Configuración de la Autenticación de Segundo Factor SWA con ISE como Servidor RADIUS

Contenido

Introducción

Este documento describe cómo configurar la autenticación de segundo factor en Secure Web Appliance con Cisco Identity Service Engine como servidor RADIUS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos en SWA.
- 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 Secure Web Appliance (SWA) y Cisco Identity Service Engine (ISE).
- ISE está integrado en Active Directory o LDAP.
- Active Directory o LDAP está configurado con un nombre de usuario 'admin' para autenticar la cuenta 'admin' predeterminada de SWA.
- 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 de segundo factor para usuarios administrativos en SWA, el dispositivo verifica la credencial de usuario con el servidor RADIUS por segunda vez después de verificar las credenciales configuradas en SWA.

Topología de red

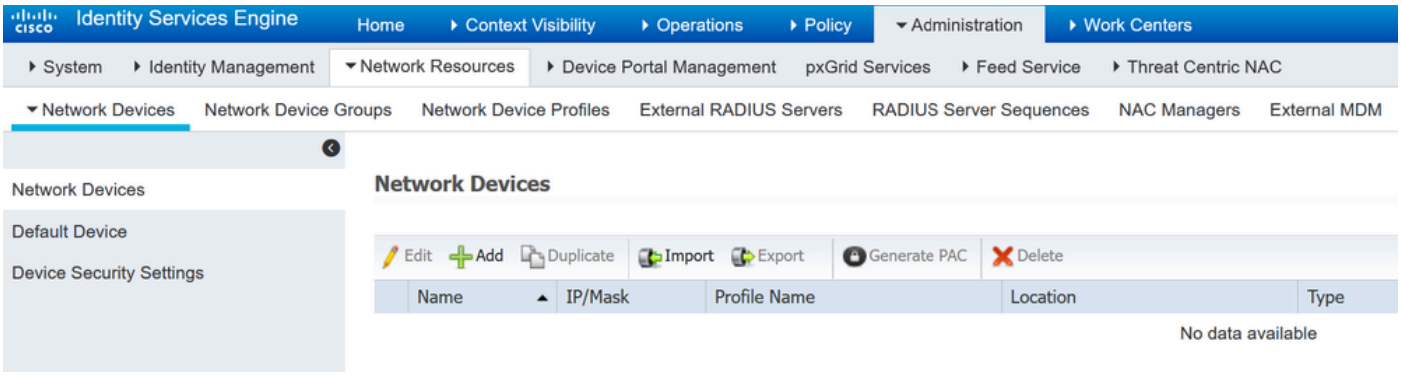
Imagen - Diagrama de topología de red

Los usuarios administrativos acceden a SWA en el puerto 443 con sus credenciales. SWA verifica las credenciales con el servidor RADIUS para la autenticación de segundo factor.

Configuration Steps

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

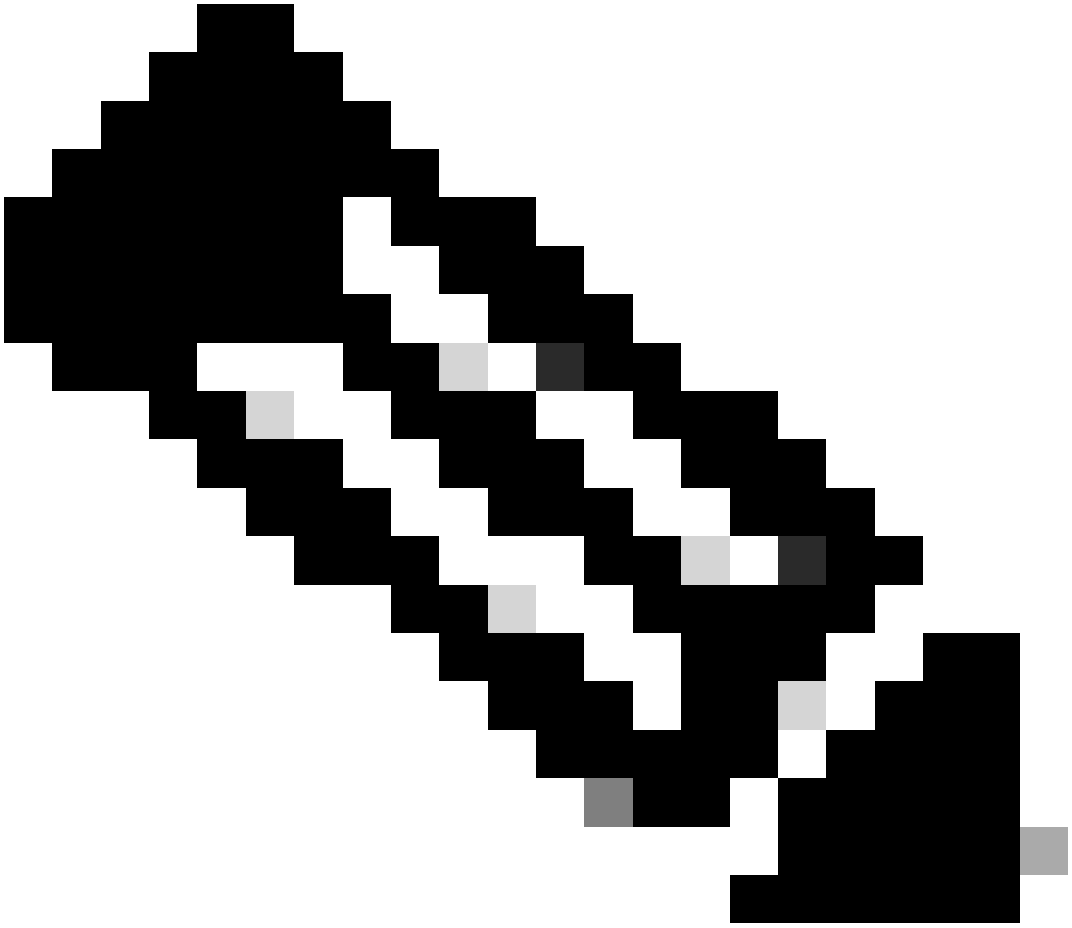
Paso 2. Configure el dispositivo de red en ISE.

Paso 2.1. Asigne un nombre al objeto de dispositivo de red.

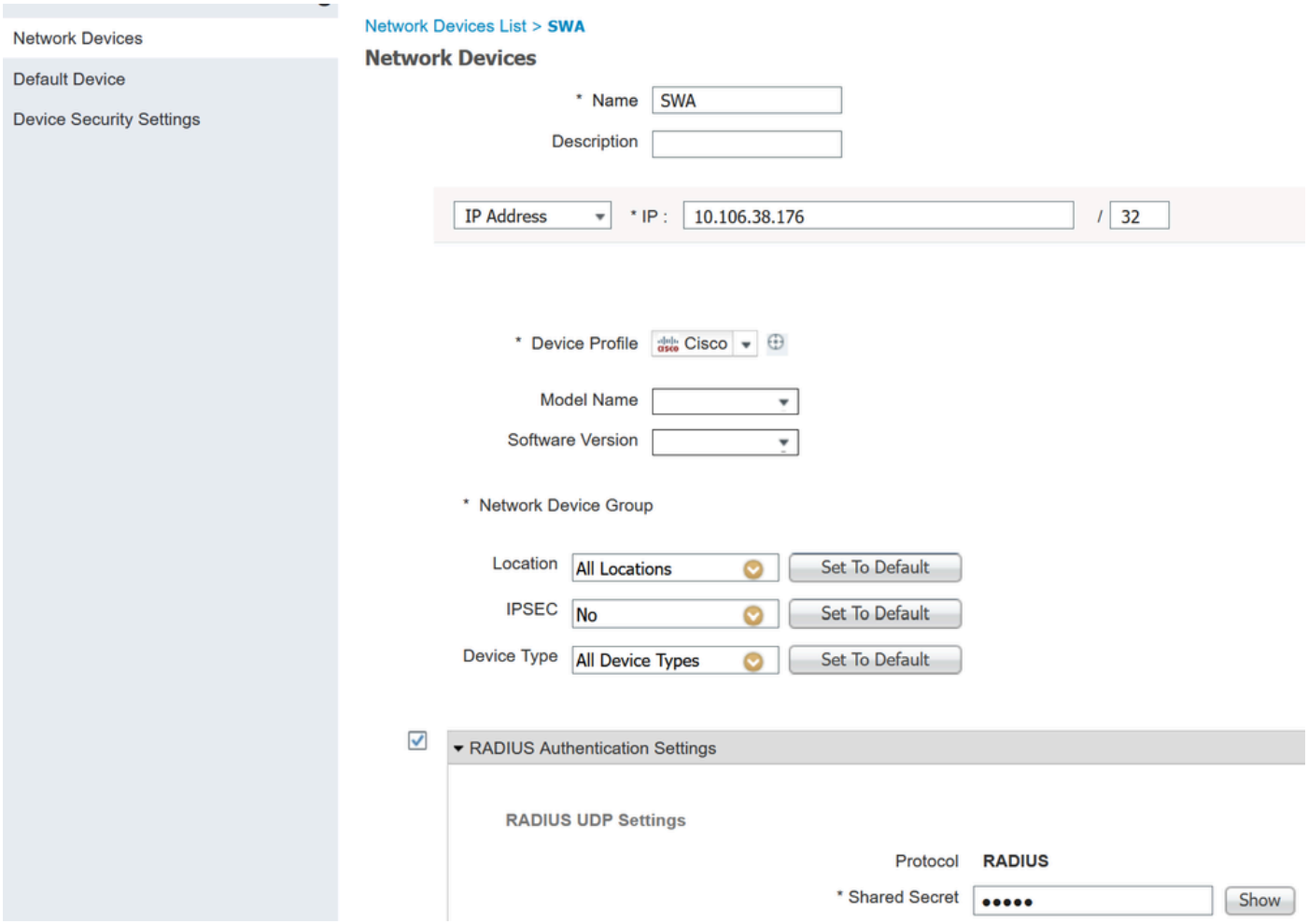
Paso 2.2. Inserte la dirección IP SWA.

Paso 2.3. Marque la casilla RADIUS.

Paso 2.4. Defina un secreto compartido.

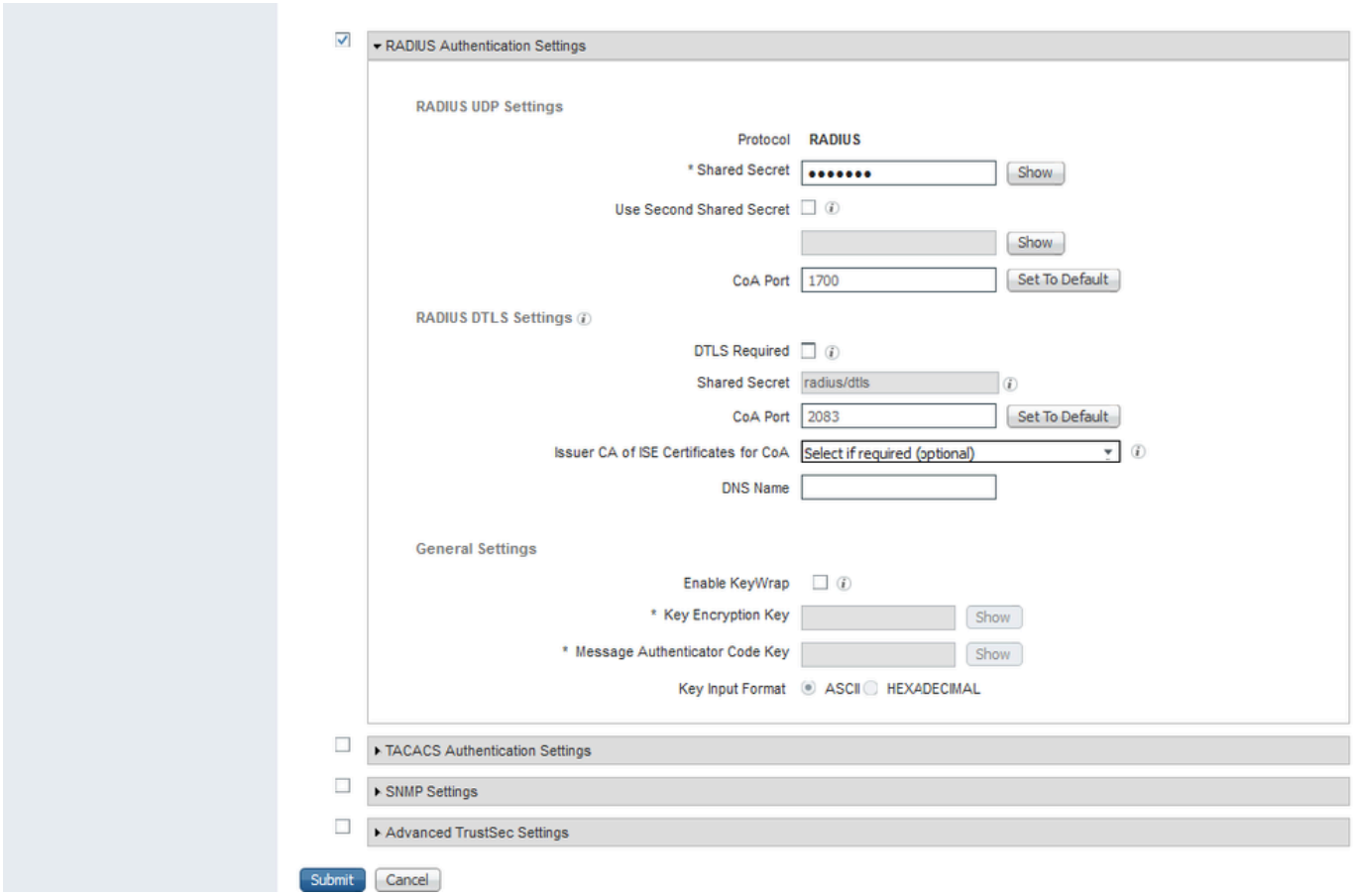


Nota: Se debe utilizar la misma clave más adelante para configurar el SWA.



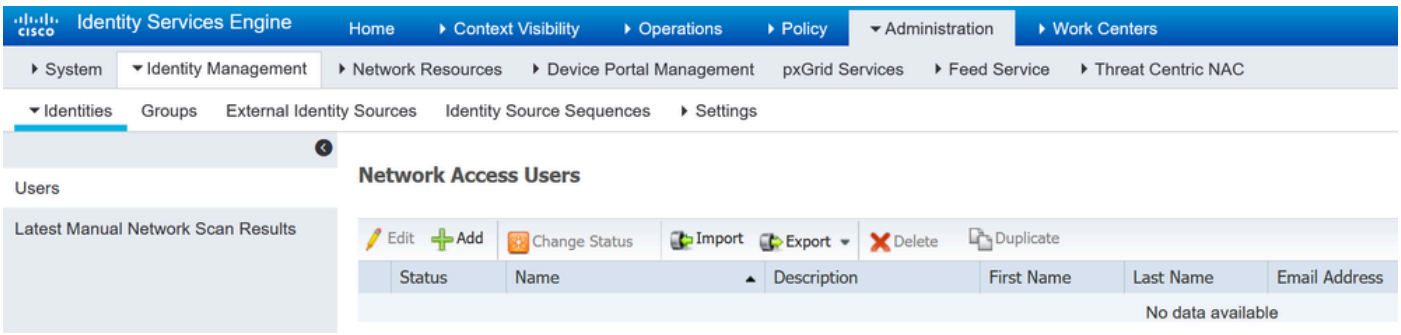
Configuración de la clave compartida del dispositivo de red SWA

Paso 2.5. Haga clic en Submit (Enviar).



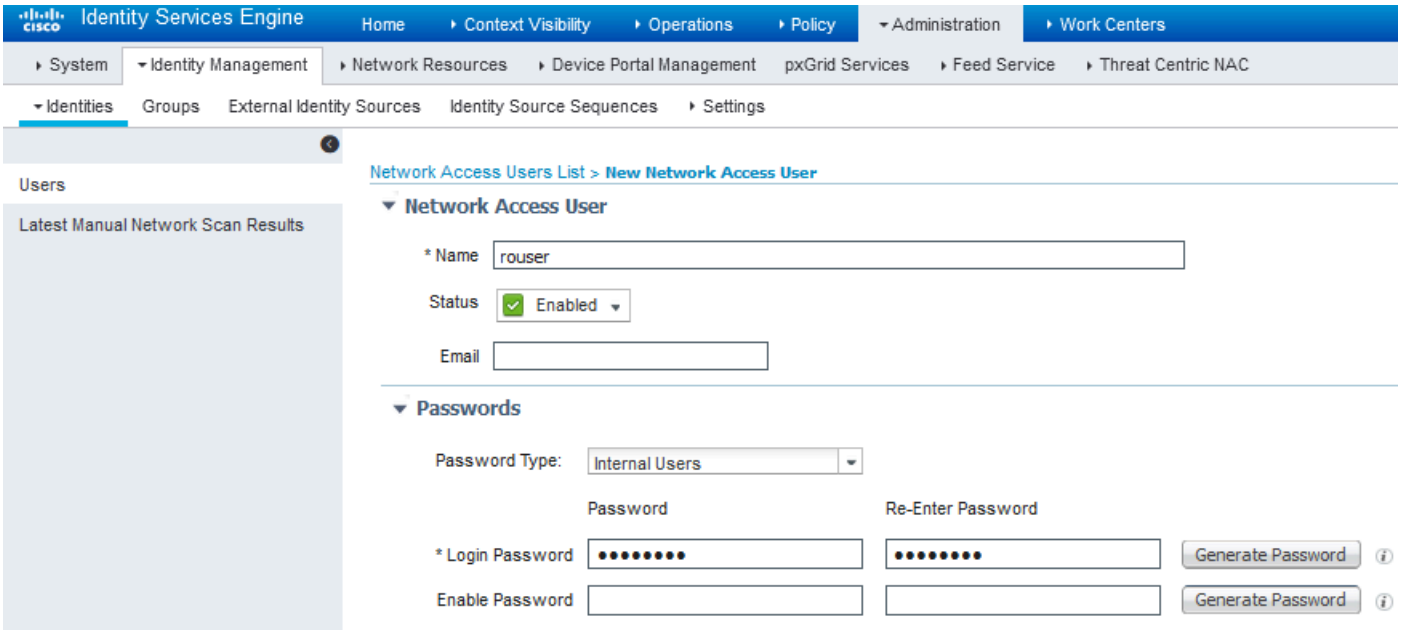
Enviar configuración de dispositivo de red

Paso 3. Debe crear Usuarios de acceso a la red que coincidan con el nombre de usuario configurado en SWA. Vaya a Administration > Identity Management > Identities > + Add.



Agregar usuarios locales en ISE

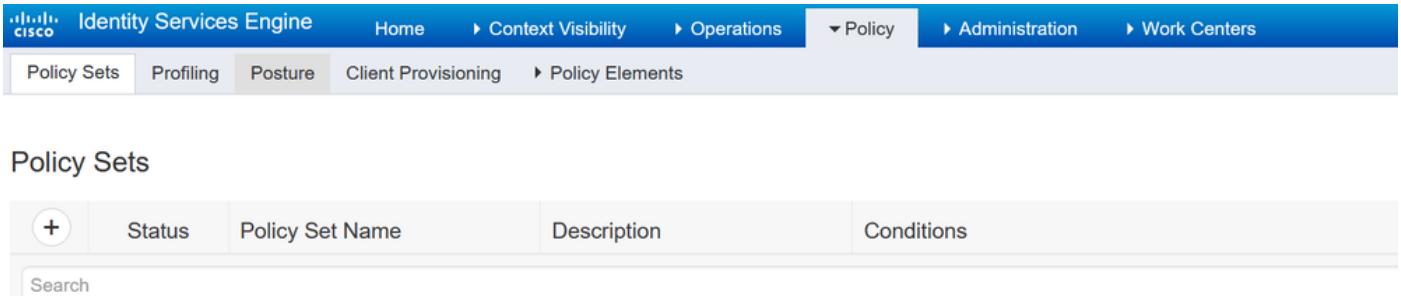
Paso 3.1. Asigne un nombre.
Paso 3.2. (Opcional) Introduzca la dirección de correo electrónico del usuario.
Paso 3.3. Establecer contraseña.
Paso 3.4. Click Save.



Agregar un usuario local en ISE

Paso 4. Cree un conjunto de políticas que coincida 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.

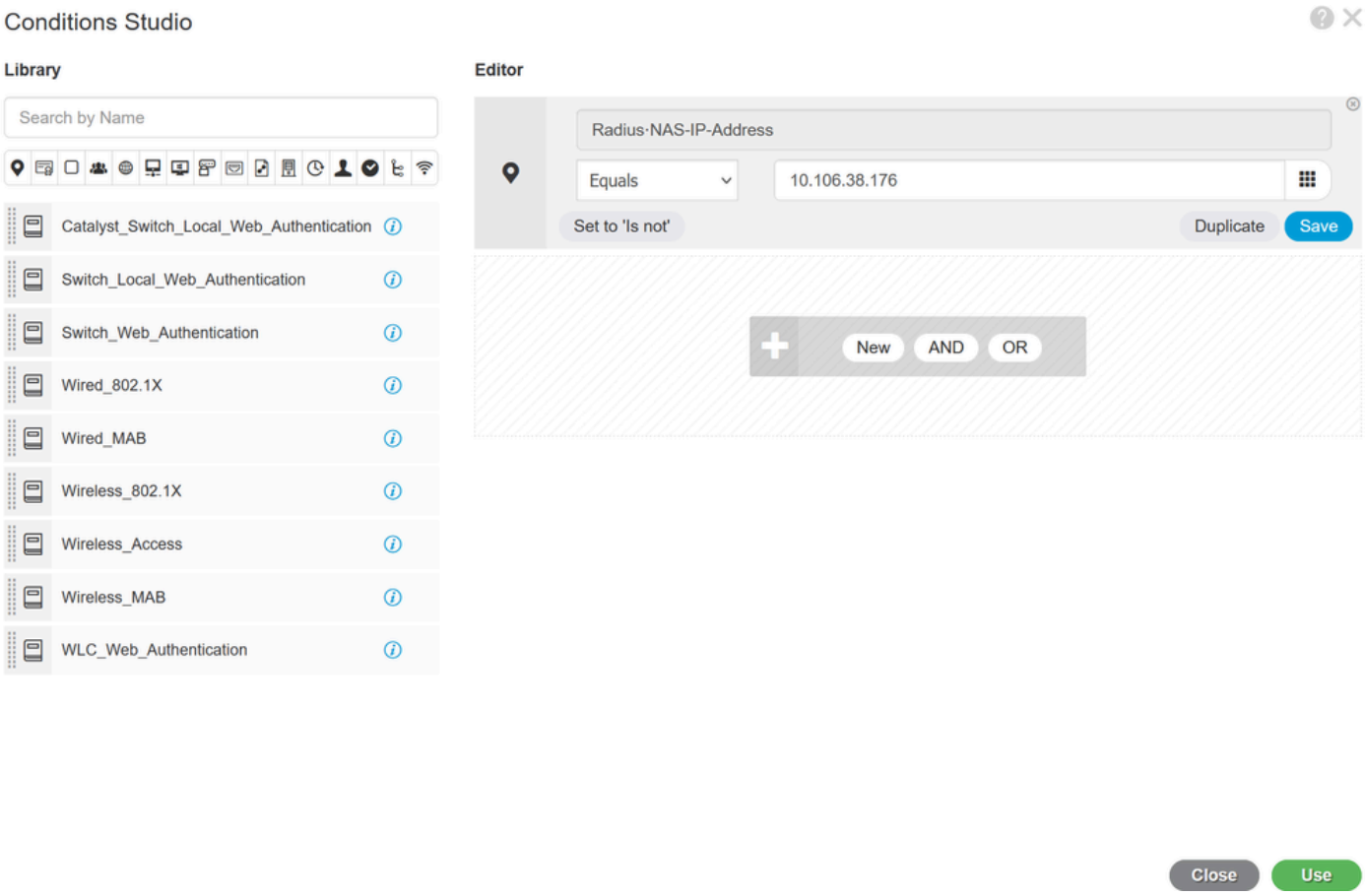


Agregar conjunto de políticas en ISE

Paso 4.1. Se coloca una nueva línea en la parte superior de los conjuntos de políticas. Introduzca el nombre de la nueva política.

Paso 4.2. Agregue una condición para que el atributo RADIUS NAS-IP-Address coincida con la dirección IP SWA.

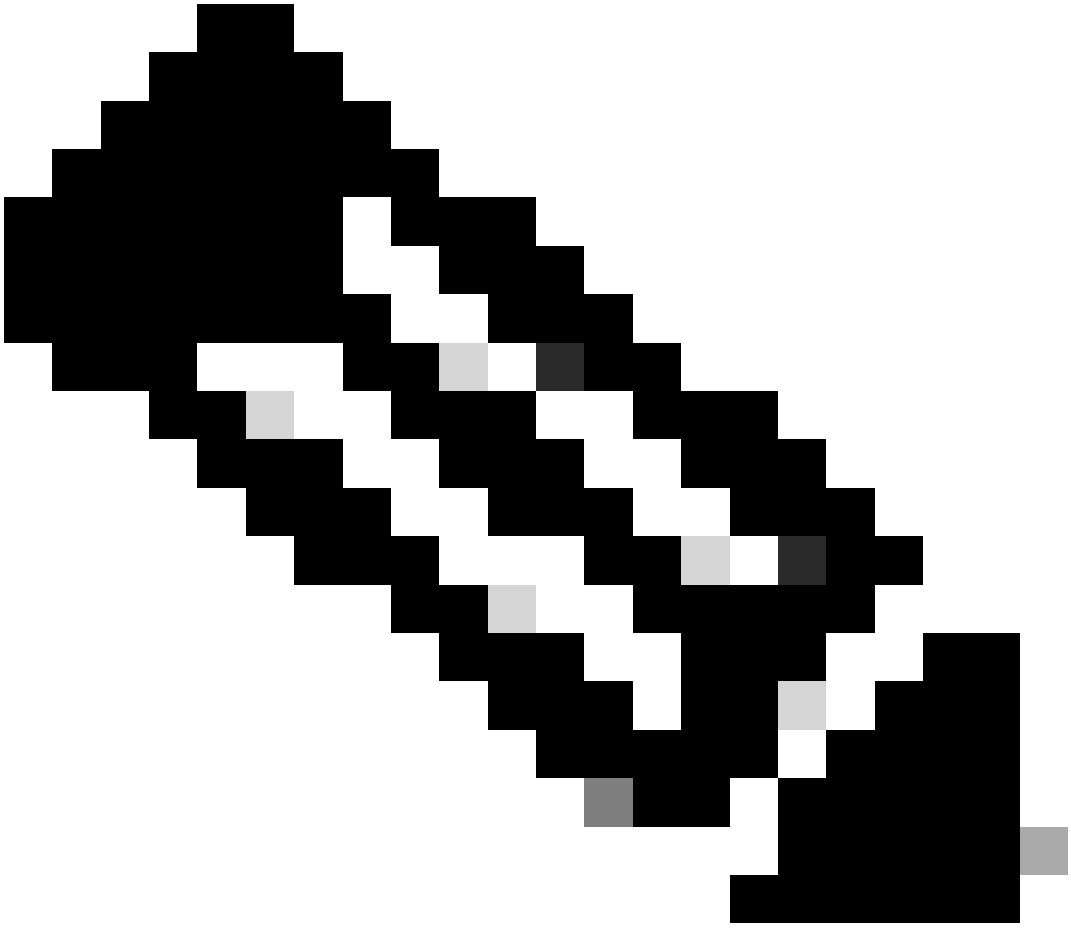
Paso 4.3. Haga clic en Utilizar para mantener los cambios y salir del editor.



Agregar política para asignar un dispositivo de red SWA

Paso 4.4. Click Save.

Guardar directiva



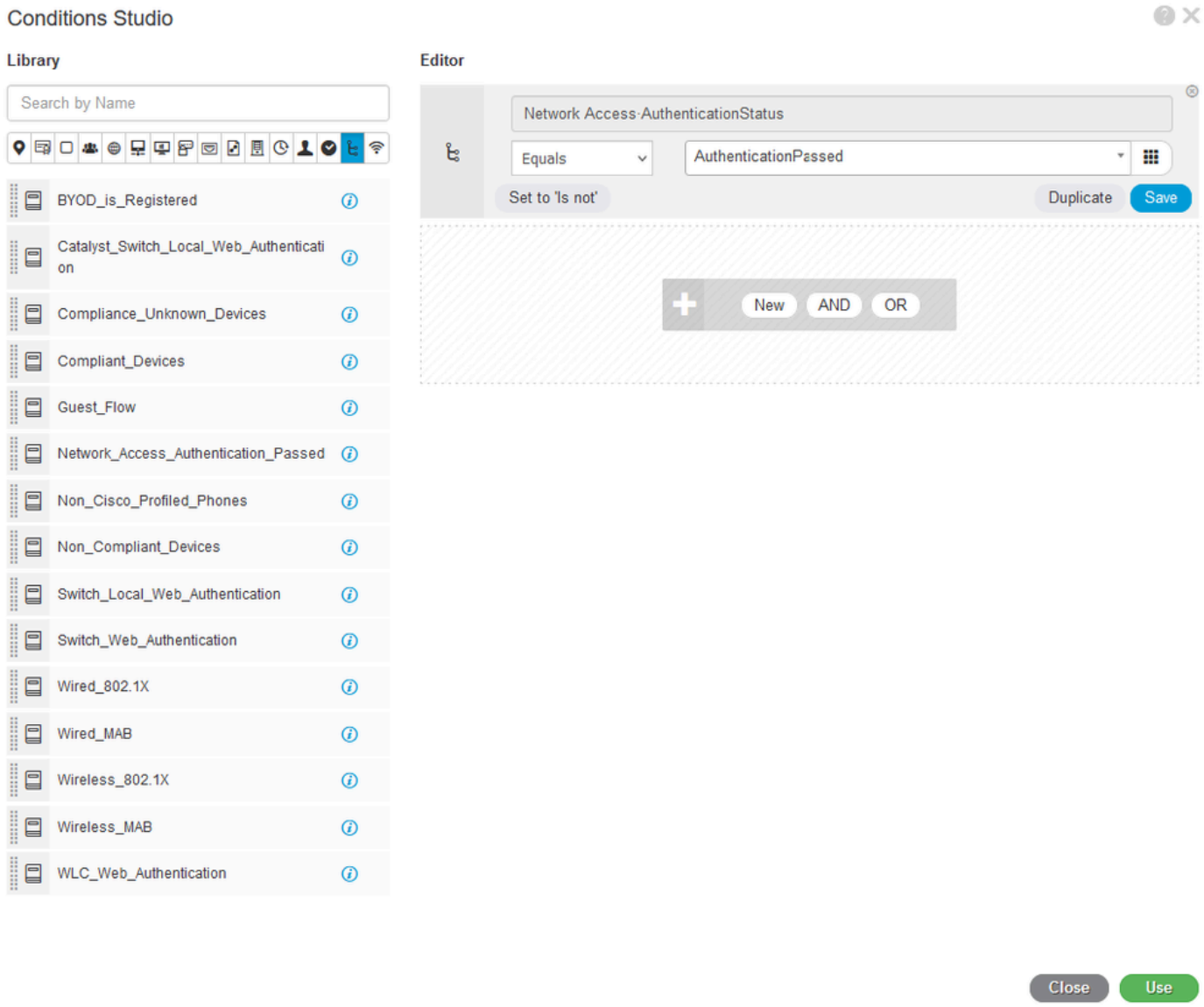
Nota: Este ejemplo permitió la lista Default Network Access Protocols . Puede crear una lista nueva y reducirla según sea necesario.

Paso 5. Para ver los nuevos conjuntos de políticas, haga clic en el icono ">" de la columna View.

Paso 5.1. Expanda el menú Directiva de autorización y haga clic en el icono + para agregar una nueva regla que permita el acceso a todos los usuarios autenticados.

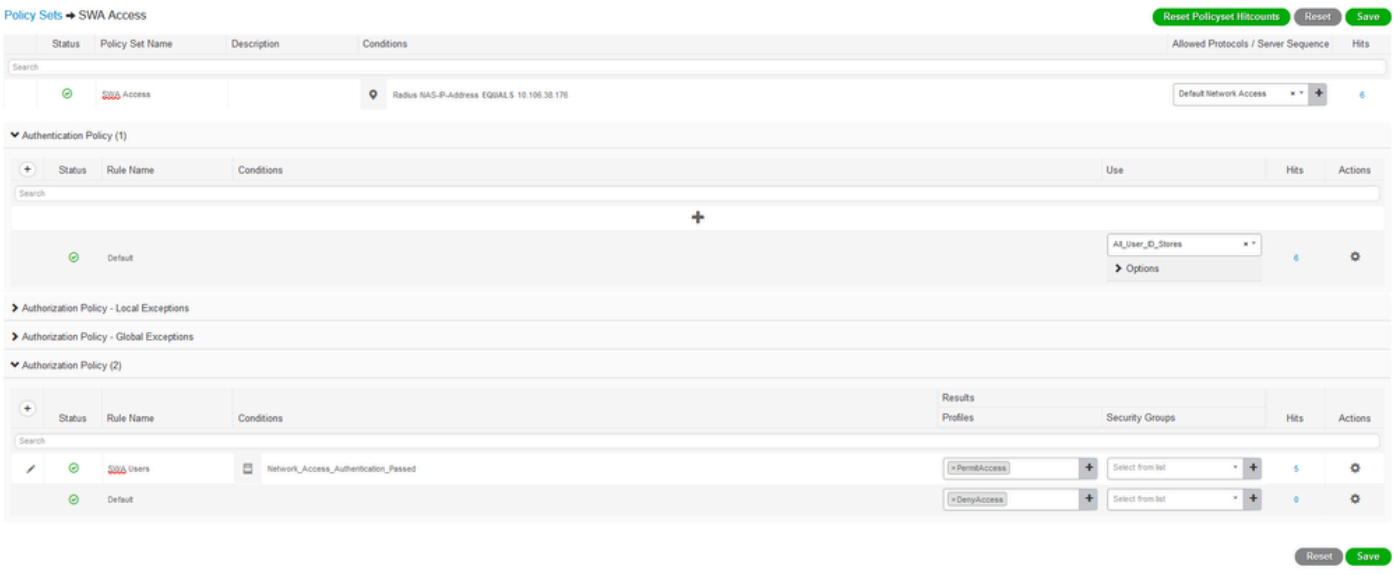
Paso 5.2. Establezca un nombre.

Paso 5.3. Establezca las condiciones para que coincidan el Acceso a la red del diccionario con el atributo AuthenticationStatus Equals AuthenticationPassed y haga clic en Usar.



Seleccionar condición de autorización

Paso 6. Establezca el valor predeterminado PermitAccess como Perfil de autorización y haga clic en Guardar.

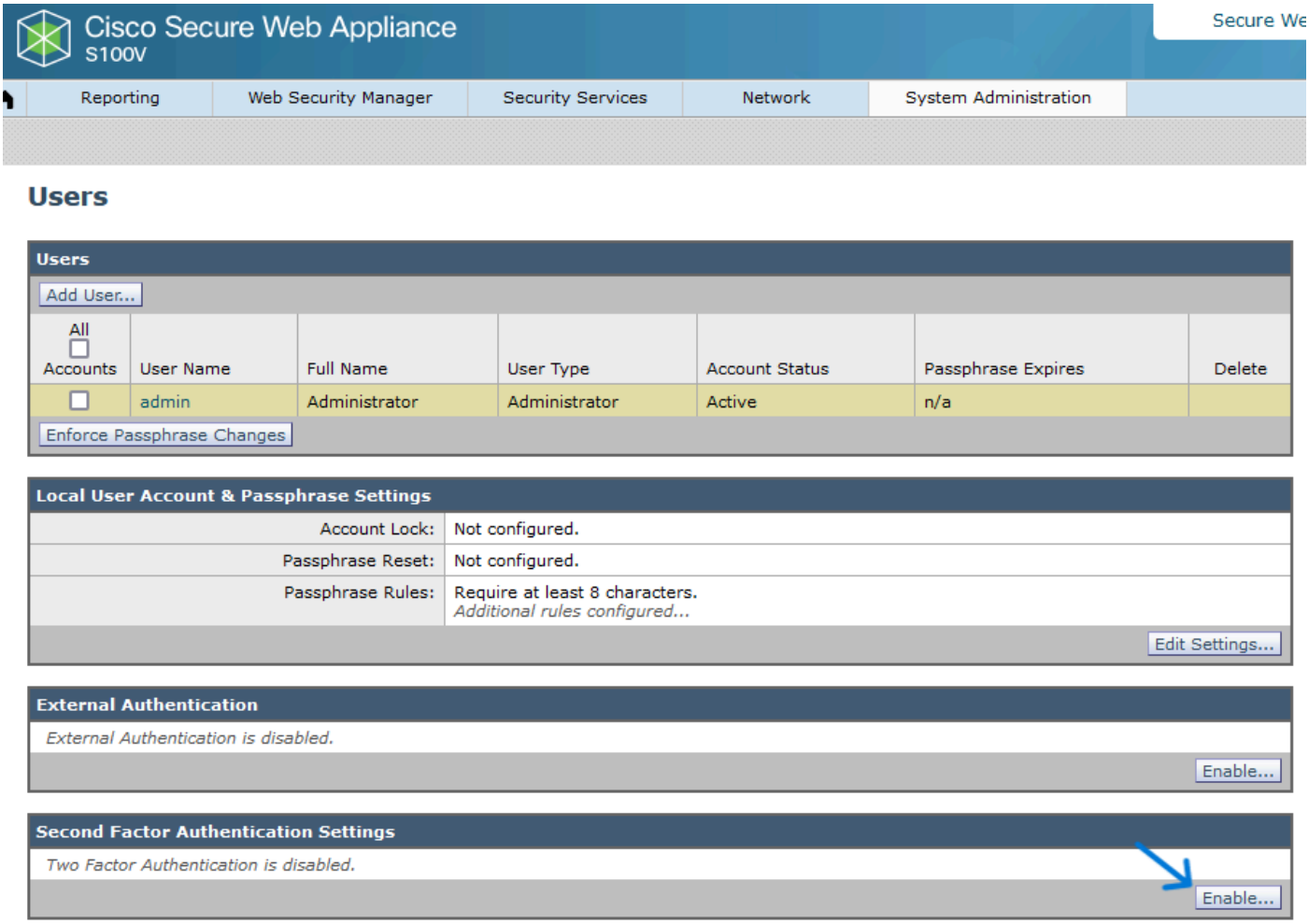


Seleccionar perfil de autorización

Configuración SWA

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

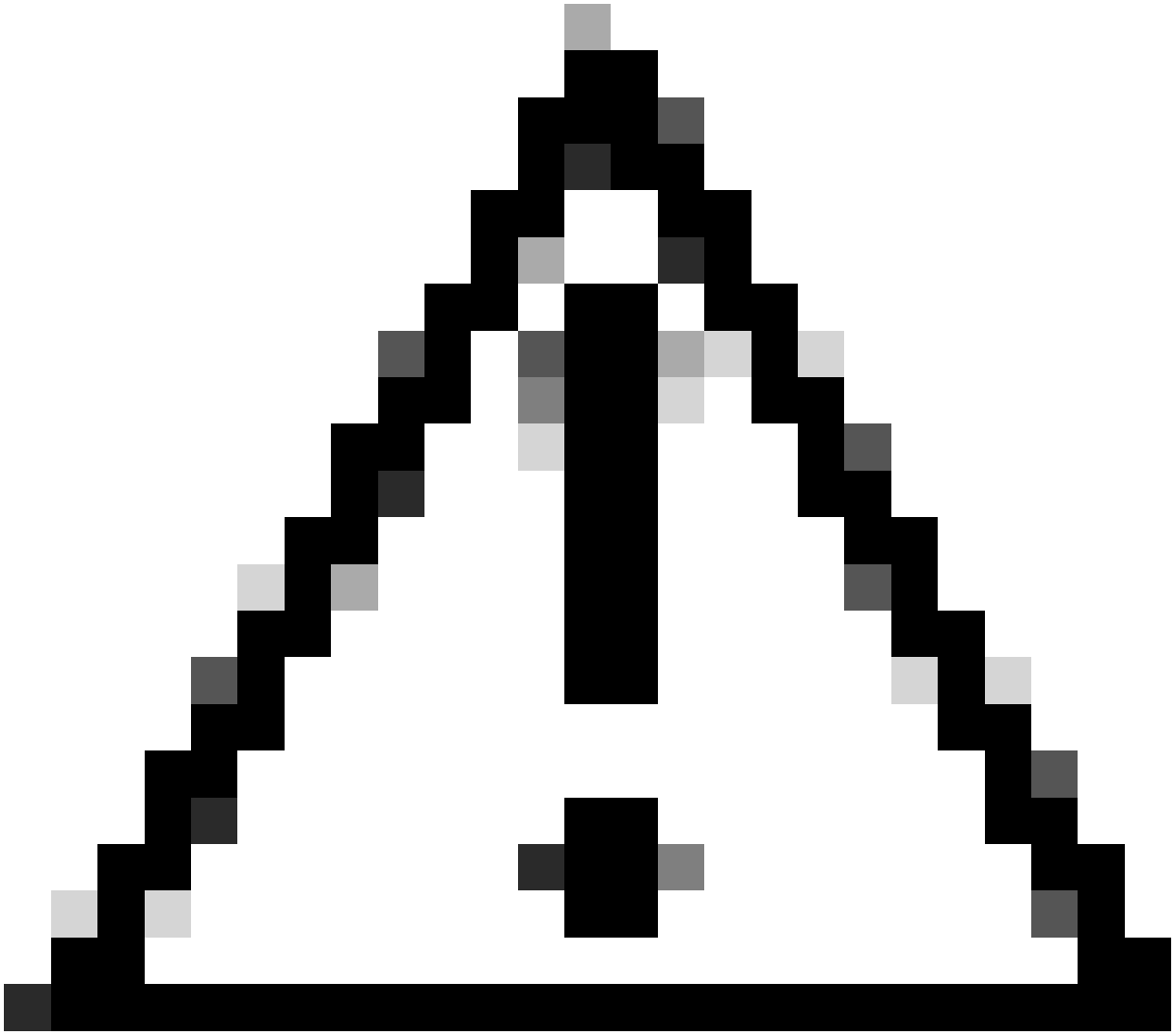
Paso 2. Haga clic en Enable en Second Factor Authentication Settings.



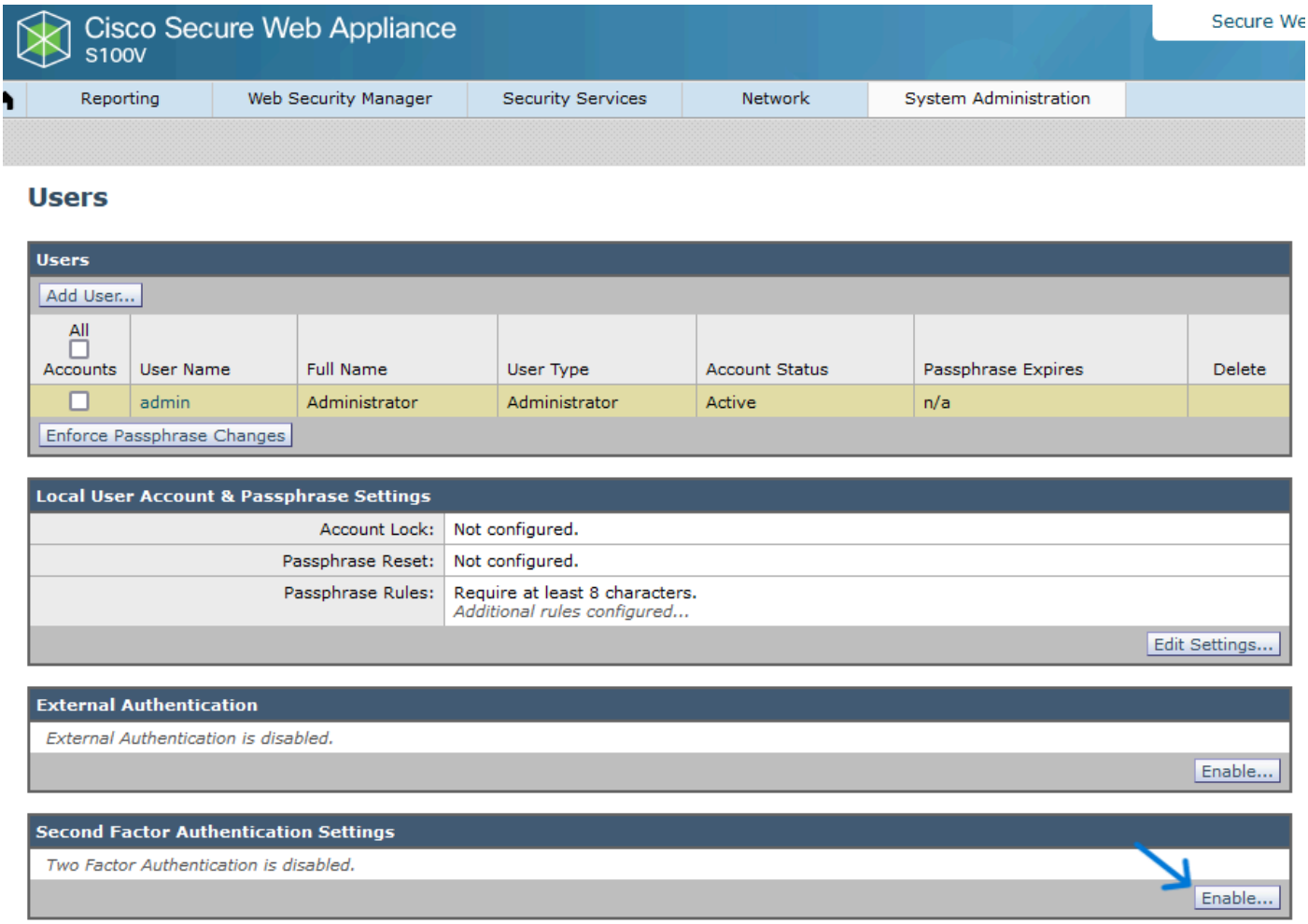
Habilitar la autenticación de segundo factor en SWA

Paso 3. Ingrese la dirección IP de ISE en el campo RADIUS Server Hostname e ingrese Shared Secret que se configura en el Paso 2 de la configuración de ISE.

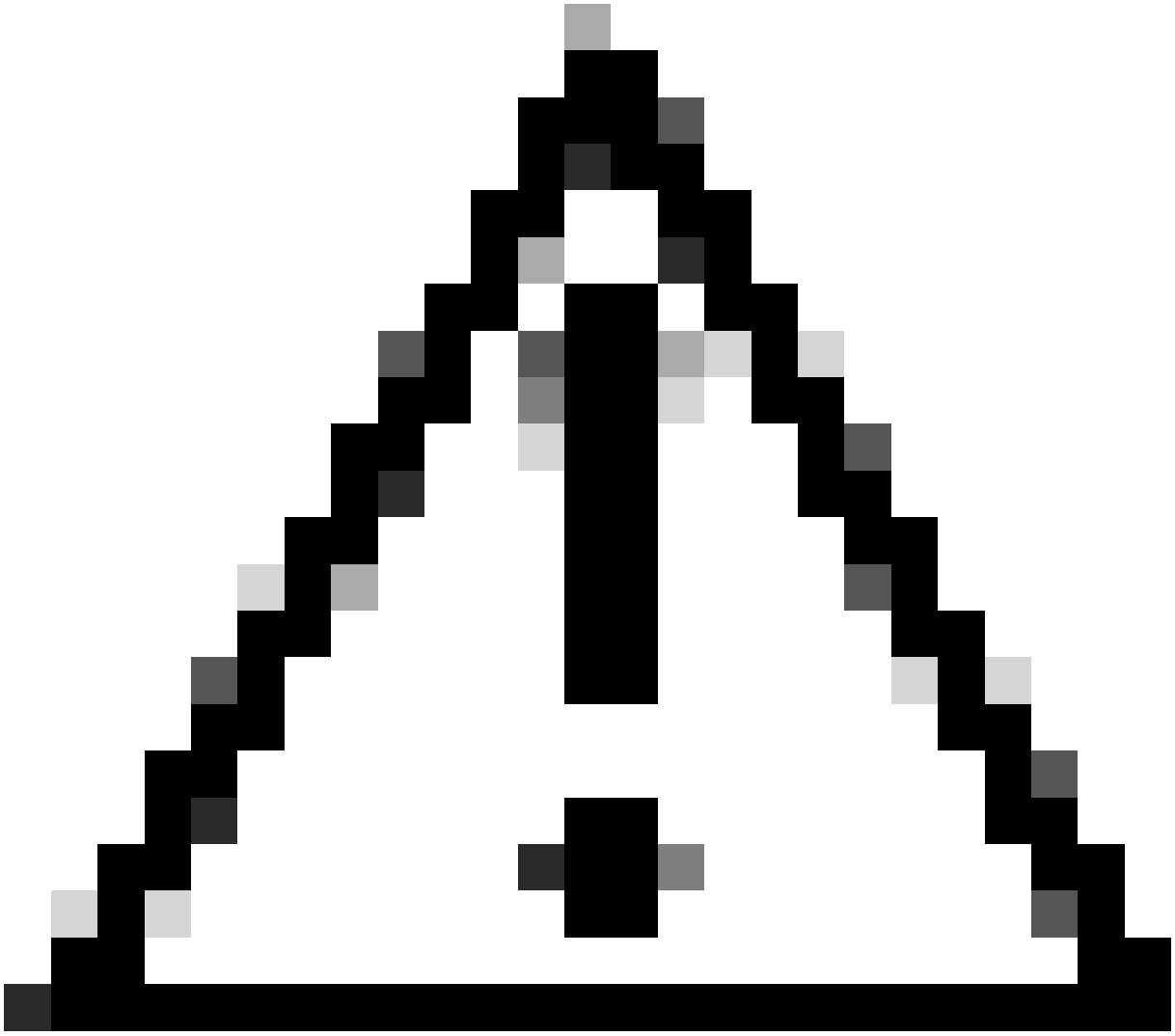
Paso 4. Seleccione los roles predefinidos necesarios que necesita que se active la aplicación de Segundo Factor.



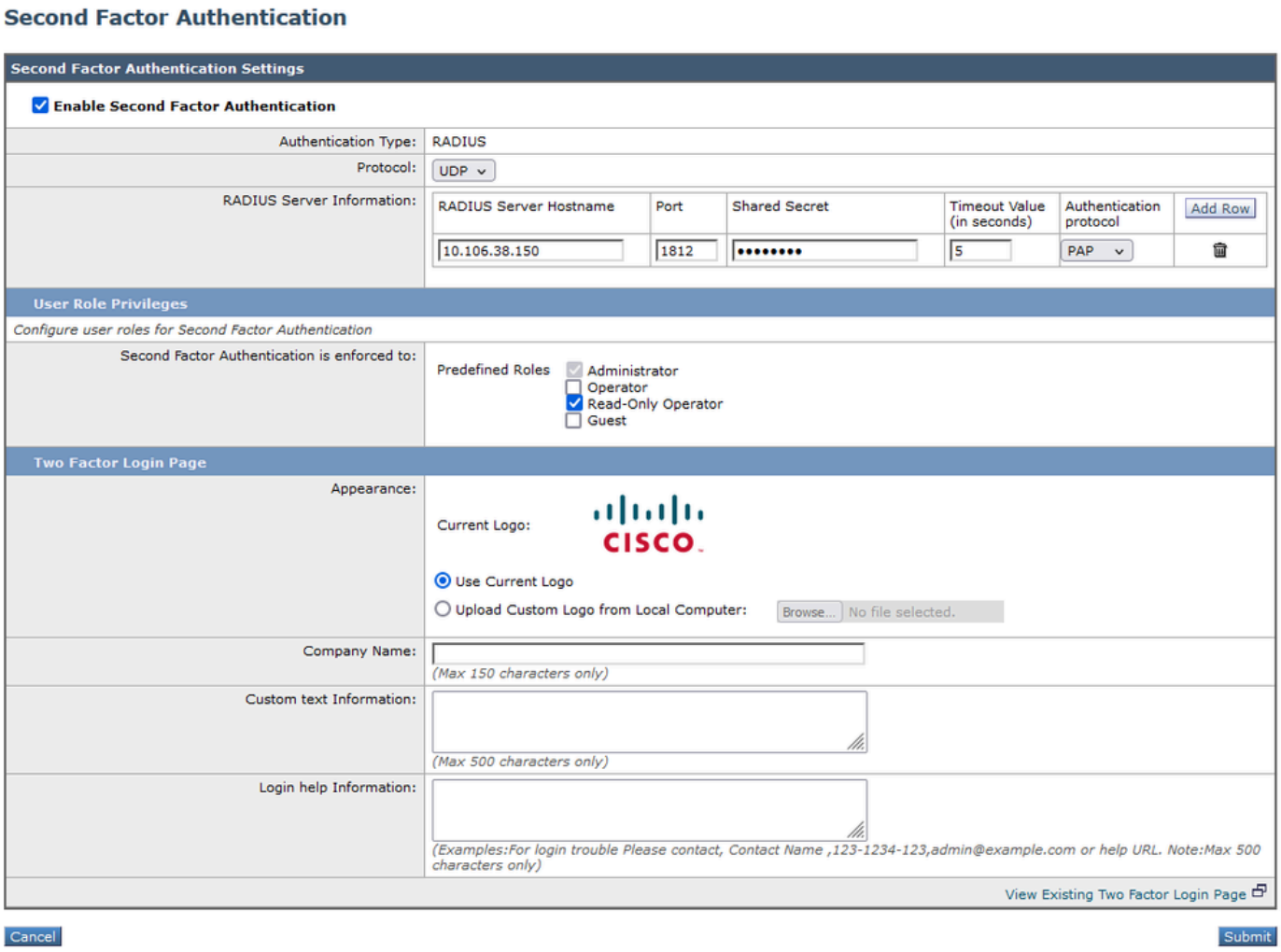
Precaución: si habilita la autenticación de segundo factor en SWA, la cuenta 'admin' predeterminada también se habilitará con la aplicación de segundo factor. Debe integrar ISE con LDAP o Active Directory (AD) para autenticar las credenciales 'admin', ya que ISE no permite configurar 'admin' como usuario de acceso a la red.



Habilitar la autenticación de segundo factor en SWA

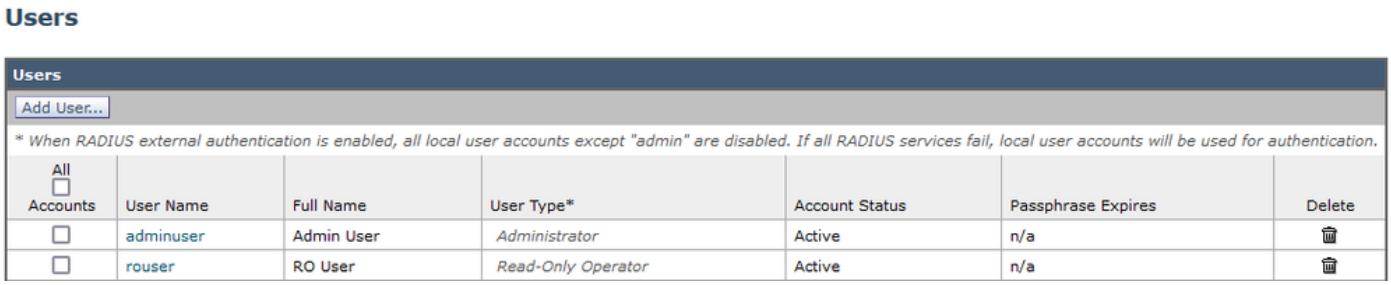


Precaución: si habilita la autenticación de segundo factor en SWA, la cuenta 'admin' predeterminada también se habilitará con la aplicación de segundo factor. Debe integrar ISE con LDAP o Active Directory (AD) para autenticar las credenciales 'admin', ya que ISE no permite configurar 'admin' como usuario de acceso a la red.



Configuración de la autenticación de segundo factor

Paso 5: Para configurar los 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.

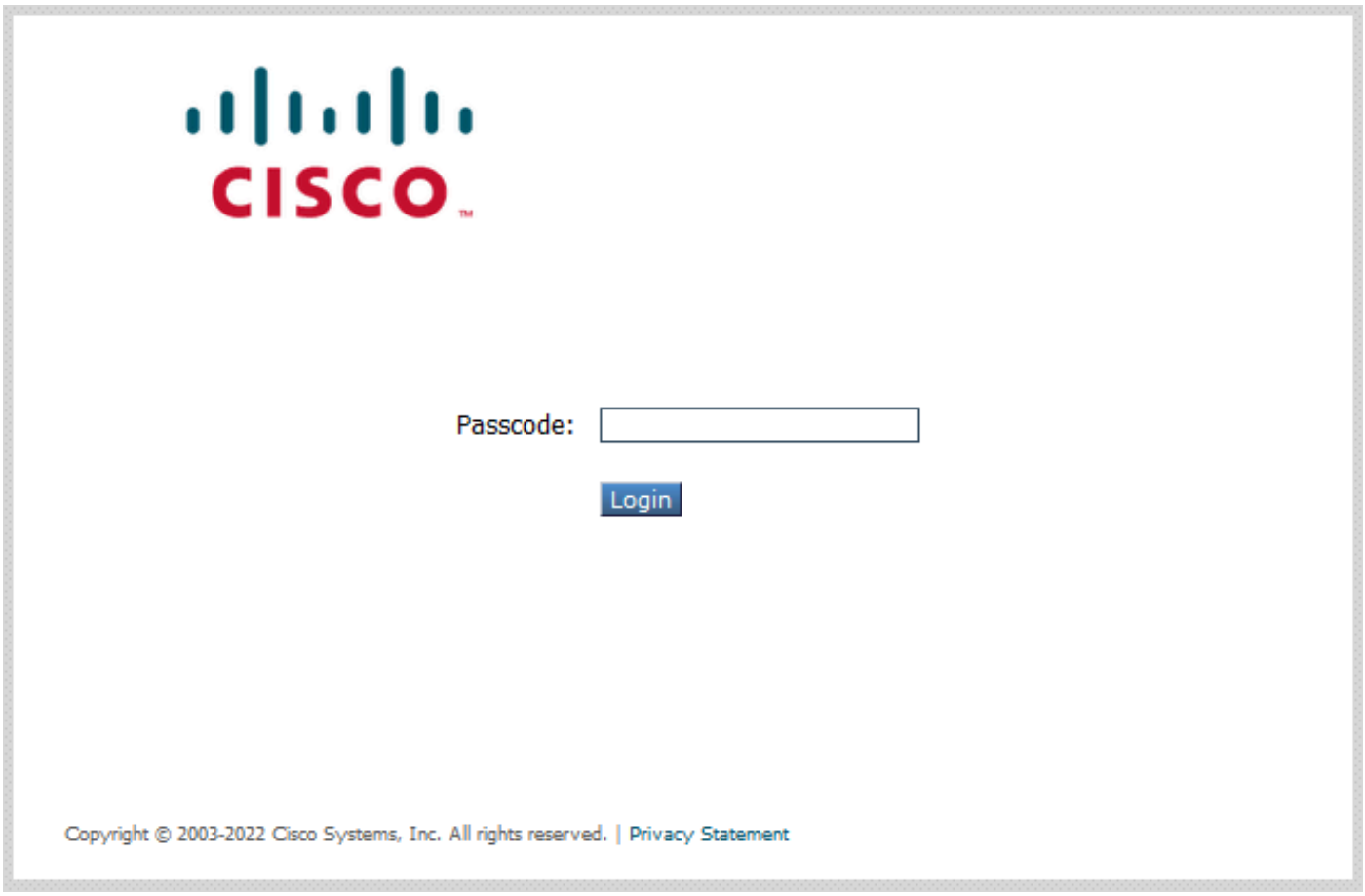


Configuración de usuario en SWA

Paso 6: Haga clic en Enviar y Registrar cambios.

Verificación

Acceda a la GUI de SWA con las credenciales de usuario configuradas. Después de una autenticación exitosa, se le redirige a la página de autenticación secundaria. Aquí debe introducir las credenciales de autenticación secundarias configuradas en ISE.



Verificar inicio de sesión de segundo factor

Referencias

- 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
- Integración de AD para la GUI de ISE y el inicio de sesión de CLI

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).