

TACACS+-verificatie configureren op Arista-Switch met ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Configuraties](#)

[TACACS+-configuratie op ISE](#)

[Arista-Switch configureren](#)

[Stap 1. TACACS+-verificatie inschakelen](#)

[Stap 2. Sla de configuratie op](#)

[Verifiëren](#)

[ISE-beoordeling](#)

[Probleemoplossing](#)

[Probleem 1](#)

[Mogelijke oorzaken](#)

[Probleem 2](#)

[Mogelijke oorzaken](#)

[Oplossing](#)

Inleiding

In dit document wordt beschreven hoe u Cisco ISE TACACS+ kunt integreren met een Arista-switch voor gecentraliseerde AAA van beheerderstoegang.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE en TACACS+ protocol.
- Arista switches

Gebruikte componenten

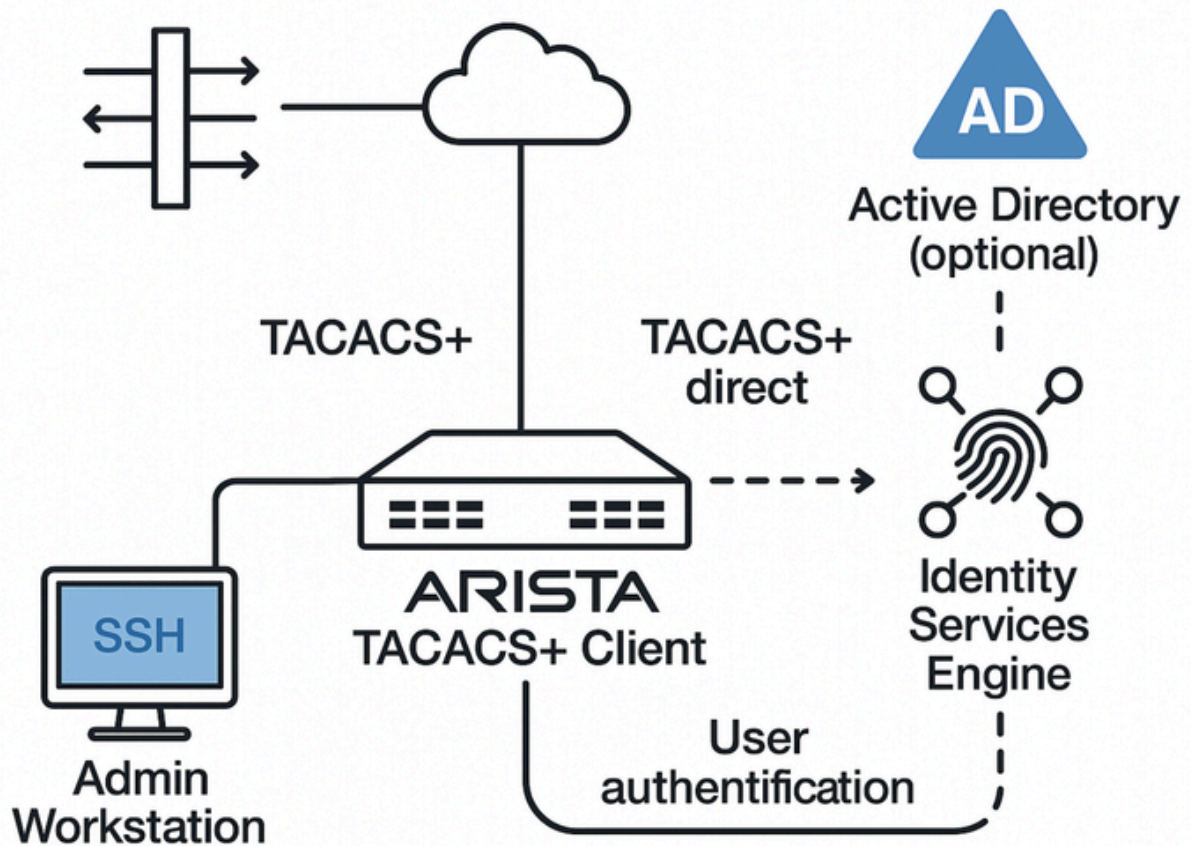
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- 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

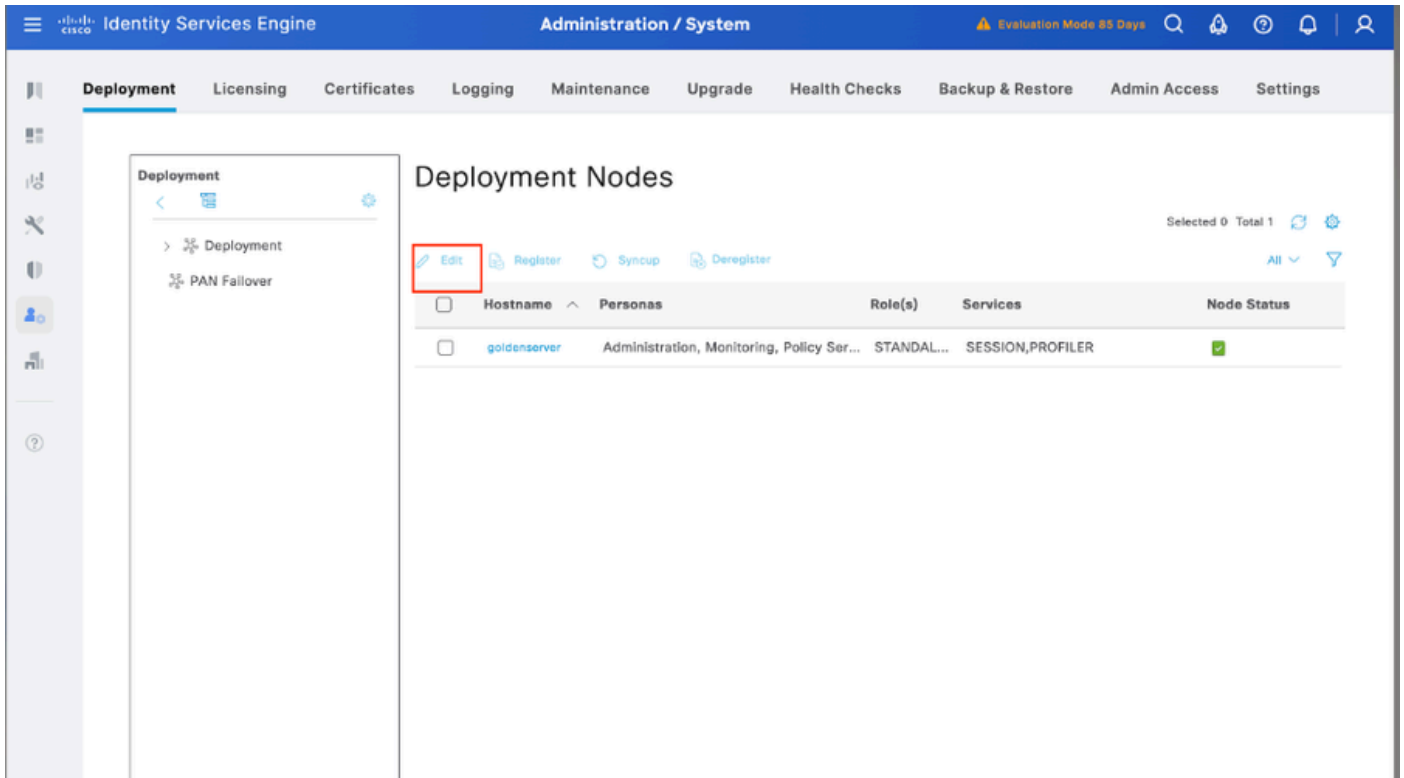


Configuraties

TACACS+-configuratie op ISE

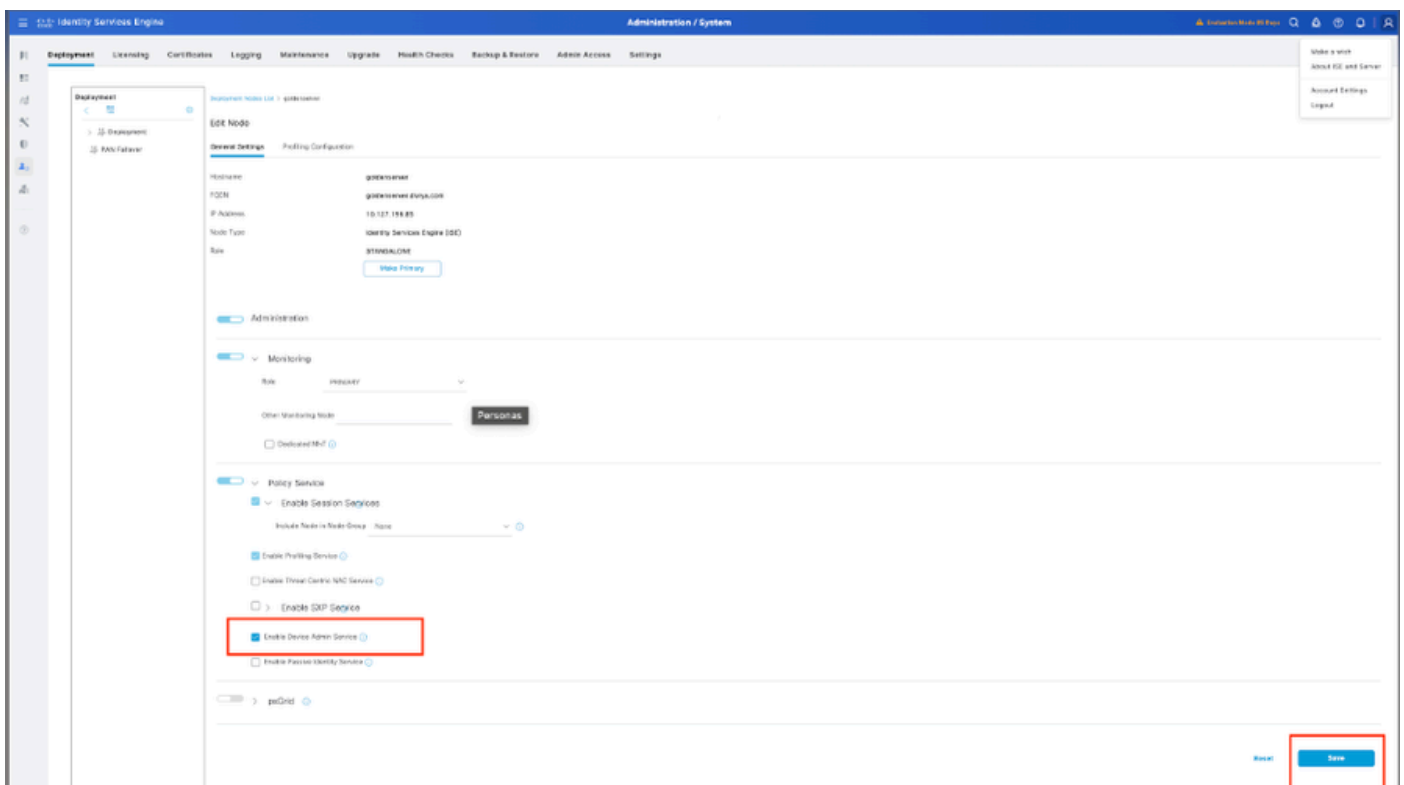
Stap 1. De eerste stap is om na te gaan of Cisco ISE over de nodige mogelijkheden beschikt om de TACACS+-verificatie af te handelen. Bevestig hiervoor dat de functie Apparaatbeheerservice is ingeschakeld in de gewenste beleidsserviceknooppunt (PSN).

Navigeer naar Beheer > Systeem > Implementatie, selecteer de juiste node waar ISE TACACS+-verificatie verwerkt en klik op Bewerken om de configuratie te bekijken.



Stap 2. Blader omlaag om de functie Apparaatbeheerservice te vinden. Houd er rekening mee dat als u deze functie inschakelt, de persona van de Beleidsservice actief moet zijn op de node, samen met de beschikbare TACACS+-licenties in de implementatie.

Schakel het selectievakje in om de functie in te schakelen en sla de configuratie vervolgens op.

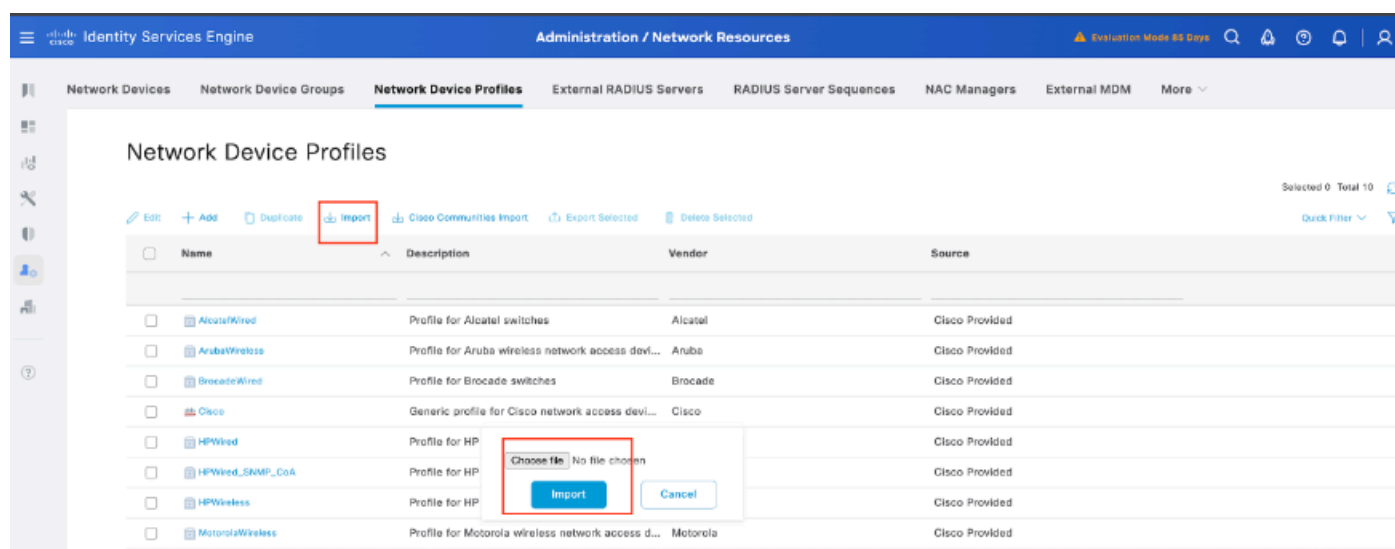


Stap 3. Het Arista Network Device Profile voor Cisco ISE verkrijgen.

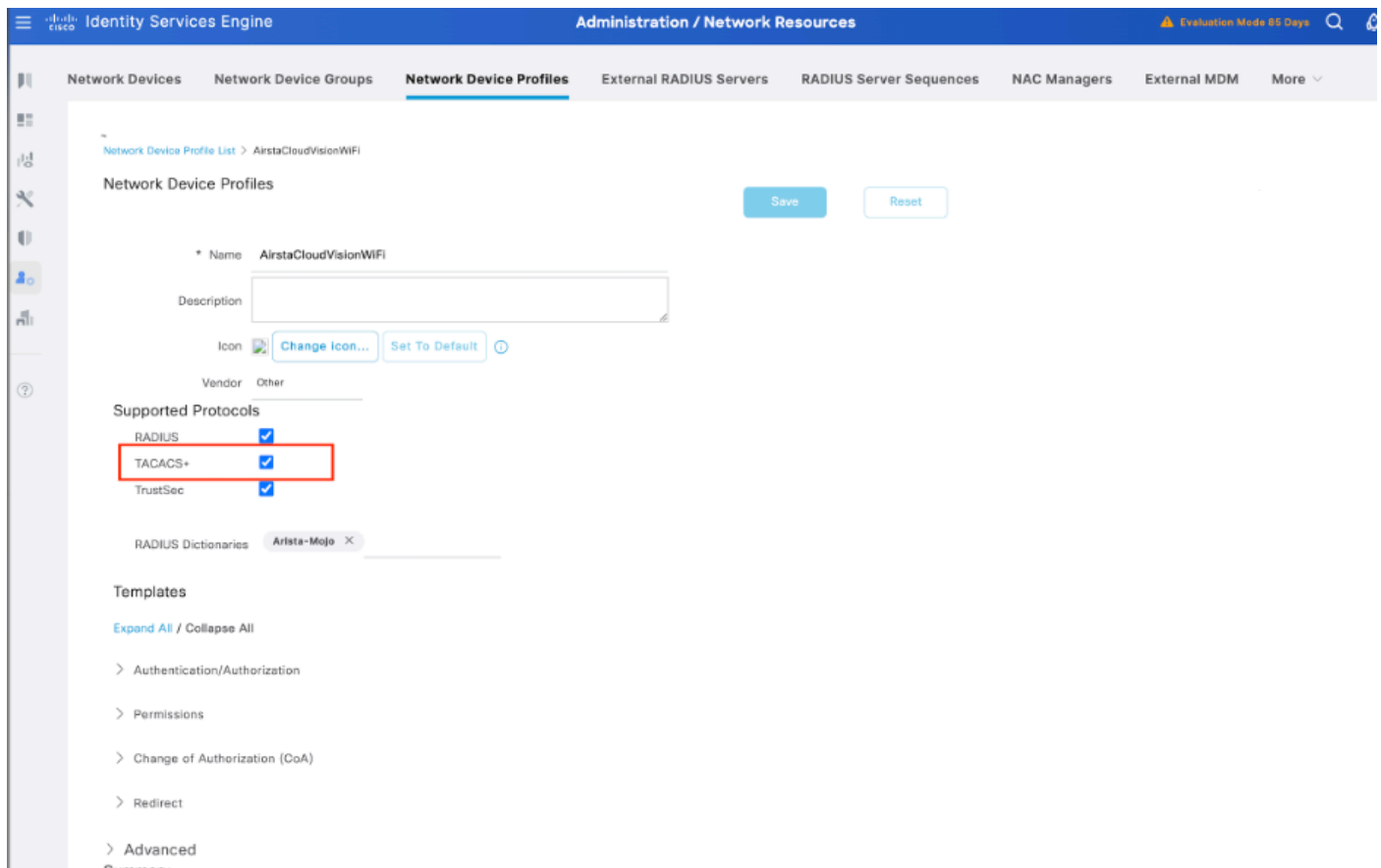
De Cisco Community heeft een speciaal NAD-profiel gedeeld voor Arista-apparaten. Dit profiel, samen met de benodigde woordenboekbestanden, is te vinden in het artikel [Arista CloudVision WiFi Dictionary en NAD Profile for ISE Integration](#). Het downloaden en importeren van dit profiel in uw ISE-installatie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

Stappen voor het importeren van het Arista NAD-profiel 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 > Netwerkapparaatprofielen
 - Klik op de knop Importeren
 - Upload het gedownloade Arista NAD profiel bestand.

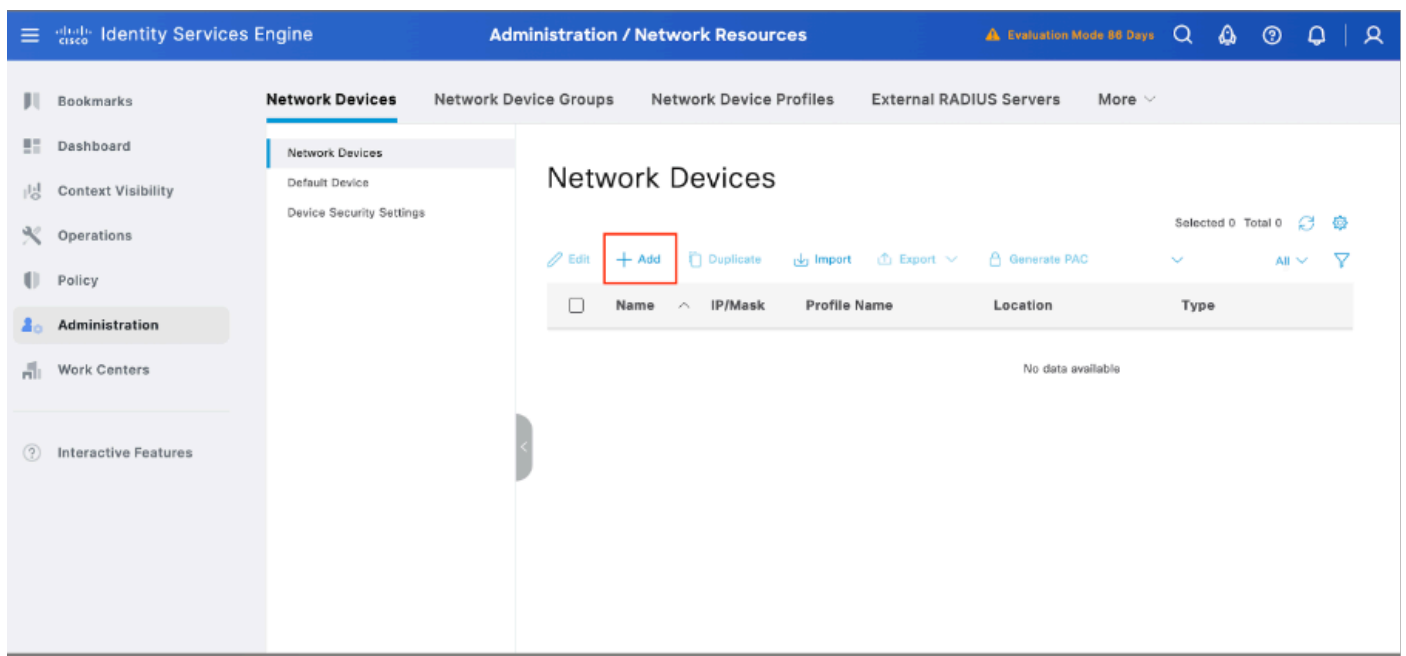


Nadat het uploaden is voltooid, navigeert u naar de optie Bewerken en schakelt u TACACS+ in als een ondersteund protocol.



Stap 2: Arista Switch toevoegen als netwerkapparaat.

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



2. Klik op Toevoegen en voer deze gegevens in:

- IP-adres: <Switch-IP>
- Type apparaat: Andere bekabelde apparaten kiezen
- Netwerkapparaatprofiel: selecteer AristaCloudVisionWiFi.

- RADIUS-verificatie-instellingen:
 - RADIUS-verificatie inschakelen.
 - Voer het gedeelde geheim in (dit moet overeenkomen met de configuratie van de switch).

3. Klik op Opslaan:

The screenshot shows the 'Administration / Network Resources' page in the Cisco ISE console. The 'Network Devices' tab is selected. The configuration for 'Arista_switch' is displayed. The 'Name' field is 'Arista_switch'. The 'Description' is 'Arista_switch for device login TACACS and'. The 'IP Address' is '32'. The 'Device Profile' is 'AristaCloudVisionWiFi'. The 'Model Name' is empty. The 'Software Version' is '4-33-2F'. The 'Network Device Group' is 'All Locations'. The 'IPSEC' is 'No'. The 'Device Type' is 'All Device Types'. The 'RADIUS Authentication Settings' section is expanded, showing 'Protocol' as 'RADIUS' and 'Shared Secret' as a redacted field. The 'Use Second Shared Secret' checkbox is unchecked.

Stap 3. Het nieuwe apparaat valideren wordt weergegeven onder Netwerkkaparameten:

The screenshot shows the 'Network Devices' list in the Cisco ISE console. The list contains one device, 'Arista_switch', with the following details:

Name	IP/Mask	Profile Name	Location	Type	Description
Arista_switch	32	AristaCloudVisionWiFi	All Locations	All Device Types	Arista_switch f

Stap 4. Het TACACS-profiel configureren.

Maak een TACACS-profiel, navigeer naar het menu Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen en selecteer vervolgens Toevoegen:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Device Administration'. The left sidebar contains various navigation options, with 'Work Centers' selected. The main content area is titled 'TACACS Profiles' and displays a table of profiles. The 'Add' button is highlighted with a red box.

Name	Type	Description
Arista Profile Admin	Shell	
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
TAC_PROFILE_PRIV15	Shell	
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

Voer een naam in, selecteer het selectievakje Standaardvoorrecht en stel de waarde in op 15. Selecteer bovendien Maximumvoorrecht, stel de waarde in op 15 en klik op Indienen:

The screenshot shows the 'TACACS Profile' configuration page in the Cisco Identity Services Engine (ISE). The 'Name' field is highlighted with a red box. The 'Default Privilege' and 'Maximum Privilege' fields are also highlighted with a red box.

TACACS Profile

Name: TAC_PROFILE_PRIV15

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☒ Default Privilege: 15 (Select 0 to 15)

☒ Maximum Privilege: 15 (Select 0 to 15)

☐ Access Control List: (Select 0 to 15)

☐ Auto Command: (Select true or false)

☒ Timeout: 60 Minutes (0-9999)

☒ Idle Time: 15 Minutes (0-9999)

Custom Attributes

Stap 5. Maak een Device Admin Policy Set die voor uw Arista-Switch moet worden gebruikt, navigeer naar het menu Work Centers > Device Administration > Device Admin Policy Sets, selecteer vervolgens vanuit een bestaande beleidsset het tandwielpictogram en selecteer vervolgens een nieuwe rij hierboven invoegen.

The screenshot shows the Cisco ISE Work Centers / Device Administration interface. The 'Device Admin Policy Sets' tab is selected. A table displays the following data:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Arista Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	27	[Edit] [Add] [Settings] [More]	[View]
✓	Default	Tacacs Default policy set		Default Device Admin		[Edit] [Add] [Settings] [More]	[View]

A context menu is open for the 'Arista Switch Access' row, showing options: 'Insert new row above', 'Insert new row below', 'Duplicate above', 'Duplicate below', and 'Delete'.

Stap 6. Geef deze nieuwe beleidsset een naam, voeg voorwaarden toe afhankelijk van de eigenschappen van de TACACS+-verificaties die worden uitgevoerd vanuit de Arista-switch en selecteer als Toegestane protocollen > Standaardapparaatbeheer, sla uw configuratie op.

The screenshot shows the Cisco ISE Work Centers / Device Administration interface. The 'Device Admin Policy Sets' tab is selected. The 'Arista Switch Access' row is highlighted with a red box. A dropdown menu is open for the 'Allowed Protocols' column, showing options: 'Default Device Admin' and 'Default Network Access'.

Stap 7. Selecteer in de optie > bekijken en selecteer vervolgens in het gedeelte Authenticatiebeleid de externe identiteitsbron die Cisco ISE gebruikt om de gebruikersnaam en referenties voor verificatie op de Arista-switch op te vragen. In dit voorbeeld komen de referenties overeen met interne gebruikers die zijn opgeslagen in ISE.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets → Arista Switch Access

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Arista Switch Access		DEVICE-Device Type EQUALS All Device Types	Default Device Admin	27

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users	22	Options

Stap 8. Scroll naar beneden tot de sectie Autorisatiebeleid naar standaardbeleid, selecteer het tandwielpictogram en plaats een regel hierboven.

Stap 9. Geef de nieuwe autorisatieregel een naam, voeg voorwaarden toe met betrekking tot de gebruiker die al is geverifieerd als groepslidmaatschap en voeg in de sectie Shell-profielen het TACACS-profiel toe dat u eerder hebt geconfigureerd, sla de configuratie op.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets → Arista Switch Access

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Arista Switch Access		DEVICE-Device Type EQUALS All Device Types	Default Device Admin	27

Authorization Policy(2)

Status	Rule Name	Conditions	Results		Hits	Actions
			Command Sets	Shell Profiles		
✓	Arista_Switch	InternalUser-identityGroup EQUALS User Identity Groups:Employee	PermitAllCommands	TAC_PROFILE_PRIV15	10	
✓	Default		DenyAllCommands	Deny All Shell Profile	5	

Arista-Switch configureren

Stap 1. TACACS+-verificatie inschakelen

Meld u aan bij de Arista switch en ga naar de configuratiemodus:

configureren

Ja!

```
tacacs-server host <ISE-IP> key <TACACS-SECRET>
```

Ja!

```
aaa-groepsserver tacacs+ ISE_TACACS
```

```
server <ISE-IP>
```

Ja!

standaard aanmeldingsgroep voor aaa-verificatie ISE_TACACS lokaal

```
aaa autorisatie exec default groep ISE_TACACS lokaal
```

```
aaa accounting commando's 15 standaard start-stop groep ISE_TACACS
```

Ja!

einde

Stap 2. Sla de configuratie op

Om de configuratie tijdens het opnieuw opstarten te behouden:

Schrijfgeheugen

OF

Opstartconfiguratie voor kopiëren-uitvoeren

Verifiëren

ISE-beoordeling

Stap 1. Controleer of de TACACS+-service actief is. Dit kan worden ingecheckt:

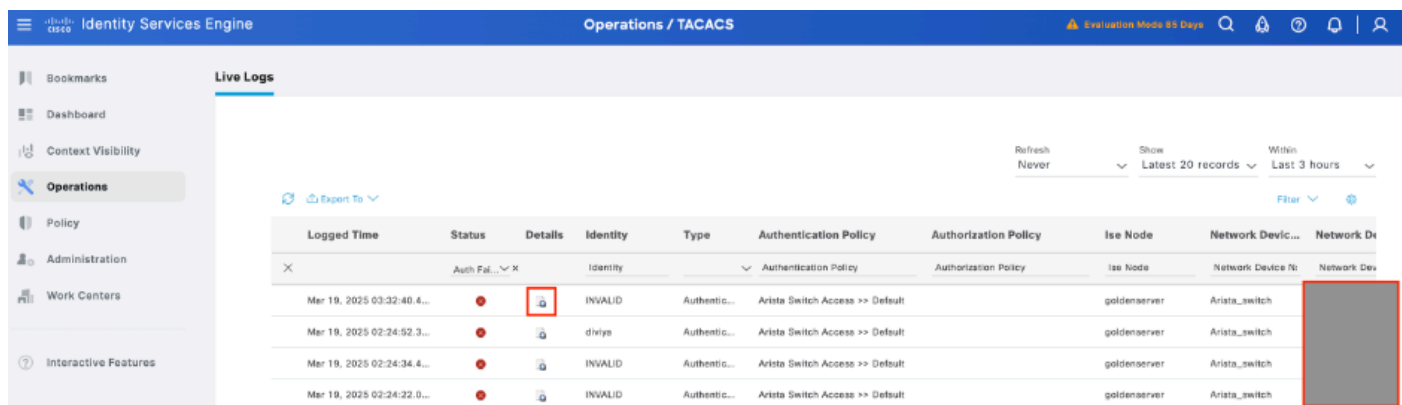
- GUI: controleer of de node is vermeld bij de service DEVICE ADMIN in > Systeem > Implementatie.
- CLI: Voer de opdracht show ports uit | neem 49 op om te bevestigen dat er verbindingen in de TCP-poort zijn die behoren tot TACACS+

```
goldenserver/admin#show ports | include 49
```

```
tcp: [REDACTED]
```

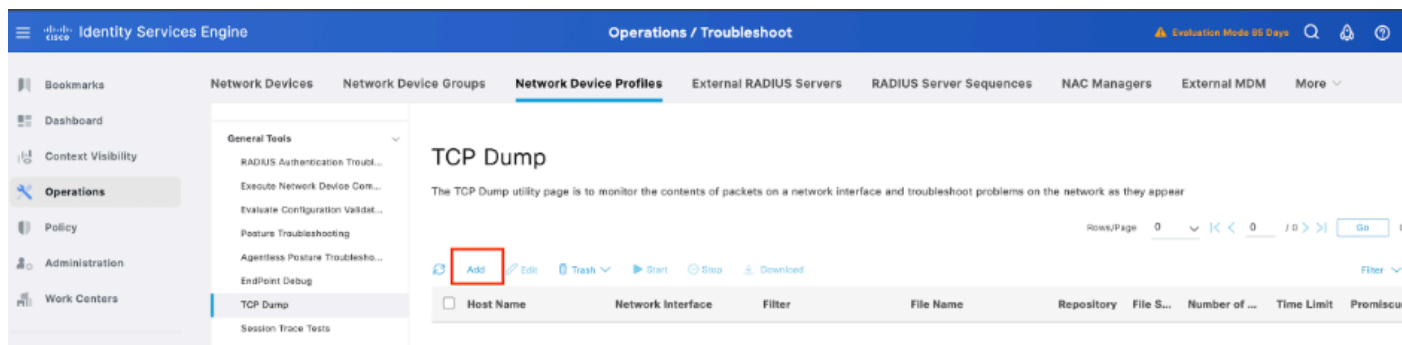
Stap 2. Bevestig of er livelogs zijn met betrekking tot TACACS+-verificatiepogingen: dit kan worden gecontroleerd in het menu Bewerkingen > TACACS > Live-logs,

Afhankelijk van de reden van de storing kunt u uw configuratie aanpassen of de oorzaak van de storing aanpakken.

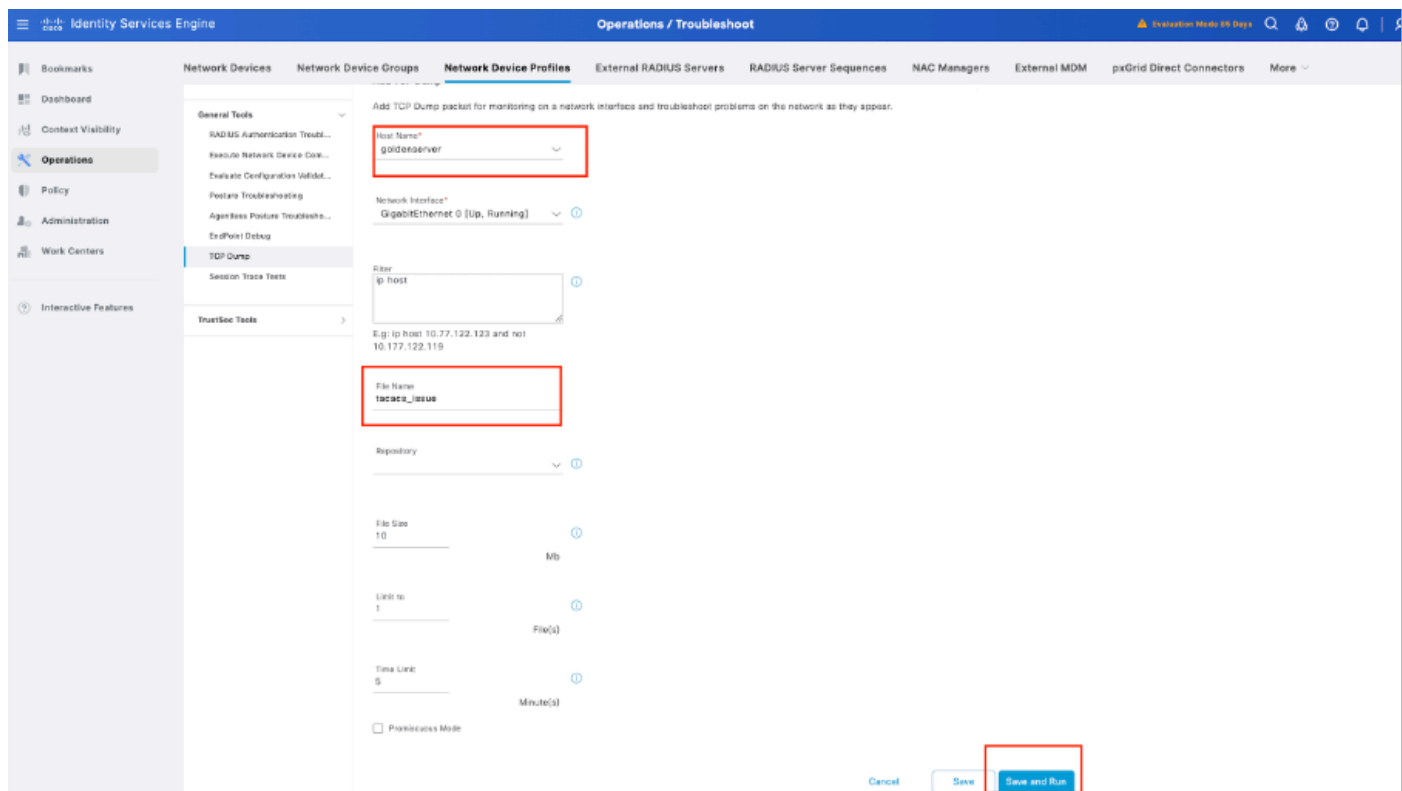


The screenshot shows the 'Live Logs' section of the Cisco Identity Services Engine. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations (highlighted), Policy, Administration, Work Centers, and Interactive Features. The main area displays a table of log entries. The table has columns: Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, Network Device, and Network Device. The first row is highlighted with a red box around the 'Details' column, which shows 'Auth Fail... X'. The second row shows 'diviya' in the 'Identity' column. The third row shows 'INVALID' in the 'Status' column. The fourth row shows 'Arista Switch Access >> Default' in the 'Authentication Policy' column. The fifth row shows 'goldenserver' in the 'Ise Node' column. The sixth row shows 'Arista_switch' in the 'Network Device' column. The seventh row shows 'Arista_switch' in the 'Network Device' column. The eighth row shows 'Arista_switch' in the 'Network Device' column. The ninth row shows 'Arista_switch' in the 'Network Device' column. The tenth row shows 'Arista_switch' in the 'Network Device' column. The eleventh row shows 'Arista_switch' in the 'Network Device' column. The twelfth row shows 'Arista_switch' in the 'Network Device' column. The thirteenth row shows 'Arista_switch' in the 'Network Device' column. The fourteenth row shows 'Arista_switch' in the 'Network Device' column. The fifteenth row shows 'Arista_switch' in the 'Network Device' column. The sixteenth row shows 'Arista_switch' in the 'Network Device' column. The seventeenth row shows 'Arista_switch' in the 'Network Device' column. The eighteenth row shows 'Arista_switch' in the 'Network Device' column. The nineteenth row shows 'Arista_switch' in the 'Network Device' column. The twentieth row shows 'Arista_switch' in the 'Network Device' column. The twenty-first row shows 'Arista_switch' in the 'Network Device' column. The twenty-second row shows 'Arista_switch' in the 'Network Device' column. The twenty-third row shows 'Arista_switch' in the 'Network Device' column. The twenty-fourth row shows 'Arista_switch' in the 'Network Device' column. The twenty-fifth row shows 'Arista_switch' in the 'Network Device' column. The twenty-sixth row shows 'Arista_switch' in the 'Network Device' column. The twenty-seventh row shows 'Arista_switch' in the 'Network Device' column. The twenty-eighth row shows 'Arista_switch' in the 'Network Device' column. The twenty-ninth row shows 'Arista_switch' in the 'Network Device' column. The thirtieth row shows 'Arista_switch' in the 'Network Device' column. The thirty-first row shows 'Arista_switch' in the 'Network Device' column. The thirty-second row shows 'Arista_switch' in the 'Network Device' column. The thirty-third row shows 'Arista_switch' in the 'Network Device' column. The thirty-fourth row shows 'Arista_switch' in the 'Network Device' column. The thirty-fifth row shows 'Arista_switch' in the 'Network Device' column. The thirty-sixth row shows 'Arista_switch' in the 'Network Device' column. The thirty-seventh row shows 'Arista_switch' in the 'Network Device' column. The thirty-eighth row shows 'Arista_switch' in the 'Network Device' column. The thirty-ninth row shows 'Arista_switch' in the 'Network Device' column. The fortieth row shows 'Arista_switch' in the 'Network Device' column. The forty-first row shows 'Arista_switch' in the 'Network Device' column. The forty-second row shows 'Arista_switch' in the 'Network Device' column. The forty-third row shows 'Arista_switch' in the 'Network Device' column. The forty-fourth row shows 'Arista_switch' in the 'Network Device' column. The forty-fifth row shows 'Arista_switch' in the 'Network Device' column. The forty-sixth row shows 'Arista_switch' in the 'Network Device' column. The forty-seventh row shows 'Arista_switch' in the 'Network Device' column. The forty-eighth row shows 'Arista_switch' in the 'Network Device' column. The forty-ninth row shows 'Arista_switch' in the 'Network Device' column. The fiftieth row shows 'Arista_switch' in the 'Network Device' column. The fifty-first row shows 'Arista_switch' in the 'Network Device' column. The fifty-second row shows 'Arista_switch' in the 'Network Device' column. The fifty-third row shows 'Arista_switch' in the 'Network Device' column. The fifty-fourth row shows 'Arista_switch' in the 'Network Device' column. The fifty-fifth row shows 'Arista_switch' in the 'Network Device' column. The fifty-sixth row shows 'Arista_switch' in the 'Network Device' column. The fifty-seventh row shows 'Arista_switch' in the 'Network Device' column. The fifty-eighth row shows 'Arista_switch' in the 'Network Device' column. The fifty-ninth row shows 'Arista_switch' in the 'Network Device' column. The sixtieth row shows 'Arista_switch' in the 'Network Device' column. The sixty-first row shows 'Arista_switch' in the 'Network Device' column. The sixty-second row shows 'Arista_switch' in the 'Network Device' column. The sixty-third row shows 'Arista_switch' in the 'Network Device' column. The sixty-fourth row shows 'Arista_switch' in the 'Network Device' column. The sixty-fifth row shows 'Arista_switch' in the 'Network Device' column. The sixty-sixth row shows 'Arista_switch' in the 'Network Device' column. The sixty-seventh row shows 'Arista_switch' in the 'Network Device' column. The sixty-eighth row shows 'Arista_switch' in the 'Network Device' column. The sixty-ninth row shows 'Arista_switch' in the 'Network Device' column. The seventieth row shows 'Arista_switch' in the 'Network Device' column. The seventy-first row shows 'Arista_switch' in the 'Network Device' column. The seventy-second row shows 'Arista_switch' in the 'Network Device' column. The seventy-third row shows 'Arista_switch' in the 'Network Device' column. The seventy-fourth row shows 'Arista_switch' in the 'Network Device' column. The seventy-fifth row shows 'Arista_switch' in the 'Network Device' column. The seventy-sixth row shows 'Arista_switch' in the 'Network Device' column. The seventy-seventh row shows 'Arista_switch' in the 'Network Device' column. The seventy-eighth row shows 'Arista_switch' in the 'Network Device' column. The seventy-ninth row shows 'Arista_switch' in the 'Network Device' column. The eightieth row shows 'Arista_switch' in the 'Network Device' column. The eighty-first row shows 'Arista_switch' in the 'Network Device' column. The eighty-second row shows 'Arista_switch' in the 'Network Device' column. The eighty-third row shows 'Arista_switch' in the 'Network Device' column. The eighty-fourth row shows 'Arista_switch' in the 'Network Device' column. The eighty-fifth row shows 'Arista_switch' in the 'Network Device' column. The eighty-sixth row shows 'Arista_switch' in the 'Network Device' column. The eighty-seventh row shows 'Arista_switch' in the 'Network Device' column. The eighty-eighth row shows 'Arista_switch' in the 'Network Device' column. The eighty-ninth row shows 'Arista_switch' in the 'Network Device' column. The ninetieth row shows 'Arista_switch' in the 'Network Device' column. The ninety-first row shows 'Arista_switch' in the 'Network Device' column. The ninety-second row shows 'Arista_switch' in the 'Network Device' column. The ninety-third row shows 'Arista_switch' in the 'Network Device' column. The ninety-fourth row shows 'Arista_switch' in the 'Network Device' column. The ninety-fifth row shows 'Arista_switch' in the 'Network Device' column. The ninety-sixth row shows 'Arista_switch' in the 'Network Device' column. The ninety-seventh row shows 'Arista_switch' in the 'Network Device' column. The ninety-eighth row shows 'Arista_switch' in the 'Network Device' column. The ninety-ninth row shows 'Arista_switch' in the 'Network Device' column. The hundredth row shows 'Arista_switch' in the 'Network Device' column.

Stap 3. Als u geen livelog ziet, gaat u verder met het vastleggen van pakketten. Navigeer naar het menu Bewerkingen > Problemen oplossen > Diagnostische hulpprogramma's > Algemene hulpprogramma's > TCP-dumping, selecteer Toevoegen:



The screenshot shows the 'TCP Dump' configuration page in the Cisco Identity Services Engine. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations (highlighted), Policy, Administration, Work Centers, and Interactive Features. The main area displays the 'TCP Dump' configuration page. The page has a title 'TCP Dump' and a description 'The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear'. The page has a table with columns: Host Name, Network Interface, Filter, File Name, Repository, File Size, Number of ..., Time Limit, and Promiscuous. The 'Host Name' column has a value 'goldenserver'. The 'Network Interface' column has a value 'GigabitEthernet 0 [Up, Running]'. The 'Filter' column has a value 'ip host'. The 'File Name' column has a value 'tacos_issue'. The 'Repository' column has a value 'tacos_issue'. The 'File Size' column has a value '10'. The 'Number of ...' column has a value '1'. The 'Time Limit' column has a value '5'. The 'Promiscuous' column has a value 'Off'. The page has a 'Save and Run' button at the bottom right.



The screenshot shows the 'TCP Dump' configuration page in the Cisco Identity Services Engine. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations (highlighted), Policy, Administration, Work Centers, and Interactive Features. The main area displays the 'TCP Dump' configuration page. The page has a title 'TCP Dump' and a description 'Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear'. The page has a table with columns: Host Name, Network Interface, Filter, File Name, Repository, File Size, Number of ..., Time Limit, and Promiscuous. The 'Host Name' column has a value 'goldenserver'. The 'Network Interface' column has a value 'GigabitEthernet 0 [Up, Running]'. The 'Filter' column has a value 'ip host'. The 'File Name' column has a value 'tacos_issue'. The 'Repository' column has a value 'tacos_issue'. The 'File Size' column has a value '10'. The 'Number of ...' column has a value '1'. The 'Time Limit' column has a value '5'. The 'Promiscuous' column has a value 'Off'. The page has a 'Save and Run' button at the bottom right.

Stap 4. Schakel de component runtime-AAA in voor foutopsporing binnen de PSN van waaruit de

verificatie wordt uitgevoerd in Operations > Troubleshoot > Debug Wizard > Debug log configuratie, selecteer PSN node, en selecteer de knop Bewerken:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Operations / Troubleshoot'. A sidebar on the left contains various menu items: Bookmarks, Dashboard, Context Visibility, Operations (highlighted), Policy, Administration, Work Centers, and Interactive Features. The main content area is titled 'Node List' and shows a table with one node: 'goldenserver' with a 'STANDALONE' replication role. Above the table are buttons for 'Edit' and 'Reset to Default'. The top right corner indicates 'Evaluation Mode 85 Days'.

The screenshot shows the 'Debug Level Configuration' page in the Cisco ISE interface. The breadcrumb trail is 'Node List > goldenserver.diviya.com'. The page title is 'Debug Level Configuration'. Below the title are buttons for 'Edit', 'Reset to Default', 'Log Filter Enable', 'Log Filter Disable', and 'Quick Filter'. A table lists the configuration for the 'runtime-AAA' component. The table has columns for 'Component Name', 'Log Level', 'Description', 'Log file Name', and 'Log Filter'. The 'runtime-AAA' component is highlighted with a red box, showing a log level of 'DEBUG' and a log filter of 'Disabled'. Below the table are 'Save' and 'Cancel' buttons.

Component Name	Log Level	Description	Log file Name	Log Filter
runtime-AAA	DEBUG	AAA runtime messages (prtt)	prtt-server.log	Disabled

Identificeer de runtime-AAA-component, stel het logboekniveau in op debuggen, reproduceer het probleem en analyseer de logs voor verder onderzoek.

Probleemoplossing

Probleem 1

De TACACS+-verificatie tussen de Cisco ISE en de Arista-switch (of een ander netwerkkapparaat) mislukt met de foutmelding:

"13036 Selected Shell Profile is DenyAccess"

Overview		Steps	
Request Type	Authentication	13013	Received TACACS+ Authentication START Request
Status	Fail	15049	Evaluating Policy Group (🔴 Step latency=1ms)
Session Key	goldenserver/541265148/80	15008	Evaluating Service Selection Policy (🔴 Step latency=0ms)
Message Text	Failed-Attempt: Authentication failed	15048	Queried PIP - DEVICE.Device Type (🔴 Step latency=2ms)
Username	diviya	15041	Evaluating Identity Policy (🔴 Step latency=3ms)
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth	15048	Queried PIP - Network Access.Protocol (🔴 Step latency=2ms)
Selected Authorization Profile	Deny All Shell Profile	15013	Selected Identity Source - Internal Users (🔴 Step latency=2ms)
Authentication Details		24210	Looking up User in Internal Users IDStore (🔴 Step latency=0ms)
Generated Time	2025-07-27 16:06:30.094000 +05:30	24212	Found User in Internal Users IDStore (🔴 Step latency=37ms)
Logged Time	2025-07-27 16:06:30.094	13045	TACACS+ will use the password prompt from global TACACS+ configuration (🔴 Step latency=0ms)
Epoch Time (sec)	1753612590	13015	Returned TACACS+ Authentication Reply (🔴 Step latency=0ms)
ISE Node	goldenserver	13014	Received TACACS+ Authentication CONTINUE Request (🔴 Step latency=68ms)
Message Text	Failed-Attempt: Authentication failed	15041	Evaluating Identity Policy (🔴 Step latency=0ms)
Failure Reason	13036 Selected Shell Profile is DenyAccess	15013	Selected Identity Source - Internal Users (🔴 Step latency=4ms)
Resolution	Check whether the Device Administration Authorization Policy rules are correct	24210	Looking up User in Internal Users IDStore (🔴 Step latency=0ms)
Root Cause	Selected Shell Profile fails for this request	24212	Found User in Internal Users IDStore (🔴 Step latency=7ms)
Username	diviya	22037	Authentication Passed (🔴 Step latency=0ms)
		15036	Evaluating Authorization Policy (🔴 Step latency=0ms)
		15048	Queried PIP - Network Access.UserName (🔴 Step latency=4ms)

De fout "13036 Selected Shell Profile is DenyAccess" in Cisco ISE betekent meestal dat tijdens een TACACS+-apparaatbeheerpoging het autorisatiebeleid overeenkomt met een shell-profiel dat is ingesteld op DenyAccess. Dit is meestal niet het gevolg van een verkeerd geconfigureerd shell-profiel zelf, maar geeft eerder aan dat geen van de geconfigureerde autorisatieregels overeenkwam met de attributen van de inkomende gebruiker (zoals groepslidmaatschap, apparaattype of locatie). Als gevolg hiervan valt ISE terug naar een standaardregel of een expliciete weigeringsregel, waardoor de toegang wordt geweigerd.

Mogelijke oorzaken

- Herziening van de regels voor het vergunningenbeleid in ISE. Bevestig dat de gebruiker of het apparaat voldoet aan de juiste regel die het beoogde shell-profiel toewijst, zoals een regel die passende toegang mogelijk maakt.
- Zorg ervoor dat de toewijzing van de AD of interne gebruikersgroep correct is en dat de beleidsvoorwaarden, zoals lidmaatschap van de gebruikersgroep, apparaattype en protocol, nauwkeurig worden gespecificeerd.
- Gebruik ISE live logs en details van de mislukte poging om precies te zien welke regel is gekoppeld en waarom.

Probleem 2

De TACACS+-verificatie tussen de Cisco ISE en de Arista-Switch (of een ander netwerkapparaat) mislukt met de foutmelding:

"13017 Ontvangen TACACS+-pakket van onbekend netwerkkapparaat of AAA-client"

Cisco ISE

Overview

Request Type	Authentication
Status	Fail
Session Key	
Message Text	Failed-Attempt: TACACS+ Request dropped
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details

Generated Time	2025-07-27 17:50:17.705000 +05:30
Logged Time	2025-07-27 17:50:17.705
Epoch Time (sec)	1753618817
ISE Node	goldenserver
Message Text	Failed-Attempt: TACACS+ Request dropped
Failure Reason	13017 Received TACACS+ packet from unknown Network Device or AAA Client
Resolution	
Root Cause	
Username	

Steps

13017 Received TACACS+ packet from unknown Network Device or AAA Client

Mogelijke oorzaken

- De meest voorkomende reden is dat het IP-adres van de switch niet wordt toegevoegd als netwerkkapparaat in ISE (onder Beheer > Netwerkbronnen > Netwerkkapparaten).
- Zorg ervoor dat het IP-adres of bereik exact overeenkomt met het bron-IP dat door de Arista-switch wordt gebruikt om TACACS+-pakketten te verzenden.
- Als uw switch een beheerinterface gebruikt, controleert u of het exacte IP-adres (niet alleen een subnet/bereik) is toegevoegd in ISE.

Oplossing

- Ga naar Beheer > Netwerkbronnen > Netwerkkapparaten in de ISE GUI.
- Controleer of het exacte bron-IP-adres op de Arista-switch wordt gebruikt voor TACACS+-communicatie (meestal de beheerinterface IP).
- Geef het gedeelde geheim op (het moet overeenkomen met wat is ingesteld op de Arista-switch).

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.