

Configureer de externe verificatie van SWA met ISE als RADIUS-server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerktopologie](#)

[Configureren](#)

[ISE-configuratie](#)

[Configuratie SWA](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de stappen om externe verificatie op Secure Web Access (SWA) te configureren met Cisco ISE als RADIUS-server.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis in Cisco Secure Web Applicatie.
- Kennis van de configuratie van het authenticatie- en autorisatiebeleid op ISE.
- Basiskennis van RADIUS.

Cisco raadt u ook aan het volgende te hebben:

- Toegang tot SWA- en ISE-administratie.
- Compatibele WSA en ISE versies.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- SWA 14.0.2-012
- ISE 3.0.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Wanneer u externe verificatie inschakelt voor administratieve gebruikers van uw SWA, verifieert het apparaat de gebruikersreferenties met een Lichtgewicht Directory Access Protocol (LDAP) of RADIUS-server zoals gespecificeerd in externe verificatieconfiguratie.

Netwerktopologie



Netwerktopologiediagram

Administratieve gebruikers hebben toegang tot SWA op poort 443 met hun referenties. SWA verifieert de referenties met de RADIUS-server.

Configureren

ISE-configuratie

Stap 1. Voeg een nieuw netwerkapparaat toe. Ga naar Beheer > Netwerkbronnen > Netwerkapparaten > +Add.

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				

SWA als netwerkapparaat toevoegen in ISE

Stap 2. Wijs een naam toe aan het object van het netwerkapparaat en voer het SWA IP-adres in.

Controleer het aanvinkvakje RADIUS en stel een gedeeld geheim in.



Opmerking: dezelfde toets moet later worden gebruikt om de RADIUS-server in SWA te configureren.

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

gedeelde sleutel voor netwerkkapparaat configureren

Stap 2.1. Klik op Verzenden.

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

Configuratie van netwerkapparaat verzenden

Stap 3. Maak de gewenste gebruikers-identiteitsgroepen. Ga naar Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen > + Toevoegen.

Opmerking: u dient verschillende gebruikersgroepen te configureren volgens het verschillende type gebruikers.

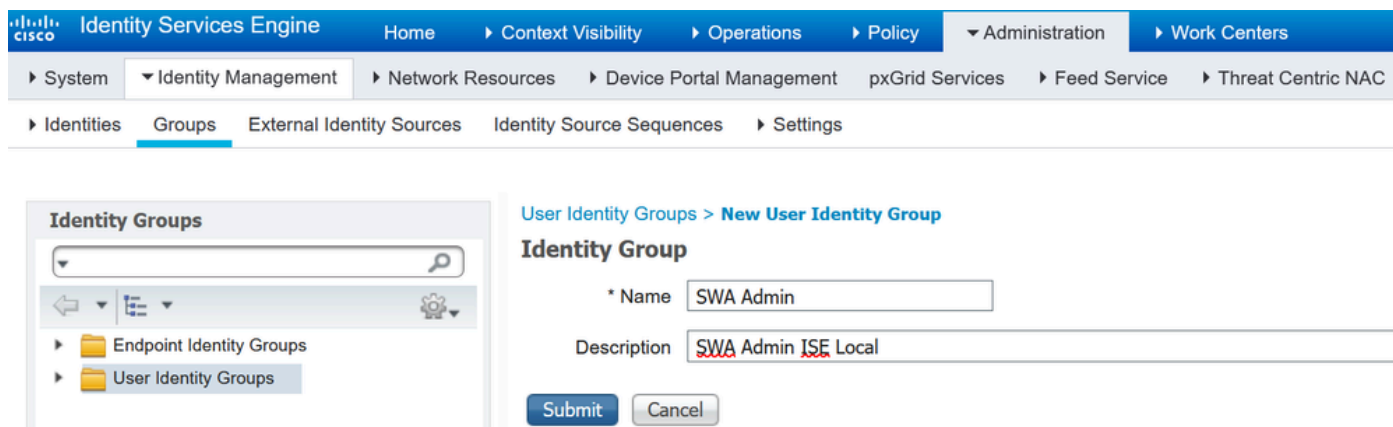
The screenshot shows the Cisco ISE Administration interface. The breadcrumb trail is: Administration > Work Centers > Identity Management > Groups. The 'User Identity Groups' section contains a table with the following data:

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

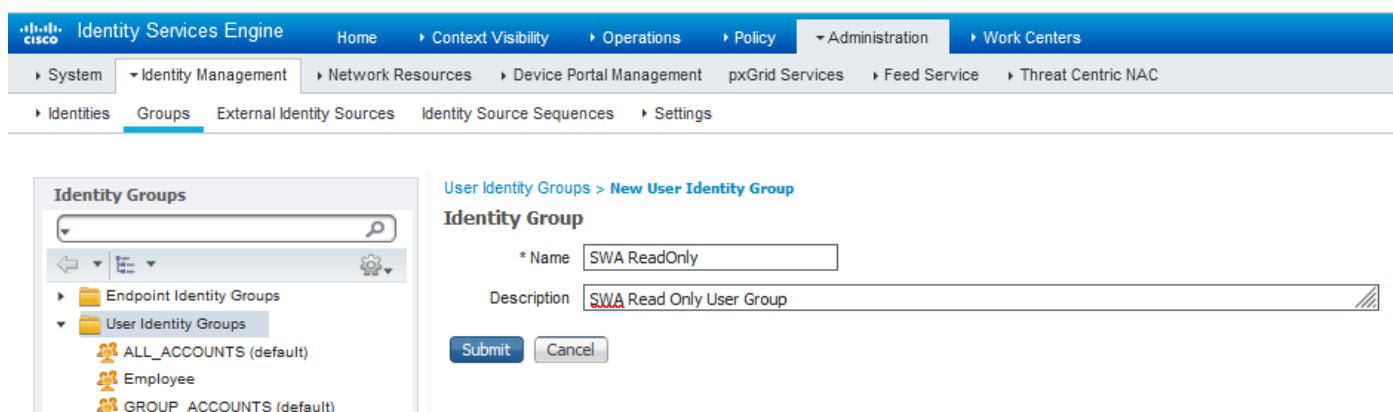
Gebruikersidentiteitsgroep toevoegen

Stap 4. Voer de naam van de groep in, beschrijving (optioneel) en Verzenden. Herhaal deze

stappen voor elke groep. In dit voorbeeld maakt u een groep voor beheerders en een groep voor alleen-lezen gebruikers.



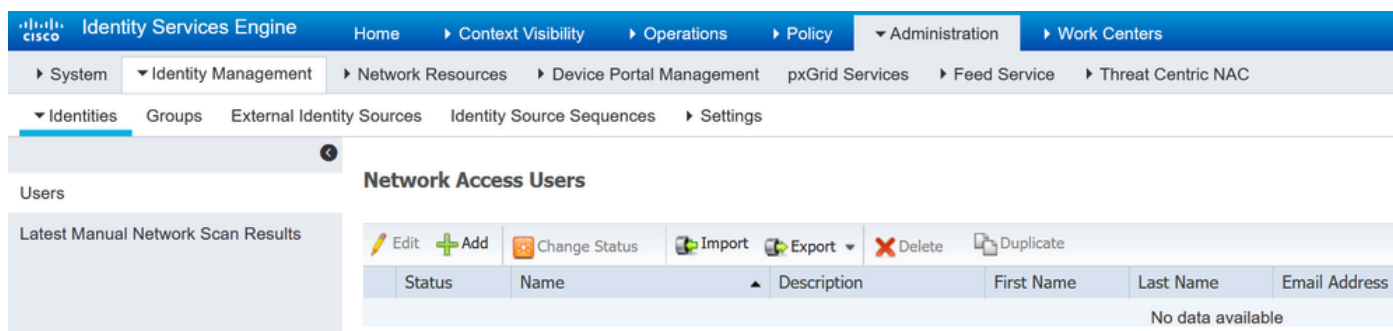
Gebruikersidentiteitsgroep toevoegen



Gebruikersidentiteitsgroep toevoegen voor SWA Lees alleen gebruikers

Stap 5. U moet gebruikers voor netwerktoegang maken die overeenkomen met de gebruikersnaam die in SWA is ingesteld.

Maak de Network Access Gebruikers en voeg ze toe aan hun correspondentgroep. Navigeren naar Administratie > Identiteitsbeheer > Identiteiten > + Toevoegen.



Voeg lokale gebruikers toe in ISE

Stap 5.1. U moet een gebruiker voor netwerktoegang aanmaken met beheerdersrechten. Ken een naam en wachtwoord toe.

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

Admin-gebruiker toevoegen

Stap 5.2. Kies SWA Admin in het gedeelte Gebruikersgroepen.

Account Disable Policy

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

User Groups

Toewijzen aan de beheerder Gebruiker

Stap 5.3. U moet een gebruiker met de rechten Alleen lezen aanmaken. Ken een naam en wachtwoord toe.

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"/> ⓘ

Alleen-lezen gebruiker toevoegen

Stap 5.4. Kies SWA ReadOnly in de sectie Gebruikersgroepen.

Account Disable Policy

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

User Groups

ⓘ

Wijs alleen-lezen gebruikersgroep toe aan de alleen-lezen gebruiker

Stap 6. Maak het autorisatieprofiel voor de beheerder.

Navigeer naar Beleid > Beleidselementen > Resultaten > Vergunningprofielen > +Add.

Definieer een naam voor het autorisatieprofiel en zorg ervoor dat het toegangstype is ingesteld op ACCESS_ACCEPTEREN.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaryes 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

Passive Identity Tracking

Vergunningsprofiel voor beheerder-gebruikers toevoegen

Stap 6.1. Navigeer in de instellingen voor geavanceerde kenmerken naar Radius > Class—[25], voer de waarde in voor de beheerder en klik op Submit.

Advanced Attributes Settings

Radius:Class = Administrator

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit Cancel

Add Authorisation Profile for Admin Gebruikers

Stap 7. Herhaal stap 6 om het autorisatieprofiel voor de alleen-lezen gebruiker te maken.

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:

Passive Identity Tracking:

Vergunningsprofiel voor alleen-lezen gebruikers toevoegen

STAP 7.1. Maak de straal:Klasse met de waarde ReadUser in plaats van Administrator dit keer.

Advanced Attributes Settings

Radius:Class = ReadUser

Attributes Details

Access Type = ACCESS_ACCEPT
Class = ReadUser

Submit Cancel

Vergunningsprofiel voor alleen-lezen gebruikers toevoegen

Stap 8. Maak beleidssets die overeenkomen met het SWA IP-adres. Dit is om toegang tot andere apparaten met deze gebruikersreferenties te voorkomen.

Navigeer naar Policy > PolicySets en klik op +pictogram in de linkerbovenhoek.

Policy Sets

+	Status	Policy Set Name	Description	Conditions
Search				

Beleidsset toevoegen in ISE

Stap 8.1. Een nieuwe regel wordt bovenaan uw Policy Sets geplaatst.

Noem het nieuwe beleid en voeg een voorwaarde voor RADIUS NAS-IP-Adres attribuut toe om het SWA IP-adres aan te passen.

Klik op Gebruik om de wijzigingen te bewaren en de editor te verlaten.

Conditions Studio ? ×

Library

📍
🗨️
📄
👤
🌐
📶
📱
📧
📅
🕒
👤
🔒
📶

- 📄 Catalyst_Switch_Local_Web_Authentication ?
- 📄 Switch_Local_Web_Authentication ?
- 📄 Switch_Web_Authentication ?
- 📄 Wired_802.1X ?
- 📄 Wired_MAB ?
- 📄 Wireless_802.1X ?
- 📄 Wireless_Access ?
- 📄 Wireless_MAB ?
- 📄 WLC_Web_Authentication ?

Editor

📍

Equals ▼

⊞

Set to 'Is not'
Duplicate
Save

+
New AND OR

Close
Use

Voeg beleid toe aan kaart SWA Network Device

Stap 8.2. Klik op Save (Opslaan).

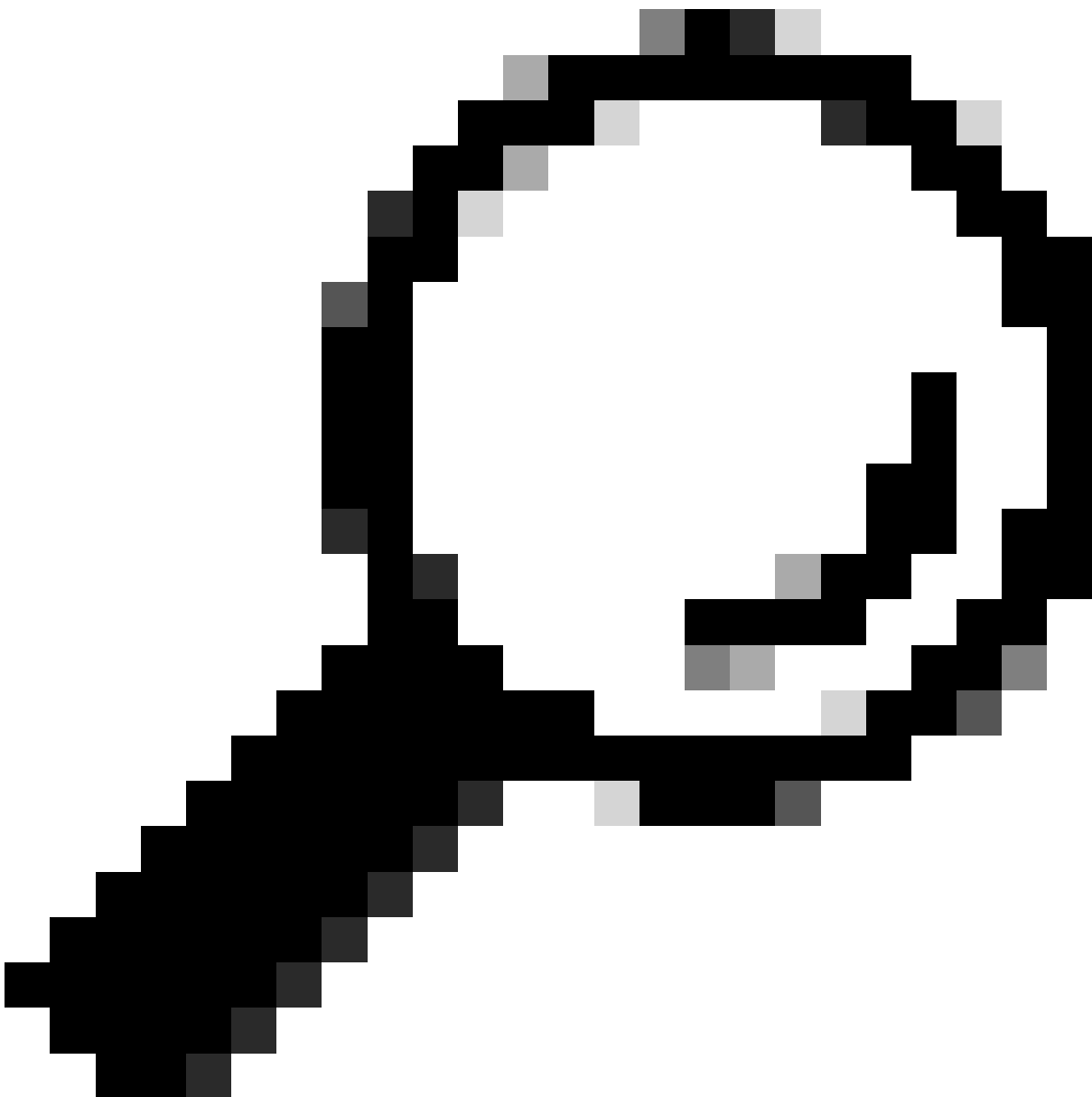
Policy Sets

[Reset Policyset Hitcounts](#)[Reset](#)[Save](#)

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
		SWA Access		Radius-NAS-IP-Address EQUALS 10.106.38.176	Default Network Access x ▾ +			
		Default	Default policy set		Default Network Access x ▾ +	0		

[Reset](#)[Save](#)

Beleidsbesparing



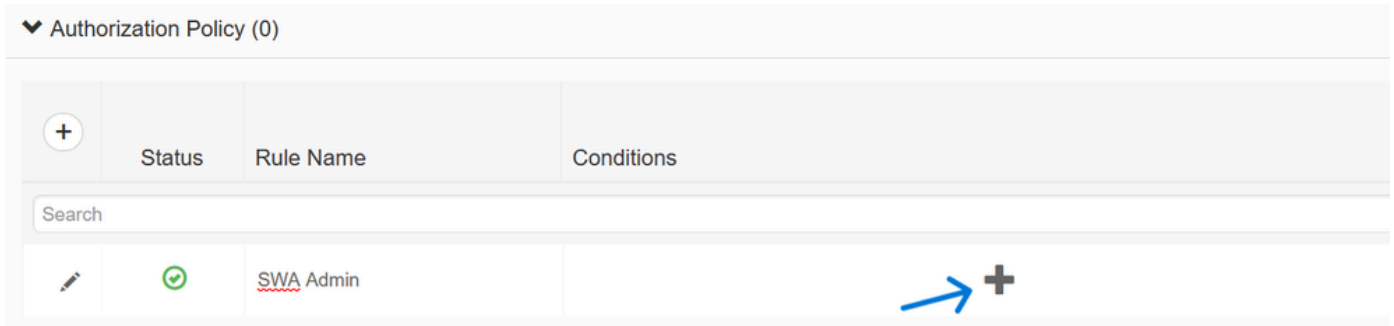
Tip: in dit artikel is de lijst Default Network Access Protocols toegestaan. U kunt een nieuwe lijst maken en indien nodig verkleinen.

Stap 9. Als u de nieuwe beleidssets wilt weergeven, klikt u op het >-pictogram in de kolom Weergave. Breid het menu van het Beleid van de Vergunning uit en klik het + pictogram om een

nieuwe regel toe te voegen om de toegang tot de gebruiker met beheerdersrechten te verlenen.

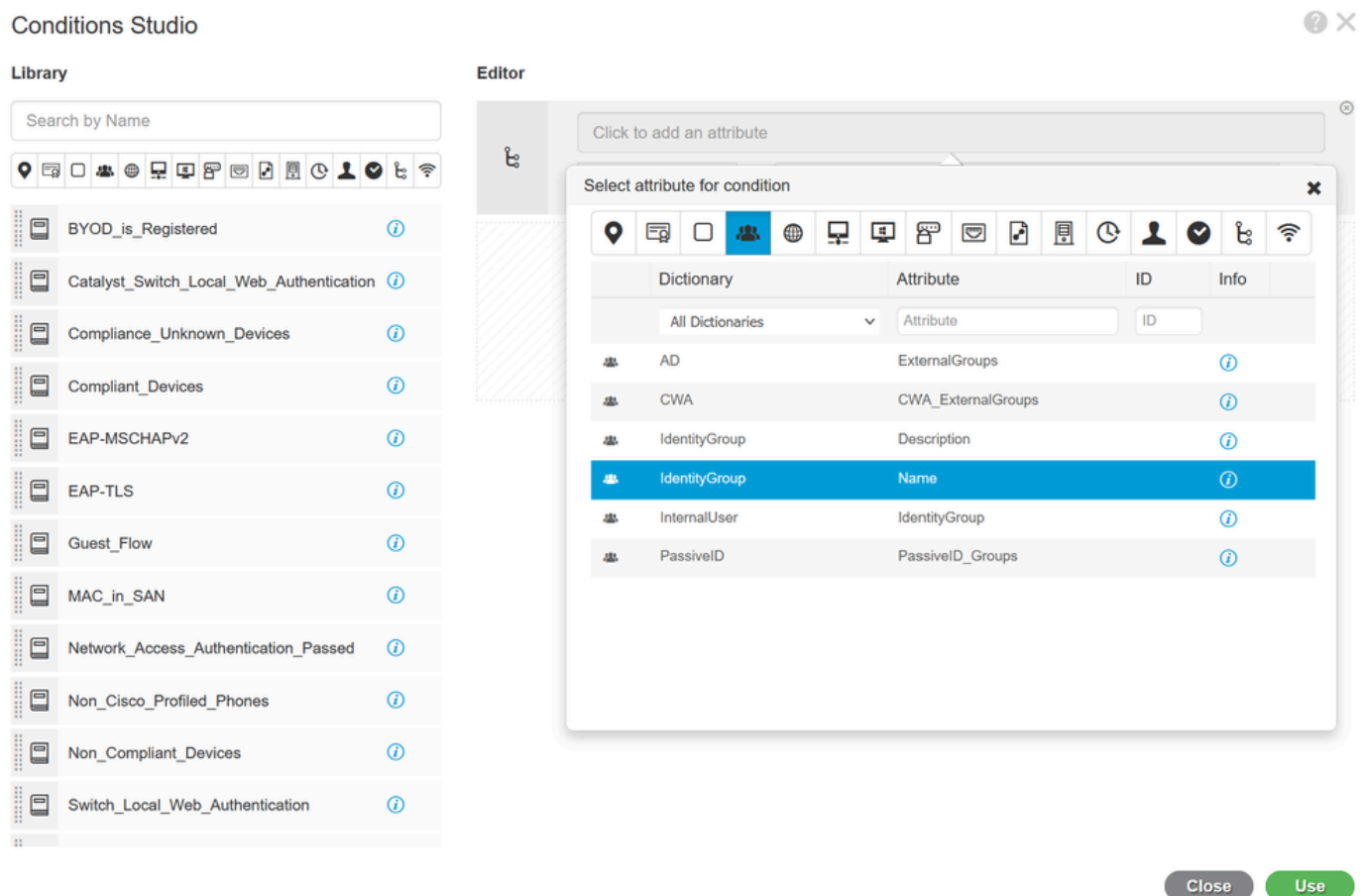
Stel een naam in.

Stap 9.1. Om een voorwaarde te creëren om Admin gebruikersgroep aan te passen, klikt u op + pictogram.



Toepassingsbeleidsvoorwaarde toevoegen

Stap 9.2. Stel de voorwaarden in om de woordenboek identiteitsgroep met attribuut naam gelijk te stellen aan gebruikers identiteitsgroepen: SWA admin.



Selecteer identiteitsgroep als voorwaarde

Stap 9.3. Scroll naar beneden en selecteer Gebruikersidentiteitsgroepen: SWA admin.

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 ⓘ

Non_Compliant_Devices ⓘ

Switch_Local_Web_Authentication ⓘ

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 naar beneden

Stap 9.4. Klik op Gebruik.

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

Set to 'Is not'

*User Identity Groups:SWA Admin

You can only select 1 item

Save

+ New AND OR

Close Use

Selecteer Autorisatiebeleid voor SWA Admin User Group

Stap 10. Klik op het pictogram + om een tweede regel toe te voegen, zodat de gebruiker toegang heeft tot alleen-lezen rechten.

Stel een naam in.

Stel de voorwaarden in om de Dictionary Identity Group met Attribute Name gelijk te stellen aan User Identity Groups: SWA ReadOnly en klik op 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

Selecteer Autorisatiebeleid voor alleen-lezen gebruikersgroep

Stap 11. Stel het autorisatieprofiel voor elke regel in en klik op Opslaan.

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 Profiles	Security Groups	Hits	Actions
✓	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

Selecteer een autorisatieprofiel

Configuratie SWA

Stap 1. Van SWA GUI navigeer aan Systeembeheer en klik Gebruikers.

Stap 2. Klik op Inschakelen in externe verificatie.

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...

Externe verificatie in SWA inschakelen

Stap 3. Voer IP-adres of FQDN van de ISE in het veld RADIUS-server Hostname in en voer hetzelfde gedeelte geheim in dat is geconfigureerd in stap 2, ISE-configuratie.

Stap 4. Selecteer Buiten geverifieerde gebruikers toewijzen aan meerdere lokale rollen in groepstoewijzing.

Stap 4.1. Voer in het veld RADIUS-klassekenmerken een beheerder in en selecteer de beheerder Rol.

Stap 4.2. Voer in het veld RADIUS-KLASSENKENMERKEN een ReadUser-waarde in en selecteer de operator Alleen-lezen rol.



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

Externe verificatieconfiguratie voor RADIUS-server

Stap 5: Om Gebruikers in SWA te configureren, klikt u op Add User. Voer een gebruikersnaam in en selecteer het gebruikerstype dat vereist is voor de gewenste rol. Voer een wachtwoordgroep in en typ een wachtwoordgroep opnieuw. Dit is vereist voor GUI-toegang als het apparaat geen verbinding kan maken met een externe RADIUS-server.

Opmerking: als het apparaat geen verbinding kan maken met een externe server, probeert het de gebruiker te verifiëren als een lokale gebruiker die is gedefinieerd in de Secure Web Applicatie.

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"/> 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	

Gebruikersconfiguratie in SWA

Stap 6: Klik op Indienen en Wijzigingen vastleggen.

Verifiëren

Open de SWA GUI met de geconfigureerde gebruikersreferenties en controleer de bewegende inloggegevens van ISE. Om de live logs in ISE te controleren, navigeer je naar Operations > Live Logs:

The screenshot displays the Cisco Identity Services Engine (ISE) interface. At the top, the Cisco logo and 'Identity Services Engine' are visible. The main content is divided into two panels: 'Overview' and 'Authentication Details'. The 'Overview' panel shows a successful authentication event for user 'adminuser' with the message '5200 Authentication succeeded'. Below this, various fields are listed, including 'Endpoint Id', 'Endpoint Profile', 'Authentication Policy' (SWA Access >> Default), 'Authorization Policy' (SWA Access >> SWA Admin), and 'Authorization Result' (SWA Admin). The 'Authentication Details' panel shows the 'Source Timestamp' and 'Received Timestamp' as '2024-01-28 17:28:31.573'. To the right of these panels, a 'Steps' section lists a sequence of 16 log entries, each with a numeric ID and a description of the authentication process, such as 'Received RADIUS Access-Request', 'RADIUS created a new session', and 'Authentication Passed'.

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

Controleer de gebruikersaanmelding bij ISE

Gerelateerde informatie

- [Gebruikershandleiding voor AsyncOS 14.0 voor Cisco Secure Web applicatie](#)
- [ISE 3.0 beheerdershandleiding](#)
- [ISE-compatibiliteitsmatrix voor beveiligde web applicatie](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.