Configuración de la autenticación externa SWA con ISE como servidor RADIUS

Contenido

Introducción

Este documento describe los pasos para configurar la autenticación externa en Secure Web Access (SWA) con Cisco ISE como servidor RADIUS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de Cisco Secure Web Appliance.
- Conocimiento de la configuración de las políticas de autenticación y autorización en ISE.
- Conocimiento básico de RADIUS.

Cisco recomienda que también tenga:

- Acceso a la administración de SWA e ISE.
- Versiones compatibles de WSA e ISE.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- SWA 14.0.2-012
- ISE 3.0.0

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.

Antecedentes

Cuando habilita la autenticación externa para los usuarios administrativos de su SWA, el dispositivo verifica las credenciales del usuario con un servidor LDAP (Protocolo ligero de acceso a directorios) o RADIUS como se especifica en la configuración de autenticación externa.

Topología de red

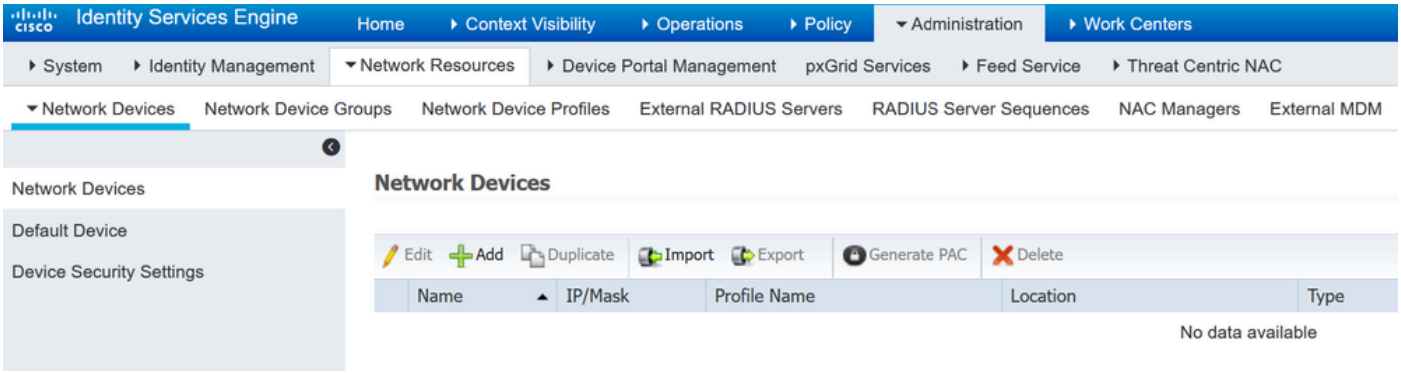
Diagrama de topología de red

Los usuarios administrativos acceden a SWA en el puerto 443 con sus credenciales. SWA verifica las credenciales con el servidor RADIUS.

Configurar

Configuración de ISE

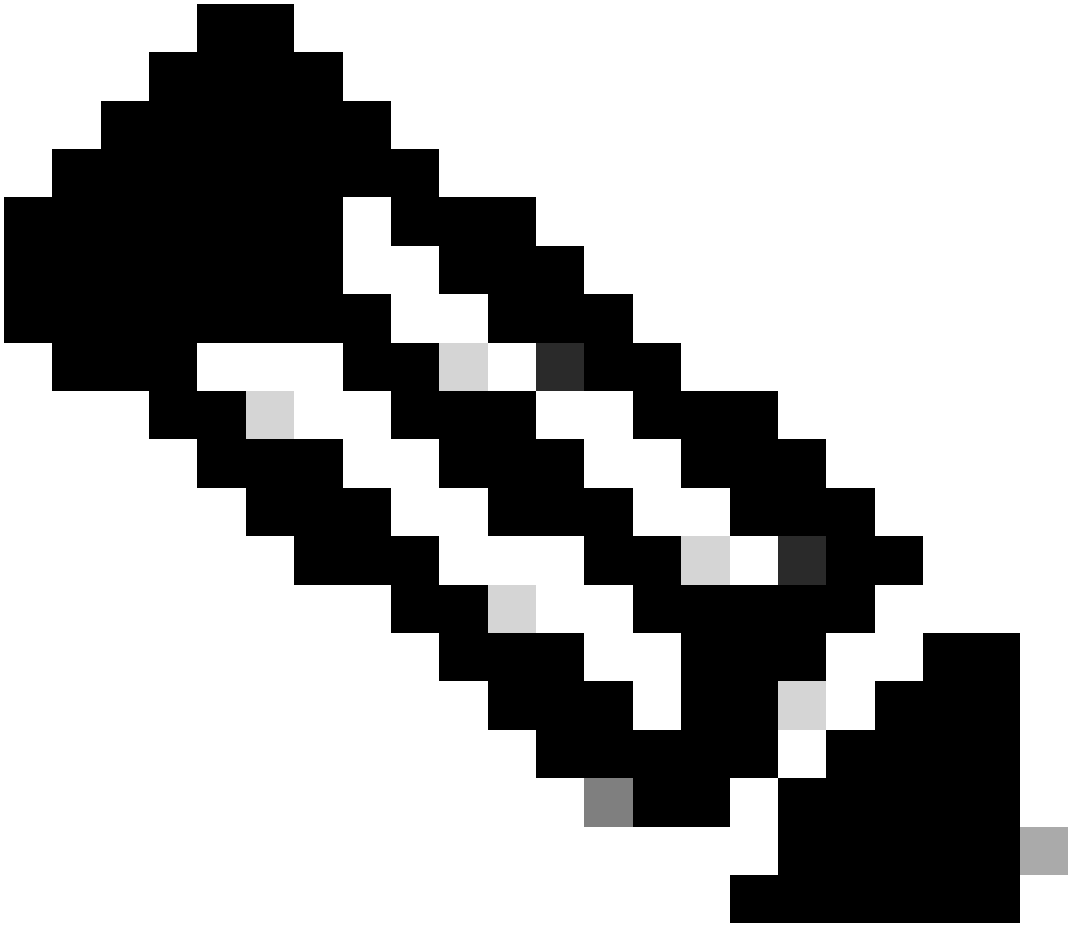
Paso 1. Agregue un nuevo dispositivo de red. Vaya a Administración > Recursos de red > Dispositivos de red > +Agregar.



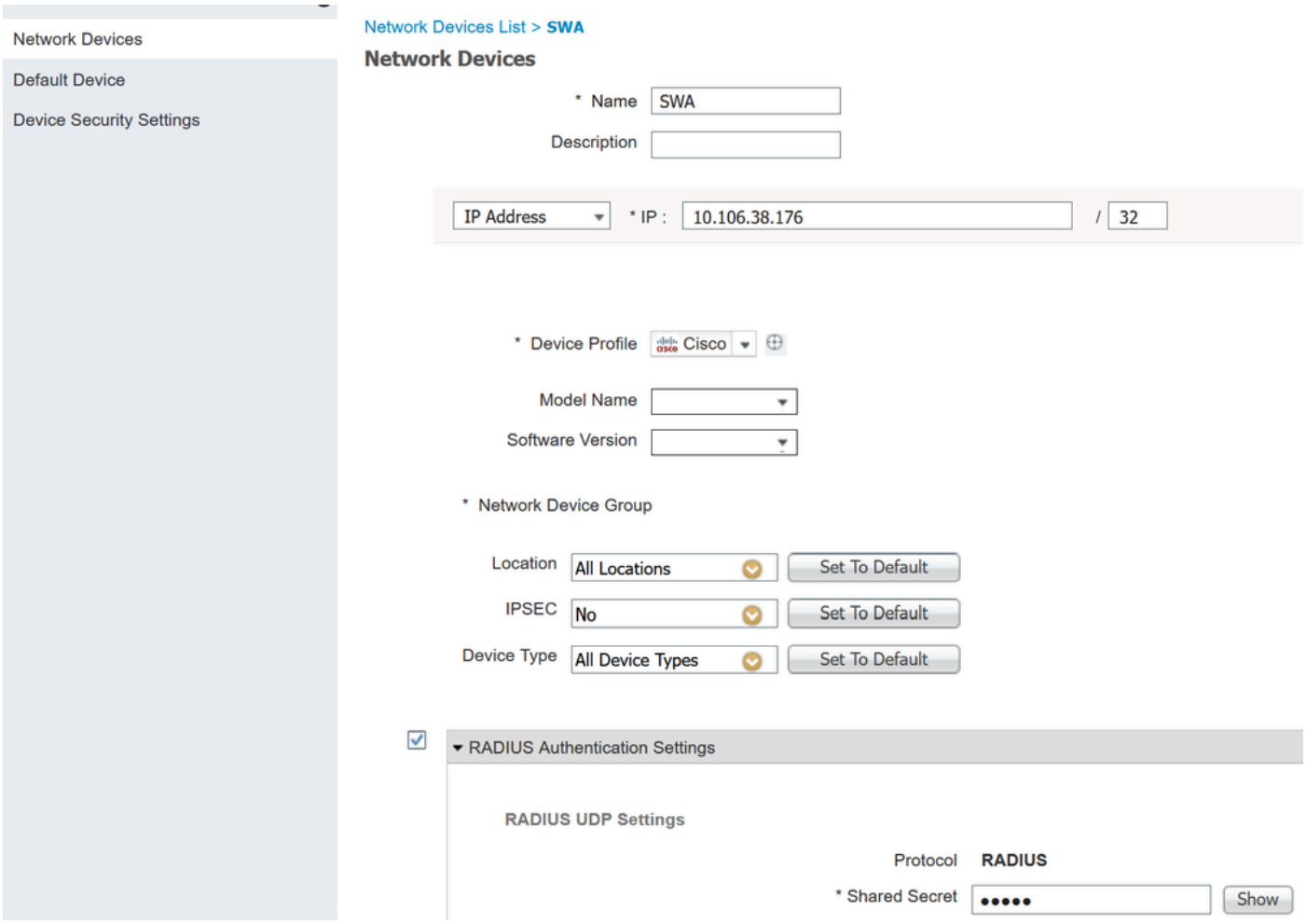
Agregar SWA como dispositivo de red en ISE

Paso 2. Asigne un Nombre al objeto de dispositivo de red e inserte la dirección IP SWA.

Marque la casilla de verificación RADIUS y defina un secreto compartido.

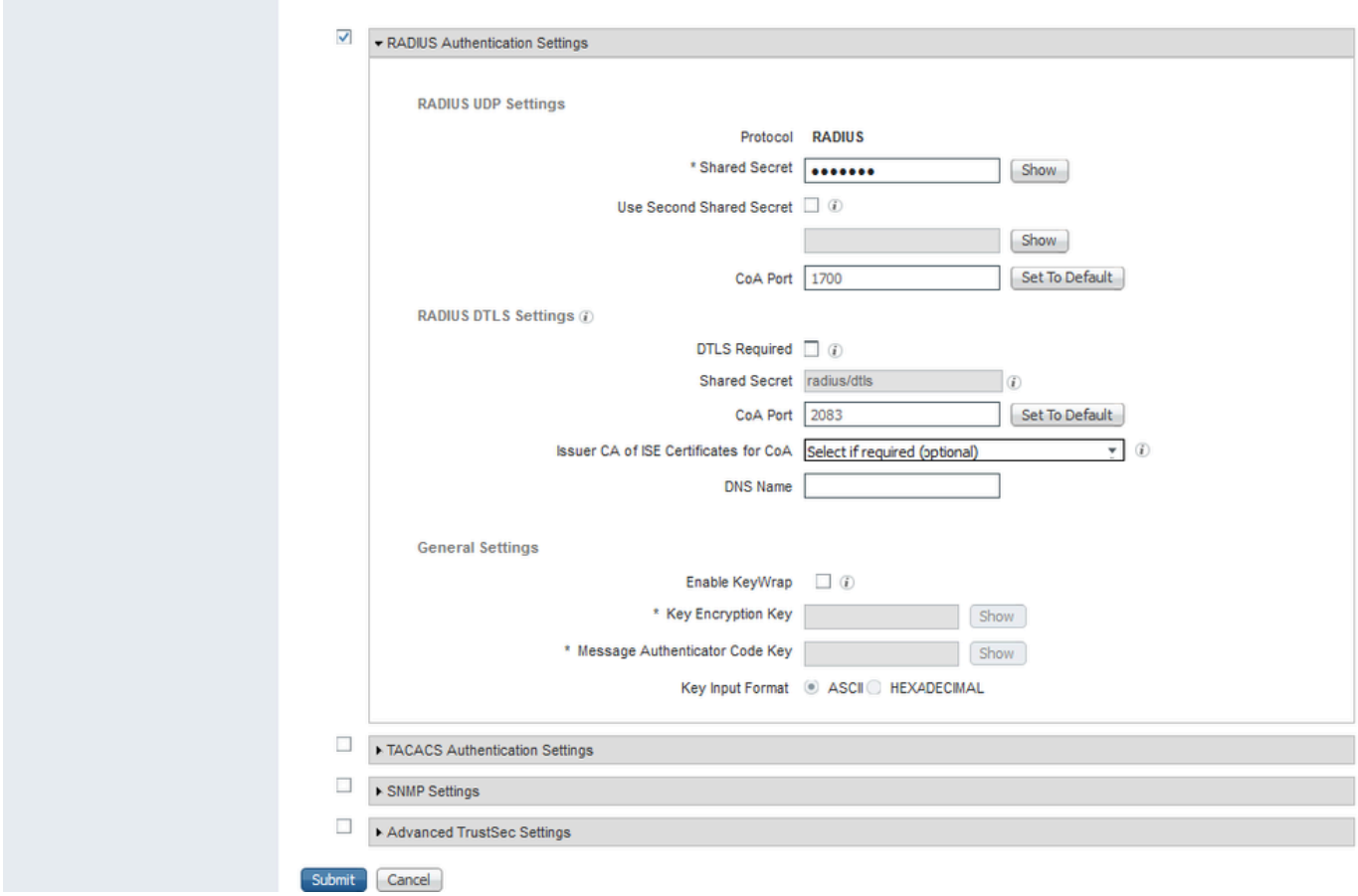


Nota: La misma clave se debe utilizar más adelante para configurar el servidor RADIUS en SWA.



Configuración de la clave compartida del dispositivo de red SWA

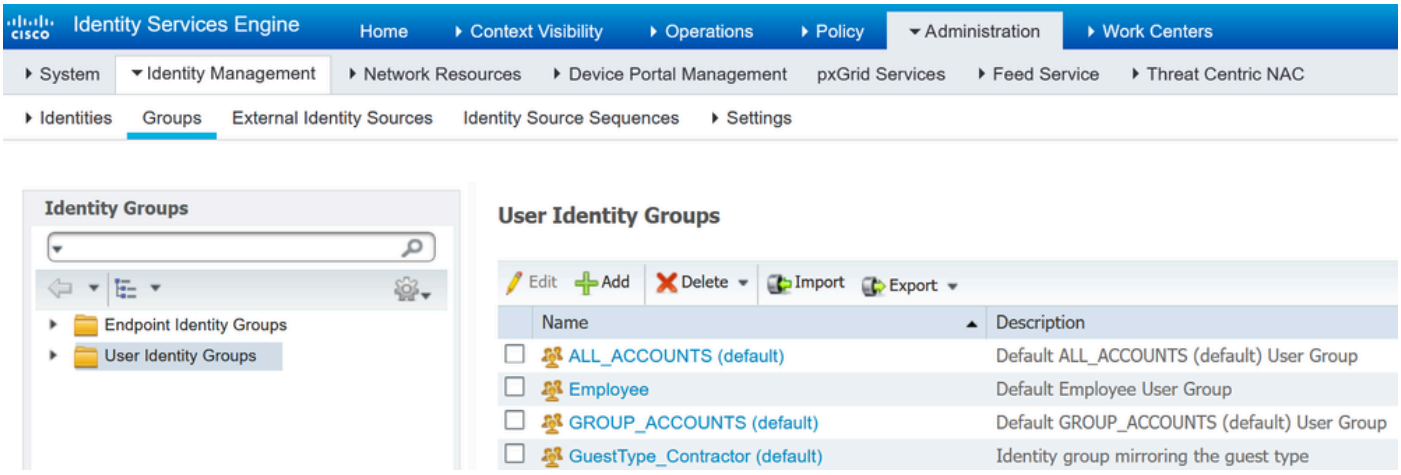
Paso 2.1. Haga clic en Submit (Enviar).



Enviar configuración de dispositivo de red

Paso 3. Cree los grupos de identidad de usuario necesarios. Vaya a Administration > Identity Management > Groups > User Identity Groups > + Add.

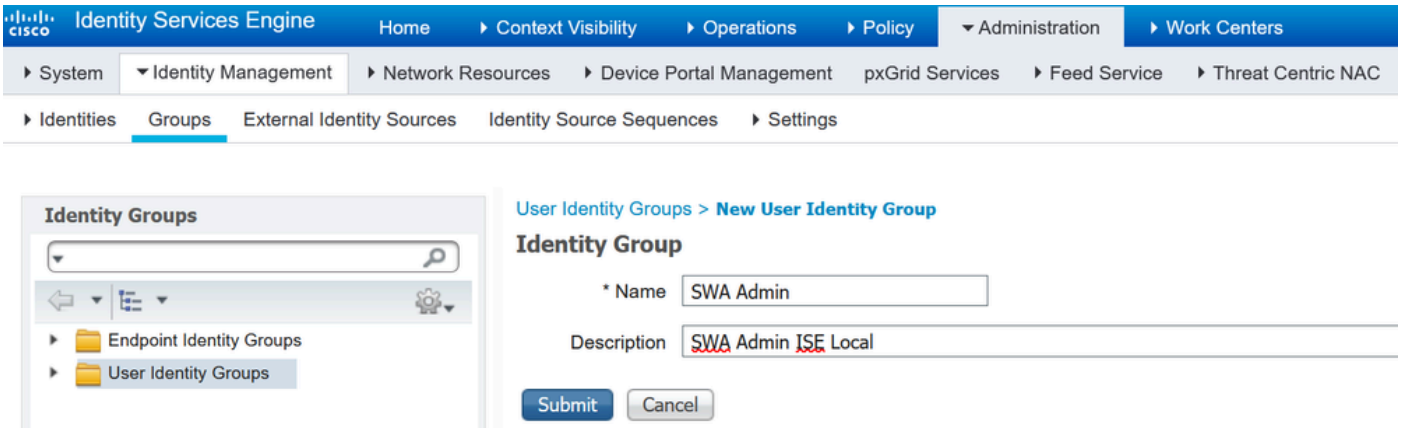
Nota: debe configurar grupos de usuarios diferentes para que coincidan con tipos de usuarios diferentes.



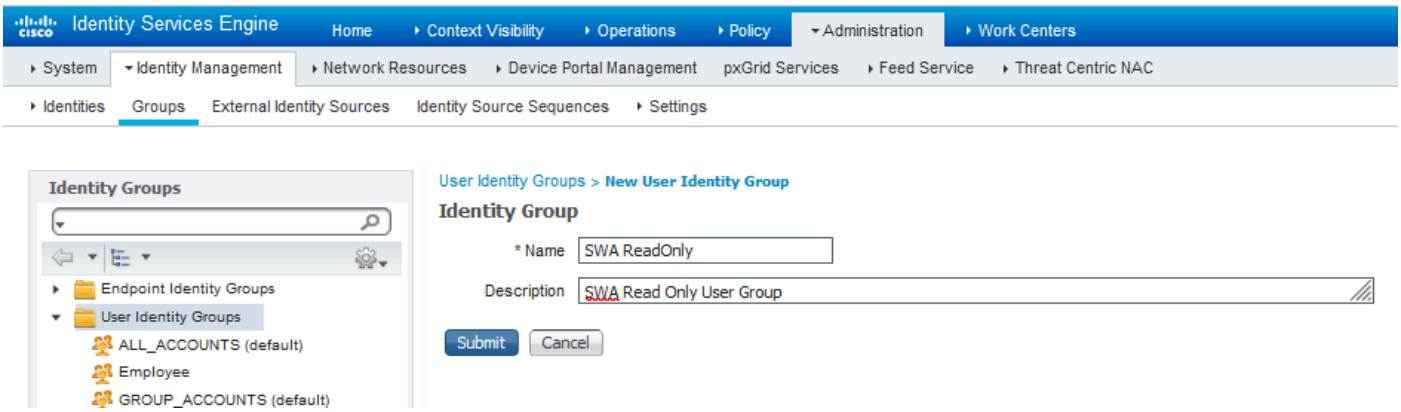
Agregar grupo de identidad de usuario

Paso 4. Introduzca el nombre del grupo, la descripción (opcional) y Enviar. Repita estos pasos

para cada grupo. En este ejemplo, se crea un grupo para usuarios administradores y otro para usuarios de sólo lectura.



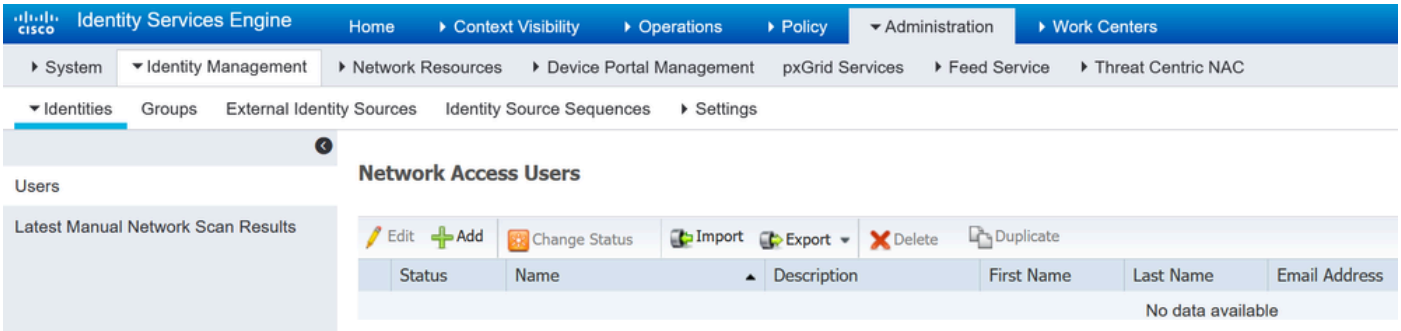
Agregar grupo de identidad de



usuarioAgregar grupo de identidad de usuario para usuarios de solo lectura SWA

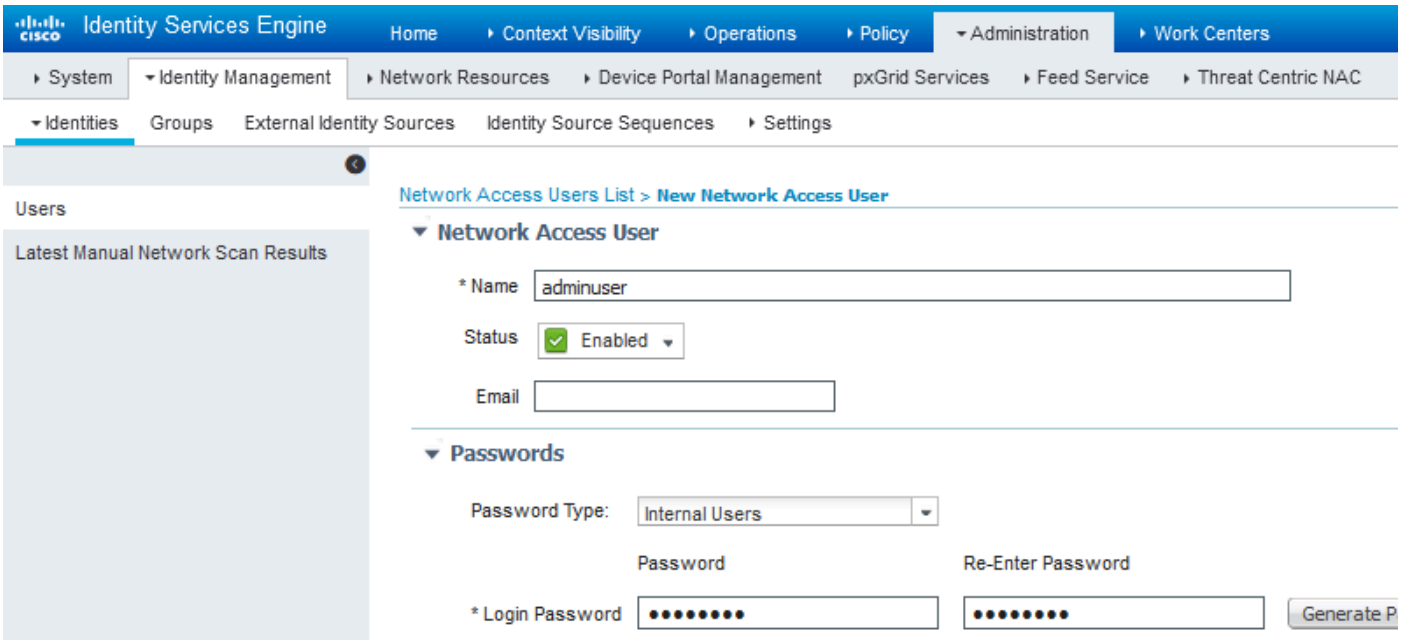
Paso 5. Debe crear usuarios de acceso a la red que coincidan con el nombre de usuario configurado en SWA.

Cree los usuarios de acceso a la red y agréguelos a su grupo correspondiente. Vaya a Administration > Identity Management > Identities > + Add.



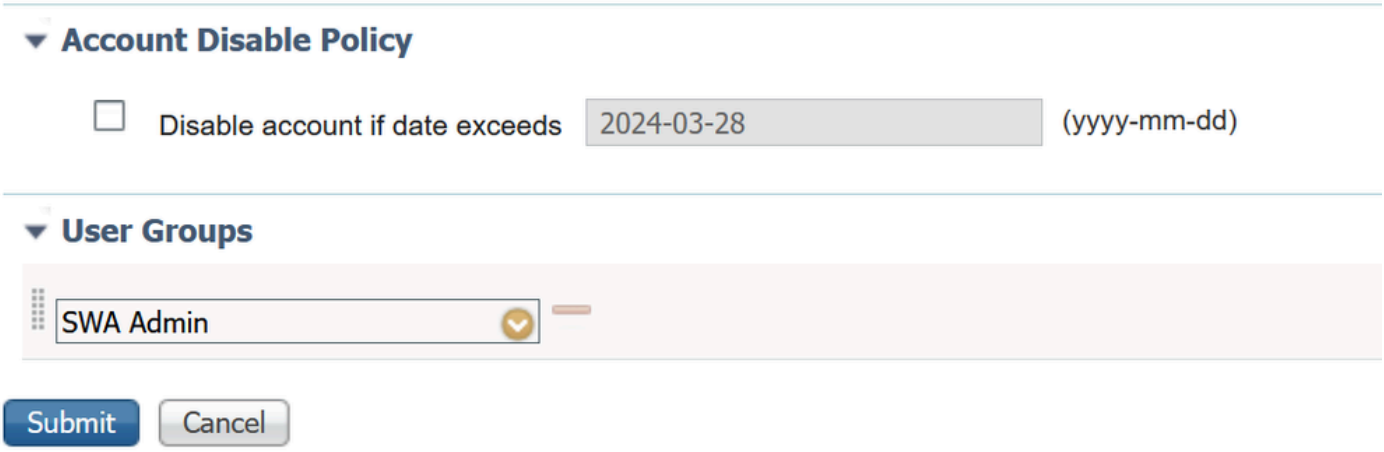
Agregar usuarios locales en ISE

Paso 5.1. Debe crear un usuario de acceso a la red con derechos de administrador. Asigne un nombre y una contraseña.



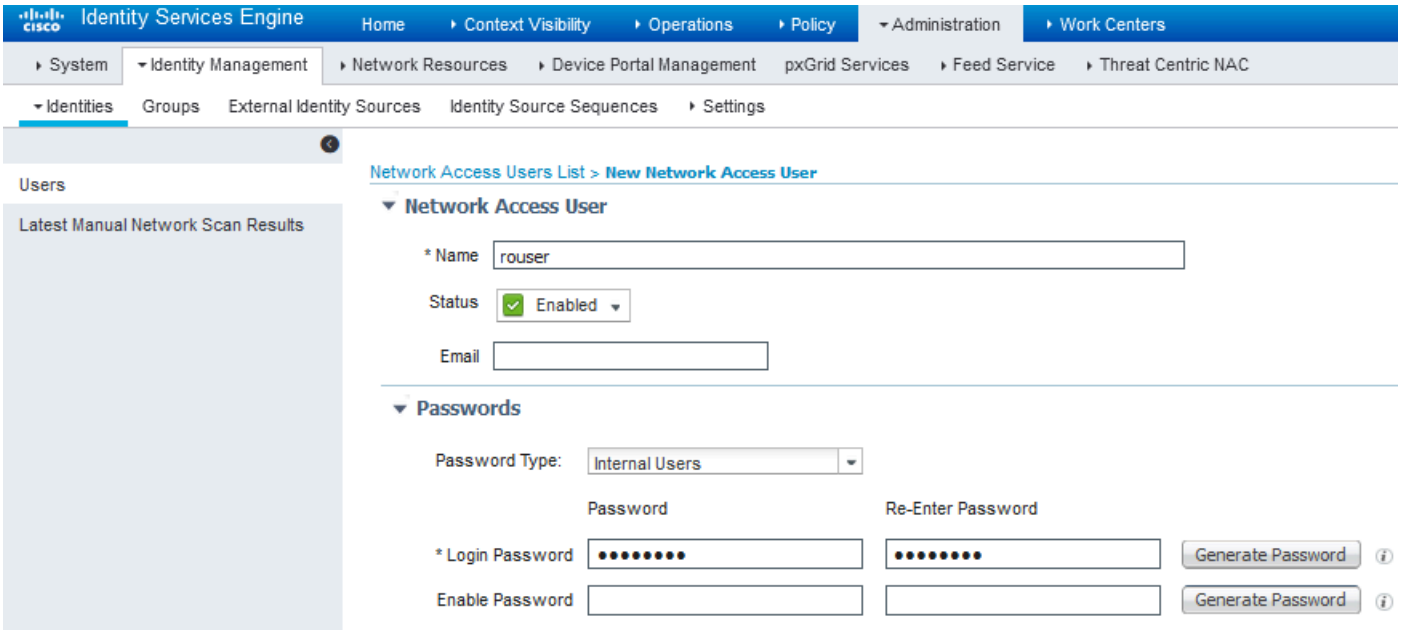
Agregar usuario administrador

Paso 5.2. Elija SWA Admin en la sección Grupos de Usuarios.



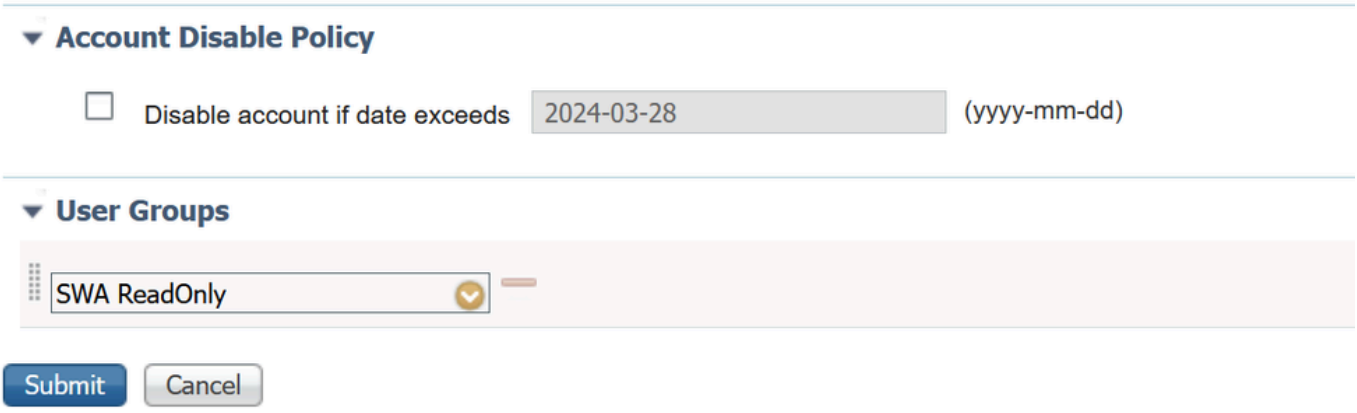
Asignar Grupo de Administradores al Usuario Administrador

Paso 5.3. Debe crear un usuario con derechos de sólo lectura. Asigne un nombre y una contraseña.



Agregar usuario de sólo lectura

Paso 5.4. Elija SWA ReadOnly en la sección Grupos de Usuarios.

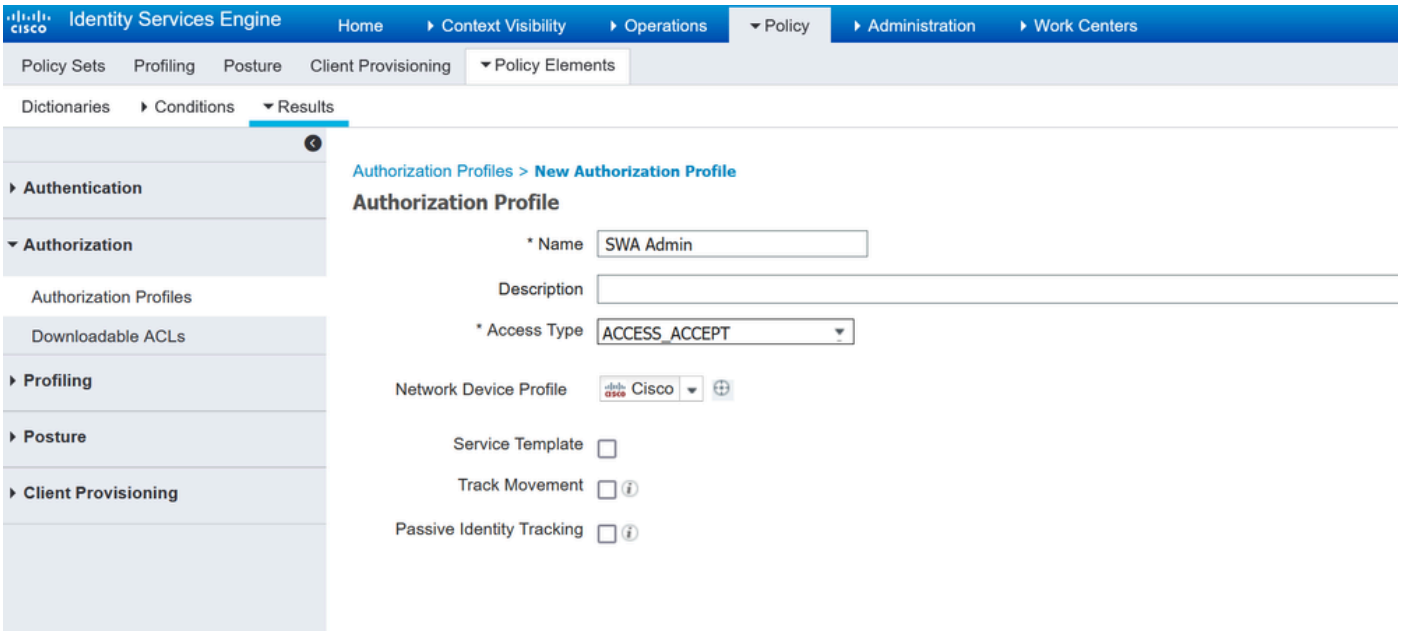


Asignar grupo de usuarios de sólo lectura al usuario de sólo lectura

Paso 6. Cree el perfil de autorización para el usuario administrador.

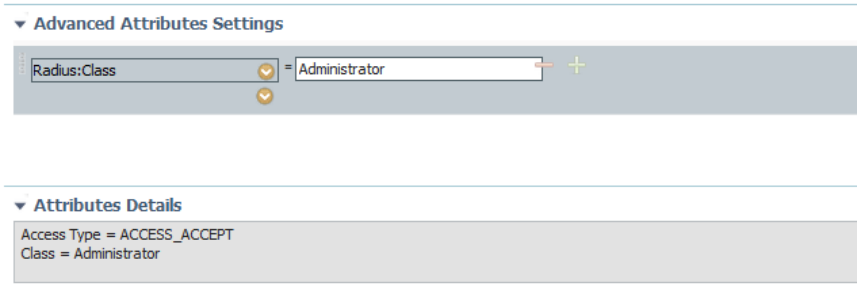
Vaya a Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización > +Agregar.

Defina un nombre para el perfil de autorización y asegúrese de que el tipo de acceso esté configurado en ACCESS_ACCEPT.



Agregar perfil de autorización para usuarios administrativos

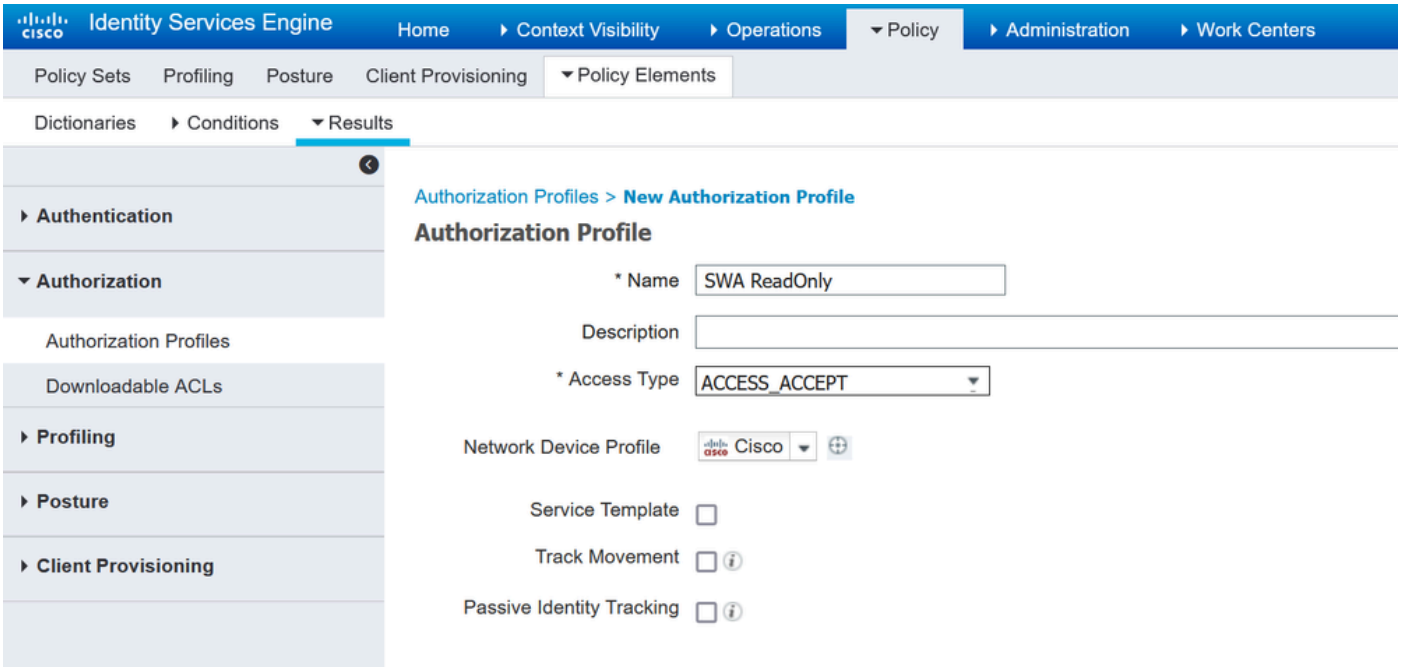
Paso 6.1. En Advanced Attributes Settings, navegue hasta Radius > Class—[25] e ingrese el valor



Administrator y haga clic en Submit .

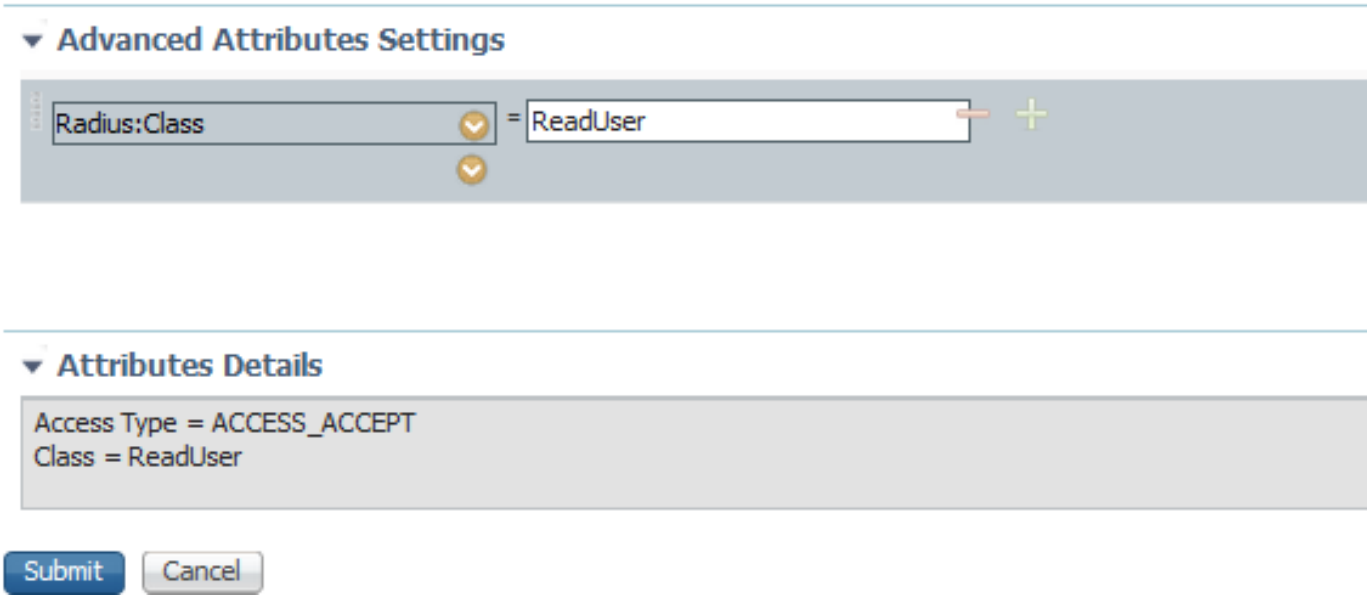
Add Authorization Profile for Admin Users

Paso 7. Repita el paso 6 para crear el perfil de autorización para el usuario de sólo lectura.



Agregar perfil de autorización para usuarios de sólo lectura

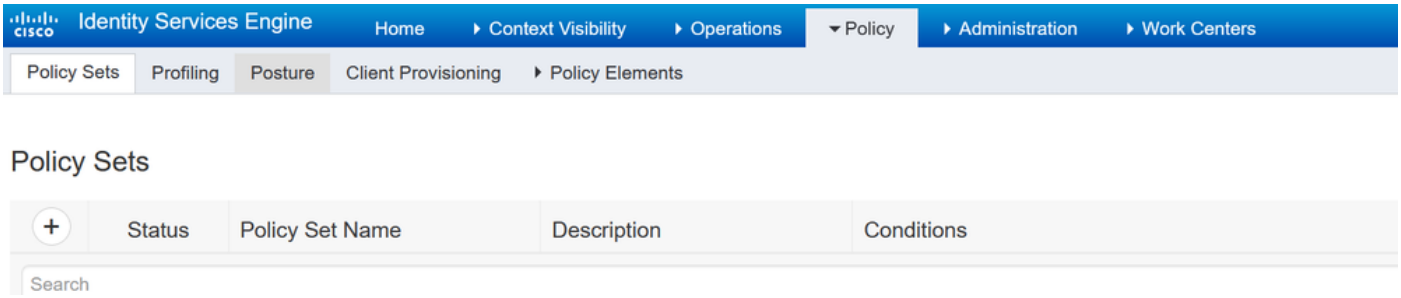
PASO 7.1. Cree la clase Radius:Class con el valor ReadUser en su lugar Administrator esta vez.



Agregar perfil de autorización para usuarios de sólo lectura

Paso 8. Cree conjuntos de políticas que coincidan con la dirección IP SWA. Esto es para evitar el acceso a otros dispositivos con estas credenciales de usuario.

Navegue hasta Policy > PolicySets y haga clic en el icono + situado en la esquina superior izquierda.

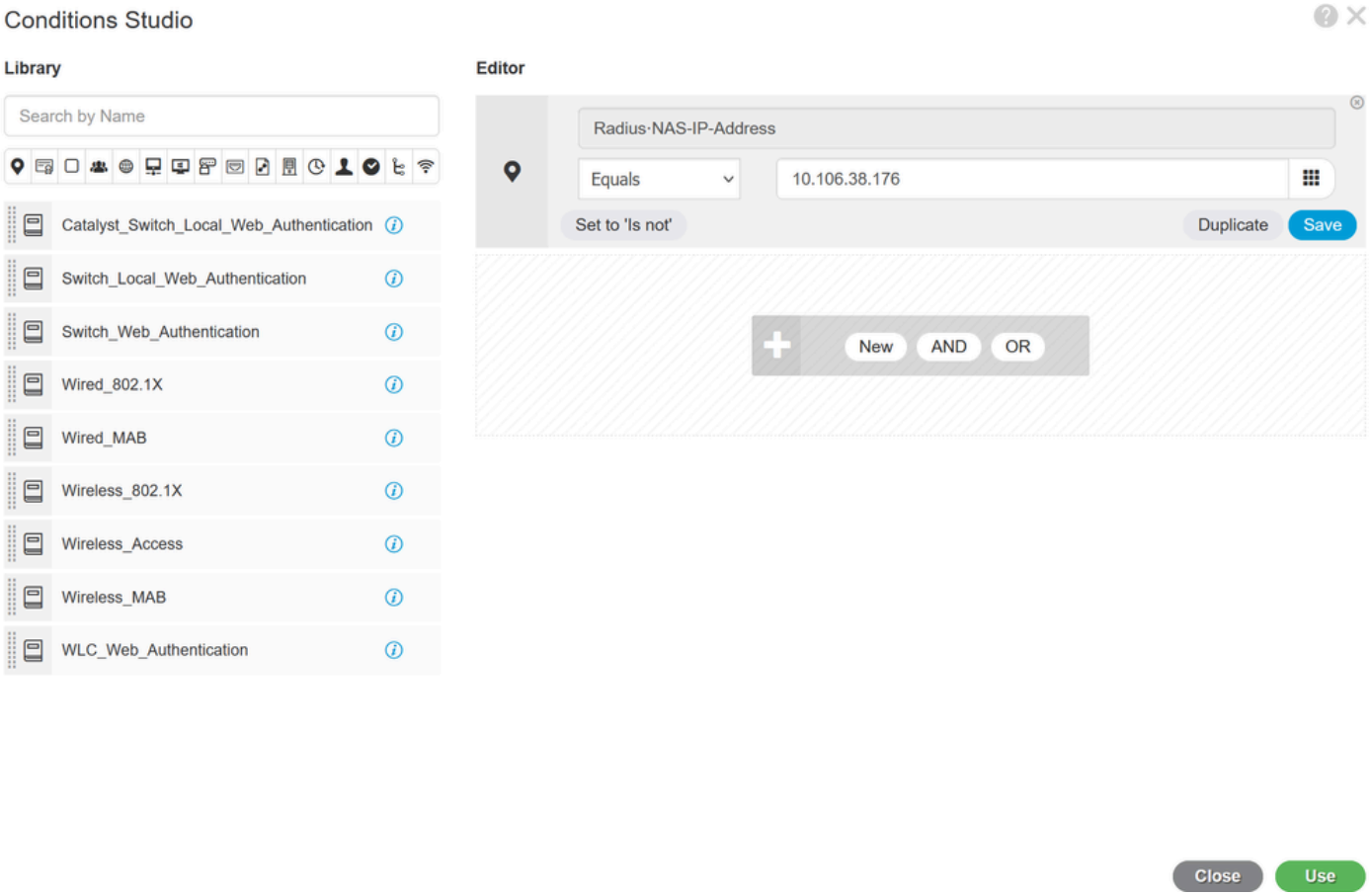


Agregar conjunto de políticas en ISE

Paso 8.1. Se coloca una nueva línea en la parte superior de los conjuntos de políticas.

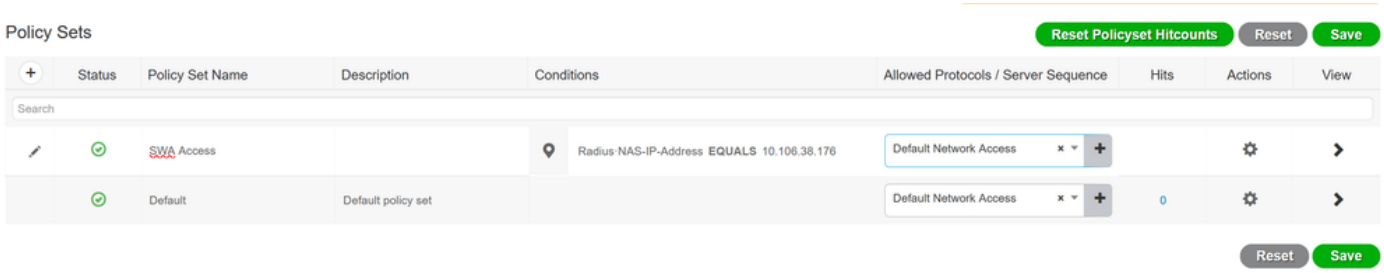
Asigne un nombre a la nueva política y agregue una condición para que el atributo RADIUS NAS-IP-Address coincida con la dirección IP SWA.

Haga clic en Utilizar para mantener los cambios y salir del editor.

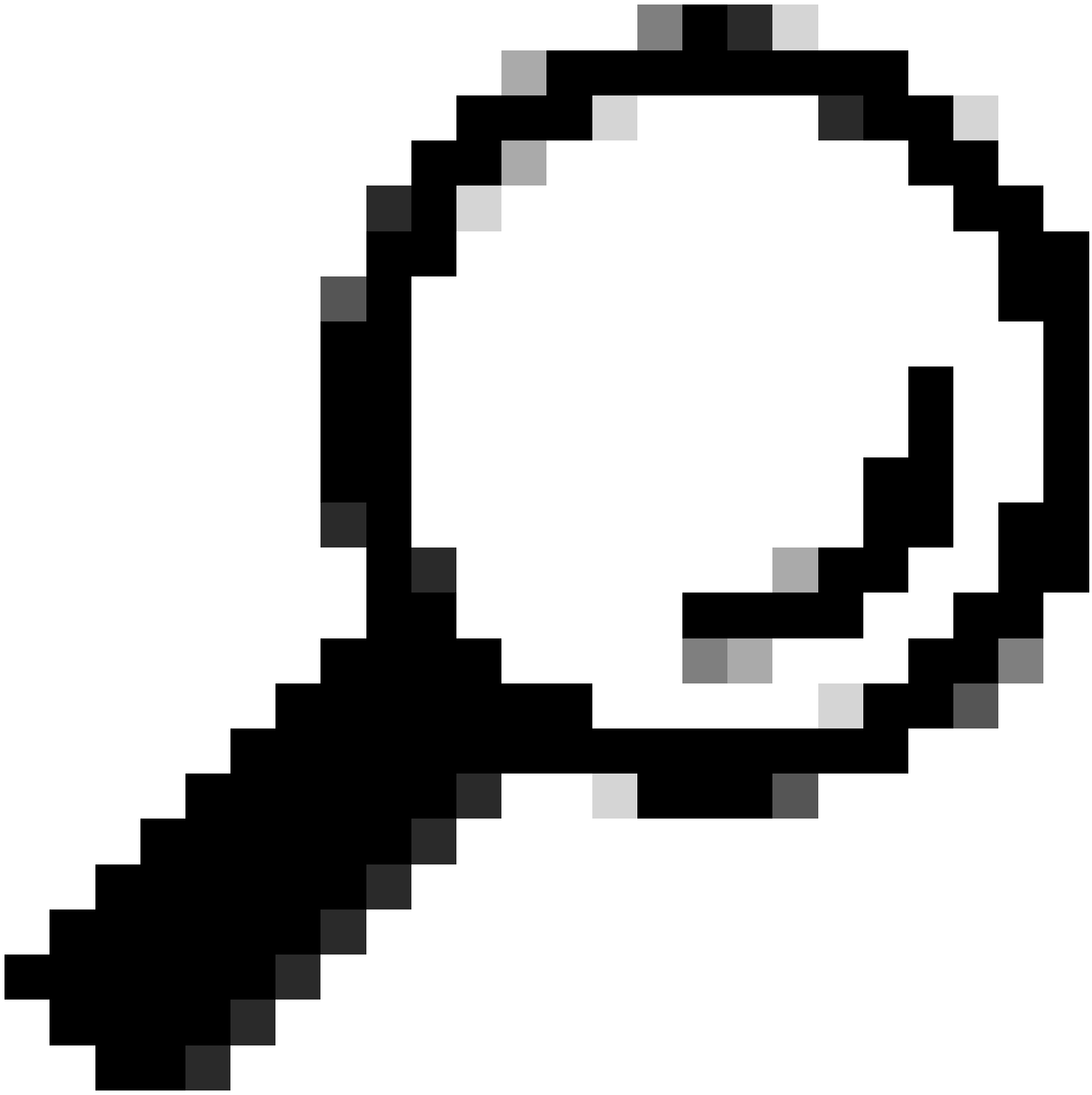


Agregar política para asignar un dispositivo de red SWA

Paso 8.2. Click Save.



Guardar directiva

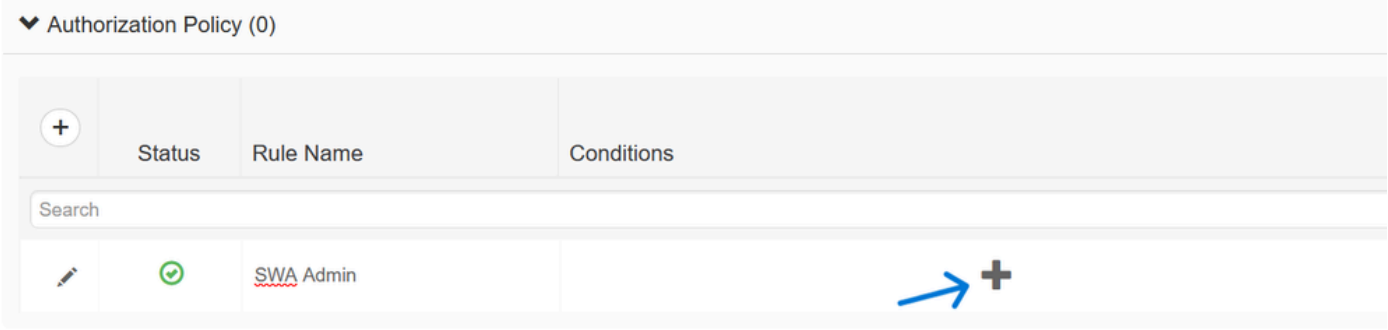


Consejo: En este artículo, se permite la lista Default Network Access Protocols . Puede crear una lista nueva y reducir las opciones según sea necesario.

Paso 9. Para ver los nuevos conjuntos de directivas, haga clic en el icono **>** en la columna Ver. Expanda el menú Authorization Policy y haga clic en el icono + para agregar una nueva regla que permita el acceso al usuario con derechos de administrador.

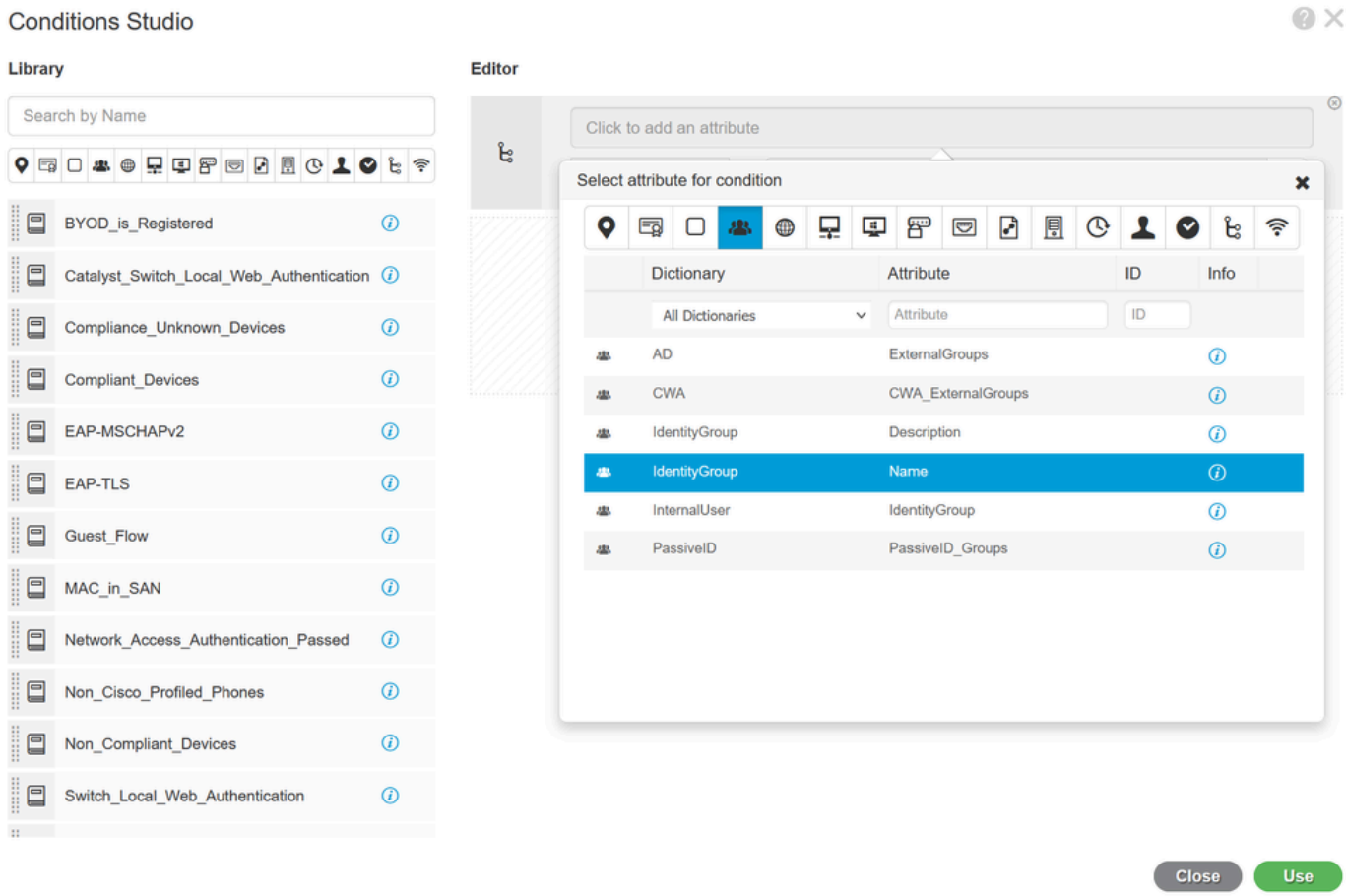
Establezca un nombre.

Paso 9.1. Para crear una condición que coincida con el grupo de usuarios administradores, haga clic en + icono.



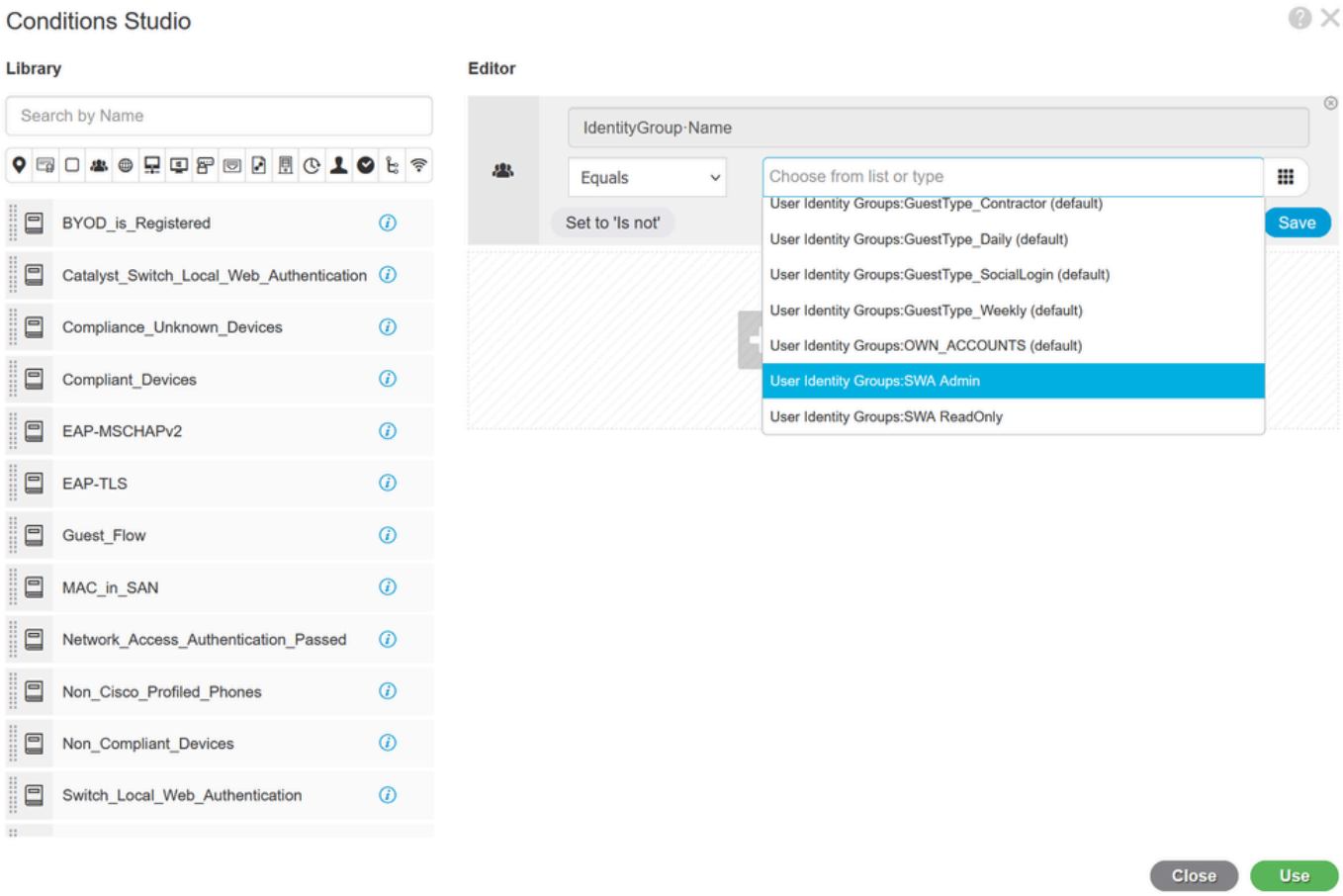
Agregar condición de directiva de autorización

Paso 9.2. Establezca las condiciones para que coincidan el grupo de identidad Dictionary con el nombre de atributo es igual a grupos de identidad de usuario: SWA admin.



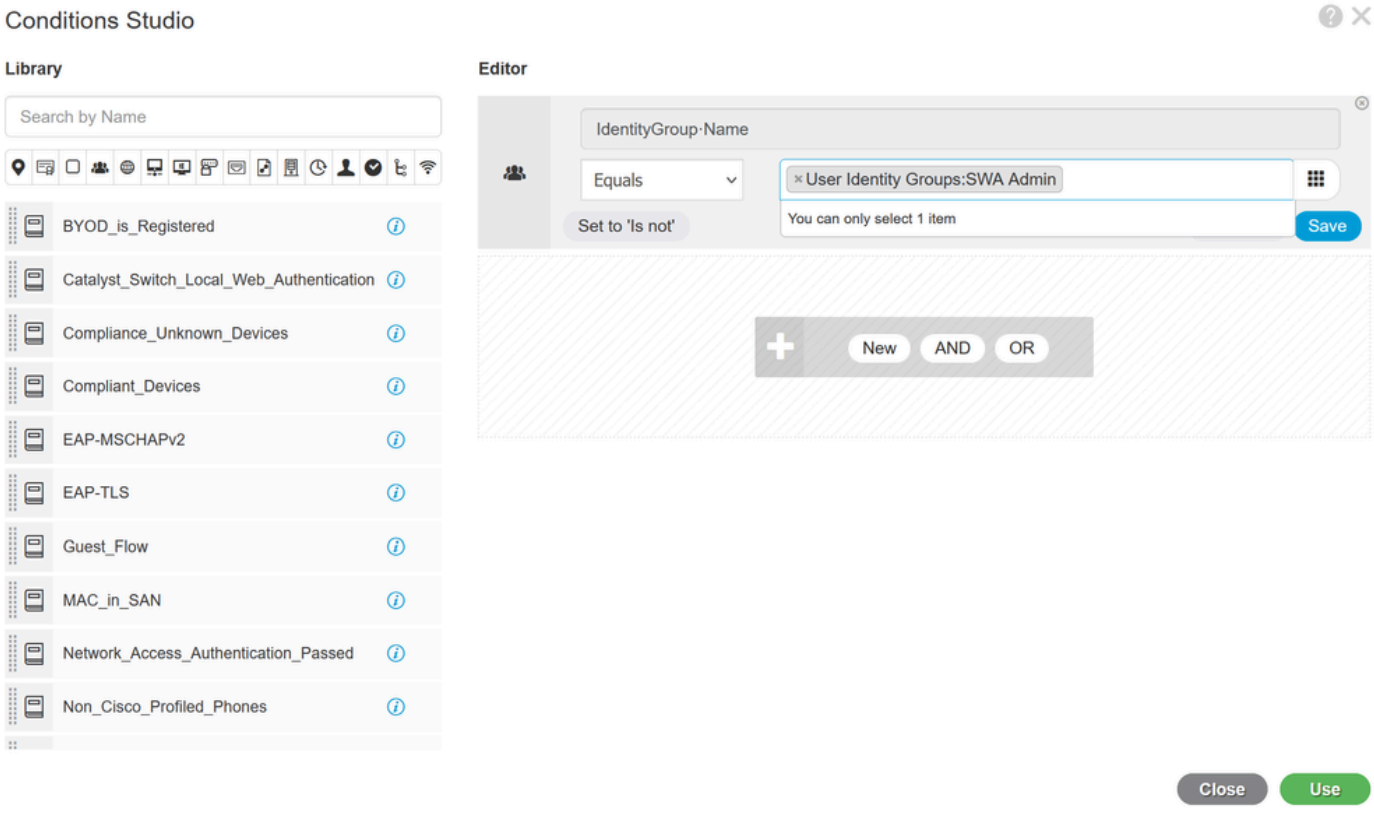
Seleccione Grupo de identidad como condición

Paso 9.3. Desplácese hacia abajo y seleccione User Identity Groups: SWA admin.



Scroll Down abd Select Identity Group Name

Paso 9.4. Haga clic en Usar.

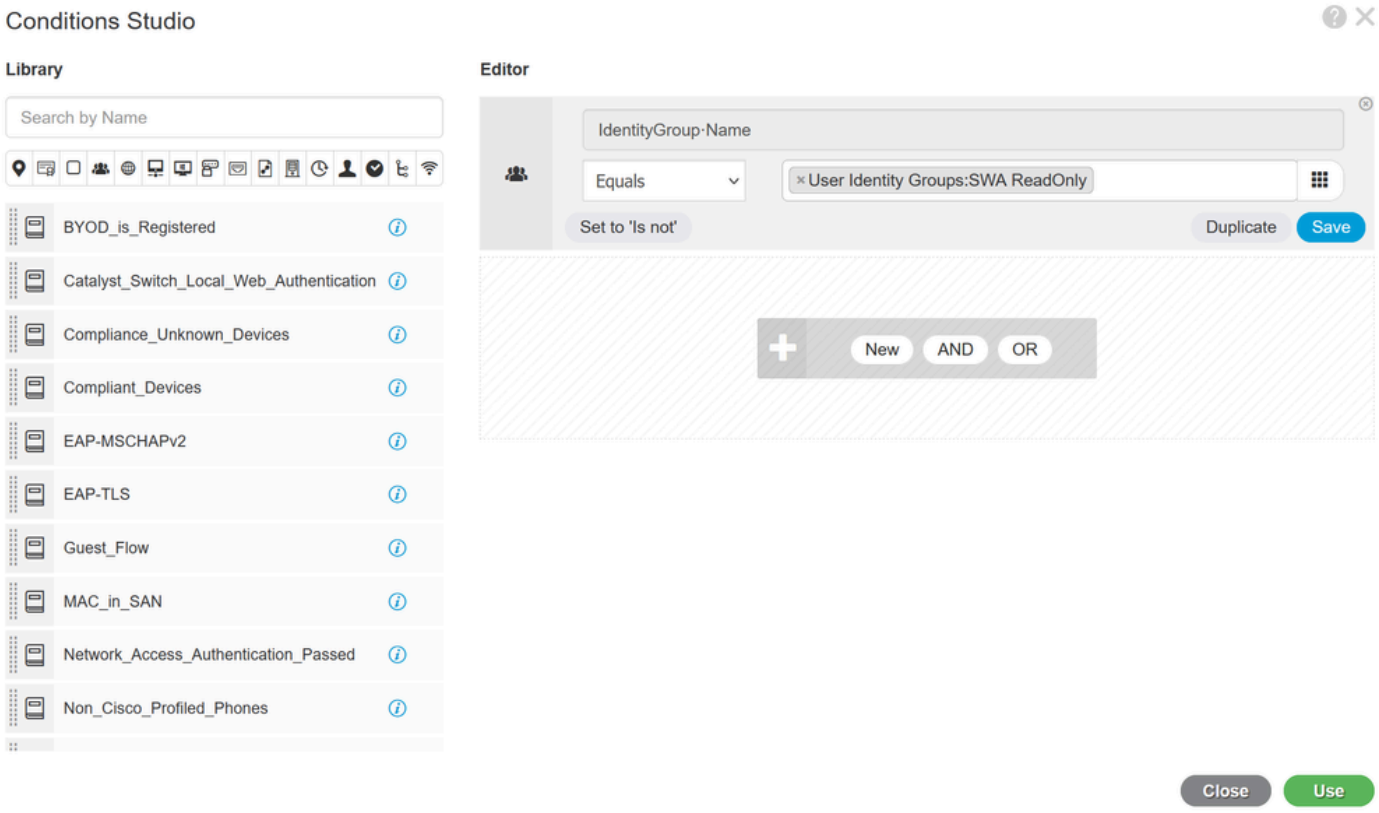


Seleccione la política de autorización para el grupo de usuarios administradores SWA

Paso 10. Haga clic en el icono + para agregar una segunda regla que permita el acceso al usuario con derechos de sólo lectura.

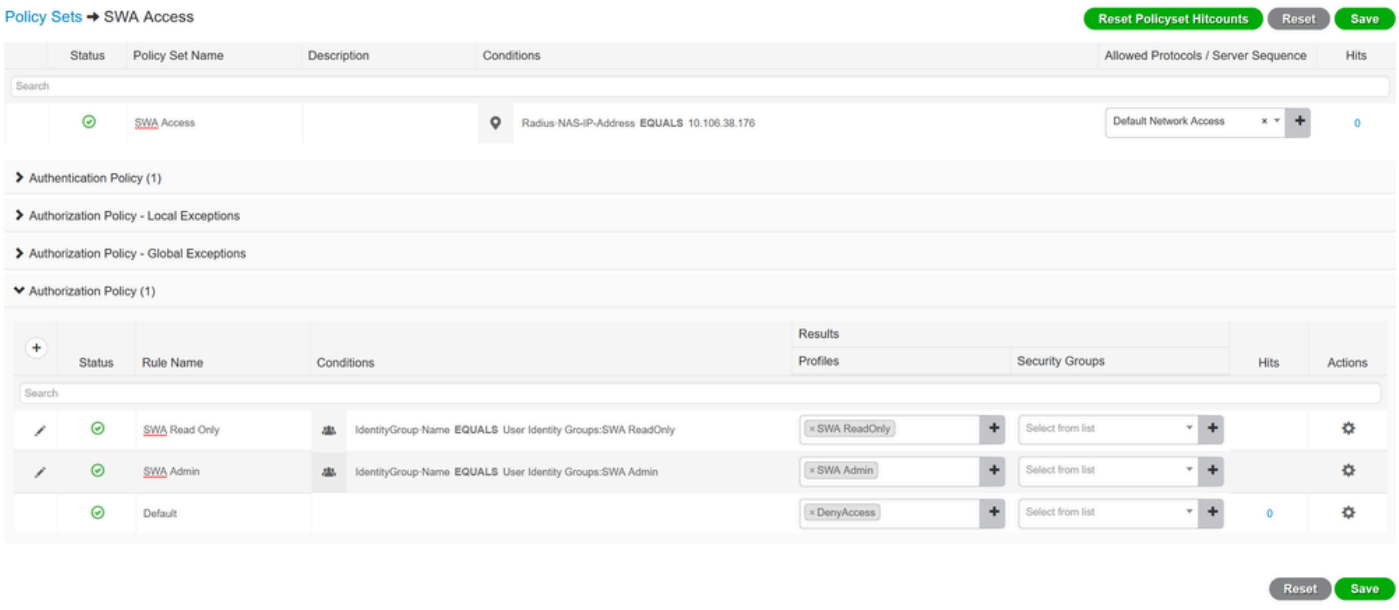
Establezca un nombre.

Establezca las condiciones para que coincidan el grupo de identidad Dictionary con el nombre de atributo es igual a grupos de identidad de usuario: SWA ReadOnly y haga clic en Use.



Seleccionar directiva de autorización para grupo de usuarios de sólo lectura

Paso 11. Establezca el perfil de autorización para cada regla y haga clic en Guardar.

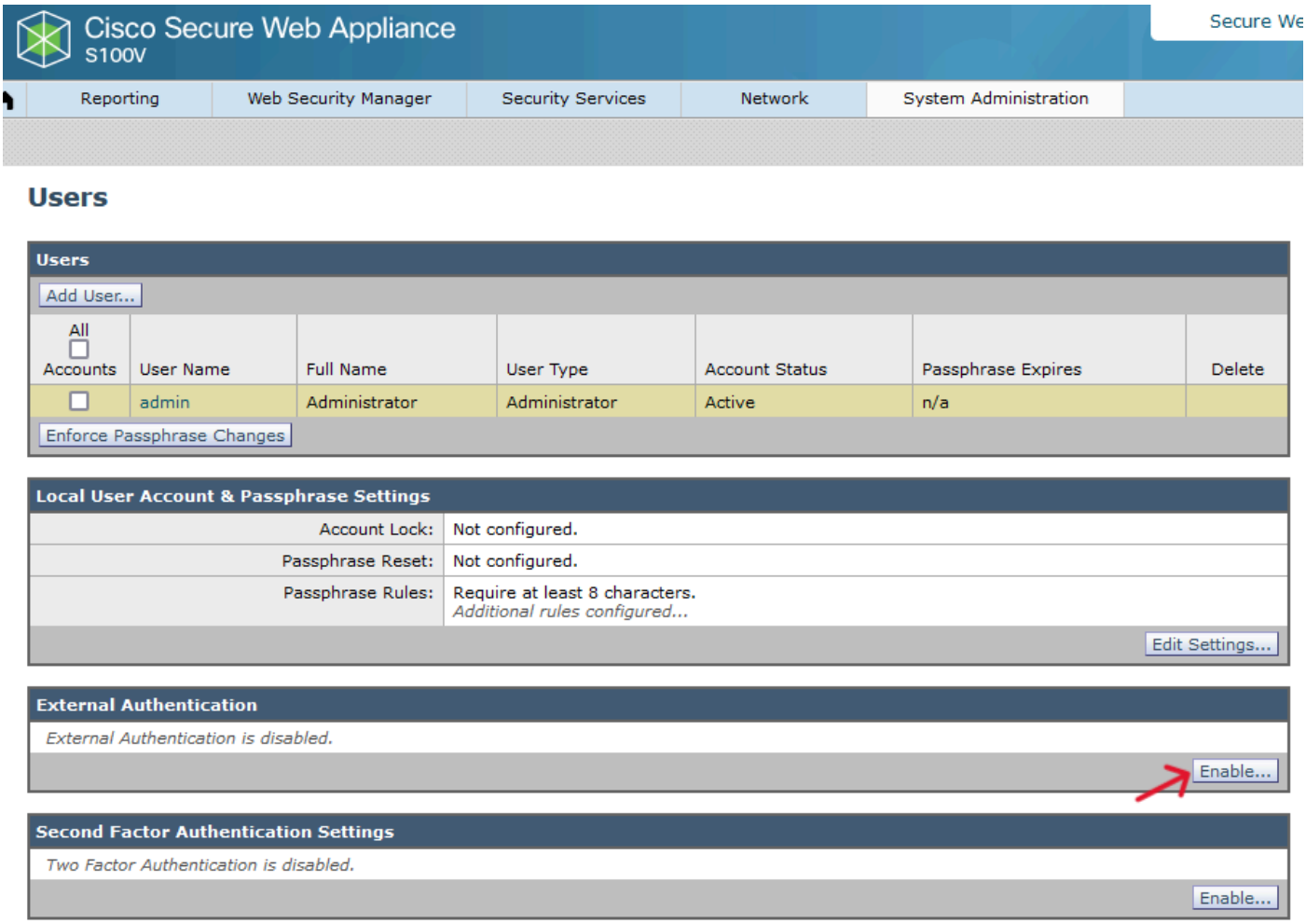


Seleccionar perfil de autorización

Configuración SWA

Paso 1. En la GUI de SWA, vaya a Administración del sistema y haga clic en Usuarios.

Paso 2. Haga clic en Enable en External Authentication.



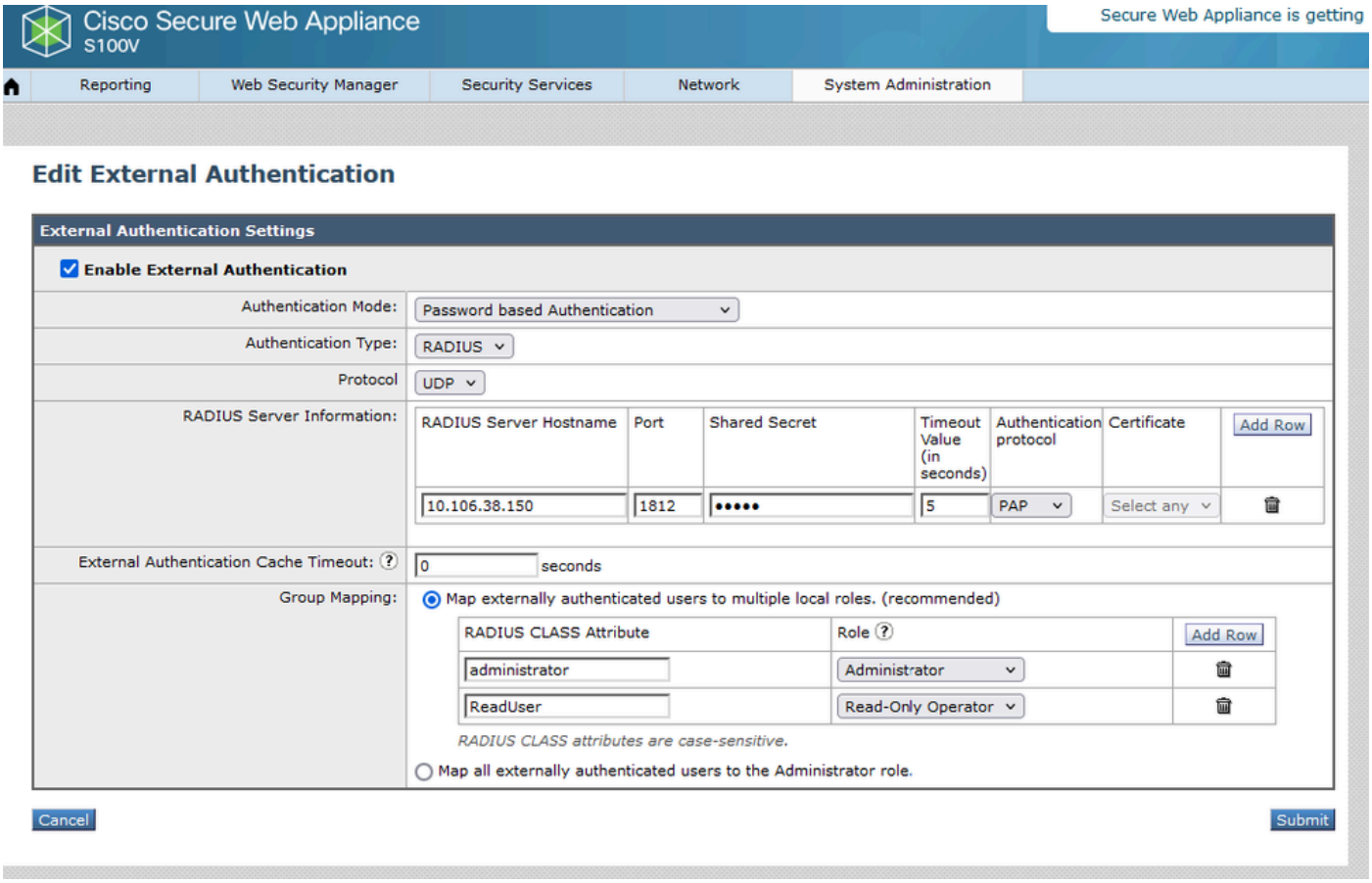
Habilitar autenticación externa en SWA

Paso 3. Ingrese la dirección IP o FQDN del ISE en el campo Nombre de host del servidor RADIUS e ingrese el mismo secreto compartido que se configura en el Paso 2, Configuración de ISE.

Paso 4. Seleccione Asignar usuarios autenticados externamente a varias funciones locales en Asignación de grupos.

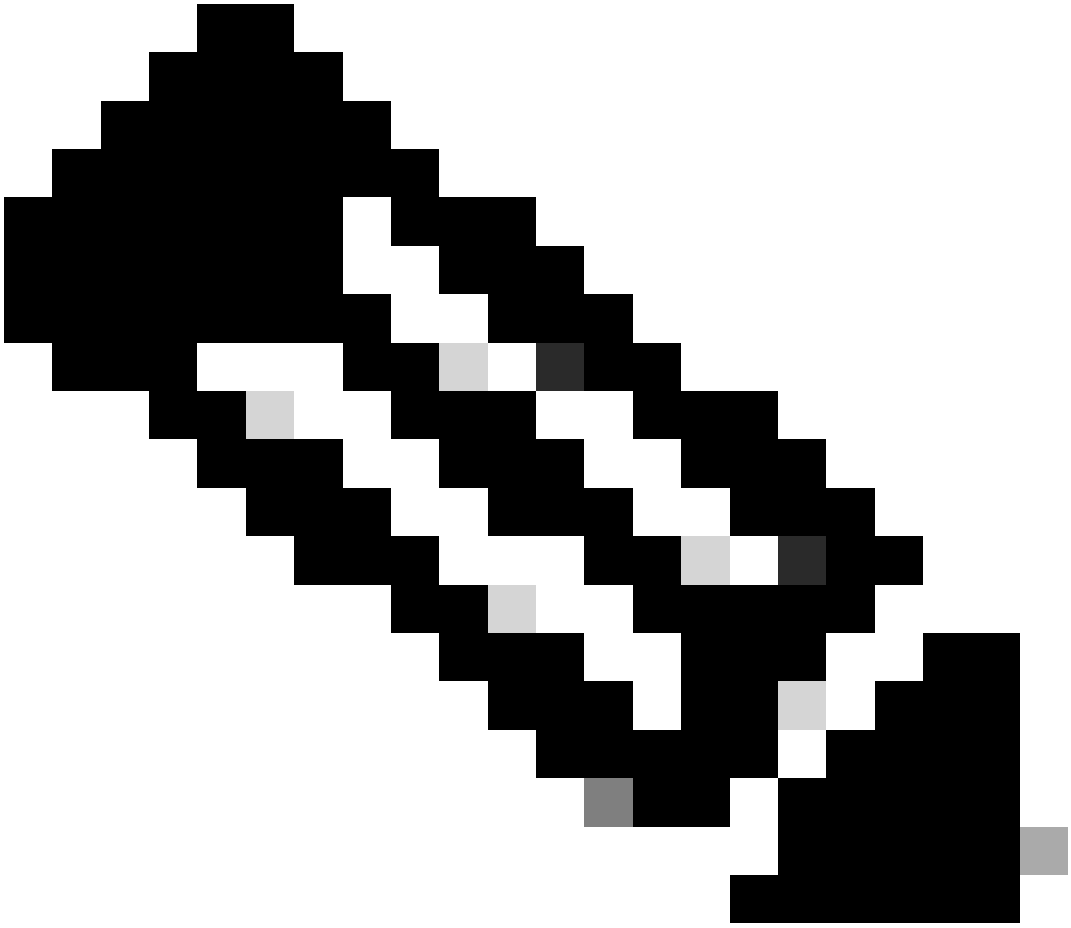
Paso 4.1. Ingrese Administrator en el campo RADIUS CLASS Attribute y seleccione el Role Administrator.

Paso 4.2. Ingrese ReadUser en el campo RADIUS CLASS Attribute y seleccione el Role Read-Only Operator.



Configuración de Autenticación Externa para el Servidor RADIUS

Paso 5: Para configurar Usuarios en SWA, haga clic en Add User (Agregar usuario). Ingrese User Name y seleccione User Type requerido para el rol deseado. Ingrese Passphrase y Retype Passphrase, que se requieren para el acceso a la GUI si el dispositivo no puede conectarse a ningún servidor RADIUS externo.



Nota: si el dispositivo no puede conectarse a ningún servidor externo, intenta autenticar al usuario como usuario local definido en el dispositivo web seguro.

Users

Users

Add User...

** When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.*

All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
☐	adminuser	Admin User	*Administrator*	Active	n/a	🗑
☐	rouser	RO User	*Read-Only Operator*	Active	n/a	🗑

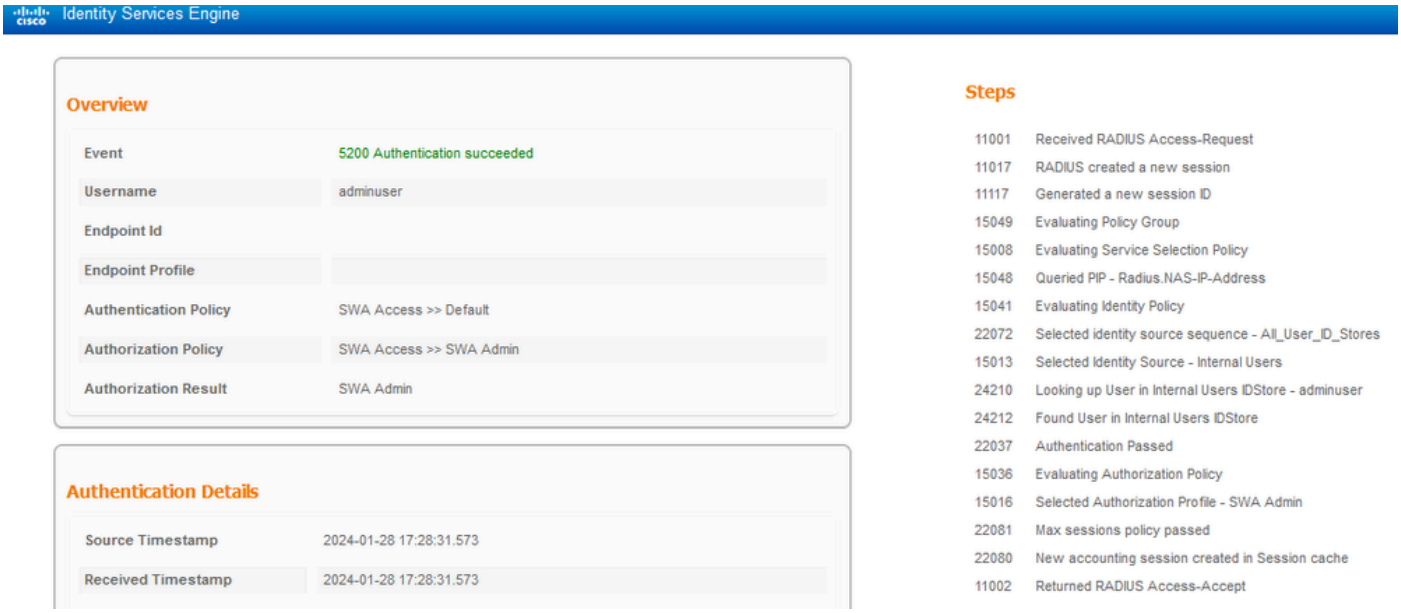
Configuración de usuario en SWA

Paso 6: Haga clic en Enviar y Registrar cambios.

Verificación

Acceda a la GUI de SWA con las credenciales de usuario configuradas y compruebe los registros

activos en ISE. Para comprobar los registros activos en ISE, vaya a Operaciones > Registros activos:



Verificar inicio de sesión de usuario ISE

Información Relacionada

- Guía del usuario de AsyncOS 14.0 para Cisco Secure Web Appliance
- Guía de administración de ISE 3.0
- Matriz de compatibilidad de ISE para Secure Web Appliance
- Soporte técnico y descargas de Cisco

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).