

ISE configureren als externe verificatie voor DNAC GUI

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Voordat u begint](#)

[Configureren](#)

[\(Option1\) configureren van DNAC externe verificatie met behulp van RADIUS](#)

[\(Optie 1\) ISE-instellingen voor RADIUS configureren](#)

[\(Optie2\) DNAC externe verificatie configureren met behulp van TACACS+](#)

[\(Optie 2\) ISE-configuratie voor TACACS+](#)

[Verifiëren](#)

[Controleer de RADIUS-configuratie](#)

[Controleer de TACACS+ configuratie](#)

[Problemen oplossen](#)

[Referenties](#)

Inleiding

Dit document beschrijft hoe u Cisco Identity Services Engine (ISE) kunt configureren als externe verificatie voor het beheer van Cisco DNA Center GUI.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- TACACS+- en RADIUS-protocollen.
- Cisco ISE-integratie met Cisco DNA Center
- Cisco ISE-beleidsevaluatie.

Gebruikte componenten


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

- Cisco Identity Services Engine (ISE) versie 3.4 patch1.
- Cisco DNA Center versie 2.3.5.5.1

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.

Voordat u begint

- Zorg ervoor dat er ten minste één RADIUS-verificatieserver is geconfigureerd op **Systeem > Instellingen > Externe services > Verificatie- en beleidsservers**.
- Alleen een gebruiker met SUPER-ADMIN-ROL permissies op DNAC kan deze procedure uitvoeren.
- Schakel externe verificatiefallback in.

 **Voorzichtig:** In releases eerder dan 2.1.x, wanneer externe verificatie is ingeschakeld, valt Cisco DNA Center terug naar lokale gebruikers als de AAA-server onbereikbaar is of als de AAA-server een onbekende gebruikersnaam afwijst. In de huidige release valt Cisco DNA Center niet terug naar lokale gebruikers als de AAA-server onbereikbaar is of als de AAA-server een onbekende gebruikersnaam afwijst. Als de externe verificatie is ingeschakeld, kunnen externe gebruikers en lokale beheerders inloggen bij Cisco DNA Center.

Als u externe verificatiefallback wilt inschakelen, selecteert u SSH in de Cisco DNA Center-instantie en voert u de opdracht deze CLI in (`magctl rbac external_auth_fallback`).

Configureren

(Option1) configureren van DNAC externe verificatie met behulp van RADIUS

Stap 1. (optioneel) Definieer een aangepaste rollen.

Configureer uw aangepaste rollen die aan uw eis voldoen, in plaats daarvan kunt u de standaard gebruikersrollen gebruiken. Dit kan worden gedaan via het tabblad **Systeem > Gebruikers & rollen > Role Based Access Control**.

Procedure

a. Creëer een nieuwe rol.

Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

1

Role Name*
DevOps-Role

Describe the role (optional)

2

Next

Functienaam DevOps

b. Definieer de toegang.

Define the Access

1

These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to [Learn More](#).

Define the **DevOps-Role** role. Custom roles permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.

1

Access	Permission	Description
> Assurance	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Assure consistent service levels with complete visibility across all aspects of your network.
> Network Analytics	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Access to Network Analytics related components.
> Network Design	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
> Network Provision	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure, upgrade, provision and manage your network devices.
> Network Services	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure additional capabilities on the network beyond basic network connectivity and access.
> Platform	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
> Security	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Manage and control secure access to the network.

2

Next

DTVops-roltoegang

c. Maak de nieuwe rol aan.

Cisco DNA Center Create a User Role

Summary
Review the **DevOps-Role** role. Make sure all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section

Role Name & Description **Edit**
Role Name DevOps-Role
Role Description

Role Capability **Edit**

ASSURANCE

Monitoring and Troubleshooting	Deny
Monitoring Settings	Deny
Troubleshooting Tools	Deny

NETWORK ANALYTICS

Data Access	Read
-------------	------

NETWORK DESIGN

Advanced Network Settings	Deny
Image Repository	Deny
Network Hierarchy	Deny
Network Profiles	Deny
Network Settings	Deny
Virtual Network	Deny

Exit Back Create Role

Samenvatting van DevOps-rol

Cisco DNA Center Create a User Role

Network Device	Deny
Port Management	Deny
Topology	Deny
License	Deny
Network Telemetry	Deny
PnP	Deny
Provision	Deny

NETWORK SERVICES

App Hosting	Deny
Bonjour	Deny
Stealthwatch	Deny
Umbrella	Deny

PLATFORM

APIs	Write
Bundles	Write
Events	Write
Reports	Write

SECURITY

Group-Based Policy	Deny
IP Based Access Control	Deny
Security Advisories	Deny

SYSTEM

Machine Reasoning	Deny
System Management	Deny

Exit Back Create Role ¹

Rol van devOps bekijken en maken

Stap 2. Configureer externe verificatie met RADIUS.

Dit kan worden gedaan via het tabblad **Systeem > Gebruikers & rollen > Externe verificatie**.

Procedure

- Als u externe verificatie in Cisco DNA Center wilt inschakelen, schakelt u het aanvinkvakje **Externe gebruiker inschakelen** in.

b. Stel de AAA-kenmerken in.

Voer Cisco AVPair in het veld AAA-kenmerken in.

c. (Optioneel) Configureer de primaire en secundaire AAA-server.

Zorg ervoor dat het RADIUS-protocol ten minste is ingeschakeld op de primaire AAA-server, of op zowel de primaire als de secundaire server.

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

- Enable External User:** A checkbox labeled 'Enable External User' is checked. This section is marked with a red box and the letter 'a'.
- AAA Attribute:** A dropdown menu is set to 'Cisco-AVPair'. This section is marked with a red box and the letter 'b'.
- AAA Server(s):** This section is marked with a red box and the letter 'c'. It contains two columns for 'Primary AAA Server' and 'Secondary AAA Server'. Each column has fields for 'IP Address' (set to 'ISE Server 1 IP' and 'ISE Server 2 IP' respectively), 'Shared Secret' (masked with asterisks), and 'Authentication Port' (set to '1812'). Below these fields are radio buttons for 'RADIUS' (selected) and 'TACACS'.

(RADIUS) externe verificatiestappen

(Optie 1) ISE-instellingen voor RADIUS configureren

Stap 1. Voeg DNAC-server toe als netwerkapparaat op ISE.

Dit kan worden gedaan via het tabblad Beheer > Netwerkbronnen > Netwerkapparaten.

Procedure

a. Definieer (DNAC) naam en IP van netwerkapparaat.

b. (Optioneel) Apparaattype classificeren voor voorwaarde beleidsinstelling.


c. Schakel RADIUS-verificatie-instellingen in.

d. RADIUS gedeeld geheim instellen.

ISE Network Device (DNAC) voor RADIUS

Stap 2. Maak RADIUS-autorisatieprofielen.

Dit kan via het tabblad worden gedaan **Beleid > Beleidselementen > Resultaten > autorisatie > Autorisatieprofielen**.

 **Opmerking:** 3x RADIUS-autorisatieprofielen maken, één voor elke gebruikersrol.

Procedure

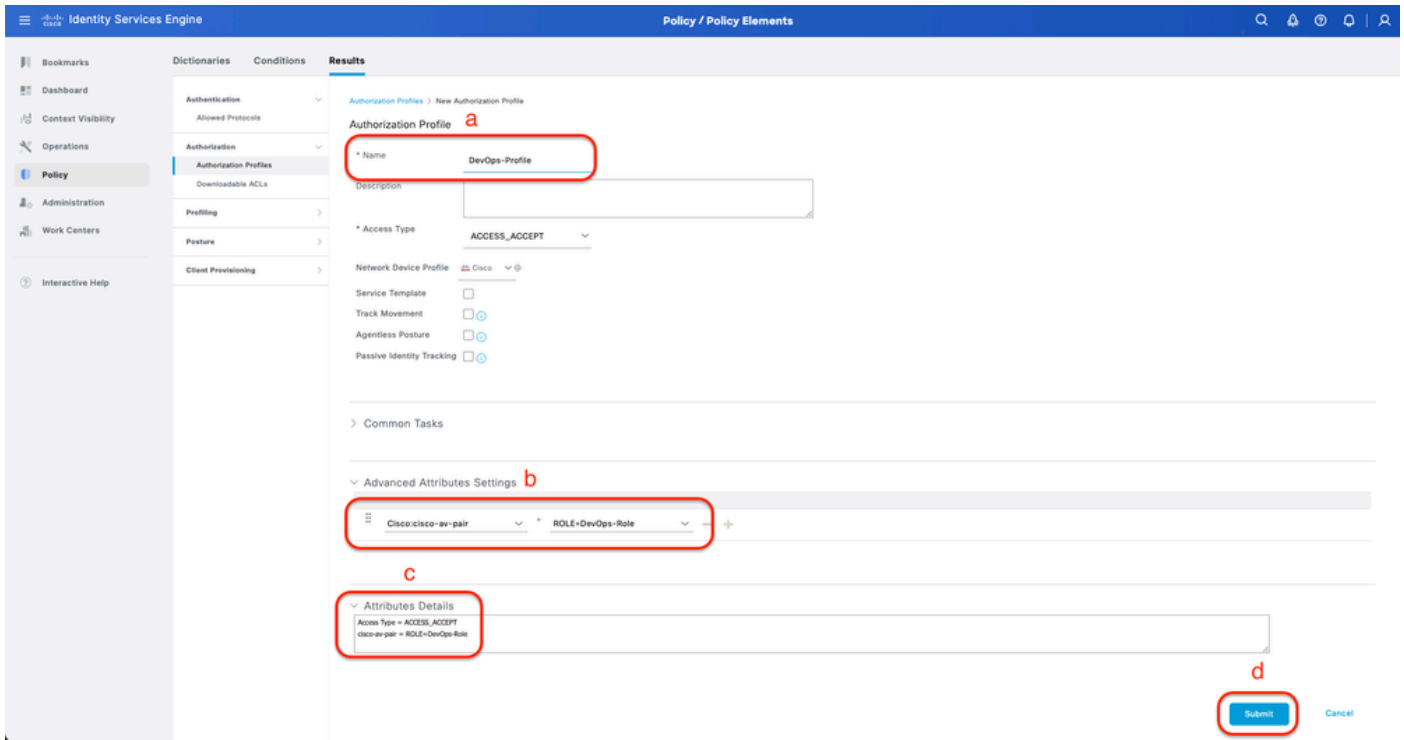
a. Klik op Add en definieer de naam van het RADIUS-autorisatieprofiel.

b. Voer het Cisco:cisco-av-paar in in de instellingen van geavanceerde kenmerken en vul de juiste gebruikersrol in.

- Voer voor de gebruikersrol (DecOps-Role) ROL=DevOps-Role in.
- Voor de gebruikersrol (NETWORK-ADMIN-ROL) voert u ROL=NETWORK-ADMIN-ROL in.
- Voer voor de gebruikersrol (SUPER-ADMIN-ROL) ROL=SUPER-ADMIN-ROL in.

c. Bekijk de details van de kenmerken.

d. Klik op Save (Opslaan).



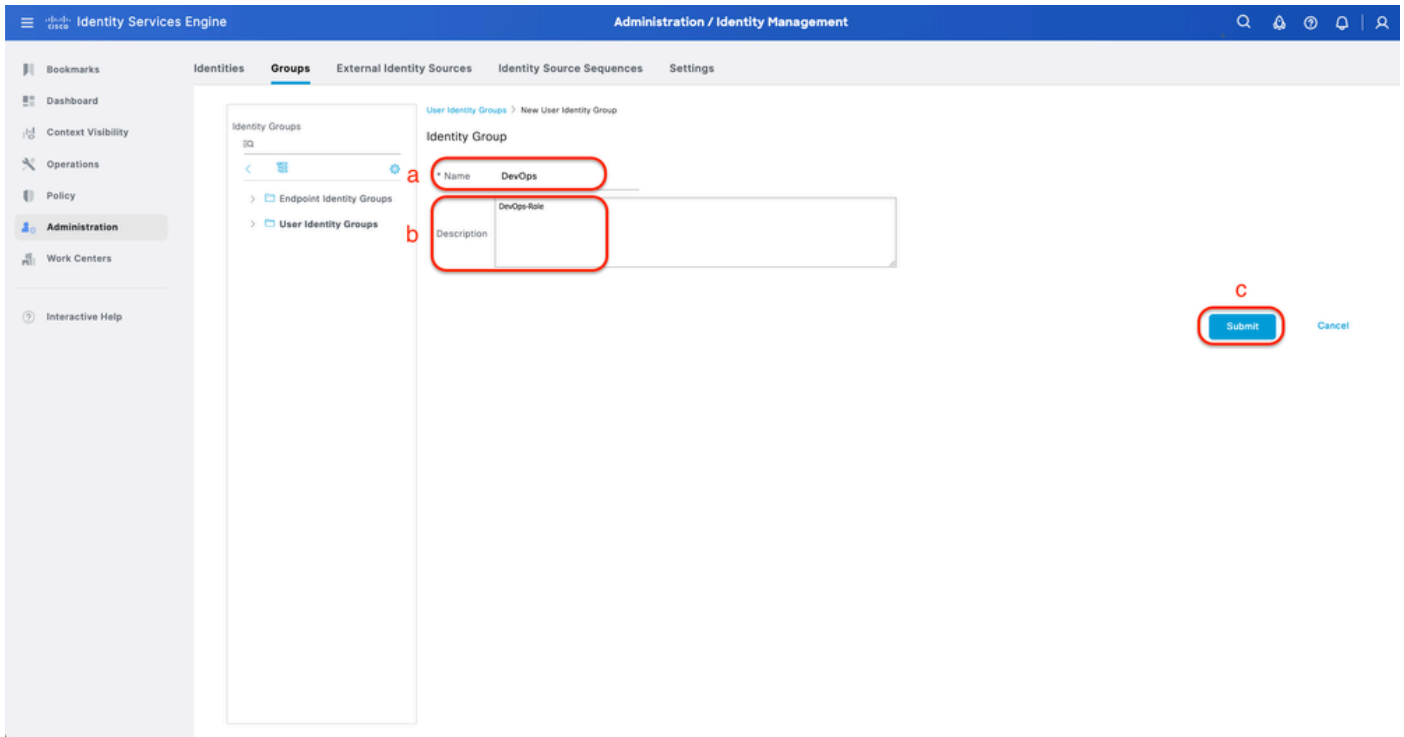
Autorisatieprofiel maken

Stap 3. Gebruikersgroep maken.

Dit kan worden gedaan via het tabblad Beheer > Identiteitsbeheer > Groepen > Gebruikersidentiteitsgroepen.

Procedure

- a. Klik op Add en definieer de naam van de identiteitsgroep
- b. (Optioneel) Definieer de beschrijving.
- c. Klik op Verzenden.



Gebruikersidentiteitsgroep maken

Stap 4. Lokale gebruiker maken.

Dit kan worden gedaan via het tabblad Beheer > Identity Management > Identity > User.

Procedure

- a. Klik op Add en definieer de gebruikersnaam.
- b. Stel het inlogwachtwoord in.
- c. Voeg de gebruiker toe aan de verwante gebruikersgroep.
- d. Klik op Verzenden.

Lokale gebruiker maken 1-2

Lokale gebruiker maken 2-2

Stap 5. (optioneel) Voeg RADIUS-beleidsset toe.

Dit kan worden gedaan via het tabblad Policy > Policy Sets.

Procedure

a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

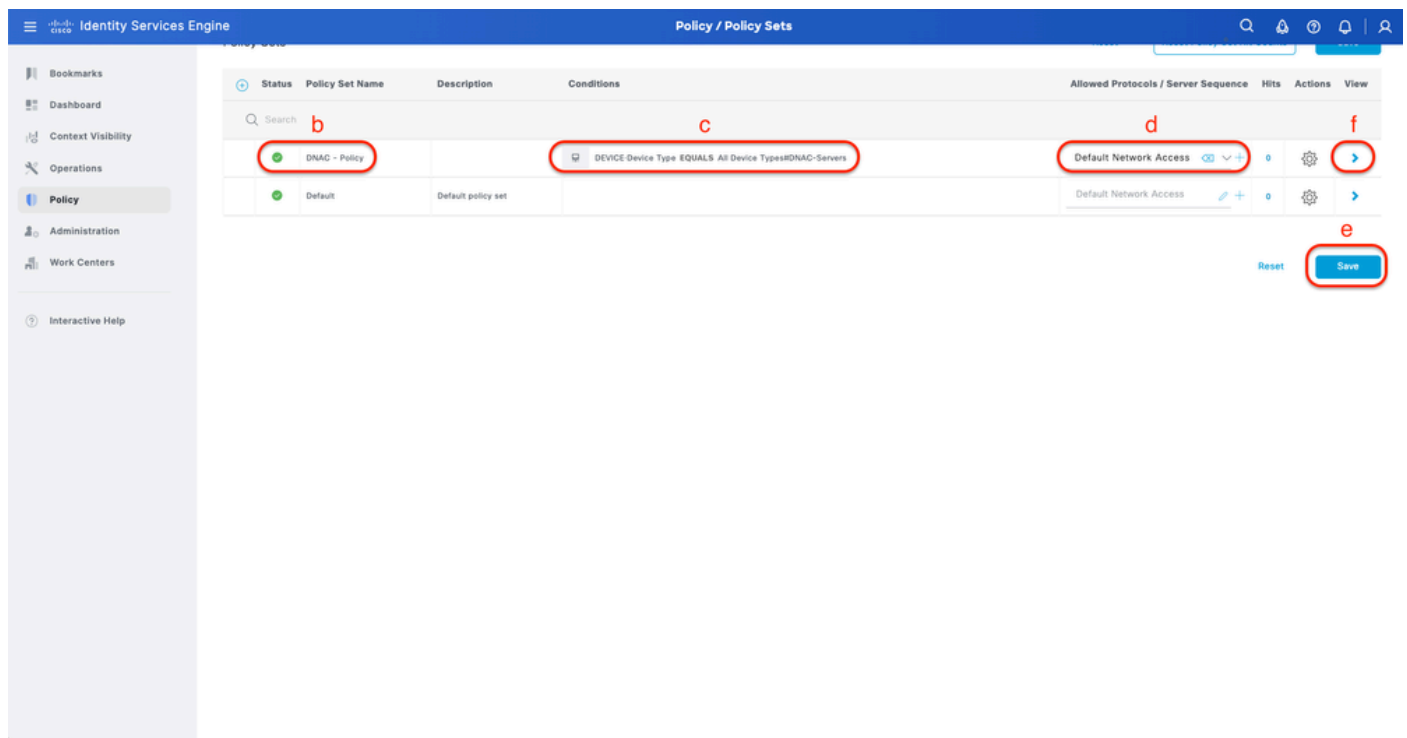
b. Bepaal de naam van de beleidsset.

c. Stel de voorwaarde voor de beleidsset in om het apparaattype te selecteren dat u eerder hebt gemaakt op (Stap 1 > b).

d. Stel de toegestane protocollen in.

e. Klik op Save (Opslaan).

f. Klik op (>) Beleidsweergave om verificatie- en autorisatieregels te configureren.



RADIUS-beleidsset toevoegen

Stap 6. Configureer het RADIUS-verificatiebeleid.

Dit kan worden gedaan via het tabblad Beleid > Beleidssets > Klik (>).

Procedure

a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Definieer de naam van het verificatiebeleid.

c. Stel de voorwaarde voor het verificatiebeleid in en selecteer het apparaattype dat u eerder hebt gemaakt (Stap 1 > b).

d. Stel het gebruik van het verificatiebeleid voor de identiteitsbron in.

e. Klik op Save (Opslaan).

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring policy sets. The main content area displays a table of policy sets under the heading 'Authentication Policy(2)'. The table has columns for Status, Rule Name, Conditions, Use, Hits, and Actions. The first row is 'DNAC - Authentication' with a condition 'DEVICE Device Type EQUALS All Device Types#DNAC-Servers'. The 'Use' column for this row shows 'Internal Users'. The 'Save' button at the bottom right is highlighted with a red circle labeled 'e'. Other elements are labeled with red letters: 'b' for the status icon, 'c' for the condition, 'd' for the user selection dropdown, and 'e' for the save button.

RADIUS-verificatiebeleid toevoegen

Stap 7. Configureer het RADIUS-autorisatiebeleid.

Dit kan worden gedaan via het tabblad Beleid > Beleidssets> Klik op (>).

Deze stap om een autorisatiebeleid te maken voor elke gebruikersrol:

- SUPER-ADMIN-ROL
- NETWERKBEHEERROL
- DevOps-Role

Procedure

a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Definieer de naam van het autorisatiebeleid.

c. Stel de voorwaarde voor het autorisatiebeleid in en selecteer de gebruikersgroep die u in hebt gemaakt (Stap 3).

d. Stel de resultaten/profielen van het autorisatiebeleid in en selecteer het autorisatieprofiel dat u hebt gemaakt in (Stap 2).

e. Klik op Save (Opslaan).

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a policy set. The main table lists policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. Below this, a detailed view of a policy rule is shown with columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. Red boxes and letters 'a' through 'e' highlight specific elements: 'a' is a gear icon for configuration, 'b' is the rule name, 'c' is the condition, 'd' is the profile, and 'e' is the save button.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	DNAC - Policy		DEVICE-Device Type EQUALS All Device Types#DNAC-Servers	Default Network Access	0

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Super Admin	IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr...	Select from list	0	⚙️
●	Network Admin	IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Network-Admin_Role_...	Select from list	0	⚙️
●	DevOps	IdentityGroup-Name EQUALS User Identity Groups:DevOps	DevOps-Profile	Select from list	0	⚙️
●	Default		DenyAccess	Select from list	0	⚙️

Toepassingsbeleid toevoegen

(Optie2) DNAC externe verificatie configureren met behulp van TACACS+

Stap 1. (optioneel) Definieer een aangepaste rollen.

Configureer uw aangepaste rollen die aan uw eis voldoen, in plaats daarvan kunt u de standaard gebruikersrollen gebruiken. Dit kan worden gedaan via het tabblad **Systeem > Gebruikers & rollen > Role Based Access Control**.

Procedure

a. Creëer een nieuwe rol.

Cisco DNA Center Create a User Role

Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

1

Role Name*

Describe the role (optional)

2

[Exit](#) [Next](#)

SecOPS Rol Naam

b. Definieer de toegang.

Cisco DNA Center Create a User Role

Define the Access

1

These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to [Learn More](#).

Define the **SecOps-Role** role. Custom roles permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.

> Network Analytics	<input type="radio"/> Deny <input type="radio"/> Read <input checked="" type="radio"/> Write	Access to Network Analytics related components.
> Network Design	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
> Network Provision	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input checked="" type="radio"/> Write	Configure, upgrade, provision and manage your network devices.
> Network Services	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure additional capabilities on the network beyond basic network connectivity and access.
> Platform	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input checked="" type="radio"/> Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
> Security	<input type="radio"/> Deny <input type="radio"/> Read <input checked="" type="radio"/> Write	Manage and control secure access to the network.
> System	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.
> Utilities	<input checked="" type="radio"/> Deny <input checked="" type="radio"/> Read <input checked="" type="radio"/> Write	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.

2

[Exit](#) [Review](#) [Back](#) [Next](#)

SecOPS roltoegang

c. Maak de nieuwe rol aan.

Cisco DNA Center Create a User Role

Summary

Review the **SecOps-Role** role. Make sure all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section.

Role Name & Description [Edit](#)

Role Name	SecOps-Role
Role Description	

Role Capability [Edit](#)

ASSURANCE

Monitoring and Troubleshooting	Deny
Monitoring Settings	Deny
Troubleshooting Tools	Deny

NETWORK ANALYTICS

Data Access	Write
-------------	-------

NETWORK DESIGN

Advanced Network Settings	Deny
Image Repository	Deny
Network Hierarchy	Deny
Network Profiles	Deny
Network Settings	Deny
Virtual Network	Deny

[Exit](#) [Back](#) [Create Role](#)

Samenvatting van SecOps-rol

Cisco DNA Center Create a User Role

PnP	Deny
Provision	Deny

NETWORK SERVICES

App Hosting	Deny
Bonjour	Deny
Stealthwatch	Deny
Umbrella	Deny

PLATFORM

APIs	Write
Bundles	Deny
Events	Deny
Reports	Deny

SECURITY

Group-Based Policy	Write
IP Based Access Control	Write
Security Advisories	Write

SYSTEM

Machine Reasoning	Deny
System Management	Deny

UTILITIES

Audit Log	Deny
Event Viewer	Read
Network Reasoner	Read

[Exit](#) [Back](#) [Create Role](#) ¹

Rol van selecties bekijken en maken

Stap 2. Configureer externe verificatie met TACACS+.

Dit kan worden gedaan via het tabblad **System > Gebruikers & rollen > Externe verificatie**.

a. Als u externe verificatie in Cisco DNA Center wilt inschakelen, schakelt u het aanvinkvakje **Externe gebruiker inschakelen** in.

b. Stel de AAA-kenmerken in.

Voer Cisco AVPair in het veld AAA-kenmerken in.

c. (Optioneel) Configureer de primaire en secundaire AAA-server.

Zorg ervoor dat het TACACS+-protocol ten minste is ingeschakeld op de primaire AAA-server, of op zowel de primaire als de secundaire server.

The screenshot shows the 'External Authentication' configuration page in Cisco DNA Center. The page is titled 'System / Users & Roles'. The left sidebar shows 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area has a heading 'External Authentication' and a sub-heading 'External Authentication'. Below this, there is a section for 'Enable External User' with a checkbox that is checked and highlighted with a red box and the letter 'a'. Below that is a section for 'AAA Attribute' with a dropdown menu set to 'Cisco-AVPair' and highlighted with a red box and the letter 'b'. Below that is a section for 'AAA Server(s)' with two columns for 'Primary AAA Server' and 'Secondary AAA Server'. Both columns have 'IP Address' set to 'ISE Server 1 IP' and 'ISE Server 2 IP' respectively, and 'Shared Secret' set to '*****'. The 'TACACS+' protocol is selected for both servers, highlighted with a red box and the letter 'c'. There are 'Reset to Default' and 'Update' buttons at the bottom of the configuration area.

Configuratiestappen (TACACS+) externe verificatie

(Optie 2) ISE-configuratie voor TACACS+

Stap 1. Schakel de Apparaatbeheerservice in.

Dit kan worden gedaan via het tabblad Beheer > System > Implementatie > Bewerken (ISE-PSN-knooppunt) > Controleren of Apparaatbeheerservice is ingeschakeld.

The screenshot shows the 'Administration / System' configuration page in Identity Services Engine. The page has a top navigation bar with 'Administration / System' and a search icon. The left sidebar shows 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', 'Work Centers', and 'Interactive Help'. The main content area has a heading 'Administration / System' and a sub-heading 'Administration / System'. Below this, there are several sections for enabling services: 'Administration' (checked), 'Monitoring' (checked), 'Policy Service' (checked), and 'pxGrid' (checked). The 'Enable Device Admin Service' checkbox is checked and highlighted with a red box and the number '1'. The 'Save' button at the bottom right is highlighted with a red box and the number '2'.

Stap 2. Voeg DNAC-server toe als netwerkapparaat op ISE.

Dit kan worden gedaan via het tabblad Beheer > Netwerkbronnen > Netwerkapparaten.

Procedure

- Definieer (DNAC) naam en IP van netwerkapparaat.
- (Optioneel) Apparaattype classificeren voor voorwaarde beleidsinstelling.
- Schakel TACACS+ verificatie-instellingen in.
- Stel TACACS+ gedeeld geheim in.

The screenshot shows the 'Network Devices' configuration page in the ISE Administration console. The page title is 'Administration / Network Resources'. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is titled 'Network Devices' and includes a 'Network Devices List' dropdown set to 'DNAC'. The form fields are: Name (DNAC), Description, IP Address (DNAC Server IP / 32), Device Profile (Cisco), Model Name, Software Version, Network Device Group, Location (All Locations), and IPSEC (No). The 'Device Type' dropdown is set to 'DNAC-Servers'. The 'TACACS+ Authentication Settings' section is expanded, showing a 'Shared Secret' field with a 'Show' button and a 'Retire' button. The 'Enable Single Connect Mode' section is also visible, with 'Legacy Cisco Device' selected.

ISE-netwerkapparaat (NAC) voor TACACS+

Stap 3. Maak TACACS+ profielen voor elke DNAC rol.

Dit kan worden gedaan via het tabblad Werkcentra > Apparaatbeheer > Beleids-elementen > Resultaten > TACACS-profielen.




Opmerking: 3x TACACS+ profielen maken, één voor elke gebruikersrol.

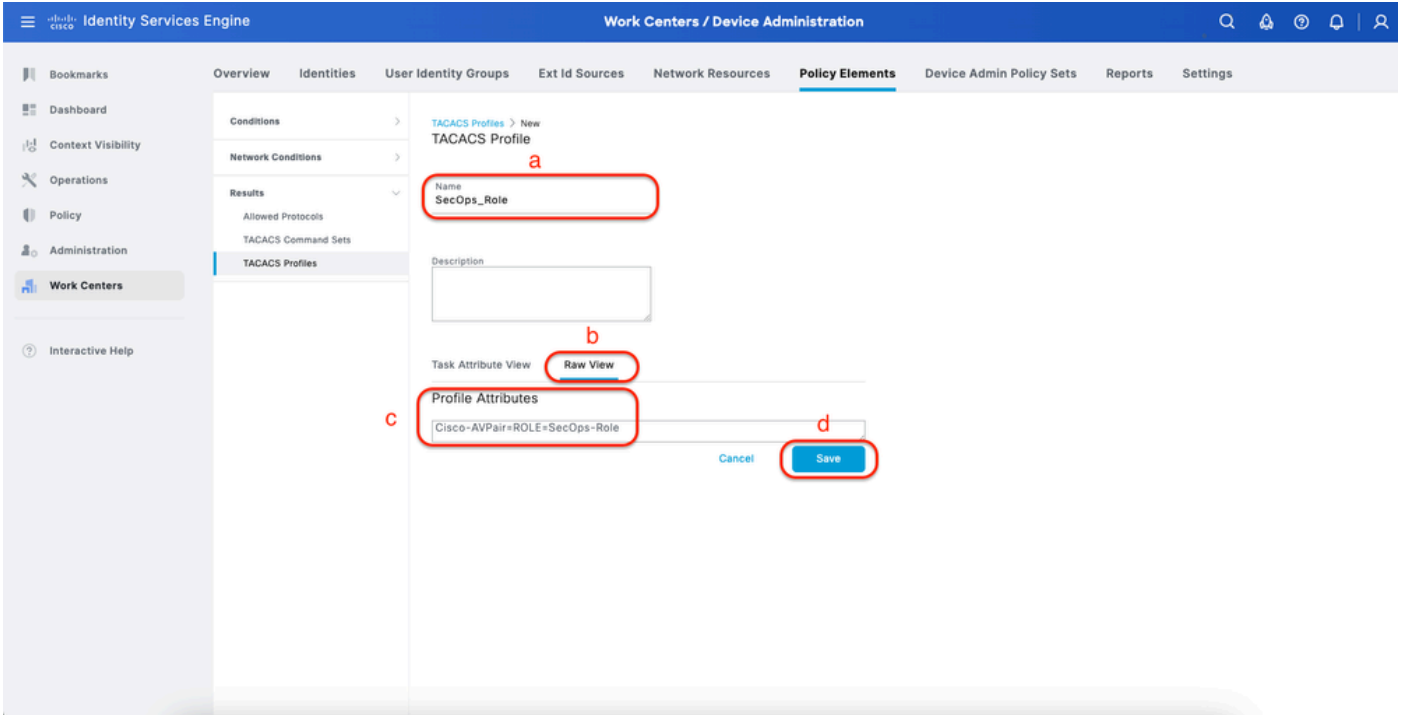
Procedure

- Klik op Add en definieer de naam van het TACACS-profiel.
- Klik op het tabblad Raw View.
- Voer de Cisco-AVPair=ROL= in en vul de juiste gebruikersrol in.
 - Voer voor de gebruikersrol (SecOps-Role) Cisco-AVPair=ROLE=SecOps-Role in.

- Voer voor de gebruikersrol (NETWORK-ADMIN-ROL) Cisco-AVPair=ROLE=NETWORK-ADMIN-ROL in.
- Voer voor de gebruikersrol (SUPER-ADMIN-ROL) Cisco-AVPair=ROLE=SUPER-ADMIN-ROL in.

 **Opmerking:** Vergeet niet dat AVPair value (Cisco-AVPair=ROLE=) een hoofdlettergevoeligheid is en ervoor zorgt dat deze overeenkomt met de DNAC User Role.

d. Klik op Save (Opslaan).



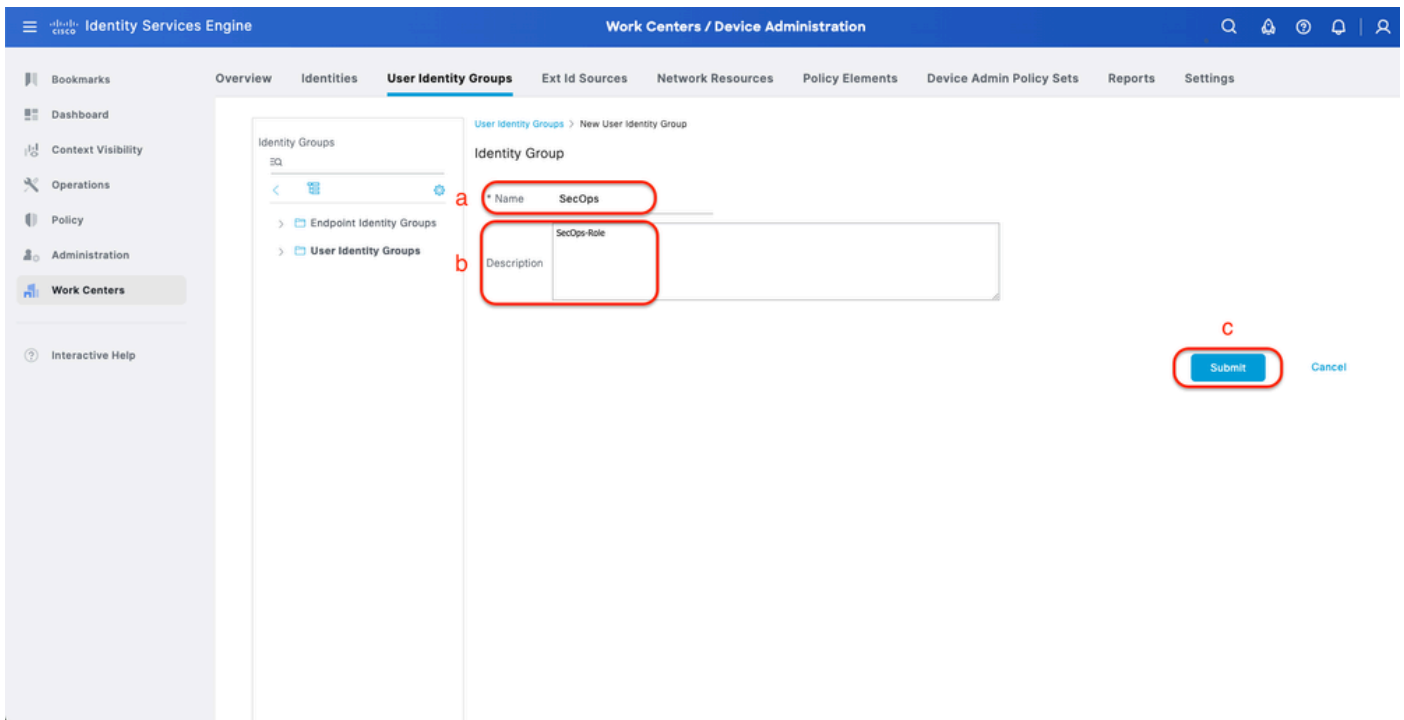
TACACS-profiel maken (secOps_Role)

Stap 4. Gebruikersgroep maken.

Dit kan worden gedaan via het tabblad Workcenters > Apparaatbeheer > Gebruikersidentiteitsgroepen.

Procedure

- Klik op Add en definieer de naam van de identiteitsgroep.
- (Optioneel) Definieer de beschrijving.
- Klik op Verzenden.



Gebruikersidentiteitsgroep maken

Stap 5. Lokale gebruiker maken.

Dit kan worden gedaan via het tabblad Work Centers > Apparaatbeheer > Identiteiten > Gebruikers.

Procedure

- a. Klik op Add en definieer de gebruikersnaam.
- b. Stel het inlogwachtwoord in.
- c. Voeg de gebruiker toe aan de verwante gebruikersgroep.
- d. Klik op Verzenden.

Lokale gebruiker maken 1-2

Lokale gebruiker maken 2-2

Stap 6. (optioneel) Voeg een TACACS+ beleidsset toe.

Dit kan worden gedaan via het tabblad Werkcentra > Apparaatbeheer > Apparaatbeheerbeleidssets.

Procedure

a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Bepaal de naam van de beleidsset.

c. Stel de Policy Set Condition in op Selecteer Apparaattype dat u eerder hebt gemaakt op (Stap 2 > b).

d. Stel de toegestane protocollen in.

e. Klik op Save (Opslaan).

f. Klik op (>) Beleidsweergave om verificatie- en autorisatieregels te configureren.

The screenshot shows the Cisco Identity Services Engine (ISE) Policy Sets configuration page. The page title is "Policy / Policy Sets". The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Help. The main content area displays a table of Policy Sets. The table has columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The first row is "DNAC - Policy" with a status of "On". The condition is "DEVICE-Device Type EQUALS All Device Types#DNAC-Servers". The allowed protocols are "Default Network Access". The view icon is a right-pointing arrow. A "Save" button is circled in red and labeled 'e'.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
On	DNAC - Policy		DEVICE-Device Type EQUALS All Device Types#DNAC-Servers	Default Network Access	0		>
On	Default	Default policy set		Default Network Access	0		>

Reeks TACACS+ beleid toevoegen

Stap 7. Configuratie van het TACACS+-verificatiebeleid.

Dit kan worden gedaan via het tabblad Werkcentra > Apparaatbeheer > Beleidssets voor Apparaatbeheer > Klik op (>).

Procedure

a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Definieer de naam van het verificatiebeleid.

c. Stel de voorwaarde voor het verificatiebeleid in en selecteer het apparaattype dat u eerder hebt gemaakt (Stap 2 > b).

d. Stel het gebruik van het verificatiebeleid voor de identiteitsbron in.

e. Klik op Save (Opslaan).

The screenshot displays the Cisco Identity Services Engine (ISE) Work Centers / Device Administration interface. The main content area shows the 'Policy Sets' configuration for 'DNAC - Policy'. A table lists policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. The 'DNAC - Authentication' policy set is highlighted with a red box labeled 'b'. Its conditions are 'DEVICE-Device Type EQUALS All Device Types#DNAC-Servers', highlighted with a red box labeled 'c'. The 'Use' column shows 'Internal Users' selected, highlighted with a red box labeled 'd'. A 'Save' button is highlighted with a red box labeled 'e'.

Tacacs+-verificatiebeleid toevoegen

Stap 8. Configureer het beleid voor TACACS+ autorisatie.

Dit kan worden gedaan via het tabblad Workcenters > Apparaatbeheer > Apparaatbeheerbeleidsets > Klik op (>).

Deze stap om een autorisatiebeleid te maken voor elke gebruikersrol:

- SUPER-ADMIN-ROL
- NETWERKBEHEERROL
- Tweede rol

Procedure

a. Klik op Acties en kies (Nieuwe rij hierboven invoegen).

b. Definieer de naam van het autorisatiebeleid.

c. Stel de voorwaarde voor het autorisatiebeleid in en selecteer de gebruikersgroep die u in hebt gemaakt (Stap 4).

d. Stel het Shell-profiel van het autorisatiebeleid in en selecteer TACACS-profiel dat u in (Stap 3) hebt gemaakt.

e. Klik op Save (Opslaan).

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

Search

DNAC - Policy DEVICE Device Type EQUALS All Device Types#DNAC Default Device Admin

> Authentication Policy(2)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
v Authorization Policy(1)

Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
✓	Super Admin	IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN	Select from list	SUPER_ADMIN_ROLE	0	⚙️
✓	Network Admin	IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Select from list	NETWORK_ADMIN_ROLE	0	⚙️
✓	SecOps	IdentityGroup-Name EQUALS User Identity Groups:SecOps	Select from list	SecOps_Role	0	⚙️
✓	Default		DenyAllCommands	Deny All Shell Profile	0	⚙️

Reset **Save**

Toepassingsbeleid toevoegen

Verifiëren

Controleer de RADIUS-configuratie

1- DNAC - Display Externe Gebruikers Systeem > Gebruikers & Rollen > Externe Verificatie > Externe Gebruikers.

U kunt de lijst bekijken van externe gebruikers die voor het eerst via RADIUS zijn aangemeld. De informatie die wordt weergegeven omvat hun gebruikersnamen en rollen.

Cisco DNA Center System / Users & Roles

User Management
Role Based Access Control
External Authentication

External Authentication

Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute here on Cisco DNA Center is the name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on Cisco DNA Center.

The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1". On ISE server, choose the cisco-av-pair attribute from cisco specific AAA attributes list. A sample configuration inside Authorization profile would look like "cisco-av-pair Role=SUPER-ADMIN-ROLE".

An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".

Enable External User

AAA Attribute
Cisco-AVPair

Reset to Default Update

AAA Server(s)

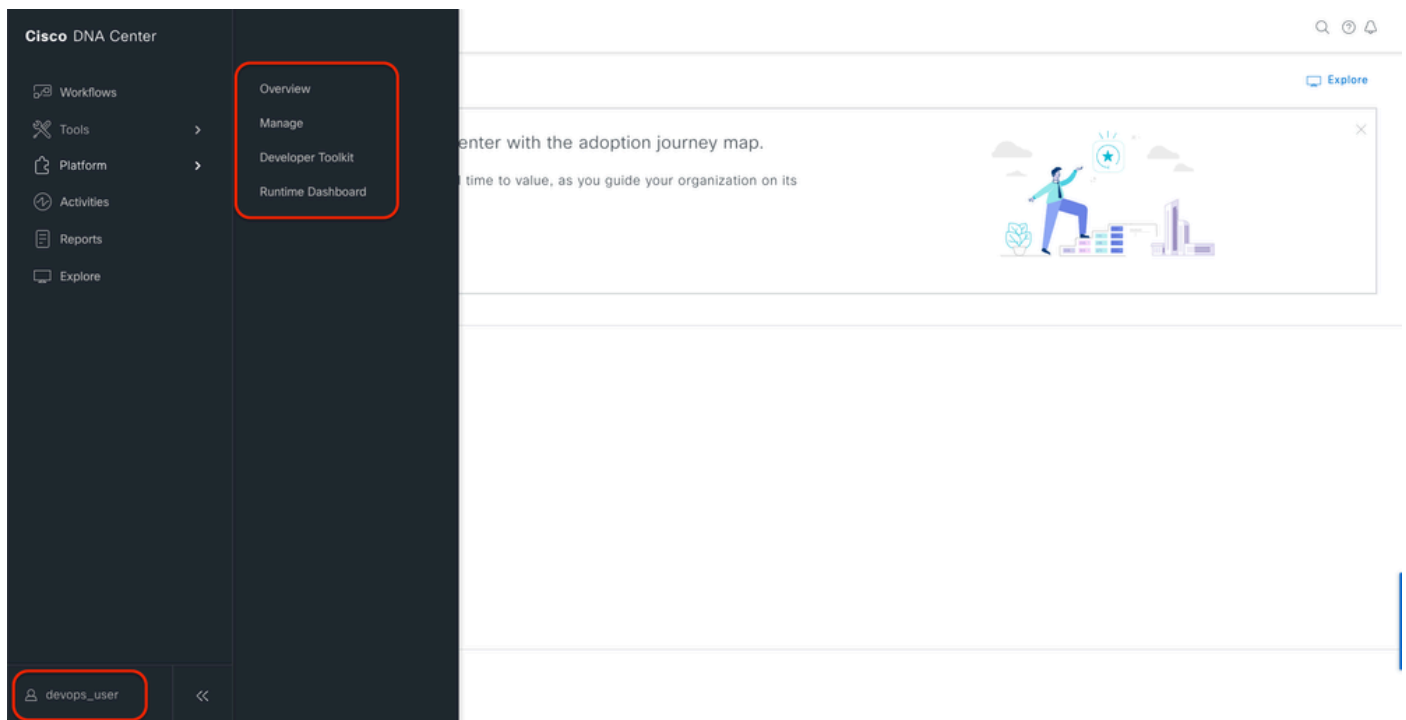
External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

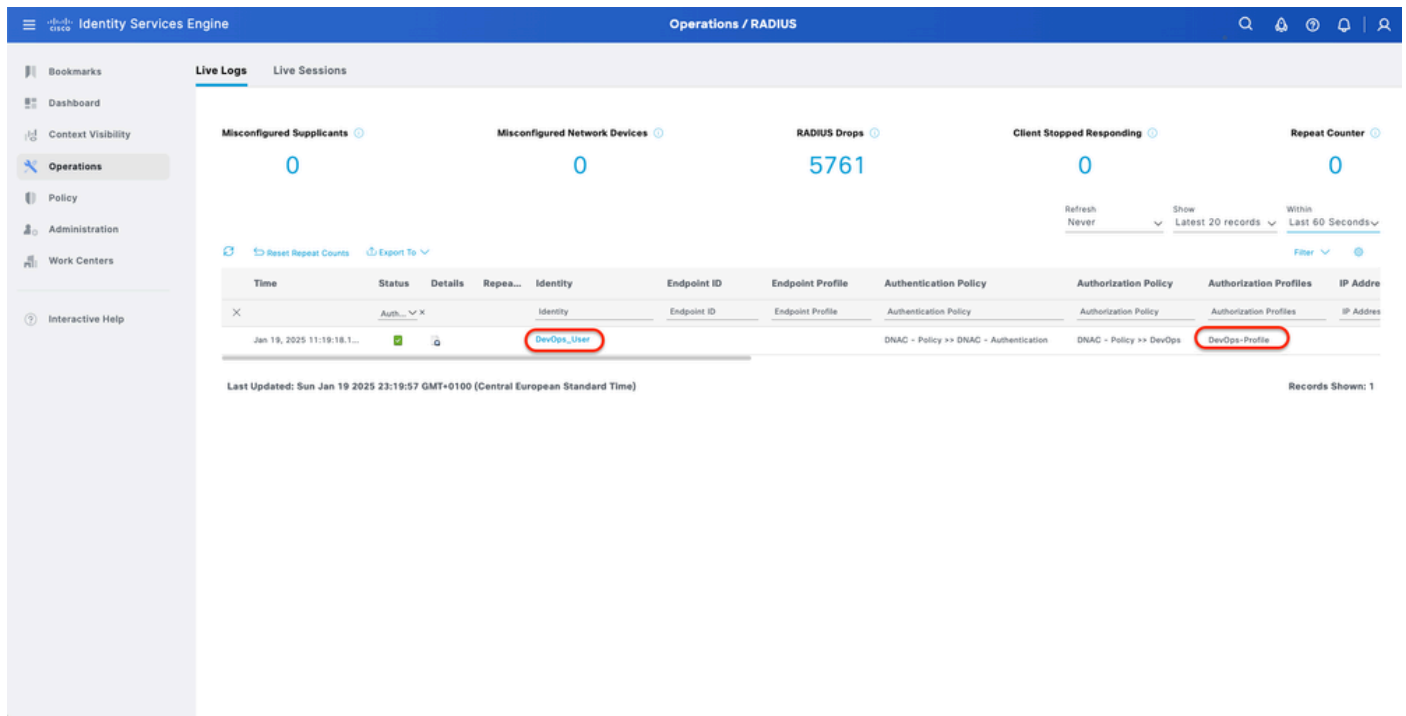
Externe gebruikers

2. DNAC - Bevestig de toegang van gebruikers.



Beperkte gebruikerstoegang

3.a ISE - RADIUS Live-logs Operations > RADIUS > Live-logs.



RADIUS live-logs

3.b ISE - RADIUS Live-logs Operations > RADIUS > Live-logs > Klik (Details) voor autorisatielogboek.

Cisco ISE

Overview

Event: 5200 Authentication succeeded

Username: DevOps_User

Endpoint Id:

Endpoint Profile:

Authentication Policy: DNAC - Policy >> DNAC - Authentication

Authorization Policy: DNAC - Policy >> DevOps

Authorization Result: DevOps-Profile

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11015	An Access-Request MUST contain at least a NAS-IP-Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing	1
11117	Generated a new session ID	2
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	2
15041	Evaluating Identity Policy	3
15048	Queried PIP - DEVICE.Device Type	4
15013	Selected Identity Source - Internal Users	3
24210	Looking up User in Internal Users IDStore - DevOps_User	0
24212	Found User in Internal Users IDStore	8
22037	Authentication Passed	1
15036	Evaluating Authorization Policy	1
15016	Selected Authorization Profile - DevOps-Profile	5
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	1
11002	Returned RADIUS Access-Accept	0

Authentication Details

Source Timestamp: 2025-01-19 23:19:18.156

Received Timestamp: 2025-01-19 23:19:18.156

Policy Server: ise34

Event: 5200 Authentication succeeded

Username: DevOps_User

User Type: User

Authentication Identity Store: Internal Users

Identity Group: User Identity Groups:DevOps

Authentication Method: PAP_ASCII

Authentication Protocol: PAP_ASCII

Network Device: DNAC

Device Type: All Device Types#DNAC-Servers

Location: All Locations

RADIUS gedetailleerde Live-logs 1-2

Cisco ISE

IdentityPolicyMatchedRule: DNAC - Authentication

AuthorizationPolicyMatchedRule: DevOps

ISEPolicySetName: DNAC - Policy

IdentitySelectionMatchedRule: DNAC - Authentication

TotalAuthnLatency: 35

ClientLatency: 0

DTLSSupport: Unknown

Network Device Profile: Cisco

Location: Location#All Locations

Device Type: Device Type#All Device Types#DNAC-Servers

IPSEC: IPSEC#Is IPSEC Device#No

Name: User Identity Groups:DevOps

EnableFlag: Enabled

RADIUS Username: DevOps_User

Device IP Address:

CPMSessionID: 0a301105095d4kCbv7kMBCoFkesRrFcdXec0uEqPP8RtG/WY

CiscoAVPair: AuthenticationIdentityStore=Internal Users, FQSubjectName=92731e30-8c01-11e6-996c-525400b48521#devops_user, UniqueSubjectID=9b4d28083db66a1f8bcc98565c8f5eaa5dedf467

Result

Class: CACS:0a301105095d4kCbv7kMBCoFkesRrFcdXec0uEqPP8RtG/WY:ise34/528427220/15433

cisco-av-pair ROLE=DevOps-Role

RADIUS gedetailleerde Live-logs 2-2

Controleer de TACACS+ configuratie

1- DNAC - Display Externe Gebruikers Systeem > Gebruikers & Rollen > Externe Verificatie > Externe Gebruikers.

U kunt de lijst bekijken van externe gebruikers die voor het eerst via TACACS+ zijn ingelogd. De informatie die wordt weergegeven omvat hun gebruikersnamen en rollen.

Cisco DNA Center System / Users & Roles

User Management
Role Based Access Control
External Authentication

AAA Attribute
Cisco-AVPair

Reset to Default Update

AAA Server(s)

Primary AAA Server Secondary AAA Server

IP Address IP Address

Shared Secret Shared Secret

View Advanced Settings View Advanced Settings

Update Update

External Users

Filter EQ Find

Username	Role	Action
secops_user	SecOps-Role	Delete

Showing 1 of 1

Externe gebruikers

2. DNAC - Bevestig de toegang van gebruikers.

Cisco DNA Center

Policy >
Workflows >
Tools >
Platform >
Activities >
Explore

Group-Based Access Control
IP & URL Based Access Control

center with the adoption journey map.
time to value, as you guide your organization on its

Network Bug Identifier
Identify bugs in the network

secops_user

Beperkte gebruikerstoegang

3.a ISE - TACACS+ Live-Logs Work Centers > Apparaatbeheer > Overzicht > TACACS LiveLog.

Identity Services Engine Operations / TACACS

Live Logs

Refresh Never Show Latest 20 records Within Last 60 Seconds

Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Shell Profile	Device Type	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#All Device Types#DNAC...	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#All Device Types#DNAC...	Lo

Last Updated: Sun Jan 19 2025 17:16:38 GMT+0100 (Central European Standard Time) Records Shown: 2

Live logs voor TACACS

3.b ISE - gedetailleerde TACACS+ Live-Logs Work Centers > Apparaatbeheer > Overzicht > TACACS Livelog > Klik (Details) voor autorisatielogboek.

Cisco ISE

Overview

Request Type: Authorization
 Status: Pass
 Session Key: ise34/526427220/13958
 Message Text: Device-Administration: Session Authorization succeeded
 Username: SecOps_User
 Authorization Policy: DNAC - Policy >> SecOps
 Shell Profile: SecOps_Role
 Matched Command Set
 Command From Device

Authorization Details

Generated Time: 2025-01-19 17:12:43.368 +1:00
 Logged Time: 2025-01-19 17:12:43.368
 Epoch Time (sec): 1737303163
 ISE Node: ise34
 Message Text: Device-Administration: Session Authorization succeeded
 Failure Reason
 Resolution
 Root Cause
 Username: SecOps_User
 Network Device Name: DNAC

Steps

Step ID	Description	Latency (ms)
13005	Received TACACS+ Authorization Request	
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	4
15041	Evaluating Identity Policy	7
15013	Selected Identity Source - Internal Users	5
24210	Looking up User in Internal Users IDStore	1
24212	Found User in Internal Users IDStore	4
22037	Authentication Passed	0
15036	Evaluating Authorization Policy	0
15048	Queried PIP - Network Access.UserName	10
15048	Queried PIP - IdentityGroup.Name	2
15017	Selected Shell Profile	2
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	0
13034	Returned TACACS+ Authorization Reply	0

Gedetailleerde live-logs 1-2 voor TACACS+

Type	Value
Service-Argument	cas-service
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
RequestLatency	38
IdentityGroup	User Identity Groups:SecOps
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	13004827410.62.150.14628131Authorization130048274
IdentitySelectionMatchedRule	DNAC - Authentication
StepLatency	1=1;2=1;3=4;4=7;5=5;6=1;7=4;8=0;9=0;10=10;11=2;12=2;13=1;14=0;15=0
TotalAuthenLatency	38
ClientLatency	0
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:SecOps
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Cisco-AVPair=ROLE+SecOps-Role; }

Gedetailleerde live-logs 2-2 voor TACACS+

Problemen oplossen

Er is momenteel geen specifieke diagnostische informatie beschikbaar voor deze configuratie.

Referenties

- [Beheerdershandleiding voor Cisco Identity Services Engine, release 3.4 > Apparaatbeheer](#)
- [Beheerdershandleiding Cisco DNA Center, release 2.3.5](#)
- [Cisco DNA Center: Rol-gebaseerde toegangscontrole met externe verificatie](#)

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.