

Configuración de la autenticación externa SWA con ISE como servidor RADIUS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Topología de red](#)

[Configurar](#)

[Configuración de ISE](#)

[Configuración SWA](#)

[Verificación](#)

[Información Relacionada](#)

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



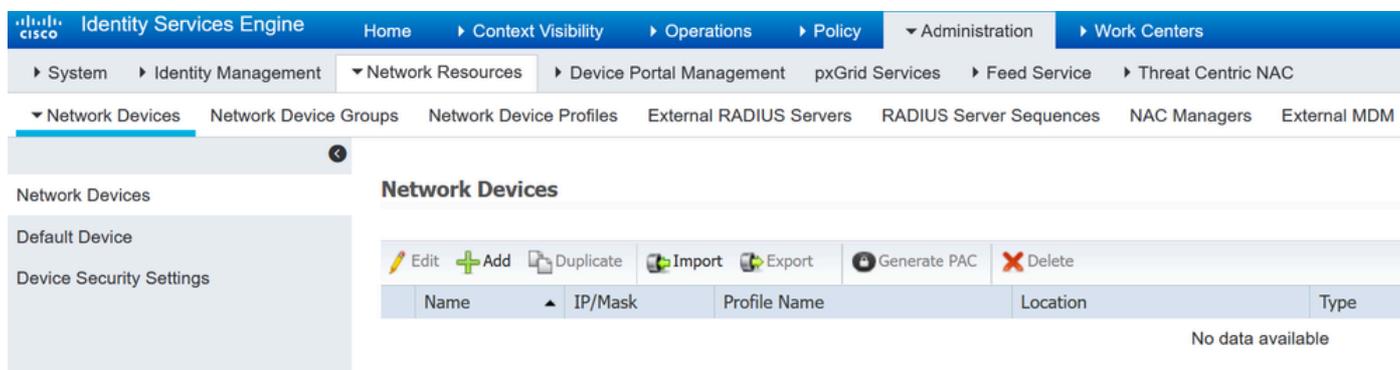
Diagrama de topología de red

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.

Network Devices

Default Device

Device Security Settings

Network Devices List > SWA

Network Devices

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Configuración de la clave compartida del dispositivo de red SWA

Paso 2.1. Haga clic en Submit (Enviar).

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

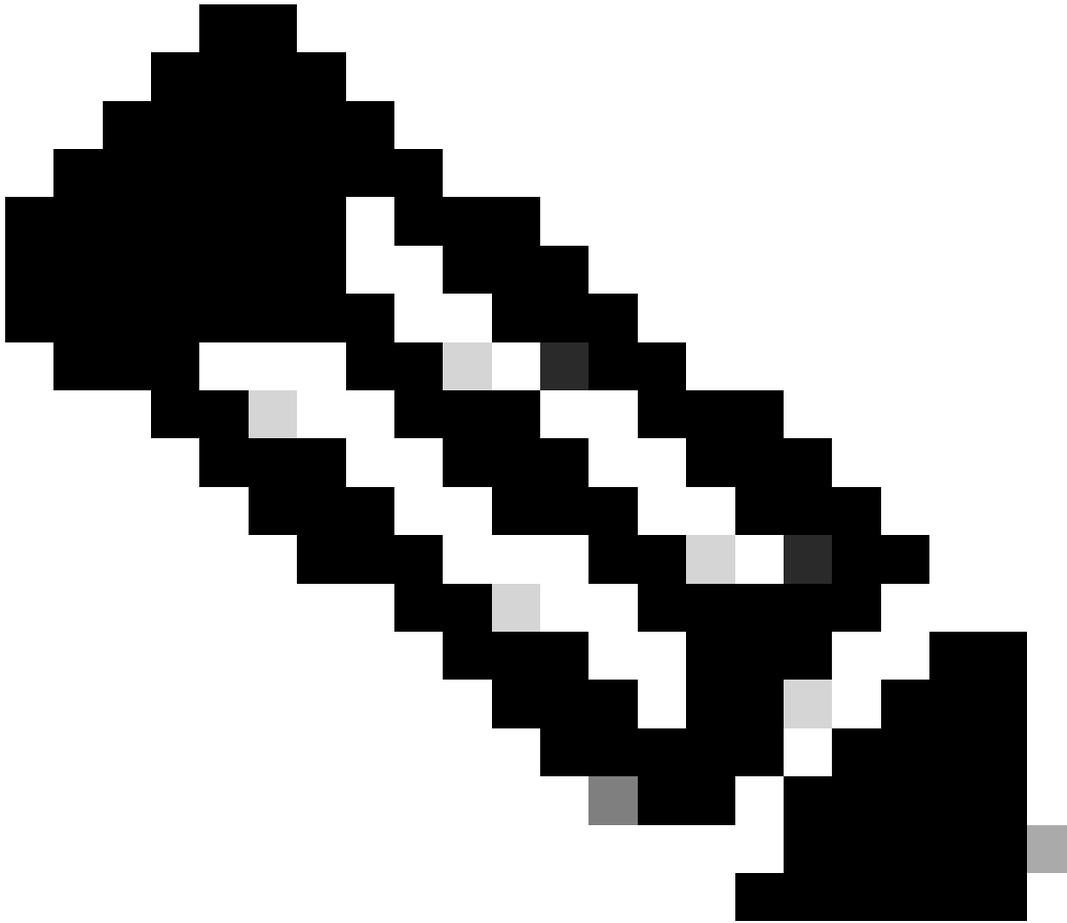
▶ TACACS Authentication Settings

▶ SNMP Settings

▶ Advanced TrustSec Settings

Enviar 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.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar 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.

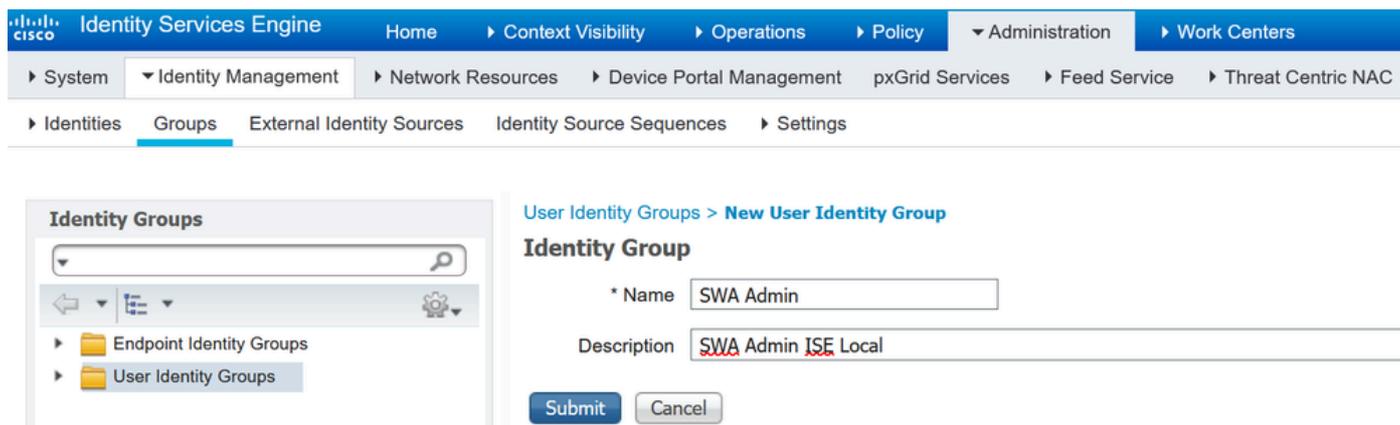
The main content area is titled 'User Identity Groups'. It features a search bar and a list of existing groups. The list has columns for 'Name' and 'Description'. The groups listed are:

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

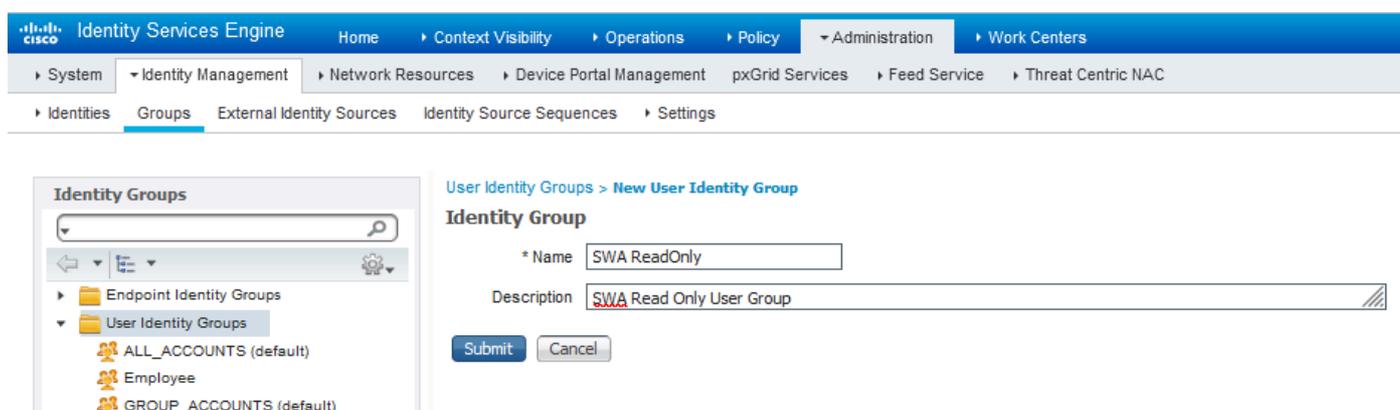
Agregar grupo de identidad de usuario

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.



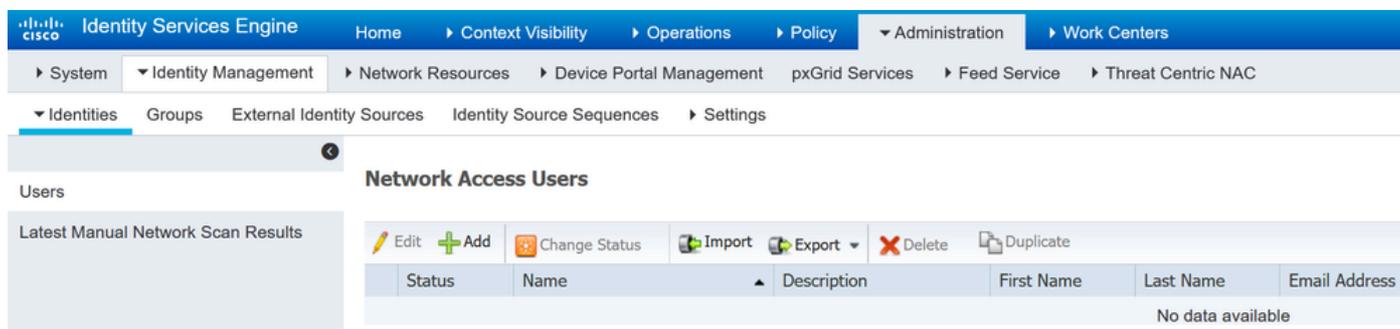
Agregar grupo de identidad de



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.

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

Agregar usuario administrador

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

Account Disable Policy

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

User Groups

SWA Admin

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.

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"/> ⓘ

Agregar usuario de sólo lectura

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

Account Disable Policy

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

User Groups

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name SWA Admin

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement *i*

Passive Identity Tracking *i*

Agregar perfil de autorización para usuarios administrativos

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

Advanced Attributes Settings

Radius:Class = Administrator

Attributes Details

Access Type = ACCESS_ACCEPT

Class = Administrator

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name SWA ReadOnly

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

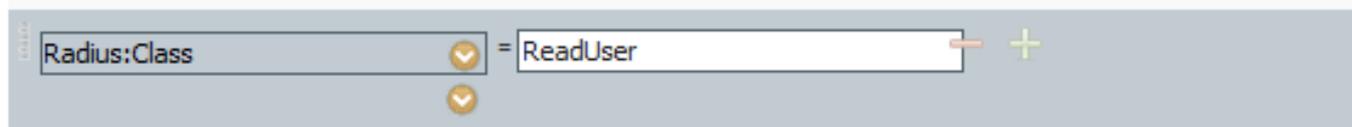
Track Movement *i*

Passive Identity Tracking *i*

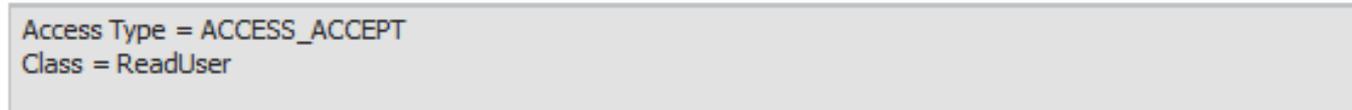
Agregar perfil de autorización para usuarios de sólo lectura

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

Advanced Attributes Settings



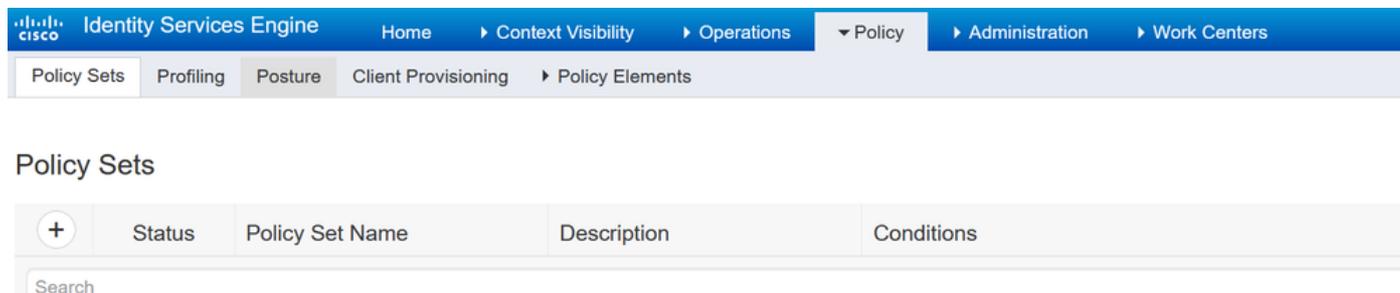
Attributes Details



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.

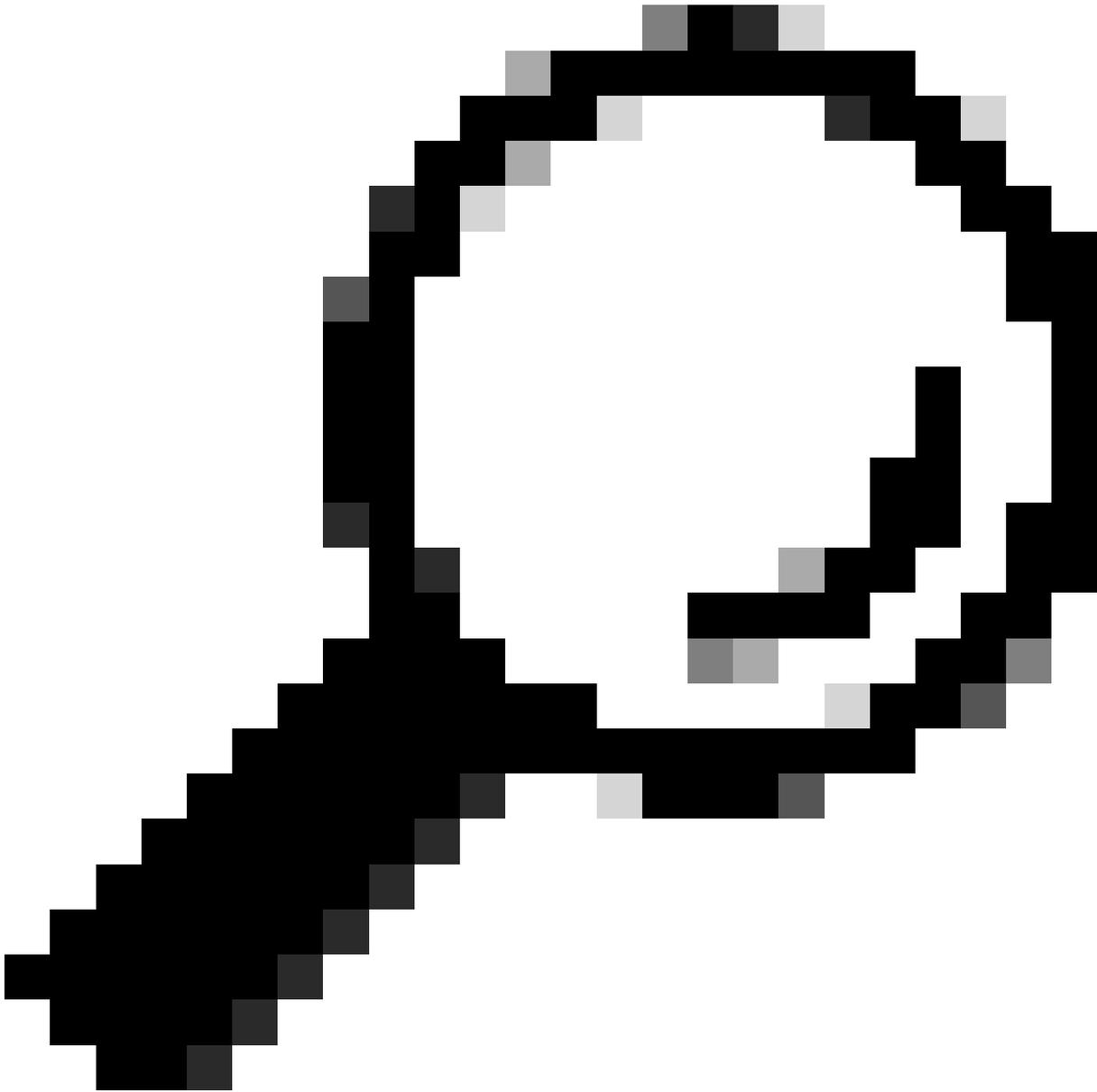


Agregar conjunto de políticas en ISE

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.



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.

▼ Authorization Policy (0)

	Status	Rule Name	Conditions
<input type="text" value="Search"/>			
		SWA Admin	

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.

Conditions Studio ? X

Library

Search by Name

- BYOD_is_Registered (i)
- Catalyst_Switch_Local_Web_Authentication (i)
- Compliance_Unknown_Devices (i)
- Compliant_Devices (i)
- EAP-MSCHAPv2 (i)
- EAP-TLS (i)
- Guest_Flow (i)
- MAC_in_SAN (i)
- Network_Access_Authentication_Passed (i)
- Non_Cisco_Profiled_Phones (i)
- Non_Compliant_Devices (i)
- Switch_Local_Web_Authentication (i)

Editor

Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
AD	ExternalGroups		(i)
CWA	CWA_ExternalGroups		(i)
IdentityGroup	Description		(i)
IdentityGroup	Name		(i)
InternalUser	IdentityGroup		(i)
PassiveID	PassiveID_Groups		(i)

Close
Use

Seleccione Grupo de identidad como condición

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

Conditions Studio



Library

Search by Name

BYOD_is_Registered (i)

Catalyst_Switch_Local_Web_Authentication (i)

Compliance_Unknown_Devices (i)

Compliant_Devices (i)

EAP-MSCHAPv2 (i)

EAP-TLS (i)

Guest_Flow (i)

MAC_in_SAN (i)

Network_Access_Authentication_Passed (i)

Non_Cisco_Profiled_Phones (i)

Non_Compliant_Devices (i)

Switch_Local_Web_Authentication (i)

Editor

IdentityGroup-Name

Equals

Set to 'Is not'

Choose from list or type

- User Identity Groups:GuestType_Contractor (default)
- User Identity Groups:GuestType_Daily (default)
- User Identity Groups:GuestType_SocialLogin (default)
- User Identity Groups:GuestType_Weekly (default)
- User Identity Groups:OWN_ACCOUNTS (default)
- User Identity Groups:SWA Admin**
- User Identity Groups:SWA ReadOnly

Save

Close Use

Scroll Down and Select Identity Group Name

Paso 9.4. Haga clic en Usar.

Conditions Studio



Library

Search by Name

BYOD_is_Registered (i)

Catalyst_Switch_Local_Web_Authentication (i)

Compliance_Unknown_Devices (i)

Compliant_Devices (i)

EAP-MSCHAPv2 (i)

EAP-TLS (i)

Guest_Flow (i)

MAC_in_SAN (i)

Network_Access_Authentication_Passed (i)

Non_Cisco_Profiled_Phones (i)

Editor

IdentityGroup-Name

Equals

Set to 'Is not'

* User Identity Groups:SWA Admin

You can only select 1 item

Save

+ New AND OR

Close Use

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.

Conditions Studio

Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Compliant_Devices

EAP-MSCHAPv2

EAP-TLS

Guest_Flow

MAC_in_SAN

Network_Access_Authentication_Passed

Non_Cisco_Profiled_Phones

Editor

IdentityGroup-Name

Equals

× User Identity Groups:SWA ReadOnly

Set to 'Is not'

Duplicate

Save

+ New AND OR

Close 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.

Policy Sets → SWA Access

Reset Pollicyset Hitcounts

Reset

Save

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	0

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
✎	✓	SWA Read Only	IdentityGroup-Name EQUALS User Identity Groups:SWA ReadOnly	× SWA ReadOnly	Select from list		⚙
✎	✓	SWA Admin	IdentityGroup-Name EQUALS User Identity Groups:SWA Admin	× SWA Admin	Select from list		⚙
	✓	Default		× DenyAccess	Select from list	0	⚙

Reset

Save

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.

Users

Add User...

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 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.



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

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...						
<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	

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:

The screenshot displays the Cisco Identity Services Engine (ISE) interface. At the top, there is a blue header with the Cisco logo and the text "Identity Services Engine". Below the header, the interface is divided into two main sections: "Overview" and "Authentication Details".

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 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).