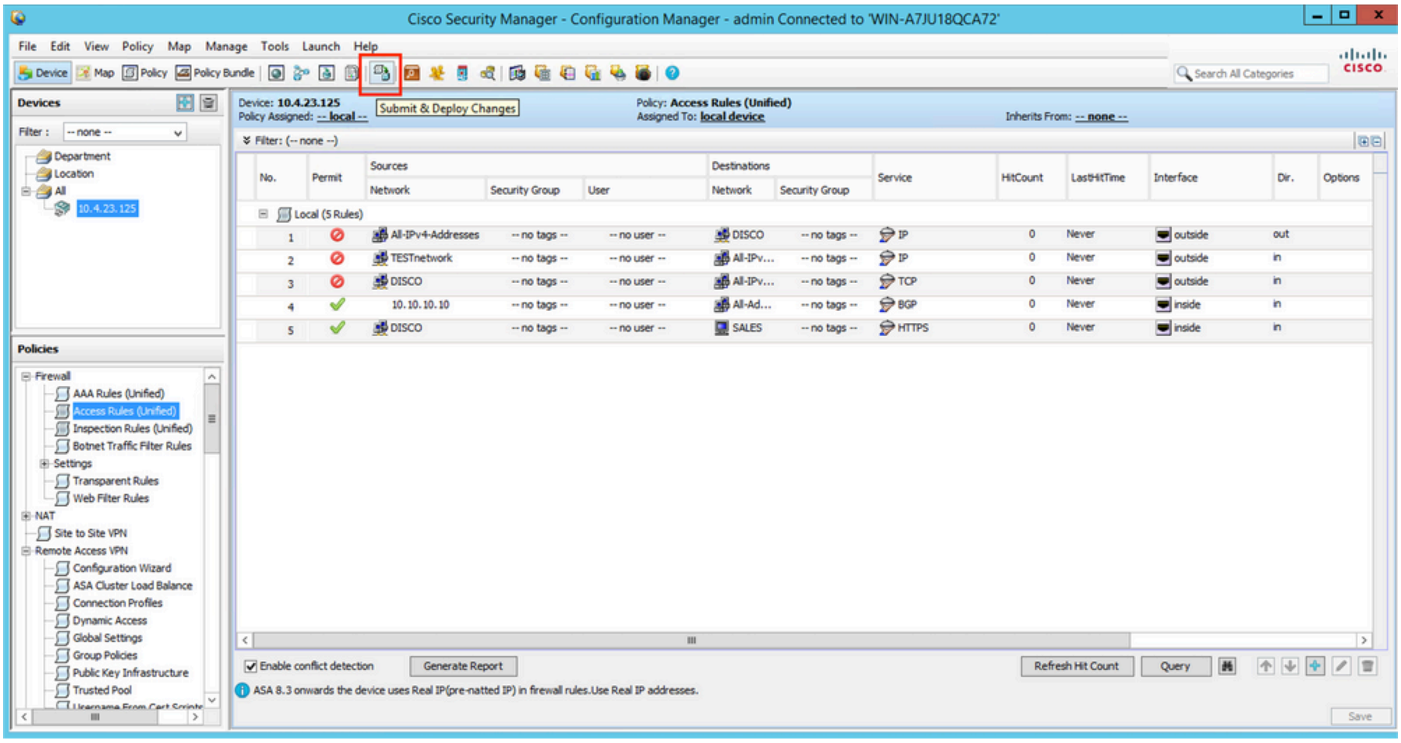
Device: 10.4.23.125
Policy Assigned: -- local --
Policy: Access Rules (Unified)
Assigned To: local device
Inherits From: -- none --
Filter: (-- none --)

		Sources			Destinations							
No.	Permit	Network	Security Group	User	Network	Security Group	Service	HitCount	LastHitTime	Interface	Dir.	Options
Local (4 Rules)												
1	⊘	All-IPv4-Addresses	-- no tags --	-- no user --	DISCO	-- no tags --	IP	0	Never	outside	out	
2	⊘	TESTnetwork	-- no tags --	-- no user --	All-IPv...	-- no tags --	IP	0	Never	outside	in	
3	⊘	DISCO	-- no tags --	-- no user --	All-IPv...	-- no tags --	TCP	0	Never	outside	in	
4	✓	10.10.10.10	-- no tags --	-- no user --	All-Ad...	-- no tags --	BGP	0	Never	inside	in	

☑ Enable conflict detection

ASA 8.3 onwards the device uses Real IP(pre-natted IP) in firewall rules.Use Real IP addresses.

Step 3. Navigate to Submit & Deploy Changes.



Cisco Security Manager - Configuration Manager - admin Connected to 'WIN-A7JU18QCA72'

Device: **10.4.23.125**
Policy Assigned: **-- local --**

Policy: **Access Rules (Unified)**
Assigned To: **local device**

Inherits From: **-- none --**

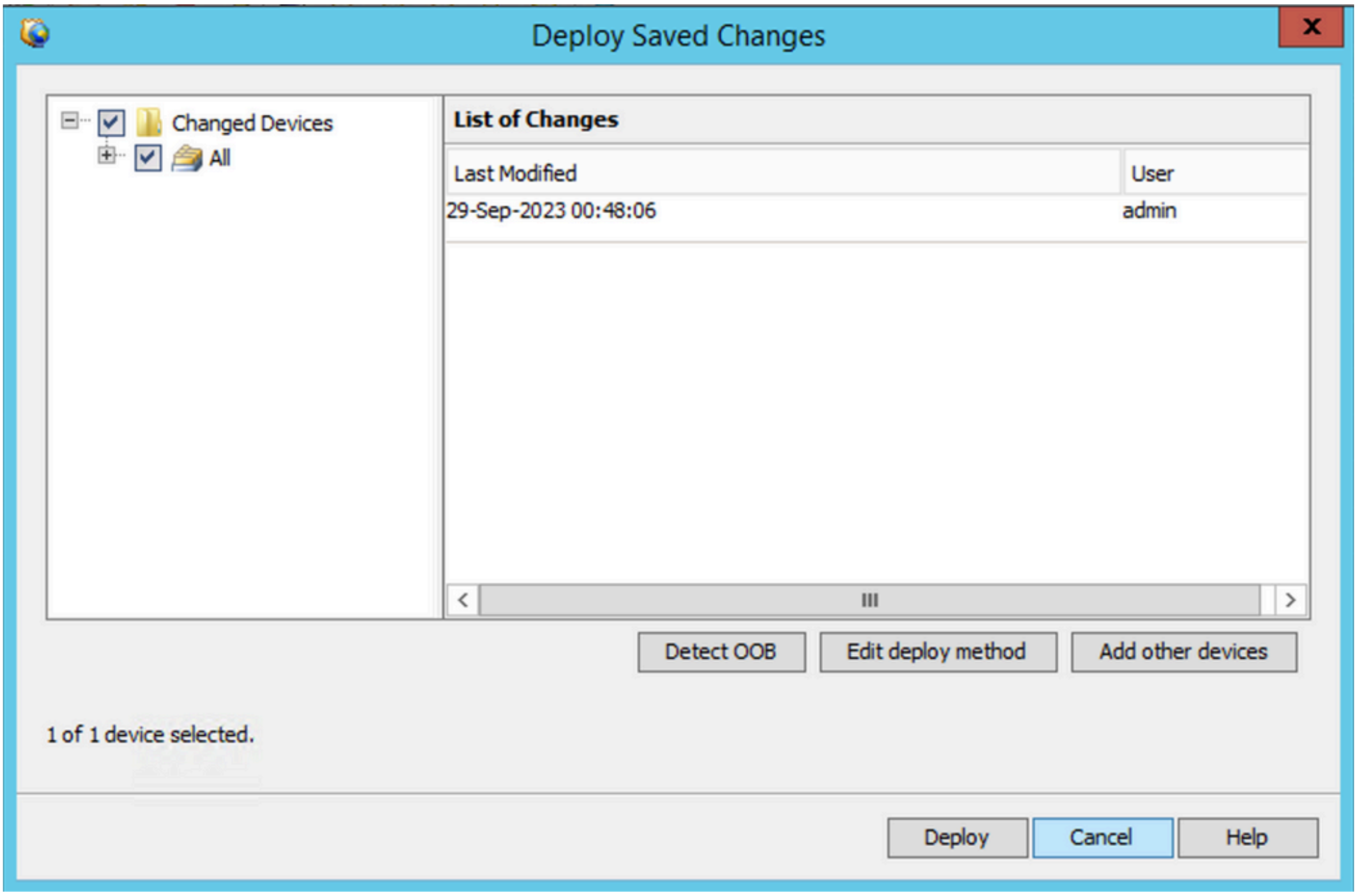
Filter: (-- none --)

No.	Permit	Sources			Destinations		Service	HitCount	LastHitTime	Interface	Dir.	Options
		Network	Security Group	User	Network	Security Group						
Local (5 Rules)												
1	⊘	All-IPv4-Addresses	-- no tags --	-- no user --	DISCO	-- no tags --	IP	0	Never	outside	out	
2	⊘	TESTnetwork	-- no tags --	-- no user --	All-IPv...	-- no tags --	IP	0	Never	outside	in	
3	⊘	DISCO	-- no tags --	-- no user --	All-IPv...	-- no tags --	TCP	0	Never	outside	in	
4	✓	10.10.10.10	-- no tags --	-- no user --	All-Ad...	-- no tags --	BGP	0	Never	inside	in	
5	✓	DISCO	-- no tags --	-- no user --	SALES	-- no tags --	HTTPS	0	Never	inside	in	

☑ Enable conflict detection

ASA 8.3 onwards the device uses Real IP(pre-natted IP) in firewall rules.Use Real IP addresses.

Step 4. Choose the devices that you want to deploy to and when you are ready, click **Deploy**.



Deploy Saved Changes

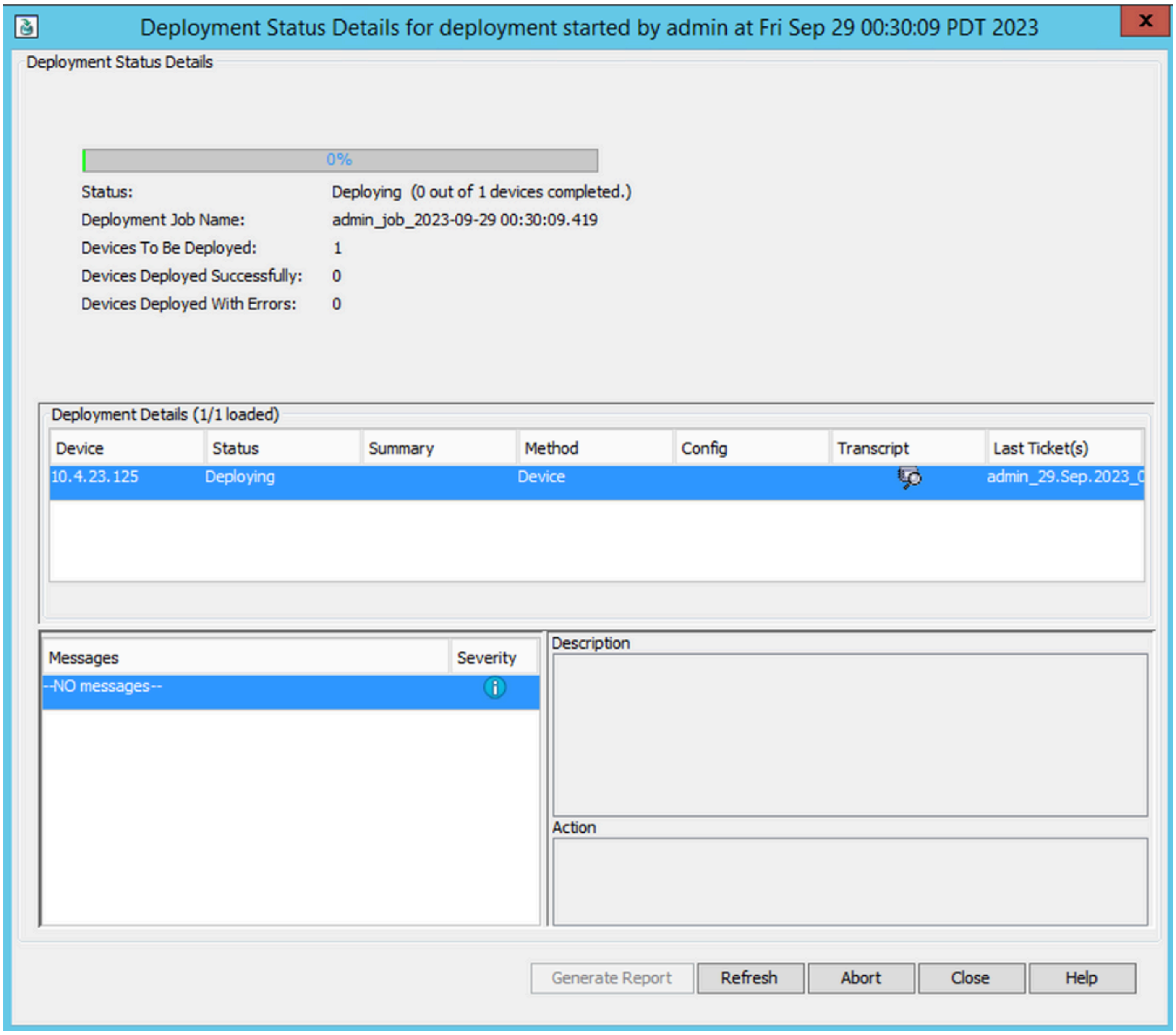
☑ Changed Devices
☑ All

List of Changes

Last Modified	User
29-Sep-2023 00:48:06	admin

1 of 1 device selected.

Note: While deployment is running, a pop-up window appears where you can monitor the progress.



Deployment Status Details for deployment started by admin at Fri Sep 29 00:30:09 PDT 2023

Deployment Status Details

0%

Status: Deploying (0 out of 1 devices completed.)
Deployment Job Name: admin_job_2023-09-29 00:30:09.419
Devices To Be Deployed: 1
Devices Deployed Successfully: 0
Devices Deployed With Errors: 0

Deployment Details (1/1 loaded)

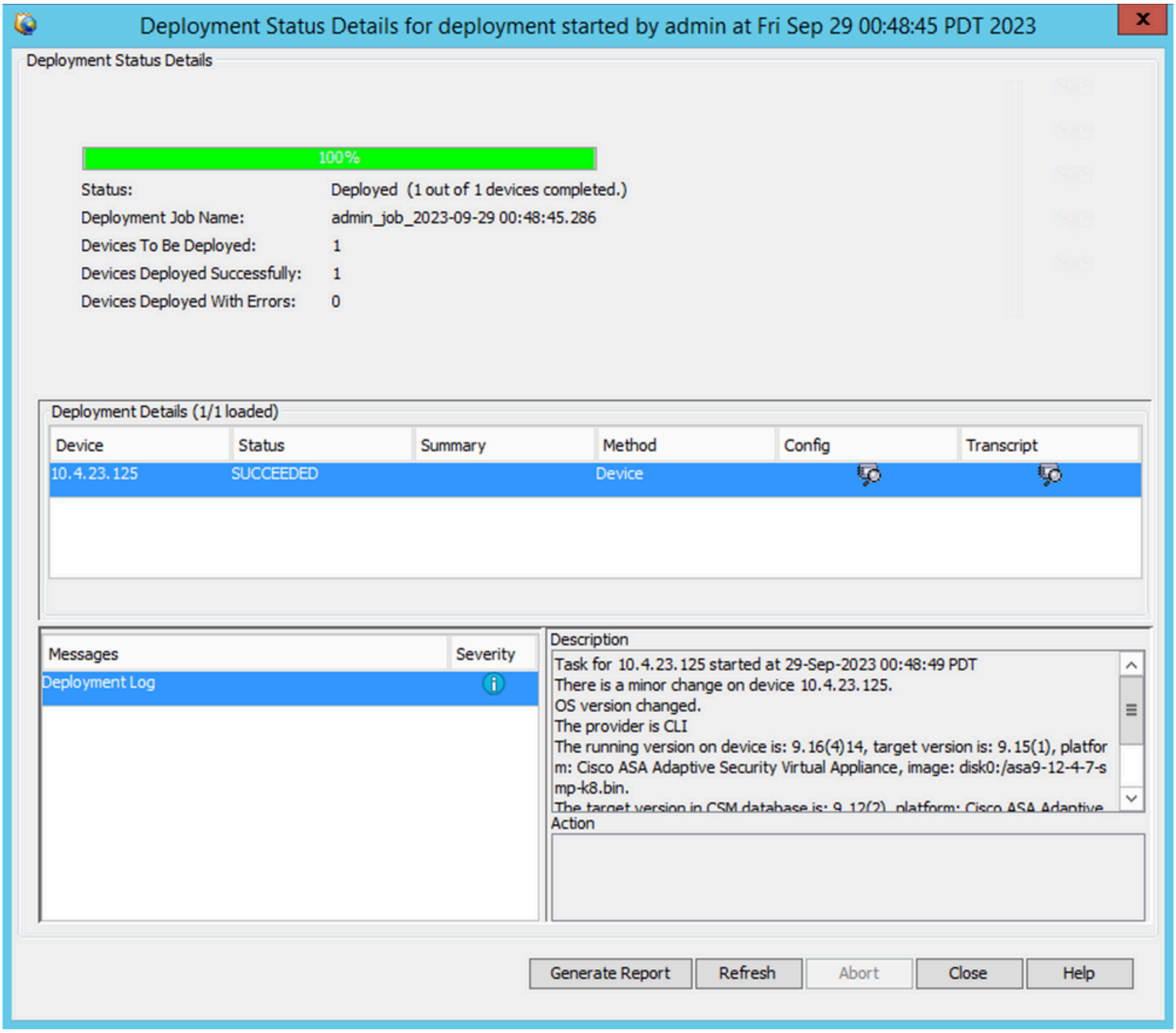
Device	Status	Summary	Method	Config	Transcript	Last Ticket(s)
10.4.23.125	Deploying		Device			admin_29.Sep.2023_(

Messages	Severity
--NO messages--	ⓘ

Description

Action

Step 5. (Optional) Once the deployment is accomplished, you can download the report or Transcript.


Deployment Status Details for deployment started by admin at Fri Sep 29 00:48:45 PDT 2023
Deployment Status Details
100%
Generate Report
Refresh
Abort
Close
Help

Status: Deployed (1 out of 1 devices completed.)
Deployment Job Name: admin_job_2023-09-29 00:48:45.286
Devices To Be Deployed: 1
Devices Deployed Successfully: 1
Devices Deployed With Errors: 0

Deployment Details (1/1 loaded)

Device	Status	Summary	Method	Config	Transcript
10.4.23.125	SUCCEEDED		Device		

Messages	Severity
Deployment Log	ⓘ

Description

```
Task for 10.4.23.125 started at 29-Sep-2023 00:48:49 PDT
There is a minor change on device 10.4.23.125.
OS version changed.
The provider is CLI
The running version on device is: 9.16(4)14, target version is: 9.15(1), platfor
m: Cisco ASA Adaptive Security Virtual Appliance, image: disk0:/asa9-12-4-7-s
mp-k8.bin.
The target version in CSM database is: 9.12(2), platform: Cisco ASA Adaptive
```

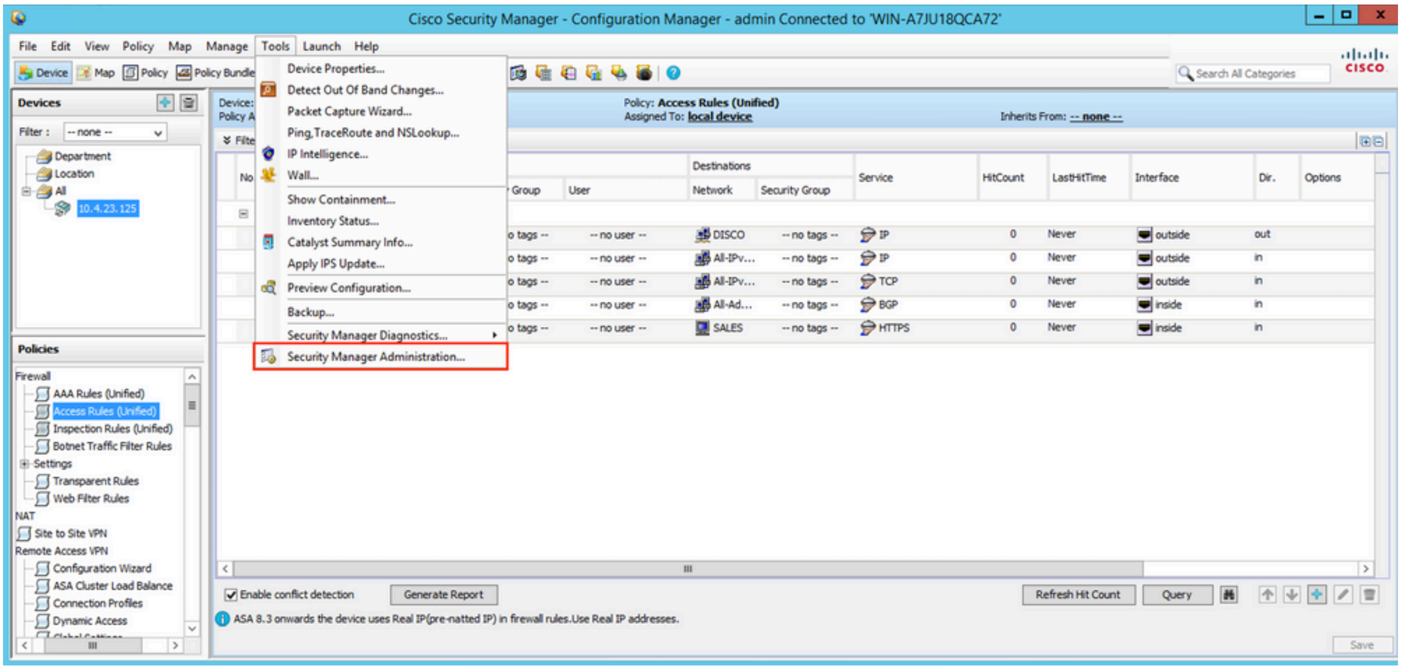
Action

Non-Workflow Mode with Ticket Management

Enable Ticket Management

In order to use the ticket base, it must be enabled. If you already have a ticket base flow enabled, skip this step.

Step 1. Navigate to Tools > Security Manager Administration.



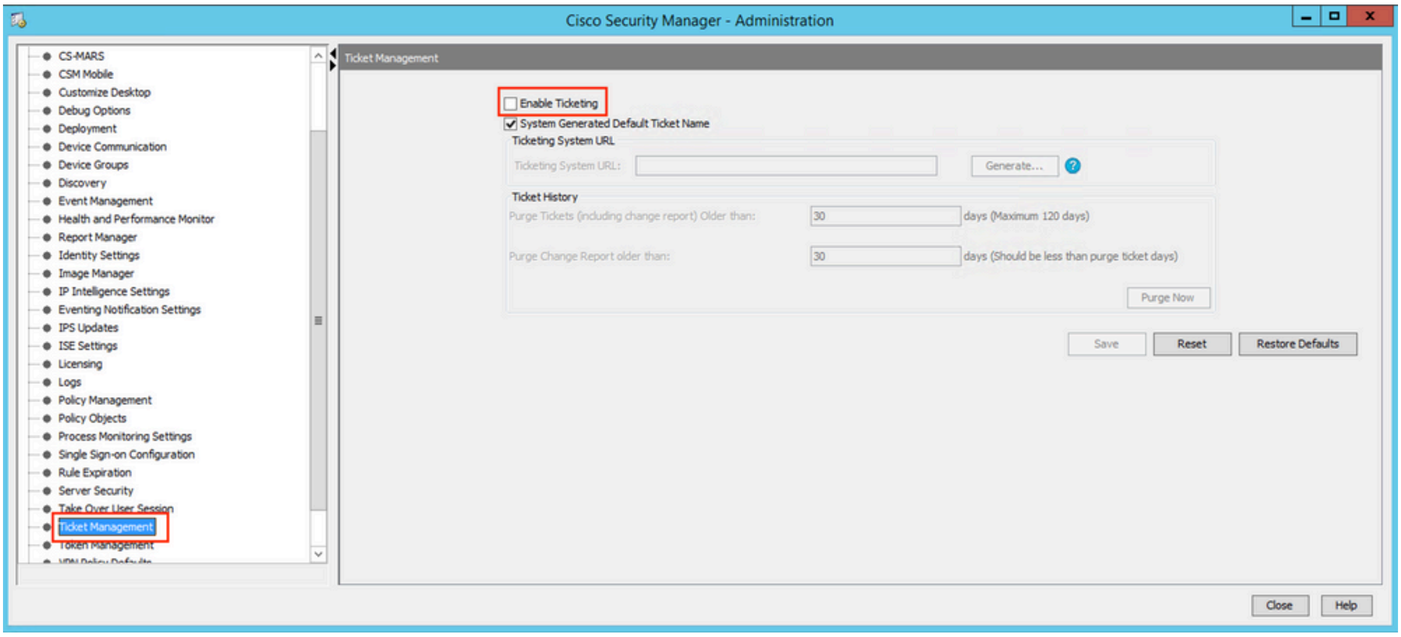
Policy: **Access Rules (Unified)**
Assigned To: **local device**
Inherits From: **-- none --**

No	Group	User	Destinations Network	Destinations Security Group	Service	HitCount	LastHitTime	Interface	Dir.	Options
	o tags --	-- no user --	DISCO	-- no tags --	IP	0	Never	outside	out	
	o tags --	-- no user --	All-IPv...	-- no tags --	IP	0	Never	outside	in	
	o tags --	-- no user --	All-IPv...	-- no tags --	TCP	0	Never	outside	in	
	o tags --	-- no user --	All-Ad...	-- no tags --	BGP	0	Never	inside	in	
	o tags --	-- no user --	SALES	-- no tags --	HTTPS	0	Never	inside	in	

☑ Enable conflict detection

ASA 8.3 onwards the device uses Real IP(pre-natted IP) in firewall rules.Use Real IP addresses.

Step 2. Navigate to **Ticket Management** and check the option **Enable Ticketing**.

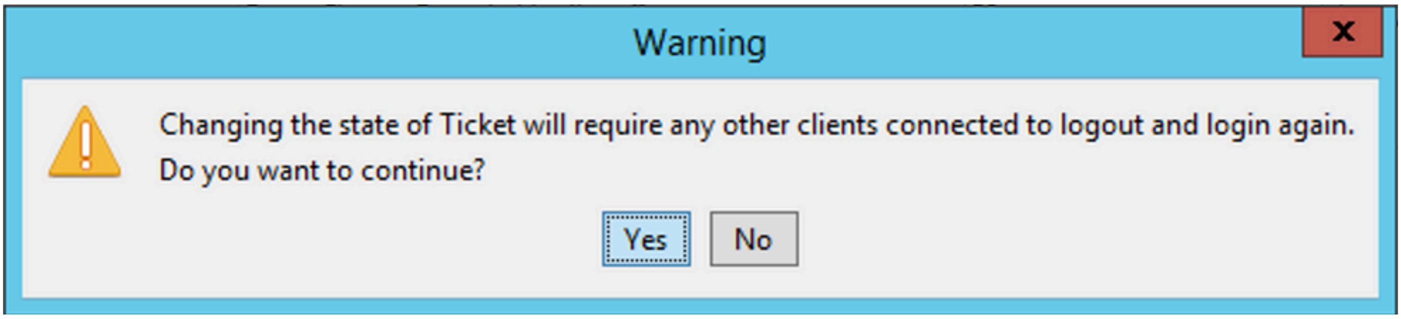


☐ Enable Ticketing
☑ System Generated Default Ticket Name

Ticketing System URL
Ticketing System URL:

Ticket History
Purge Tickets (including change report) Older than: 30 days (Maximum 120 days)
Purge Change Report older than: 30 days (Should be less than purge ticket days)

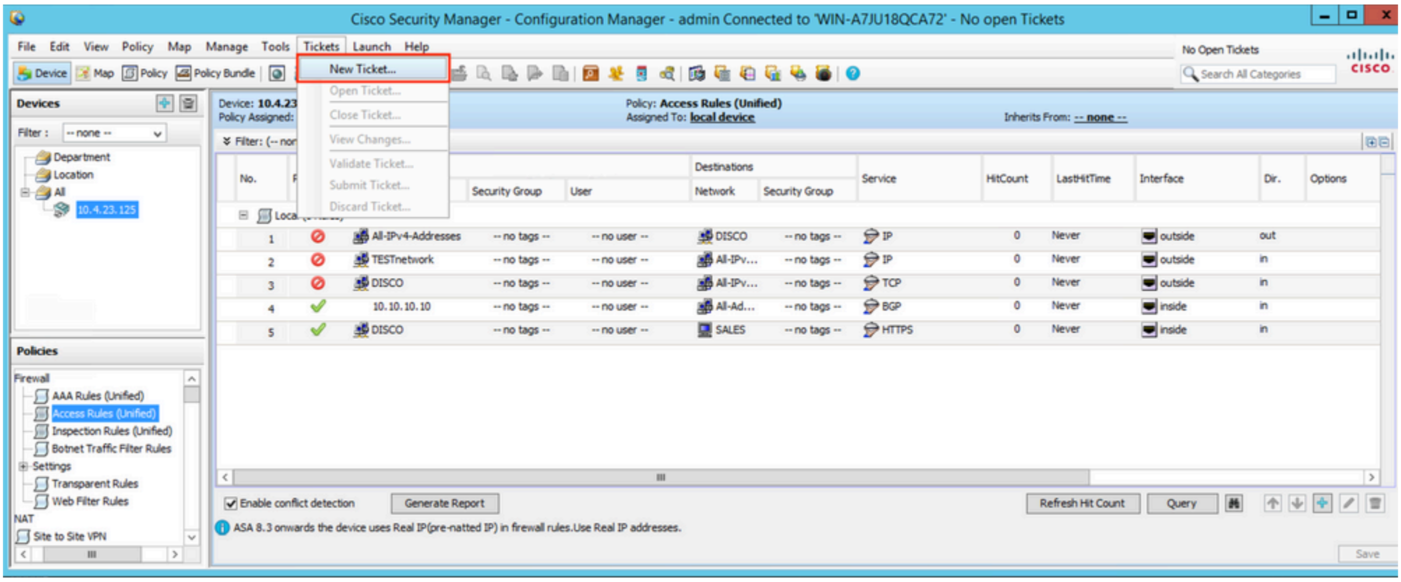
Step 3. Click **yes** in order to confirm that you understand the warning and want to proceed.



Changing the state of Ticket will require any other clients connected to logout and login again.
Do you want to continue?

Deployment with Non-Workflow Mode with Ticket Management

Step 1. Open a new ticket by navigating to **Ticket** > **New ticket.**



Device: 10.4.23
Policy Assigned:

Policy: Access Rules (Unified)
Assigned To: local device

Inherits From: -- none --

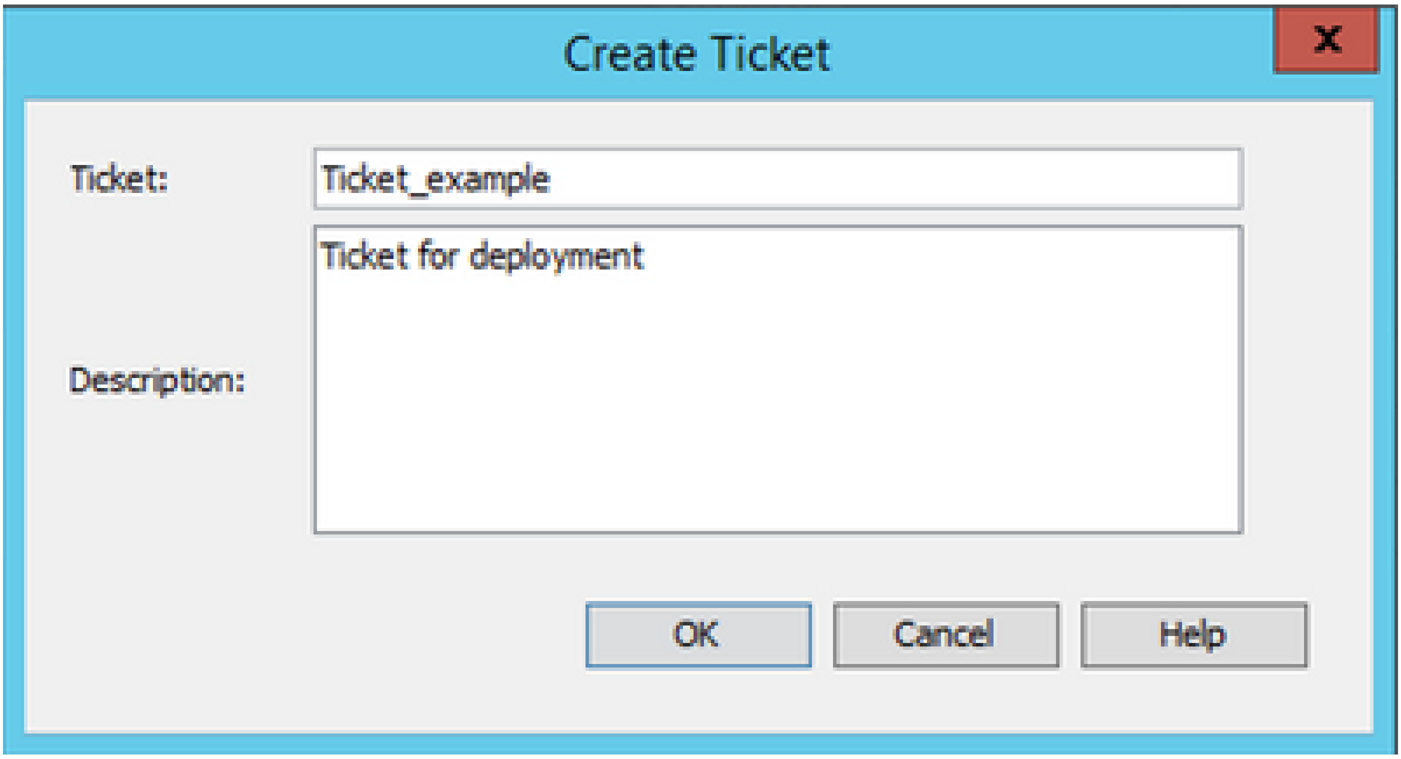
Filter: (-- non

				Destinations							
No.			Security Group	User	Network	Security Group	Service	HitCount	LastHitTime	Interface	Dir.	Options
1	🚫	All-IPv4-Addresses	-- no tags --	-- no user --	DISCO	-- no tags --	IP	0	Never	outside	out	
2	🚫	TESTnetwork	-- no tags --	-- no user --	All-IPv...	-- no tags --	IP	0	Never	outside	in	
3	🚫	DISCO	-- no tags --	-- no user --	All-IPv...	-- no tags --	TCP	0	Never	outside	in	
4	✓	10.10.10.10	-- no tags --	-- no user --	All-Ad...	-- no tags --	BGP	0	Never	inside	in	
5	✓	DISCO	-- no tags --	-- no user --	SALES	-- no tags --	HTTPS	0	Never	inside	in	

☑ Enable conflict detection

ASA 8.3 onwards the device uses Real IP(pre-natted IP) in firewall rules.Use Real IP addresses.

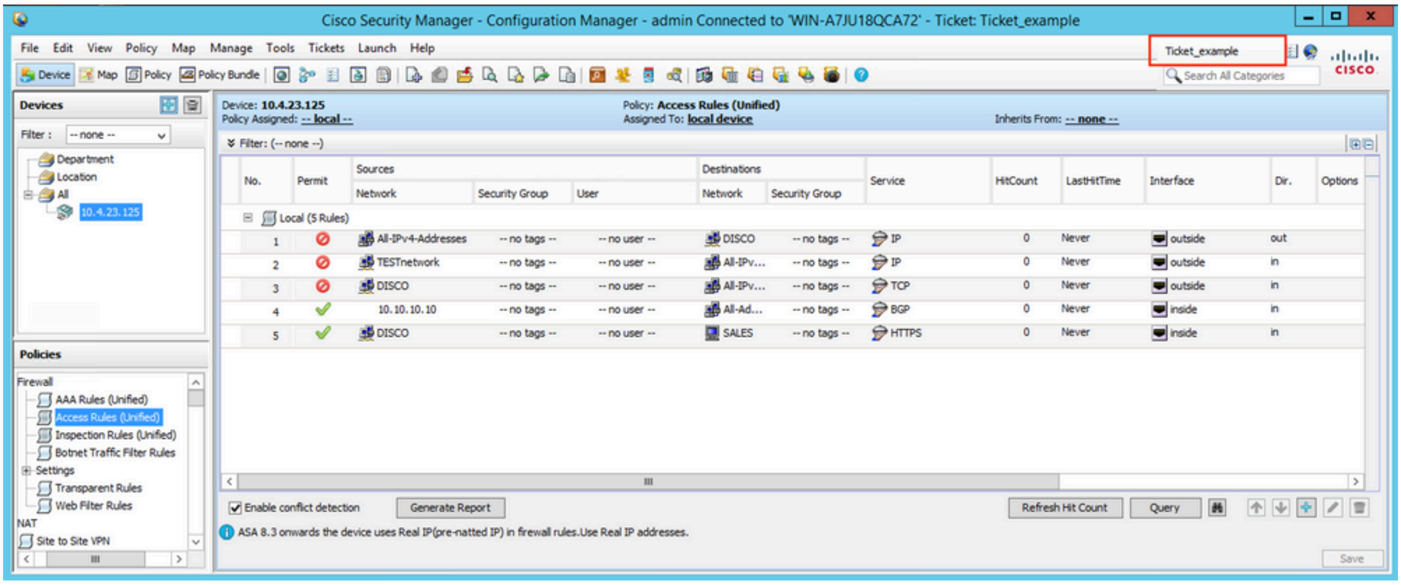
Step 2. Name the new ticket and add a description.



Ticket: Ticket_example

Description: Ticket for deployment

Tip: You can verify the new ticket is open and the current ticket in use, at the top right of the screen.



Cisco Security Manager - Configuration Manager - admin Connected to 'WIN-A7JU18QCA72' - Ticket: Ticket_example

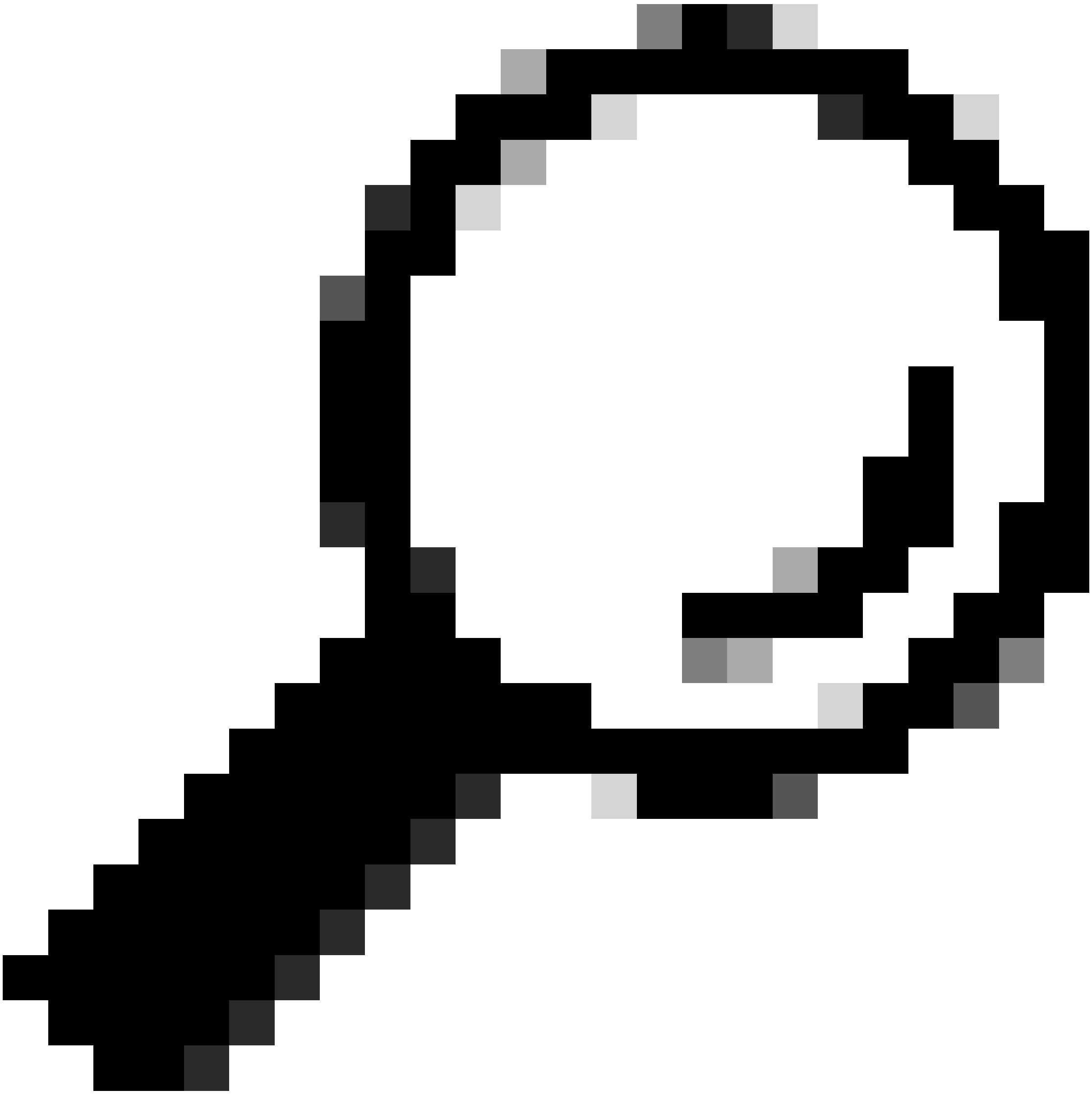
Device: **10.4.23.125**
Policy Assigned: **-- local --**
Policy: **Access Rules (Unified)**
Assigned To: **local device**
Inherits From: **-- none --**

Filter: (-- none --)

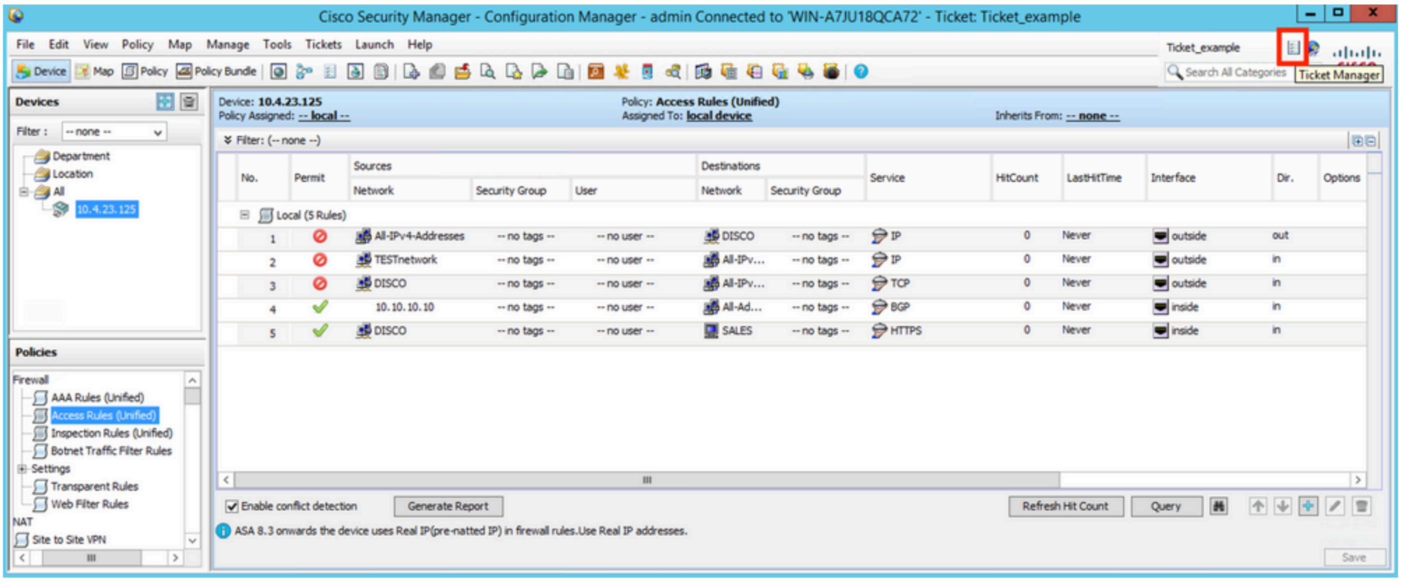
No.	Permit	Sources			Destinations		Service	HitCount	LastHitTime	Interface	Dir.	Options
		Network	Security Group	User	Network	Security Group						
Local (5 Rules)												
1	⊘	All-IPv4-Addresses	-- no tags --	-- no user --	DISCO	-- no tags --	IP	0	Never	outside	out	
2	⊘	TESTnetwork	-- no tags --	-- no user --	All-IPv...	-- no tags --	IP	0	Never	outside	in	
3	⊘	DISCO	-- no tags --	-- no user --	All-IPv...	-- no tags --	TCP	0	Never	outside	in	
4	✓	10.10.10.10	-- no tags --	-- no user --	All-Ad...	-- no tags --	BGP	0	Never	inside	in	
5	✓	DISCO	-- no tags --	-- no user --	SALES	-- no tags --	HTTPS	0	Never	inside	in	

☑ Enable conflict detection

ASA 8.3 onwards the device uses Real IP(pre-natted IP) in firewall rules.Use Real IP addresses.



Tip: Alternatively you can use Ticket Manager in order to Create, Submit, and Discard tickets by clicking on the top right button.



Cisco Security Manager - Configuration Manager - admin Connected to 'WIN-A7JU18QCA72' - Ticket: Ticket_example

Device: 10.4.23.125
Policy Assigned: -- local --
Policy: Access Rules (Unified)
Assigned To: local device
Inherits From: -- none --

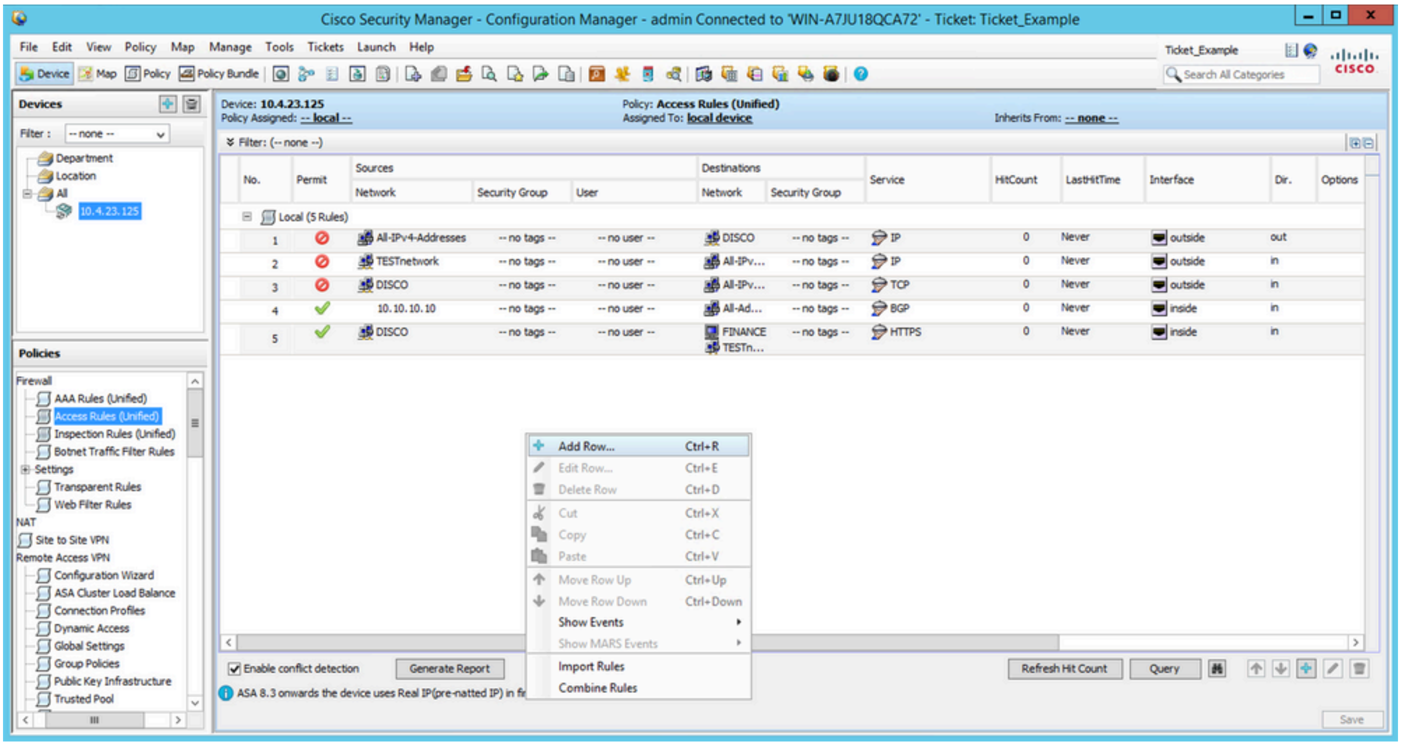
Filter: (-- none --)

No.	Permit	Sources			Destinations		Service	HitCount	LastHitTime	Interface	Dir.	Options
		Network	Security Group	User	Network	Security Group						
Local (5 Rules)												
1	⊘	All-IPv4-Addresses	-- no tags --	-- no user --	DISCO	-- no tags --	IP	0	Never	outside	out	
2	⊘	TESTnetwork	-- no tags --	-- no user --	All-IPv...	-- no tags --	IP	0	Never	outside	in	
3	⊘	DISCO	-- no tags --	-- no user --	All-IPv...	-- no tags --	TCP	0	Never	outside	in	
4	✓	10.10.10.10	-- no tags --	-- no user --	All-Ad...	-- no tags --	BGP	0	Never	inside	in	
5	✓	DISCO	-- no tags --	-- no user --	SALES	-- no tags --	HTTPS	0	Never	inside	in	

☑ Enable conflict detection

ASA 8.3 onwards the device uses Real IP(pre-natted IP) in firewall rules.Use Real IP addresses.

Step 3. Make necessary changes to the configuration and save.



Cisco Security Manager - Configuration Manager - admin Connected to 'WIN-A7JU18QCA72' - Ticket: Ticket_Example

Device: 10.4.23.125
Policy Assigned: -- local --
Policy: Access Rules (Unified)
Assigned To: local device
Inherits From: -- none --

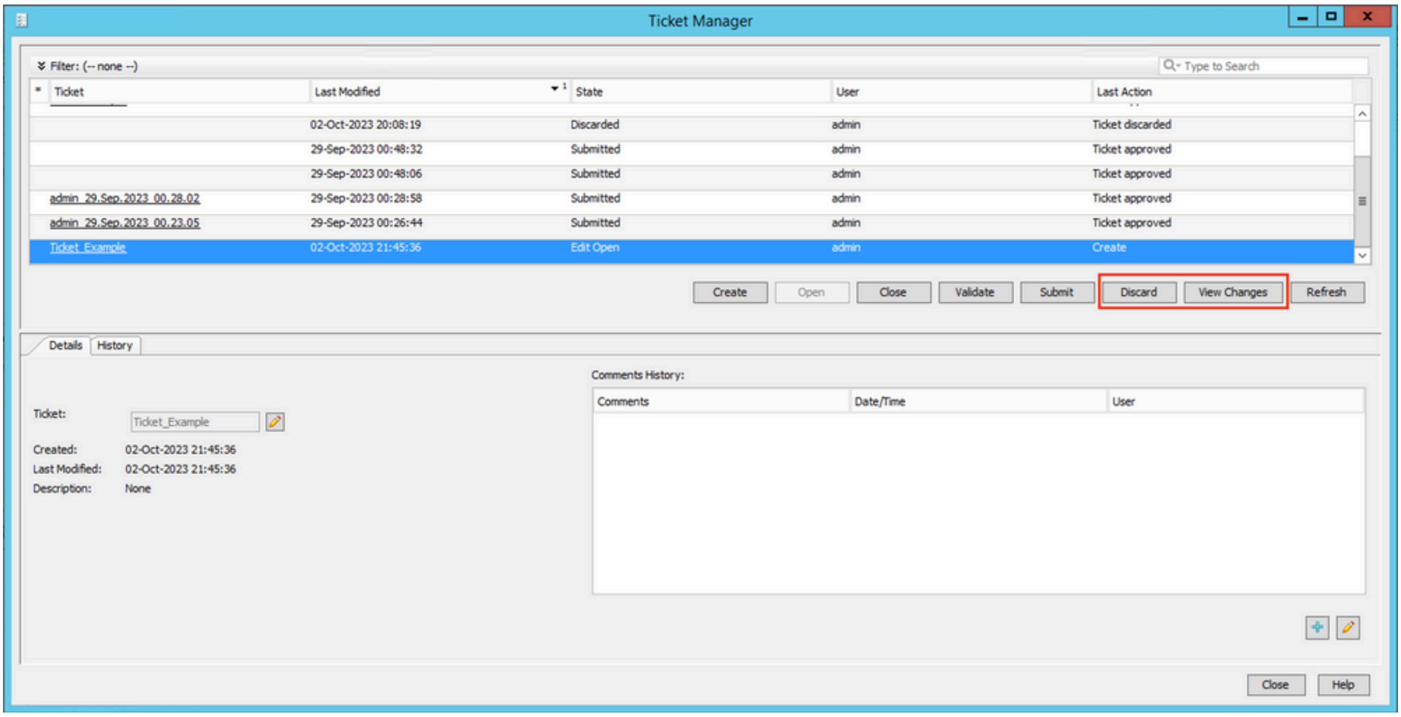
Filter: (-- none --)

No.	Permit	Sources			Destinations		Service	HitCount	LastHitTime	Interface	Dir.	Options
		Network	Security Group	User	Network	Security Group						
Local (5 Rules)												
1	⊘	All-IPv4-Addresses	-- no tags --	-- no user --	DISCO	-- no tags --	IP	0	Never	outside	out	
2	⊘	TESTnetwork	-- no tags --	-- no user --	All-IPv...	-- no tags --	IP	0	Never	outside	in	
3	⊘	DISCO	-- no tags --	-- no user --	All-IPv...	-- no tags --	TCP	0	Never	outside	in	
4	✓	10.10.10.10	-- no tags --	-- no user --	All-Ad...	-- no tags --	BGP	0	Never	inside	in	
5	✓	DISCO	-- no tags --	-- no user --	FINANCE TESTn...	-- no tags --	HTTPS	0	Never	inside	in	

☑ Enable conflict detection

ASA 8.3 onwards the device uses Real IP(pre-natted IP) in fi

Step 4. (Optional) You can Discard or View Changes.



Ticket	Last Modified	State	User	Last Action
	02-Oct-2023 20:08:19	Discarded	admin	Ticket discarded
	29-Sep-2023 00:48:32	Submitted	admin	Ticket approved
	29-Sep-2023 00:48:06	Submitted	admin	Ticket approved
admin_29.Sep.2023_00.28.02	29-Sep-2023 00:28:58	Submitted	admin	Ticket approved
admin_29.Sep.2023_00.23.05	29-Sep-2023 00:26:44	Submitted	admin	Ticket approved
Ticket_Example	02-Oct-2023 21:45:36	Edit Open	admin	Create

Ticket: Ticket_Example

Created: 02-Oct-2023 21:45:36

Last Modified: 02-Oct-2023 21:45:36

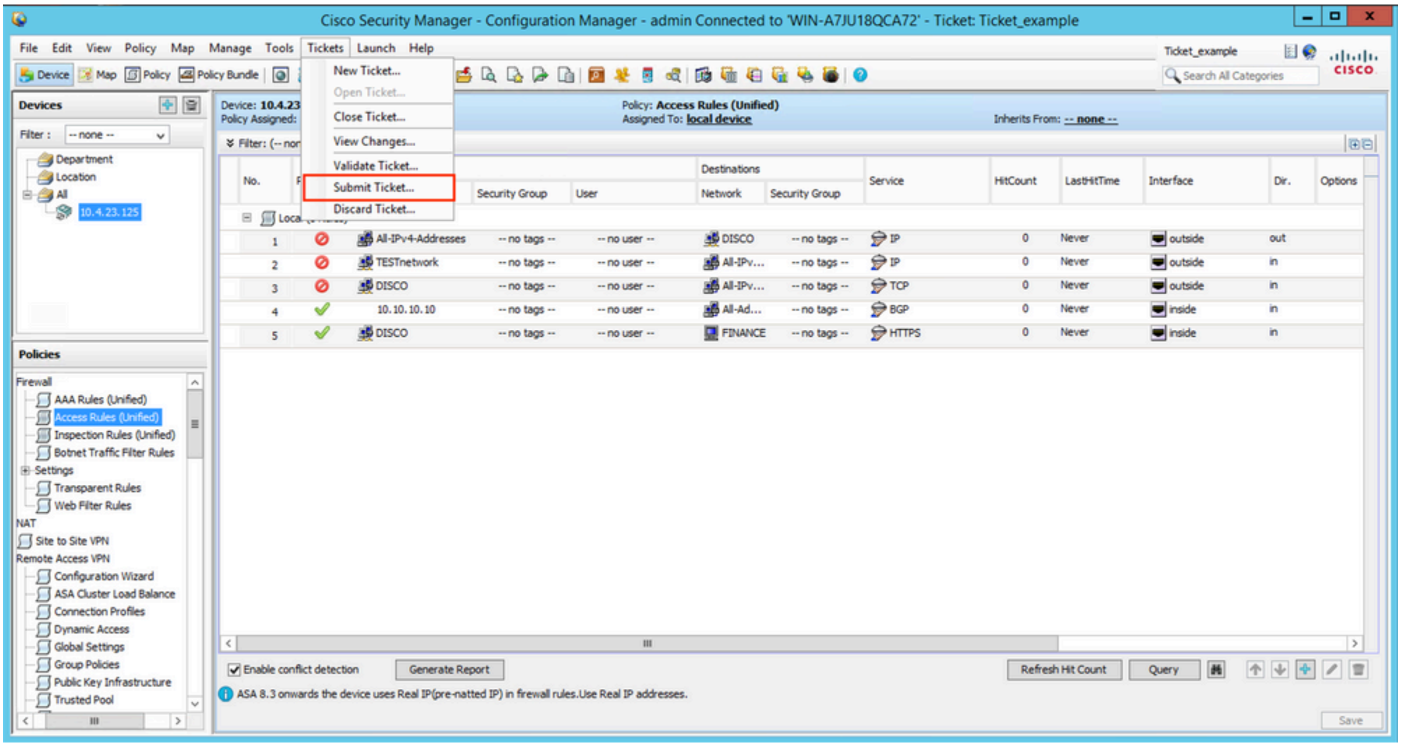
Description: None

Comments History:

Comments	Date/Time	User

Caution: Discarding a Ticket undoes all configuration changes made on the ticket.

Step 5. Submit the ticket once configuration changes have been approved and validations have been done.



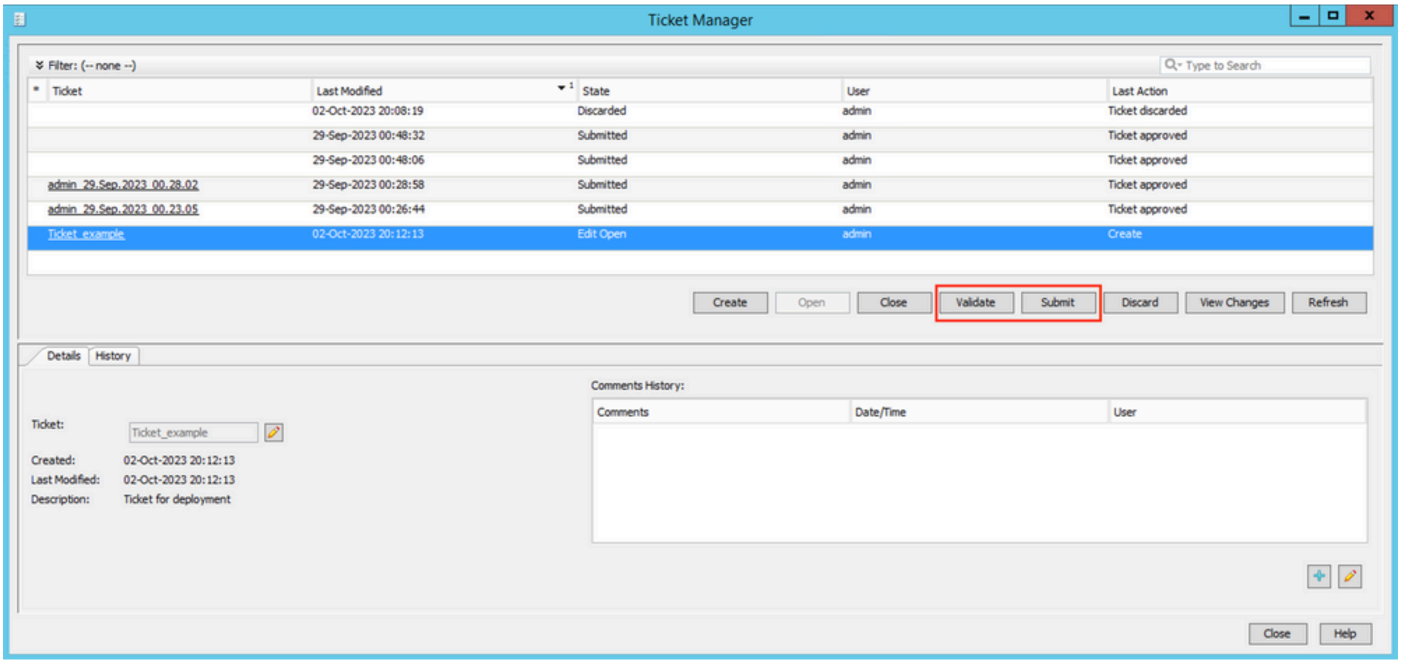
Device: 10.4.23
Policy Assigned:

Policy: Access Rules (Unified)
Assigned To: local device
Inherits From: -- none --

No.					Destinations							
			Security Group	User	Network	Security Group	Service	HitCount	LastHitTime	Interface	Dir.	Options
1	⊘	All-IPv4-Addresses	-- no tags --	-- no user --	DISCO	-- no tags --	IP	0	Never	outside	out	
2	⊘	TESTnetwork	-- no tags --	-- no user --	All-IPv...	-- no tags --	IP	0	Never	outside	in	
3	⊘	DISCO	-- no tags --	-- no user --	All-IPv...	-- no tags --	TCP	0	Never	outside	in	
4	✓	10.10.10.10	-- no tags --	-- no user --	All-Ad...	-- no tags --	BGP	0	Never	inside	in	
5	✓	DISCO	-- no tags --	-- no user --	FINANCE	-- no tags --	HTTPS	0	Never	inside	in	

ASA 8.3 onwards the device uses Real IP(pre-natted IP) in firewall rules.Use Real IP addresses.

Tip: Validation and submission of tickets can also be done by the Ticket Manager.



*	Ticket	Last Modified	State	User	Last Action
		02-Oct-2023 20:08:19	Discarded	admin	Ticket discarded
		29-Sep-2023 00:48:32	Submitted	admin	Ticket approved
		29-Sep-2023 00:48:06	Submitted	admin	Ticket approved
	admin_29.Sep.2023_00.28.02	29-Sep-2023 00:28:58	Submitted	admin	Ticket approved
	admin_29.Sep.2023_00.23.05	29-Sep-2023 00:26:44	Submitted	admin	Ticket approved
	Ticket_example	02-Oct-2023 20:12:13	Edit Open	admin	Create

Ticket: Ticket_example

Created: 02-Oct-2023 20:12:13

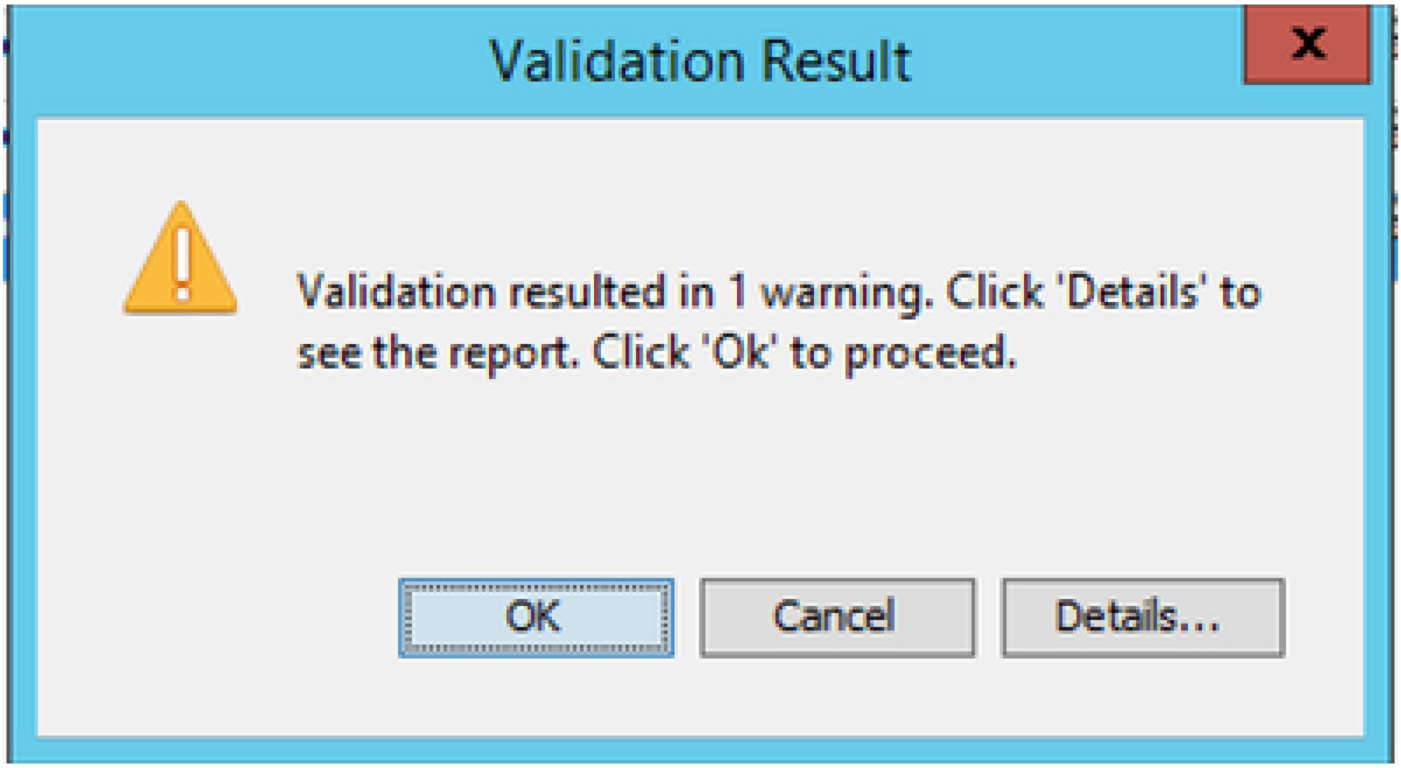
Last Modified: 02-Oct-2023 20:12:13

Description: Ticket for deployment

Comments History:

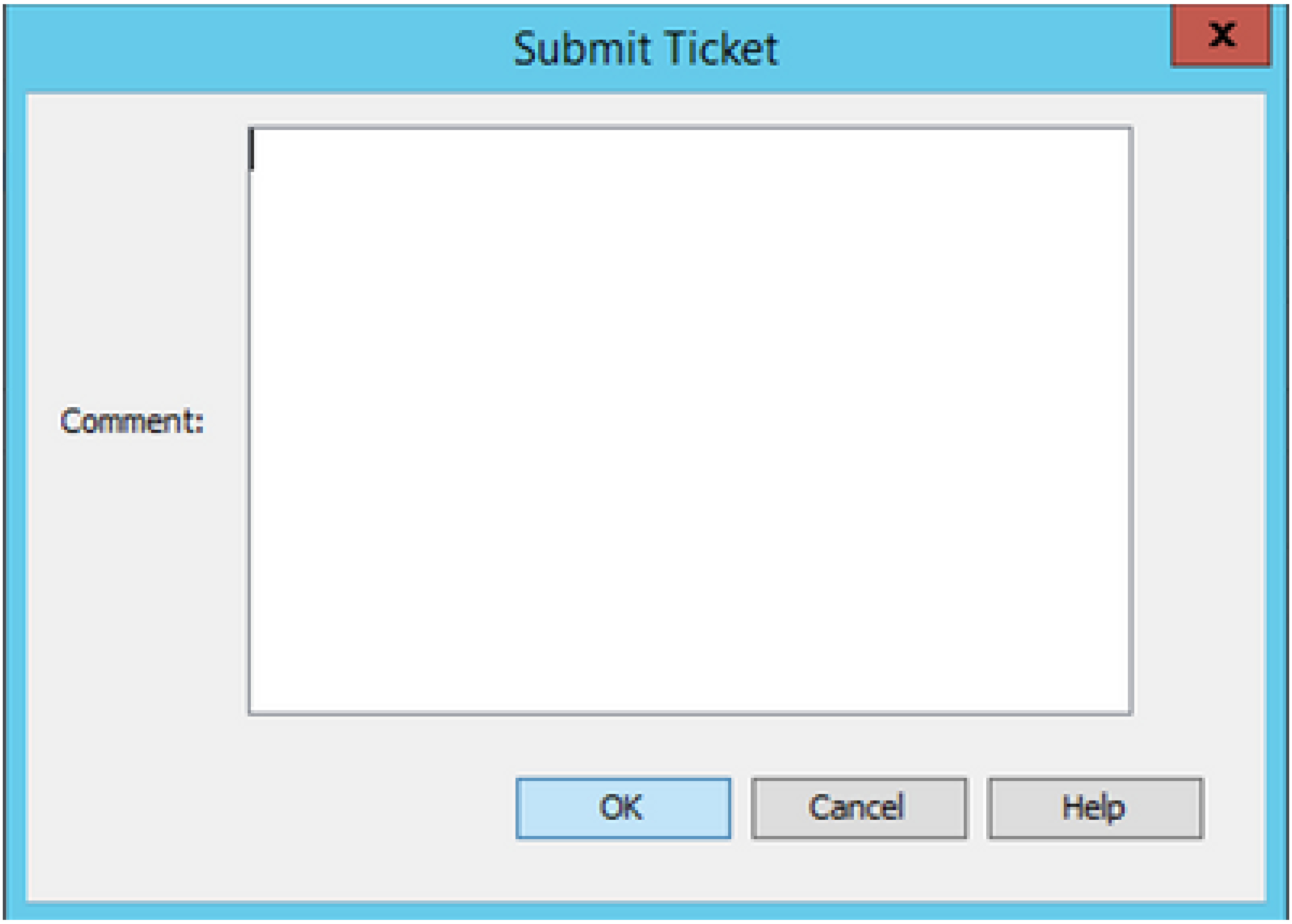
Comments	Date/Time	User

Step 6. Click OK when validations have been reviewed.



Validation resulted in 1 warning. Click 'Details' to see the report. Click 'Ok' to proceed.

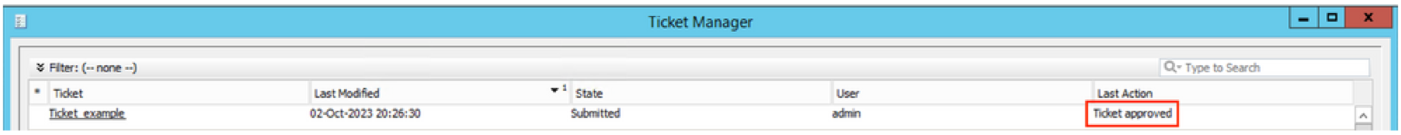
Step 7. Submit ticket.



Submit Ticket
x
Comment:
OK
Cancel
Help

Tip: You can leave a comment when submitting a ticket.

Step 8. Review the status of the ticket and ensure that it was successfully approved before proceeding with deployment.

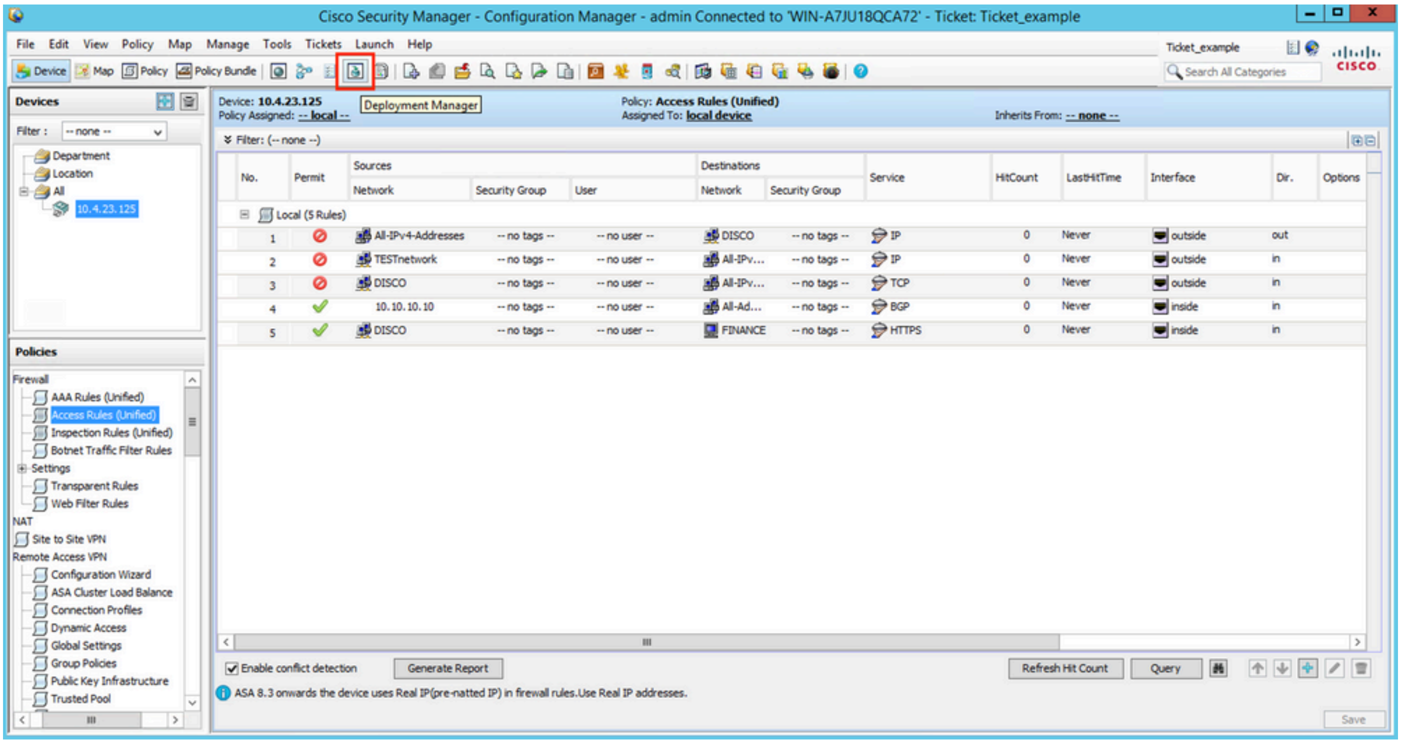


Ticket Manager

Filter: (-- none --)

Ticket	Last Modified	State	User	Last Action
Ticket_example	02-Oct-2023 20:26:30	Submitted	admin	Ticket approved

Step 9. Navigate to **Deployment Manager**.



Cisco Security Manager - Configuration Manager - admin Connected to 'WIN-A7JU18QCA72' - Ticket: Ticket_example

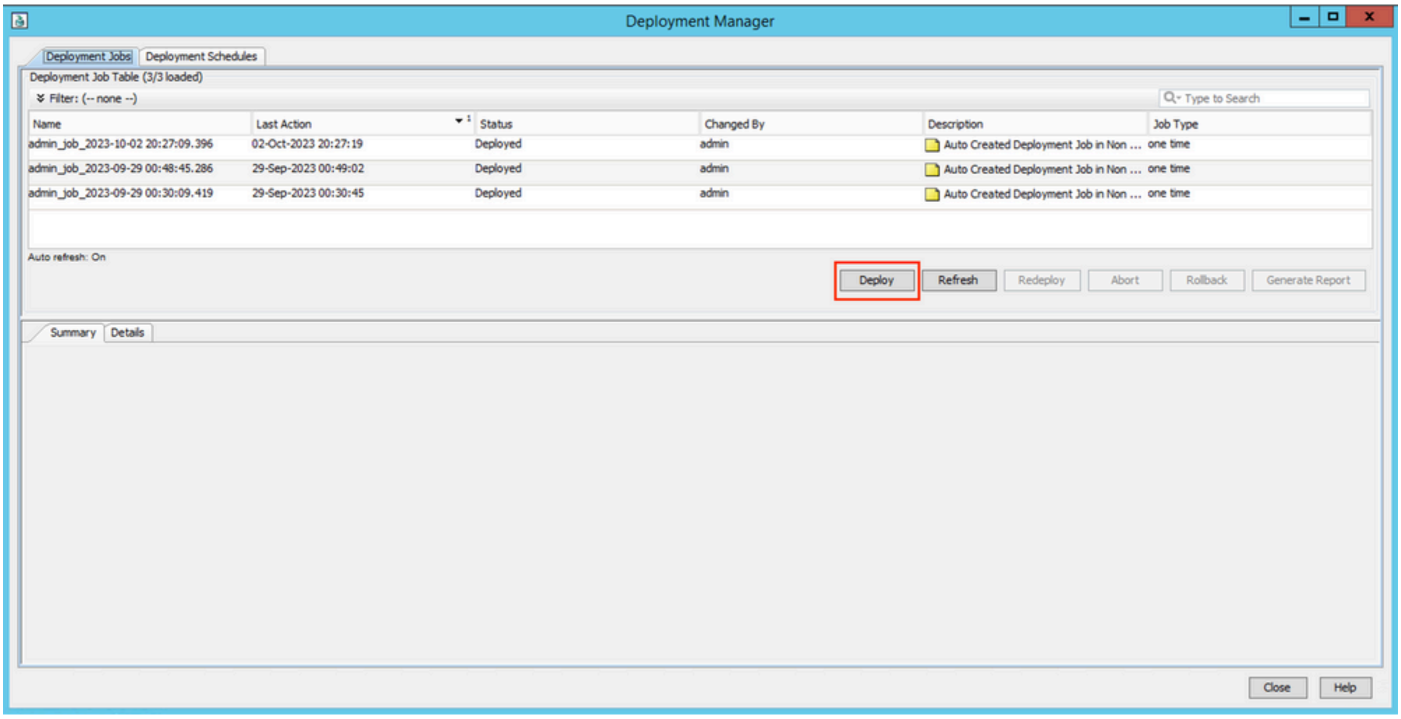
Device: 10.4.23.125
Policy Assigned: -- local --
Policy: Access Rules (Unified)
Assigned To: local device
Inherits From: -- none --
Filter: (-- none --)

No.	Permit	Sources			Destinations		Service	HitCount	LastHitTime	Interface	Dir.	Options
		Network	Security Group	User	Network	Security Group						
Local (5 Rules)												
1	⊘	All-IPv4-Addresses	-- no tags --	-- no user --	DISCO	-- no tags --	IP	0	Never	outside	out	
2	⊘	TESTnetwork	-- no tags --	-- no user --	All-IPv...	-- no tags --	IP	0	Never	outside	in	
3	⊘	DISCO	-- no tags --	-- no user --	All-IPv...	-- no tags --	TCP	0	Never	outside	in	
4	✓	10.10.10.10	-- no tags --	-- no user --	All-Ad...	-- no tags --	BGP	0	Never	inside	in	
5	✓	DISCO	-- no tags --	-- no user --	FINANCE	-- no tags --	HTTPS	0	Never	inside	in	

☑ Enable conflict detection

ASA 8.3 onwards the device uses Real IP(pre-natted IP) in firewall rules.Use Real IP addresses.

Step 10. Click **Deploy** when you are ready to push configuration changes.



Deployment Manager

Deployment Jobs | Deployment Schedules

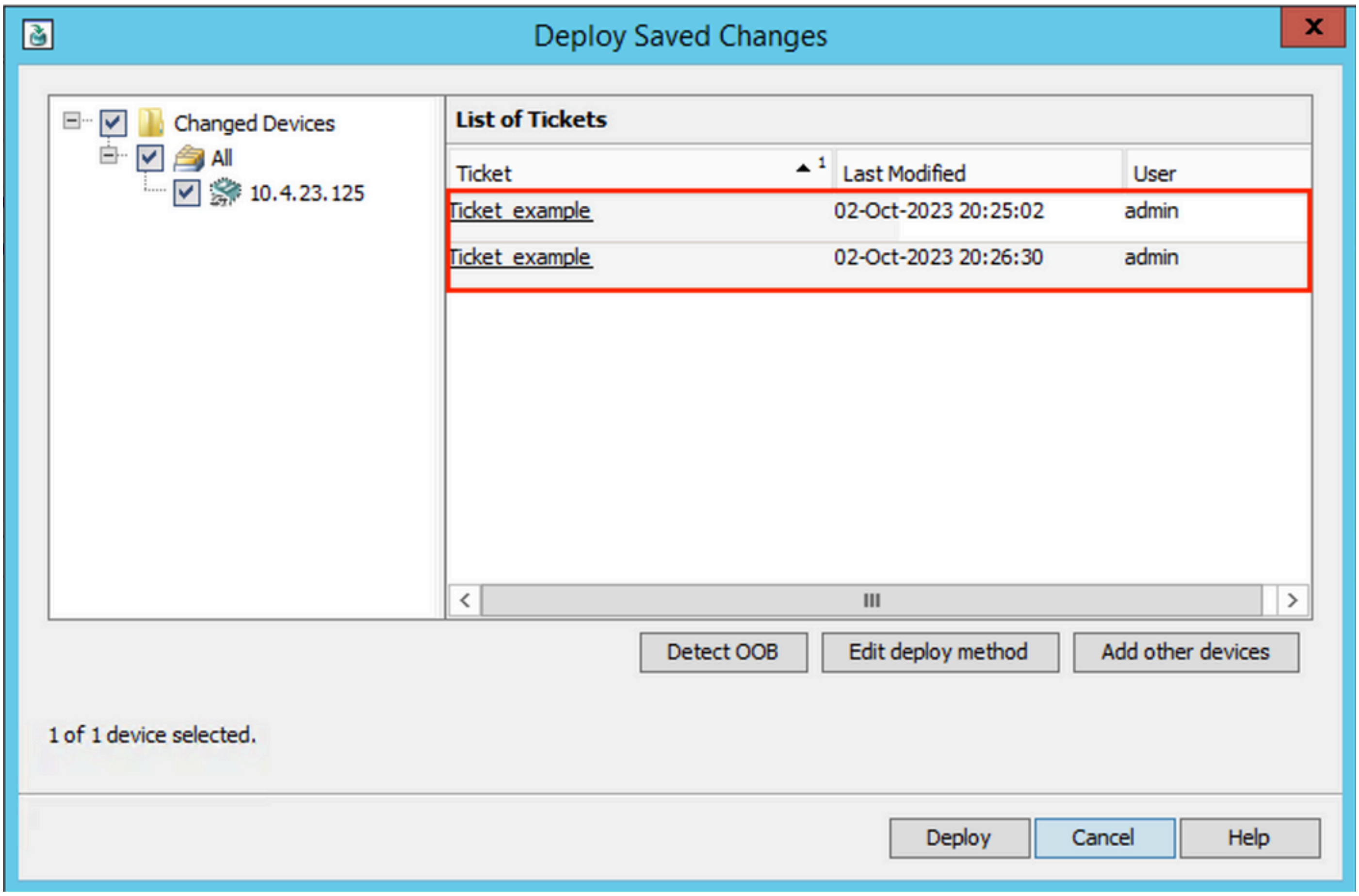
Deployment Job Table (3/3 loaded)

Filter: (-- none --)

Name	Last Action	Status	Changed By	Description	Job Type
admin_job_2023-10-02 20:27:09.396	02-Oct-2023 20:27:19	Deployed	admin	Auto Created Deployment Job in Non ...	one time
admin_job_2023-09-29 00:48:45.286	29-Sep-2023 00:49:02	Deployed	admin	Auto Created Deployment Job in Non ...	one time
admin_job_2023-09-29 00:30:09.419	29-Sep-2023 00:30:45	Deployed	admin	Auto Created Deployment Job in Non ...	one time

Auto refresh: On

Step 11. The deployment window shows Tickets to deploy and to what devices it is targeting. Once the information has been reviewed, click **Deploy**.

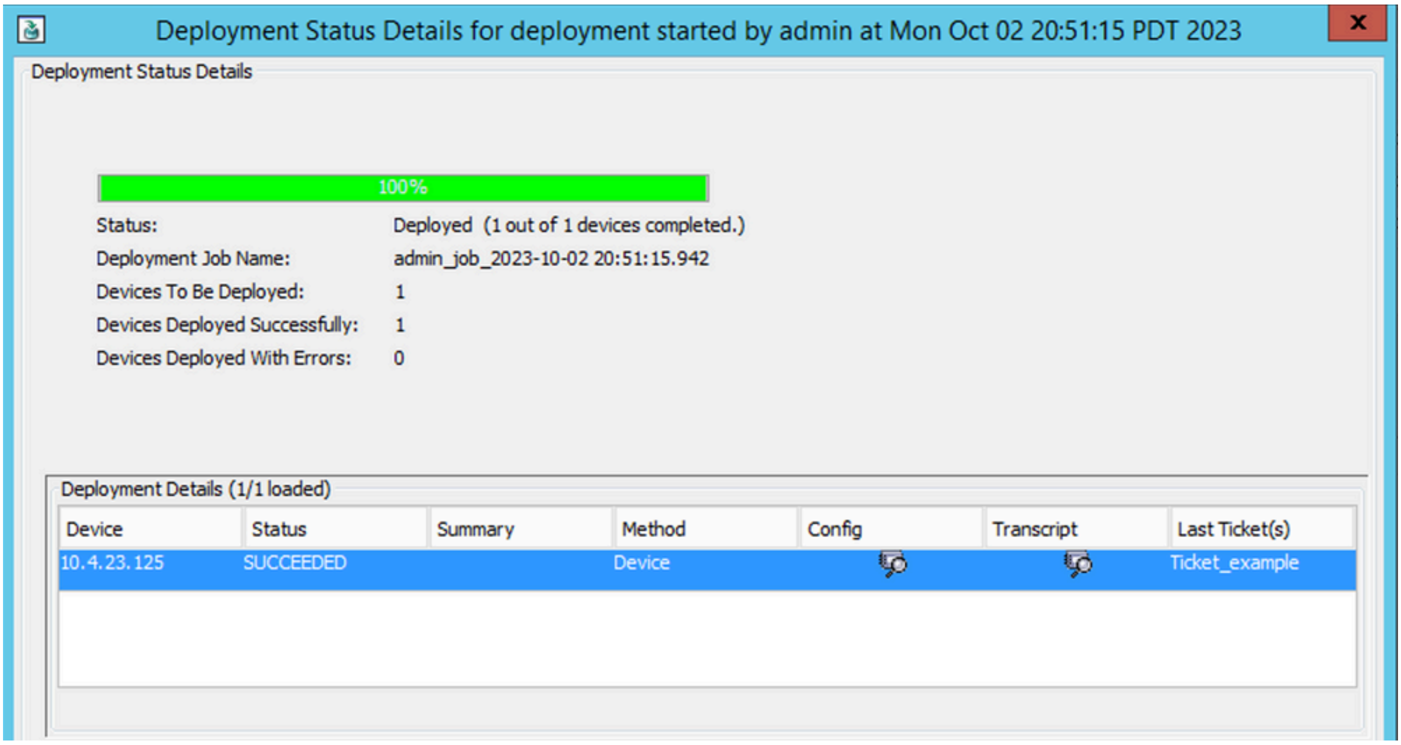


List of Tickets

Ticket	Last Modified	User
Ticket_example	02-Oct-2023 20:25:02	admin
Ticket_example	02-Oct-2023 20:26:30	admin

1 of 1 device selected.

Step 12. Monitor deployment and review the final status.



Deployment Status Details for deployment started by admin at Mon Oct 02 20:51:15 PDT 2023
Deployment Status Details
100%

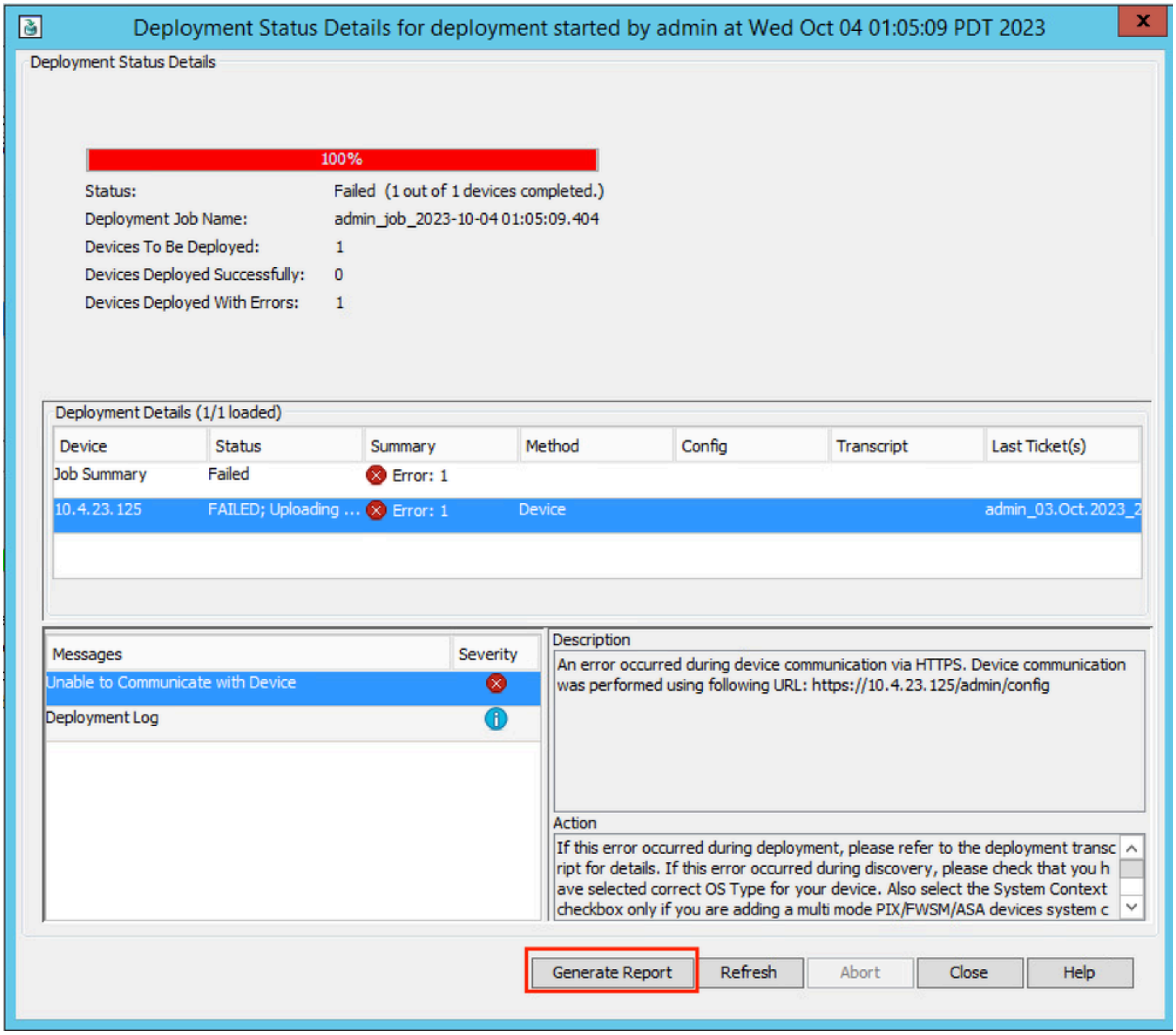
Status: Deployed (1 out of 1 devices completed.)
Deployment Job Name: admin_job_2023-10-02 20:51:15.942
Devices To Be Deployed: 1
Devices Deployed Successfully: 1
Devices Deployed With Errors: 0

Deployment Details (1/1 loaded)

Device	Status	Summary	Method	Config	Transcript	Last Ticket(s)
10.4.23.125	SUCCEEDED		Device			Ticket_example

Troubleshoot

In case the deployment fails, it can be useful to review the report of the deployment. You can generate it by clicking **Generate Report** when the deployment has finished.



Deployment Status Details for deployment started by admin at Wed Oct 04 01:05:09 PDT 2023

Deployment Status Details

Status:	Failed (1 out of 1 devices completed.)
Deployment Job Name:	admin_job_2023-10-04 01:05:09.404
Devices To Be Deployed:	1
Devices Deployed Successfully:	0
Devices Deployed With Errors:	1

Deployment Details (1/1 loaded)

Device	Status	Summary	Method	Config	Transcript	Last Ticket(s)
Job Summary	Failed	☒ Error: 1				
10.4.23.125	FAILED; Uploading ...	☒ Error: 1	Device			admin_03.Oct.2023_2

Messages	Severity
Unable to Communicate with Device	☒
Deployment Log	ⓘ

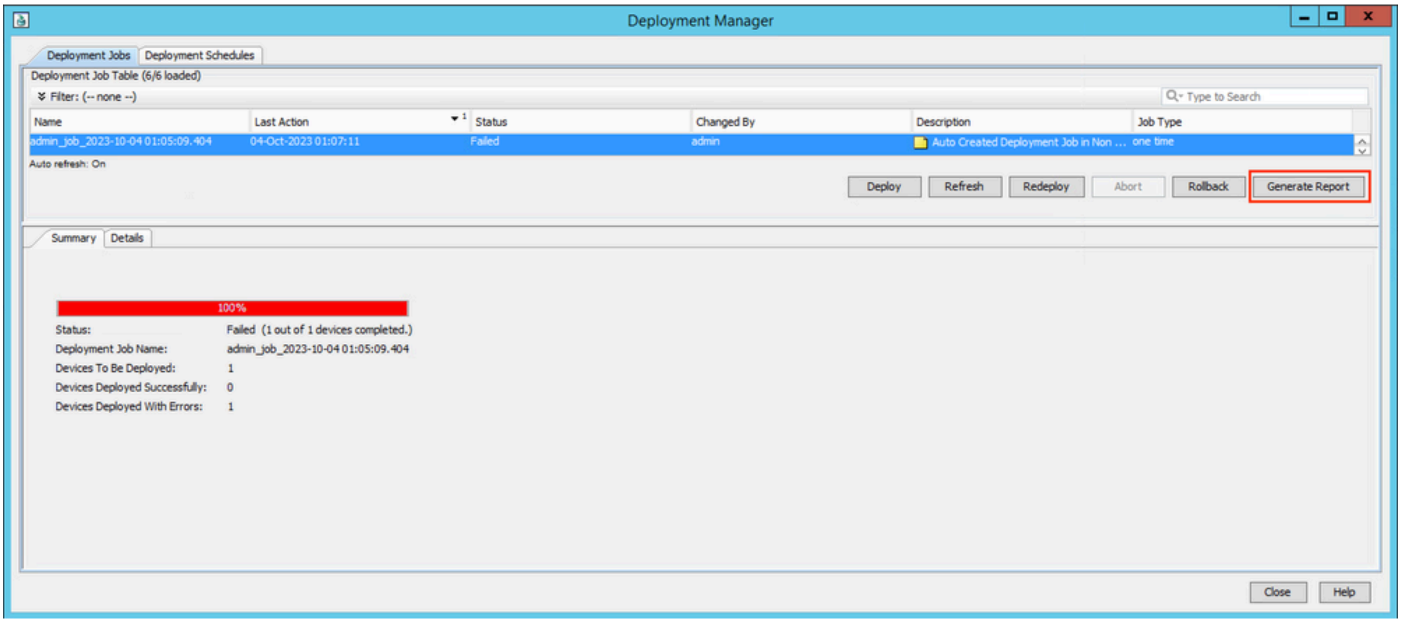
Description

An error occurred during device communication via HTTPS. Device communication was performed using following URL: https://10.4.23.125/admin/config

Action

If this error occurred during deployment, please refer to the deployment transcript for details. If this error occurred during discovery, please check that you have selected correct OS Type for your device. Also select the System Context checkbox only if you are adding a multi mode PIX/FWSM/ASA devices system c

Alternatively, you can navigate to **Deployment Manager**, choose the deployment, and click **Generate Report**.



Deployment Manager

Deployment Job Table (6/6 loaded)

Filter: (-- none --)

Name	Last Action	Status	Changed By	Description	Job Type
admin_job_2023-10-04 01:05:09.404	04-Oct-2023 01:07:11	Failed	admin	Auto Created Deployment Job in Non ...	one time

Auto refresh: On

Status:	Failed (1 out of 1 devices completed.)
Deployment Job Name:	admin_job_2023-10-04 01:05:09.404
Devices To Be Deployed:	1
Devices Deployed Successfully:	0
Devices Deployed With Errors:	1