

Op RADIUS gebaseerde beheerdersaanmelding configureren op Arista Switch

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Configureren](#)

[Cisco ISE configureren](#)

[Stap 1. Het Arista Network Device Profile voor Cisco ISE verkrijgen](#)

[Stap 2. Arista-Switch toevoegen als netwerkkapparaat](#)

[Stap 3. Het nieuwe apparaat valideren wordt weergegeven onder Netwerkkapparaten](#)

[Stap 4. De vereiste groepen voor gebruikersidentiteit maken](#)

[Stap 5. Stel een naam in voor de AdminUser Identity Group](#)

[Stap 6. Maak de lokale gebruikers en voeg ze toe aan hun correspondentengroep](#)

[Stap 7. Het autorisatieprofiel voor de beheerdersgebruiker maken](#)

[Stap 8. Een beleidsset maken die overeenkomt met het IP-adres van Arista Switch](#)

[Stap 9. De nieuwe beleidsset bekijken](#)

[Arista-Switch configureren](#)

[Stap 1. RADIUS-verificatie inschakelen](#)

[Stap 2. Configuratie opslaan](#)

[Verifiëren](#)

[ISE-beoordeling](#)

[Probleemoplossing](#)

[Scenario 1: "5405 RADIUS Request verwijderd"](#)

[Probleem](#)

[Mogelijke oorzaken](#)

[Oplossing](#)

[Scenario 2: Arista Switch faalt bij failover naar back-up van ISE PSN](#)

[Probleem](#)

[Mogelijke oorzaken](#)

[Oplossing](#)

Inleiding

In dit document wordt beschreven hoe u de Cisco Identity Services Engine (ISE) configureert om aanmeldingen van beheerders op Arista-switches te verifiëren met RADIUS.

Voorwaarden

Vereisten

Voordat u doorgaat, moet u ervoor zorgen dat:

- Cisco ISE (versie 3.x aanbevolen) is geïnstalleerd en operationeel.
- Arista switch met EOS met RADIUS-ondersteuning.
- Active Directory (AD) of Interne gebruikersdatabase geconfigureerd in ISE.

Gebruikte componenten

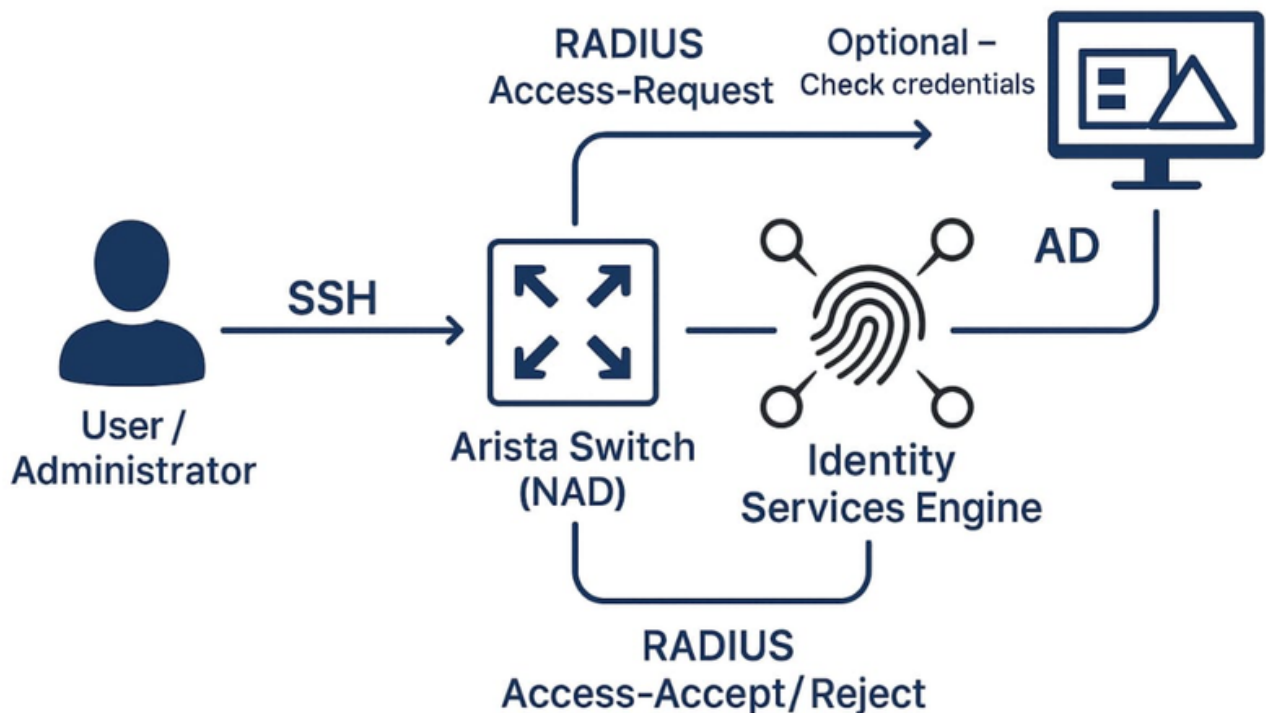
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Arista switch Software image versie: 4.33.2F
- Cisco Identity Services Engine (ISE) versie 3.3 Patch 4

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.

Netwerkdigram

RADIUS Device Authentication



Hier is een netwerkdigram dat op RADIUS gebaseerde apparaatverificatie illustreert voor een Arista-switch met Cisco ISE, met Active Directory (AD) als optionele verificatiebron.

Het diagram omvat:

- Arista Switch (fungeert als het netwerktoegangsapparaat, NAD)
- Cisco ISE (als RADIUS-server)
- Active Directory (AD) [Optioneel] (gebruikt voor identiteitsverificatie)
- Gebruiker/beheerder (die inlogt via SSH)

Configureren

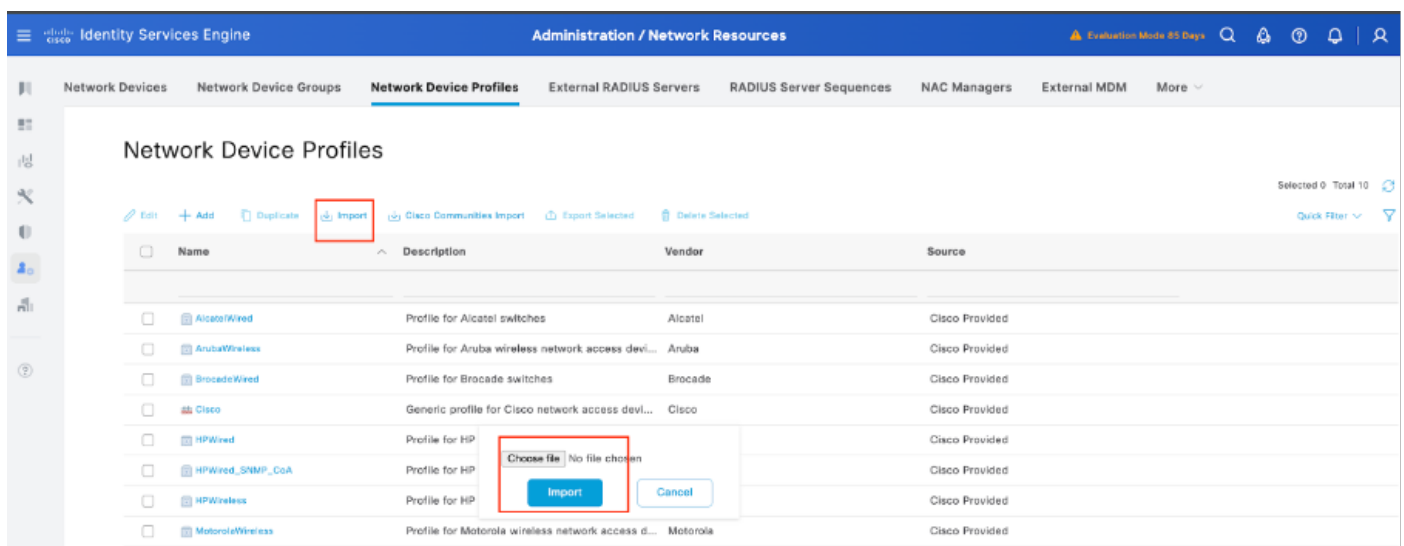
Cisco ISE configureren

Stap 1. Het Arista Network Device Profile voor Cisco ISE verkrijgen

De Cisco Community heeft een speciaal NAD-profiel gedeeld voor Arista-apparaten. Dit profiel, samen met de benodigde woordenboekbestanden, is te vinden in het artikel [Arista CloudVision WiFi Dictionary en NAD Profile for ISE Integration](#). Het downloaden en importeren van dit profiel in uw ISE-installatie vergemakkelijkt een soepelere integratie

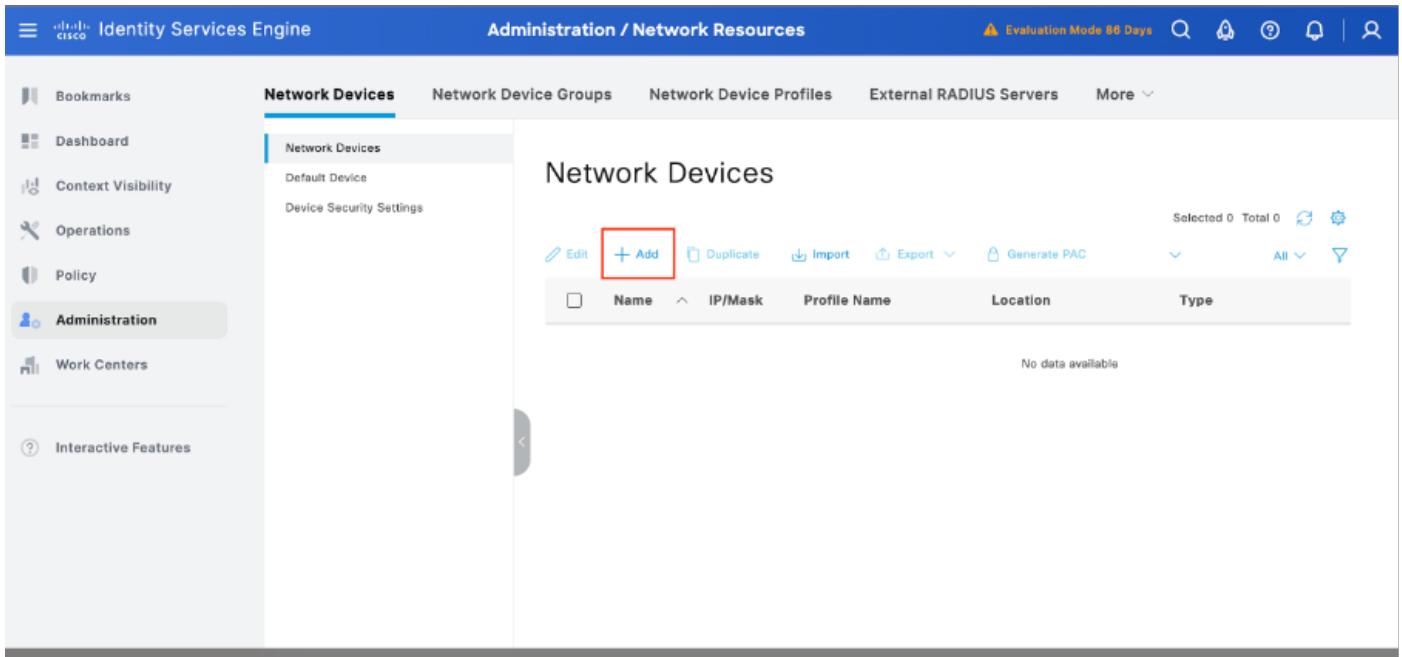
Dit zijn de stappen om het Arista NAD-profiel te importeren in Cisco ISE:

1. Download het profiel:
 - Ontvang het Arista NAD profiel via de bovenstaande Cisco Community link [Cisco Community](#).
2. Toegang tot Cisco ISE:
 - Meld u aan bij uw Cisco ISE-beheerconsole
3. Het NAD-profiel importeren:
 - Navigeer naar Beheer > Netwerkbronnen > Netwerkkapparaatprofielen
 - Klik op de knop Importeren
 - Upload het gedownloade Arista NAD profiel bestand.



Stap 2. Arista-Switch toevoegen als netwerkapparaat

1. Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten > +Toevoegen.



2. Klik op Toevoegen en voer de volgende gegevens in:

1. Naam: Arista-Switch
2. IP-adres: <Switch-IP>
3. Type apparaat: Andere bekabelde apparaten kiezen
4. Netwerkapparaatprofiel: selecteer AirstaCloudVisionWiFi.
5. RADIUS-verificatie-instellingen:
 1. RADIUS-verificatie inschakelen
 2. Voer het gedeelde geheim in (dit moet overeenkomen met de configuratie van de switch).

3. Klik op Opslaan.

Identity Services Engine Administration / Network Resources Evaluation Mode 85 Days

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

Network Devices List > Arista_switch

Network Devices

Name Arista_switch

Description Arista_switch for device login

IP Address IP / 32

Device Profile AristaCloudVisionWiFi

Model Name

Software Version 4-33-2F

Network Device Group

Location All Locations [Set To Default](#)

IPSEC No [Set To Default](#)

Device Type All Device Types [Set To Default](#)

☒ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret ***** [Show](#)

Stap 3. Het nieuwe apparaat valideren wordt weergegeven onder Netwerkkaparameters

Identity Services Engine Administration / Network Resources Evaluation Mode 85 Days

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

Network Devices

Selected 0 Total 1

[Edit](#) [+ Add](#) [Duplicate](#) [Import](#) [Export](#) [Generate PAC](#) [Delete](#)

Name	IP/Mask	Profile Name	Location	Type	Description
☐ Arista_switch	<u>IP</u>	<u>AristaCloudVisionWiFi</u>	All Locations	All Device Types	Arista_switch for device login

Stap 4. De vereiste groepen voor gebruikersidentiteit maken

Navigeer naar Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen > + Toevoegen:

The screenshot shows the Cisco Identity Services Engine Administration / Identity Management interface. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is titled 'User Identity Groups' and displays a list of groups. The 'Add' button is highlighted with a red box.

Name	Description
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
Arista_switch_Admin	Arista switch admin user login testing with golden version
Employee	Default Employee User Group
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
GuestType_Contractor (default)	Identity group mirroring the guest type
GuestType_Daily (default)	Identity group mirroring the guest type
GuestType_Self registered guest	Identity group mirroring the guest type
GuestType_SocialLogin (default)	Identity group mirroring the guest type
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Stap 5. Stel een naam in voor de groep Gebruikersidentiteit beheerder

Klik op Indienen om de configuratie op te slaan:

The screenshot shows the Cisco Identity Services Engine Administration / Identity Management interface. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is titled 'Arista_switch_Admin' and displays the configuration for the 'Arista_switch_Admin' group. The 'Save' button is highlighted.

Identity Group

* Name: Arista_switch_Admin

Description: Arista switch admin user login testing with golden version

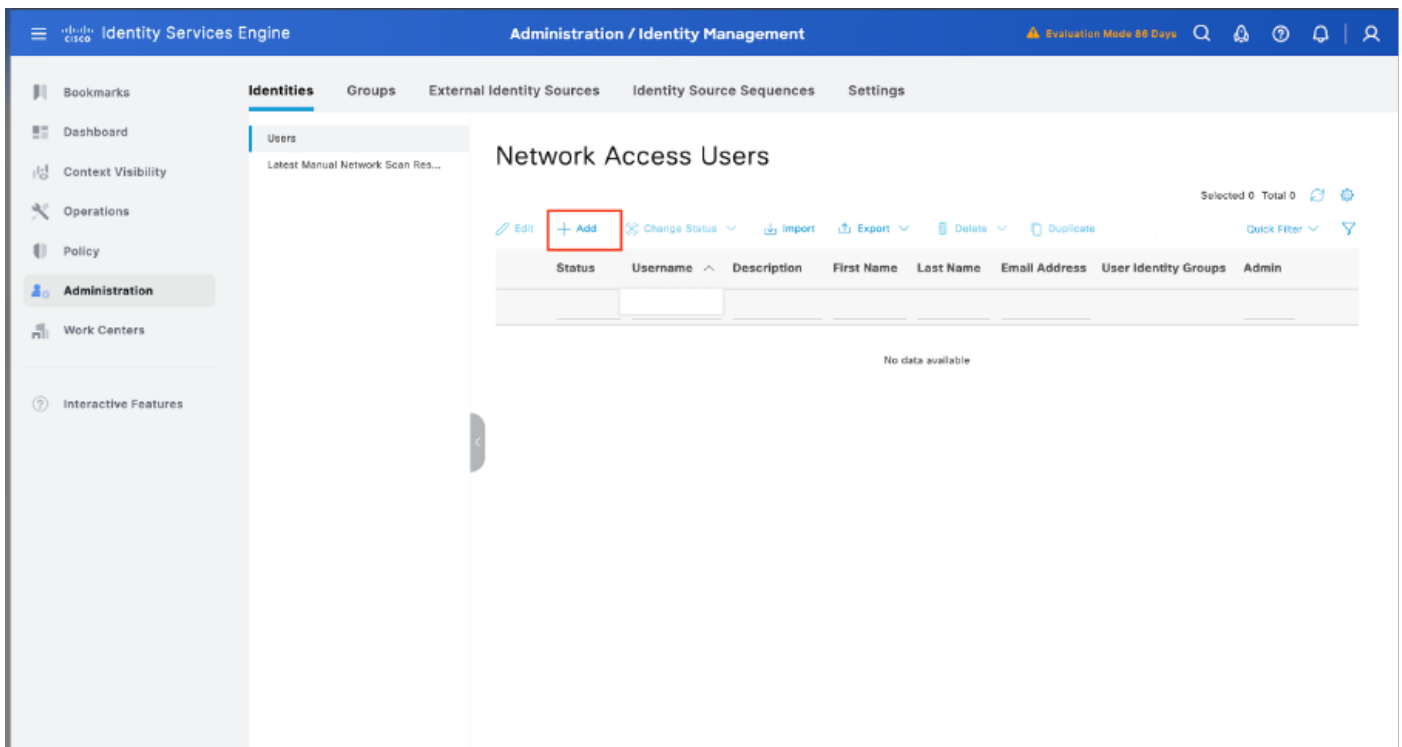
Member Users

Users: diviya (Selected 0 Total 1)

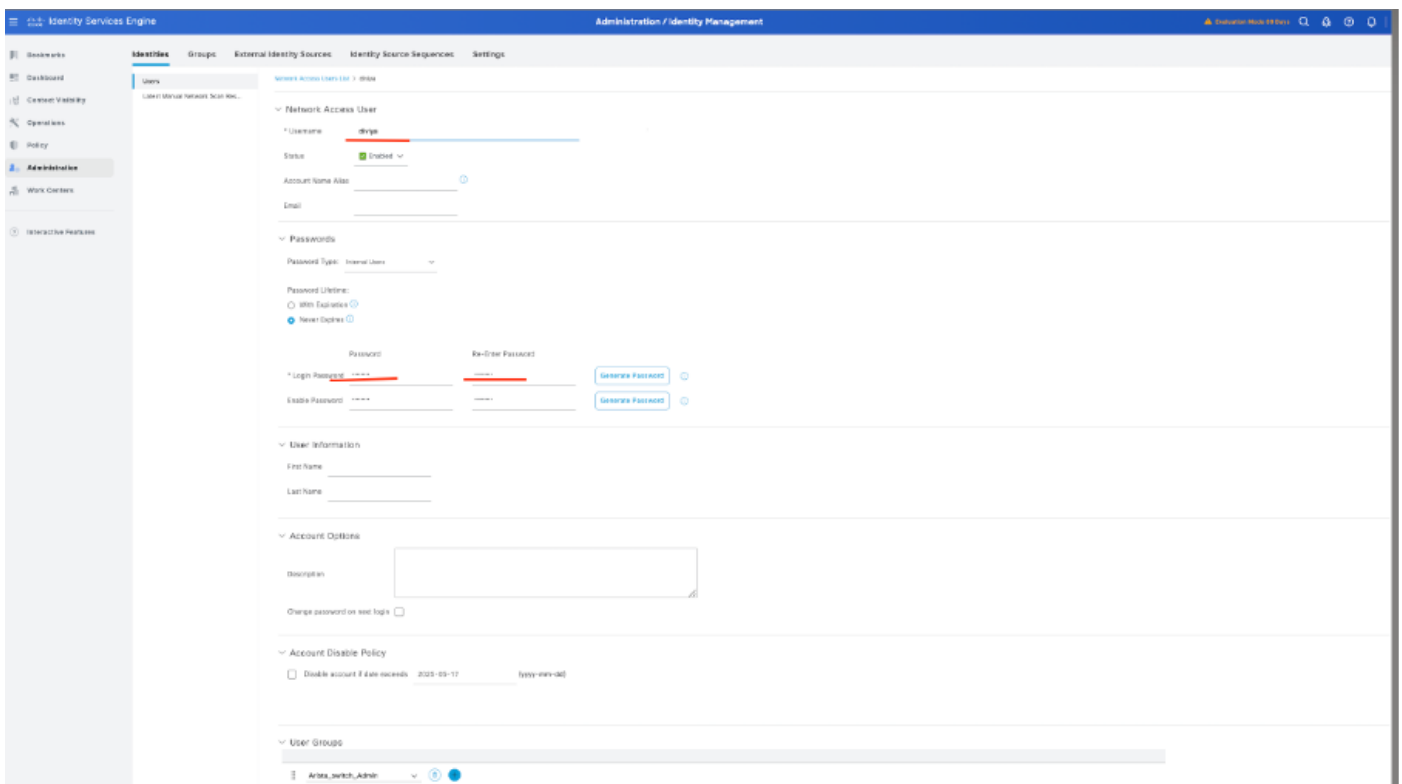
Status	Email	Username	First Name	Last Name
Enabled		diviya		

Stap 6. Maak de lokale gebruikers aan en voeg ze toe aan hun correspondentengroep

Navigeer naar Beheer > Identiteitsbeheer > Identiteiten > + Toevoegen:



6.1. Voeg de gebruiker met beheerdersrechten toe. Stel een naam, wachtwoord in en wijs deze toe aan Arista_switch_Admin, scroll omlaag en klik op Indienen om de wijzigingen op te slaan.



Stap 7. Maak het autorisatieprofiel voor de beheerdersgebruiker

Navigeer naar Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen > +Toevoegen.

Definieer een naam voor het autorisatieprofiel, laat het toegangstype ACCESS_ACCEPT staan en

voeg cisco-av-pair=shell:roles="admin" toe onder Geavanceerde attributeninstellingen en klik Indienen.

Identity Services Engine Policy / Policy Elements

Authorization Profiles > Arista_switch_Admin

Authorization Profile

* Name: Arista_switch_Admin

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: AristaCloudMgmtWEE

Common Tasks

ACL

Security Group

Advanced Attributes Settings

Cisco:cisco-av-pair * shell:roles="admin"

Attributes Details

Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:roles="admin"

Stap 8. Maak een beleidsset die overeenkomt met het IP-adres van Arista Switch

Dit om te voorkomen dat andere apparaten toegang verlenen aan de gebruikers.

Navigeer naar Beleid > Beleidssets > Pictogramteken toevoegen in de linkerbovenhoek.

Policy Sets

Status Policy Set Name Description Conditions

Default Default policy set

Default Network Access

Reset Save

8.1 Een nieuwe regel wordt bovenaan uw Beleidssets geplaatst. Klik op het pictogram Toevoegen om een nieuwe voorwaarde te configureren.

Policy Sets

Status Policy Set Name Description Conditions

New Policy Set 1

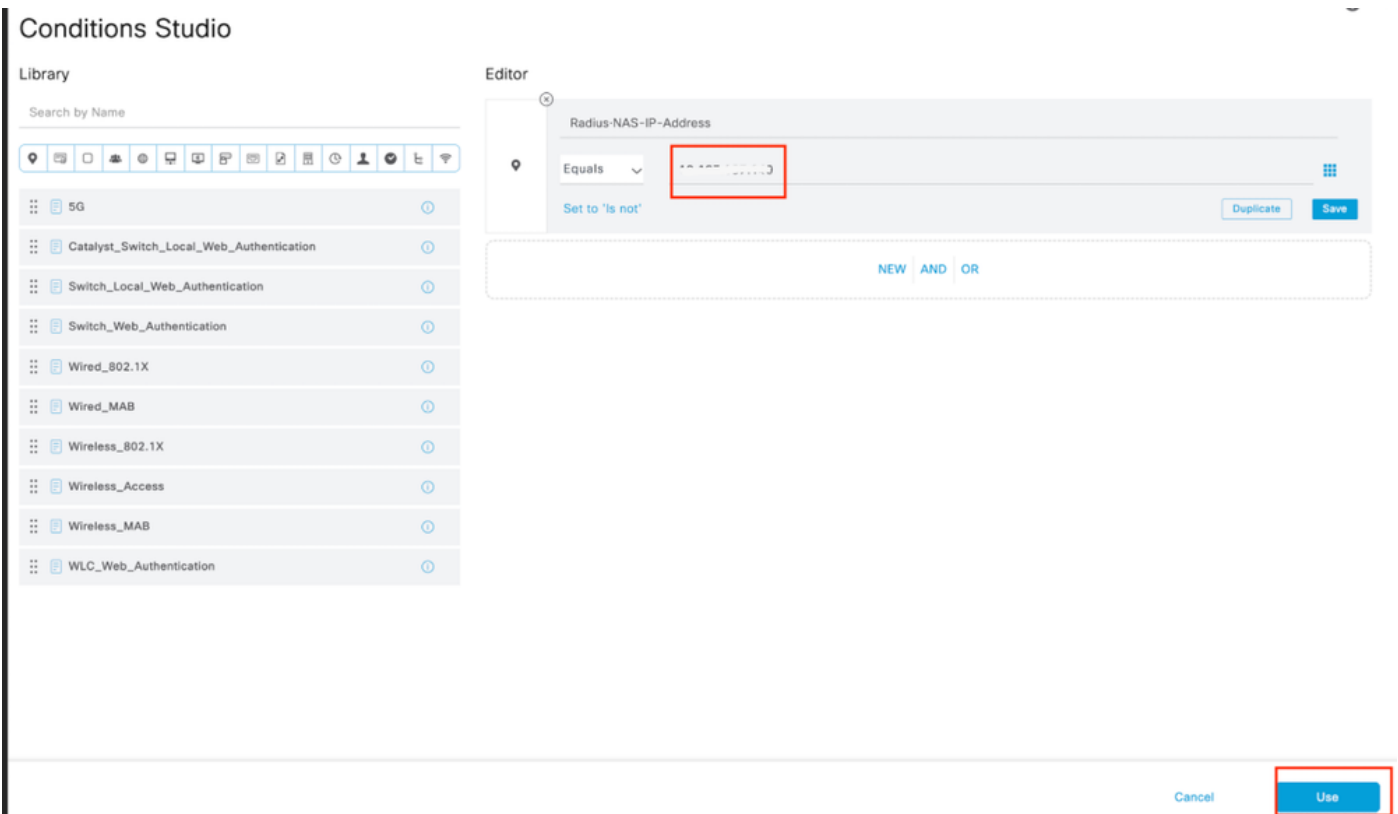
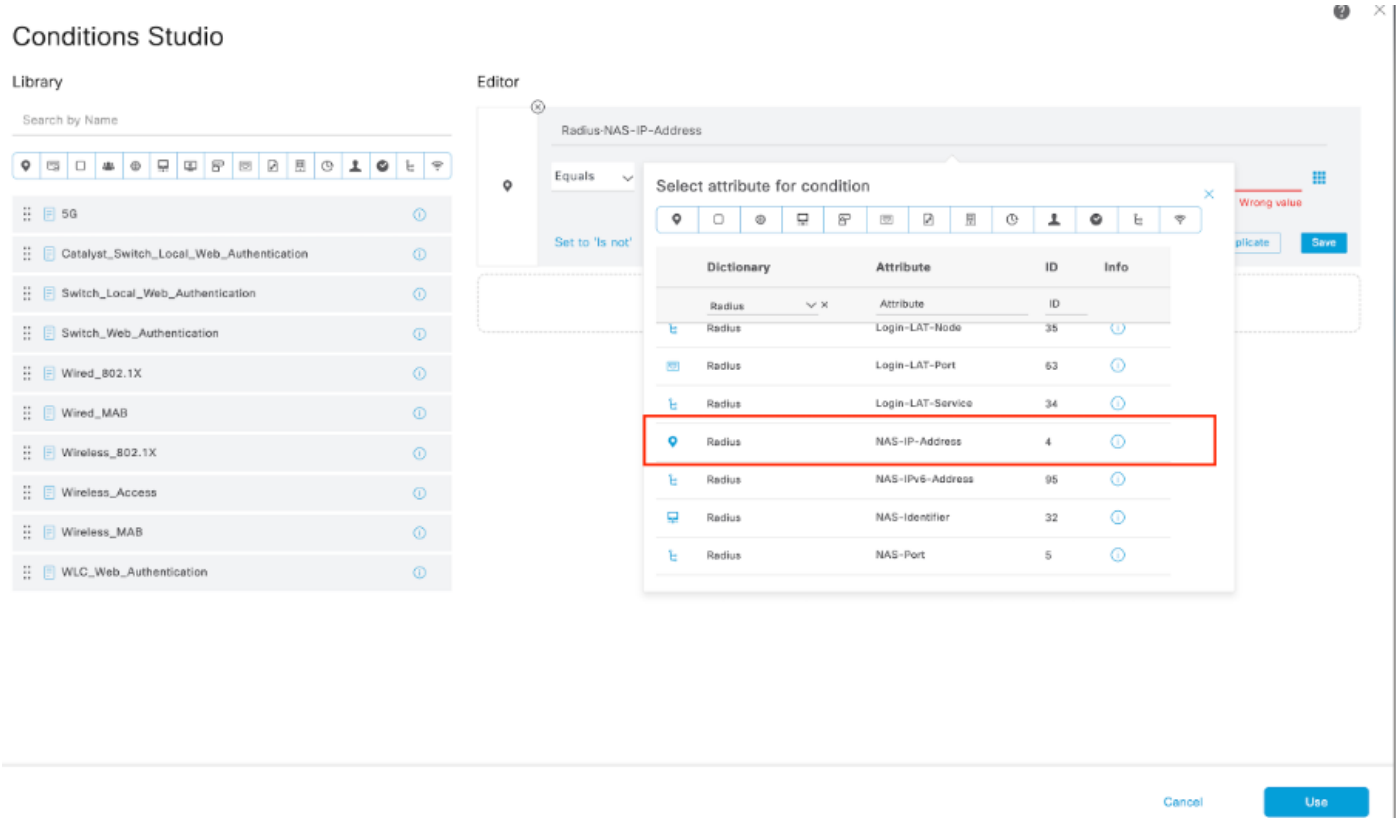
Default Default policy set

Default Network Access

Reset Save

8.2 Voeg een topvoorwaarde toe voor het kenmerk RADIUS NAS-IP-Address dat overeenkomt

met het IP-adres van Arista switch en klik vervolgens op Gebruiken.



8.3 Klik na voltooiing op Opslaan:

Identity Services Engine

Policy / Policy Sets

Evaluation Mode 88 Days

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Features

Policy Sets

Reset

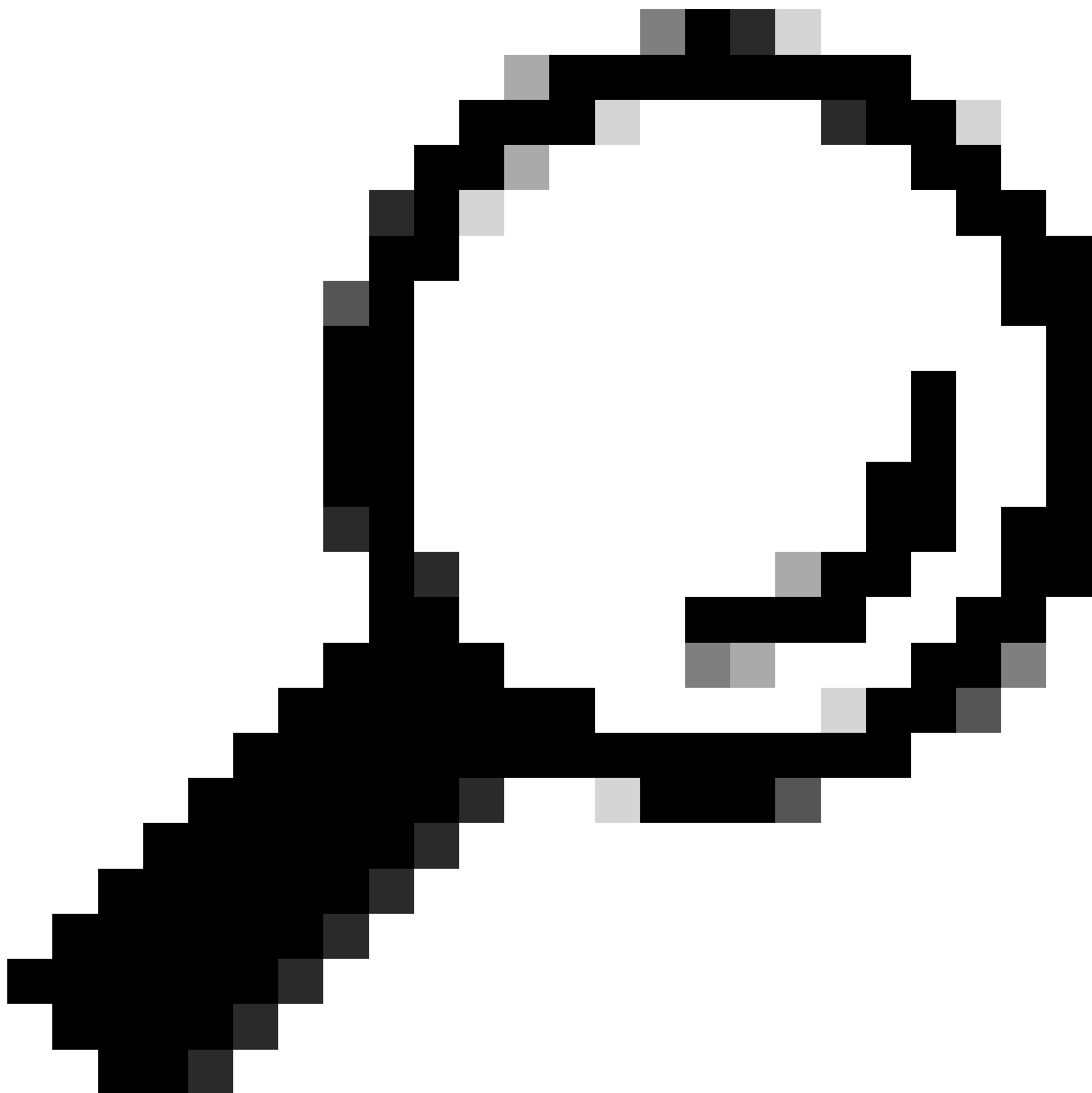
Reset Policyset Hitcounts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Arista_switch_radius login		Radius NAS-IP-Address EQUALS	Default Network Access	26		
✓	Wired		DEVICE-Device Type EQUALS All Device Types	Default Network Access	3		
✓	Default	Default policy set		Default Network Access	0		

Reset

Save



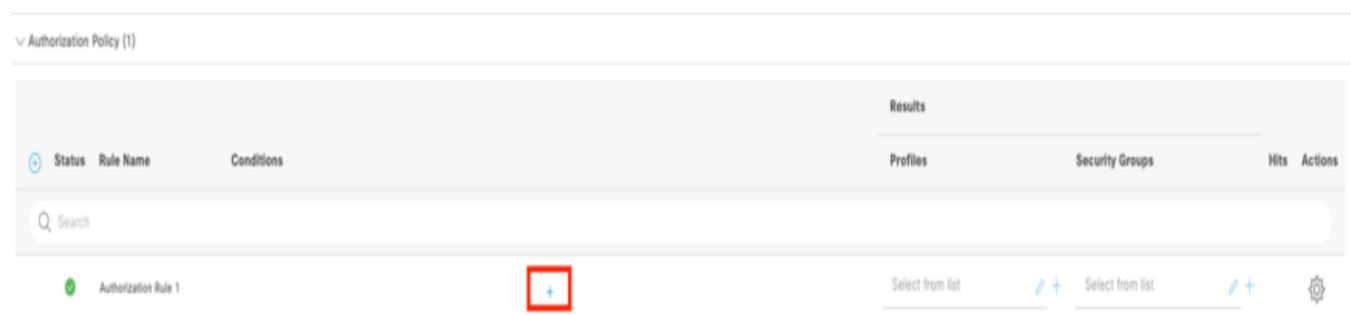
Tip: voor deze oefening hebben we de lijst met standaardprotocollen voor netwerktoegang toegestaan. U kunt een nieuwe lijst maken en deze naar behoefte verfijnen.

Stap 9. Bekijk de nieuwe beleidsset

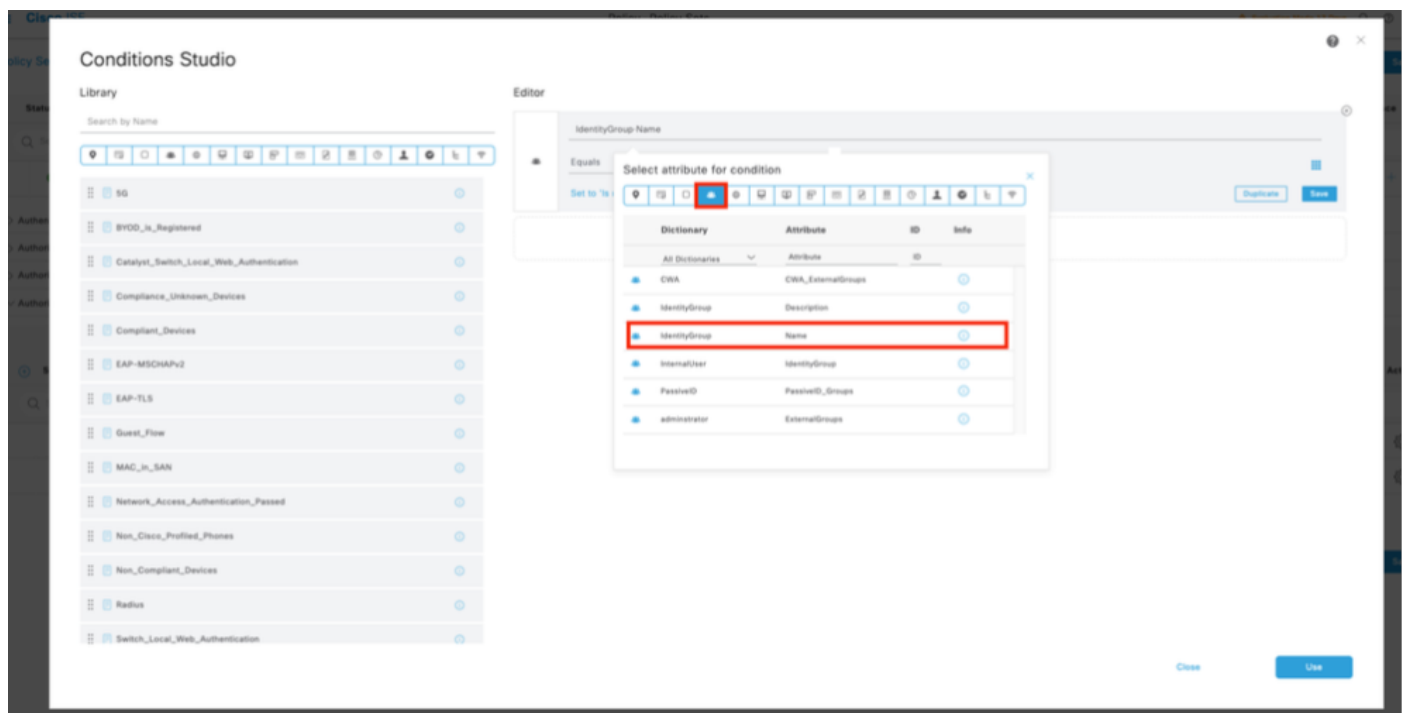
Klik op het pictogram > dat aan het einde van de rij wordt geplaatst:



9.1 Vouw het menu Autorisatiebeleid uit en klik op (+) om een nieuwe voorwaarde toe te voegen.



9.2 Stel de voorwaarden in die overeenkomen met de Identiteitsgroep woordenboek met Naam attribuut is gelijk aan Gebruikersidentiteitsgroepen: Arista_switch_Admin (de groepsnaam die is gemaakt in stap 7) en klik op Gebruik.



Conditions Studio

Library

Search by Name

5G	
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_Profiling_Phones	
Non-Compliant_Devices	
Switch_Local_Web_Authentication	
Switch_Web_Authentication	

Editor

IdentityGroup-Name

Equals User Identity Groups:Arista_switch_Admin

Set to 'Is not'

Duplicate Save

NEW AND OR

Cancel

Use

9.3 De nieuwe voorwaarde valideren die is geconfigureerd in het autorisatiebeleid, en vervolgens een gebruikersprofiel toevoegen onder Profielen:

Authorization Policy(2)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Search						
✓	Arista_Radius_login	IdentityGroup-Name EQUALS User Identity Groups:Arista_switch_Admin	Arista_switch_Admin	Select from list	9	⚙️
✓	Default		DenyAccess	Select from list	0	⚙️

Reset Save

Arista-Switch configureren

Stap 1. RADIUS-verificatie inschakelen

Meld u aan bij de Arista-switch en voer de configuratiemodus in:

configureren

Ja!

```
radius-server host <ISE-IP>-sleutel <RADIUS-SECRET>
```

RADIUS-SERVER TIME-OUT 5

RADIUS-SERVER RETRANSMISSIE 3

RADIUS-SERVER DEADTIME 30

Ja!

aaa-groepsserverradius ISE

server <ISE-IP>

Ja!

standaard aanmeldingsgroep voor aaa-verificatie ISE lokaal

aaa authorization exec default group ISE lokaal

aaa accounting exec default start-stop groep ISE

aaa accounting commando's 15 standaard start-stop groep ISE

standaard start-stop groep ISE van het aaa-boekhoudsysteem

Ja!

einde

Stap 2. Configuratie opslaan

Instellingen voor opnieuw opstarten behouden:

schrijfgeheugen

of

Opstartconfiguratie voor kopiëren-uitvoeren

Verifiëren

ISE-beoordeling

1. Probeer in te loggen op de Arista-Switch met de nieuwe Radius-referenties:

1.1 Navigeer naar Bewerkingen > Straal > Live logs.

1.2 De weergegeven informatie geeft aan of een gebruiker zich succesvol heeft aangemeld.

Identity Services Engine Operations / RADIUS

Evaluation Mode 60 Days

Bookmarks Dashboard Context Visibility **Operations** Policy Administration Work Centers Interactive Features

Live Logs Live Sessions

Click here to do visibility setup Do not show this again.

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 5

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization...	Authoriz...
Mar 18, 2025 07:08:22.0...			4	diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 07:08:21.9...			1	diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 07:08:21.9...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 07:08:21.9...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...

2. Controleer de details van de sessie voor de mislukte status:

Identity Services Engine Operations / RADIUS

Evaluation Mode 60 Days

Bookmarks Dashboard Context Visibility **Operations** Policy Administration Work Centers Interactive Features

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 6

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To

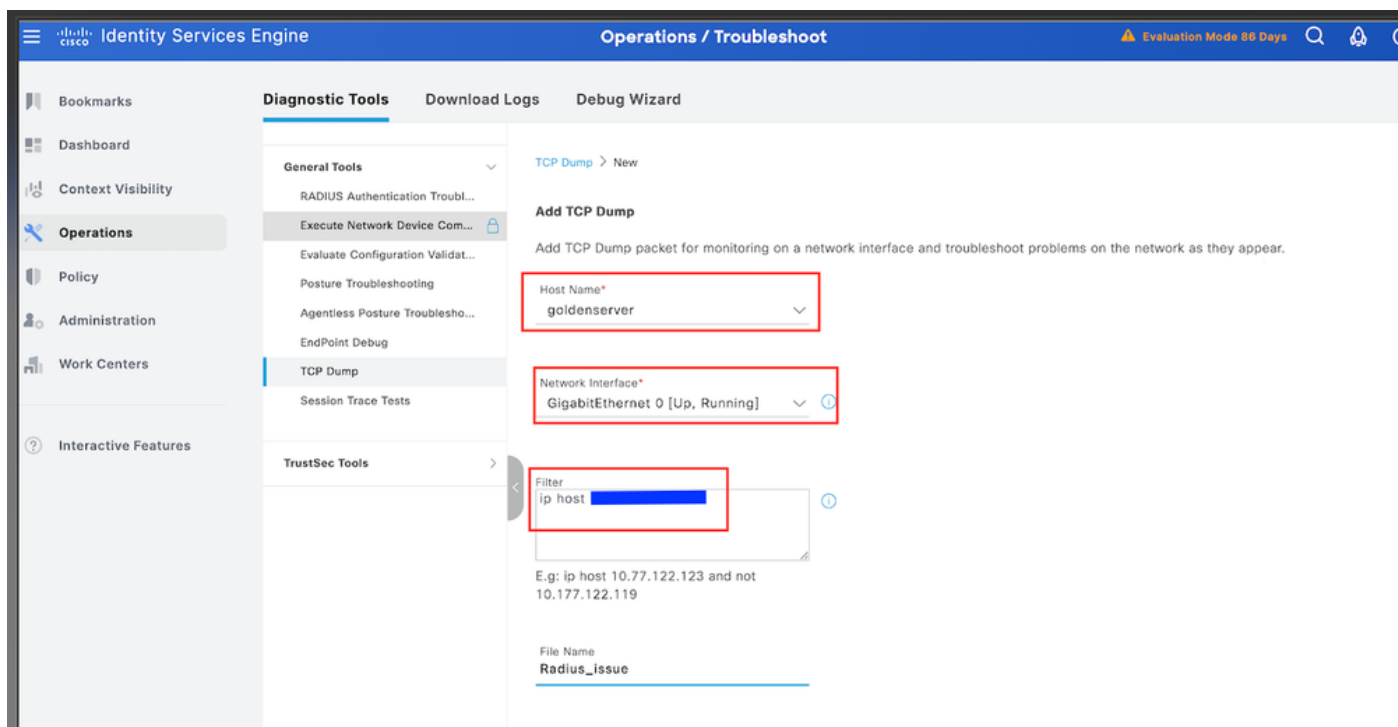
Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization...	Authoriz...
Mar 18, 2025 05:57:12.4...	Auth Failed			diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 05:57:02.5...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 05:56:16.3...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...
Mar 18, 2025 05:56:08.0...				diviya			Arista_switch_rad...	Arista_switch_f...	Arista_swi...

3. Voor verzoeken die niet in Radius Live-logs worden weergegeven, controleert u of het UDP-verzoek de ISE-node bereikt via een pakketopname.

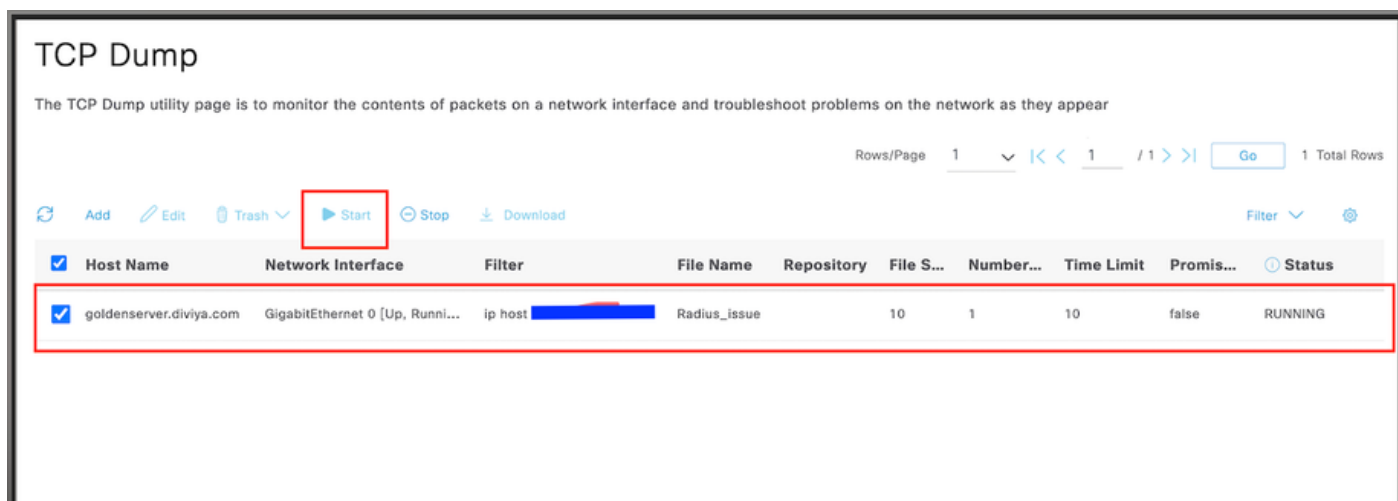
3.1. Navigeer naar Bewerkingen > Problemen oplossen > Diagnostische hulpmiddelen > TCP-dump.

3.2. Voeg een nieuwe opname toe en download het bestand naar uw lokale systeem om te controleren of de UDP-pakketten aankomen op de ISE-node.

3.3. Vul de gevraagde informatie in, blader omlaag en klik op Opslaan.



3.4. Selecteer en start de opname.



3.5. Probeer tijdens het uitvoeren van de ISE-opname in te loggen op de Arista-Switch.

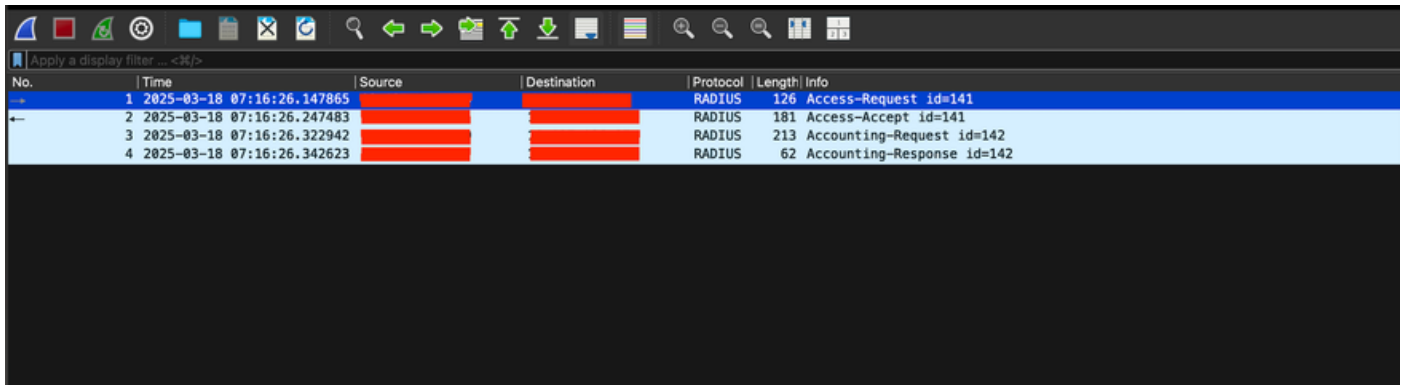
3.6. Stop de TCP-dump in ISE en download het bestand naar een lokaal systeem.

3.7. Verkeersoutput beoordelen.

Verwachte output:

Pakket nr. 1. Verzoek van de Arista-Switch aan de ISE-server via poort 1812 (RADIUS).

Pakket nr. 2. Reactie van de ISE-server waarbij het oorspronkelijke verzoek wordt geaccepteerd.



No.	Time	Source	Destination	Protocol	Length	Info
1	2025-03-18 07:16:26.147865			RADIUS	126	Access-Request id=141
2	2025-03-18 07:16:26.247483			RADIUS	181	Access-Accept id=141
3	2025-03-18 07:16:26.322942			RADIUS	213	Accounting-Request id=142
4	2025-03-18 07:16:26.342623			RADIUS	62	Accounting-Response id=142

Probleemoplossing

Scenario 1: "5405 RADIUS Request verwijderd"

Probleem

In dit scenario wordt het probleem opgelost met de fout "5405 RADIUS Request dropped" met de reden "11007 Kan netwerkkapparaat of AAA-client niet vinden" in Cisco ISE wanneer een netwerkkapparaat (zoals een Arista-switch) probeert te verifiëren.

Mogelijke oorzaken

- De Cisco Identity Services Engine (ISE) kan de Arista-switch niet identificeren omdat het IP-adres niet wordt vermeld bij bekende netwerkkapparaten.
- Het RADIUS-verzoek is afkomstig van een IP-adres dat ISE niet herkent als een geldig netwerkkapparaat of AAA-client.
- De configuratie van de switch en de ISE kan niet overeenkomen (zoals een onjuist IP-adres of een gedeeld geheim).

Oplossing

- Voeg de switch toe aan de Cisco ISE-lijst van netwerkkapparaten met het juiste IP-adres.
- Controleer of het IP-adres en het gedeelde geheim dat in ISE is geconfigureerd, exact overeenkomen met wat op de switch is ingesteld.
- Na correctie moet het RADIUS-verzoek naar behoren worden herkend en verwerkt.

Scenario 2: Arista Switch faalt bij failover naar back-up van ISE PSN

Probleem

Een Arista-switch is geconfigureerd om Cisco ISE te gebruiken voor RADIUS-verificatie. Wanneer de primaire ISE Policy Service Node (PSN) niet beschikbaar is, wordt de switch niet automatisch

overgezet naar een back-up-PSN. Hierdoor worden verificatielogs alleen weergegeven vanaf de primaire ISE-PSN en zijn er geen logboeken van de secundaire/back-up-PSN wanneer de primaire PSN is uitgeschakeld.

Mogelijke oorzaken

- De RADIUS-serverconfiguratie van de Arista-switch verwijst alleen naar de primaire ISE-node, zodat back-upservers niet worden gebruikt.
- De RADIUS-serverprioriteit is niet goed ingesteld of de back-up ISE IP ontbreekt in de configuratie.
- De instellingen voor time-out en opnieuw verzenden op de switch zijn te laag ingesteld, waardoor terugvallen naar de back-up-PSN wordt voorkomen.
- De switch gebruikt een FQDN voor de PSN, maar de DNS-resolutie retourneert niet alle A-records, waardoor alleen de hoofdserver wordt gecontacteerd.

Oplossing

- Zorg ervoor dat meerdere ISE PSN-IP's worden ingevoerd in de RADIUS-servergroepconfiguratie van de switch. Hierdoor kan de switch de back-up ISE PSN gebruiken als de primaire server niet bereikbaar is.

Voorbeeldconfiguratie:

```
radius-server host <ISE1-IP>-sleutel <secret>
```

```
radius-server host <ISE2-IP>-sleutel <secret>
```

- Controleer of de RADIUS-serverprioriteit, time-out en waarden voor opnieuw verzenden correct zijn geconfigureerd voor een betrouwbare failover.
- Als u FQDN's gebruikt, controleert u de DNS-instellingen en -resolutie om ervoor te zorgen dat alle IP-adressen van PSN worden geretourneerd en door de switch worden gebruikt.

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.