Configurar a autenticação do segundo fator SWA com ISE como um servidor RADIUS

Contents

Introdução

Este documento descreve como configurar a autenticação de segundo fator no Secure Web Appliance com o Cisco Identity Service Engine como um servidor RADIUS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimentos básicos em SWA.
- Conhecimento da configuração das políticas de autenticação e autorização no ISE.
- Conhecimento RADIUS básico.

A Cisco recomenda que você também tenha:

- Acesso de administração do Secure Web Appliance (SWA) e do Cisco Identity Service Engine (ISE).
- Seu ISE é integrado ao Ative Diretory ou LDAP.
- O Ative Diretory ou LDAP está configurado com um nome de usuário 'admin' para autenticar a conta 'admin' padrão do SWA.
- Versões compatíveis do WSA e do ISE.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- SWA 14.0.2-012
- ISE 3.0.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Quando você habilita a autenticação de segundo fator para usuários administrativos no SWA, o dispositivo verifica a credencial do usuário com o servidor RADIUS pela segunda vez após verificar as credenciais configuradas no SWA.

Topologia de rede

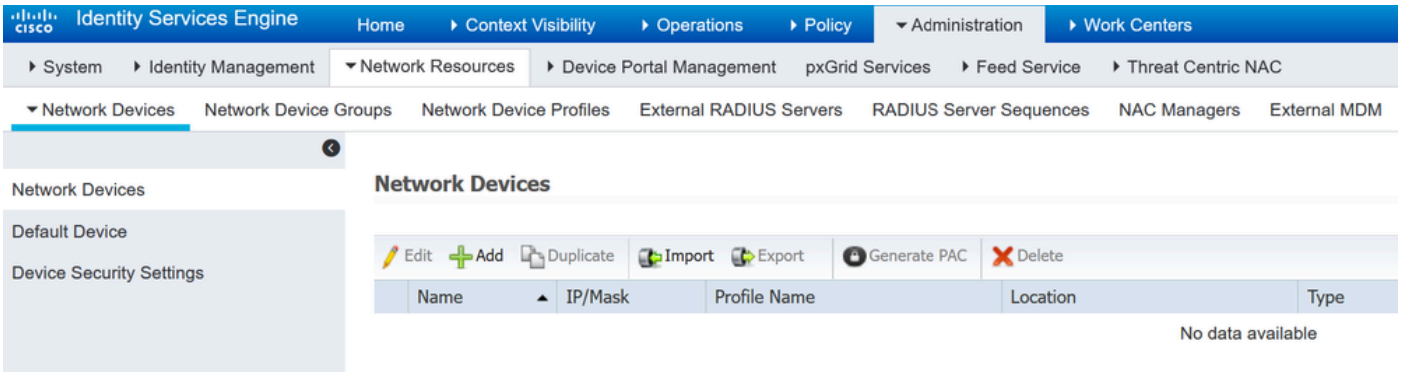
Imagem - Diagrama de topologia de rede

Os usuários administrativos acessam o SWA na porta 443 com suas credenciais. O SWA verifica as credenciais com o servidor RADIUS para a autenticação de segundo fator.

Configuration Steps

Configuração do ISE

Etapa 1. Adicione um novo dispositivo de rede. Navegue até Administração > Recursos de rede > Dispositivos de rede > +Adicionar.



Adicionar SWA como dispositivo de rede no ISE

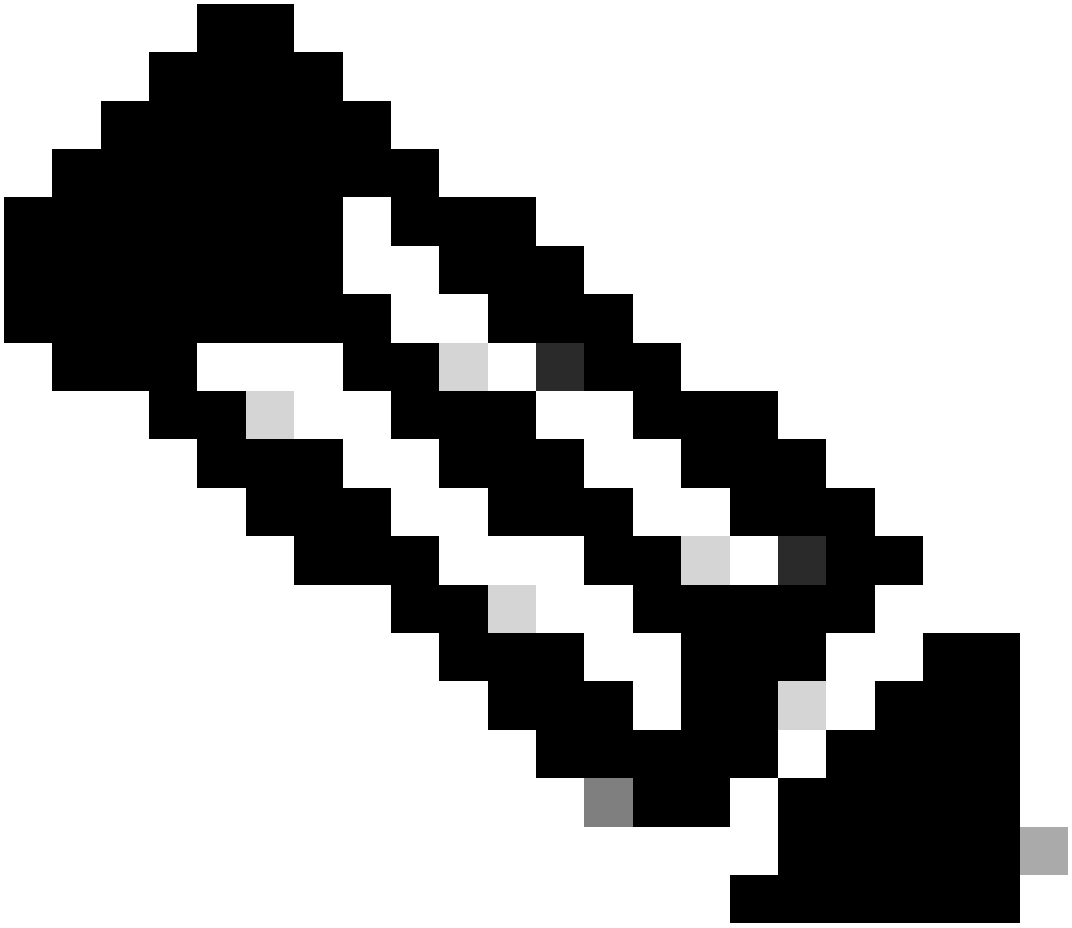
Etapa 2. Configure o dispositivo de rede no ISE.

Etapa 2.1. Atribua um Nome ao objeto de dispositivo de rede.

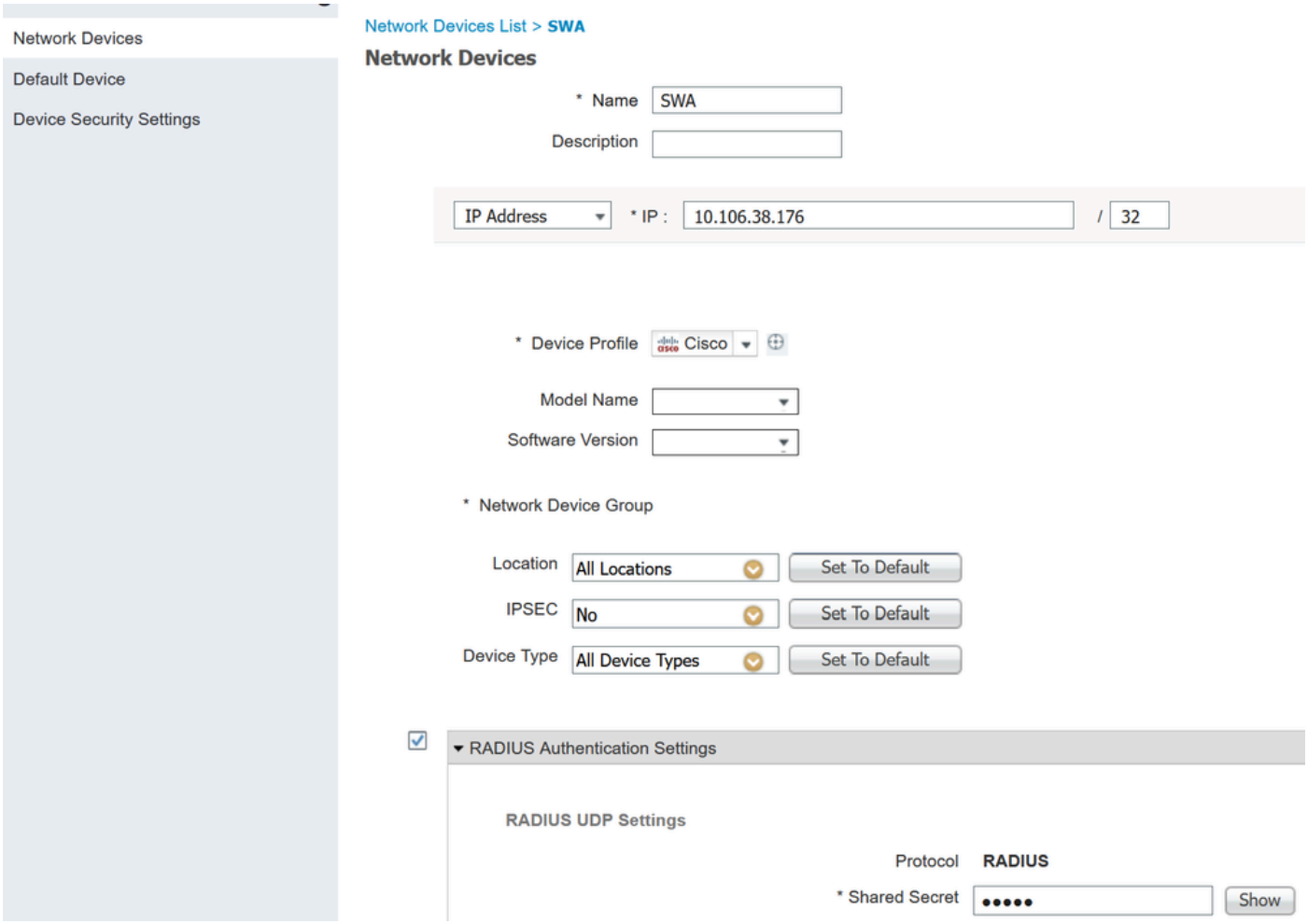
Etapa 2.2. Insira o endereço IP do SWA.

Etapa 2.3. Marque a caixa de seleção RADIUS.

Etapa 2.4. Defina um segredo compartilhado.

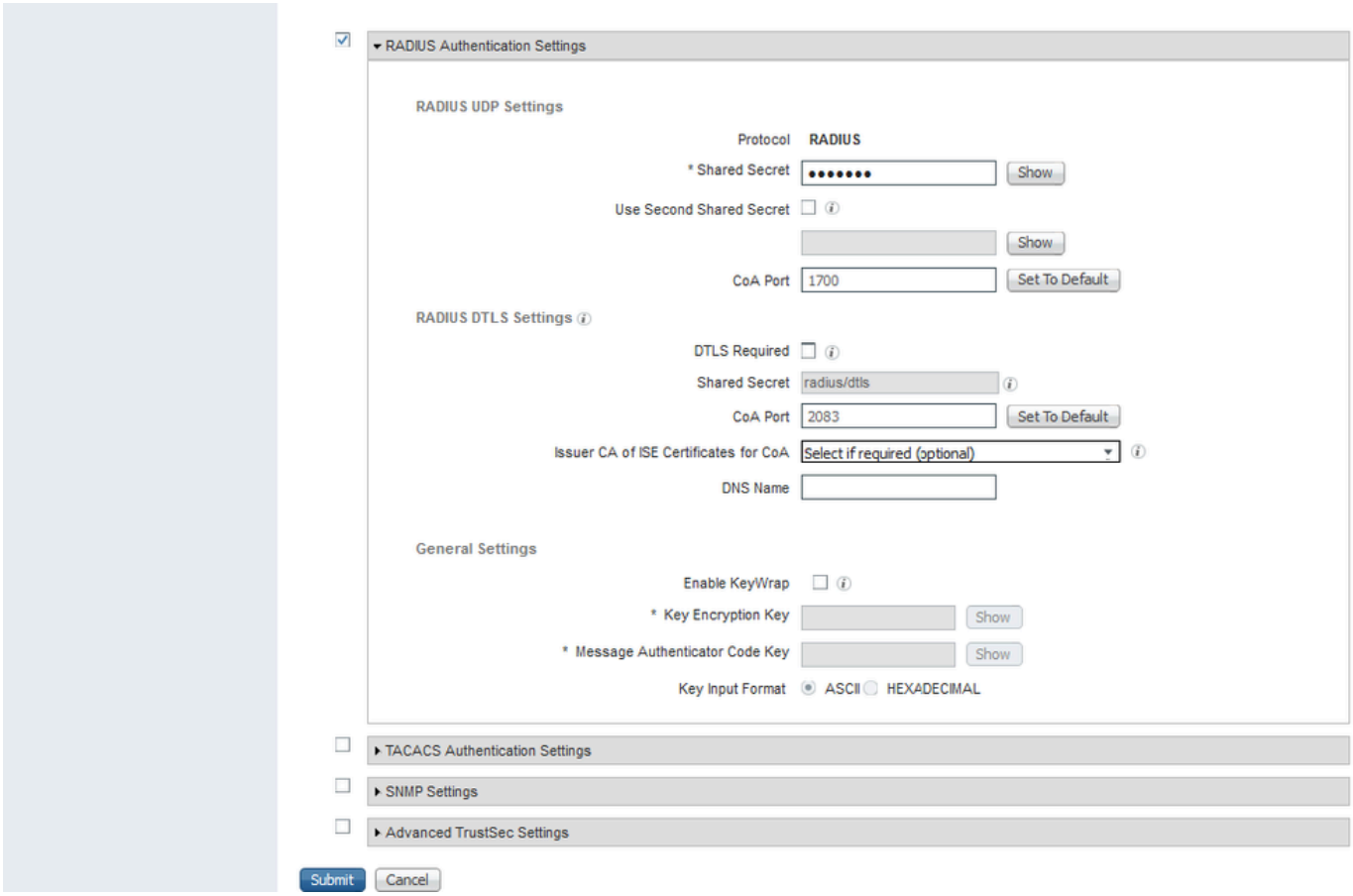


Observação: a mesma chave deve ser usada posteriormente para configurar o SWA.



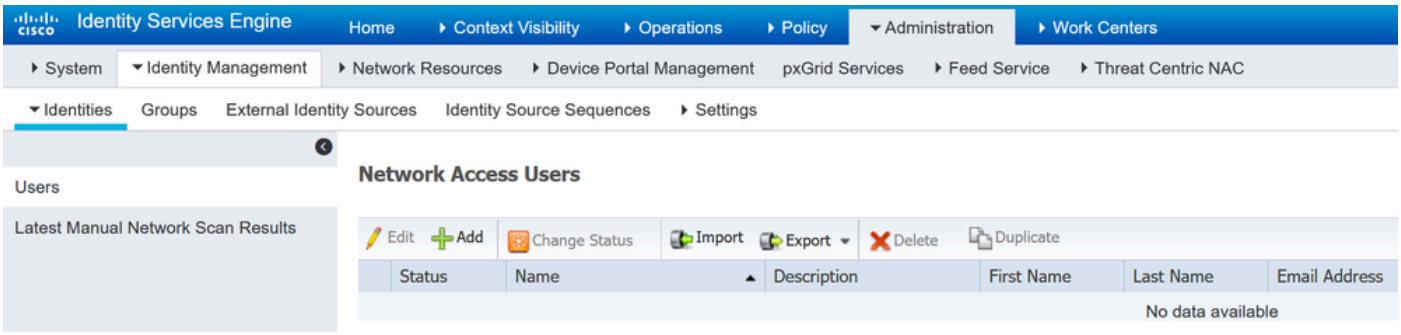
Configurar chave compartilhada do dispositivo de rede SWA

Etapa 2.5. Clique em Submit.



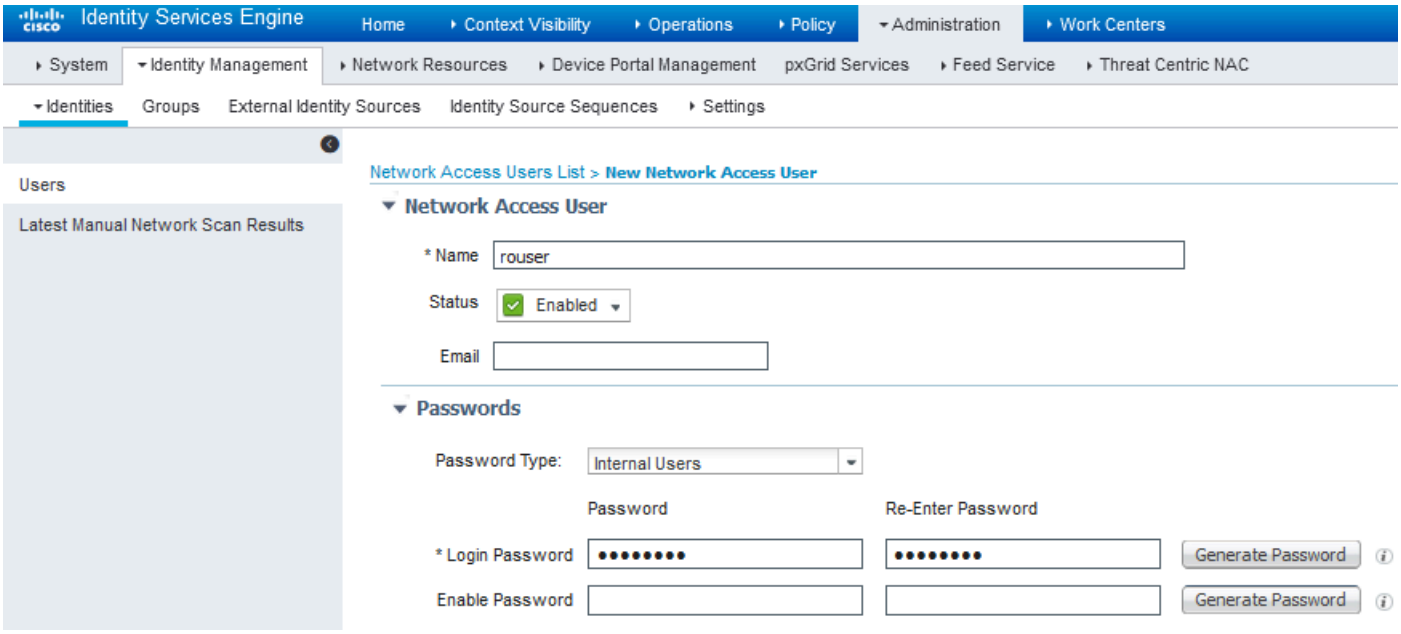
Enviar configuração do dispositivo de rede

Etapa 3. Você precisa criar Usuários de acesso à rede que correspondam ao nome de usuário configurado no SWA. Navegue até Administração > Gerenciamento de identidades > Identidades > + Adicionar.



Adicionar usuários locais no ISE

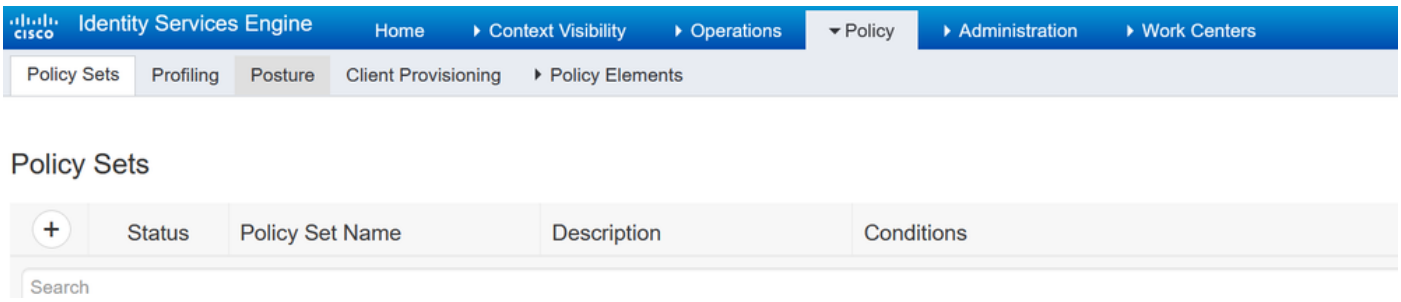
Etapa 3.1. Atribua um Nome.
Etapa 3.2. (Opcional) Insira o endereço de e-mail do usuário.
Etapa 3.3. Definir senha.
Etapa 3.4. Click Save.



Adicionar um usuário local no ISE

Etapa 4. Crie um conjunto de políticas que corresponda ao endereço IP SWA. Isso evita o acesso a outros dispositivos com essas credenciais de usuário.

Navegue até Policy > PolicySets e clique no ícone + no canto superior esquerdo.

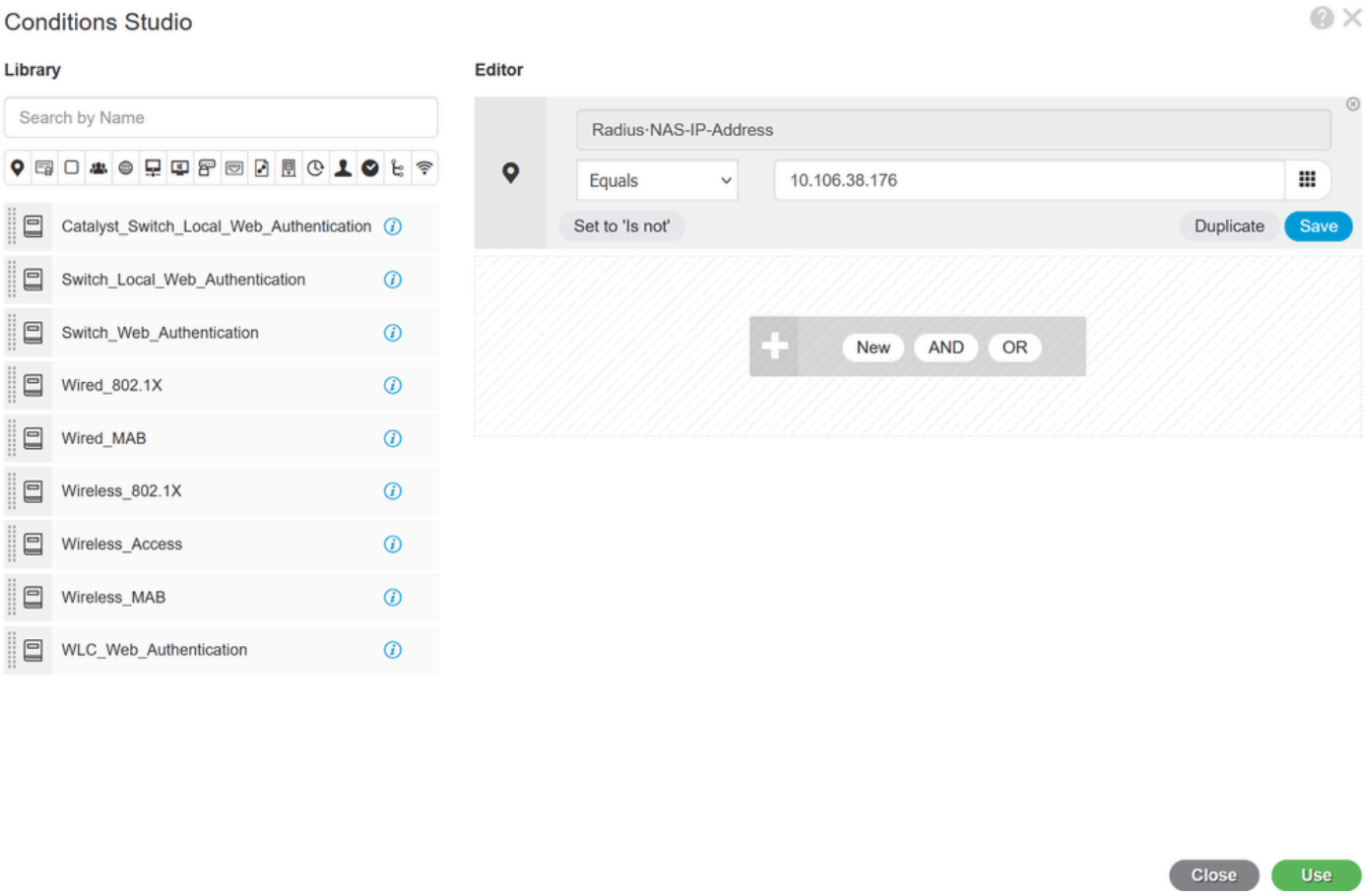


Adicionar conjunto de políticas no ISE

Etapa 4.1. Uma nova linha é colocada na parte superior dos conjuntos de políticas. Digite o nome da nova política.

Etapa 4.2. Adicione uma condição para o atributo RADIUS NAS-IP-Address corresponder ao endereço IP do SWA.

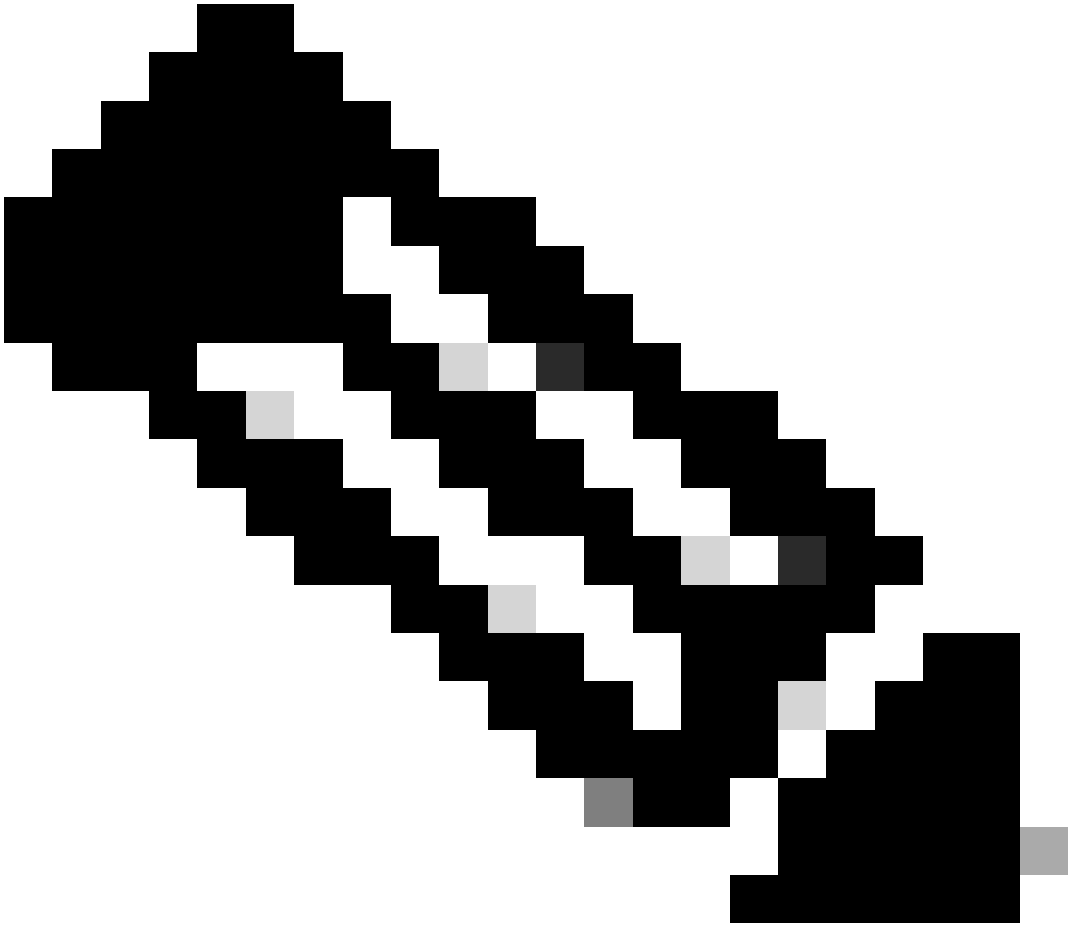
Etapa 4.3. Clique em Usar para manter as alterações e sair do editor.



Adicionar política para mapear o dispositivo de rede SWA

Etapa 4.4. Click Save.

Salvamento de política



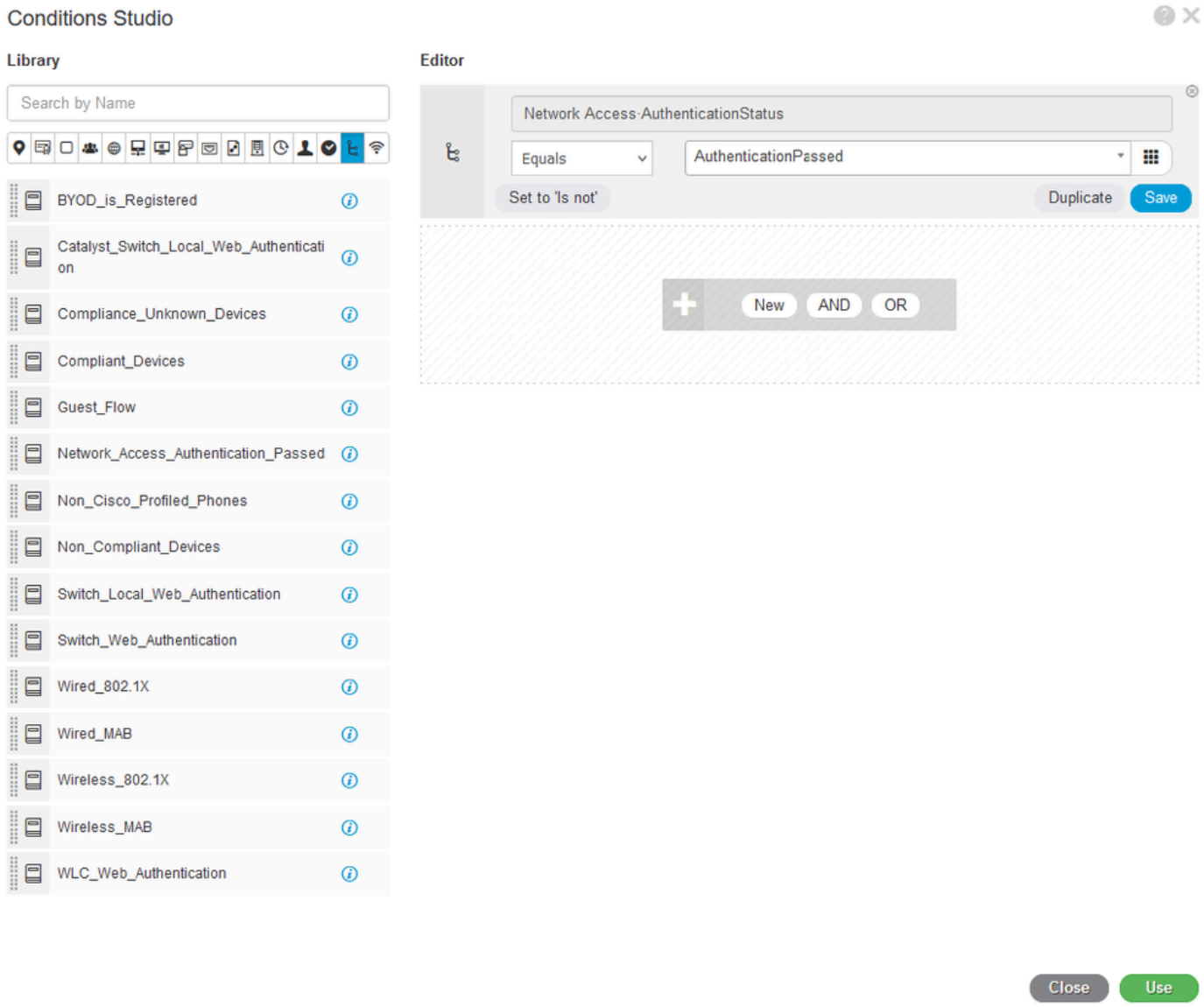
Observação: este exemplo permitiu a lista Default Network Access Protocols. Você pode criar uma nova lista e restringi-la conforme necessário.

Etapa 5. Para exibir os novos conjuntos de políticas, clique no ícone ">" na colunaExibir.

Etapa 5.1. Expanda o menu Authorization Policy (Diretiva de autorização) e clique no ícone + para adicionar uma nova regra para permitir o acesso a todos os usuários autenticados.

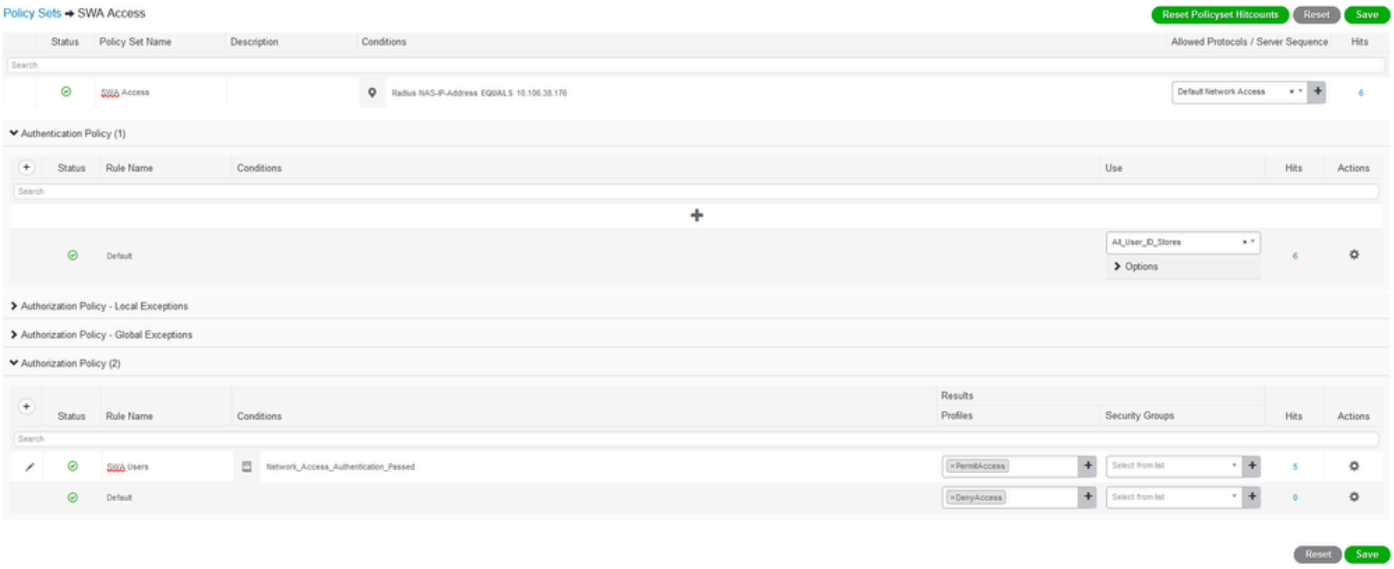
Etapa 5.2. Defina um nome.

Etapa 5.3. Defina as condições para corresponder ao Acesso à Rede do Dicionário com o Atributo AuthenticationStatus Equals AuthenticationPassed e clique em Use.



Selecionar condição de autorização

Etapa 6. Defina o PermitAccess padrão como Perfil de autorização e clique em Salvar.

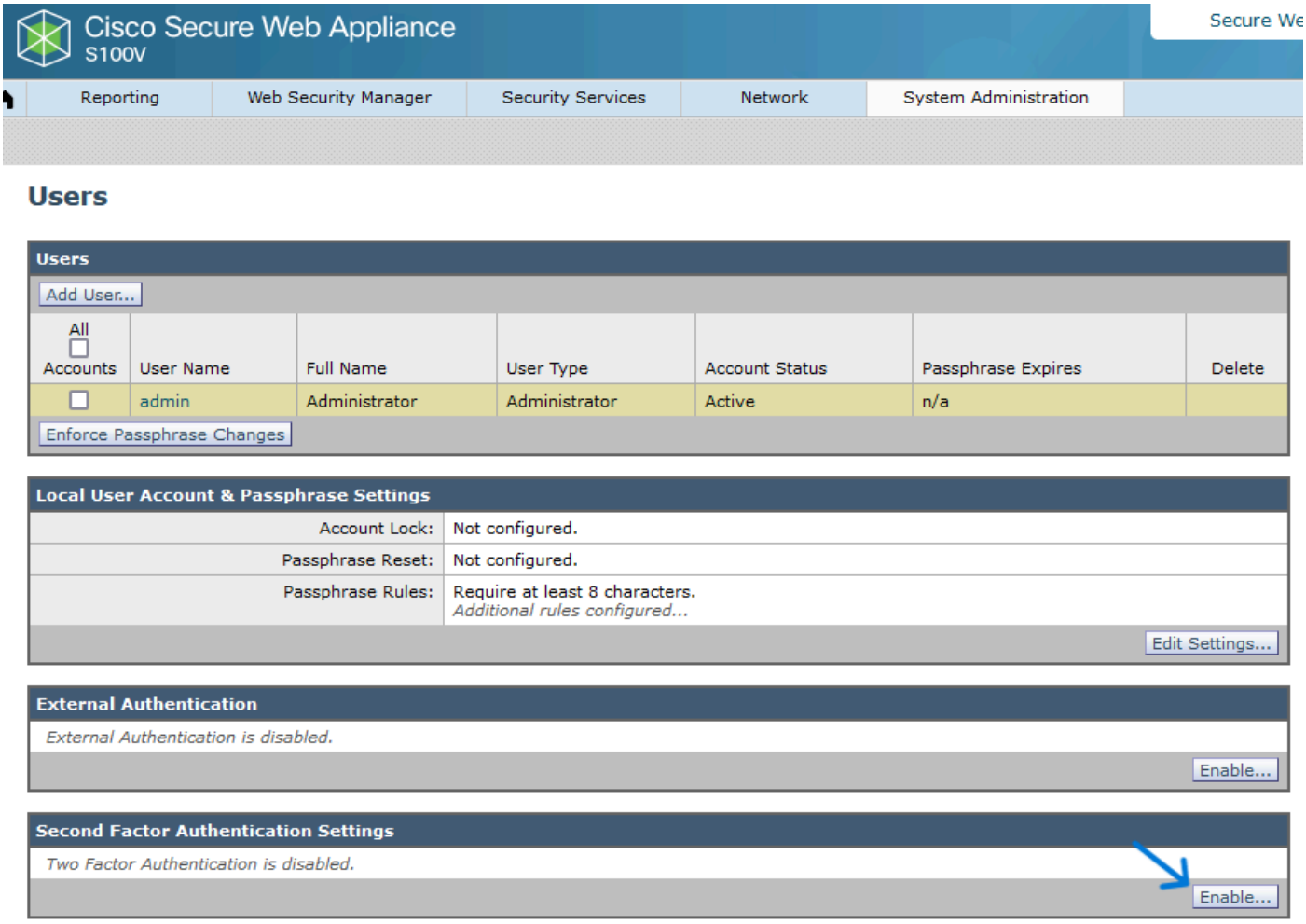


Selecionar perfil de autorização

Configuração de SWA

Etapa 1. Na GUI do SWA, navegue para Administração do sistema e clique em Usuários.

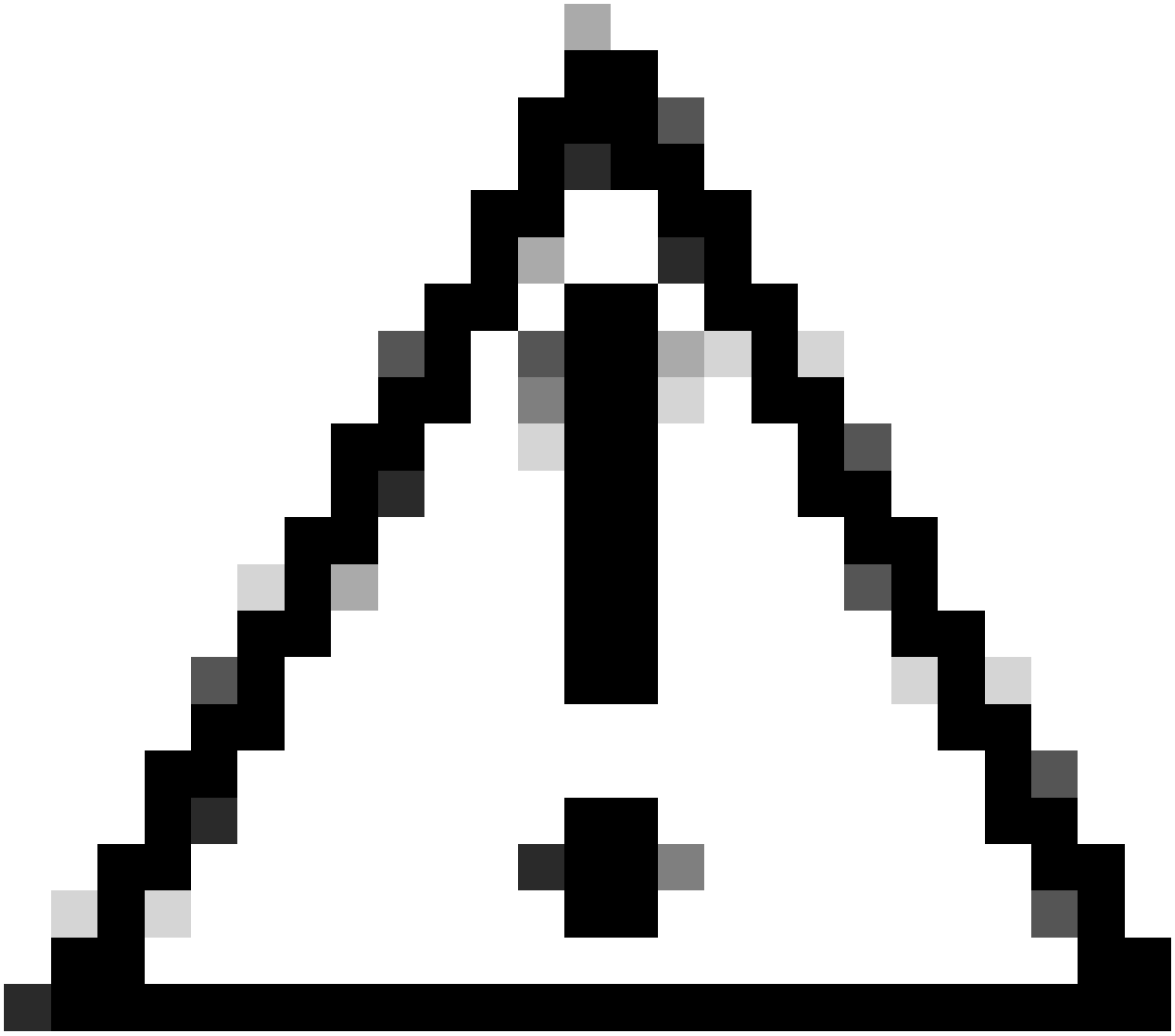
Etapa 2. Clique em Enable em Second Fator Authentication Settings.



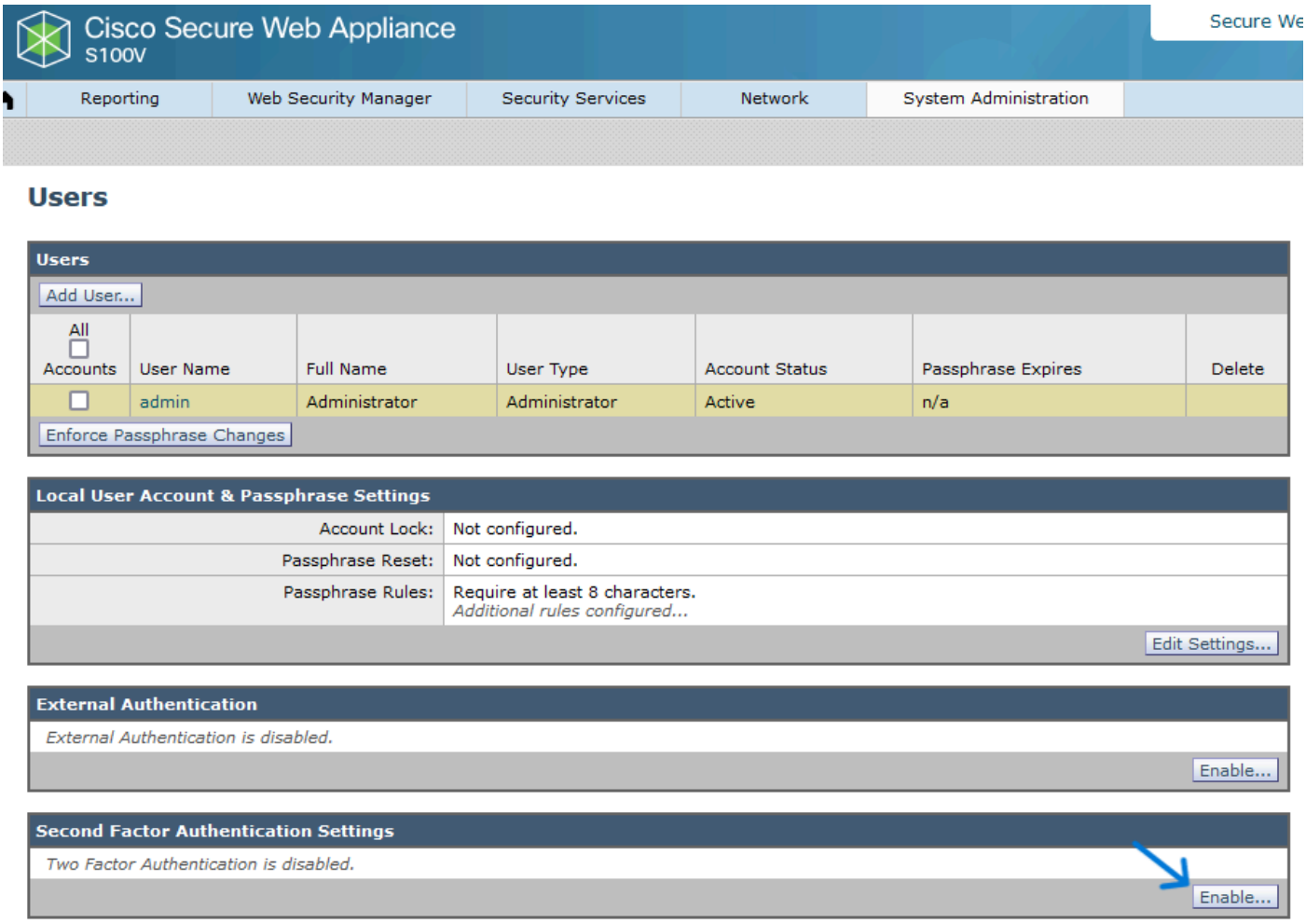
Habilitar segunda autenticação de fator em SWA

Etapa 3. Insira o endereço IP do ISE no campo RADIUS Server Hostname e insira Shared Secret que está configurado na Etapa 2 da configuração do ISE.

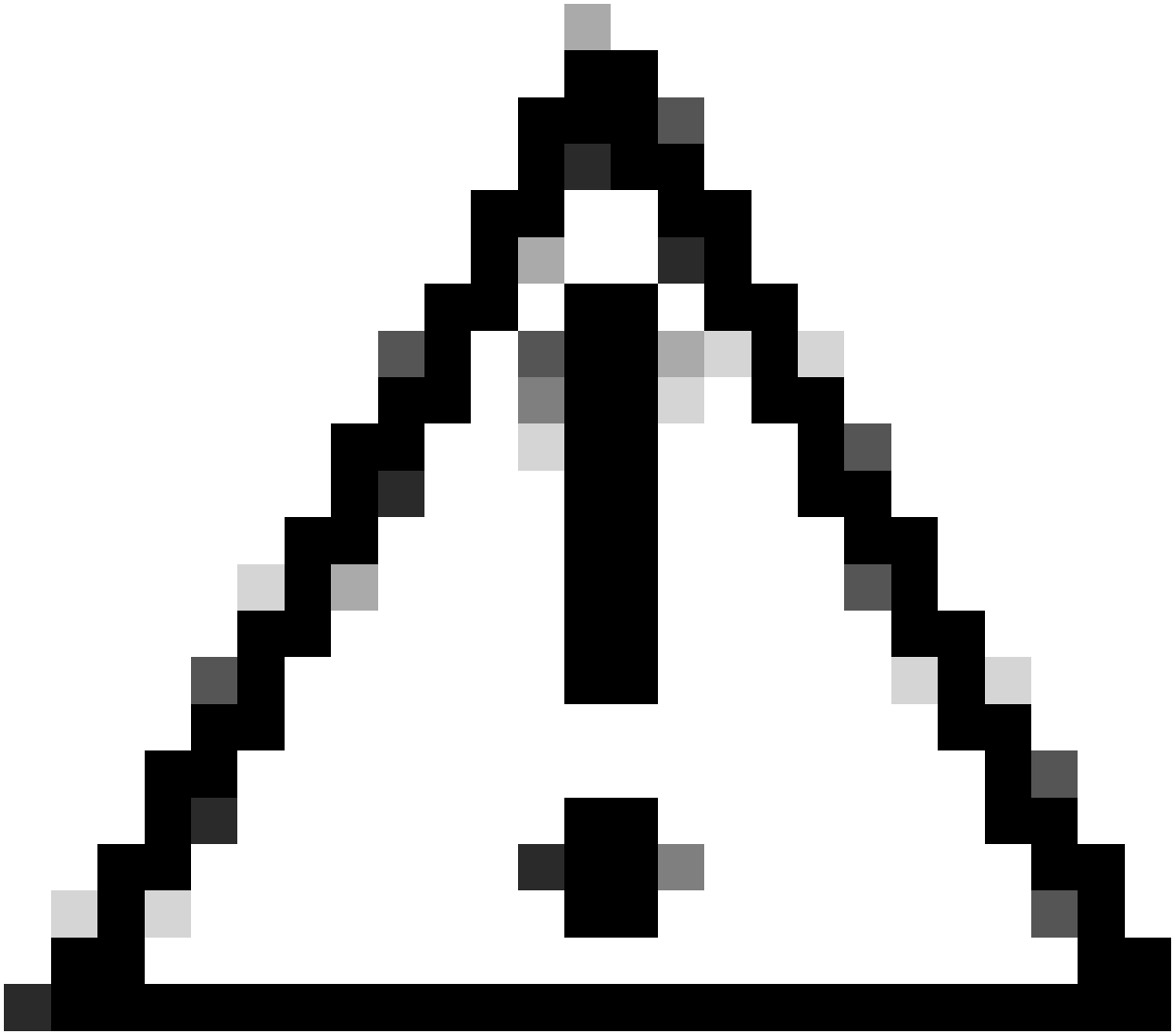
Etapa 4. Selecione as Funções Predefinidas necessárias que você precisa que a imposição do Segundo Fator esteja habilitada.



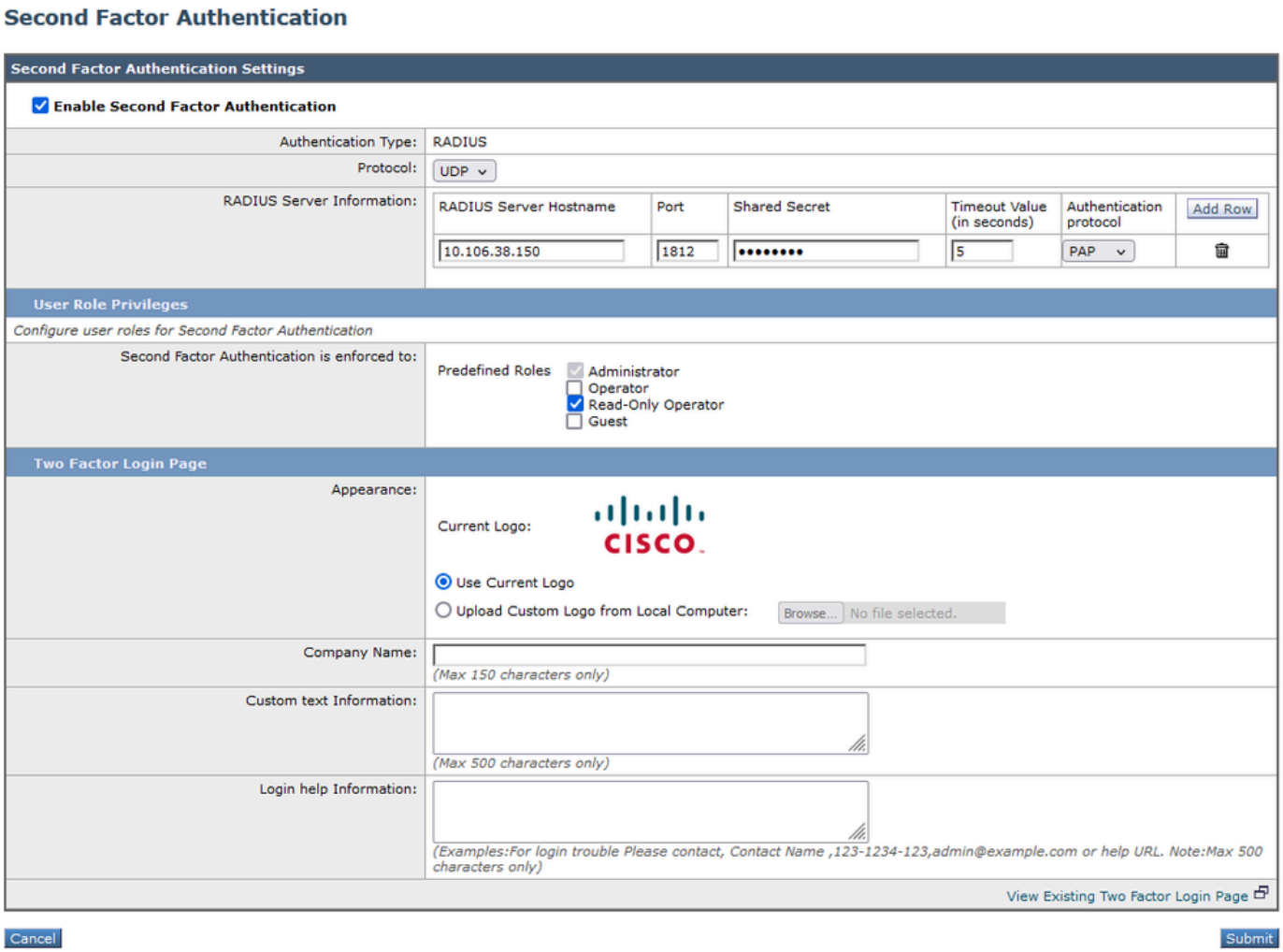
Cuidado: se você habilitar a autenticação de segundo fator no SWA, a conta 'admin' padrão também será habilitada com a aplicação de Segundo Fator. É necessário integrar o ISE com LDAP ou Ative Diretory (AD) para autenticar credenciais 'admin', pois o ISE não permite configurar 'admin' como um usuário de acesso à rede.



Habilitar segunda autenticação de fator em SWA

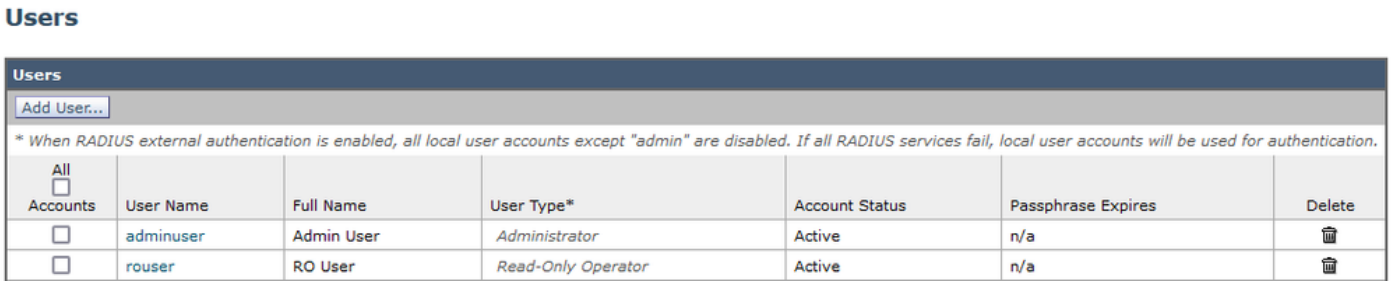


Cuidado: se você habilitar a autenticação de segundo fator no SWA, a conta 'admin' padrão também será habilitada com a aplicação de Segundo Fator. É necessário integrar o ISE com LDAP ou Ative Diretory (AD) para autenticar credenciais 'admin', pois o ISE não permite configurar 'admin' como um usuário de acesso à rede.



Configurar Autenticação de Segundo Fator

Etapa 5: Para configurar usuários no SWA, clique em Adicionar usuário. Insira User Name e selecione User Type necessário para a função desejada. Insira Passphrase e Redigite Passphrase.

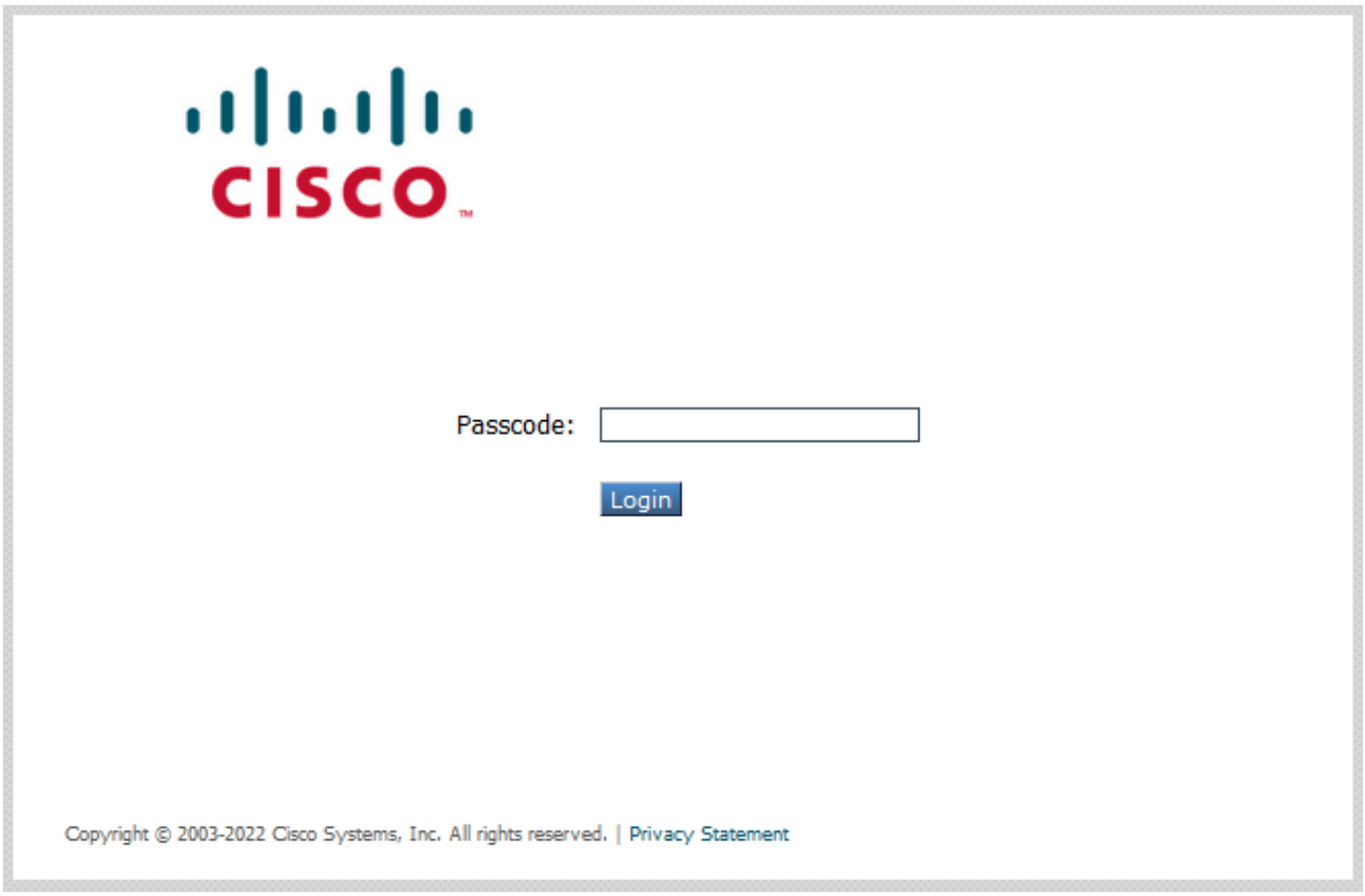


Configuração do usuário no SWA

Etapa 6: Clique em Enviar e em Confirmar alterações.

Verificar

Acesse a GUI do SWA com as credenciais de usuário configuradas. Após a autenticação bem-sucedida, você será redirecionado para a página de autenticação secundária. Aqui, você precisa inserir as credenciais de autenticação secundária configuradas no ISE.



Verificar o login do segundo fator

Referências

- Manual do usuário do AsyncOS 14.0 para Cisco Secure Web Appliance
- Guia do administrador do ISE 3.0
- Matriz de compatibilidade do ISE para Secure Web Appliance
- Integrar o AD para GUI do ISE e CLI Fazer login

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.