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

Contenido

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.

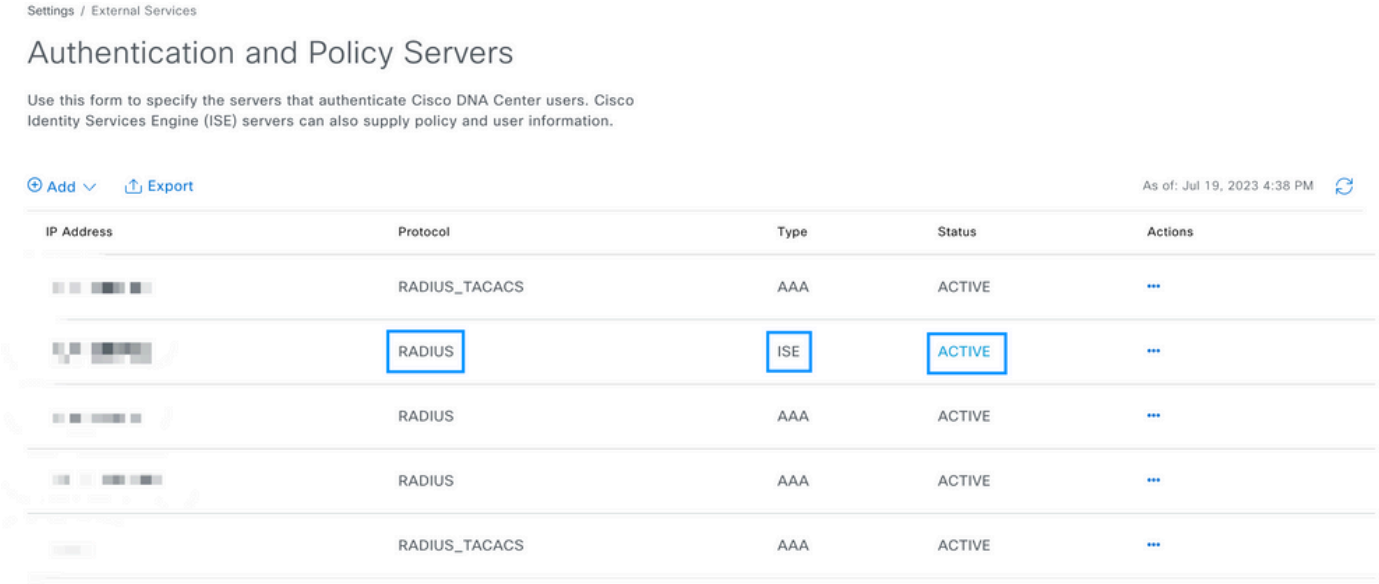
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

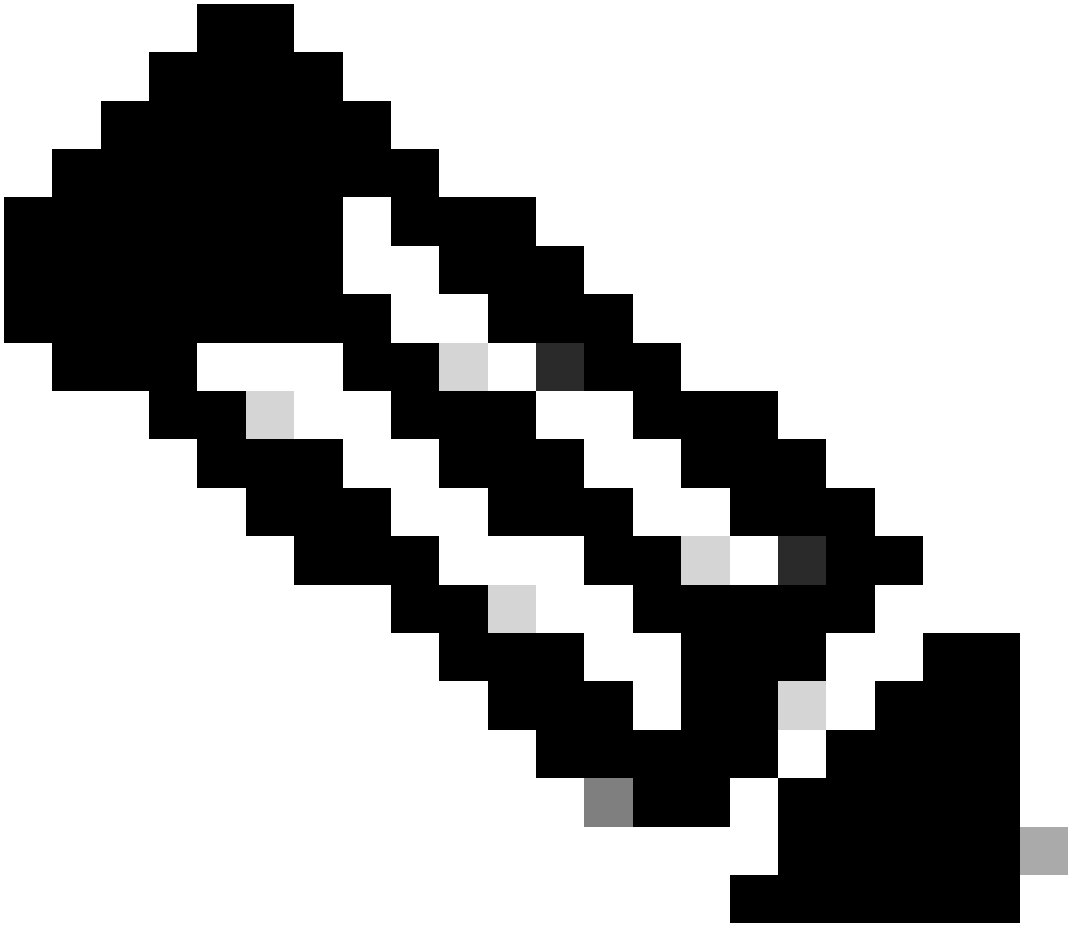
Configurar

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

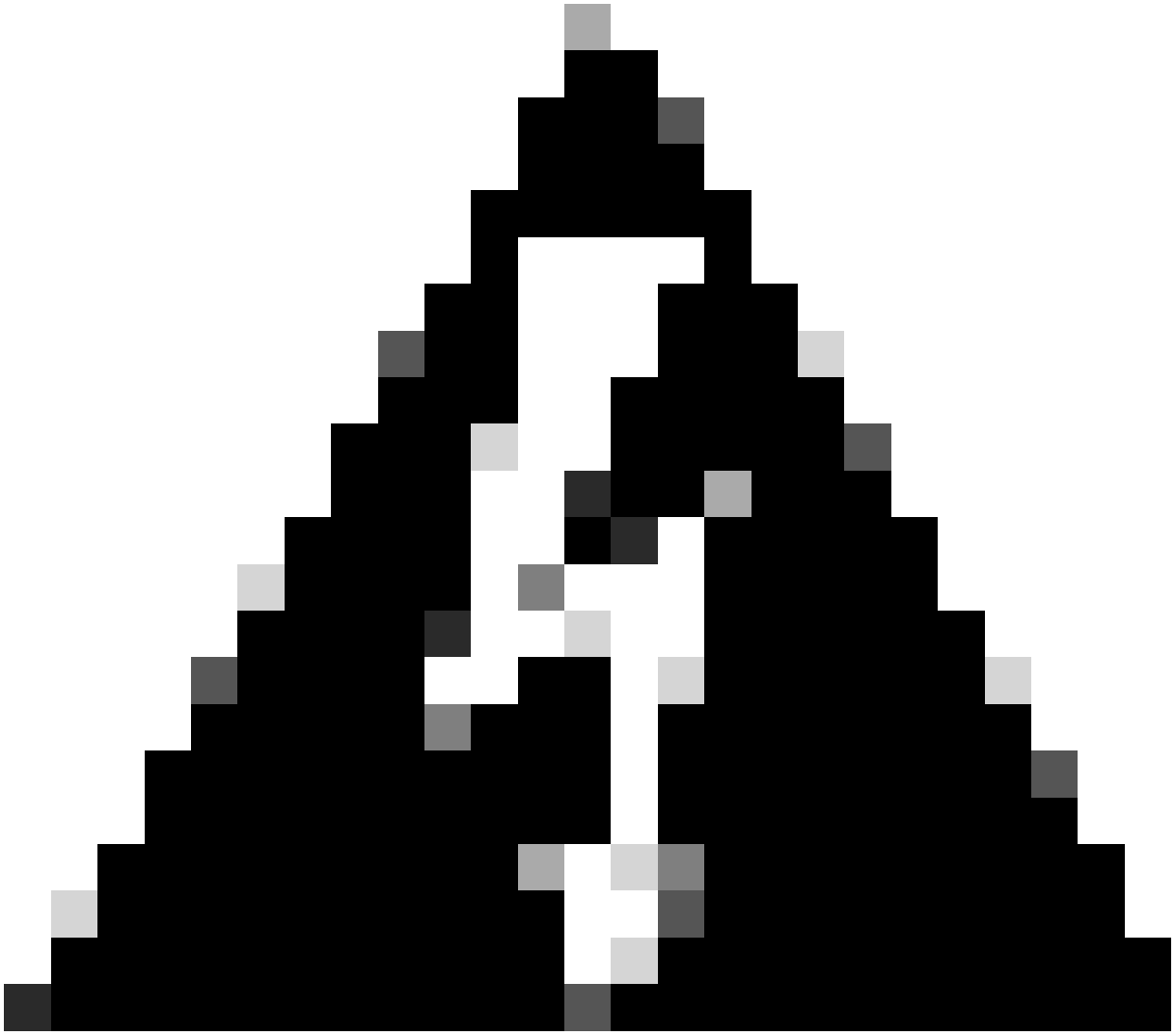
Authentication and Policy Servers.

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





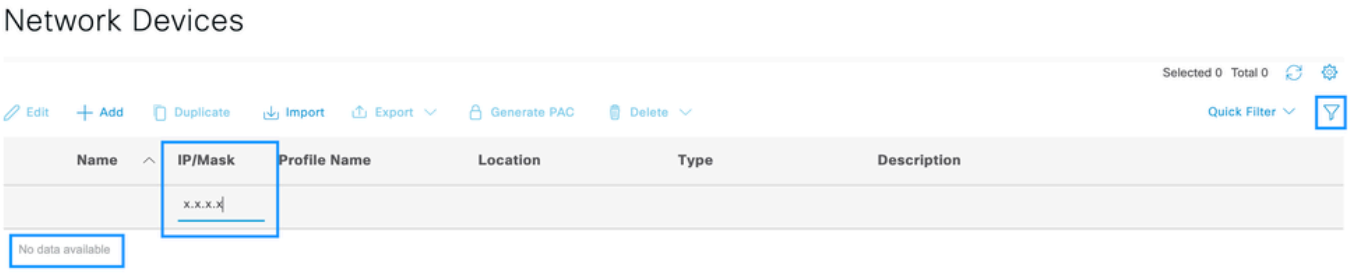
Nota: El tipo de protocolo RADIUS_TACACS funciona para este documento.



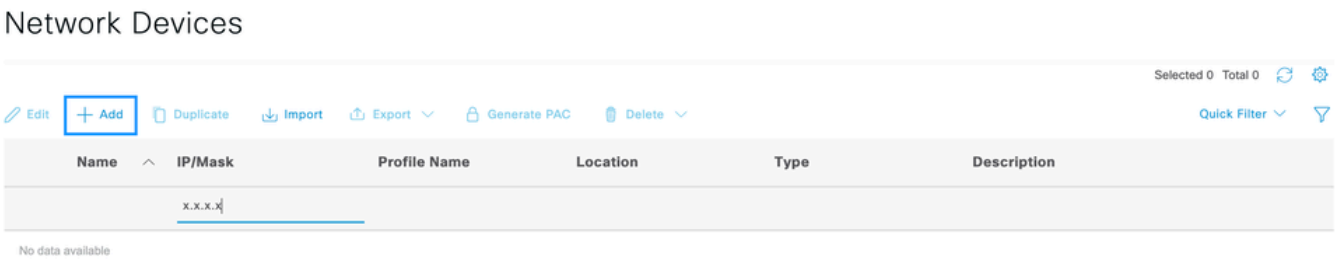
Advertencia: en caso de que el servidor ISE no esté en estado activo, primero debe corregir la integración.

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.

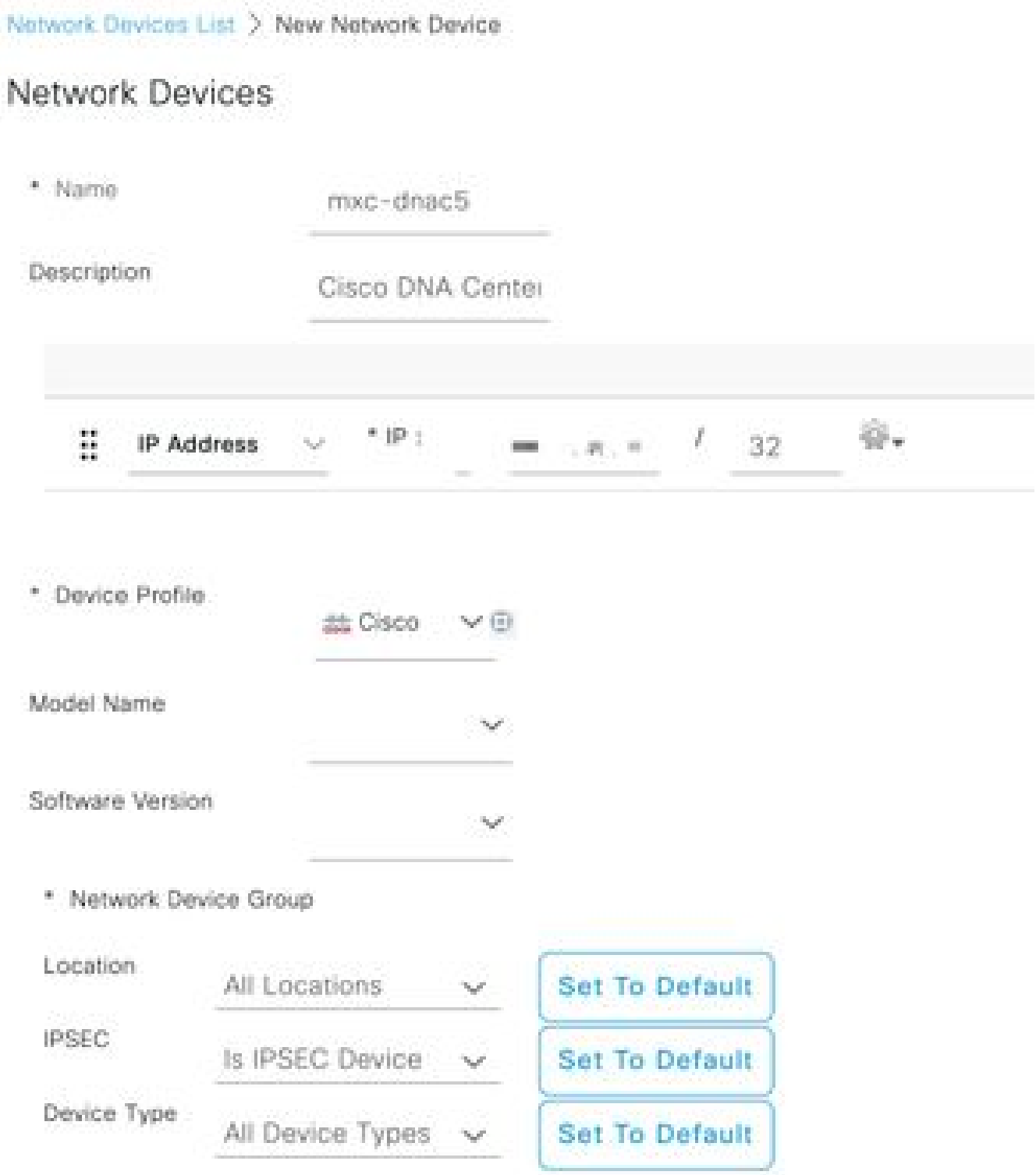
Si falta la entrada, debe ver el mensaje No hay datos disponibles.



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



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.



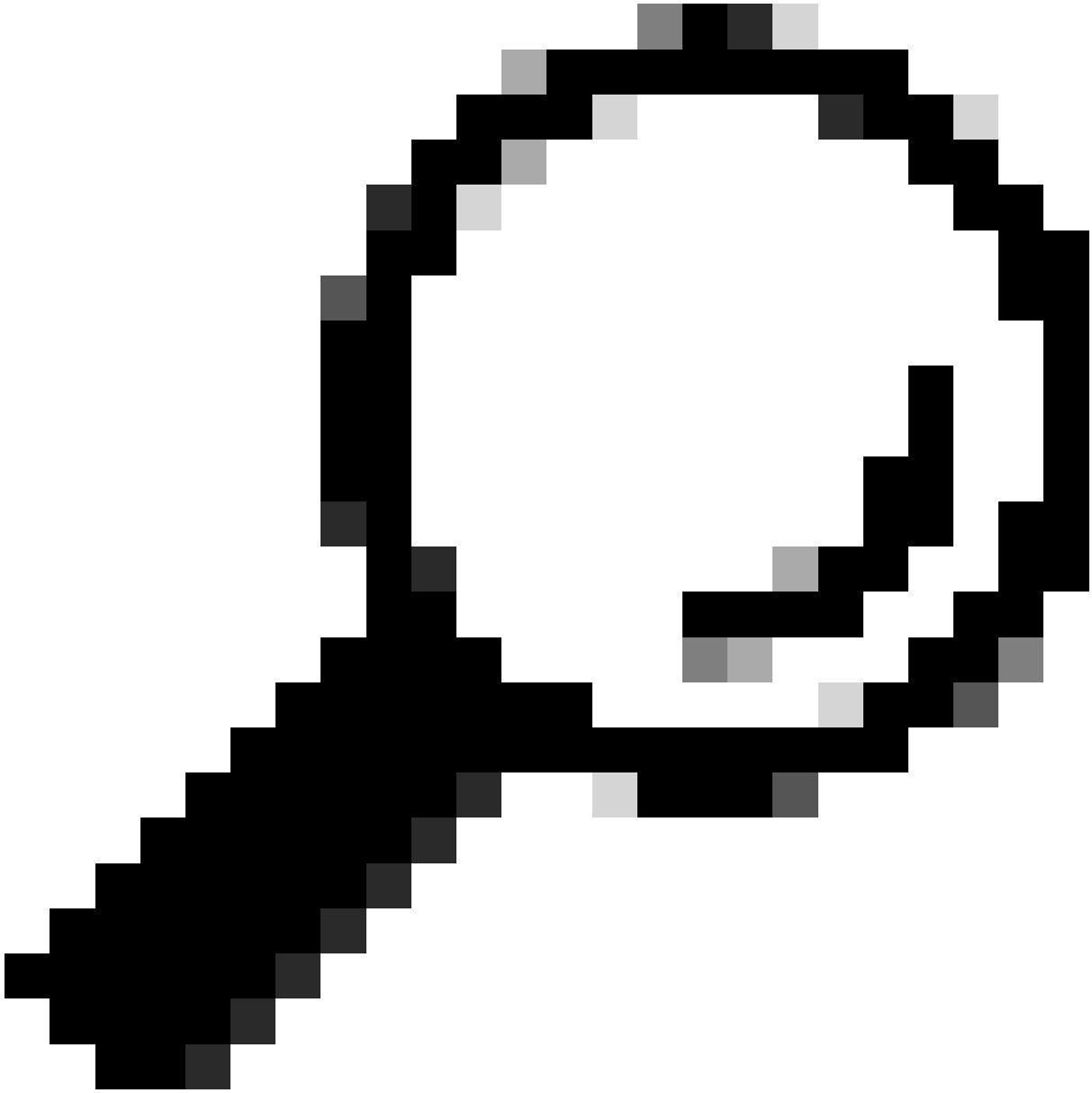
Desplácese hacia abajo y habilite RADIUS Authentication Settings haciendo clic en su casilla de verificación y configure un Shared Secret.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret ••••••••• Show

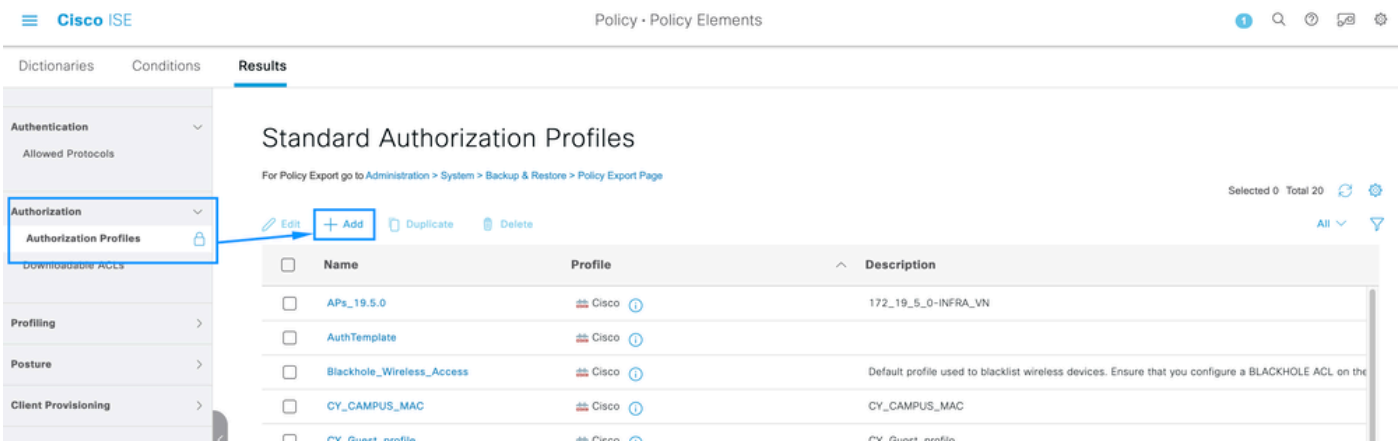


Sugerencia: este secreto compartido se necesitará más adelante, así que guárdelo en otro lugar.

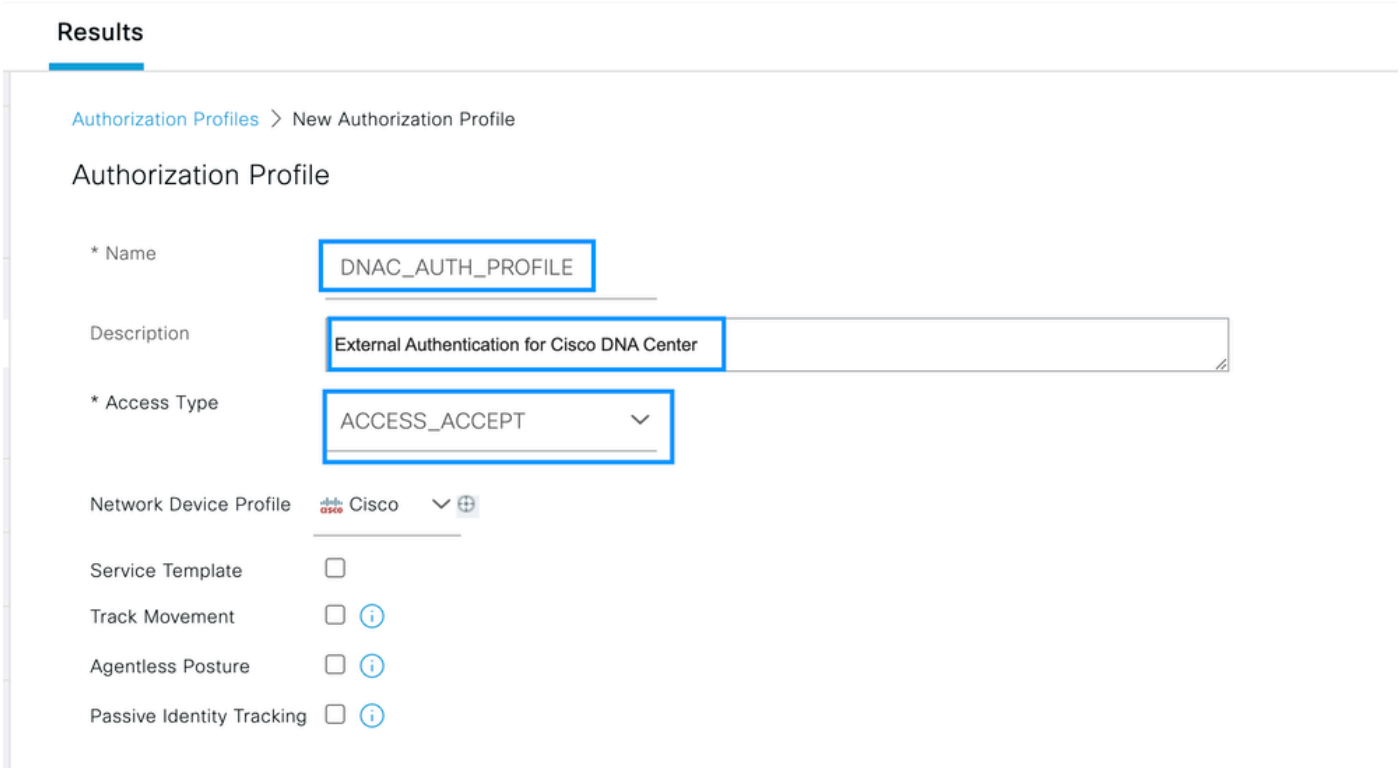
Solo entonces, haga clic en Submit.

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 ACCES_ACCEPT.

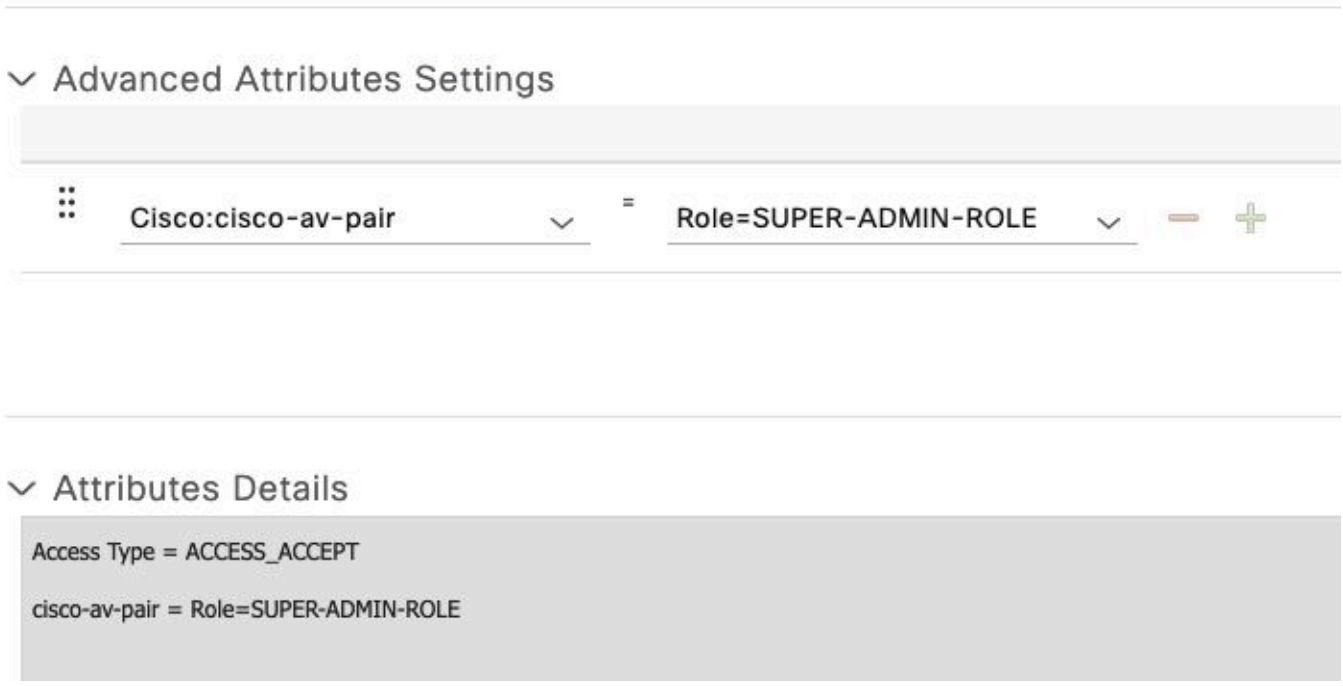


Desplácese hacia abajo y configure Advanced Attributes Settings (Parámetros de atributos avanzados).

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

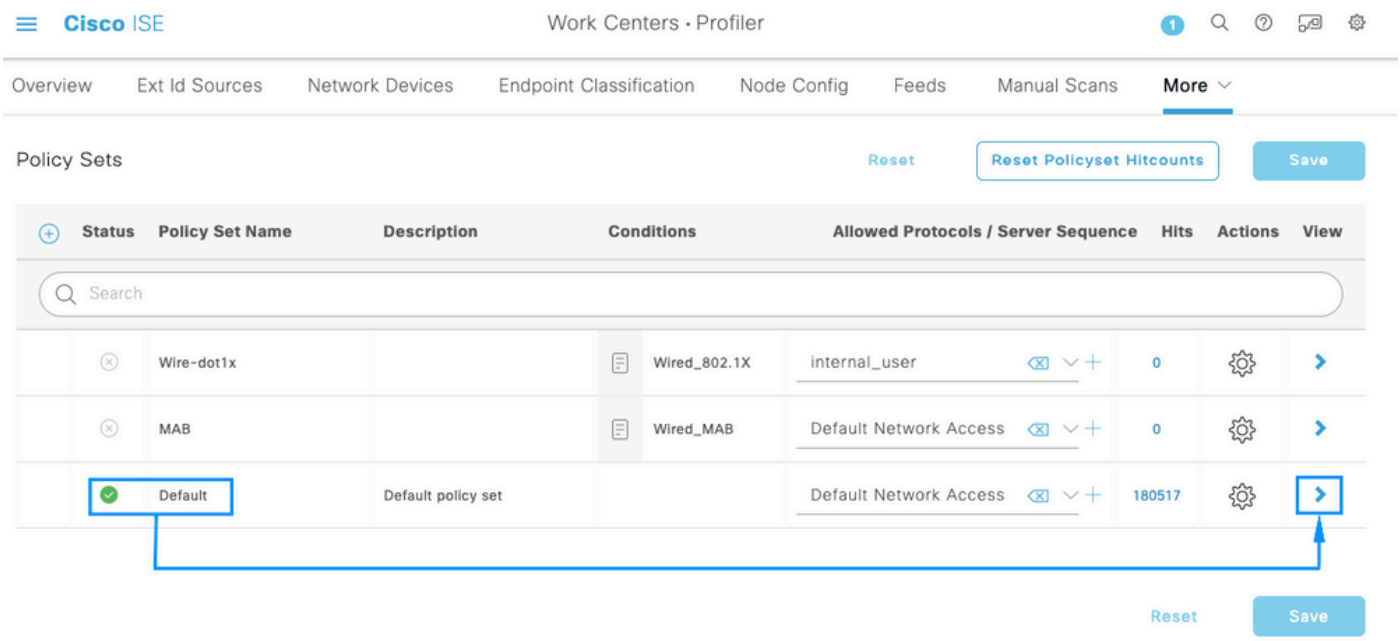
En la columna derecha, escriba manualmente Role=SUPER-ADMIN-ROLE.

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

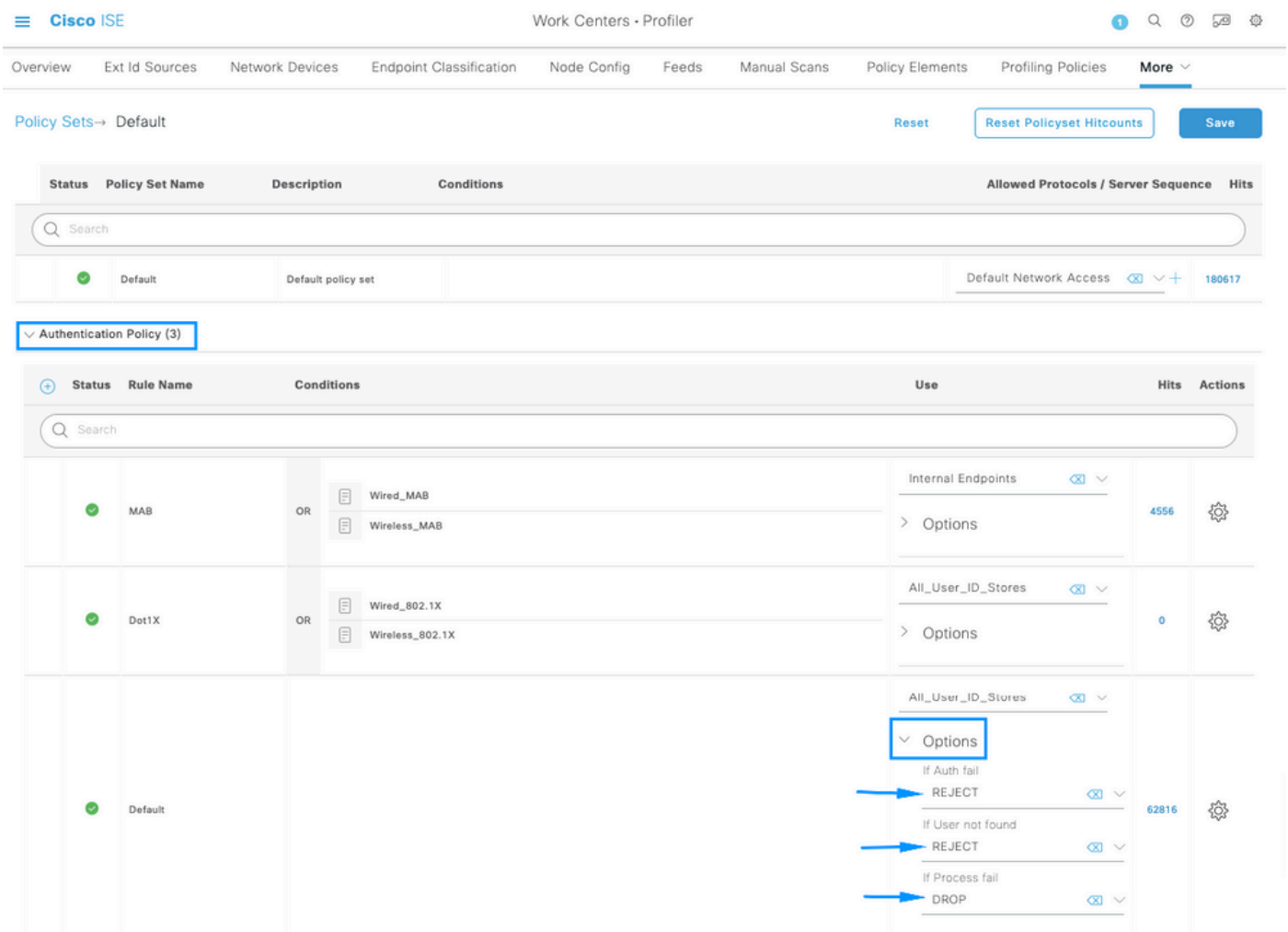


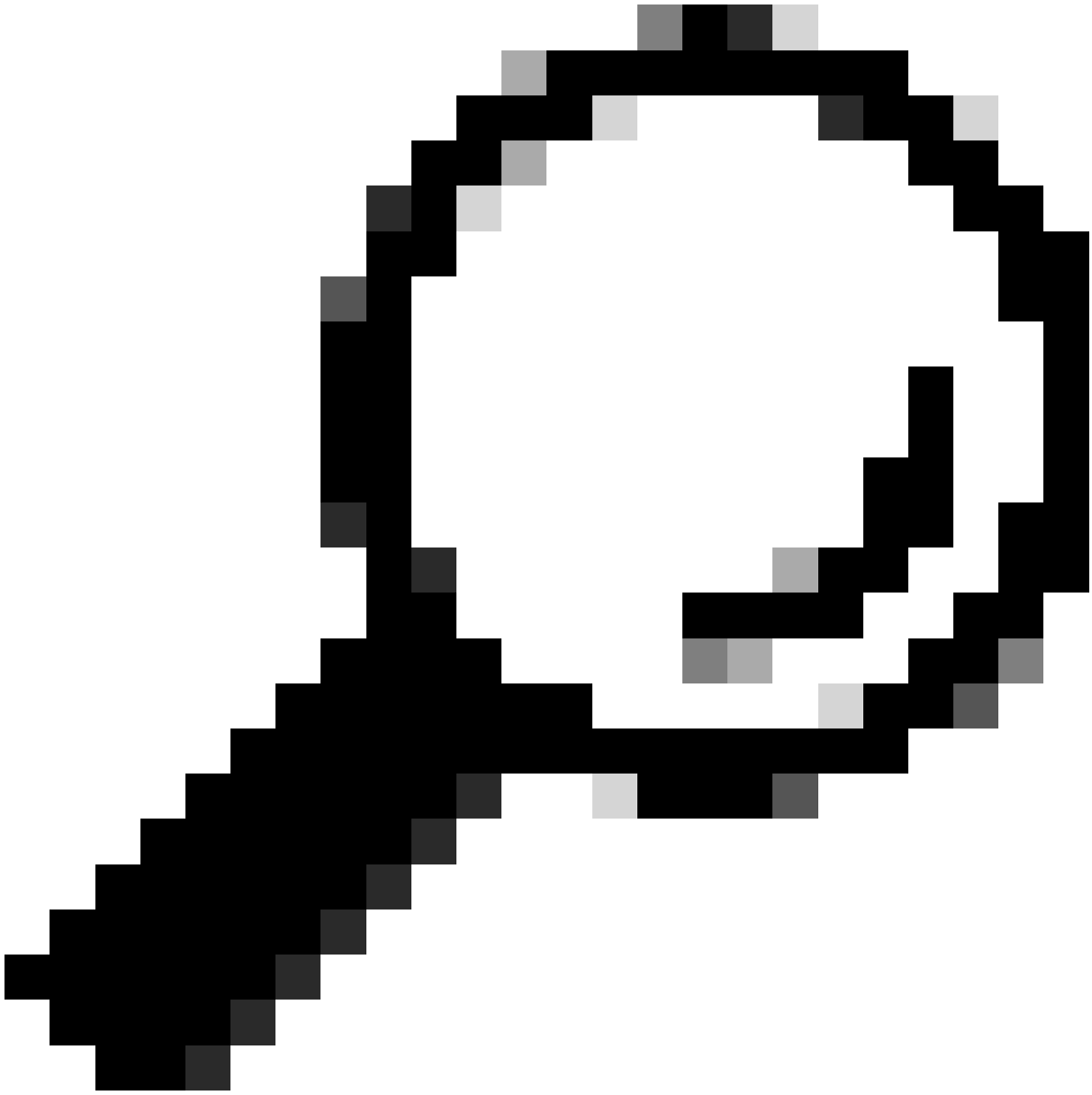
Paso 4. En el servidor ISE, navegue hasta Centros de trabajo > Profiler > Conjuntos de políticas, para configurar la política de autenticación y autorización.

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



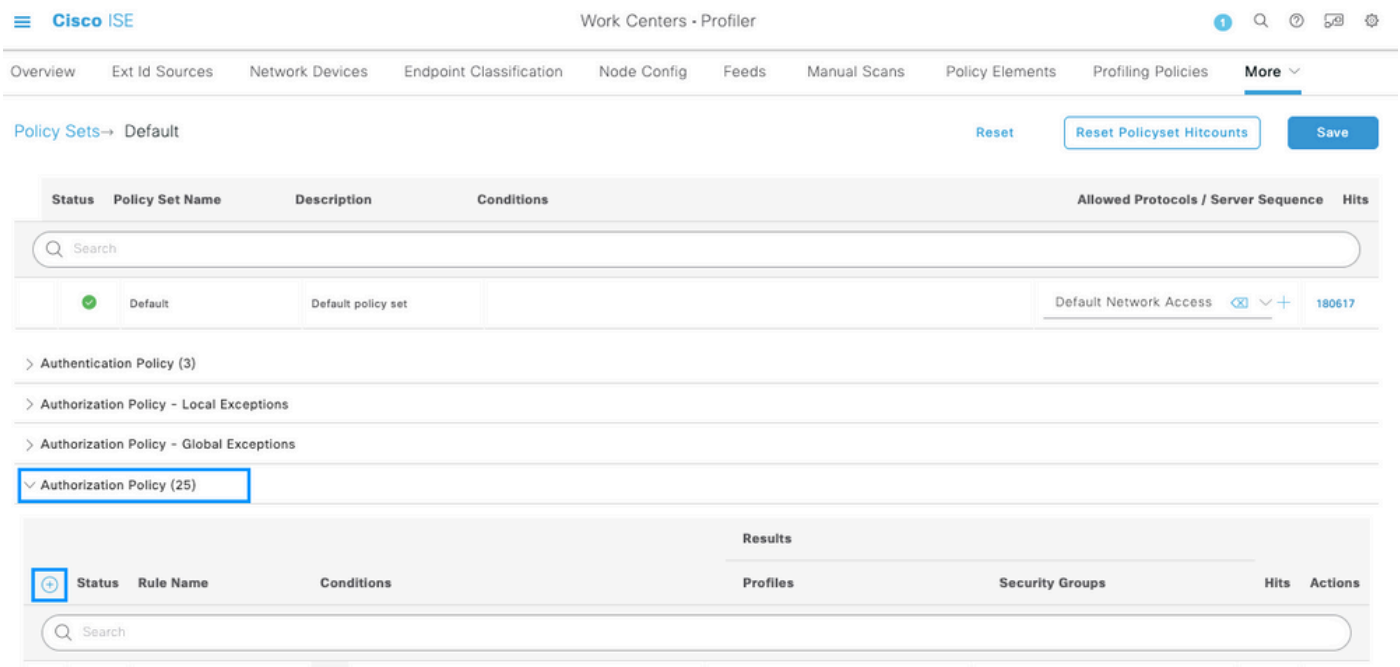
Dentro del Conjunto de políticas predeterminadas, expanda la Política de autenticación y en la sección Predeterminado, expanda las Opciones y asegúrese de que coincidan con la siguiente configuración.



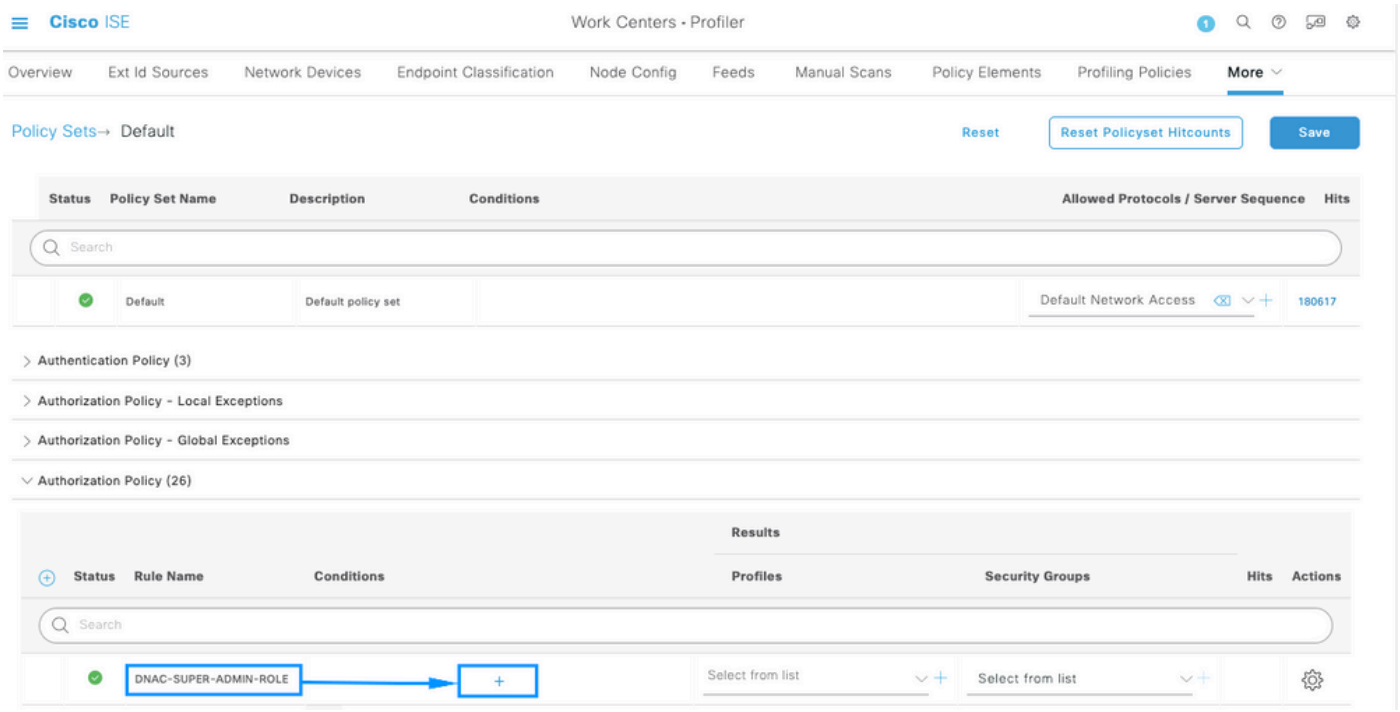


Sugerencia: el RECHAZO configurado en las 3 opciones también funciona

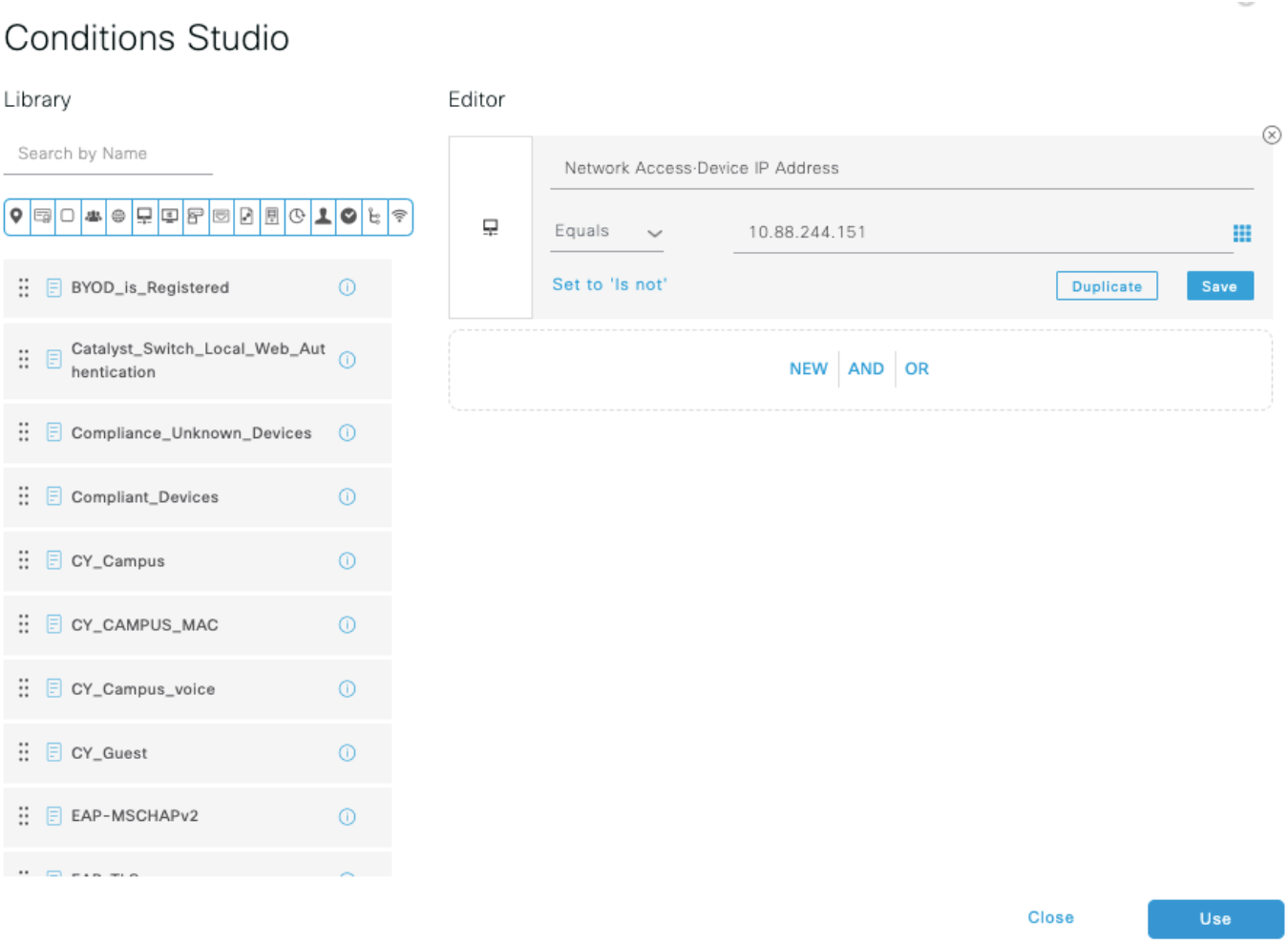
Dentro del Conjunto de directivas predeterminado, expanda la Directiva de autorización y seleccione el icono Agregar para crear una nueva Condición de autorización.



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

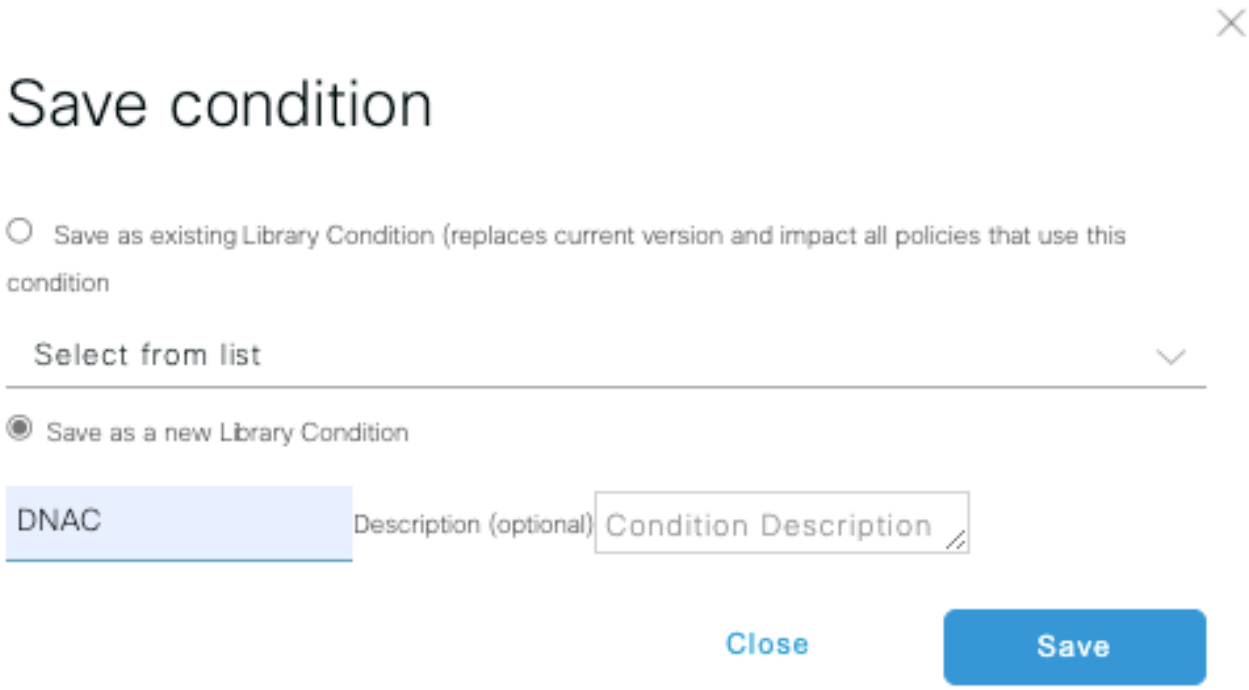


Como parte de la Condición, asóciela a la Dirección IP del Dispositivo de Red configurada en el Paso 2.

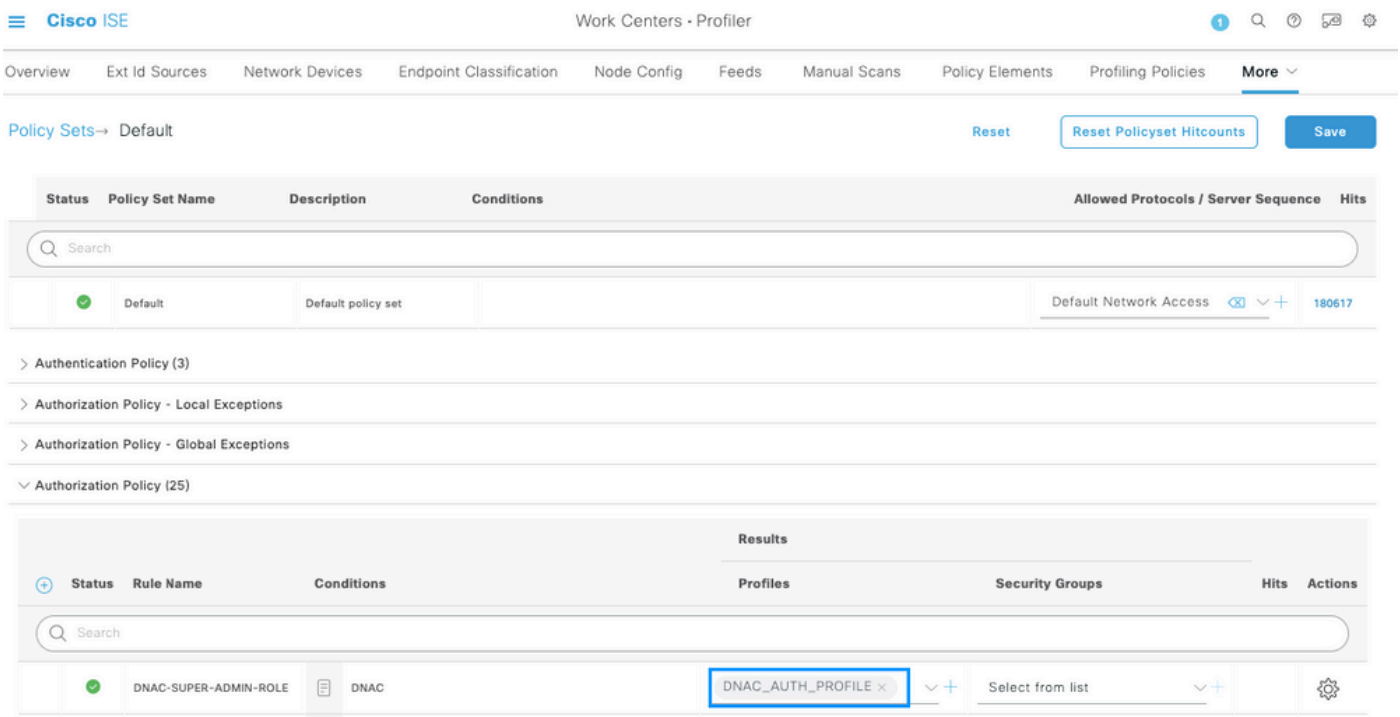


Haga clic en Guardar.

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



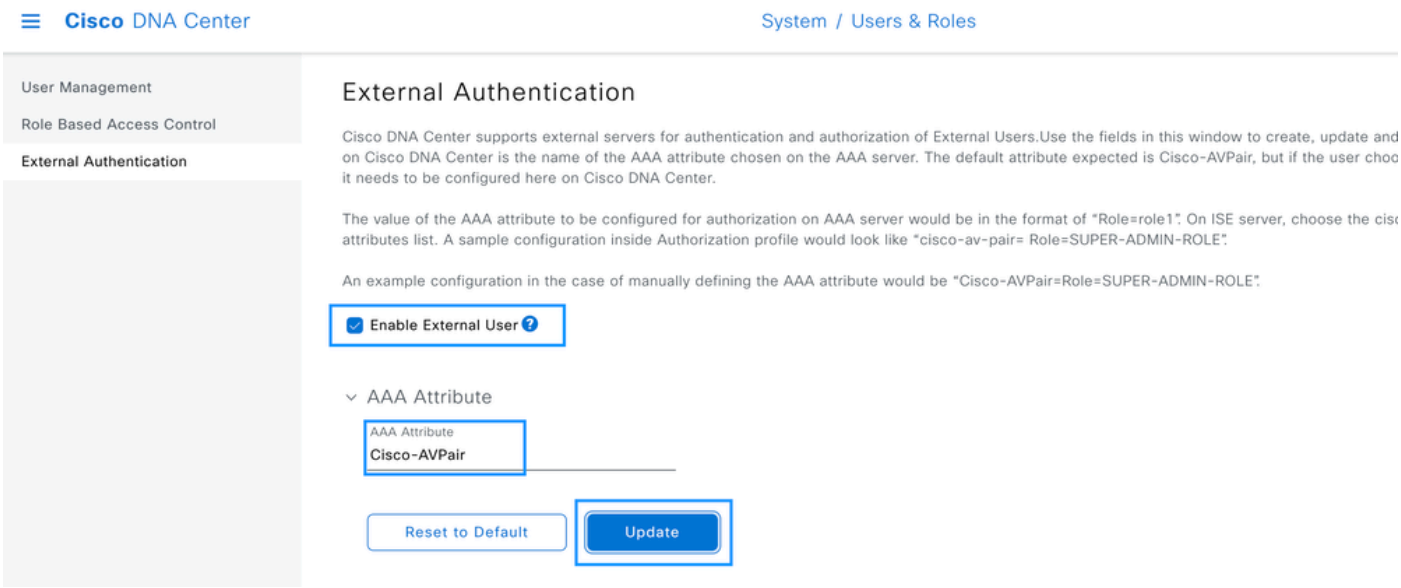
Por último, configure el perfil creado en el paso 3.

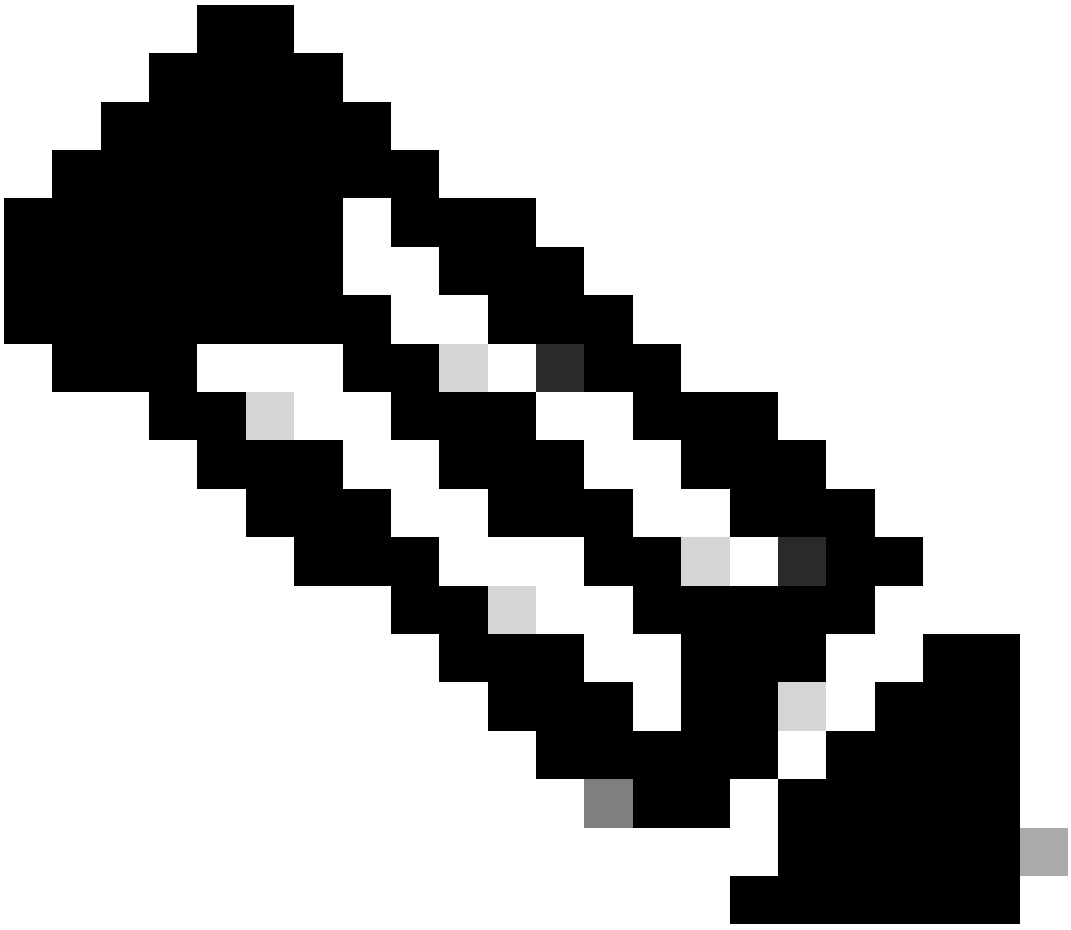


Haga clic en Guardar.

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

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



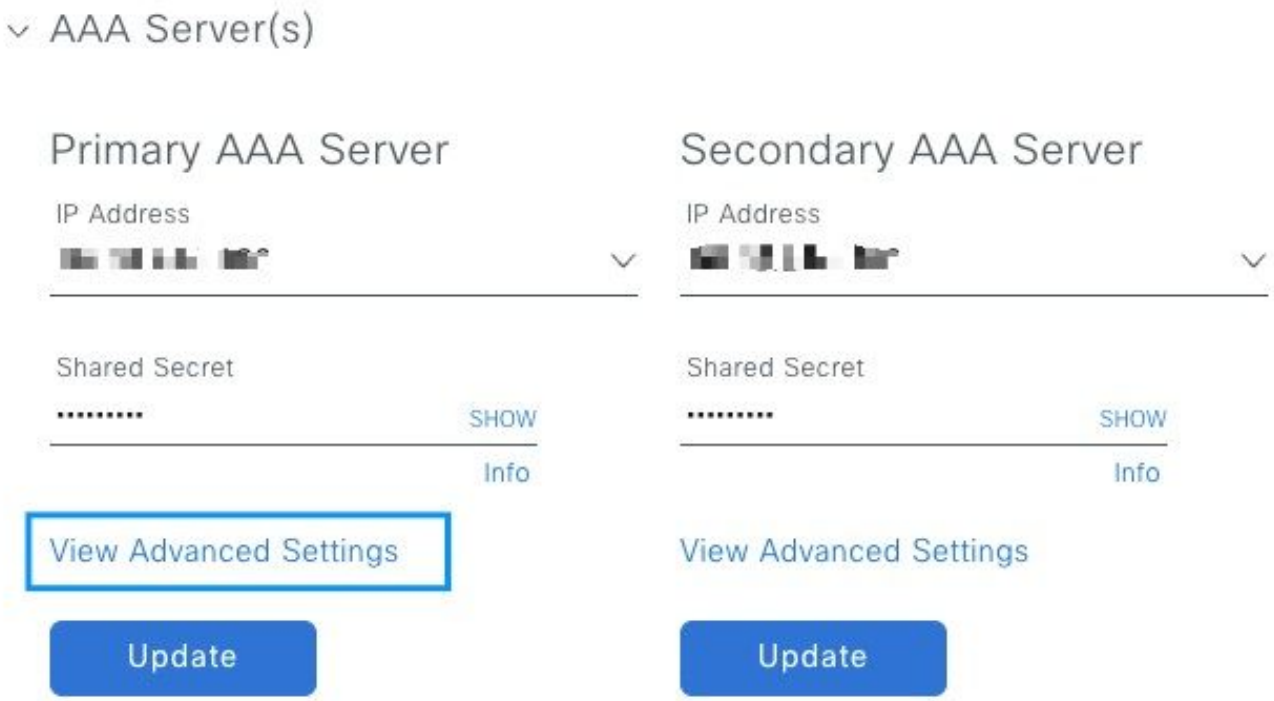


Nota: El servidor ISE utiliza el atributo Cisco-AVPair en el servidor, por lo que la

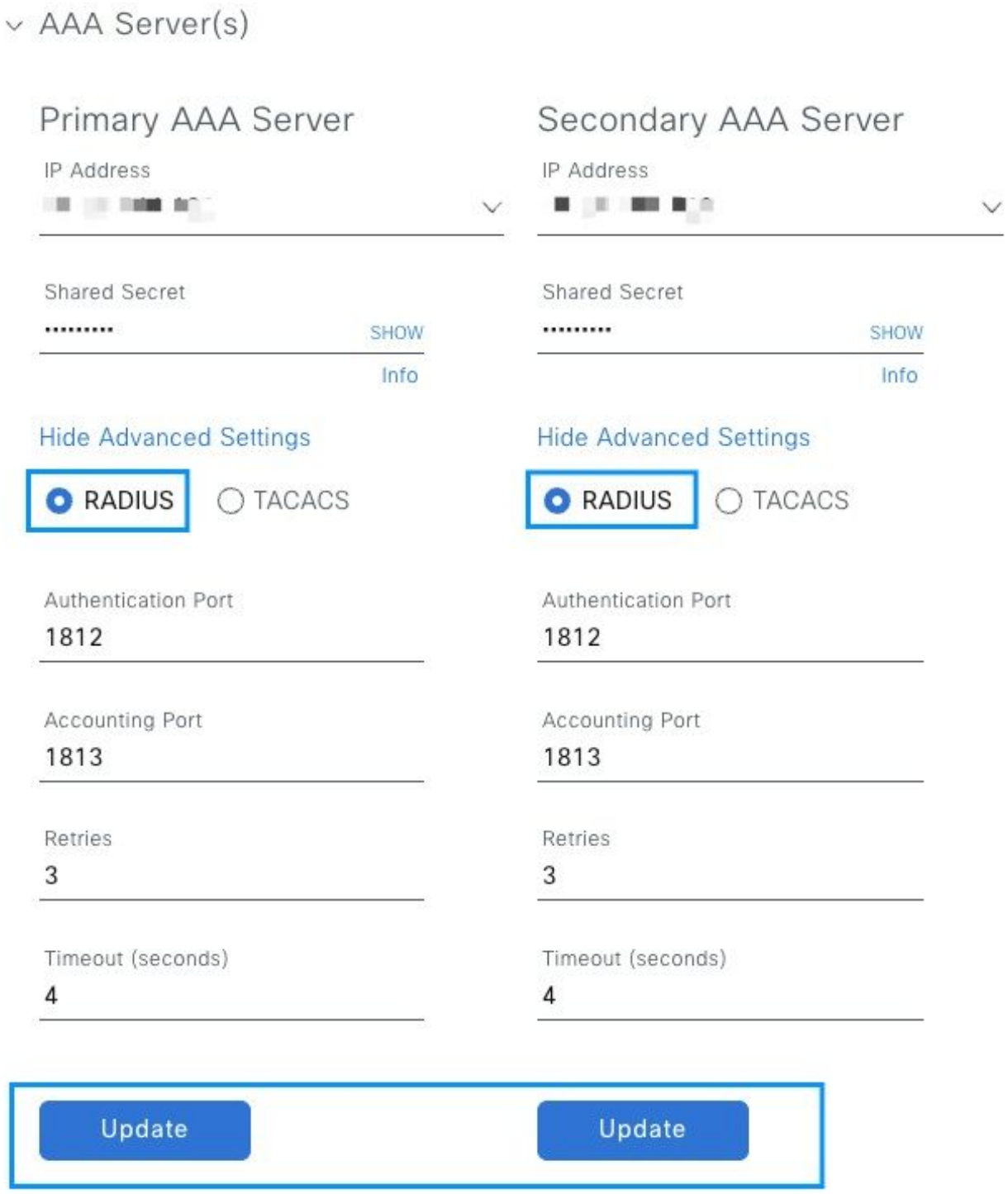
configuración del paso 3 es válida.

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.

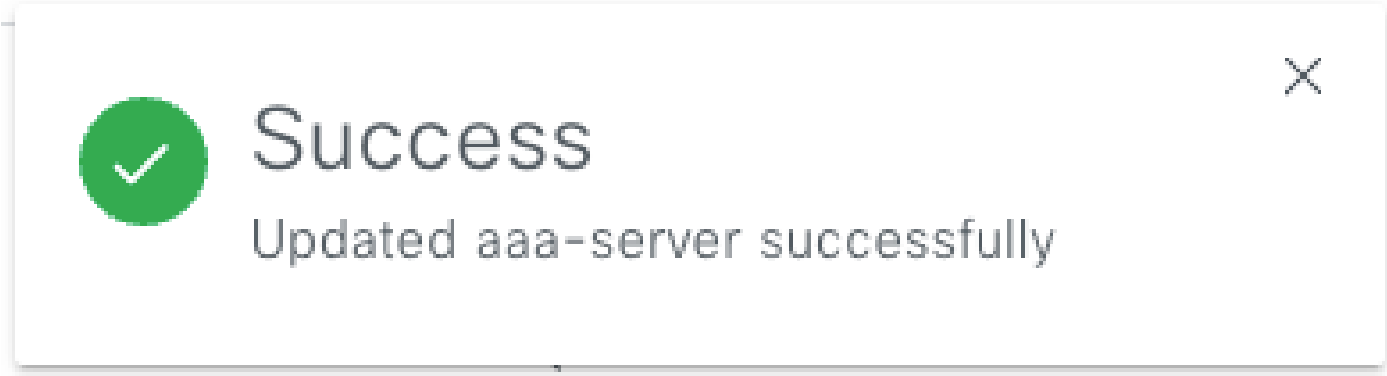
A continuación, haga clic en Ver configuración avanzada.

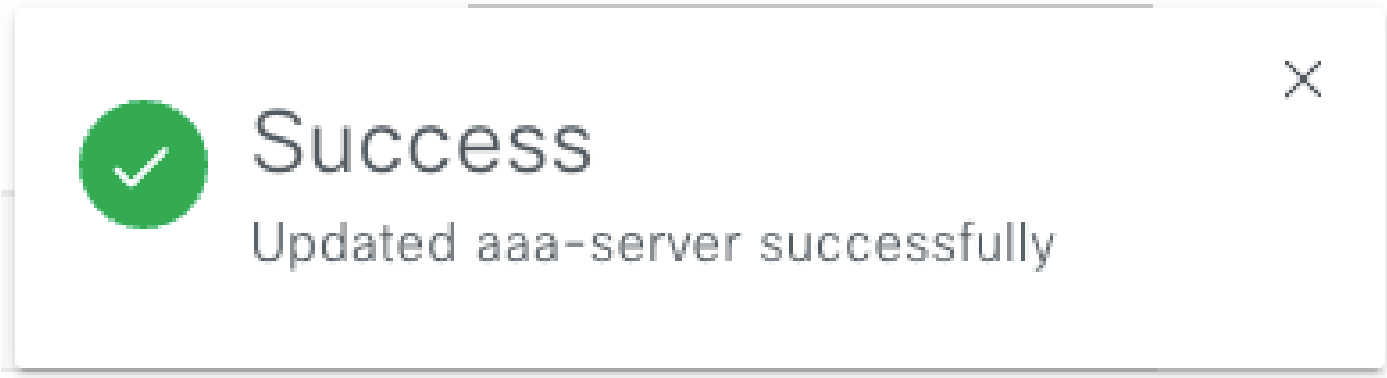


Compruebe que la opción RADIUS esté seleccionada y haga clic en el botón Update (Actualizar) en ambos servidores.



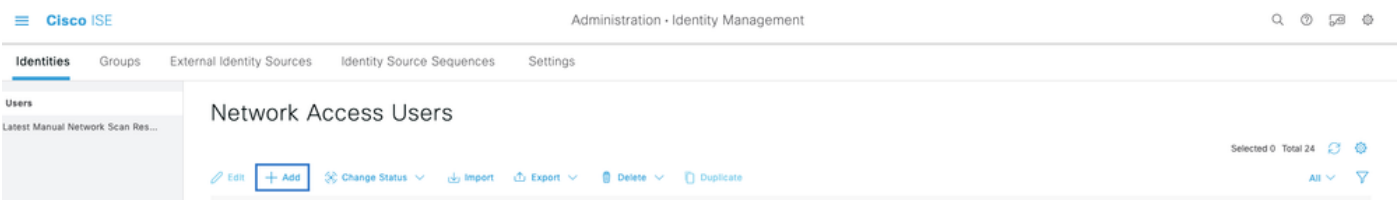
Debe ver un mensaje de Confirmación para cada uno.





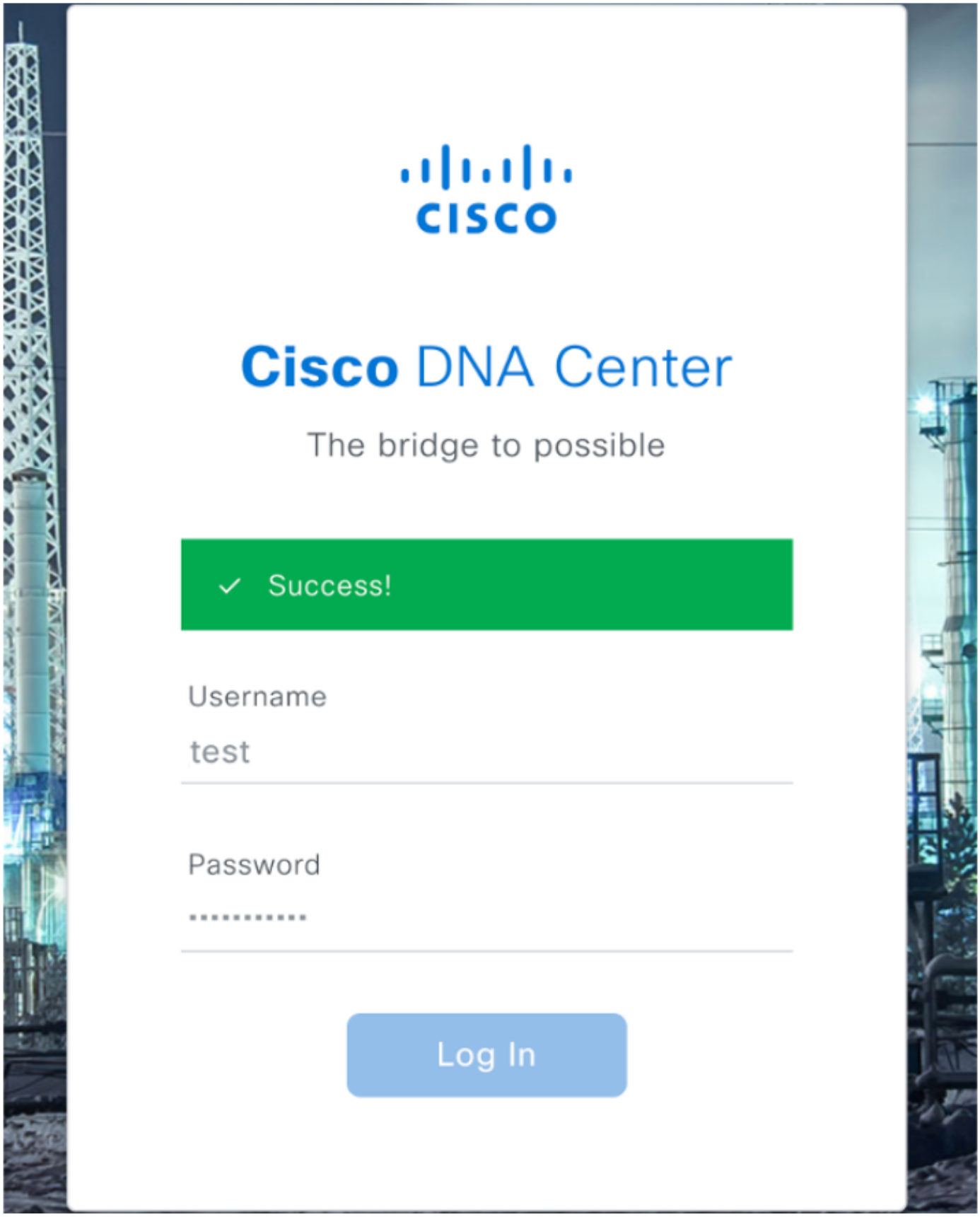
Ahora puede iniciar sesión con cualquier identidad de ISE creada en el menú de ISE > Administración > Gestión de identidad > Identidades > Usuarios.

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.

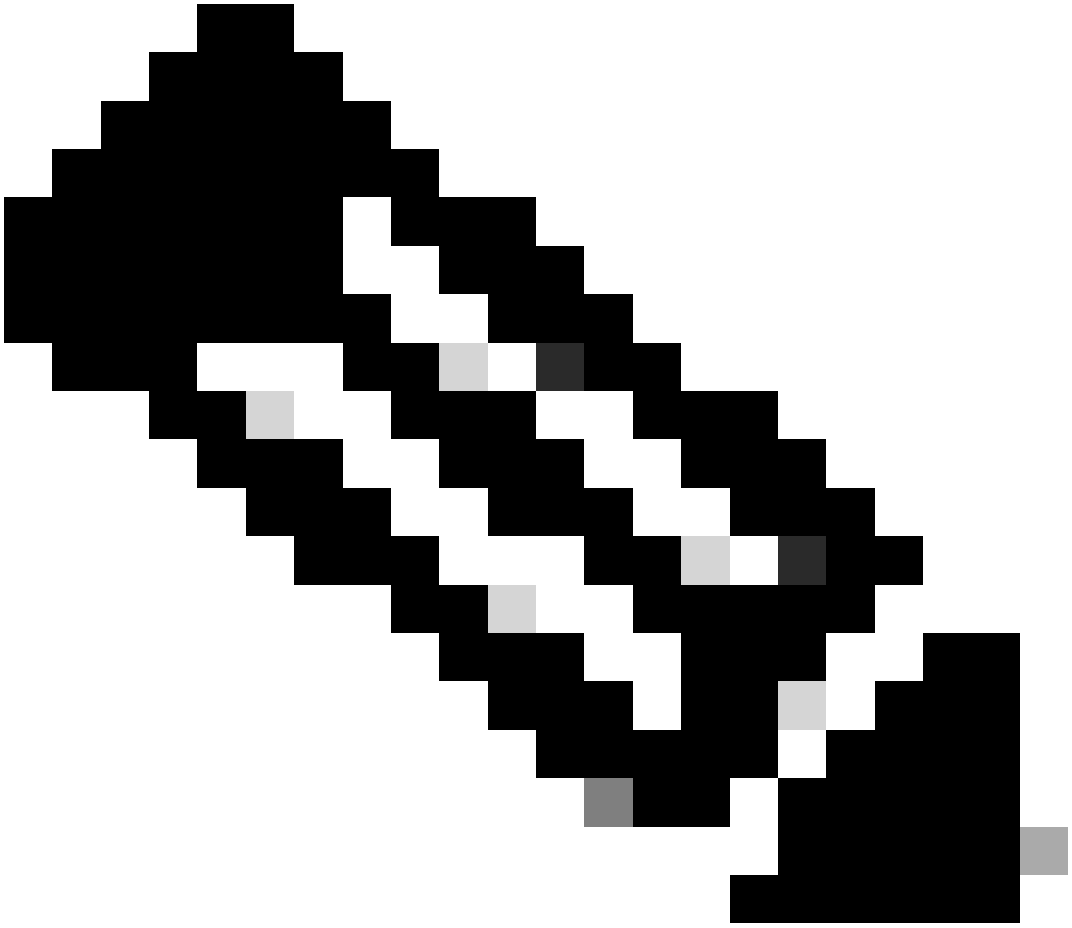


Verificación

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

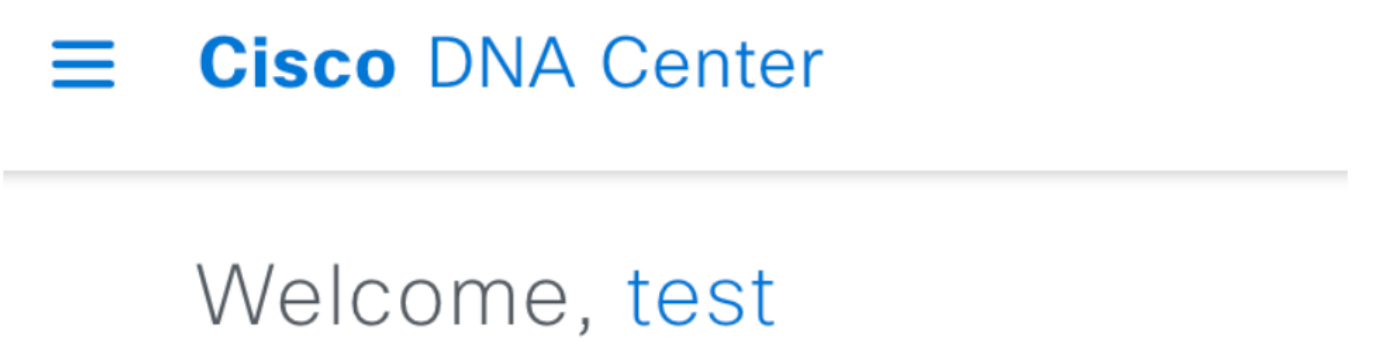


Inicio de sesión en DNA Center



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

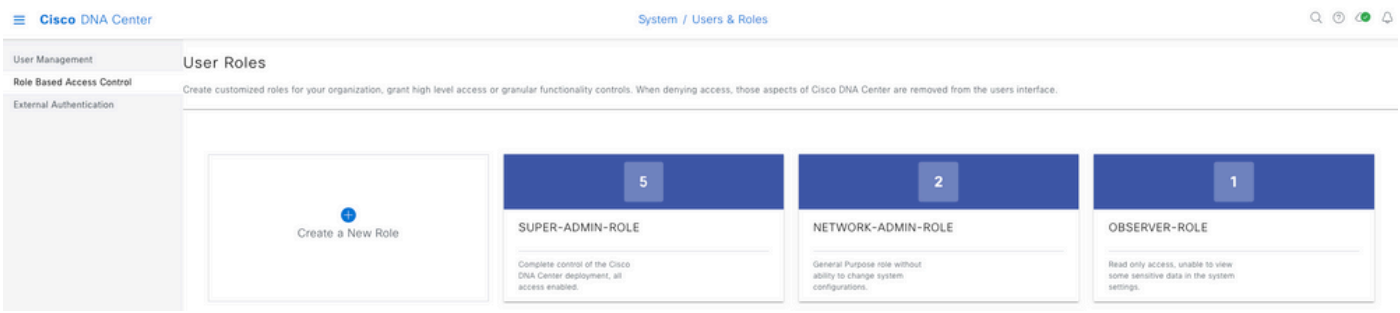
Una vez que el inicio de sesión se haya realizado correctamente, el nombre de usuario se muestra en la GUI del Cisco DNA Center



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).