

Catalyst Center External Authentication TACACS configureren met ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Cisco Identity Services Engine \(ISE\)](#)

[Licentie en inschakelen van de TACACS+-services](#)

[Admin-gebruiker maken en netwerkkapparaat toevoegen](#)

[TACACS+ profiel configureren](#)

[TACACS+-beleid configureren](#)

[Cisco Catalyst Center](#)

[De ISE/AAA-server configureren](#)

[De externe verificatie inschakelen en configureren.](#)

[Verifiëren](#)

[Problemen oplossen](#)

[1. Misconfiguratie van attributen](#)

[2. Gedeelde geheime mismatch](#)

Inleiding

In dit document worden de stappen beschreven die nodig zijn om de Cisco Identity Services Engine te integreren met Catalyst Center om de TACACS+-verificatie in te schakelen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beheerderstoegang tot zowel Cisco ISE als Cisco Catalyst Center.
- Basiskennis van AAA (Authenticatie, Autorisatie en Boekhouding) concepten.
- Werkende kennis van het TACACS+ protocol.
- Netwerkconnectiviteit tussen Catalyst Center en de ISE-server.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversie:

- Cisco Catalyst Center versie 2.3.7.x
- Cisco Identity Services Engine (ISE) versie 3.x (of hoger)
- TACACS+-protocol voor externe gebruikersverificatie

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

Met deze integratie kunnen externe gebruikers zich aanmelden bij Catalyst Center voor administratieve toegang en beheer.

Configureren

Cisco Identity Services Engine (ISE)

Licentie en inschakelen van de TACACS+-services

Voordat u begint met de TACACS+-configuratie in ISE, moet u bevestigen dat de juiste licentie is geïnstalleerd en dat de functie is ingeschakeld.

1. Controleer of u de PID-licentie L-ISE-TACACS-ND= in het [Cisco Smart Software Manage](#)- of [Cisco License Central](#)-portaal hebt.

Schakel Apparaatbeheer in het ISE-licentieportaal in.

- De Device Admin-licentie (PID: L-ISE-TACACS-ND=) maakt TACACS+-services mogelijk op een Policy Service Node (PSN).

- Navigeer naar:

Beheer > Systeem > Licenties

- Schakel het selectievakje voor Apparaatbeheer onder de laagopties in.

Tier ☒ Essential ☒ Advantage ☒ Premier ☒ Device Admin

Virtual Appliance ☒ ISE VM License

This enables the ISE features for the purchased licenses to be tracked by Cisco Smart Licensing.

By clicking Register you will agree to the Terms&Conditions. You can download Terms&Conditions on [Smart Licensing Resources](#).

[Reset](#)

[Update](#)

Apparaatbeheer

☐	Premier	Enabled	Released Entitlement	0	-	Dec 27,2024 18:16:00 PM
☐	Device Admin	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM
Virtual Appliance						
	ISE VM License	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM

Licentieapparaatbeheer

3. Schakel de Apparaatbeheerservice in op de ISE-node waarop de TACACS+-service wordt uitgevoerd.

- Navigeer naar:

Beheer > Systeem > Implementatie > De node selecteren

- Selecteer de optie Apparaatbeheerservice inschakelen.

Cisco ISE Administration · System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Deployment Nodes List > ise-mxc1

Deployment

- > Deployment
- > PAN Fallover

Edit Node

General Settings Profiling Configuration

Hostname ise-mxc1

FQDN ise-mxc1.cisco.com

IP Address 10.88.244.180

Node Type Identity Services Engine (ISE)

Role STANDALONE [Make Primary](#)

☒ Administration

☒ > Monitoring

☒ Policy Service

- ☒ Enable Session Services ⓘ
- Include Node in Node Group
None ⓘ
- ☒ Enable Profiling Service ⓘ
- ☐ Enable Threat Centric NAC Service ⓘ
- ☒ > Enable SXP Service ⓘ
- ☒ Enable Device Admin Service ⓘ
- ☐ Enable Passive Identity Service ⓘ

☒ > pxGrid ⓘ

Apparaatbeheerservice inschakelen

Admin-gebruiker maken en netwerkkaparaat toevoegen

1. Maak de beheerdersgebruiker aan.

- Deze gebruikersaccount wordt gebruikt om in te loggen op de Catalyst Center UI via ISE-verificatie.
- Navigeer naar:
Workcenters > Netwerkttoegang > Identiteiten > Netwerkttoegang gebruiker
- Voeg een nieuwe gebruiker toe (bijvoorbeeld catc-user).
- Als de gebruiker al bestaat, gaat u verder met de volgende stap.

2. Maak het netwerkkaparaat aan.

- Navigeer naar:
Workcenters > Netwerkttoegang > Identiteiten > Netwerkbbron

- Voeg het IP-adres van Catalyst Center toe, of definieer het subnet waar het IP van Catalyst Center zich bevindt.
- Als het apparaat al bestaat, controleert u of het de volgende parameters bevat:
 - De TACACS-verificatie-instellingen zijn ingeschakeld.
 - Het gedeelde geheim is geconfigureerd en bekend (sla deze waarde op, zoals later vereist in Catalyst Center).

The screenshot shows the Cisco ISE interface for configuring a Network Device. The 'Network Resources' tab is selected. The device 'Catalyst-Center_6' is being configured. The 'TACACS Authentication Settings' section is highlighted with a red box, showing the 'Shared Secret' field with a 'Show' button and a 'Retire' button. The 'Legacy Cisco Device' radio button is selected.

TACACS-verificatie-instellingen

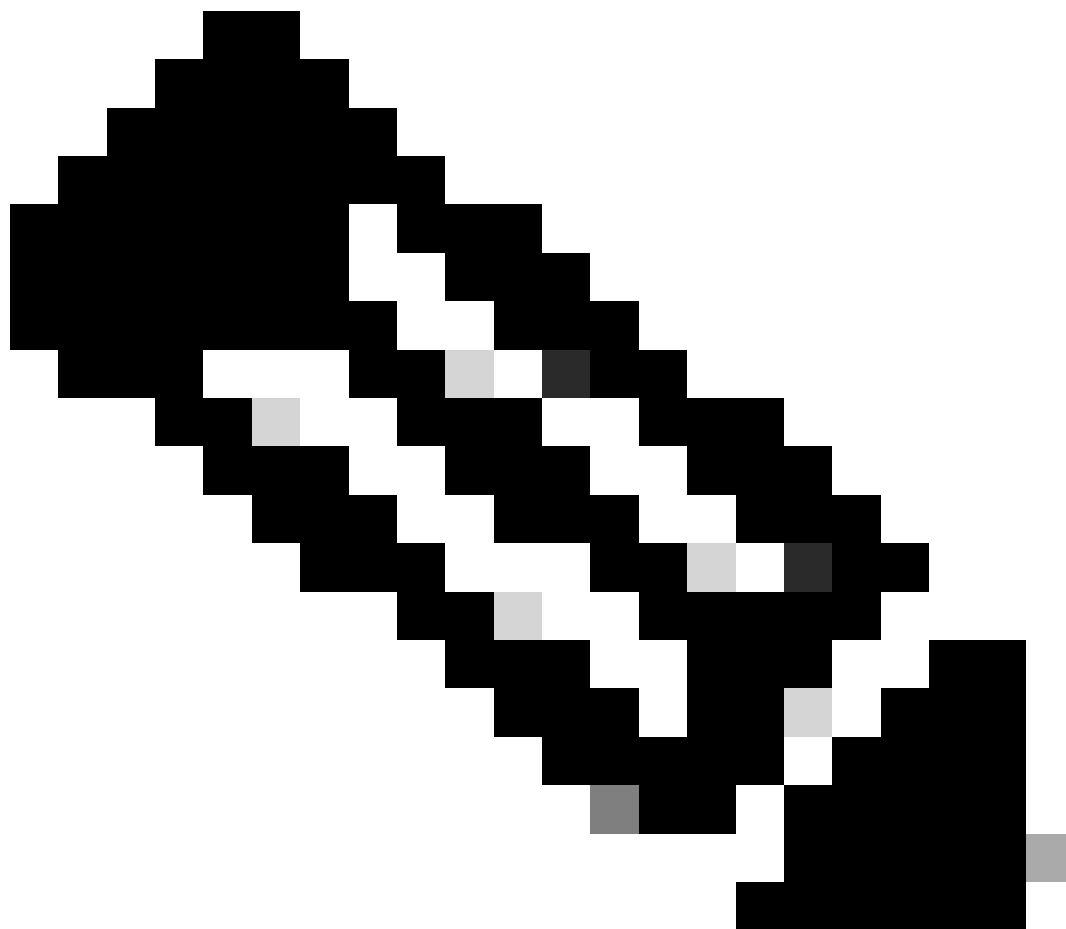
TACACS+ profiel configureren

1. Maak een nieuw TACACS+ profiel aan.

- Navigeer naar:
 - Workcenters > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-profielen
- Voeg een profielnaam toe.
- Voeg als volgt een aangepast kenmerk toe:
 - Type: Verplicht

- Sla het profiel op.

TACACS+-profiel



Opmerking: Cisco Catalyst Center ondersteunt externe verificatie-, autorisatie- en boekhoudservers (AAA) voor toegangscontrole. Als u een externe server gebruikt voor verificatie en autorisatie van externe gebruikers, kunt u externe verificatie inschakelen in Cisco Catalyst Center. De standaardinstelling voor het AAA-kenmerk komt overeen met het standaardinstelling voor het gebruikersprofiel.

De standaard AAA-attribuuwaarde van het TACACS-protocol is cisco-av-pair.

De standaard AAA-attribuuwaarde van het RADIUS-protocol is Cisco-AVPair.

Wijziging is alleen vereist als uw AAA-server een aangepast kenmerk heeft in het gebruikersprofiel. Op de AAA-server is het formaat van de AAA-attribuuwaarde Role=role1. Op de Cisco Identity Services Engine (Cisco ISE)-server kan de gebruiker tijdens het configureren van het RADIUS- of TACACS-profiel een cisco av-pair als AAA-kenmerk selecteren of invoeren.

U kunt het AAA-kenmerk bijvoorbeeld handmatig selecteren en configureren als cisco-av-pair=Role=SUPER-ADMIN-ROLE of Cisco-AVPair=Role=SUPER-ADMIN-ROLE.

2. Maak een TACACS+-opdrachtset aan.

- Navigeer naar:

Workcenters > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-opdrachtsets

- Voeg een naam toe.
- Schakel de optie Toestaan in als een opdracht hieronder niet wordt vermeld.
- Sla de opdrachtset op.

The screenshot shows the Cisco ISE interface for creating a TACACS Command Set. The breadcrumb trail is: TACACS Command Sets > PermitAllCommands > Command Set. The page has a sidebar with navigation options: Conditions, Network Conditions, Results, Allowed Protocols, TACACS Command Sets (selected), and TACACS Profiles. The main content area has a form with the following fields:

- Name:** PermitAllCommands
- Description:** (empty text box)
- Commands:** A section with a checkbox labeled "Permit any command that is not listed below" which is checked.
- Buttons:** Add, Trash, Edit, Move Up, Move Down.
- Table:** A table with columns: Grant, Command, Arguments. It is currently empty with the message "No data found."
- Buttons:** Cancel, Save.

TACACS-opdrachtsets

TACACS+-beleid configureren

1. Maak een nieuwe TACACS+-beleidsset aan.

- Navigeer naar:

Workcenters > Apparaatbeheer > Beleidsset Apparaatbeheer

- Voeg een naam toe voor de beleidsset.
- Configureer de conditie.
 - In dit voorbeeld komt de voorwaarde overeen met het IP-adres van Catalyst Center.

The screenshot shows the Conditions Studio interface. The left sidebar has a search bar and a list of conditions. The main area is the Editor, which shows a condition configuration for "Network Access Device IP Address". The condition is set to "Equals" with the value "10.88.244.160". There are buttons for "Duplicate" and "Save". At the bottom, there are links for "NEW", "AND", and "OR".

1.3 Selecteer Standaardapparaatbeheer in de toegestane protocollen/serverreeks.

Selecteer Standaardapparaatbeheer

2. Configureer de beleidsset.

- Klik rechts op de pijl (>) om de beleidsset uit te vouwen en te configureren.
- Voeg een nieuwe regel toe onder Machtigingsbeleid.
- Configureer de nieuwe regel als volgt:
 - Naam: Voer een beschrijvende regelnaam in.
 - Voorwaarde: in dit voorbeeld kwam de voorwaarde overeen met Alle apparaattypen.

Alle apparaattypen

- Opdrachtset: Selecteer de TACACS+ Opdrachtset die eerder is gemaakt.
- Shell-profiel: Selecteer het TACACS+-profiel dat eerder is gemaakt.

TACACS+-opdrachtset

Cisco Catalyst Center

De ISE/AAA-server configureren

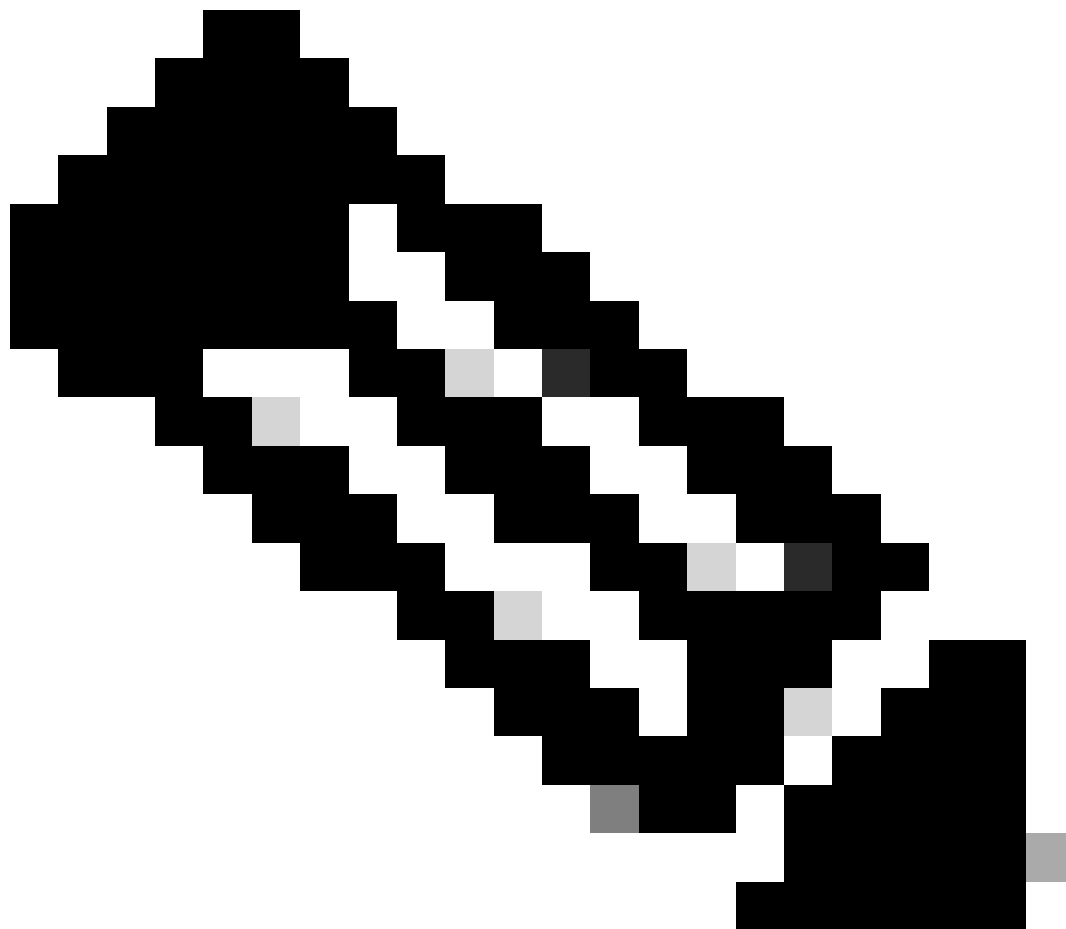
1. Meld u aan bij de webinterface van Catalyst Center.

- Navigeer naar:

Hoofdmenu > Systeem > Instellingen > Externe services > Verificatie- en beleidsservers

2. Een nieuwe server toevoegen. U kunt kiezen tussen ISE of AAA.

- Voor deze demo wordt de AAA server optie gebruikt.
-



Opmerking: voor een Catalyst Center-cluster kan slechts één ISE-cluster worden geconfigureerd.

3. Configureer deze opties en sla vervolgens op:

- Voer het IP-adres van de AAA-server in.
- Voeg het gedeelde geheim toe (hetzelfde geheim dat is geconfigureerd in de Cisco ISE Network Resource).
- Schakel Geavanceerde instellingen in op Aan (Aan).
- Controleer de optie TACACS.

Add AAA server



Server IP Address*

10.88.244.180

Shared Secret*

.....

[SHOW](#)



Advanced Settings

Protocol



RADIUS



TACACS



Enable KeyWrap

Authentication Port*

1812

Accounting Port*

1813

Port

49

Retries*

3

Timeout (seconds)*

4

Verificatie- en beleidsservers

Cisco Catalyst Center

System / Settings

External Ser X

External Services

Authentication and Policy Servers

Integrity Verification

SD-Access Compatibility Matrix

IP Address Manager

Cloud Access Login

Cisco AI Analytics

Sniffwatch

Talos IP Reputation

Settings / External Services

Authentication and Policy Servers

Use this form to specify the servers that authenticate Catalyst Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

Add

Export

IP Address

Protocol

Type

Status

Actions

192.168.31.228

RADIUS

ISE

INACTIVE

10.88.244.180

RADIUS_TACACS

AAA

ACTIVE

As of Sep 11, 2025 5:52 PM

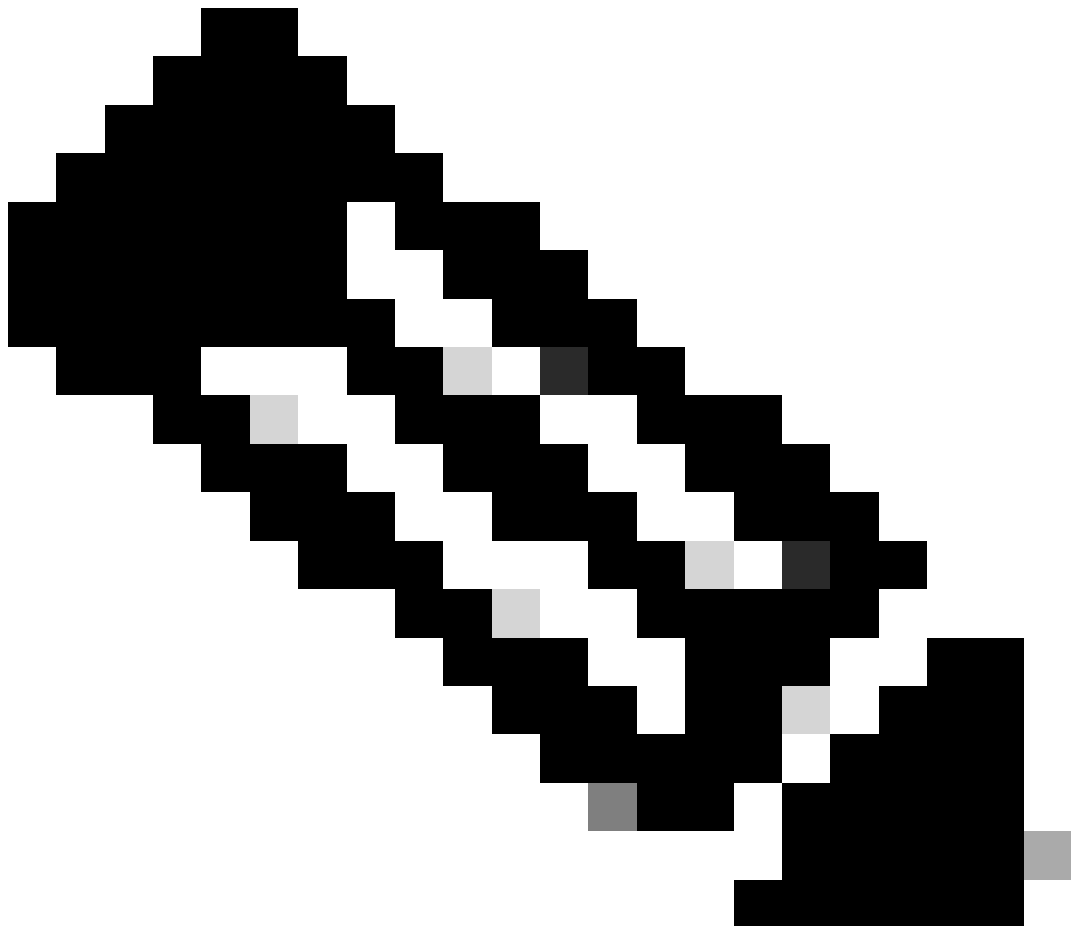
Geavanceerde instellingen

De externe verificatie inschakelen en configureren.

1. Navigeer naar de pagina Externe verificatie:

Hoofdmenu > Systeem > Gebruiker en rol > Externe verificatie

2. Voeg het AAA-kenmerk cisco-av-pair toe en klik op Bijwerken om de wijzigingen op te slaan.



Opmerking: Deze stap is niet verplicht omdat het standaardkenmerk voor TACACS+ al cisco-av-pair is, maar het wordt als een best practice beschouwd om het expliciet te

configureren.

3. Selecteer onder Primaire AAA-server de eerder geconfigureerde AAA-server.

- Klik op Geavanceerde instellingen bekijken om extra opties weer te geven.
- Selecteer de optie TACACS+.
- Voer het gedeelde geheim in dat is geconfigureerd in de netwerkbron van Cisco ISE.
- Klik op Bijwerken om de wijzigingen op te slaan.

4. Schakel het selectievakje Externe gebruiker in.

- Met deze actie wordt de configuratie automatisch opgeslagen.

The screenshot shows the 'External Authentication' configuration page in Cisco Catalyst Center. The page is divided into several sections:

- Enable External User:** A checkbox that is checked.
- AAA Attribute:** A dropdown menu showing 'cisco-av-pair'.
- AAA Server(s):** A section with two columns for 'Primary AAA Server' and 'Secondary AAA Server'. Both have IP addresses set to '10.88.244.180'. Below each IP address is a 'Shared Secret' field.
- Advanced Settings:** A section with radio buttons for 'RADIUS' and 'TACACS+'. 'TACACS+' is selected. There is an 'Update' button next to it.
- Port:** A dropdown menu showing '49'.
- Replies:** A dropdown menu showing '3'.
- Timeout (seconds):** A dropdown menu showing '4'.
- Update:** A button at the bottom left of the configuration section.

A success message is displayed in the bottom right corner: 'Success Successfully saved external authentication settings.'

externe verificatie

Verifiëren

1. Open een nieuwe browsersessie of gebruik de incognitomodus en log in op de webpagina Catalyst Center met de gebruikersaccount die is geconfigureerd in Cisco ISE.
2. Controleer in Catalyst Center of de aanmelding succesvol is.



Inloggen Catalyst Center configureren Externe verificatie TACACS met ISE

3. Vanuit Cisco ISE de logboeken valideren:

Bewerkingen > TACACS > Live-logs

- Verificatiestatus: Pass
- Autorisatie status: Pass

Cisco ISE

Operations - TACACS

License Warning

Live Logs

Export To

Refresh

Never

Show

Latest 20 records

Within

Last 3 hours

Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Isa Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
X			Identity		Authentication Policy	Authorization Policy	Isa Node	Network Device Nam	Network Device	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Command	Shell Profile
Sep 12, 2025 12:12:20.801...			cisco-user	Authentication	CatC_TACACS_Profile >> Auth...	CatC_TACACS_Profile >> Authori...	isa-mac1	Catalyst-Centr_8	10.88.244.160	Device Type680 D...	LocationRAI Locat...	console		10.189.17.203		CatC_TACACS_P...
Sep 12, 2025 12:12:20.798...			cisco-user	Authentication	CatC_TACACS_Profile >> Default		isa-mac1	Catalyst-Centr_8	10.88.244.160	Device Type680 D...	LocationRAI Locat...	console		10.189.17.203		

Last Updated: Thu Sep 11 2025 18:14:58 GMT-0600 (Central Standard Time)

Records Shown: 2

Live-logs

4. Vergelijk in de Autorisatiedetails de volgende uitvoer met:

- Berichttekst: Apparaatbeheer: sessieautorisatie geslaagd
- Alle responsattributen: cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes	
All Response Attributes	cisco-av-pair=Role=SUPER-ADMIN-ROLE

cisco-av-pair=Role=SUPER-ADMIN-ROL

Problemen oplossen

Hier zijn enkele veelvoorkomende problemen die u kunt tegenkomen tijdens de integratie en hoe u ze kunt identificeren:

1. Misconfiguratie van attributen

Symptoom in Catalyst Center: ongeldige aanmeldingsreferenties



Cisco Catalyst Center

The bridge to possible

 Invalid Login Credentials

Username

catc-user

Password

[SHOW](#)

Log In

Misconfiguratie van attributen

- Symptoom in Cisco ISE (TACACS Logs):

- Verificatie: Pass
- Autorisatie: Pass

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:25.881...			kati-user	Authentication	CatC_TACACS_Profile <=> Authenti...	CatC_TACACS_Profile <=> Authenti...	ise-mst1	Catalyst-Center_8	10.88.244.160	Device TypeAAA D...	LocationAAA Locat...	console		10.188.17.203		CatC_TACACS_Pt...
Sep 12, 2025 12:12:26.788...			kati-user	Authentication	CatC_TACACS_Profile <=> Default		ise-mst1	Catalyst-Center_8	10.88.244.160	Device TypeAAA D...	LocationAAA Locat...	console		10.188.17.203		

Misconfiguratie van attributen

- Mogelijke oorzaken:
 - Er bestaat een spatie in de attribuutwaarde.

Voorbeeld:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes

All Response Attributes cisco-av-pair=Role=SUPER-ADMIN-ROLE

Misconfiguratie van attributen

- Het attribuut is onjuist geconfigureerd, het trefwoord Role= is gemist.

Voorbeeld:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes

All Response Attributes cisco-av-pair=Role=SUPER-ADMIN-ROLE

Misconfiguratie van attributen

2. Gedeelde geheime mismatch

- Symptoom: verificatiepakketten mislukken tussen Catalyst Center en Cisco ISE.

- Mogelijke oorzaak: Het gedeelde geheim dat is geconfigureerd in de netwerkbron van ISE komt niet overeen met het gedeelde geheim dat is geconfigureerd in Catalyst Center > Externe verificatie.

Hoe te verifiëren:

- Controleer de configuratie van de netwerkbron in ISE.
- Vergelijk het gedeelde geheim met de configuratie onder Catalyst Center > Externe verificatie.

Voorbeeld:

Authentication Details

Generated Time 2025-09-11 18:22:24.078000 +00:00

Logged Time 2025-09-11 18:22:24.078

Epoch Time (sec) 1757614944

ISE Node ise-mxc1

Message Text Failed-Attempt: Authentication failed

Failure Reason 13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets

Resolution

Root Cause

Username

Network Device Name Catalyst-Center_6

Network Device IP 10.88.244.160

Network Device Groups IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types

Device Type Device Type#All Device Types

Location Location#All Locations

Device Port

Remote Address

Gedeelde geheime mismatch

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.