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

Inhoud

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

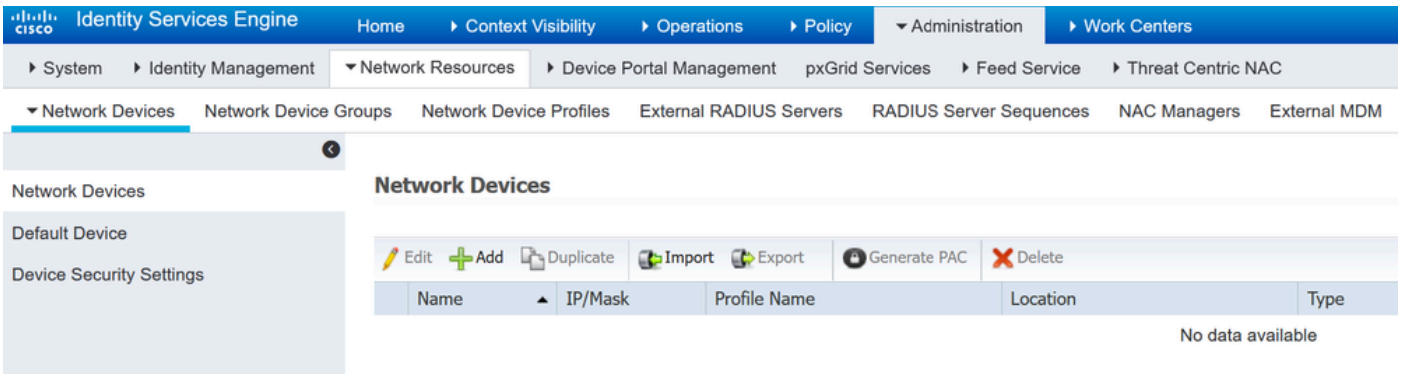
Netwerktopologiediagram

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

Configureren

ISE-configuratie

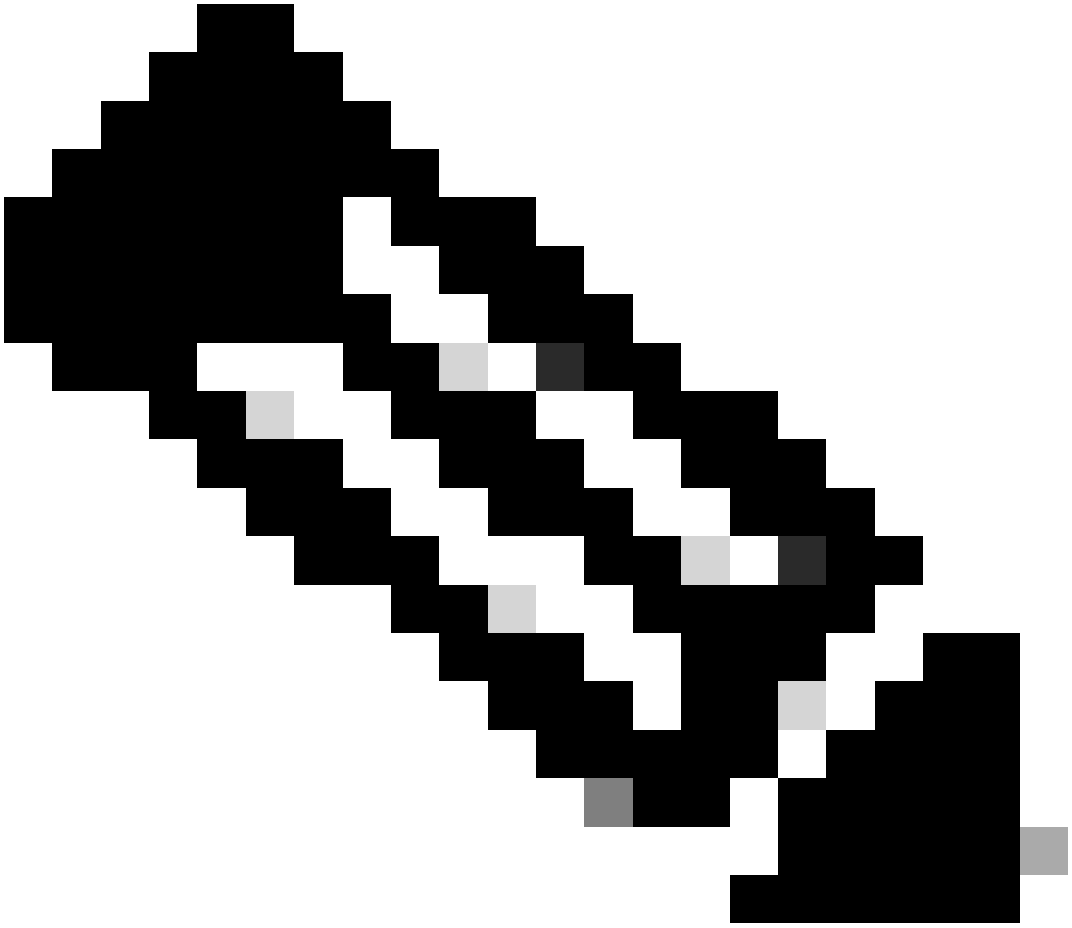
Stap 1. Voeg een nieuw netwerkapparaat toe. Ga naar Beheer > Netwerkbronnen > Netwerkapparaten > +Add.



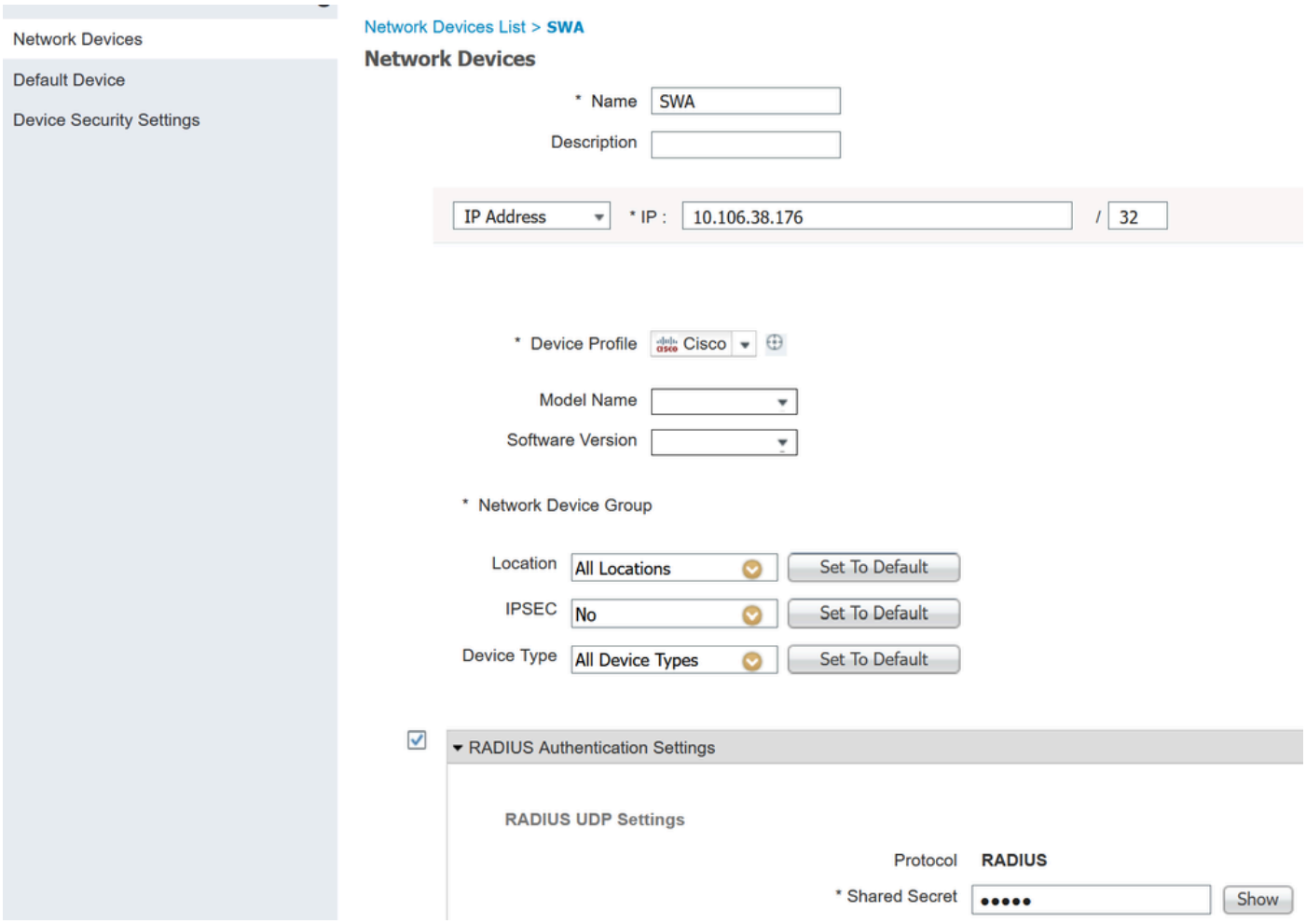
SWA als netwerkapparaat toevoegen in ISE

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.

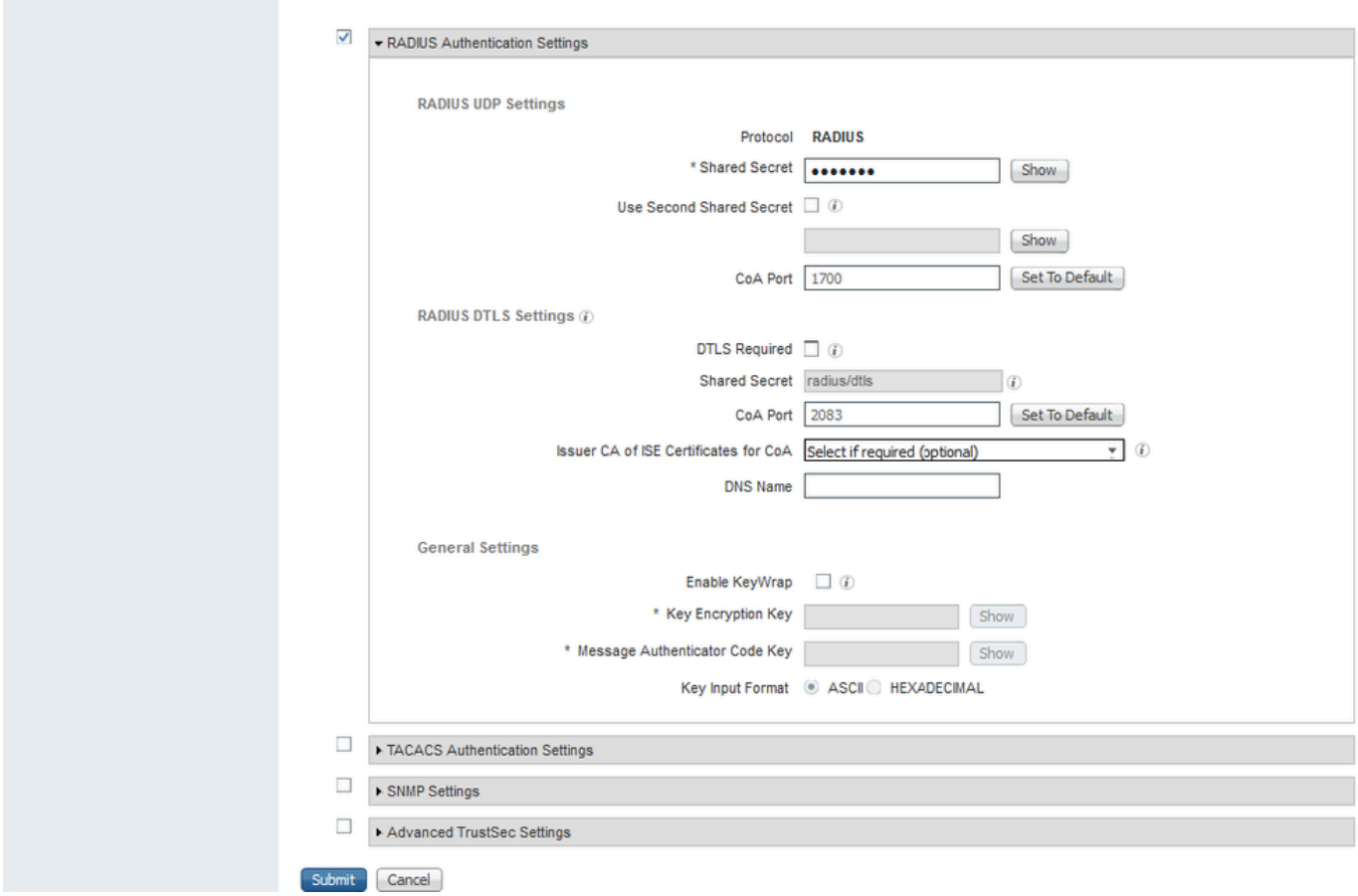


Opmerking: dezelfde toets moet later worden gebruikt om de RADIUS-server in SWA te configureren.



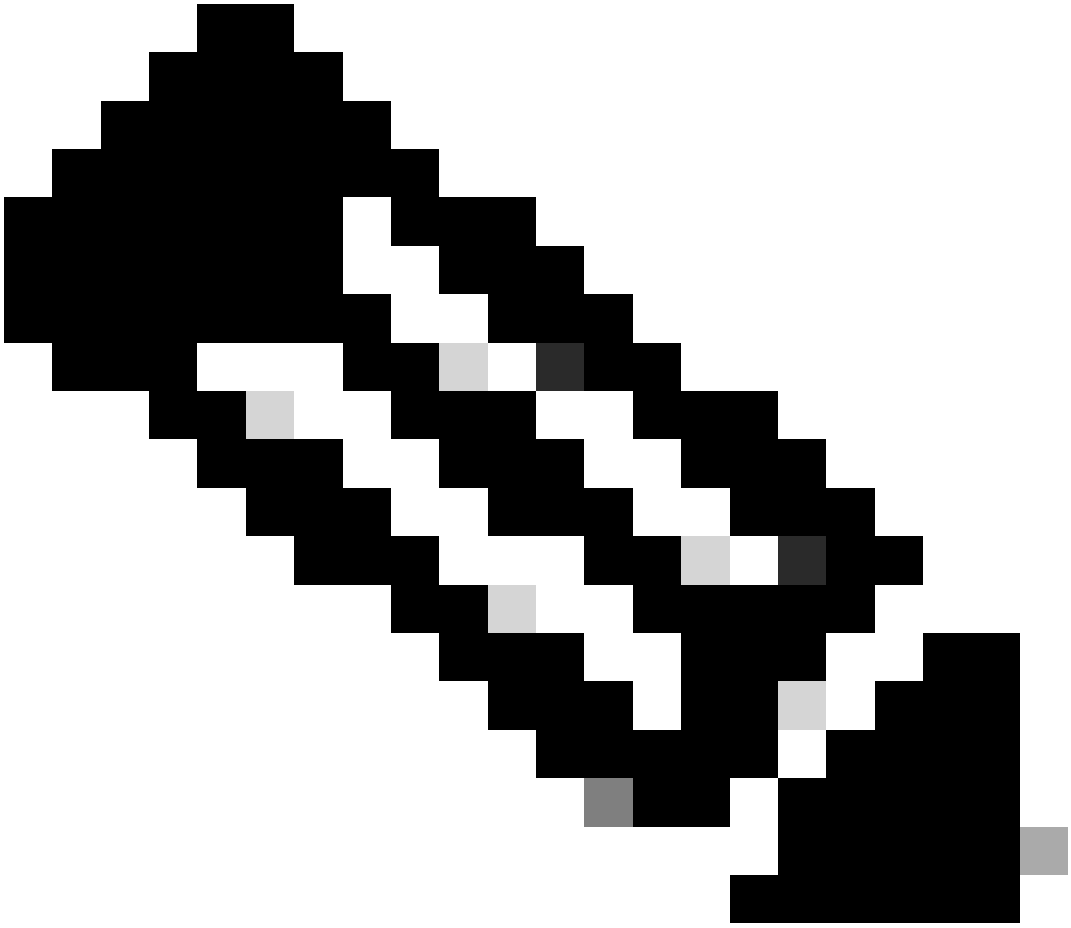
gedeelde sleutel voor netwerkapparaat configureren

Stap 2.1. Klik op Verzenden.

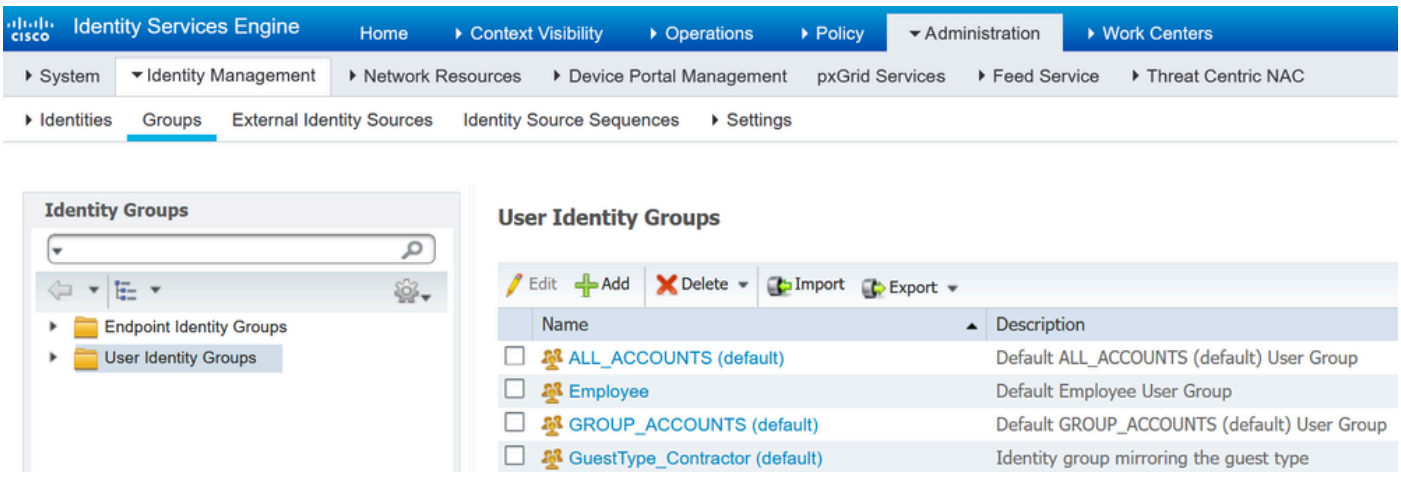


Configuratie van netwerkapparaat verzenden

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



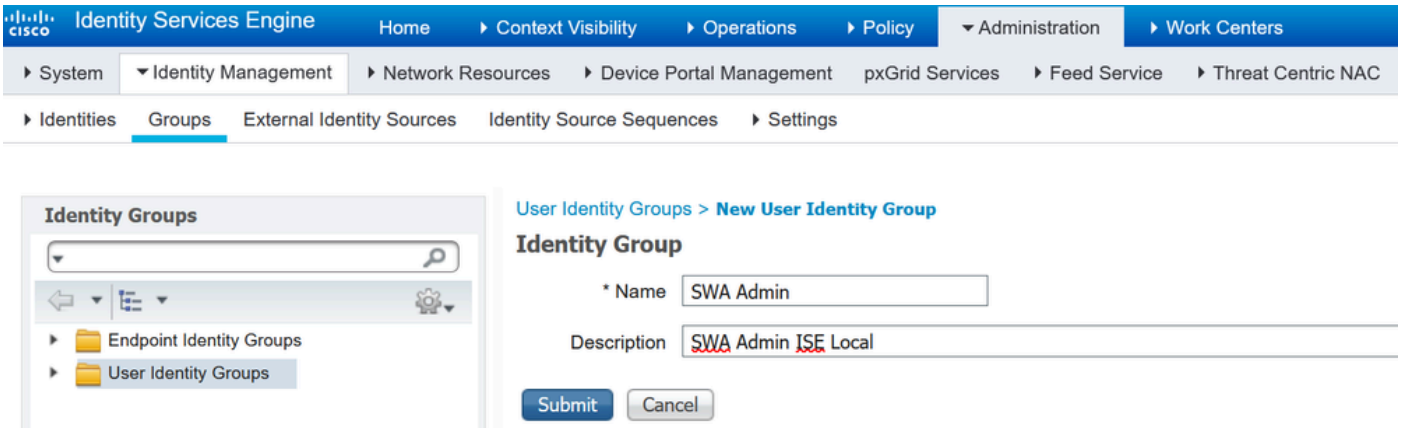
Opmerking: u dient verschillende gebruikersgroepen te configureren volgens het verschillende type gebruikers.



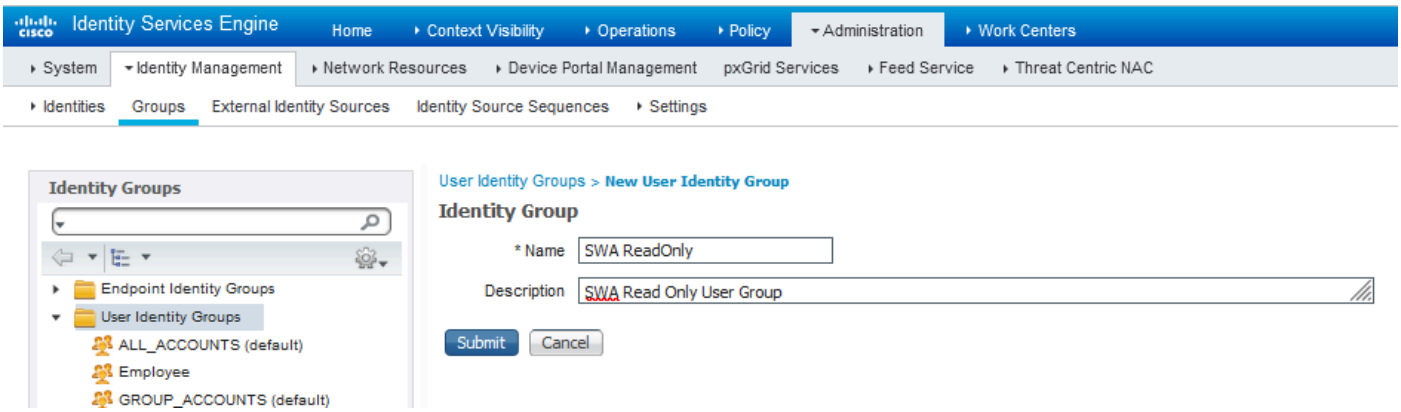
Gebruikersidentiteitsgroep toevoegen

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.



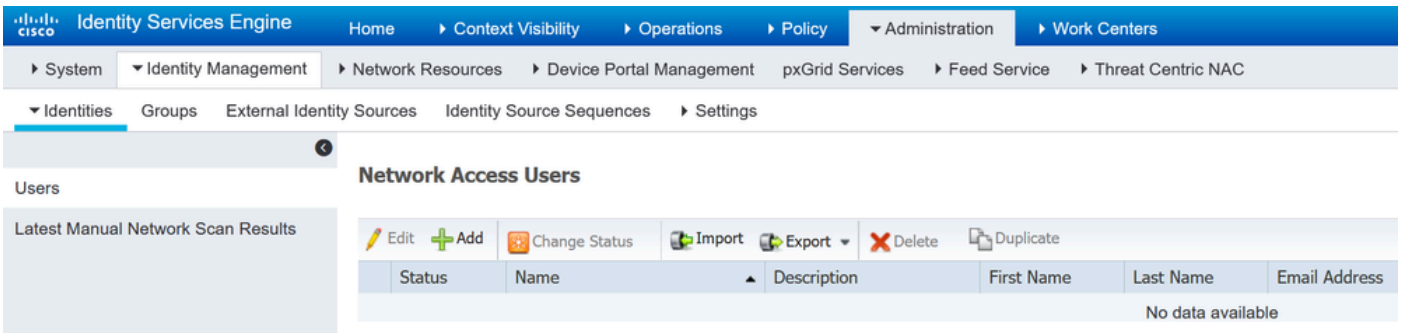
Gebruikersidentiteitsgroep toevoegen



Gebruikersidentiteitsgroep toevoegen voor SWA Lees alleen gebruikers

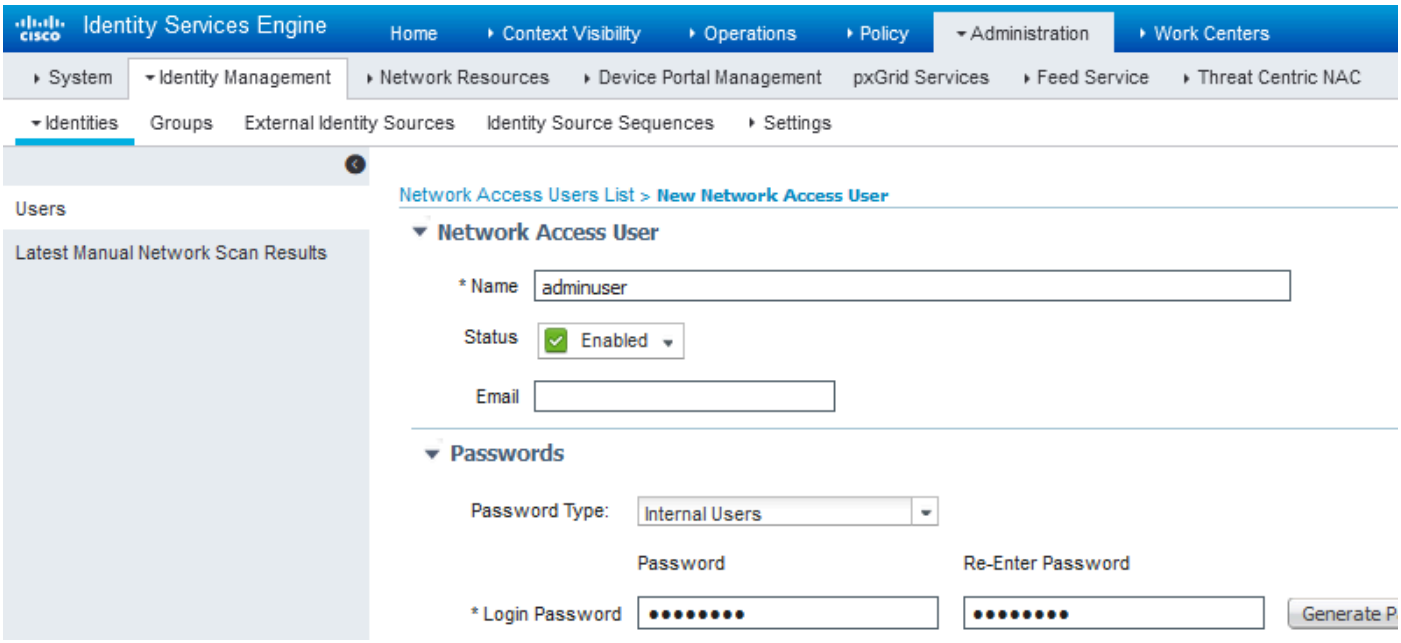
Stap 5. U moet gebruikers voor netwerktoegang maken die overeenkomen met de gebruikersnaam die in SWA is ingesteld.

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



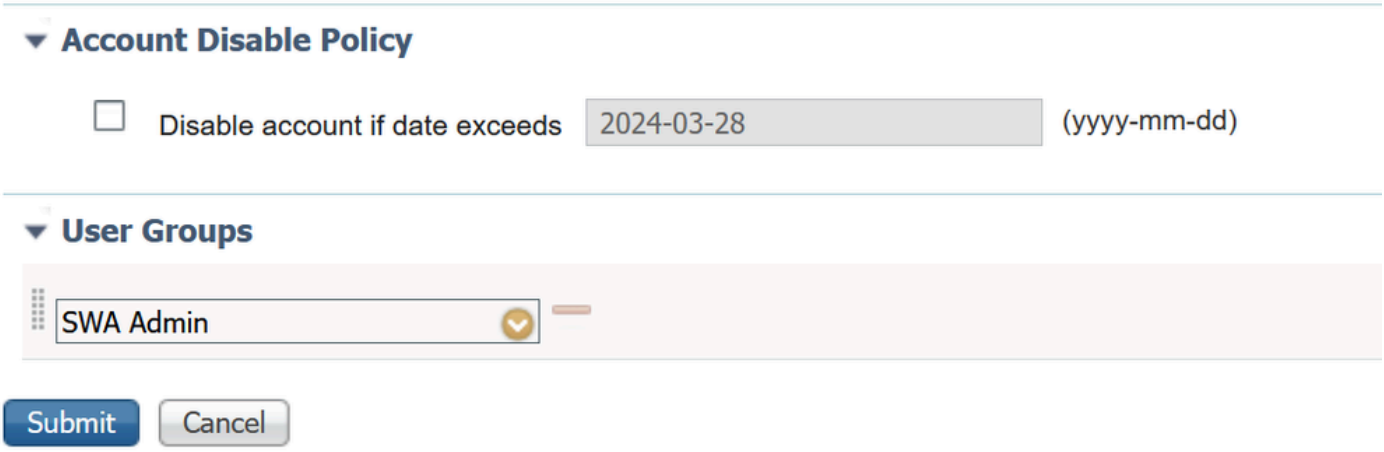
Voeg lokale gebruikers toe in ISE

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



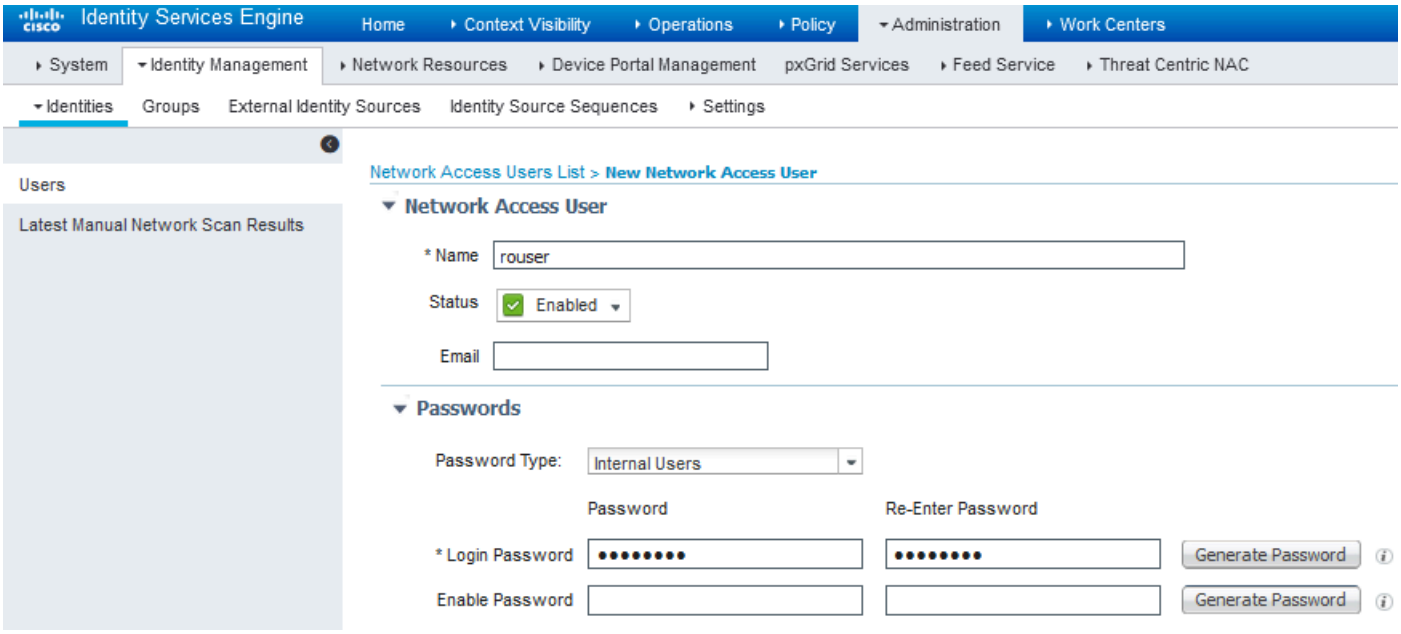
Admin-gebruiker toevoegen

Stap 5.2. Kies SWA Admin in het gedeelte Gebruikersgroepen.



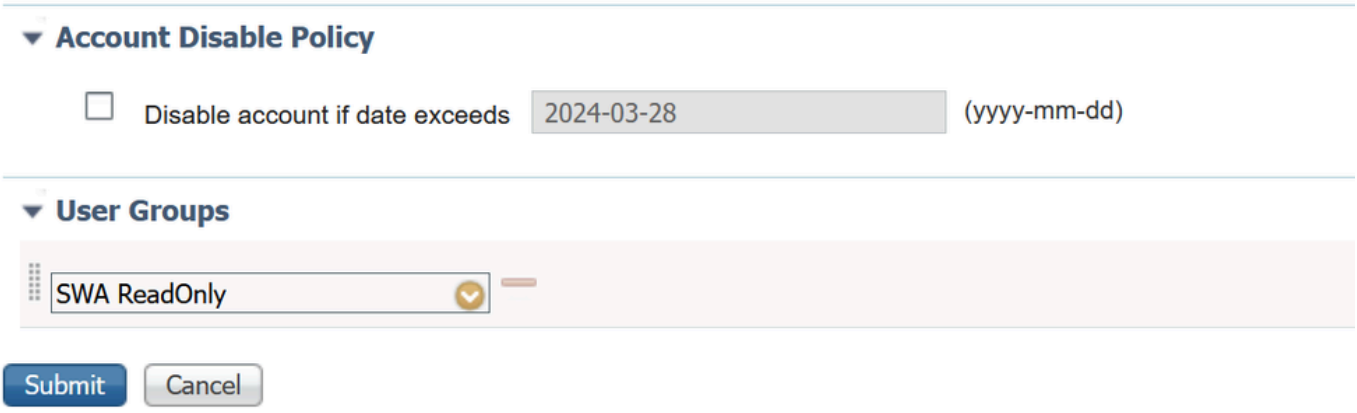
Toewijzen aan de beheerder Gebruiker

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



Alleen-lezen gebruiker toevoegen

Stap 5.4. Kies SWA ReadOnly in de sectie Gebruikersgroepen.

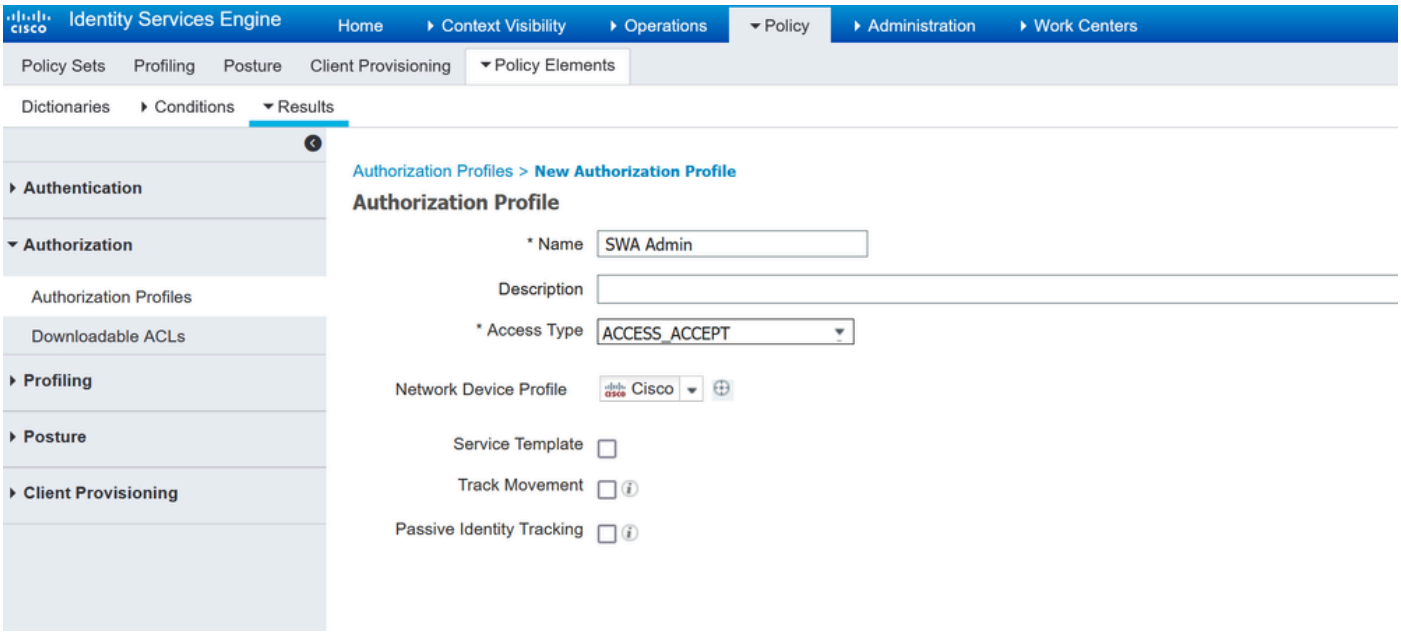


Wijs alleen-lezen gebruikersgroep toe aan de alleen-lezen gebruiker

Stap 6. Maak het autorisatieprofiel voor de beheerder.

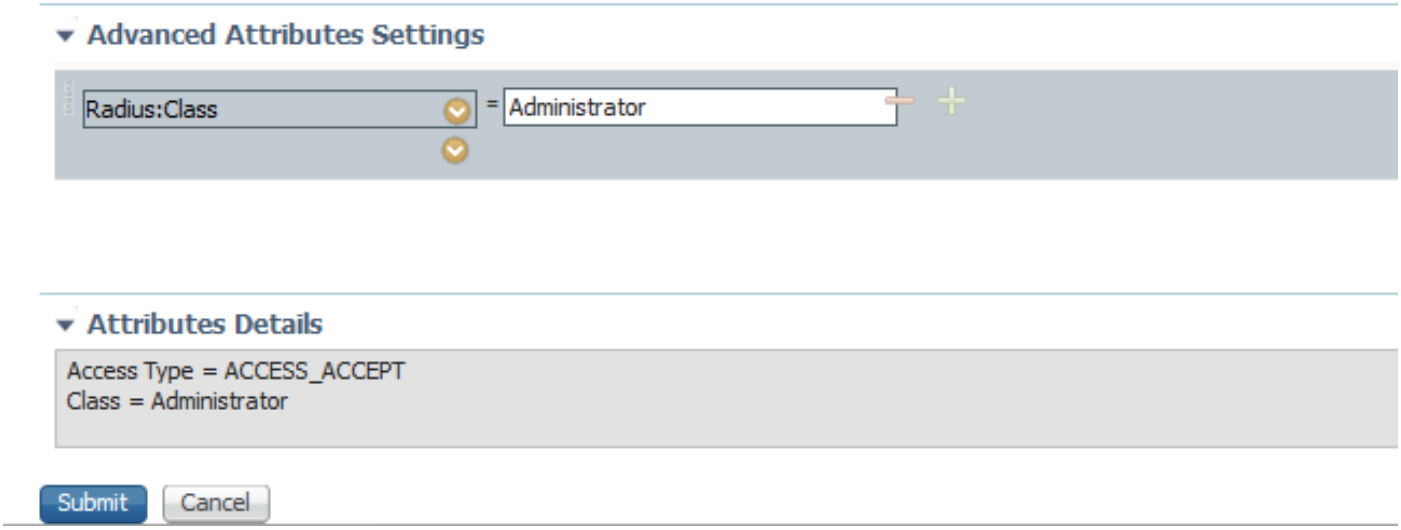
Navigeer naar Beleid > Beleidselementen > Resultaten > Vergunningprofielen > +Add.

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



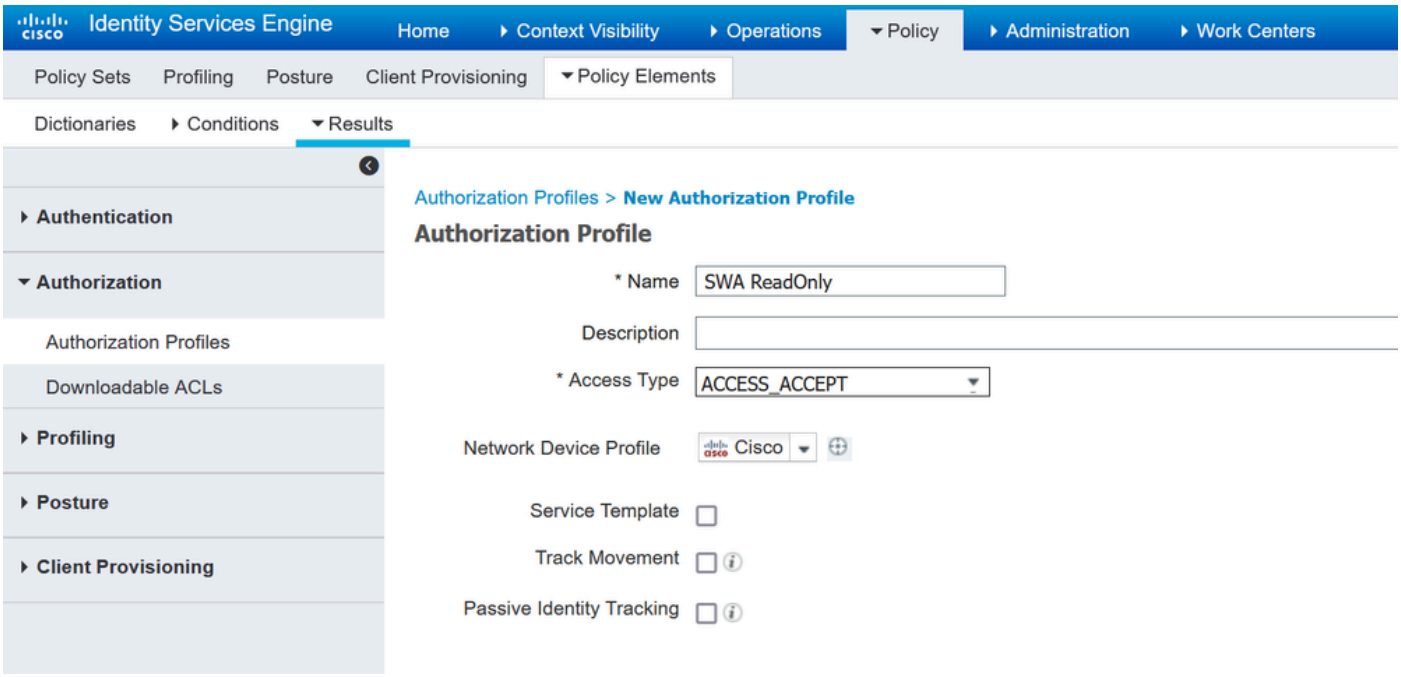
Vergunningsprofiel voor beheerder-gebruikers toevoegen

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.



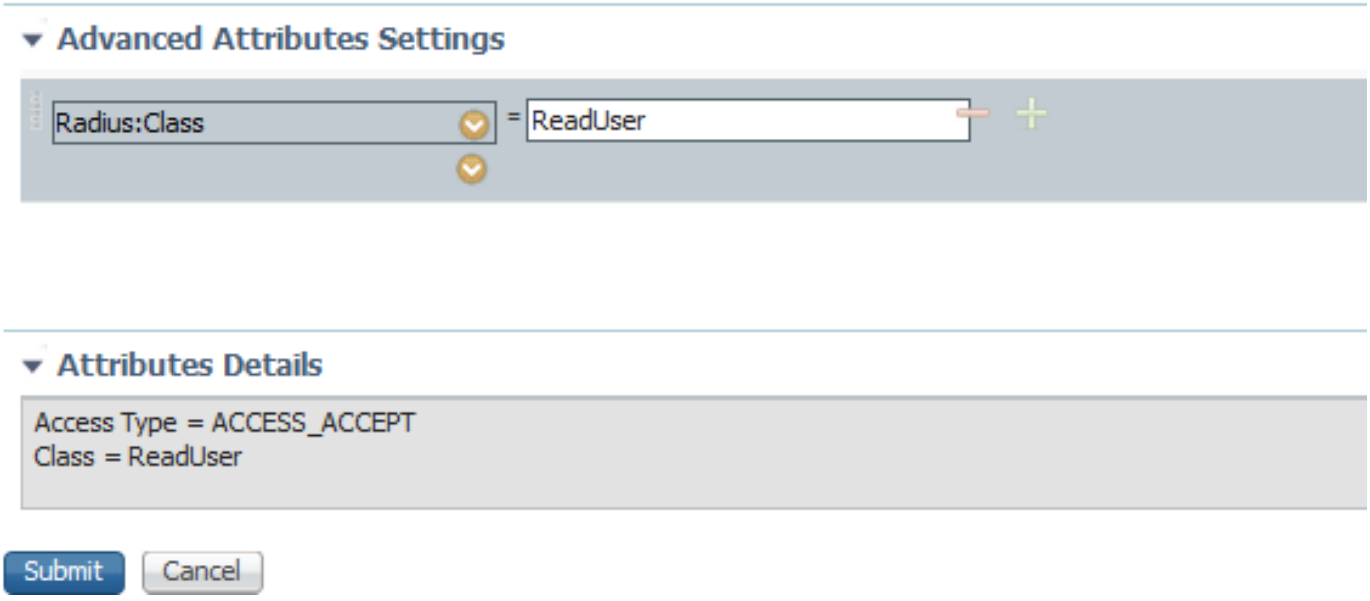
Add Authorisation Profile for Admin Gebruikers

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



Vergunningsprofiel voor alleen-lezen gebruikers toevoegen

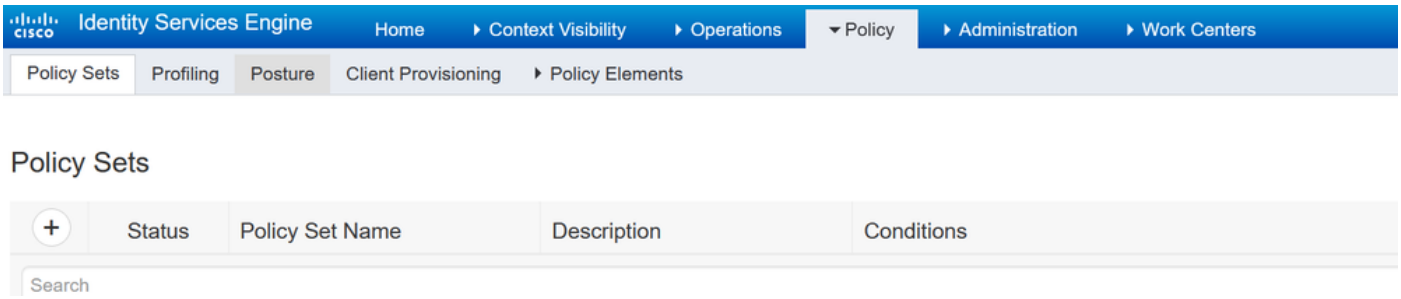
STAP 7.1. Maak de straal:Klasse met de waarde ReadUser in plaats van Administrator dit keer.



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.

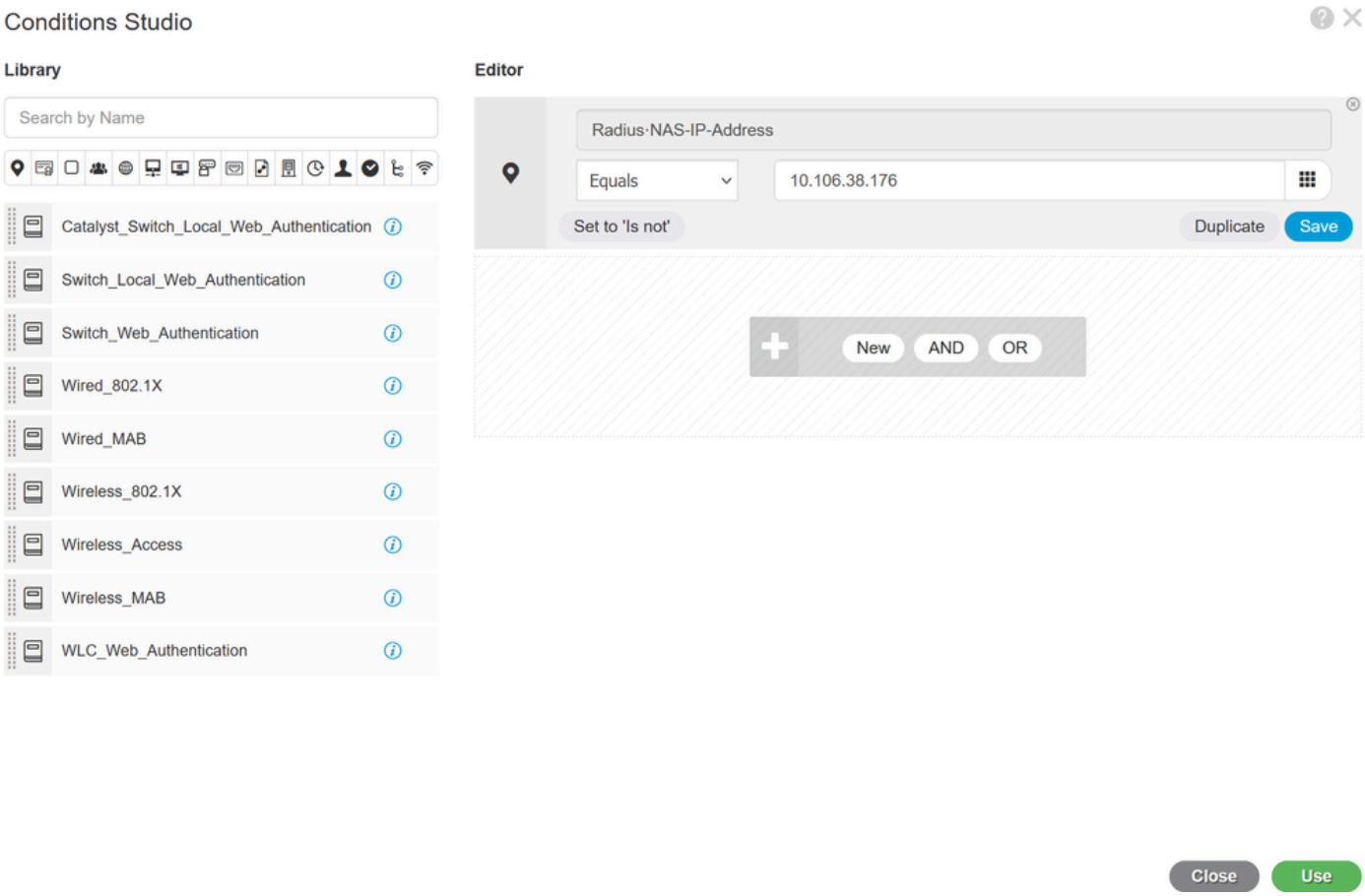


Beleidsset toevoegen in ISE

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.

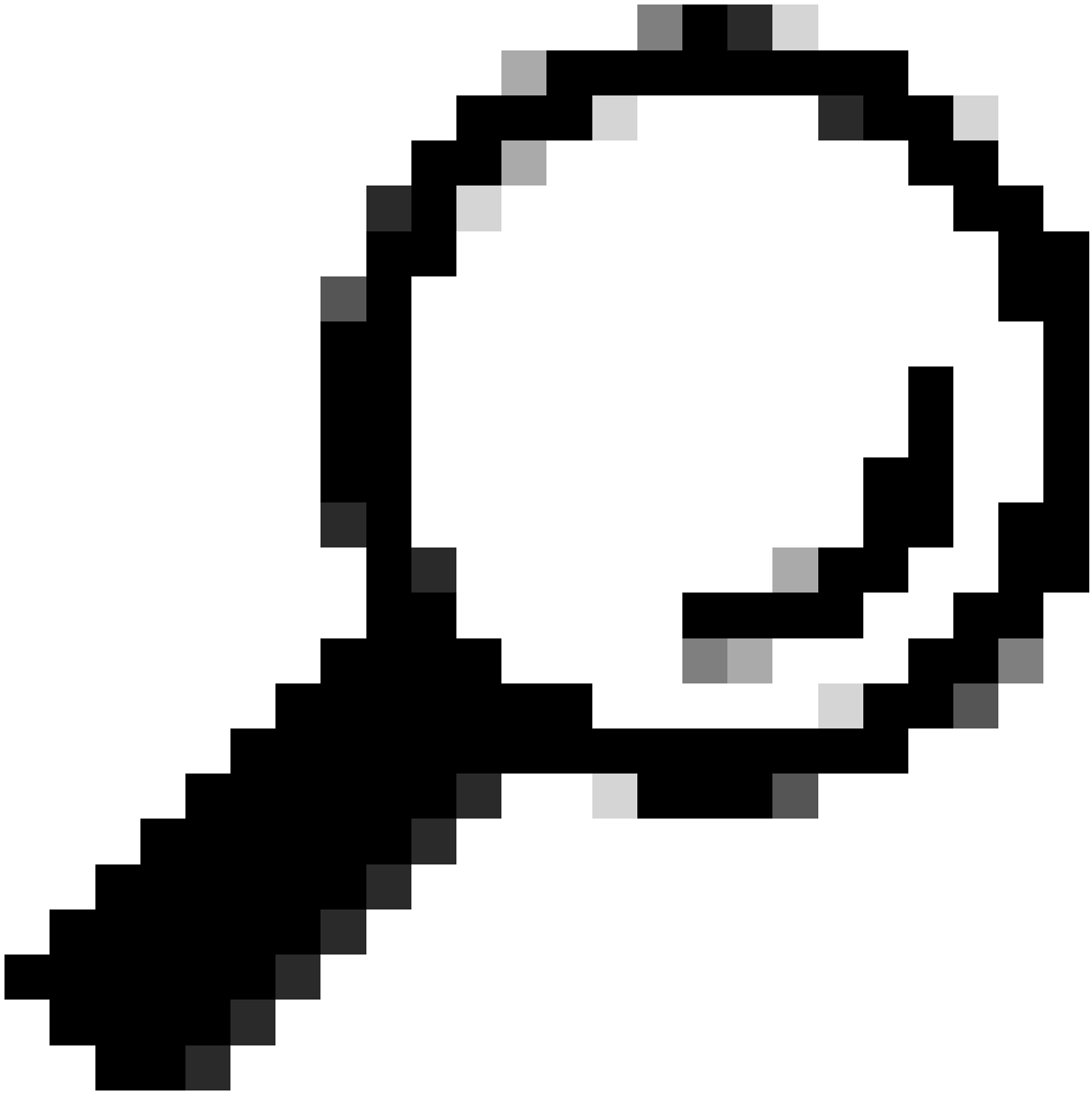
Klik op Gebruik om de wijzigingen te bewaren en de editor te verlaten.



Voeg beleid toe aan kaart SWA Network Device

Stap 8.2. Klik op Save (Opslaan).

Beleidsbesparing



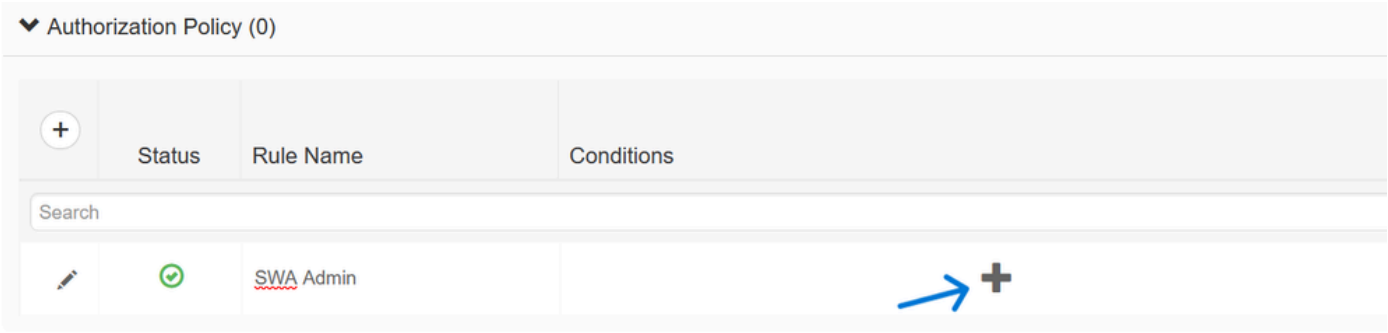
Tip: in dit artikel is de lijst Default Network Access Protocols toegestaan. U kunt een nieuwe lijst maken en indien nodig verkleinen.

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.

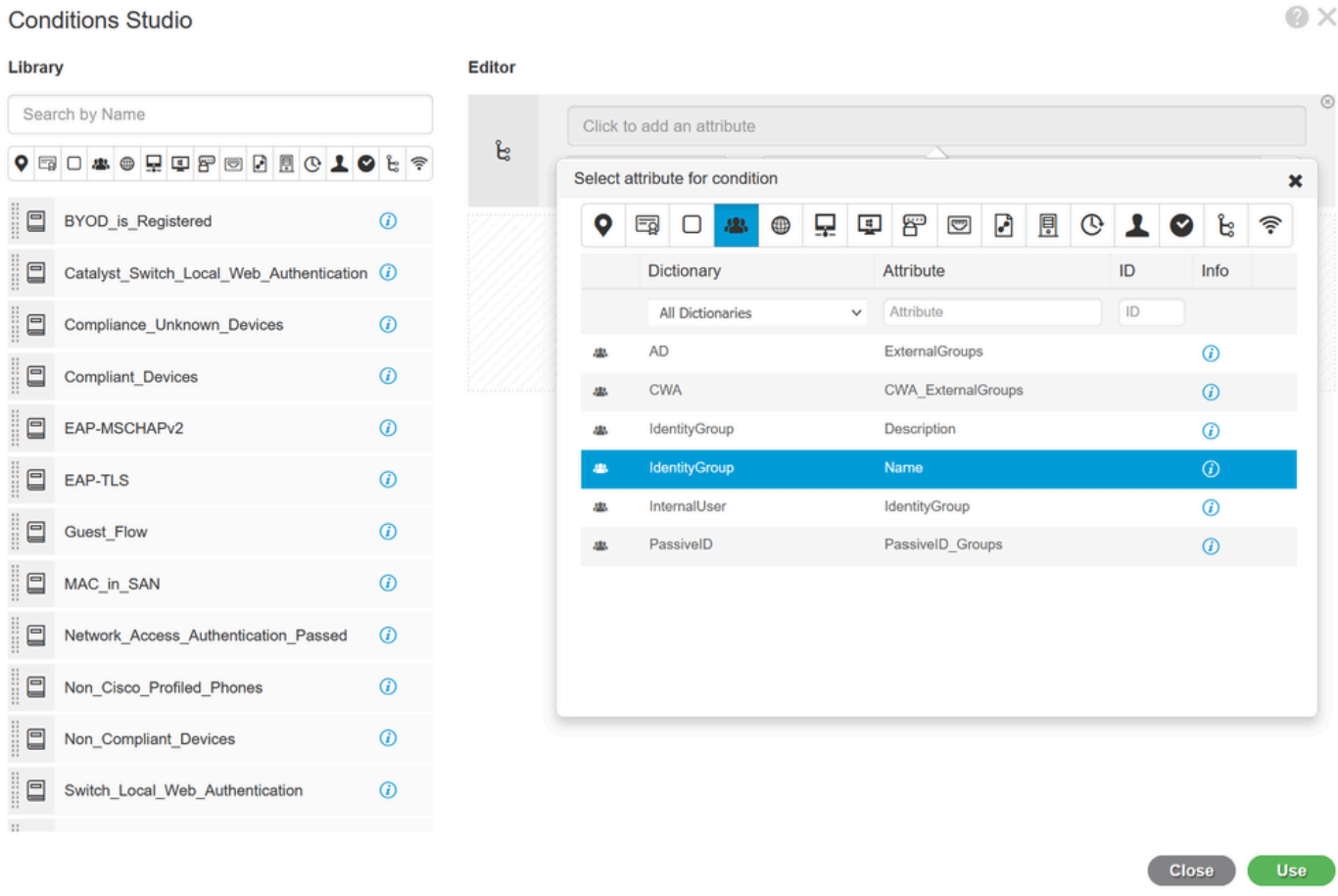
Stel een naam in.

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



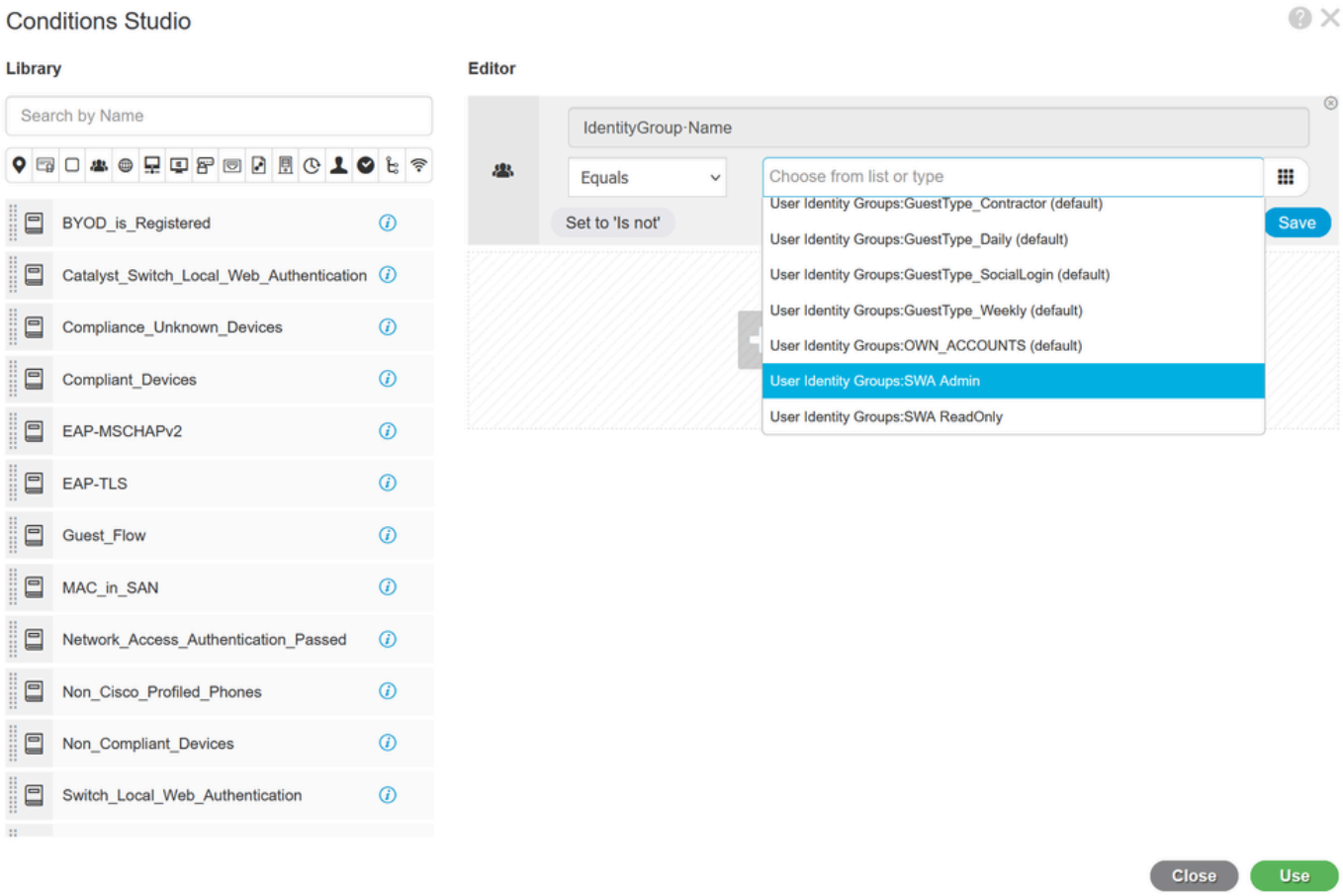
Toepassingsbeleidsvoorwaarde toevoegen

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



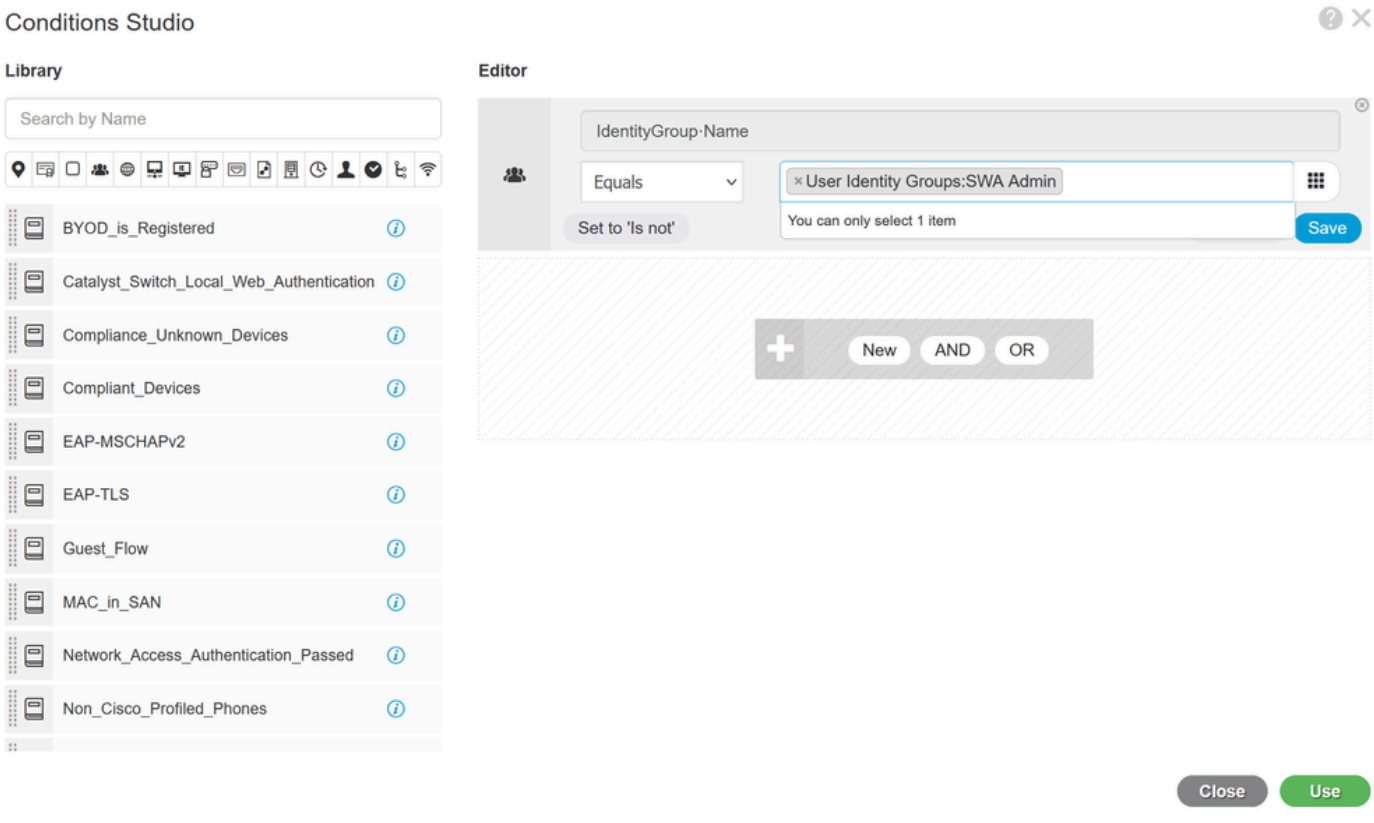
Selecteer identiteitsgroep als voorwaarde

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



Scroll naar beneden

Stap 9.4. Klik op Gebruik.

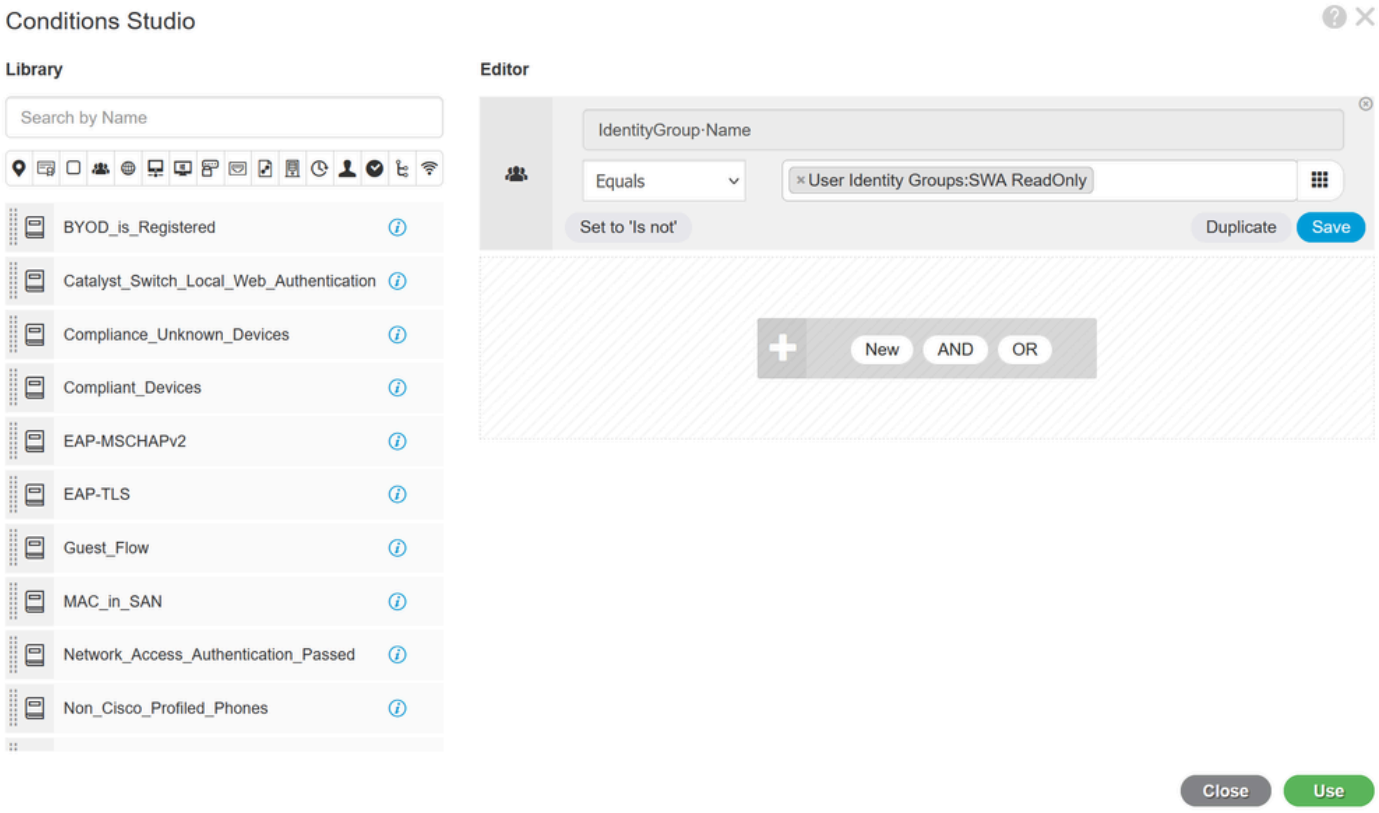


Selecteer Autorisatiebeleid voor SWA Admin User Group

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

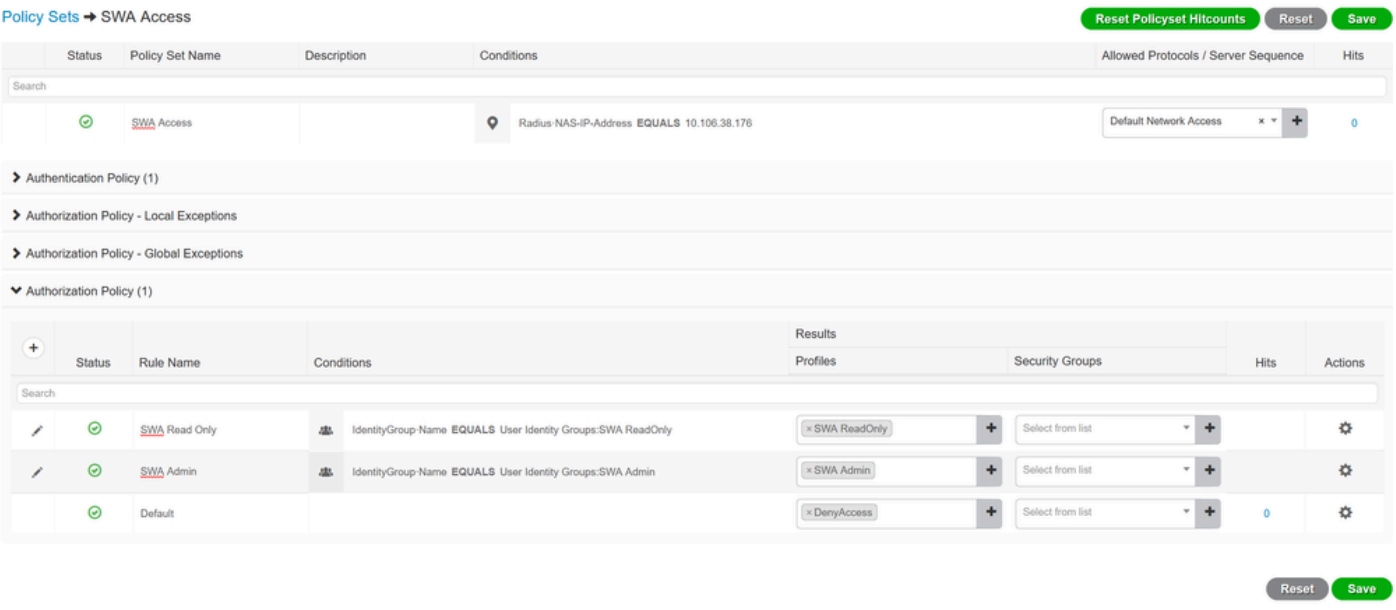
Stel een naam in.

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.



Selecteer Autorisatiebeleid voor alleen-lezen gebruikersgroep

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

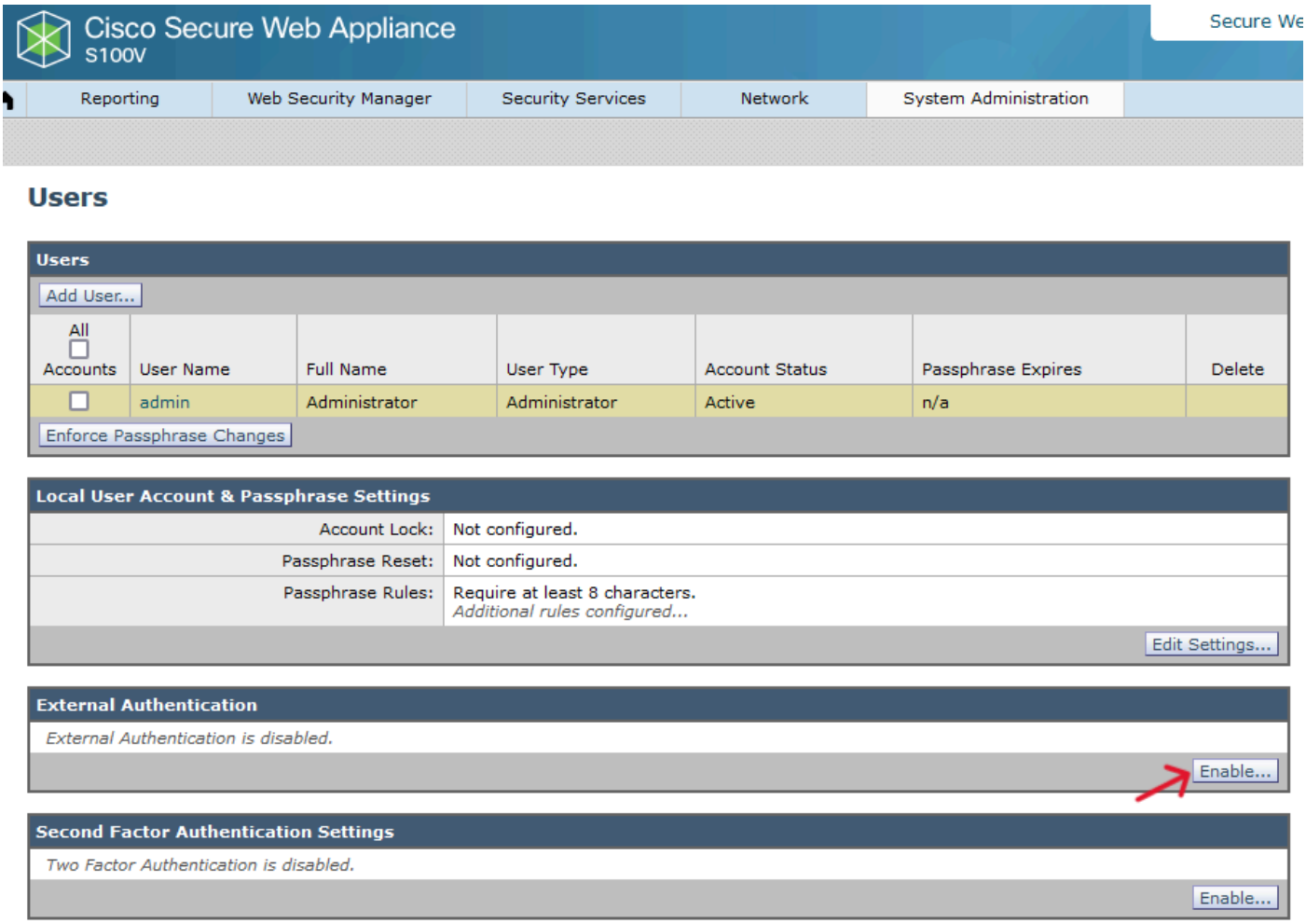


Selecteer een autorisatieprofiel

Configuratie SWA

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

Stap 2. Klik op Inschakelen in externe verificatie.



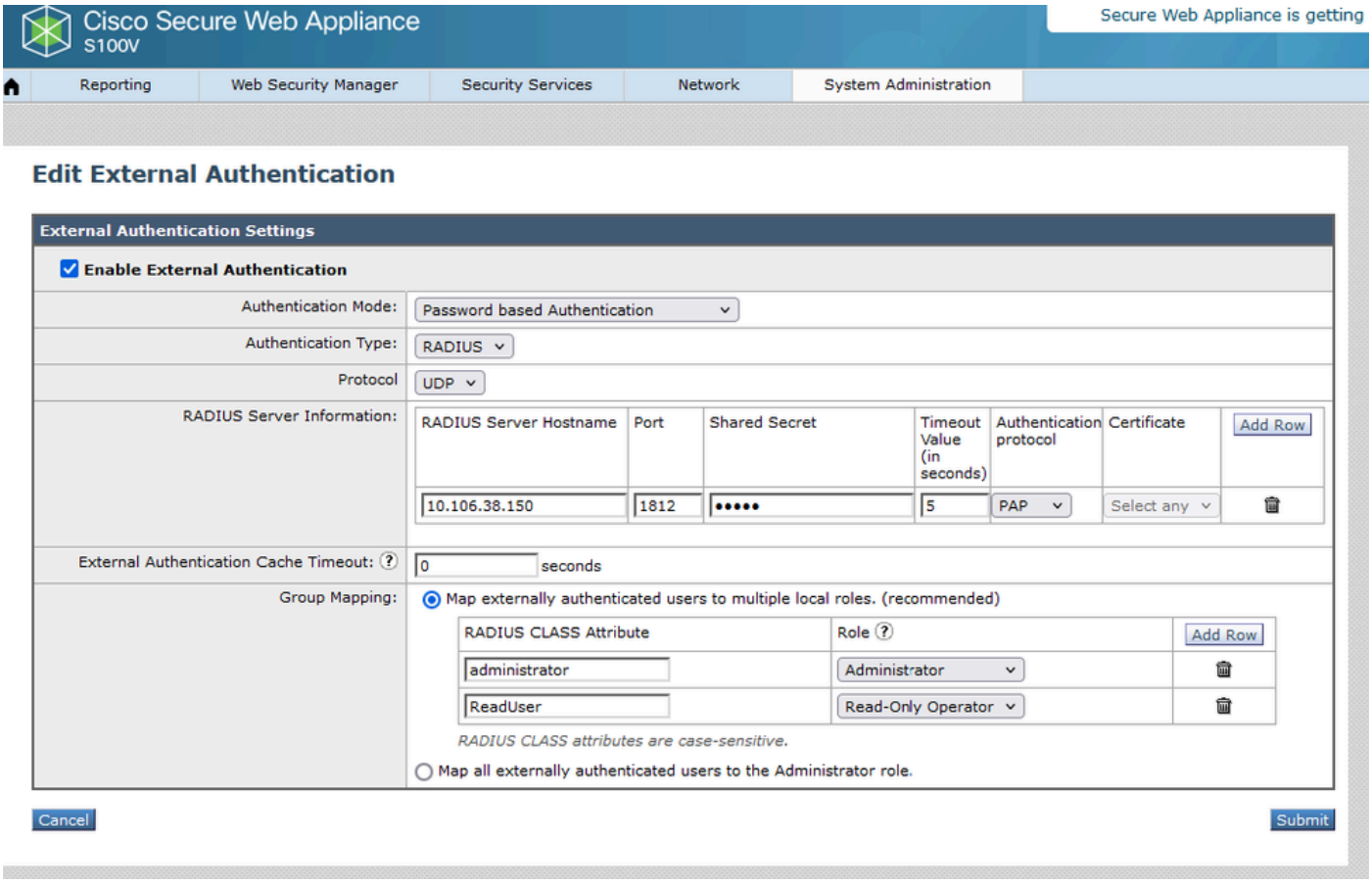
Externe verificatie in SWA inschakelen

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

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

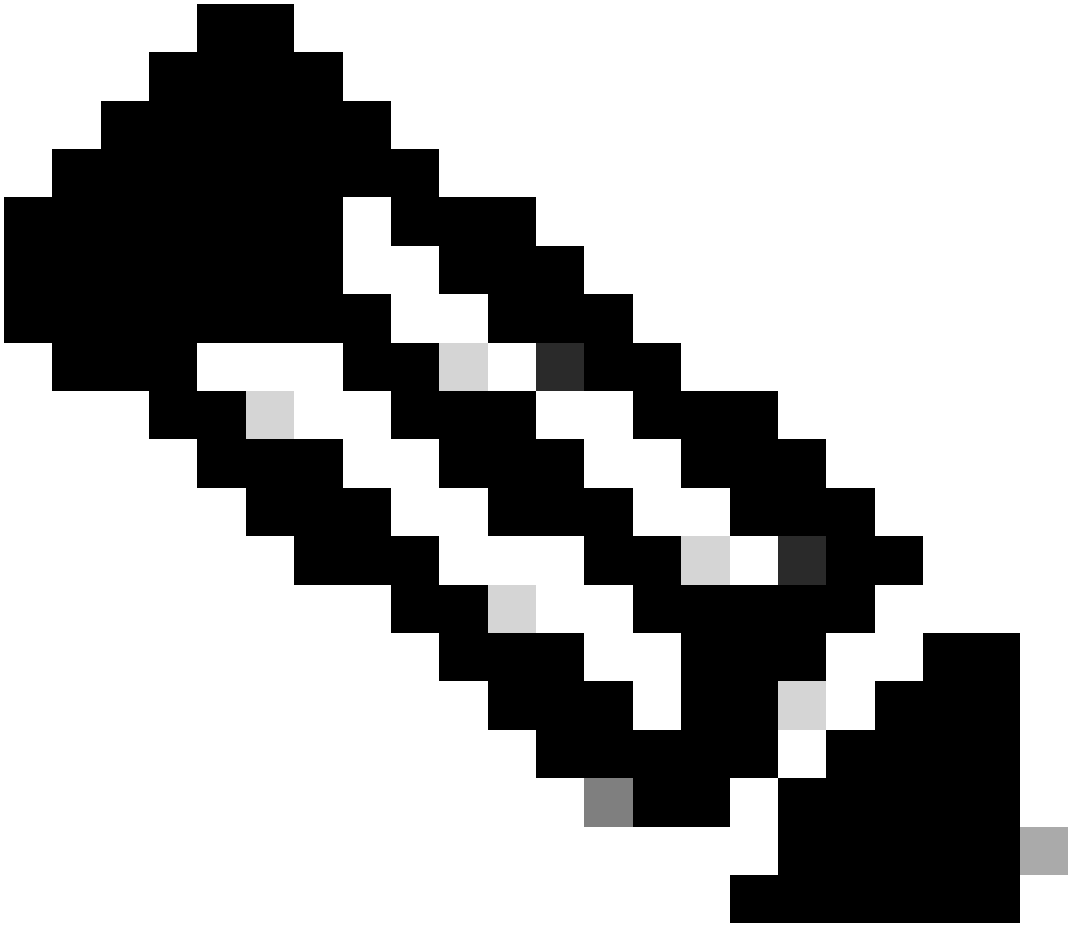
Stap 4.1. Voer in het veld RADIUS-klassekenmerken een beheerder in en selecteer de beheerder Rol.

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



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...

** 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.*

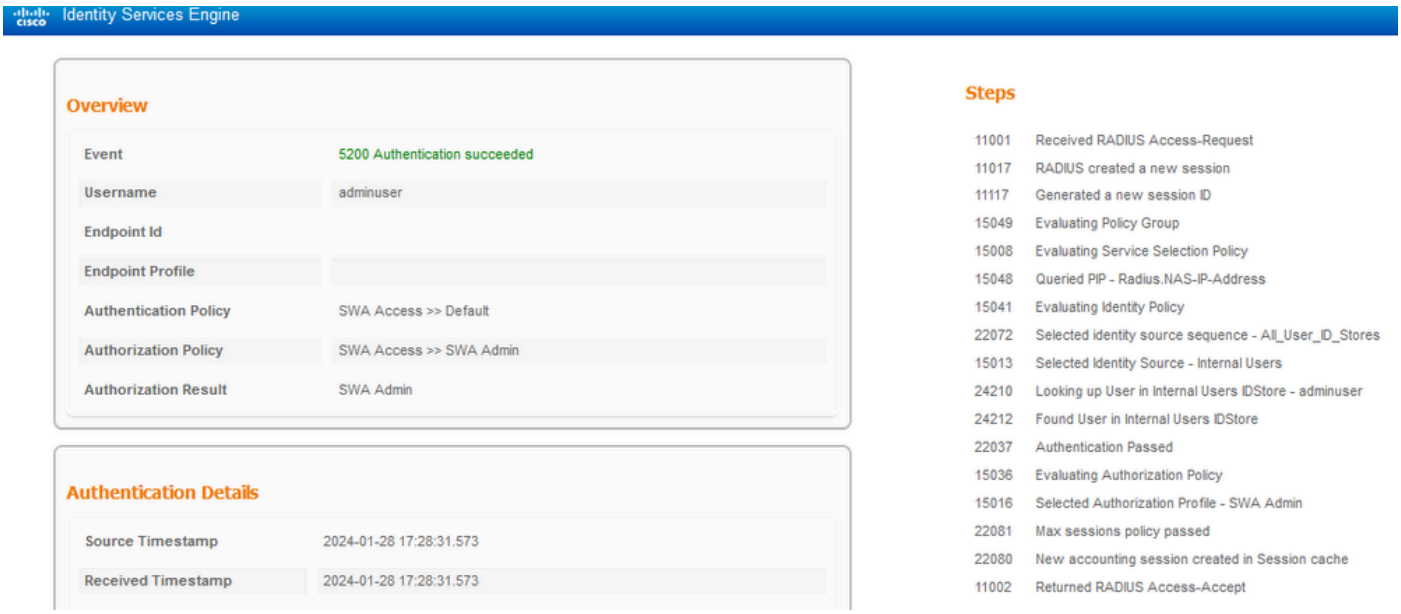
All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
☐	adminuser	Admin User	*Administrator*	Active	n/a	🗑
☐	rouser	RO User	*Read-Only Operator*	Active	n/a	🗑

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:



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.