

Configurar a autenticação externa do SWA com o ISE como um servidor RADIUS

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Topologia de rede](#)

[Configurar](#)

[Configuração do ISE](#)

[Configuração de SWA](#)

[Verificar](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas para configurar a autenticação externa no Secure Web Access (SWA) com o Cisco ISE como um servidor RADIUS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico no Cisco Secure Web Appliance.
- Conhecimento da configuração das políticas de autenticação e autorização no ISE.
- Conhecimento RADIUS básico.

A Cisco recomenda que você também tenha:

- Acesso de administração SWA e ISE.
- 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 externa para usuários administrativos do seu SWA, o dispositivo verifica as credenciais do usuário com um servidor LDAP ou RADIUS, conforme especificado na configuração de autenticação externa.

Topologia de rede



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.

Configurar

Configuração do ISE

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

A captura de tela mostra a interface de administração do Cisco Identity Services Engine (ISE). O menu de navegação superior inclui Home, Context Visibility, Operations, Policy, Administration e Work Centers. O menu de navegação secundário mostra System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service e Threat Centric NAC. O menu de navegação terciário mostra Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers e External MDM. A seção principal, intitulada 'Network Devices', contém botões para Edit, Add, Duplicate, Import, Export, Generate PAC e Delete. Abaixo dos botões, há uma tabela com cabeçalhos: Name, IP/Mask, Profile Name, Location e Type. O conteúdo da tabela é 'No data available'.

Adicionar SWA como dispositivo de rede no ISE

Etapa 2. Atribua um Name ao objeto do dispositivo de rede e insira o endereço IP do SWA.

Marque a caixa de seleção RADIUS e defina um segredo compartilhado.



Observação: a mesma chave deve ser usada posteriormente para configurar o servidor RADIUS no 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 2.1. 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

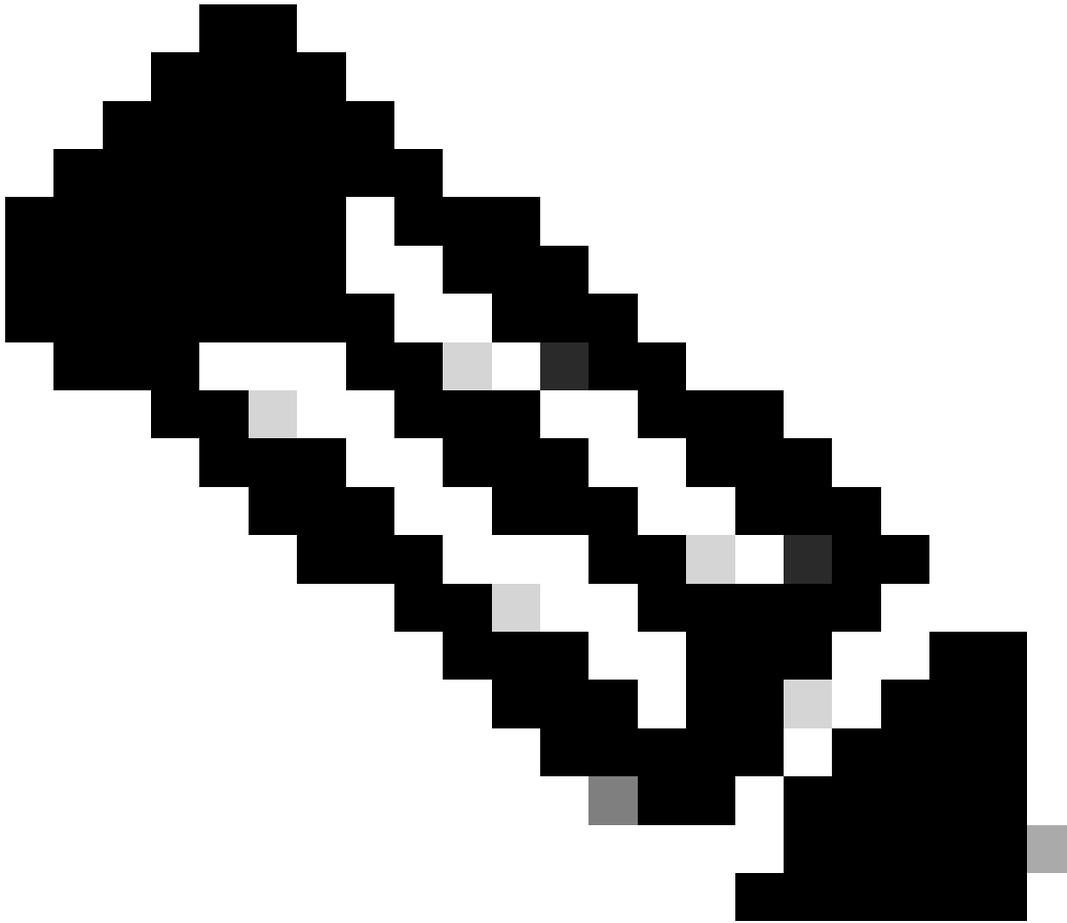
▶ TACACS Authentication Settings

▶ SNMP Settings

▶ Advanced TrustSec Settings

Enviar configuração do dispositivo de rede

Etapa 3. Crie os Grupos de Identidade de Usuário necessários. Navegue até Administração > Gerenciamento de identidades > Grupos > Grupos de identidades do usuário > + Adicionar.



Observação: você precisa configurar diferentes grupos de usuários para corresponder a diferentes tipos de usuários.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes: Identity Services Engine, Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The 'Administration' menu is expanded to show: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The 'Identity Management' menu is further expanded to show: Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The 'Groups' menu item is selected.

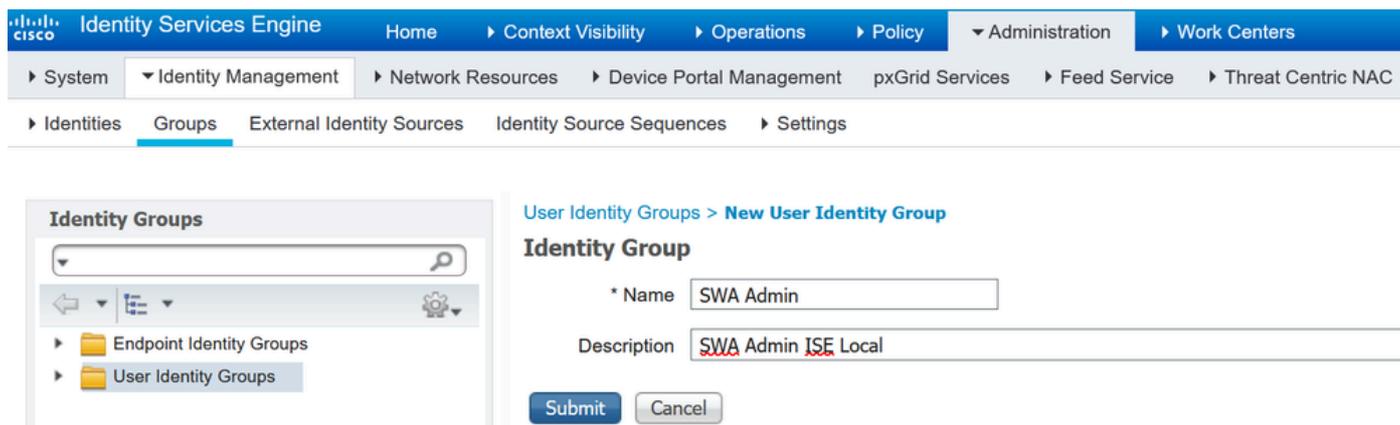
The main content area is titled 'User Identity Groups'. It features a toolbar with 'Edit', '+ Add', 'X Delete', 'Import', and 'Export' buttons. Below the toolbar is a table with the following data:

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type

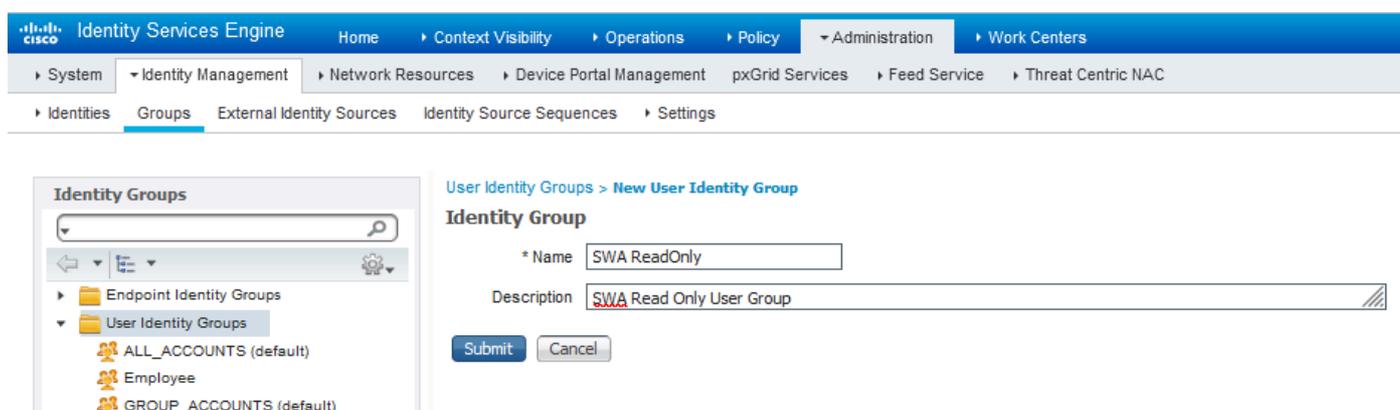
Adicionar grupo de identidade do usuário

Etapa 4. Insira o nome do grupo, a descrição (opcional) e Enviar. Repita essas etapas para cada

grupo. Neste exemplo, você cria um grupo para usuários Administradores e outro para usuários Somente leitura.



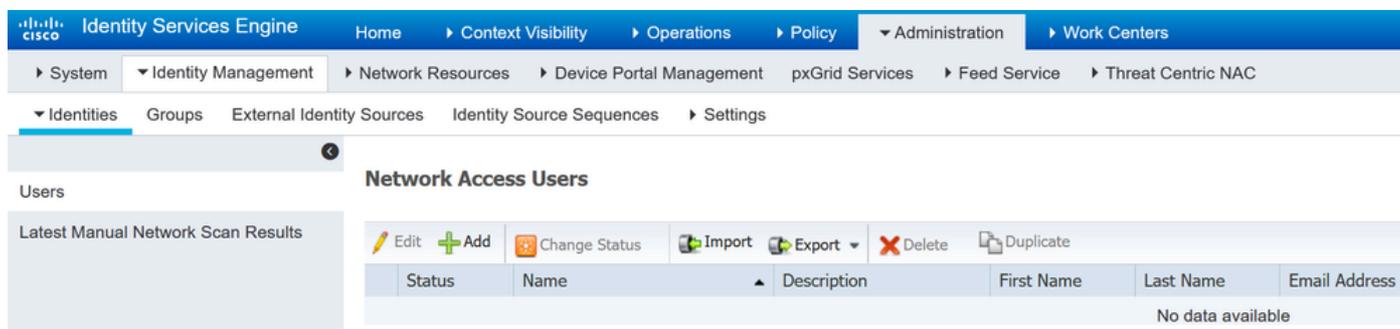
Adicionar



grupo de identidade de usuárioAdicionar grupo de identidade de usuário para usuários somente leitura do SWA

Etapa 5. Você precisa criar usuários de acesso à rede que correspondam ao nome de usuário configurado no SWA.

Crie os Usuários de Acesso à Rede e adicione-os ao seu grupo de correspondentes. Navegue até Administração > Gerenciamento de identidades > Identidades > + Adicionar.



Adicionar usuários locais no ISE

Etapa 5.1. Você precisa criar um Network Access Users com direitos de administrador. Atribua um nome e uma senha.

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 adminuser

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

* Login Password

Adicionar usuário administrador

Etapa 5.2. Escolha SWA Admin na seção Grupos de usuários.

Account Disable Policy

Disable account if date exceeds 2024-03-28 (yyyy-mm-dd)

User Groups

SWA Admin

Atribuir grupo de administradores ao usuário administrador

Etapa 5.3. Você precisa criar um usuário com direitos Somente Leitura. Atribua um nome e uma senha.

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	<input type="password" value="••••••"/>	<input type="password" value="••••••"/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

Adicionar usuário somente leitura

Etapa 5.4. Escolha SWA ReadOnly na seção User Groups.

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

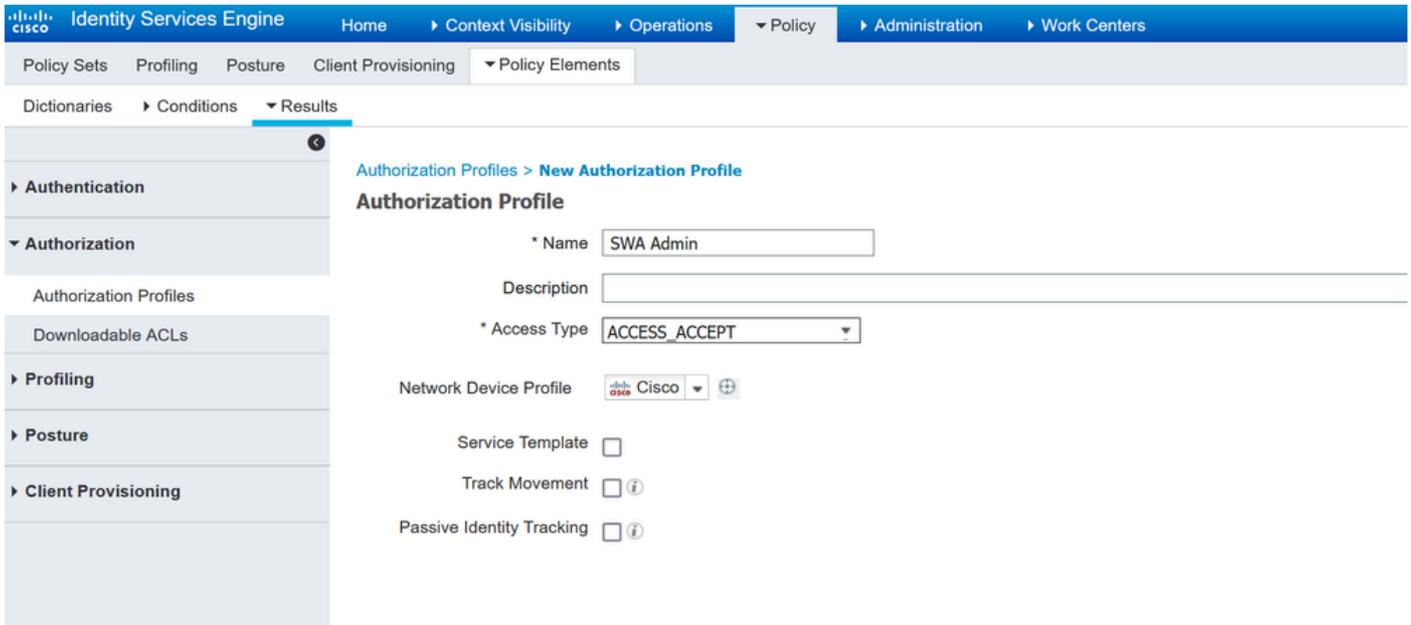
User Groups

Atribuir grupo de usuários somente leitura ao usuário somente leitura

Etapa 6. Crie o perfil de autorização para o usuário Admin.

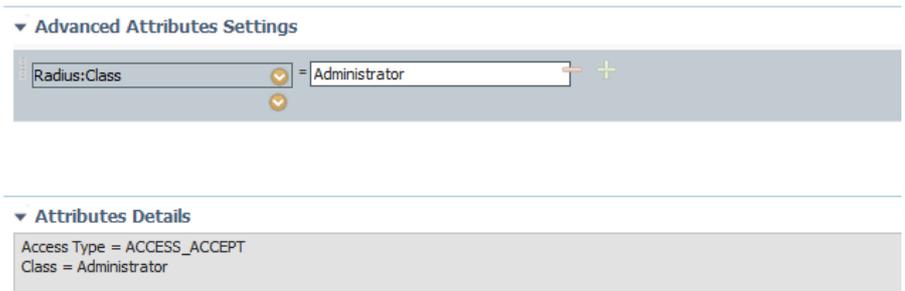
Navegue até Política > Elementos de política > Resultados > Autorização > Perfis de autorização > +Adicionar.

Defina um nome para o perfil de autorização e certifique-se de que o tipo de acesso esteja definido como ACCESS_ACCEPT.



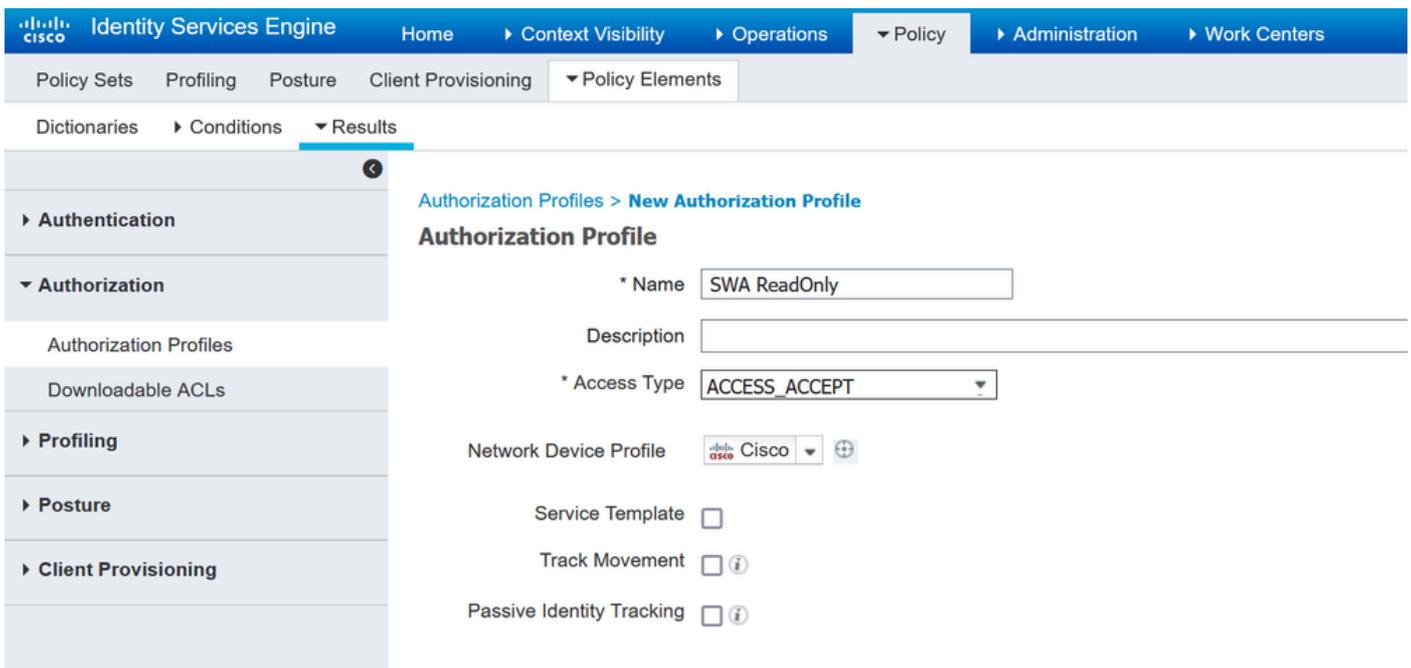
Adicionar perfil de autorização para usuários administradores

Etapa 6.1. Nas Advanced Attributes Settings, navegue até Radius > Class—[25], insira o valor



Administrator e clique em Submit. Add Authorization Profile for Admin Users

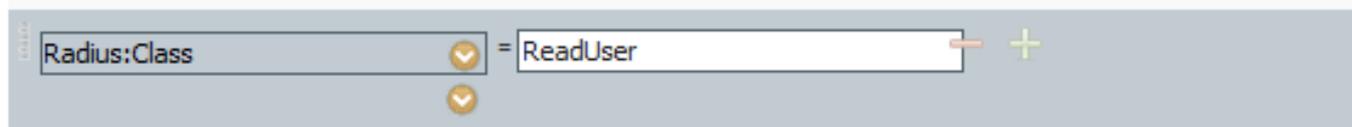
Passo 7. Repita a etapa 6 para criar o perfil de autorização para o usuário somente leitura.



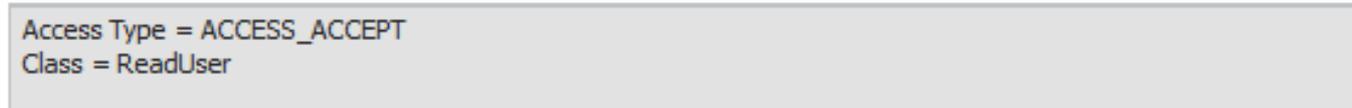
Adicionar perfil de autorização para usuários somente leitura

ETAPA 7.1. Desta vez, crie Radius:Class com o valor ReadUser em vez de Administrator.

Advanced Attributes Settings



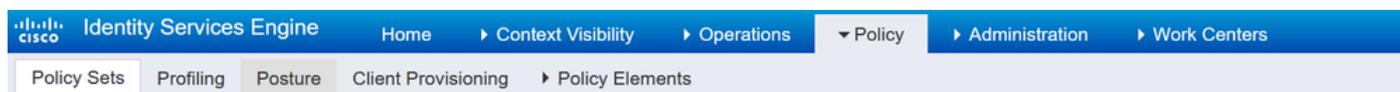
Attributes Details



Adicionar perfil de autorização para usuários somente leitura

Etapa 8. Crie conjuntos de políticas que correspondam ao endereço IP SWA. Isso evita o acesso a outros dispositivos com essas credenciais de usuário.

Navegue para Política > Conjuntos de políticas e clique no ícone + no canto superior esquerdo.



Policy Sets

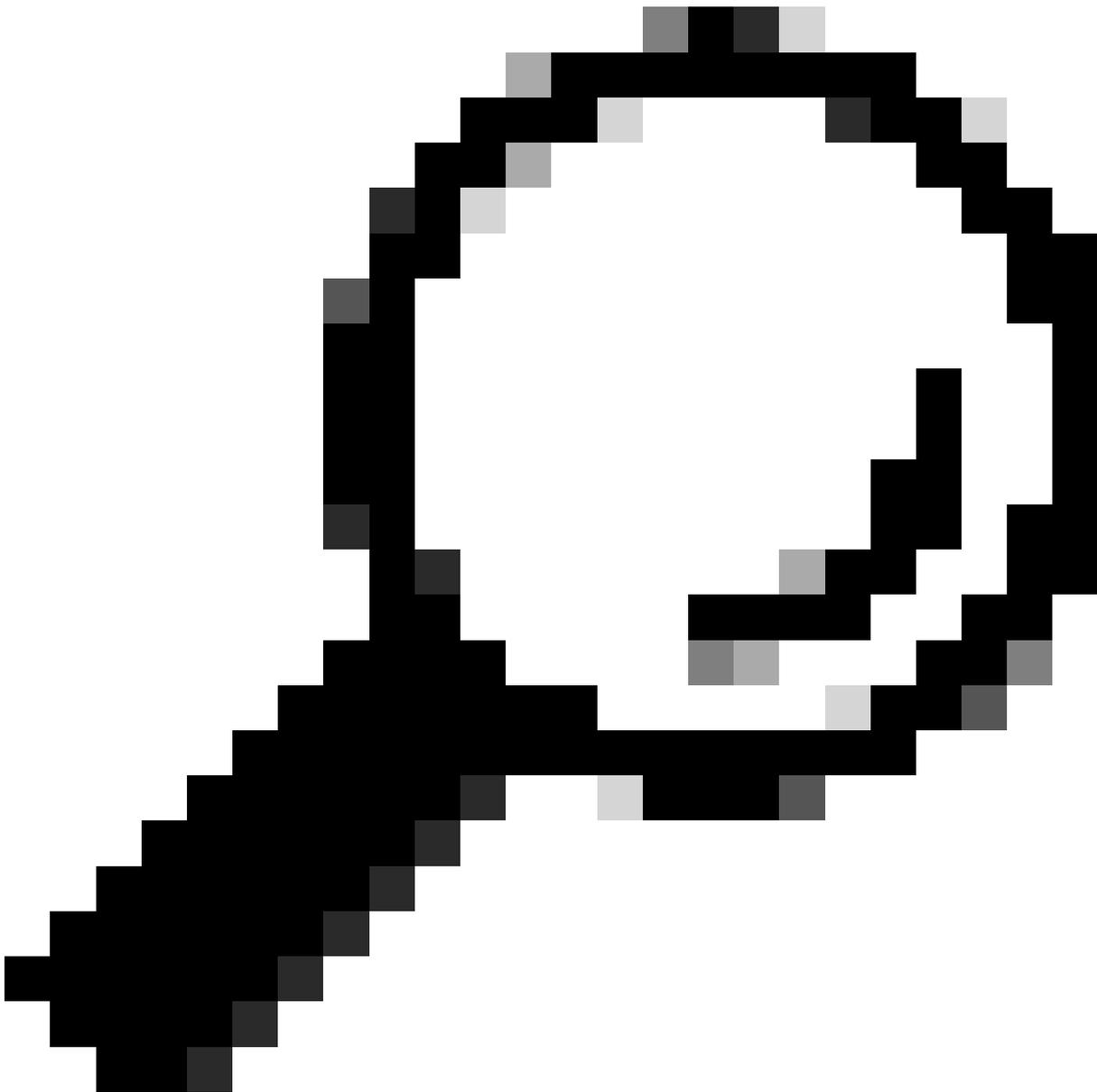
+	Status	Policy Set Name	Description	Conditions
Search				

Adicionar conjunto de políticas no ISE

Etapa 8.1. Uma nova linha é colocada na parte superior dos conjuntos de políticas.

Nomeie a nova política e adicione uma condição para que o atributo RADIUS NAS-IP-Address corresponda ao endereço IP do SWA.

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



Dica: neste artigo, a lista Default Network Access Protocols é permitida. Você pode criar uma nova lista e restringir conforme necessário.

Etapa 9. Para exibir os novos conjuntos de políticas, clique no ícone > na coluna Exibir. Expanda o menu Authorization Policy e clique no ícone + para adicionar uma nova regra para permitir o acesso ao usuário com direitos administrativos.

Defina um nome.

Etapa 9.1. Para criar uma condição que corresponda ao grupo de usuários Admin, clique no ícone +.

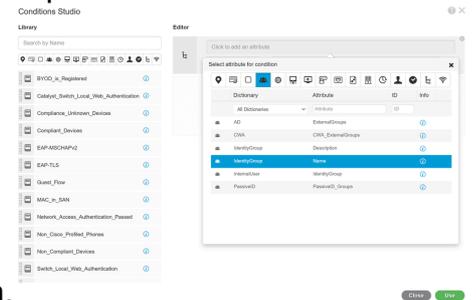
▼ Authorization Policy (0)

	Status	Rule Name	Conditions
		<u>SWA Admin</u>	

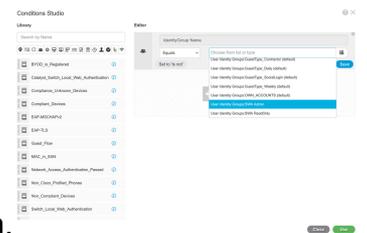
Search

Adicionar condição de política de autorização

Etapa 9.2. Defina as condições para corresponder ao Dicionário Grupo de Identidade com o



Atributo Nome igual à Identidade do Usuário Grupos: SWA admin.
 Selecione Grupo de Identidade como Condição



Etapa 9.3. Role para baixo e selecione User Identity Groups: SWA admin.
 Role para baixo e selecione Identity Group Name

Etapa 9.4. Clique em Usar.



Users

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 autenticação externa em SWA

Etapa 3. Insira o endereço IP ou o FQDN do ISE no campo Nome de host do servidor RADIUS e insira o mesmo segredo compartilhado que está configurado na Etapa 2, Configuração do ISE.

Etapa 4. Selecione Mapear usuários autenticados externamente para várias funções locais em Mapeamento de grupos.

Etapa 4.1. Informe Administrador no campo Atributo CLASSE RADIUS e selecione a Função Administrador.

Etapa 4.2. Digite ReadUser no campo Atributo CLASS RADIUS e selecione a função Operador somente leitura.



Edit External Authentication

External Authentication Settings

Enable External Authentication

Authentication Mode: Password based Authentication

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:							Add Row
RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Certificate		
10.106.38.150	1812	*****	5	PAP	Select any		

External Authentication Cache Timeout: 0 seconds

Group Mapping:

Map externally authenticated users to multiple local roles. (recommended)

RADIUS CLASS Attribute	Role	Add Row
administrator	Administrator	
ReadUser	Read-Only Operator	

RADIUS CLASS attributes are case-sensitive.

Map all externally authenticated users to the Administrator role.

Cancel Submit

Configuração de Autenticação Externa para Servidor RADIUS

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 Retype Passphrase, que são necessários para acesso à GUI se o dispositivo não puder se conectar a um servidor RADIUS externo.

Observação: se o equipamento não puder se conectar a nenhum servidor externo, ele tentará autenticar o usuário como um usuário local definido no Secure Web Appliance.

Users

Users						
<input type="button" value="Add User..."/>						
<small>* 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.</small>						
<input type="checkbox"/> 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 e verifique os registros em

tempo real no ISE. Para verificar os logs ao vivo no ISE, navegue para Operations > Live Logs:

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	adminuser
Endpoint Id	
Endpoint Profile	
Authentication Policy	SWA Access >> Default
Authorization Policy	SWA Access >> SWA Admin
Authorization Result	SWA Admin

Authentication Details

Source Timestamp	2024-01-28 17:28:31.573
Received Timestamp	2024-01-28 17:28:31.573

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11117 Generated a new session ID
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Radius.NAS-IP-Address
- 15041 Evaluating Identity Policy
- 22072 Selected identity source sequence - All_User_ID_Stores
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore - adminuser
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15016 Selected Authorization Profile - SWA Admin
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept

Verificar o login do usuário ISE

Informações Relacionadas

- [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](#)
- [Suporte técnico e downloads da Cisco](#)

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.