Configure RADIUS External Authentication on DNA Center and ISE 3.1

Contents

Introduction

This document describes how to configure RADIUS External Authentication on Cisco DNA Center using a Cisco ISE server running 3.1 release.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco DNA Center and Cisco ISE already integrated and integration is on Active Status.

Components Used

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

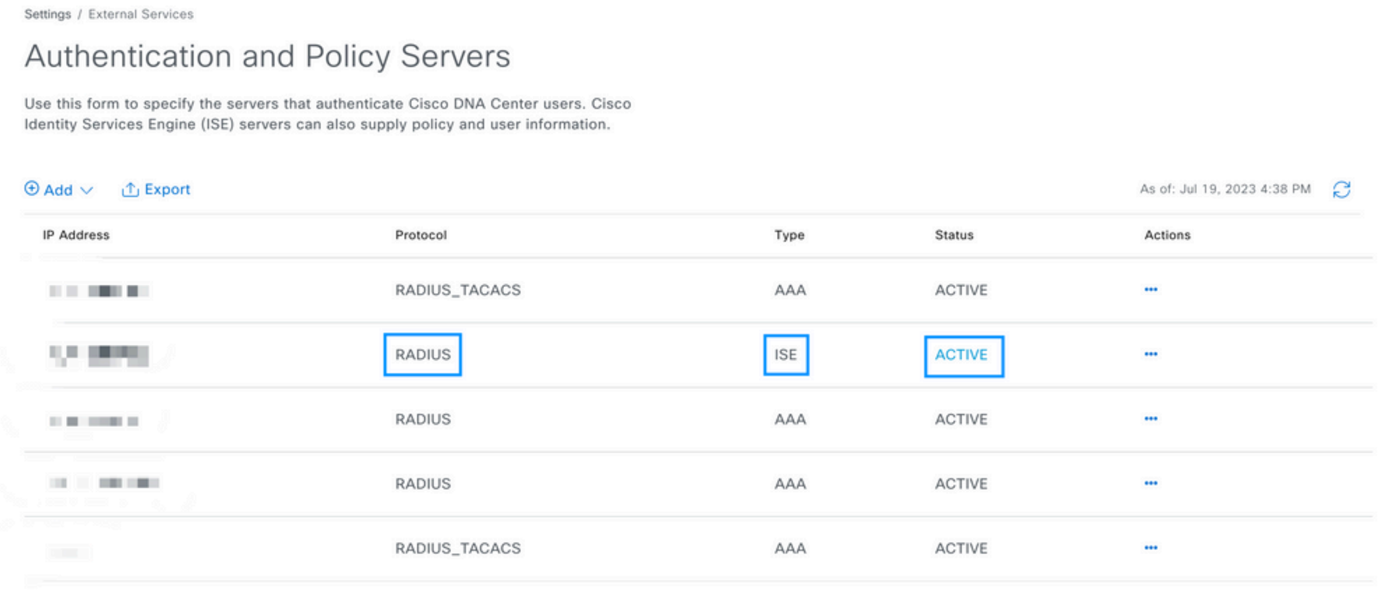
- Cisco DNA Center 2.3.5.x release.
- Cisco ISE 3.1release.

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.

Configure

Step 1. Login to the Cisco DNA Center GUI and navigate to**System > Settings > Authentication and Policy Servers.**

Verify **RADIUS** protocol is configured and the ISE status is **Active** for the **ISE Type** server.



Settings / External Services

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

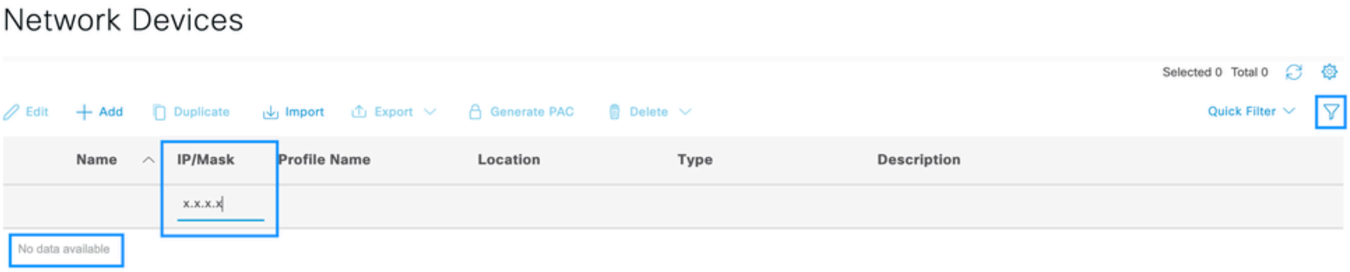
IP Address	Protocol	Type	Status	Actions
[redacted]	RADIUS_TACACS	AAA	ACTIVE	•••
[redacted]	RADIUS	ISE	ACTIVE	•••
[redacted]	RADIUS	AAA	ACTIVE	•••
[redacted]	RADIUS	AAA	ACTIVE	•••
[redacted]	RADIUS_TACACS	AAA	ACTIVE	•••

Note: **RADIUS_TACACS Protocol type** works for this document.

Warning: In case the ISE server is not on Active Status, you must need to fix the integration first.

Step 2. On ISE Server navigate to **Administration > Network Resources > Network Devices**, click on the **Filter** icon, write the **Cisco DNA Center IP Address** and confirm if an entry exist. If it does, proceed to the **Step 3.**

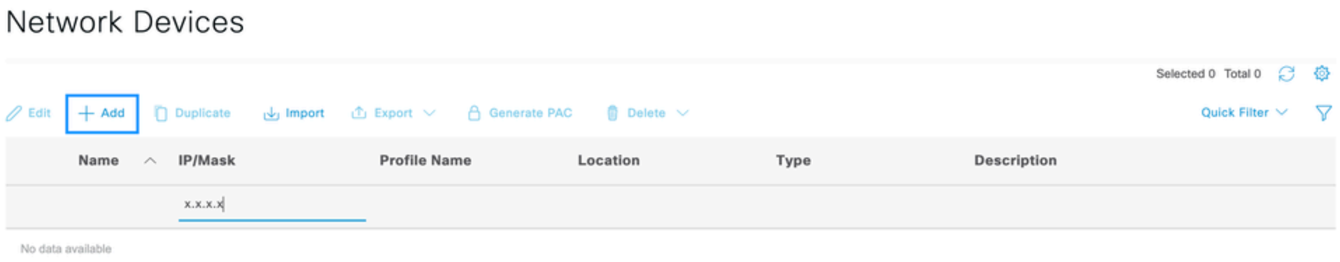
If the entry is missing, you must see the **No data available** message.



Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

In this case, you must create a Network Device for Cisco DNA Center, so click on the **Add button**.

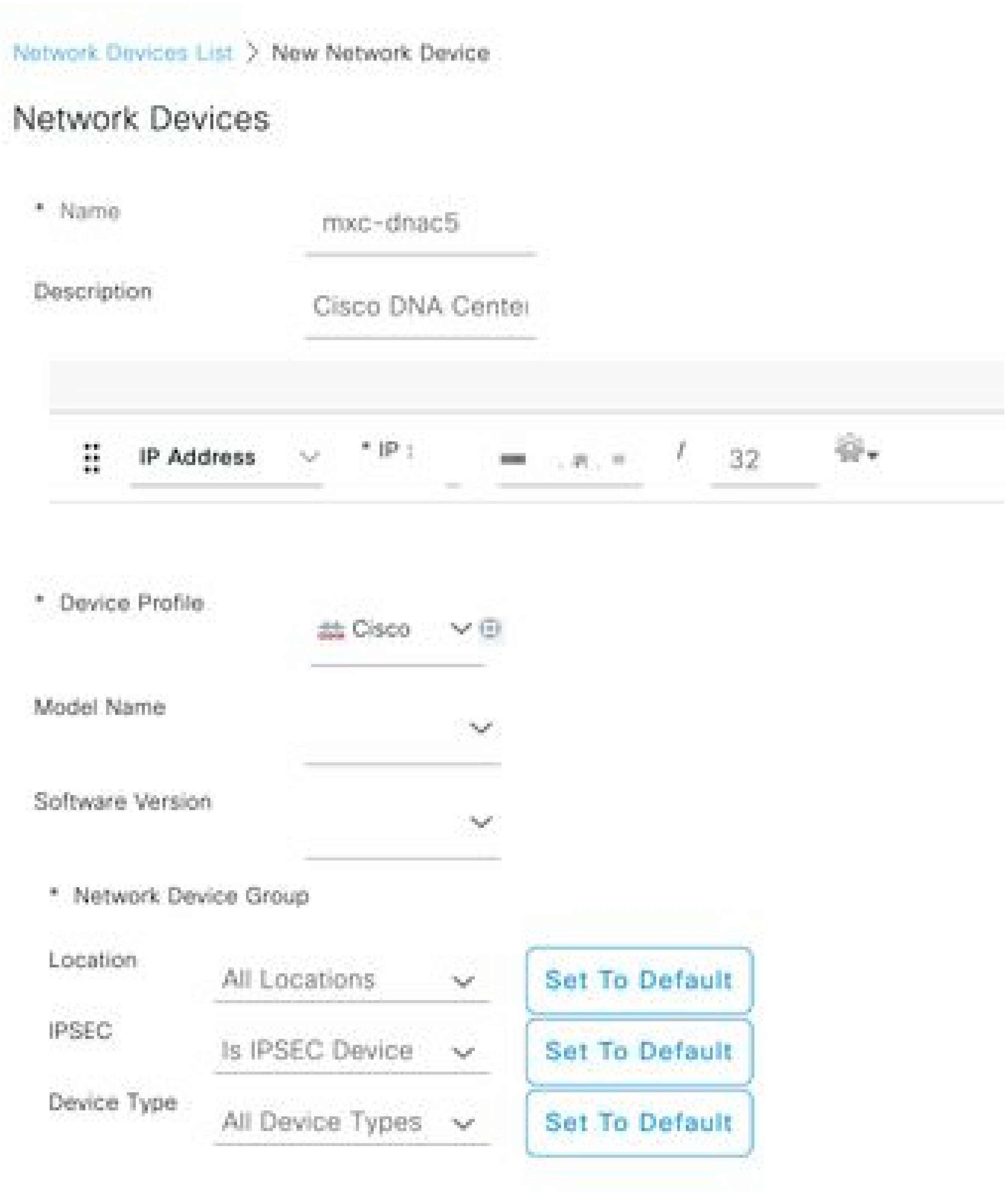


Network Devices

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

Configure the Name, Description and IP Address (or Addresses) from Cisco DNA Center, all other settings are set to Default values and are not needed for the purpose of this document.



Network Devices List > New Network Device

Network Devices

* Name: mxc-dnac5

Description: Cisco DNA Cente

IP Address * IP : [redacted] / 32

* Device Profile: Cisco

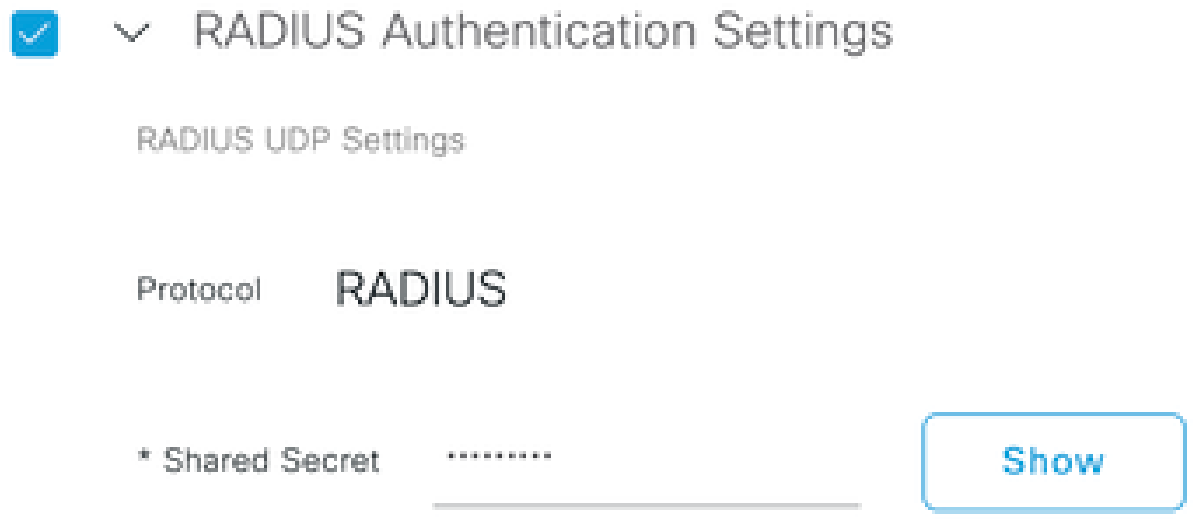
Model Name:

Software Version:

* Network Device Group

Location	All Locations	Set To Default
IPSEC	Is IPSEC Device	Set To Default
Device Type	All Device Types	Set To Default

Scroll down and enable the **RADIUS Authentication Settings** by click on its check box and configure a **Shared Secret.**

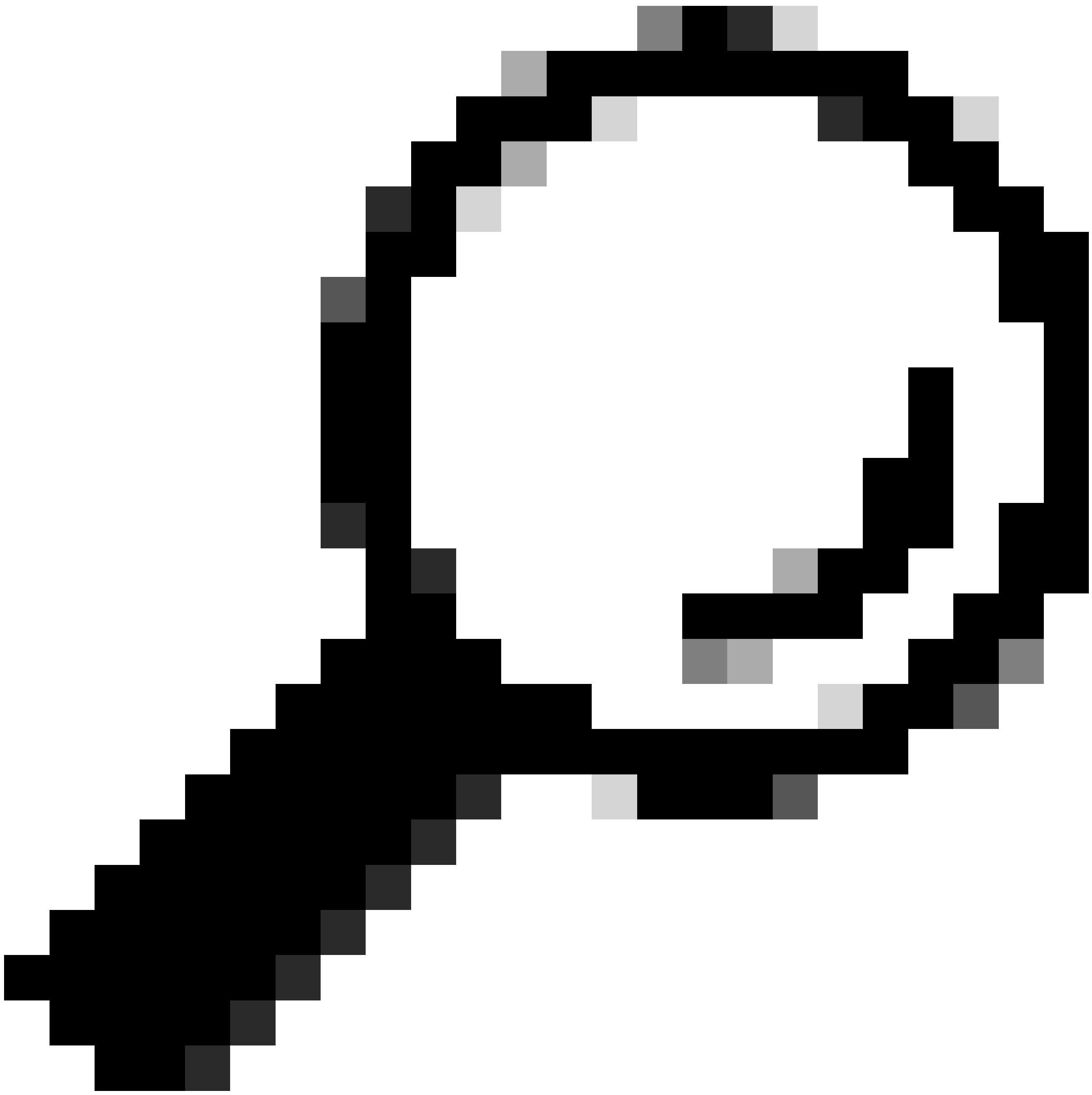


☑ ⌄ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret ··········

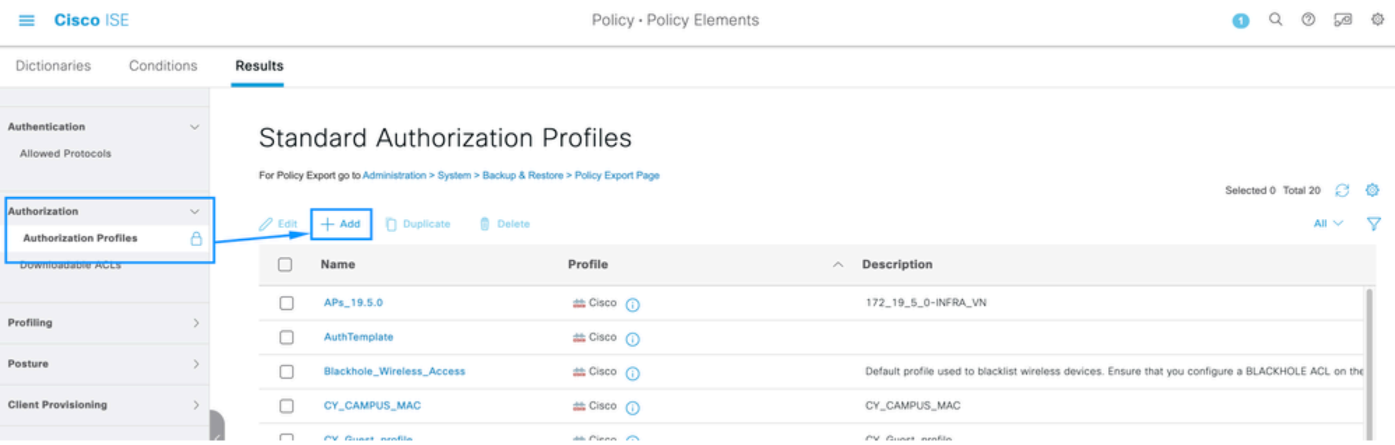


Tip: This **Shared Secret** is going to be needed later, so save it somewhere else.

Only then, click on **Submit**.

Step 3. On ISE Server navigate to **Policy** > **Policy Elements** > **Results**, to create the **Authorization Profile.**

Make sure you are under **Authorization** > **Authorization Profiles**, then select the **Add** option.

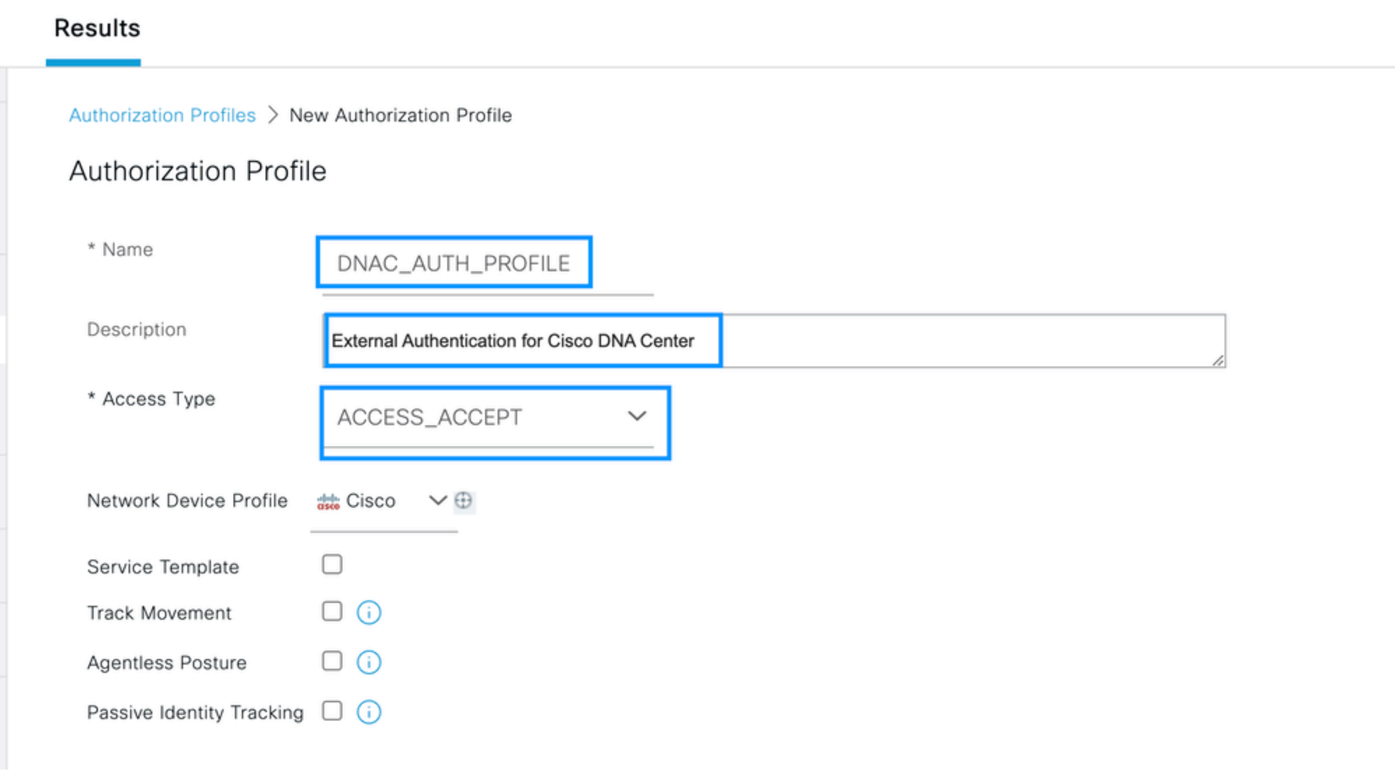


Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

☐	Name	Profile	Description
☐	APs_19.5.0	Cisco	172_19_5_0-INFRA_VN
☐	AuthTemplate	Cisco	
☐	Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the
☐	CY_CAMPUS_MAC	Cisco	CY_CAMPUS_MAC
☐	CY_Guest_profile	Cisco	CY_Guest_profile

Configure **Name**, add a **Description** just to keep a record of the new Profile and make sure that the **Access Type** is set to **ACCES_ACCEPT.**



Authorization Profile

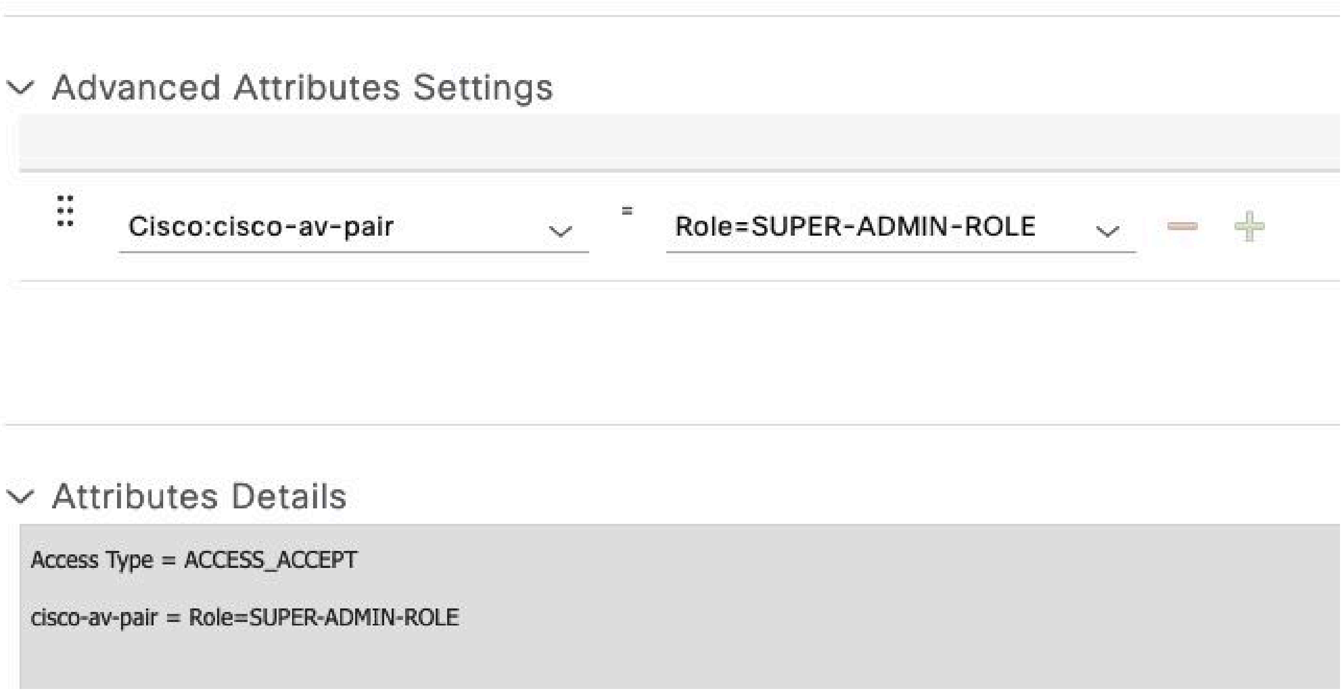
* Name	DNAC_AUTH_PROFILE
Description	External Authentication for Cisco DNA Center
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	☐
Track Movement	☐
Agentless Posture	☐
Passive Identity Tracking	☐

Scroll down and configure the **Advanced Attributes Settings.**

On the **left** column search for the **cisco-av-pair** option and select it.

On the **right** column **manually** type **Role=SUPER-ADMIN-ROLE.**

Once it looks like the image below, click on **Submit**.



Advanced Attributes Settings

Cisco:cisco-av-pair = Role=SUPER-ADMIN-ROLE

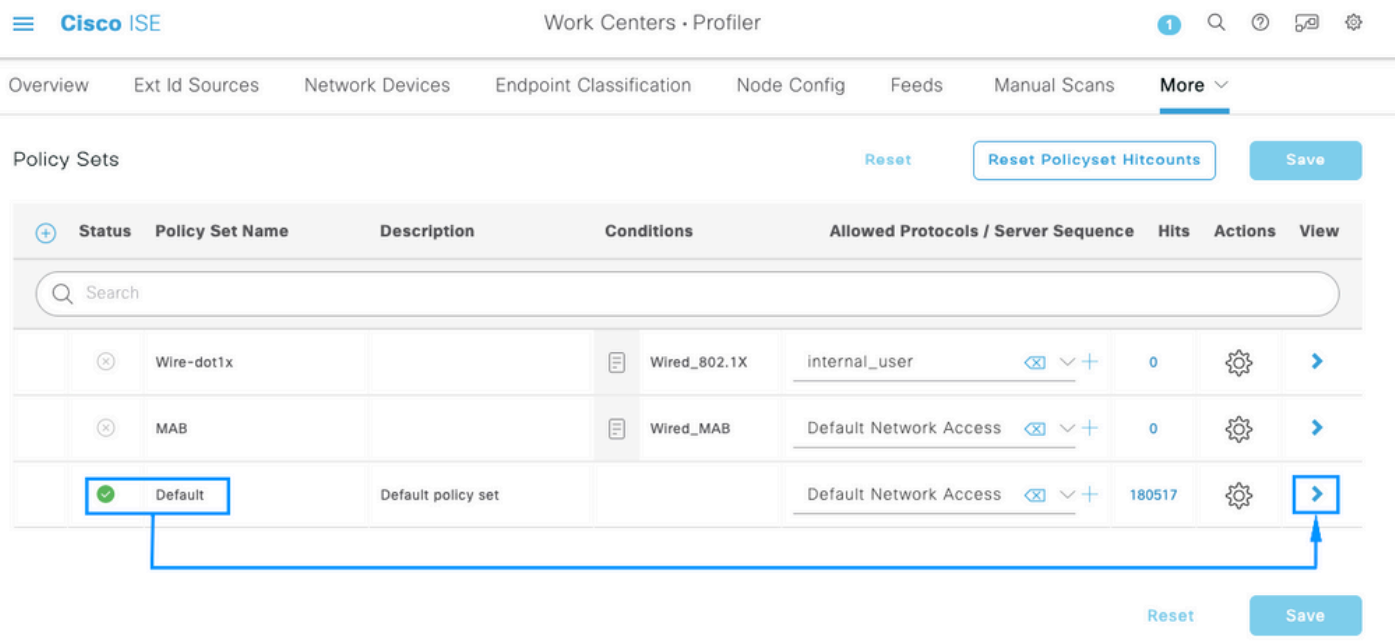
Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = Role=SUPER-ADMIN-ROLE

Step 4. On ISE Server navigate to **Work Centers > Profiler > Policy Sets**, to configure the **Authentication & Authorization Policy.**

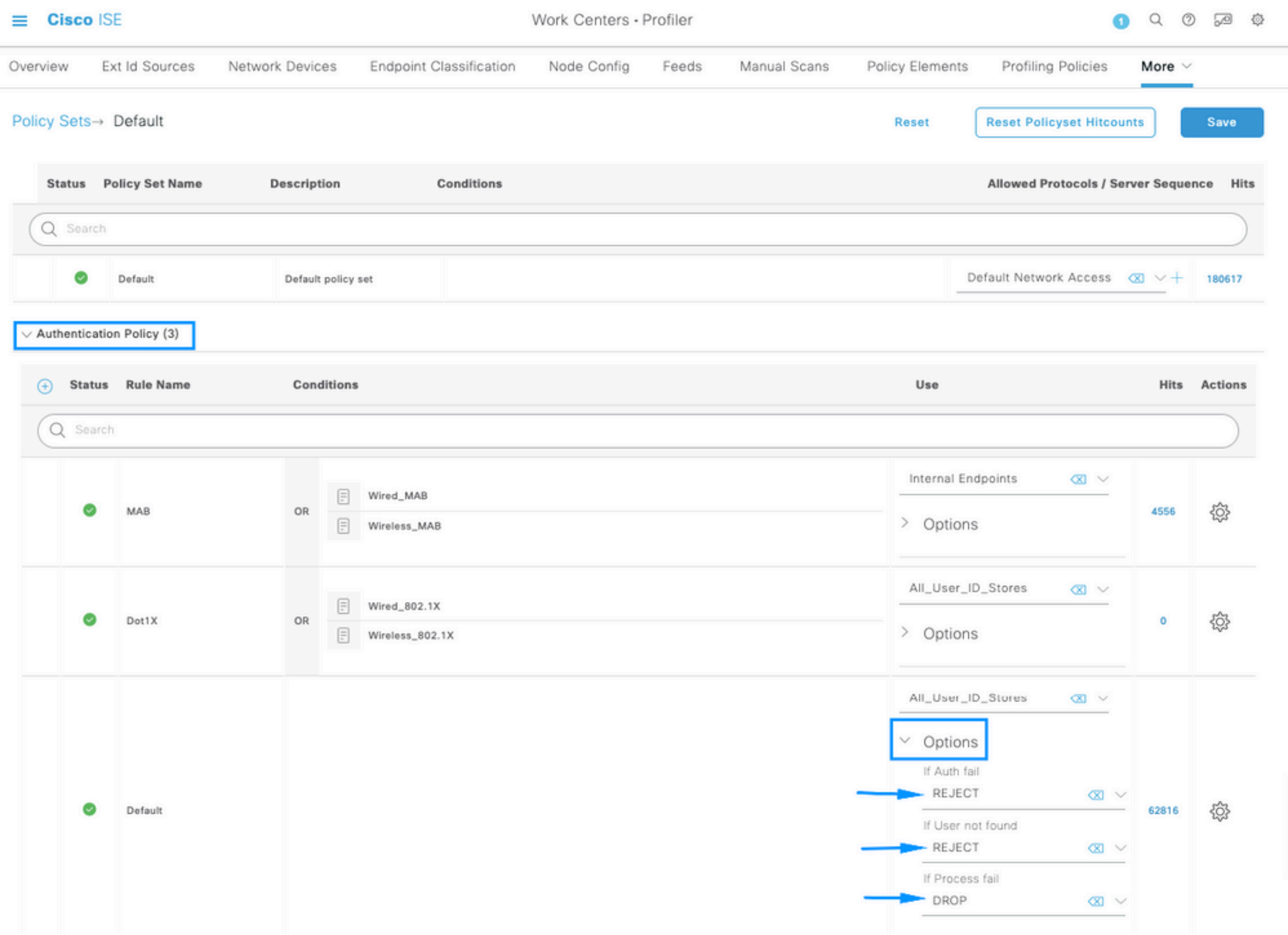
Identify the **Default** policy and click on the **blue arrow** to configure it.



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
⊗	Wire-dot1x		Wired_802.1X	internal_user	0	⚙	>
⊗	MAB		Wired_MAB	Default Network Access	0	⚙	>
✓	Default	Default policy set		Default Network Access	180517	⚙	>

Inside the **Default Policy Set**, expand the **Authentication Policy** and under the **Default** section, expand the **Options** and make sure that they match the configuration bellow.



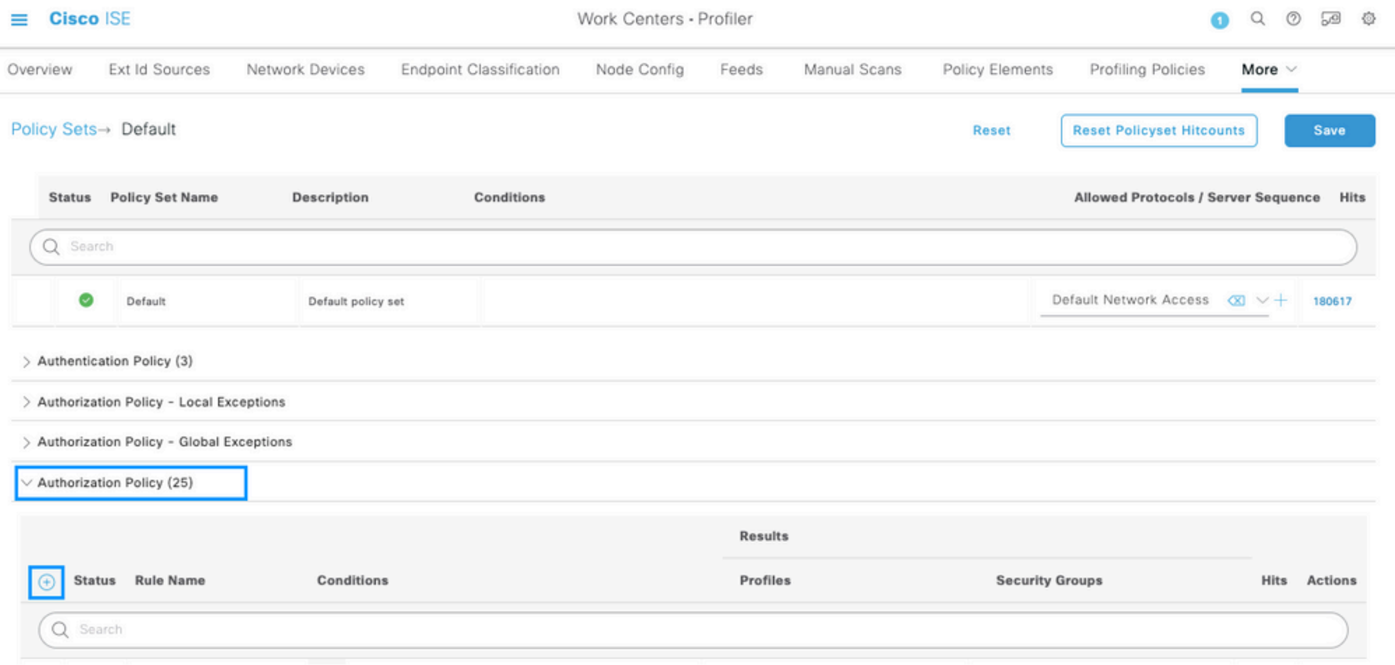
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	180617

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	4556	⚙
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙
●	Default		All_User_ID_Stores Options If Auth fail REJECT If User not found REJECT If Process fail DROP	62816	⚙

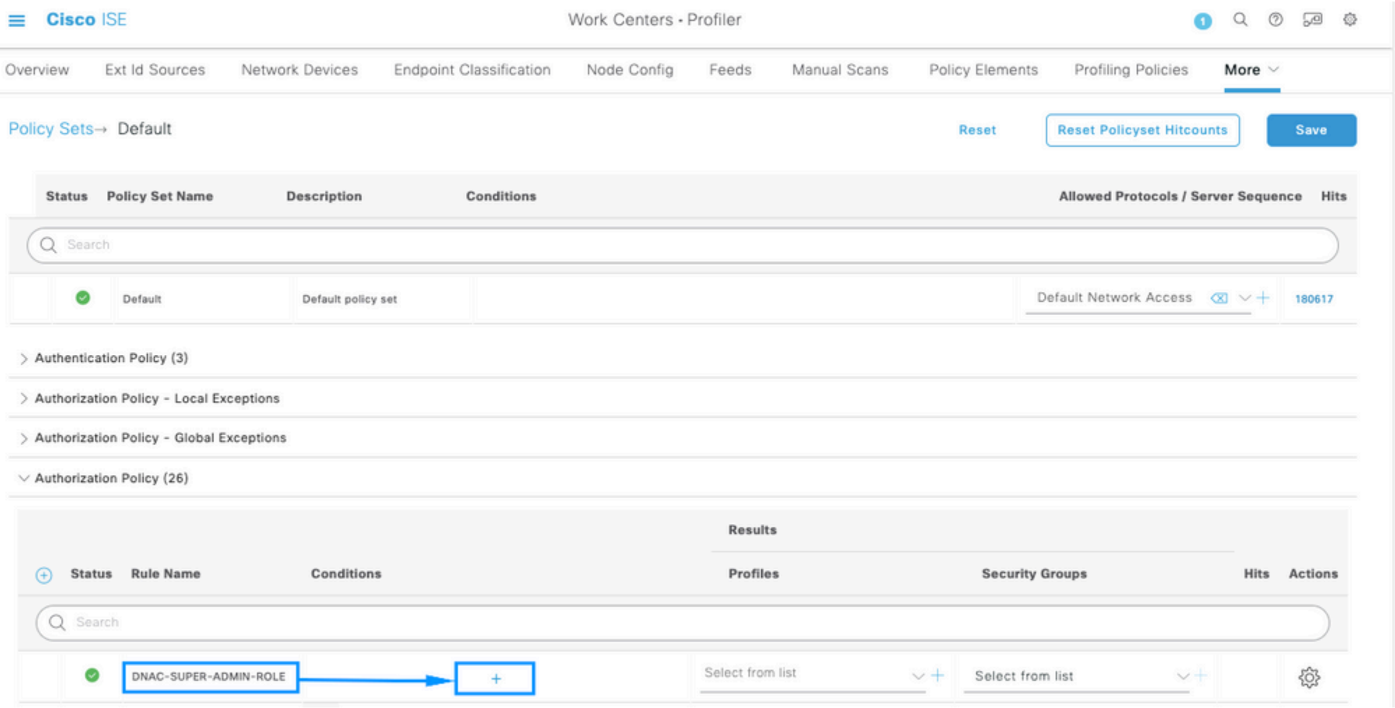
Tip: REJECT configured on the 3 options also works

Inside the **Default Policy Set**, expand the **Authorization Policy** and select the **Add** icon to create a new **Authorization Condition**.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

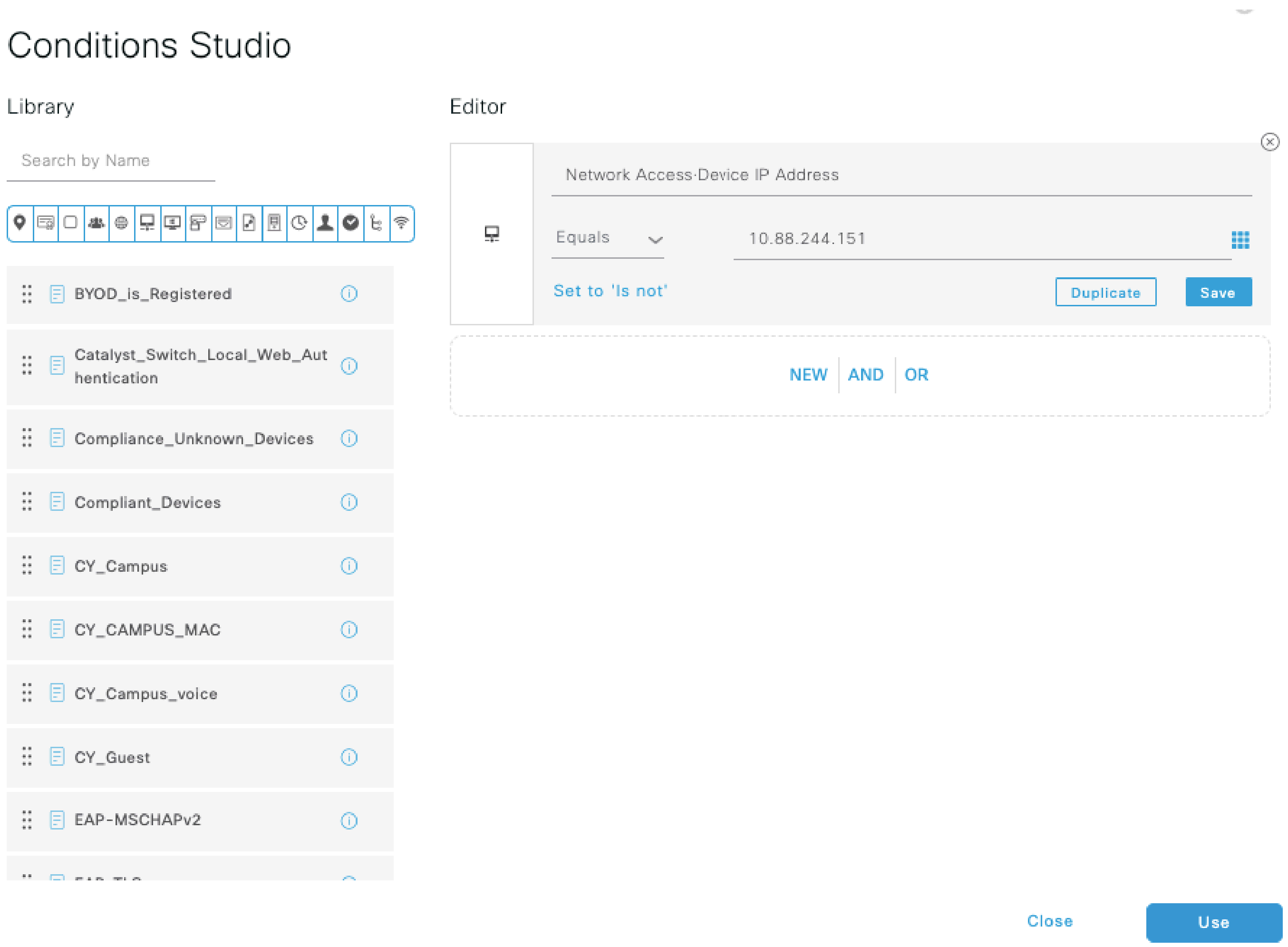
Configure a **Rule Name**, and click on the Add icon to configure the **Condition**.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	DNAC-SUPER-ADMIN-ROLE	+	Select from list	Select from list		⚙

As part of the **Condition**, associate it to the **Network Device IP Address** configured on **Step 2**.



Conditions Studio

Library

Search by Name

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- CY_Campus
- CY_CAMPUS_MAC
- CY_Campus_voice
- CY_Guest
- EAP-MSCHAPv2

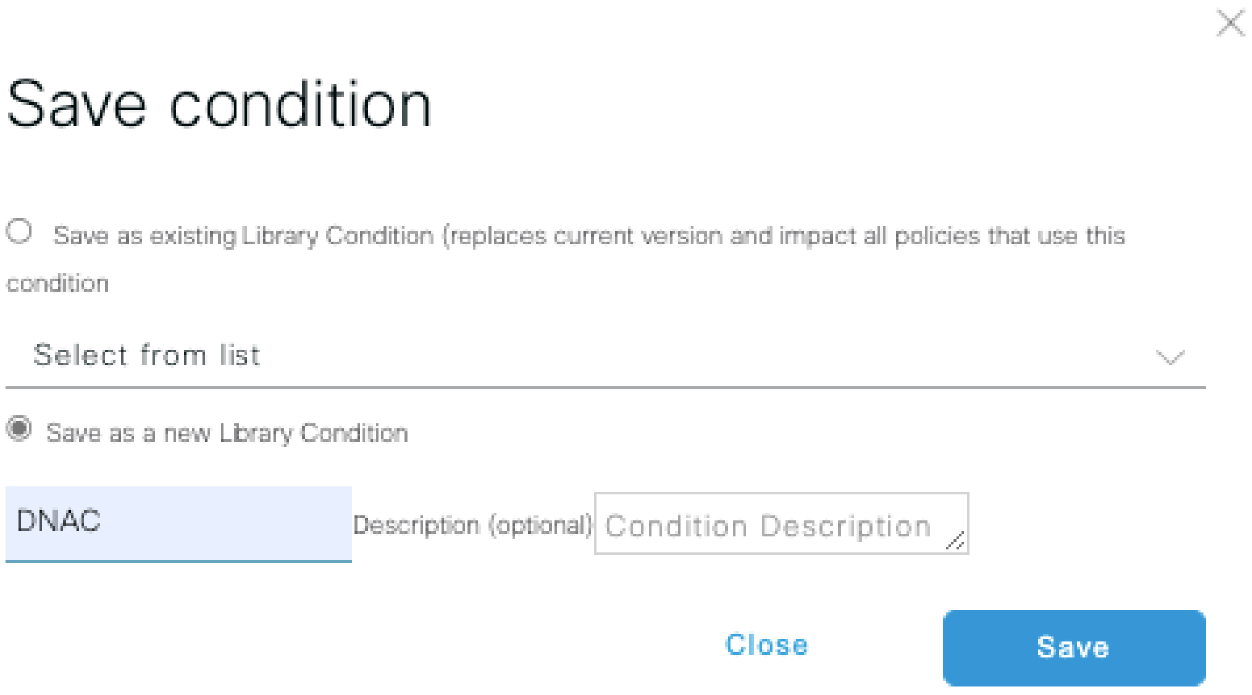
Editor

Network Access·Device IP Address

Equals 10.88.244.151

Click on **Save.**

Save it as a new **Library Condition**, and named it as you wish, on this case it is named as DNAC.



Save condition

○ Save as existing Library Condition (replaces current version and impact all policies that use this condition

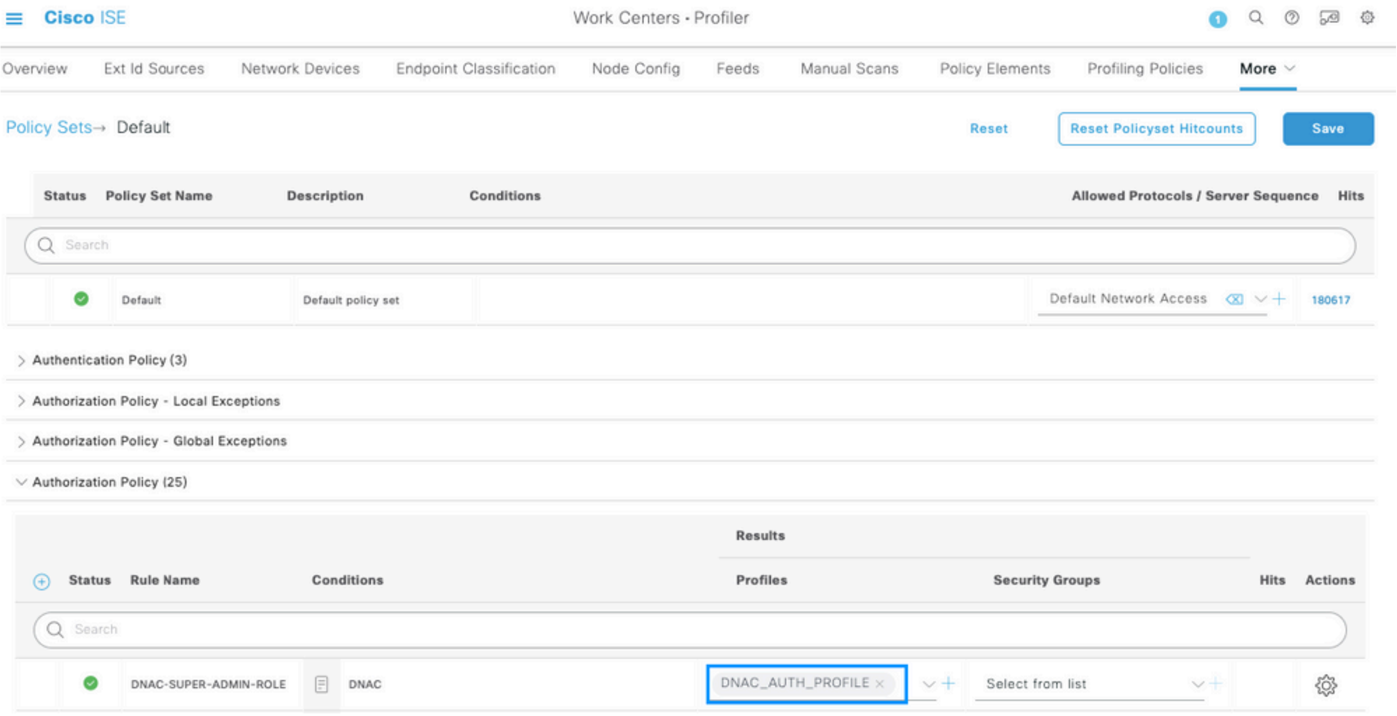
Select from list

● Save as a new Library Condition

DNAC

Description (optional) Condition Description

Finally, configure the **Profile** created on Step 3.



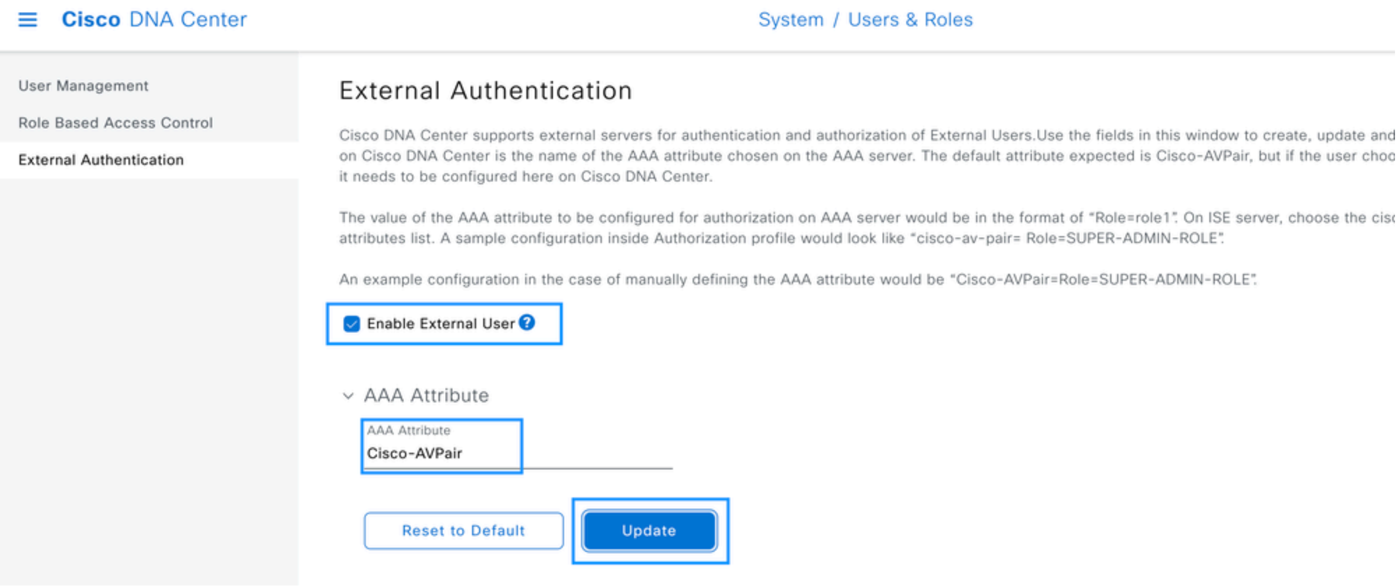
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	180617

		Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	DNAC-SUPER-ADMIN-ROLE	DNAC	DNAC_AUTH_PROFILE	Select from list		

Click on **Save**.

Step 5. Login to the Cisco DNA Center GUI and navigate to**System > Users & Roles > External Authentication.**

Click on the **Enable External User** option and set the **AAA Attribute** as **Cisco-AVPair.**



External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users.Use the fields in this window to create, update and
on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user choo
it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisc
attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair= Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

☑ Enable External User

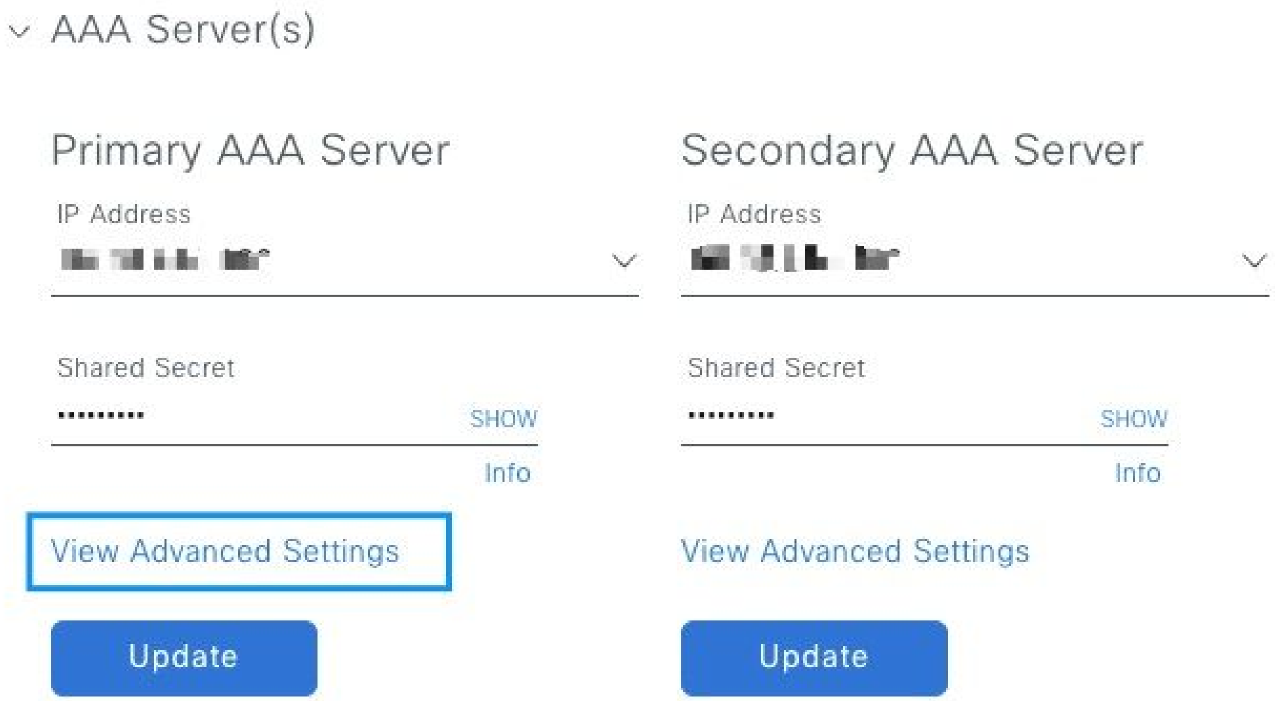
AAA Attribute

AAA Attribute: Cisco-AVPair

Note: ISE Server use the attribute **Cisco-AVPair** on the backend, so the configuration on **Step 3** is valid.

Scroll down to see the **AAA Server(s)** configuration section. Configure the **IP Address** from ISE Server on **Step 1** and the Shared Secret configured on Step 3.

Then click on **View Advanced Settings.**



⌄ AAA Server(s)

Primary AAA Server

IP Address
[redacted]

Shared Secret
•••••••••• SHOW

Info

View Advanced Settings

Update

Secondary AAA Server

IP Address
[redacted]

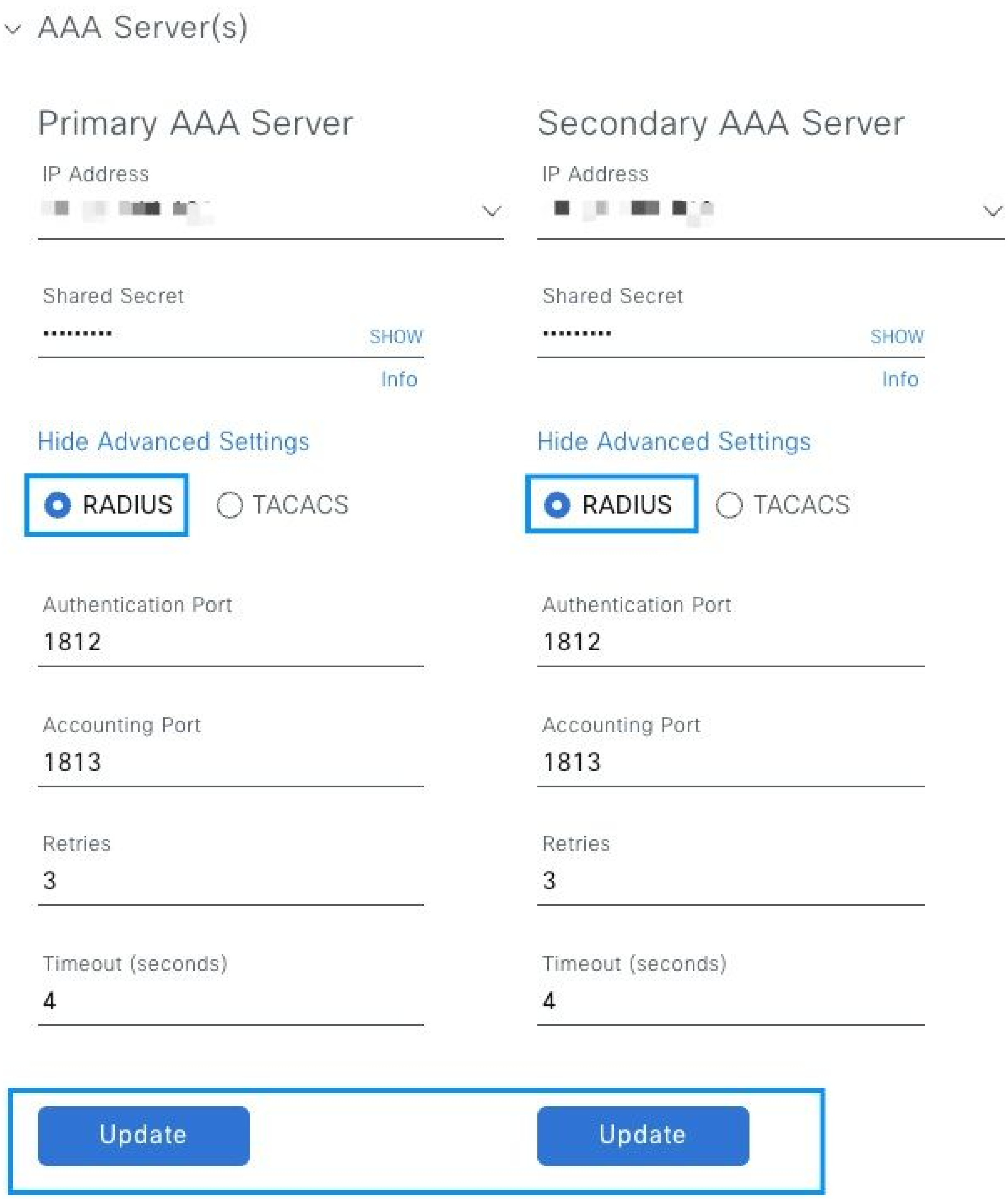
Shared Secret
•••••••••• SHOW

Info

View Advanced Settings

Update

Verify that RADIUS option is selected and click the Update button on both Servers.



AAA Server(s)

Primary AAA Server

IP Address: [redacted]

Shared Secret: •••••••••• SHOW

Info

Hide Advanced Settings

● RADIUS ○ TACACS

Authentication Port: 1812

Accounting Port: 1813

Retries: 3

Timeout (seconds): 4

Secondary AAA Server

IP Address: [redacted]

Shared Secret: •••••••••• SHOW

Info

Hide Advanced Settings

● RADIUS ○ TACACS

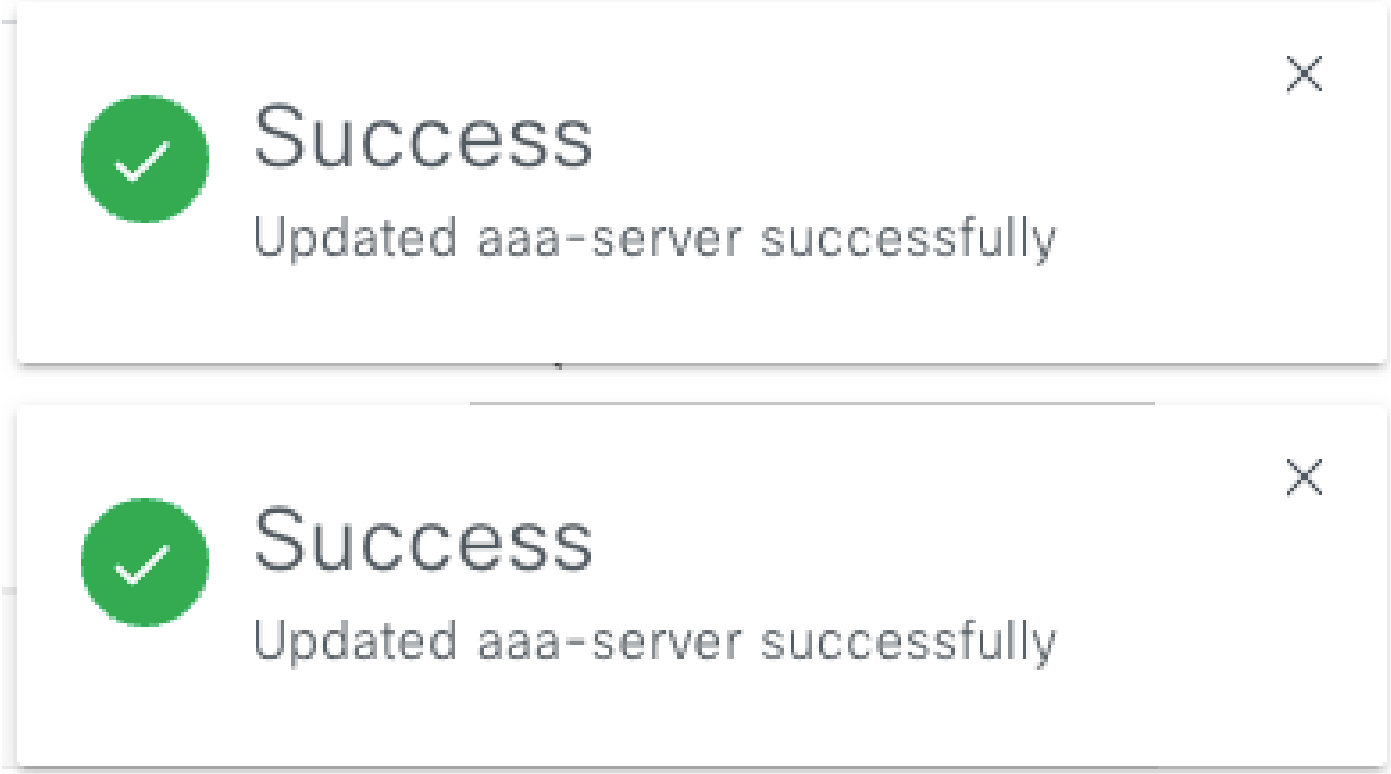
Authentication Port: 1812

Accounting Port: 1813

Retries: 3

Timeout (seconds): 4

You must see a Success message for each.



Success

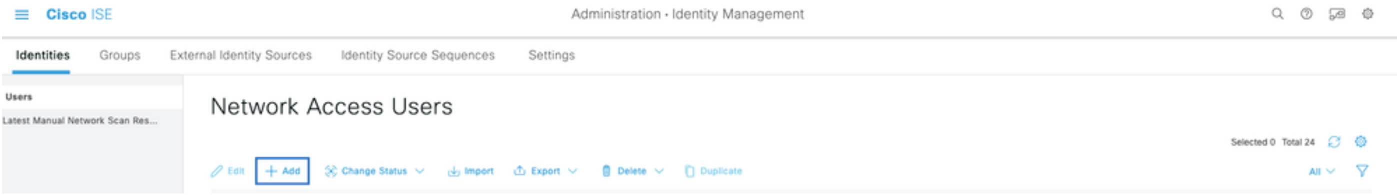
Updated aaa-server successfully

Success

Updated aaa-server successfully

Now you are be able to login with any ISE Identity created under ISE menu > Administration > Identity Management > Identities > Users.

In case you don't have any created, login to ISE, navigate to above path, and add a new **Network Access User.**

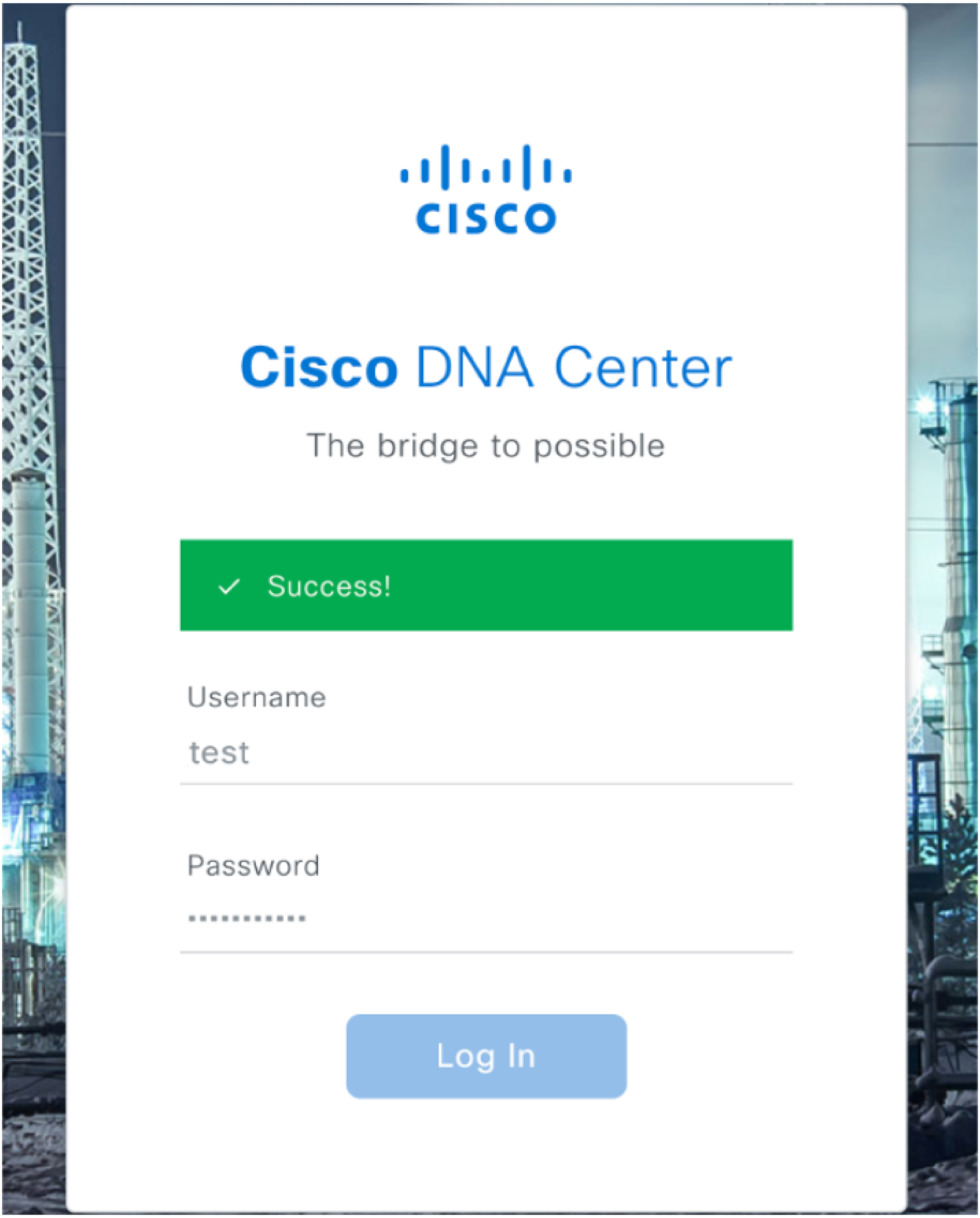


Cisco ISE
Administration · Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Res...
Edit
Add
Change Status
Import
Export
Delete
Duplicate
Selected 0 Total 24
All

Network Access Users

Verify

Load the Cisco DNA Center GUI and Log in with a User from ISE identities.



Cisco DNA Center

The bridge to possible

✓ Success!

Username

test

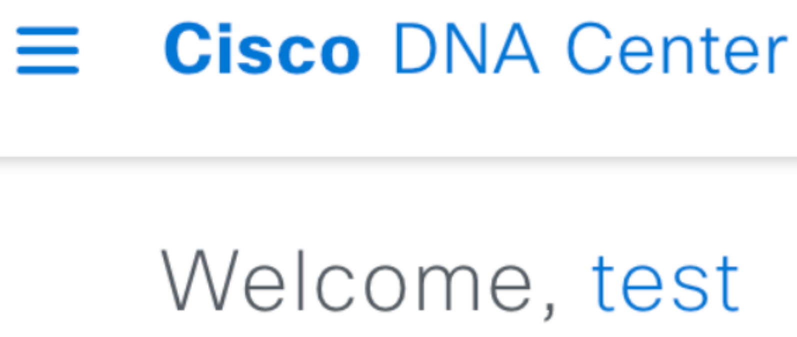
Password

••••••••••

DNA Center Log In

Note: Any user on ISE identities is able to login now. You can add more granularity to the Authentication rules on ISE Server.

After the login Succeed the Username is displayed on the Cisco DNA Center GUI

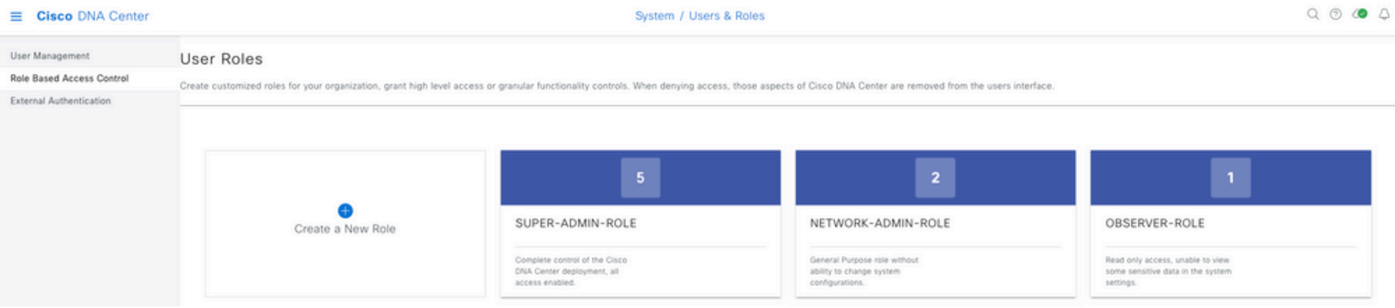


Welcome, test

Welcome Screen

More Roles

You can repeat these steps for every role on Cisco DNA Center, as default we have: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE** and **OBSERVER-ROLE.**



User Roles

Create customized roles for your organization, grant high level access or granular functionality controls. When denying access, those aspects of Cisco DNA Center are removed from the users interface.

5 SUPER-ADMIN-ROLE

Complete control of the Cisco DNA Center deployment, all access enabled.

2 NETWORK-ADMIN-ROLE

General Purpose role without ability to change system configurations.

1 OBSERVER-ROLE

Read only access, unable to view some sensitive data in the system settings.

On this document we use the **SUPER-ADMIN-ROLE** role example, nevertheless, you can configure one Authorization Profile on ISE for every role on Cisco DNA Center, the only consideration is that the Role configured on Step 3 needs to match exactly (case sensitive) the Role name on Cisco DNA Center.