

Configure RADIUS External Authentication on DNA Center and ISE 3.1

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

[More Roles](#)

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 3.1 release.

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.

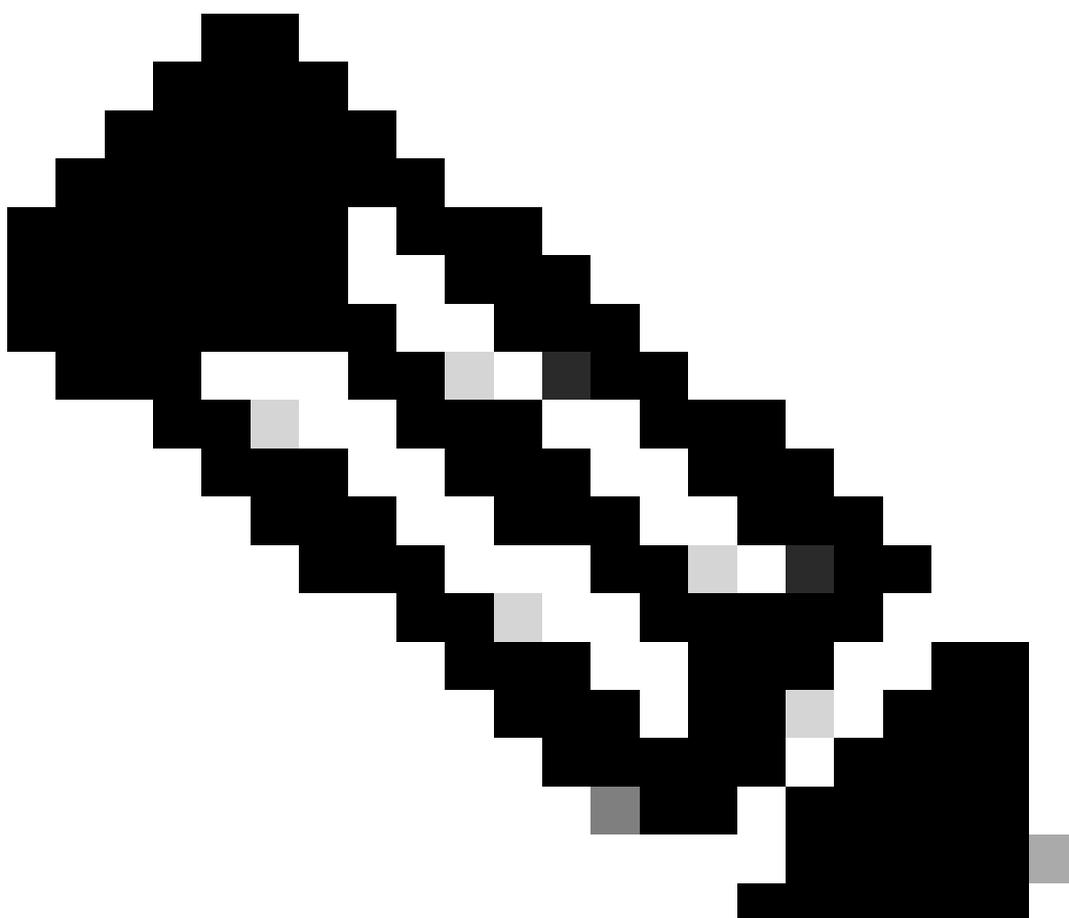
Authentication and Policy Servers

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.

[Add](#) [Export](#)

As of: Jul 19, 2023 4:38 PM [Refresh](#)

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.

Network Devices

Selected 0 Total 0

Edit + Add Duplicate Import Export Generate PAC Delete Quick Filter

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

Selected 0 Total 0  

 Edit **+ Add**  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

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

* Name

Description

 IP Address 

* Device Profile

Model Name

Software Version

* Network Device Group

Location

[Set To Default](#)

IPSEC

[Set To Default](#)

Device Type

[Set To Default](#)

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



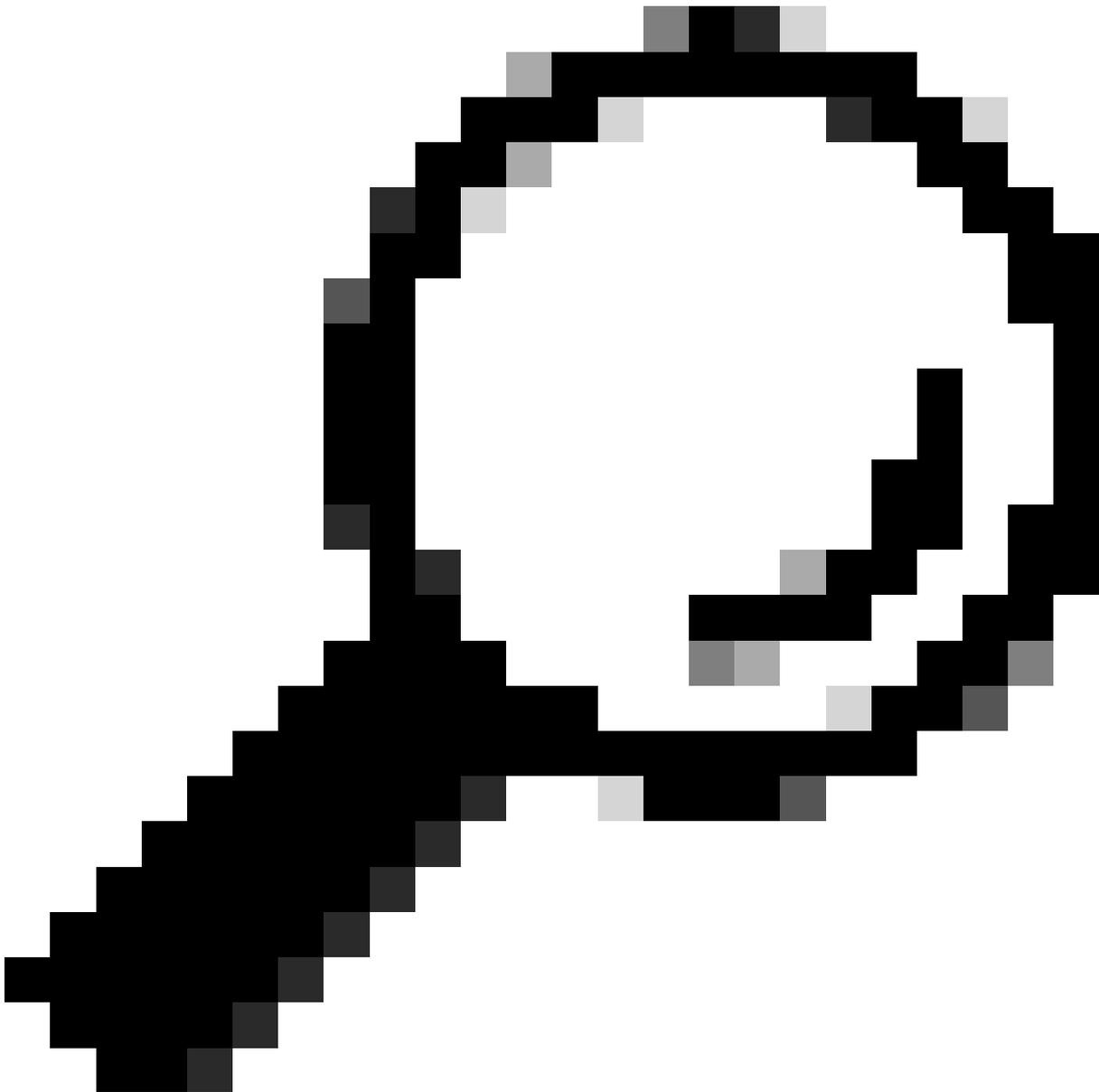
✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Show

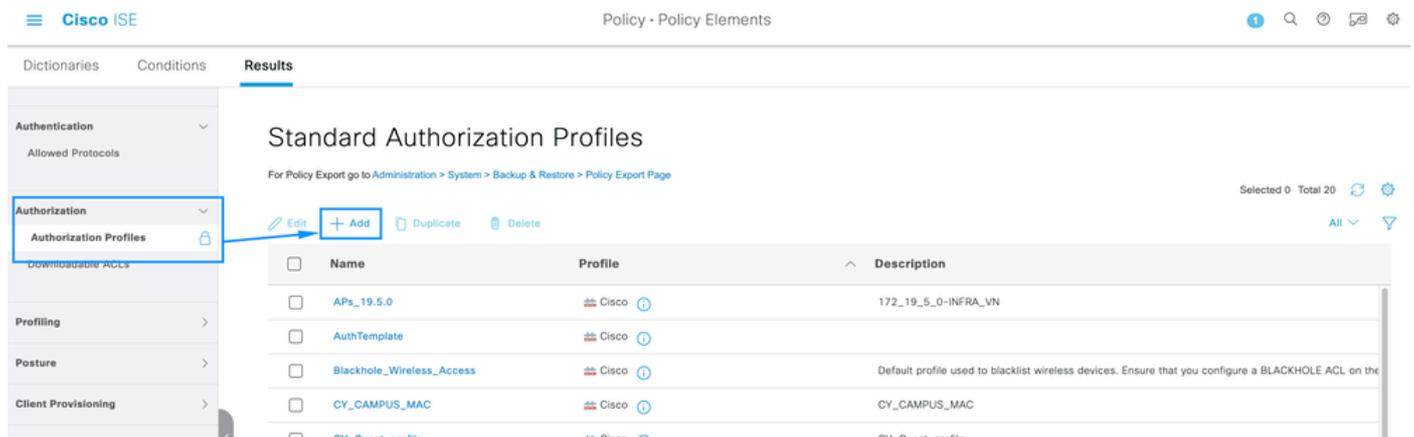


Tip: This **Shared Secret** is going to be needed later, so save it somewhere else.

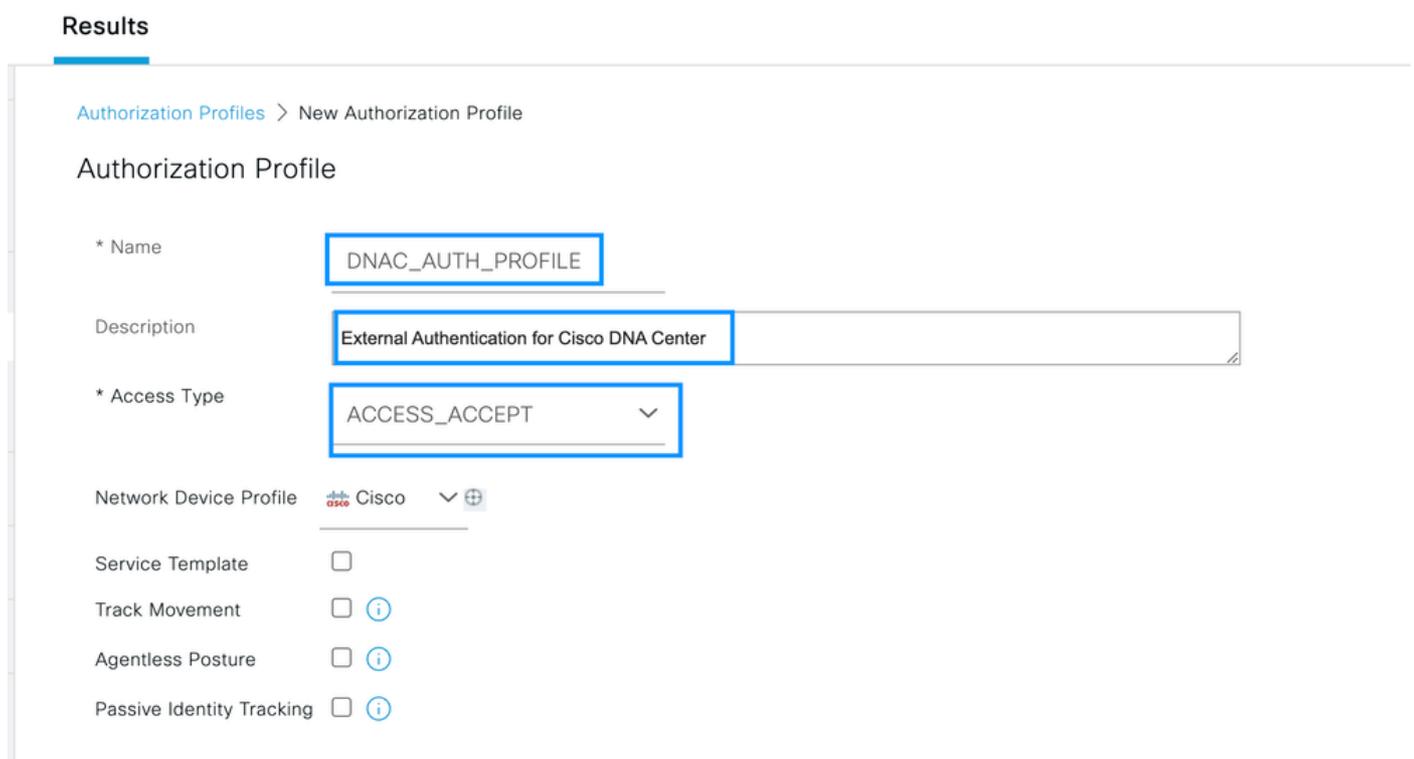
Only then, click on **Submit**.

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.



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

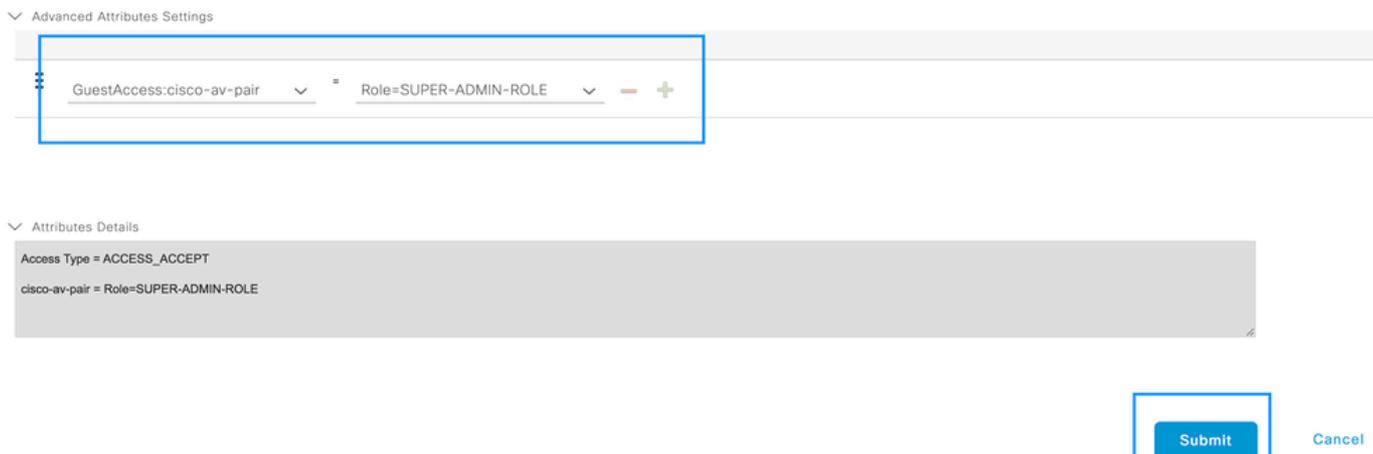


Scroll down and configure the **Advanced Attributes Settings**.

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

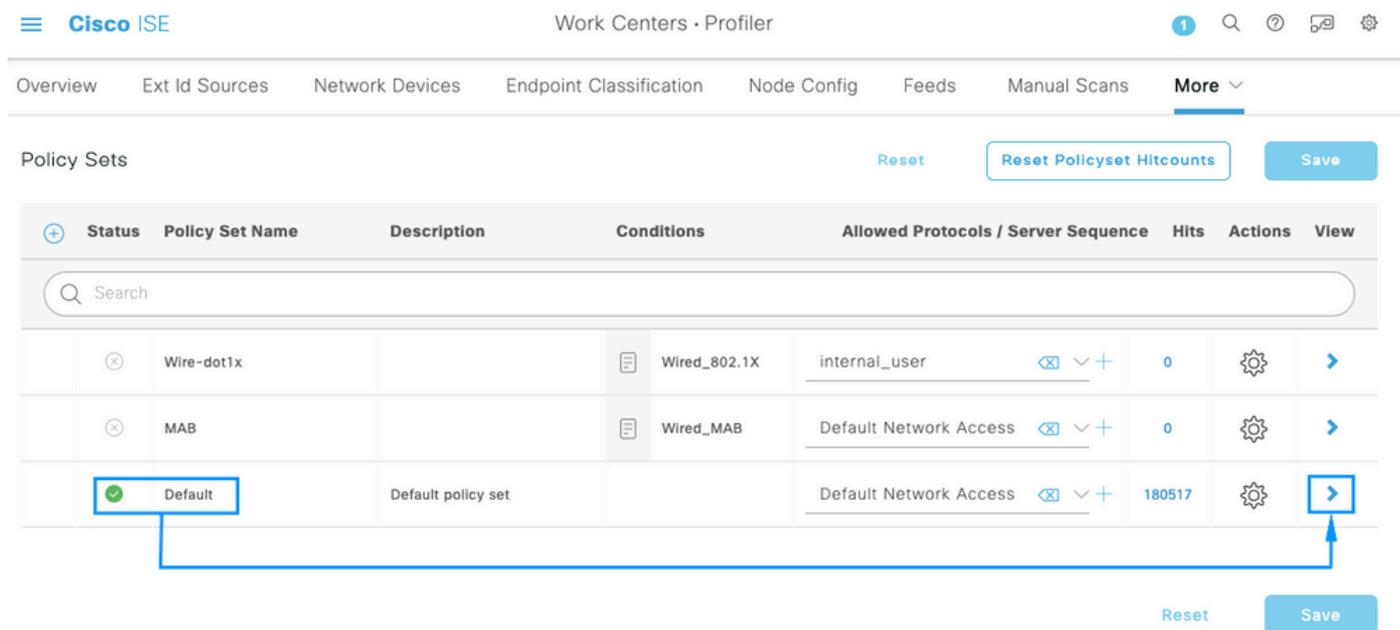
On the **right** column **manually** type **Role=SUPER-ADMIN-ROLE**.

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



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.



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 below.

Policy Sets → Default

Reset

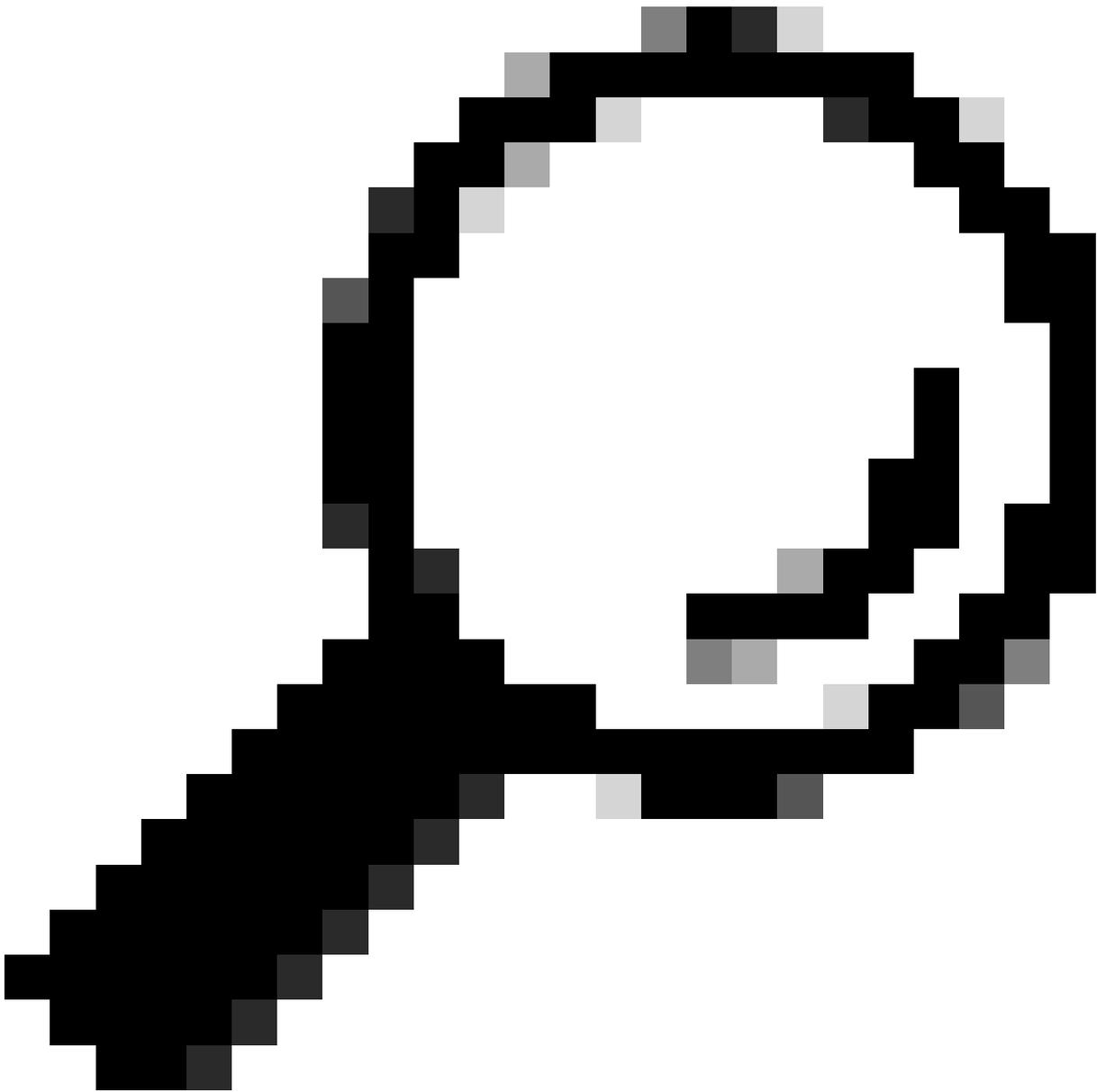
Reset Policyset Hitcounts

Save

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**.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

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

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (25)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
+						

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

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies More

Policy Sets → Default Reset Reset Policyset Hitcounts Save

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

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (26)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
+	DNAC-SUPER-ADMIN-ROLE					

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

Set to 'Is not'

Duplicate Save

NEW | AND | OR

Close

Use

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

Close

Save

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

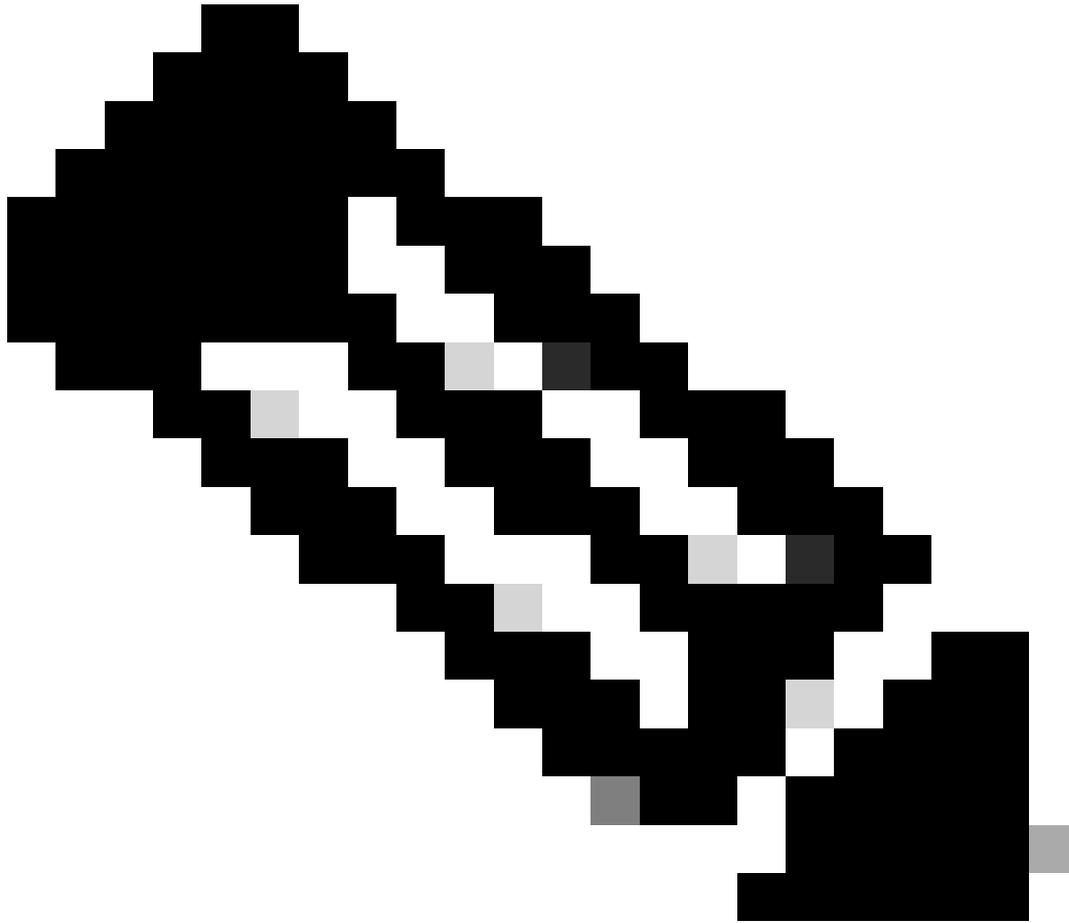
The screenshot shows the Cisco ISE Work Centers - Profiler interface. The top navigation bar includes 'Cisco ISE' and 'Work Centers - Profiler'. Below the navigation bar, there are tabs for 'Overview', 'Ext Id Sources', 'Network Devices', 'Endpoint Classification', 'Node Config', 'Feeds', 'Manual Scans', 'Policy Elements', 'Profiling Policies', and 'More'. The main content area is titled 'Policy Sets -> Default' and includes buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. A table lists policy sets with columns for 'Status', 'Policy Set Name', 'Description', 'Conditions', 'Allowed Protocols / Server Sequence', and 'Hits'. The first row shows a green status icon, 'Default' as the policy set name, 'Default policy set' as the description, and 'Default Network Access' as the allowed protocols with a hit count of 180617. Below this table, there are expandable sections for 'Authentication Policy (3)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (25)'. The 'Authorization Policy (25)' section is expanded, showing a table with columns for 'Status', 'Rule Name', 'Conditions', 'Profiles', 'Security Groups', 'Hits', and 'Actions'. The first row in this table shows a green status icon, 'DNAC-SUPER-ADMIN-ROLE' as the rule name, 'DNAC' as the conditions, 'DNAC_AUTH_PROFILE' as the profile, and 'Select from list' as the security groups. A search bar is located above the table.

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**.

The screenshot shows the Cisco DNA Center System / Users & Roles External Authentication configuration page. The left sidebar contains 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area is titled 'External Authentication' and includes a description: '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.' Below the description, there are two paragraphs of text explaining the AAA attribute format and an example configuration. The 'Enable External User' checkbox is checked and highlighted with a blue box. Below this, the 'AAA Attribute' section is expanded, showing a text input field with 'Cisco-AVPair' entered and highlighted with a blue box. At the bottom, there are two buttons: 'Reset to Default' and 'Update', with the 'Update' button highlighted with a blue box.



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

10.10.10.10



Shared Secret

SHOW

Info

[View Advanced Settings](#)

Update

Secondary AAA Server

IP Address

10.10.10.10



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

██████████



Shared Secret

SHOW

Info

Hide Advanced Settings

RADIUS

TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

Timeout (seconds)

4

Update

Secondary AAA Server

IP Address

██████████



Shared Secret

SHOW

Info

Hide Advanced Settings

RADIUS

TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

Timeout (seconds)

4

Update

You must see a Success message for each.



Success

Updated aaa-server successfully



Success

Updated aaa-server successfully



Verify

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



Cisco DNA Center

The bridge to possible

✓ Success!

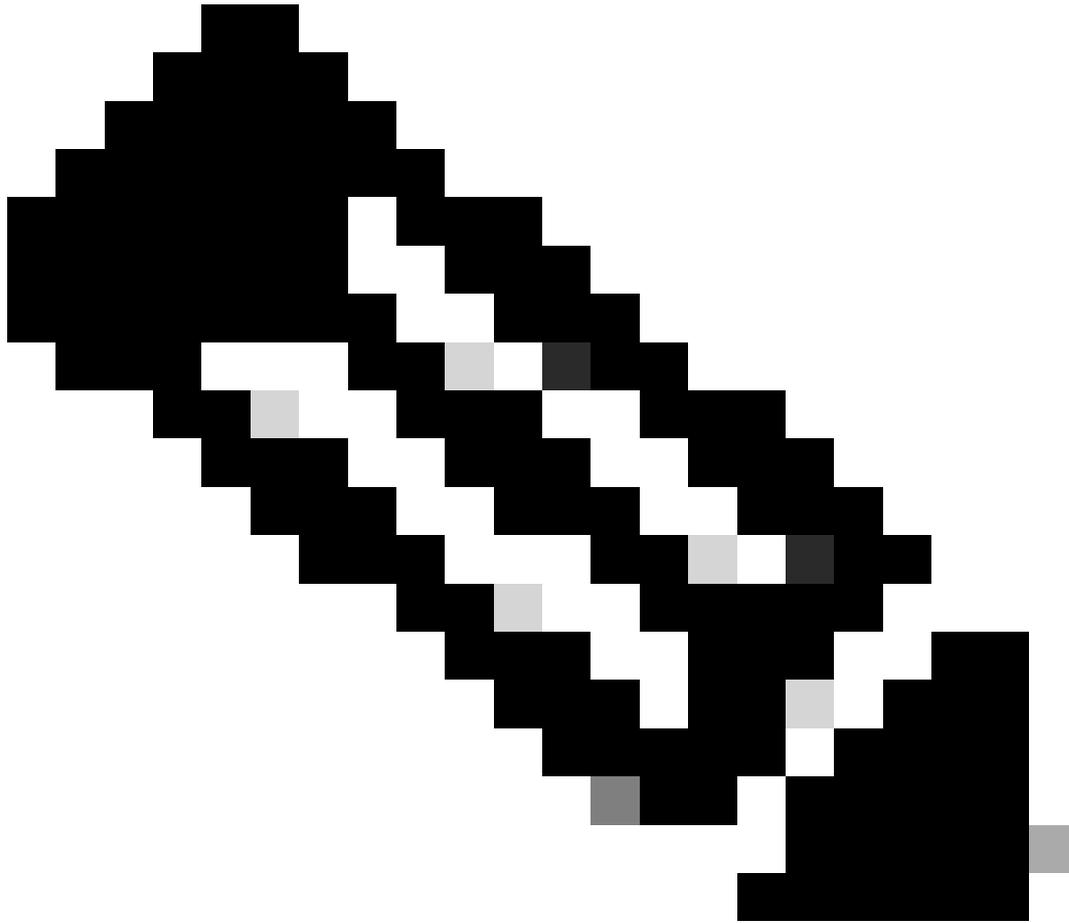
Username

test

Password

.....

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**.

The screenshot shows the Cisco DNA Center interface for managing user roles. The breadcrumb path is "System / Users & Roles". The main heading is "User Roles" with a sub-heading "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." On the left, there is a sidebar with "User Management" selected. The main content area contains four cards: "Create a New Role" (with a plus icon), "SUPER-ADMIN-ROLE" (ranked 5), "NETWORK-ADMIN-ROLE" (ranked 2), and "OBSERVER-ROLE" (ranked 1). Each role card includes a brief description of its permissions.

Role Name	Rank	Description
CREATE A NEW ROLE		
SUPER-ADMIN-ROLE	5	Complete control of the Cisco DNA Center deployment, all access enabled.
NETWORK-ADMIN-ROLE	2	General Purpose role without ability to change system configurations.
OBSERVER-ROLE	1	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.