

# Configuración de la autenticación externa RADIUS en DNA Center e ISE 3.1

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Más funciones](#)

---

## Introducción

Este documento describe cómo configurar la autenticación externa RADIUS en Cisco DNA Center mediante un servidor Cisco ISE que ejecute la versión 3.1.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco DNA Center y Cisco ISE ya están integrados y la integración se encuentra en estado activo.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco DNA Center 2.3.5.x Release.
- Cisco ISE versión 3.1.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

Paso 1. Inicie sesión en la GUI de Cisco DNA Center y navegue hasta `System > Settings >`

## Authentication and Policy Servers.

Verifique que el protocolo RADIUS esté configurado y que el estado de ISE sea Activo para el servidor de tipo de ISE.

Settings / External Services

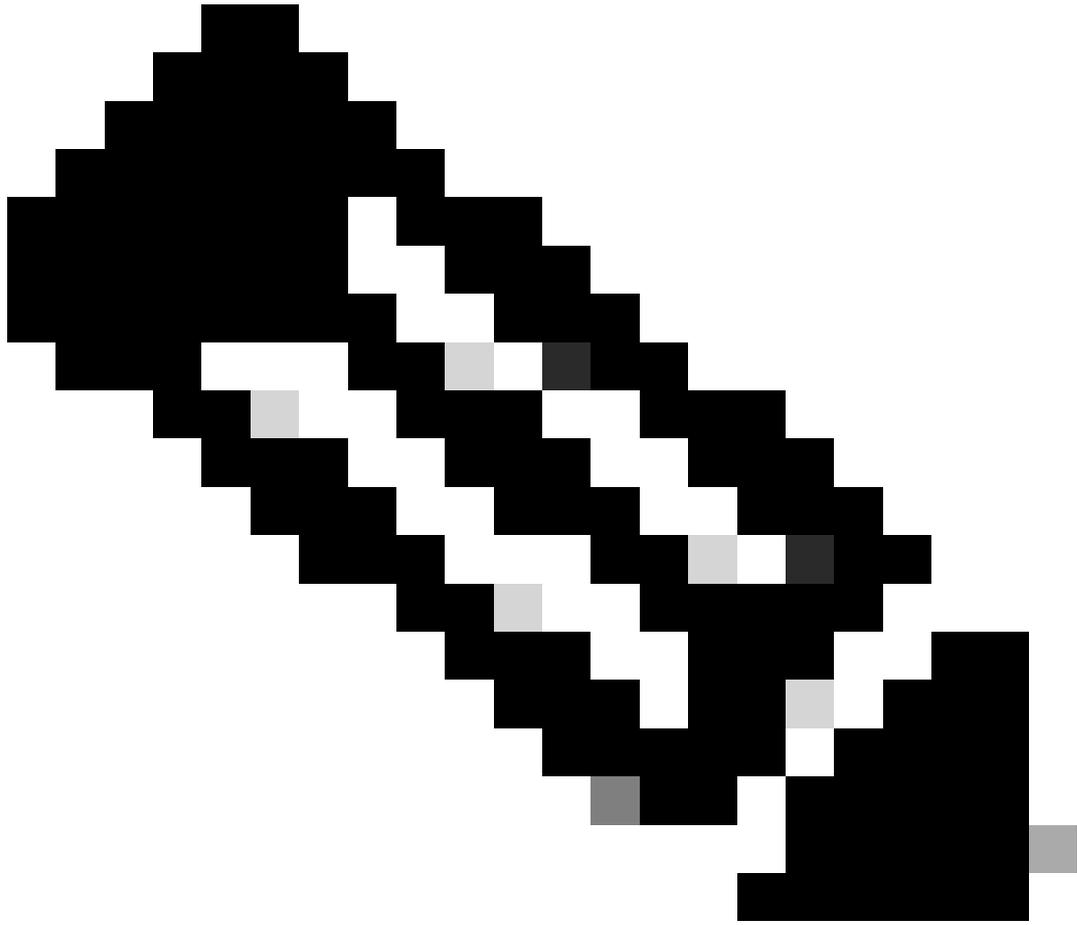
### Authentication and Policy Servers

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.

[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	...



Nota: El tipo de protocolo RADIUS\_TACACS funciona para este documento.

---



Advertencia: en caso de que el servidor ISE no esté en estado activo, primero debe corregir la integración.

Paso 2. En ISE Server, navegue hasta Administration > Network Resources > Network Devices, haga clic en el icono Filter, escriba la dirección IP de Cisco DNA Center y confirme si existe una entrada. Si es así, vaya al paso 3.

Si falta la entrada, debe ver el mensaje No hay datos disponibles.

## Network Devices

Selected 0 Total 0  

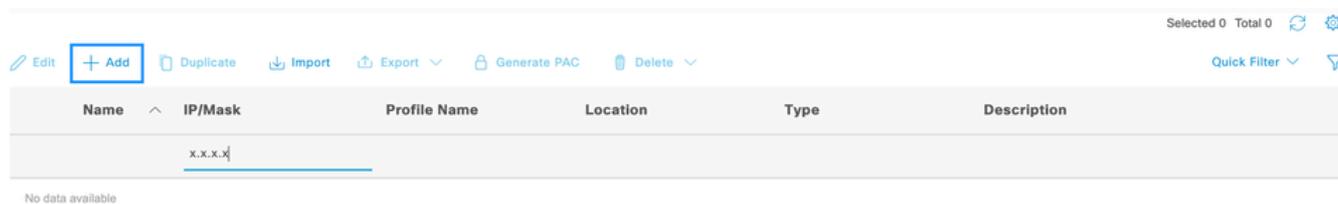
 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete  Quick Filter 

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

No data available

En este caso, debe crear un dispositivo de red para Cisco DNA Center, así que haga clic en el botón Add.

## 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 el nombre, la descripción y la dirección IP (o direcciones) desde Cisco DNA Center; el resto de las configuraciones se establecen en los valores predeterminados y no son necesarias para los fines de este documento.

## Network Devices

\* Name

Description

IP Address  \* IP :    /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

Desplácese hacia abajo y habilite RADIUS Authentication Settings haciendo clic en su casilla de verificación y configure un Shared Secret.



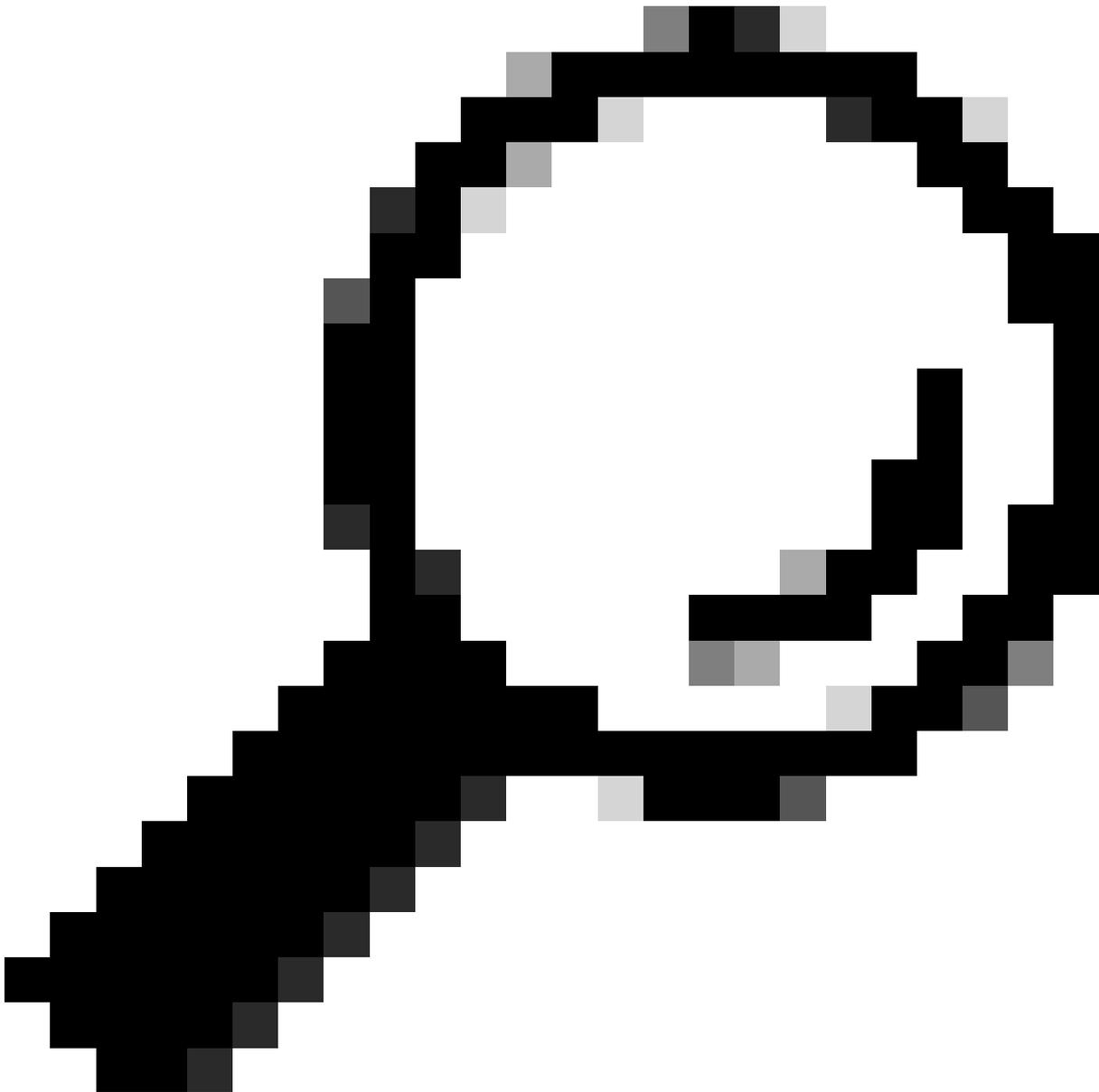
## ✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret .....

Show

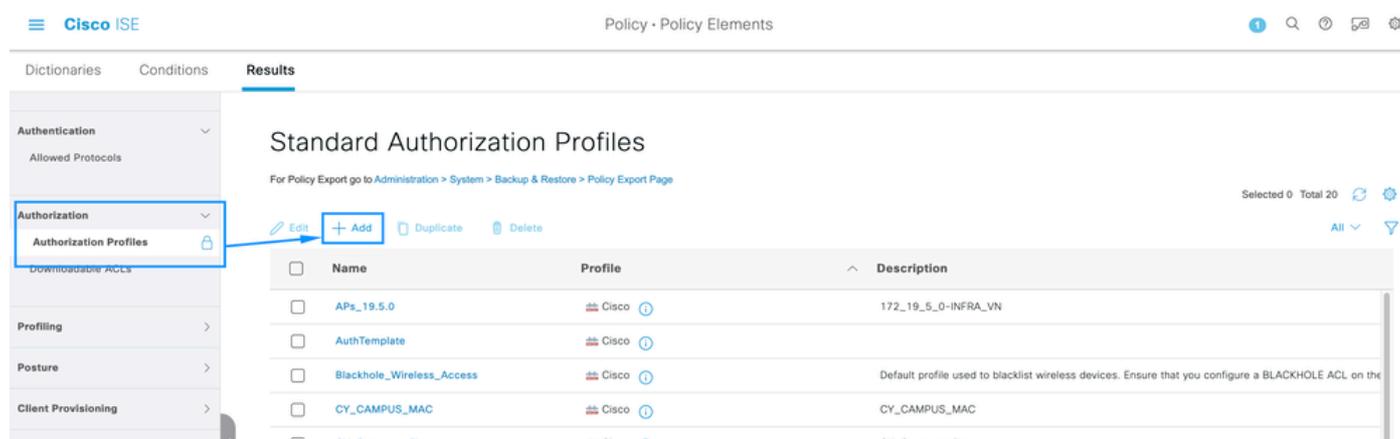


Sugerencia: este secreto compartido se necesitará más adelante, así que guárdelo en otro lugar.

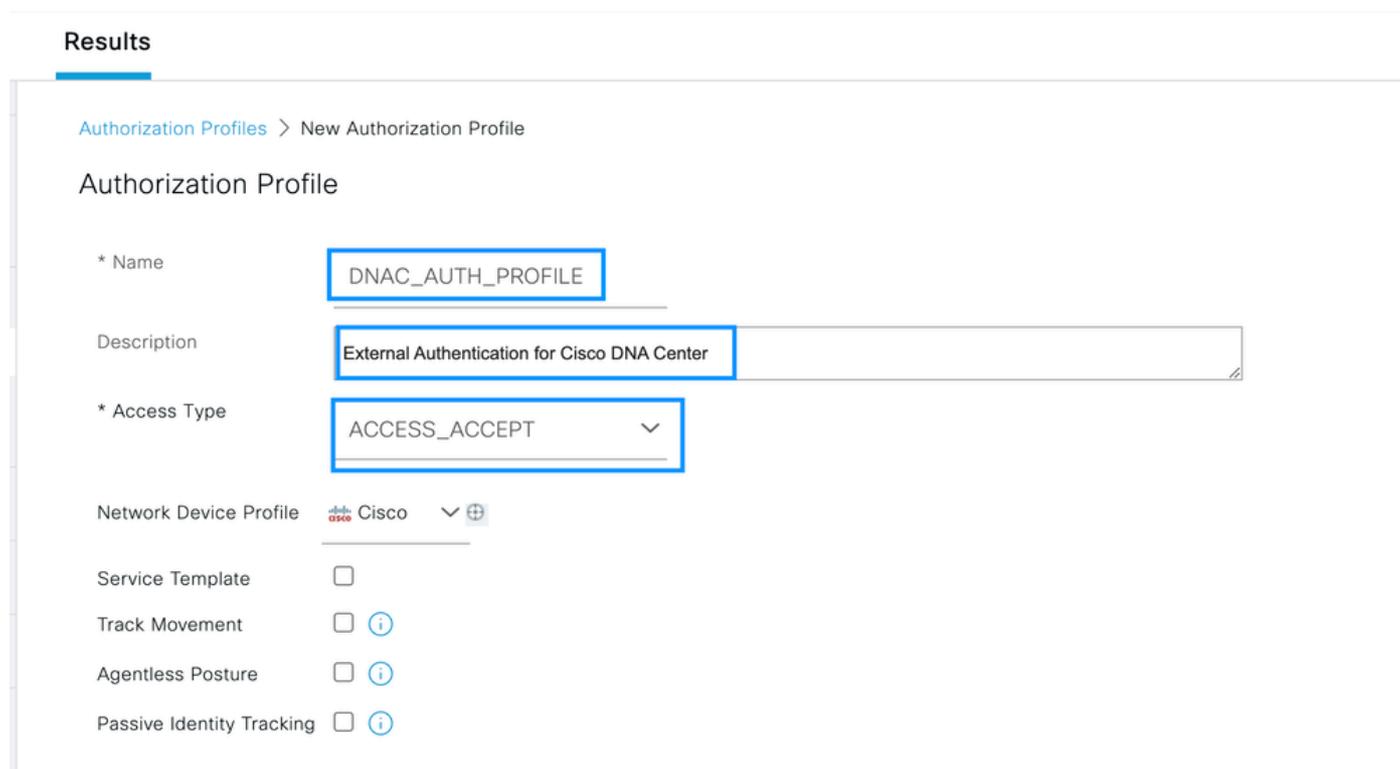
Solo entonces, haga clic en Submit.

Paso 3. En el servidor ISE, vaya a Policy > Policy Elements > Results, para crear el perfil de autorización.

Asegúrese de que se encuentra en Authorization > Authorization Profiles, luego seleccione la opción Add.



Configure Name, agregue una Description sólo para mantener un registro del nuevo perfil y asegúrese de que el Access Type esté configurado en ACCESS\_ACCEPT.



Desplácese hacia abajo y configure Advanced Attributes Settings (Parámetros de atributos avanzados).

En la columna izquierda, busque la opción cisco-av-pair y selecciónela.

En la columna derecha, escriba manualmente Role=SUPER-ADMIN-ROLE.

Una vez que se parezca a la imagen de abajo, haga clic en 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

Paso 4. En el servidor ISE, navegue hasta Centros de trabajo > Profiler > Conjuntos de políticas, para configurar la política de autenticación y autorización.

Identifique la política Default y haga clic en la flecha azul para configurarla.

Policy Sets

Reset

Reset Policyset Hitcounts

Save

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	⚙️	➔

Reset Save

Dentro del Conjunto de políticas predeterminadas, expanda la Política de autenticación y en la sección Predeterminado, expanda las Opciones y asegúrese de que coincidan con la siguiente configuración.

Policy Sets → Default

Reset

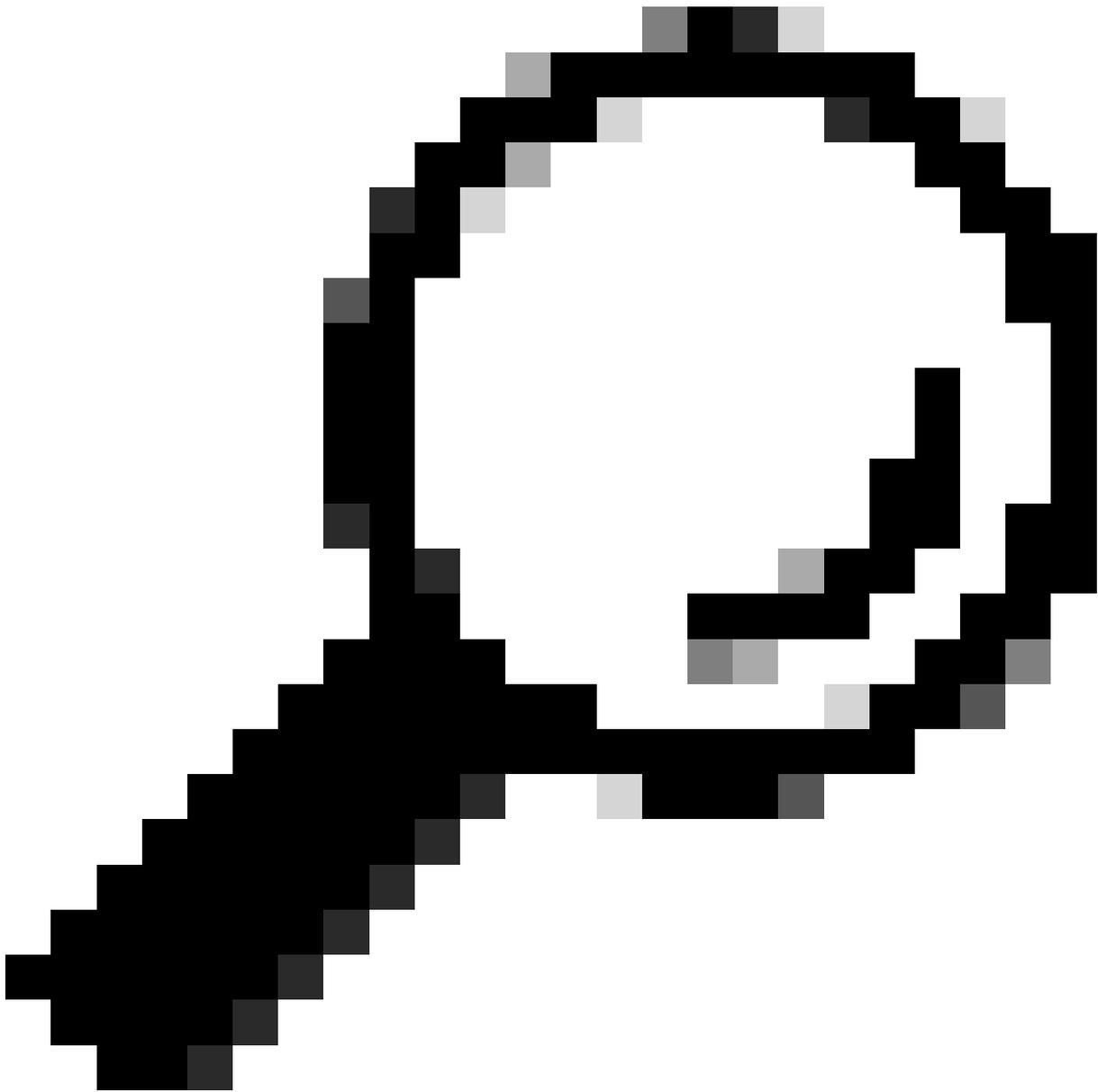
Reset Policyset Hitcounts

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	⚙️



Sugerencia: el RECHAZO configurado en las 3 opciones también funciona

---

Dentro del Conjunto de directivas predeterminado, expanda la Directiva de autorización y seleccione el icono Agregar para crear una nueva Condición de autorización.

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 un nombre de regla y haga clic en el icono Add (Agregar) para configurar la condición.

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		Select from list	Select from list			

Como parte de la Condición, asóciela a la Dirección IP del Dispositivo de Red configurada en el Paso 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

Haga clic en Guardar.

Guárdelo como una nueva Condición de Biblioteca, y nombrelo como desee, en este caso se nombra comoDNAC.



# 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

Por último, configure el perfil creado en el paso 3.

The screenshot shows the Cisco ISE GUI for configuring a new library condition. The 'Save as a new Library Condition' option is selected. The condition name is 'DNAC' and the description is 'Condition Description'. The 'Save' button is highlighted.

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

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

Haga clic en Guardar.

Paso 5. Inicie sesión en la GUI de Cisco DNA Center y navegue hasta Sistema > Usuarios y funciones > Autenticación externa.

Haga clic en la opción Enable External User y establezca el atributo AAA como Cisco-AVPair.

User Management

Role Based Access Control

External Authentication

## 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".

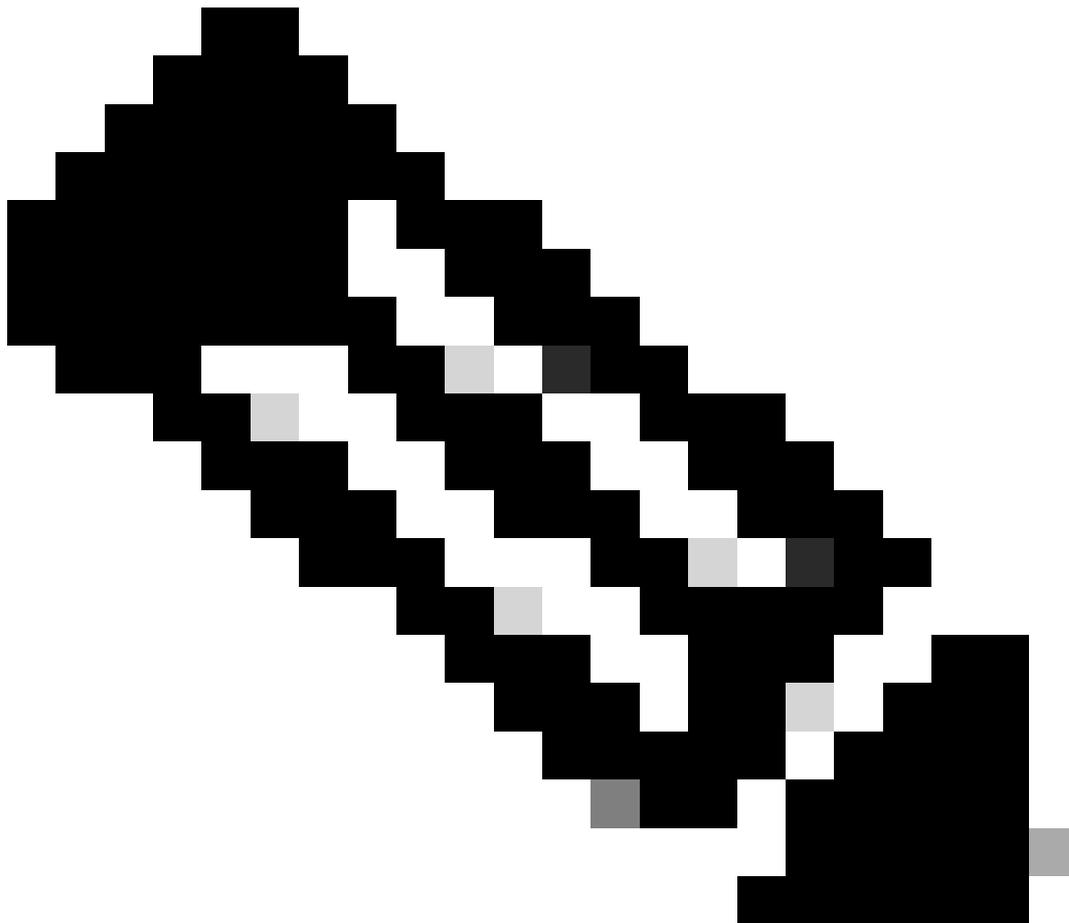
Enable External User ?

AAA Attribute

AAA Attribute  
Cisco-AVPair

Reset to Default

Update



Nota: El servidor ISE utiliza el atributo Cisco-AVPair en el servidor, por lo que la

---

configuración del paso 3 es válida.

---

Desplácese hacia abajo para ver la sección de configuración AAA Server(s). Configure la dirección IP del servidor ISE en el paso 1 y la clave secreta compartida configurada en el paso 3.

A continuación, haga clic en Ver configuración avanzada.

▼ AAA Server(s)

### Primary AAA Server

IP Address

██████████



Shared Secret

.....

SHOW

Info

[View Advanced Settings](#)

Update

### Secondary AAA Server

IP Address

██████████



Shared Secret

.....

SHOW

Info

[View Advanced Settings](#)

Update

Compruebe que la opción RADIUS esté seleccionada y haga clic en el botón Update (Actualizar) en ambos servidores.

∨ 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

### Secondary AAA Server

IP Address

██████████



Shared Secret

\*\*\*\*\*

SHOW

Info

Hide Advanced Settings

RADIUS

TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

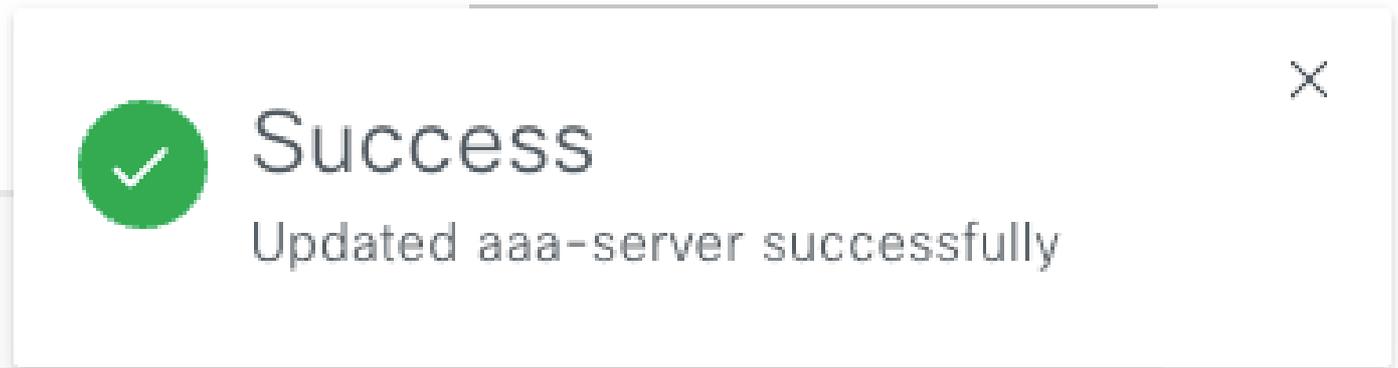
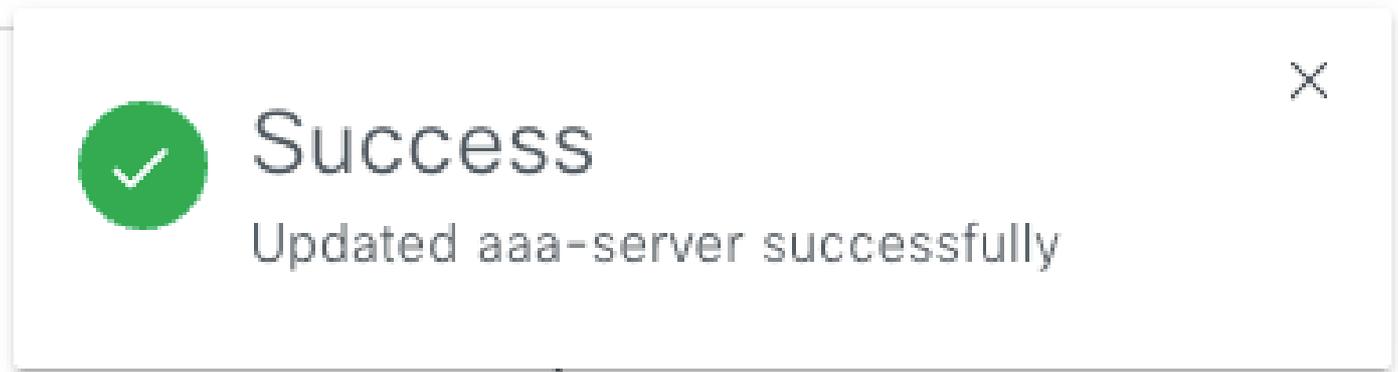
Timeout (seconds)

4

Update

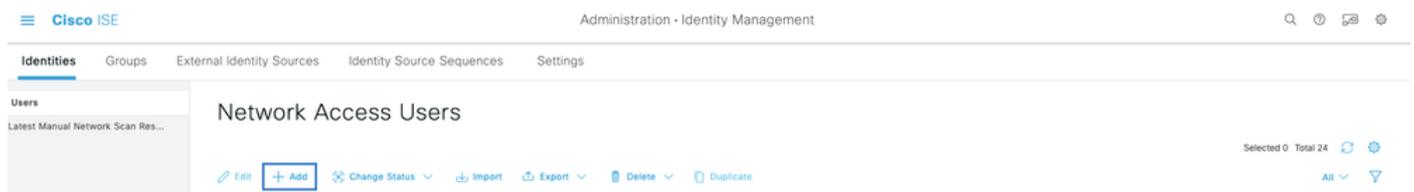
Update

Debe ver un mensaje de Confirmación para cada uno.



Ahora puede iniciar sesión con cualquier identidad de ISE creada en el menú de ISE > Administración > Gestión de identidad > Identidades > Usuarios.

En caso de que no haya creado ninguno, inicie sesión en ISE, navegue hasta la ruta anterior y agregue un nuevo usuario de acceso a la red.



## Verificación

Cargar la GUI de Cisco DNA Center e inicie sesión con un usuario de las identidades de ISE.



# Cisco DNA Center

The bridge to possible

✓ Success!

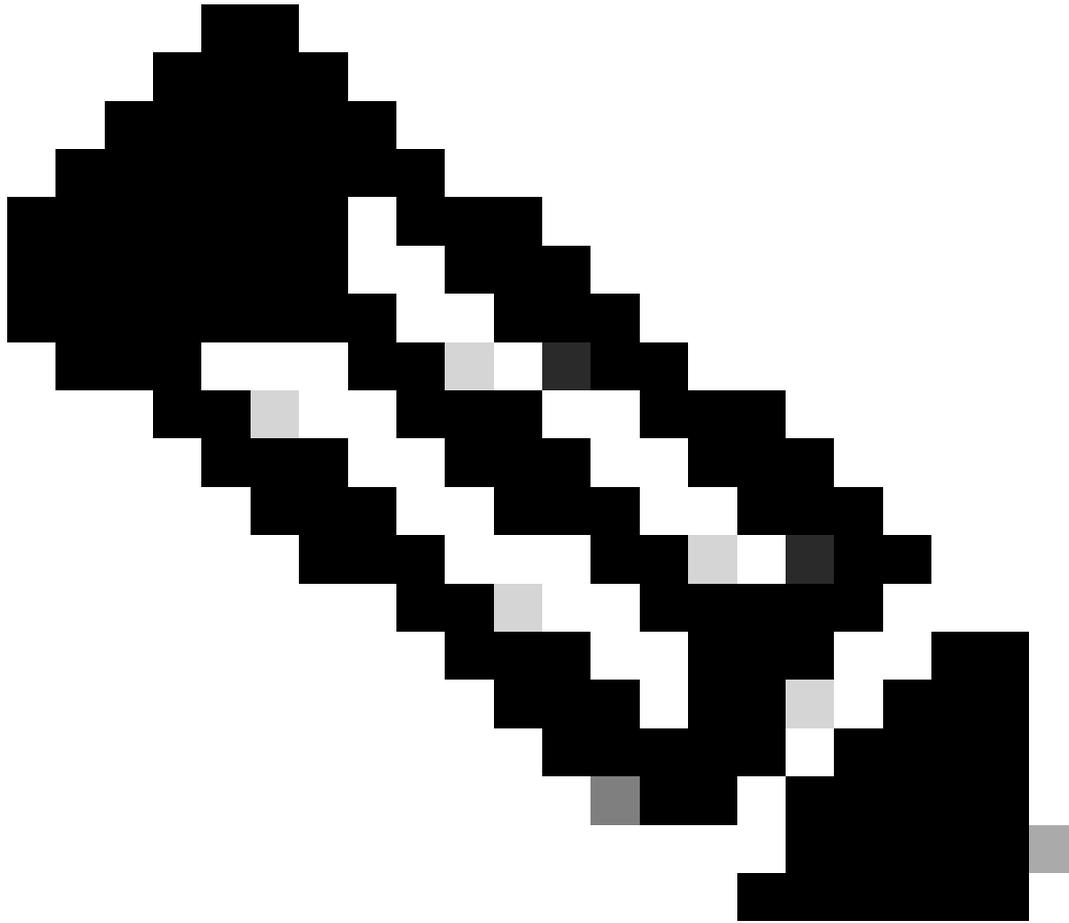
Username

test

Password

.....

Log In



Nota: cualquier usuario con identidades ISE puede iniciar sesión ahora. Puede agregar más granularidad a las reglas de autenticación en el servidor ISE.

---

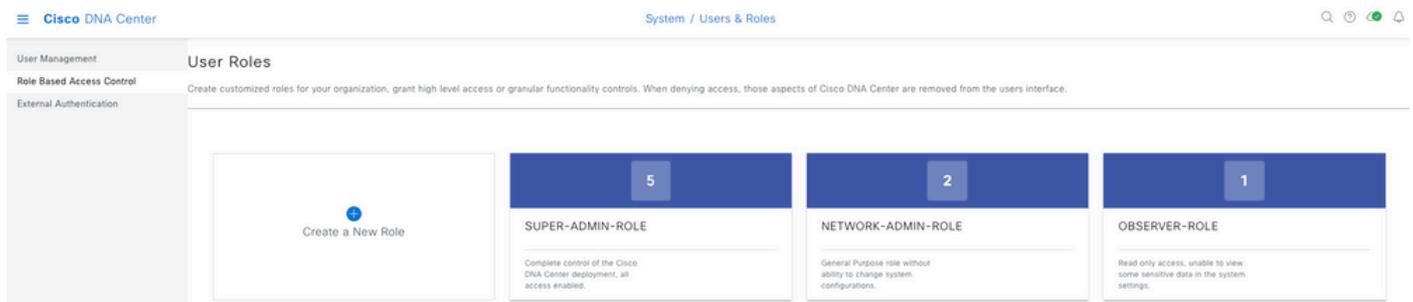
Una vez que el inicio de sesión se haya realizado correctamente, el nombre de usuario se muestra en la GUI del Cisco DNA Center

## Welcome, test

Pantalla de bienvenida

### Más funciones

Puede repetir estos pasos para cada rol en Cisco DNA Center, como opción predeterminada que tenemos: SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE y OBSERVER-ROLE.



En este documento utilizamos el ejemplo de rol SUPER-ADMIN-ROLE; sin embargo, puede configurar un perfil de autorización en ISE para cada rol en Cisco DNA Center, la única consideración es que el rol configurado en el paso 3 debe coincidir exactamente (distingue entre mayúsculas y minúsculas) con el nombre del rol en Cisco DNA Center.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).