

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

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Topologia de rede](#)

[Configuration Steps](#)

[Configuração do ISE](#)

[Configuração de SWA](#)

[Verificar](#)

[Referências](#)

---

## 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 Active Directory ou LDAP.
- O Active Directory 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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices

Default Device

Device Security Settings

**Network Devices**

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type
No data available				

Adicionar SWA como dispositivo de rede no ISE

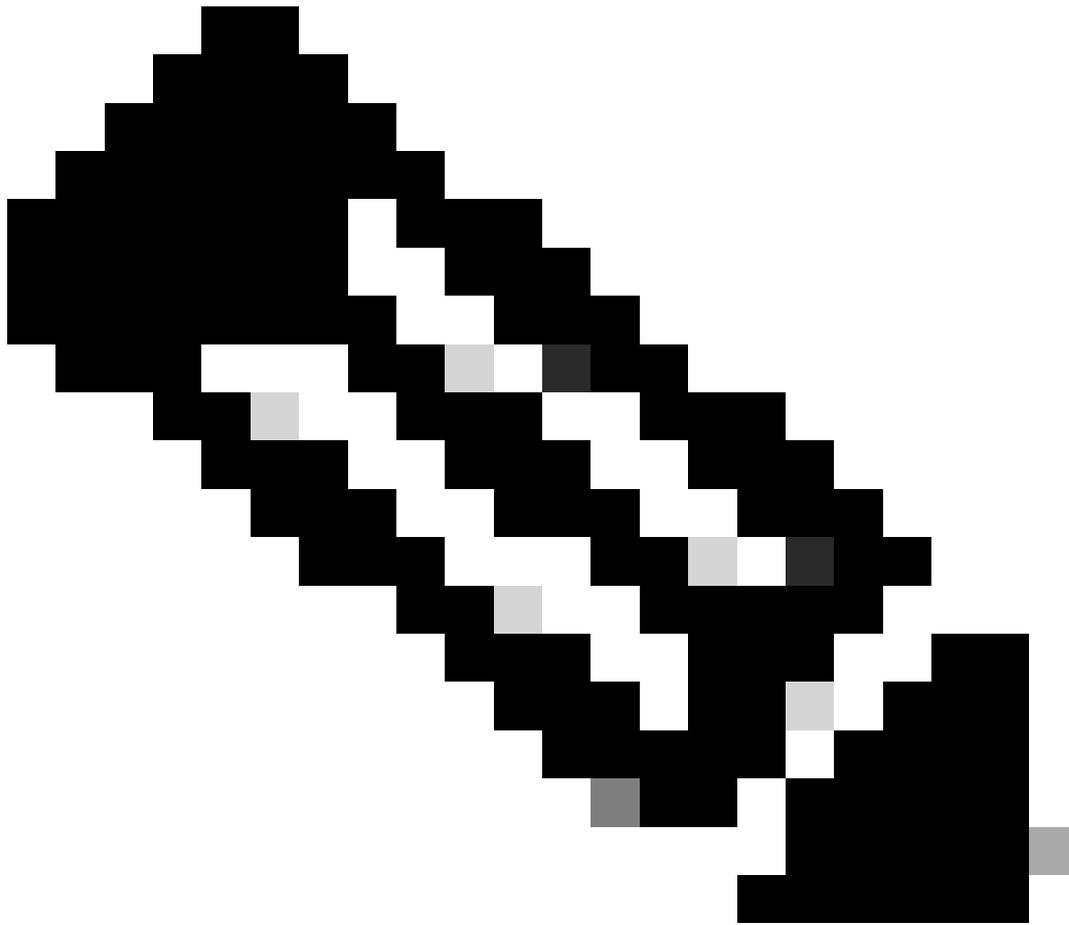
Etapa 2. Configure o dispositivo de rede no ISE.

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.

---

Network Devices

Default Device

Device Security Settings

[Network Devices List > SWA](#)

### Network Devices

\* Name

Description

IP Address  /

\* Device Profile  Cisco

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

**RADIUS Authentication Settings**

#### RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret

Configurar chave compartilhada do dispositivo de rede SWA

Etapa 2.5. Clique em Submit.

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol: **RADIUS**

\* Shared Secret:

Use Second Shared Secret:  ⓘ

CoA Port:

**RADIUS DTLS Settings ⓘ**

DTLS Required:  ⓘ

Shared Secret:  ⓘ

CoA Port:

Issuer CA of ISE Certificates for CoA:  ⓘ

DNS Name:

**General Settings**

Enable KeyWrap:  ⓘ

\* Key Encryption Key:

\* Message Authenticator Code Key:

Key Input Format:  ASCII  HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

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.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

**Network Access Users**

Users

Latest Manual Network Scan Results

Status	Name	Description	First Name	Last Name	Email Address
No data available					

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.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

**Network Access User**

\* Name:

Status:  Enabled

Email:

---

**Passwords**

Password Type:

Password:  Re-Enter Password:

\* Login Password:   ⓘ

Enable Password:   ⓘ

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.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

Policy Sets

+	Status	Policy Set Name	Description	Conditions
Search				

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.





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 coluna Exibir.

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.

## Conditions Studio

### Library

Search by Name

BYOD\_is\_Registered

Catalyst\_Switch\_Local\_Web\_Authentication

Compliance\_Unknown\_Devices

Compliant\_Devices

Guest\_Flow

Network\_Access\_Authentication\_Passed

Non\_Cisco\_Profiled\_Phones

Non\_Compliant\_Devices

Switch\_Local\_Web\_Authentication

Switch\_Web\_Authentication

Wired\_802.1X

Wired\_MAB

Wireless\_802.1X

Wireless\_MAB

WLC\_Web\_Authentication

### Editor

Network Access:AuthenticationStatus

Equals AuthenticationPassed

Set to 'Is not'

Duplicate Save

+ New AND OR

Close Use

Selecionar condição de autorização

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

Policy Sets → SWA Access

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	SWA Access		Radius NAS-IP-Address EQUALS 10.106.38.176	Default Network Access	6

▼ Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		AI_User_ID_Stores	6	

► Authorization Policy - Local Exceptions

► Authorization Policy - Global Exceptions

▼ Authorization Policy (2)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
✓	SWA Users	Network_Access_Authentication_Passed	PermitAccess	Select from list		5	
✓	Default		DenyAccess	Select from list		0	

Reset Policyset Hitcounts Reset Save

Reset Save

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.

Cisco Secure Web Appliance S100V

Reporting Web Security Manager Security Services Network System Administration Secure We

### Users

Add User...

<input type="checkbox"/> All Accounts	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	

Enforce Passphrase Changes

#### Local User Account & Passphrase Settings

Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. Additional rules configured...

Edit Settings...

#### External Authentication

External Authentication is disabled.

Enable...

#### Second Factor Authentication Settings

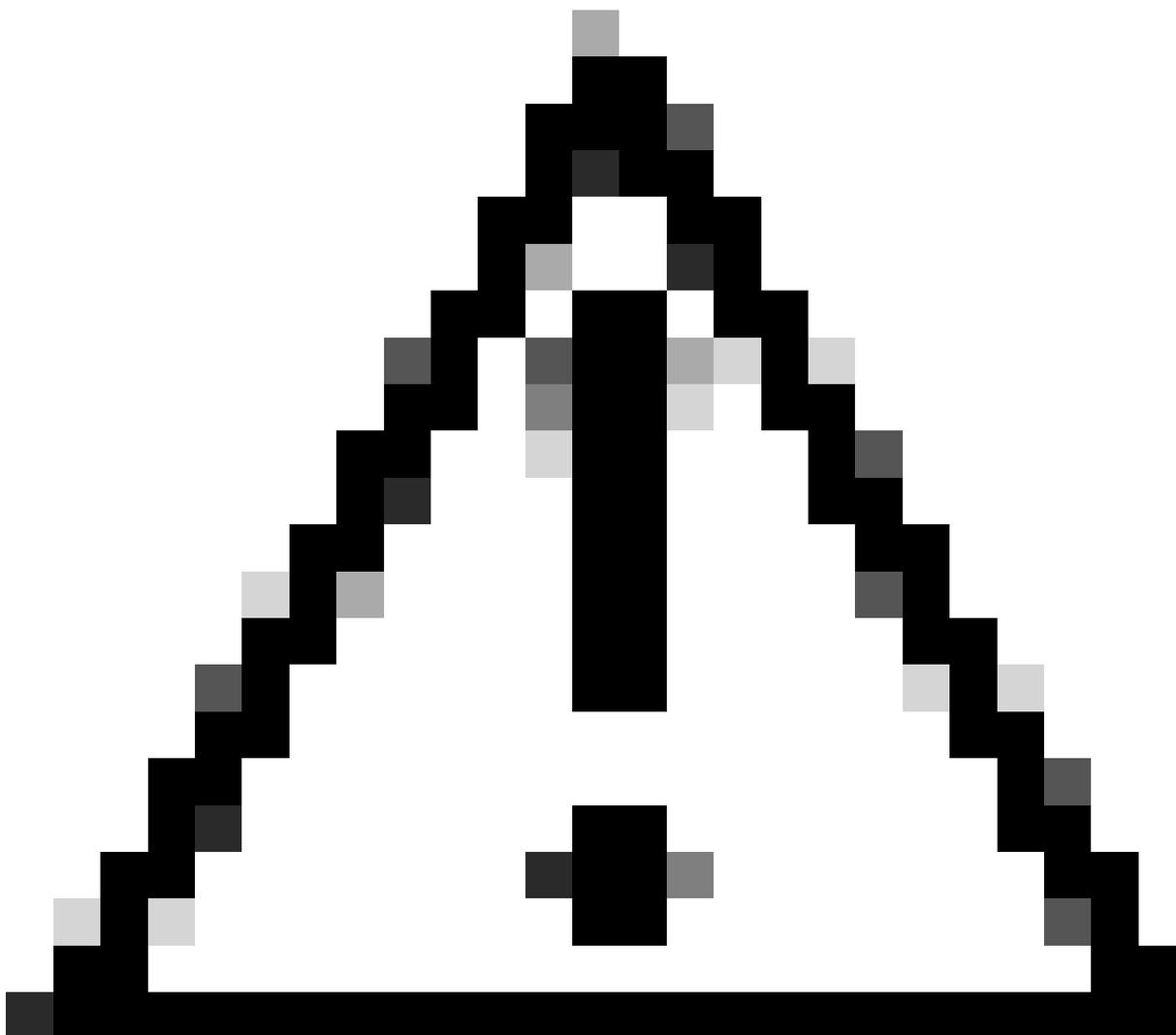
Two Factor Authentication is disabled.

Enable...

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.

---



## Users

Users						
<a href="#">Add User...</a>						
<input type="checkbox"/>	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	
<a href="#">Enforce Passphrase Changes</a>						

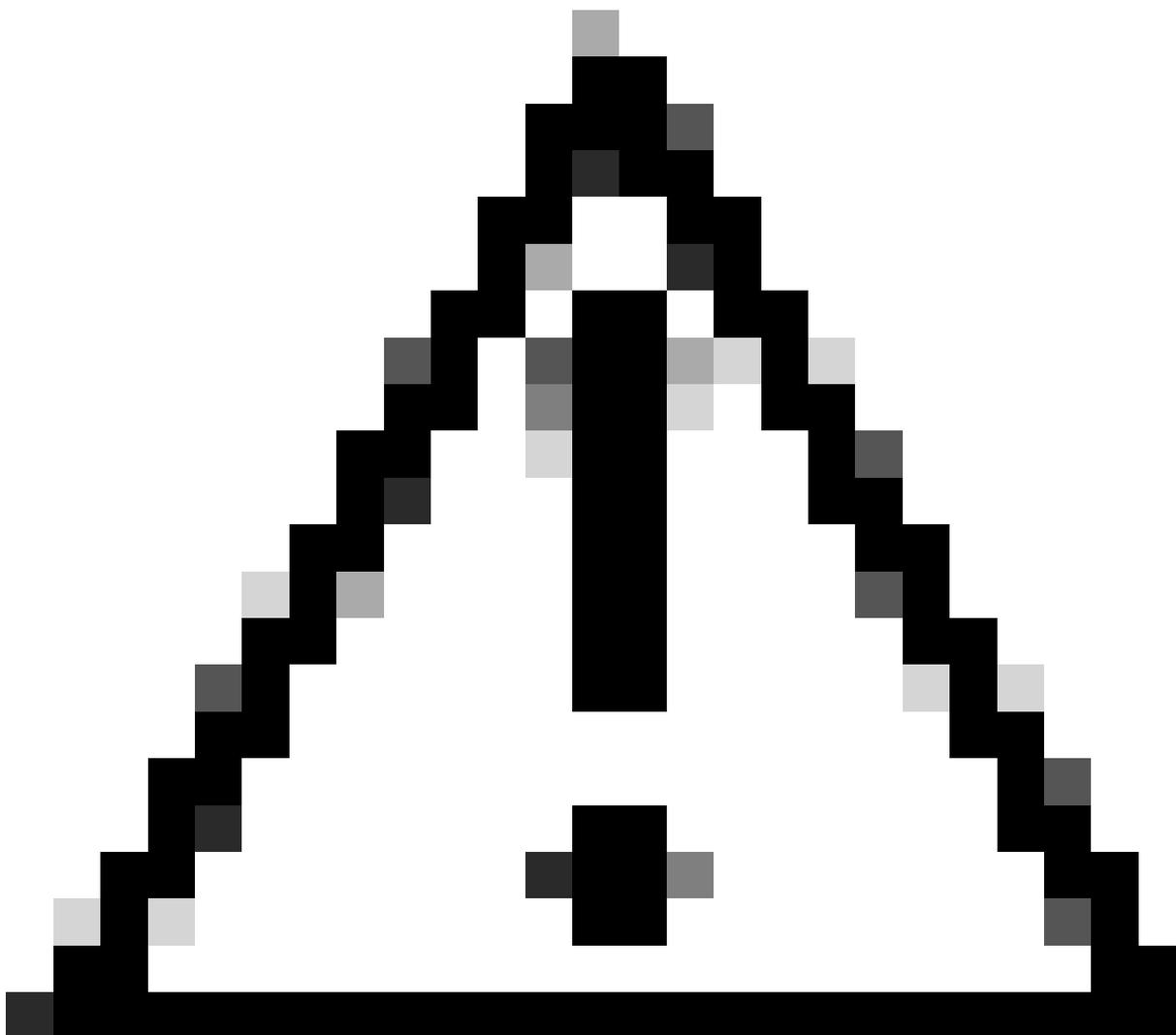
Local User Account & Passphrase Settings	
Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. <i>Additional rules configured...</i>
<a href="#">Edit Settings...</a>	

External Authentication	
<i>External Authentication is disabled.</i>	
<a href="#">Enable...</a>	

Second Factor Authentication Settings	
<i>Two Factor Authentication is disabled.</i>	
<a href="#">Enable...</a>	



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 Directory (AD) para autenticar credenciais 'admin', pois o ISE não permite configurar 'admin' como um usuário de acesso à rede.

---

## Second Factor Authentication

**Second Factor Authentication Settings**

**Enable Second Factor Authentication**

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:	RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Add Row
	<span style="border: 1px solid #ccc; padding: 2px;">10.106.38.150</span>	<span style="border: 1px solid #ccc; padding: 2px;">1812</span>	<span style="border: 1px solid #ccc; padding: 2px;">*****</span>	<span style="border: 1px solid #ccc; padding: 2px;">5</span>	<span style="border: 1px solid #ccc; padding: 2px;">PAP</span>	🗑️

**User Role Privileges**

Configure user roles for Second Factor Authentication

Second Factor Authentication is enforced to:

Predefined Roles

- Administrator
- Operator
- Read-Only Operator
- Guest

**Two Factor Login Page**

Appearance:

Current Logo:

Use Current Logo

Upload Custom Logo from Local Computer: Browse... No file selected.

Company Name:   
(Max 150 characters only)

Custom text Information:   
(Max 500 characters only)

Login help Information:   
(Examples: For login trouble Please contact, Contact Name ,123-1234-123,admin@example.com or help URL. Note:Max 500 characters only)

[View Existing Two Factor Login Page](#)

Cancel
Submit

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.

### 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
<input type="checkbox"/>	adminuser	Admin User	Administrator	Active	n/a	🗑️
<input type="checkbox"/>	rouser	RO User	Read-Only Operator	Active	n/a	🗑️

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.



Passcode:

Login

Copyright © 2003-2022 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

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.