Autorisatie van ISE 2.0-opdracht voor TACACS+ verificatie configureren

Inhoud

Inleiding

Dit document beschrijft hoe u een TACACS+ verificatie- en opdrachtautorisatie kunt configureren op basis van het groepslidmaatschap van Microsoft Active Directory (AD).

Achtergrondinformatie

Om Tacacs+ verificatie en opdrachtautorisatie te configureren op basis van Microsoft Active Directory (AD)-groepslidmaatschap van een gebruiker met Identity Service Engine (ISE) 2.0 en hoger, gebruikt ISE AD als externe identiteitsopslag om resources op te slaan zoals gebruikers, machines, groepen en kenmerken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS-router is volledig operationeel
- Connectiviteit tussen router en ISE.
- ISE-server is opgestart en heeft een verbinding met Microsoft AD

Gebruikte componenten

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

- Cisco Identity Service Engine 2.0
- Cisco IOS®-softwarerelease 15.4(3)M3
- Microsoft Windows Server 2012 R2

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.

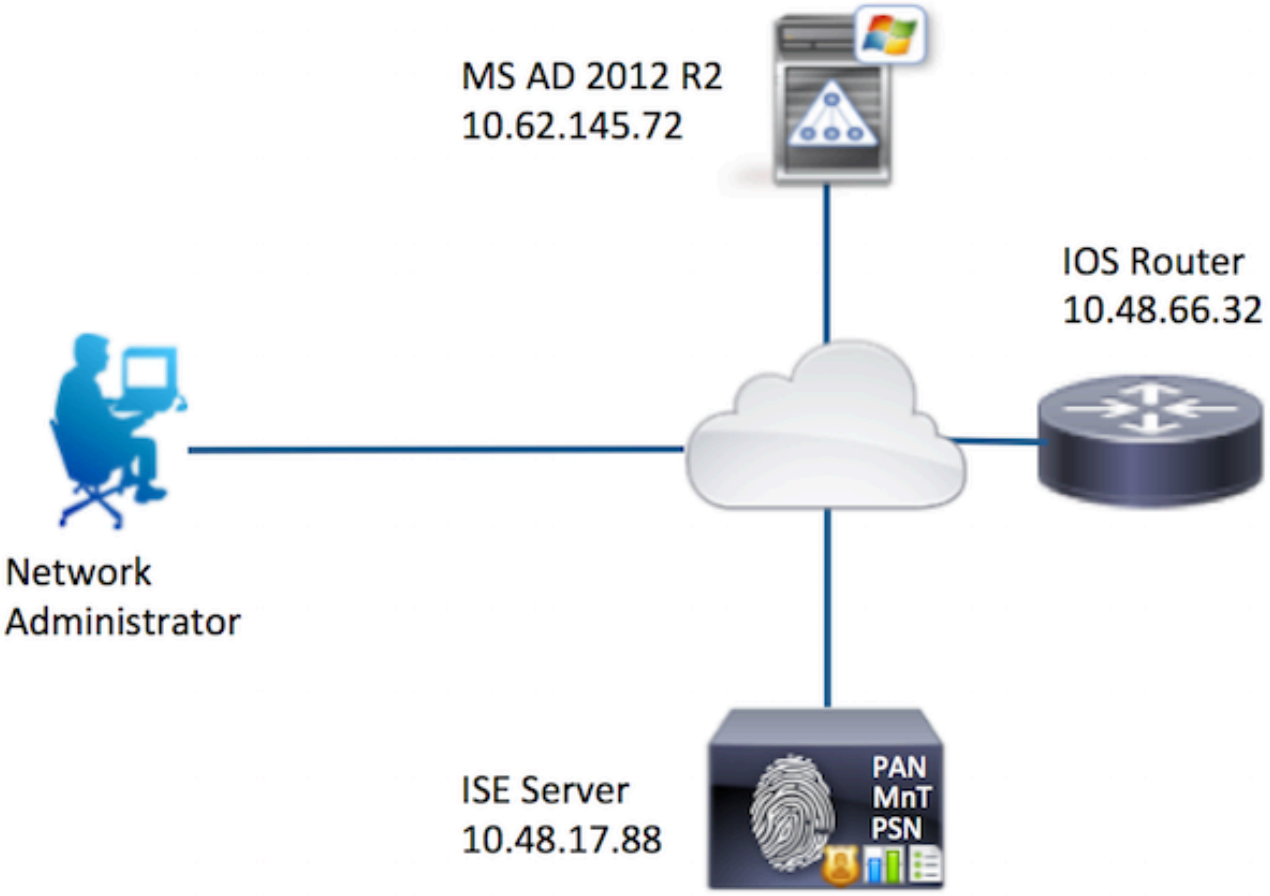
Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

Het doel van de configuratie is:

- Telnet-gebruiker verifiëren via AD
- Machtigen telnet gebruiker zodat het wordt geplaatst in de geprivilegieerde EXEC modus na de login
- Controleer en verstuur elke uitgevoerde opdracht naar ISE voor verificatie

Netwerkdiagram

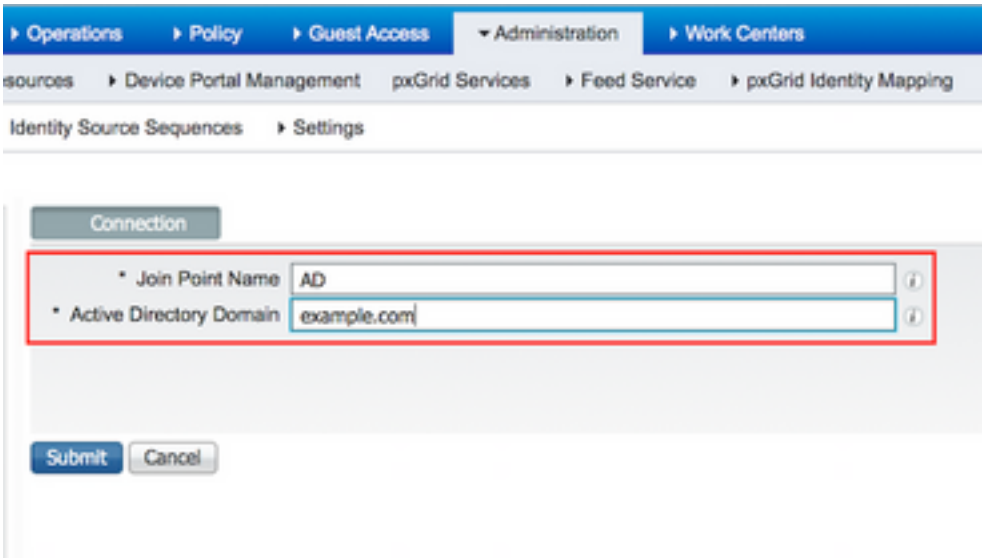


Configuraties

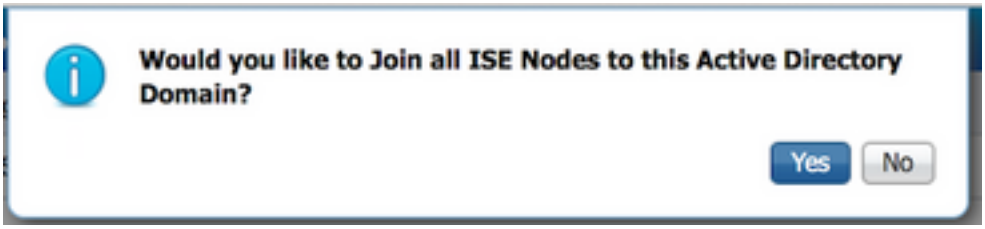
Configureer ISE voor verificatie en autorisatie

Meld u aan bij ISE 2.0 op Active Directory

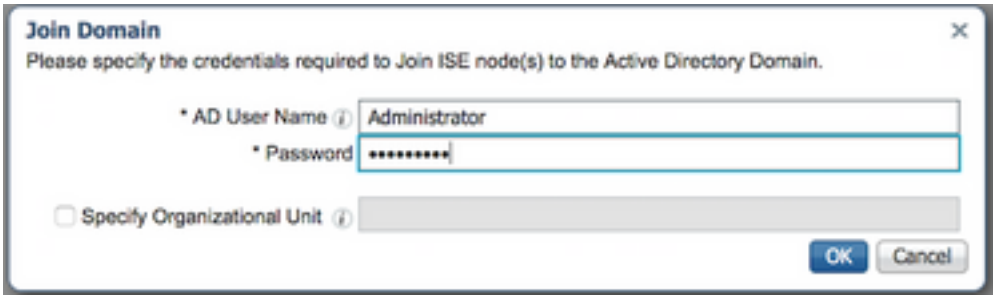
1. Ga naar **Beheer > Identiteitsbeheer > Externe identiteitsopslag > Active Directory > Toevoegen**. Geef de Join Point Name, Active Directory Domain en klik op **Indienen.**



2. Klik op **Ja** wanneer u wordt gevraagd om toe te treden tot alle ISE-knooppunten in dit Active Directory-domein.



3. Typ AD Gebruikersnaam en wachtwoord en klik op **OK**.

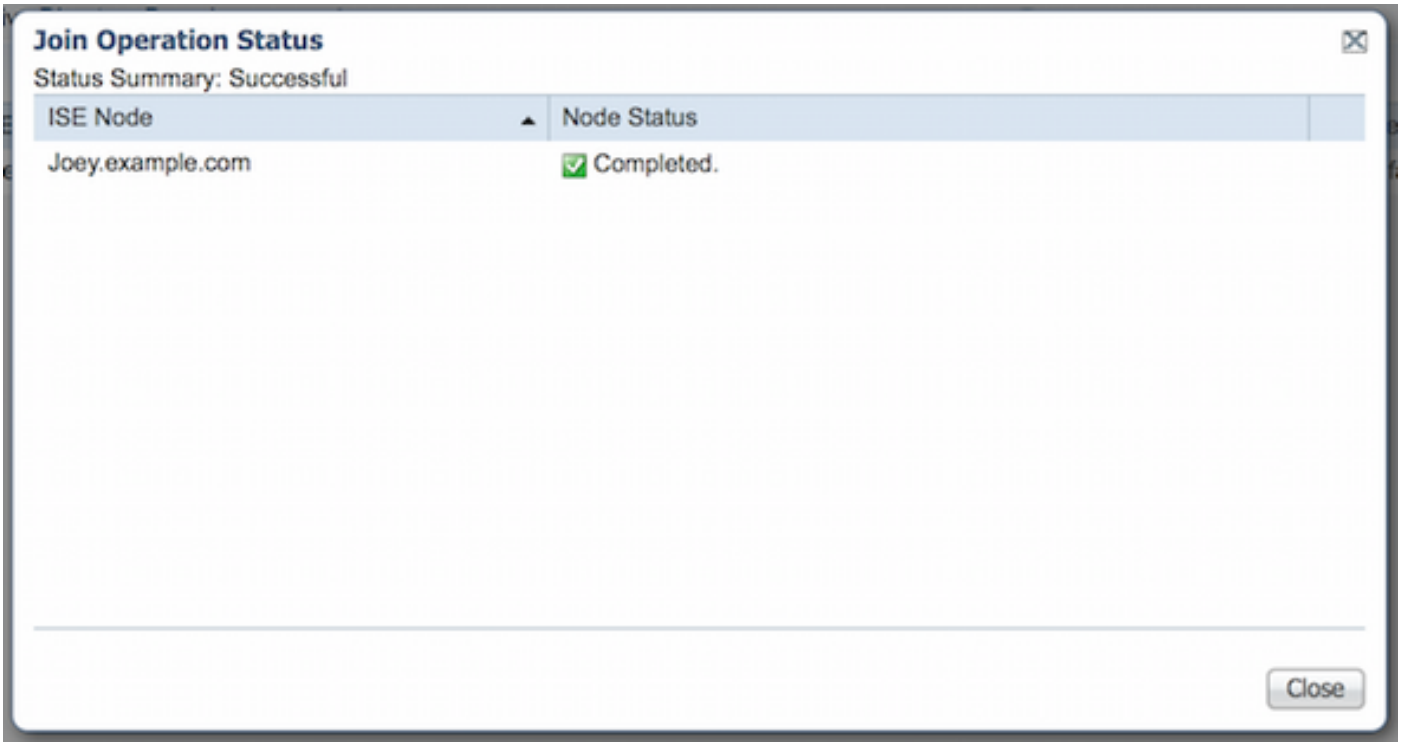


Een AD-account dat vereist is voor domeintoegang in ISE kan een van de volgende zijn:

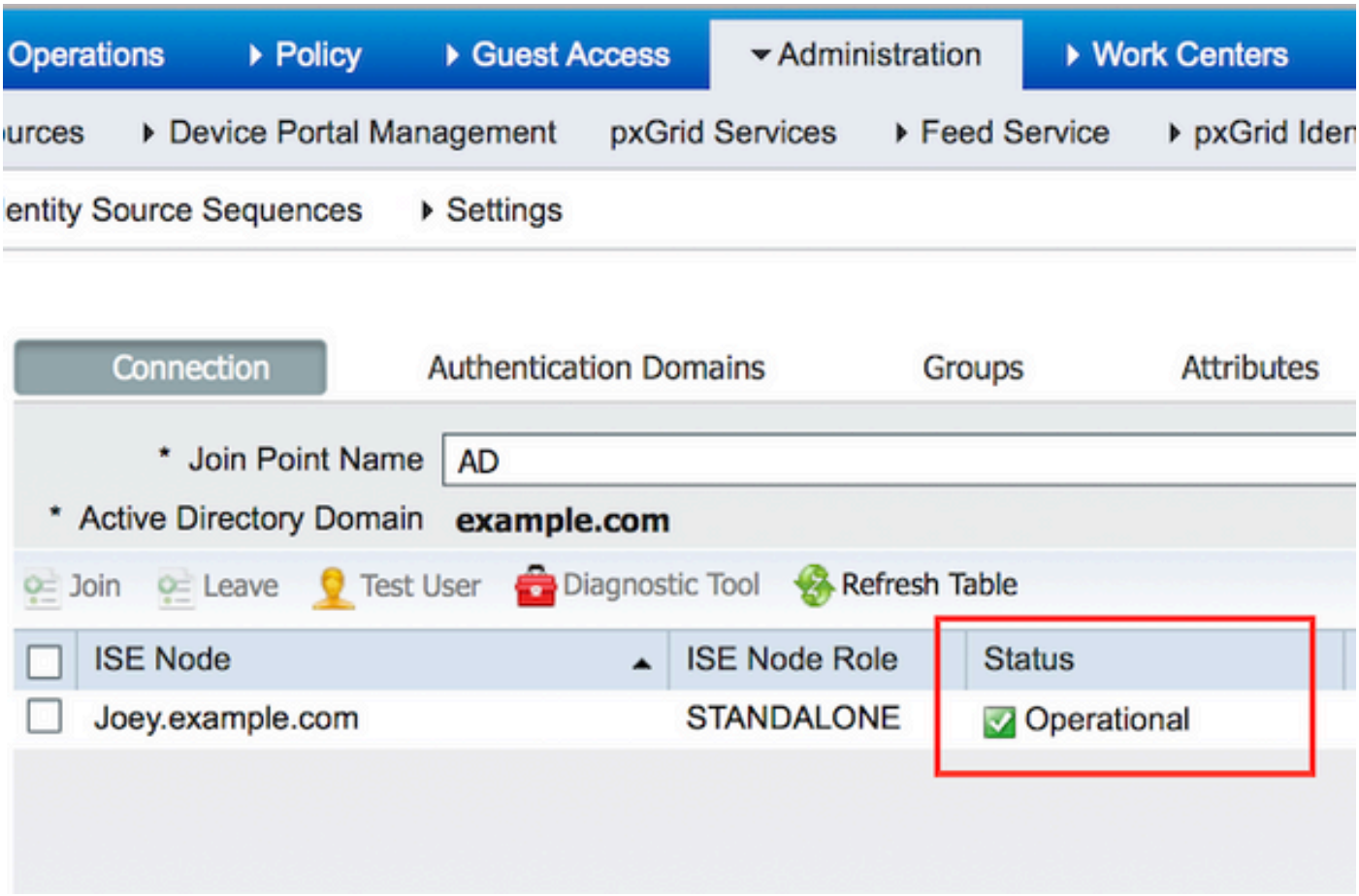
- Voeg werkstations toe aan domeingebruikersrecht in het betreffende domein
- Computer Objects maken of Computer Objects toestemming verwijderen op de respectievelijke computers container waar de account van de ISE-machine is gemaakt voordat deze zich bij de ISE-machine aansluit

Opmerking: Cisco raadt aan het uitsluiting-beleid voor de ISE-account uit te schakelen en de AD-infrastructuur te configureren om waarschuwingen naar de beheerder te verzenden als er een verkeerd wachtwoord voor die account wordt gebruikt. Wanneer het verkeerde wachtwoord is ingevoerd, maakt of wijzigt ISE de machinerekening niet wanneer dit nodig is en ontkent zij daarom mogelijk alle verificaties.

4. Bekijk de status van de bewerking. De status van het knooppunt moet worden weergegeven als voltooid. Klik op **Close** (Sluiten).



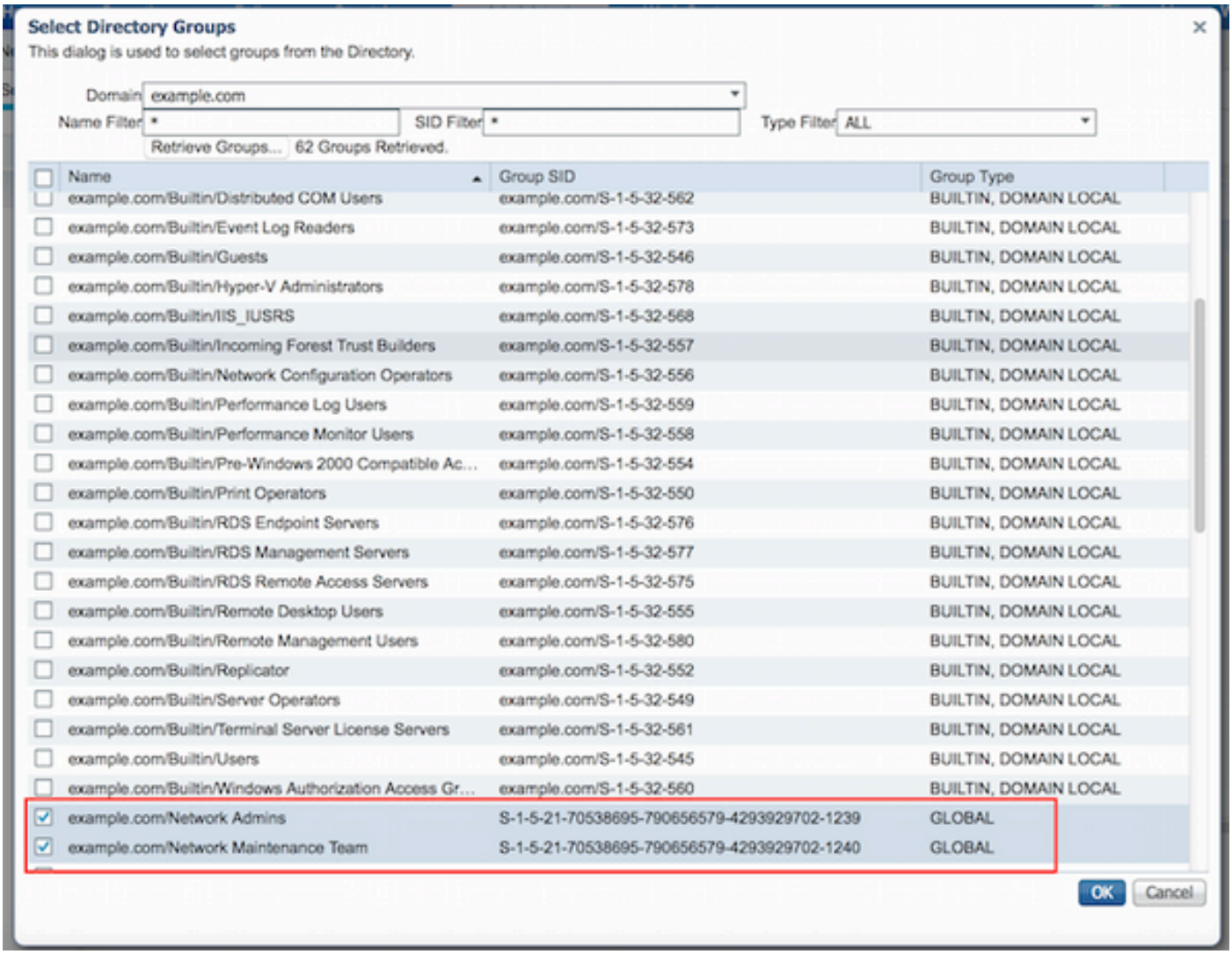
5. De AD-status is operationeel.



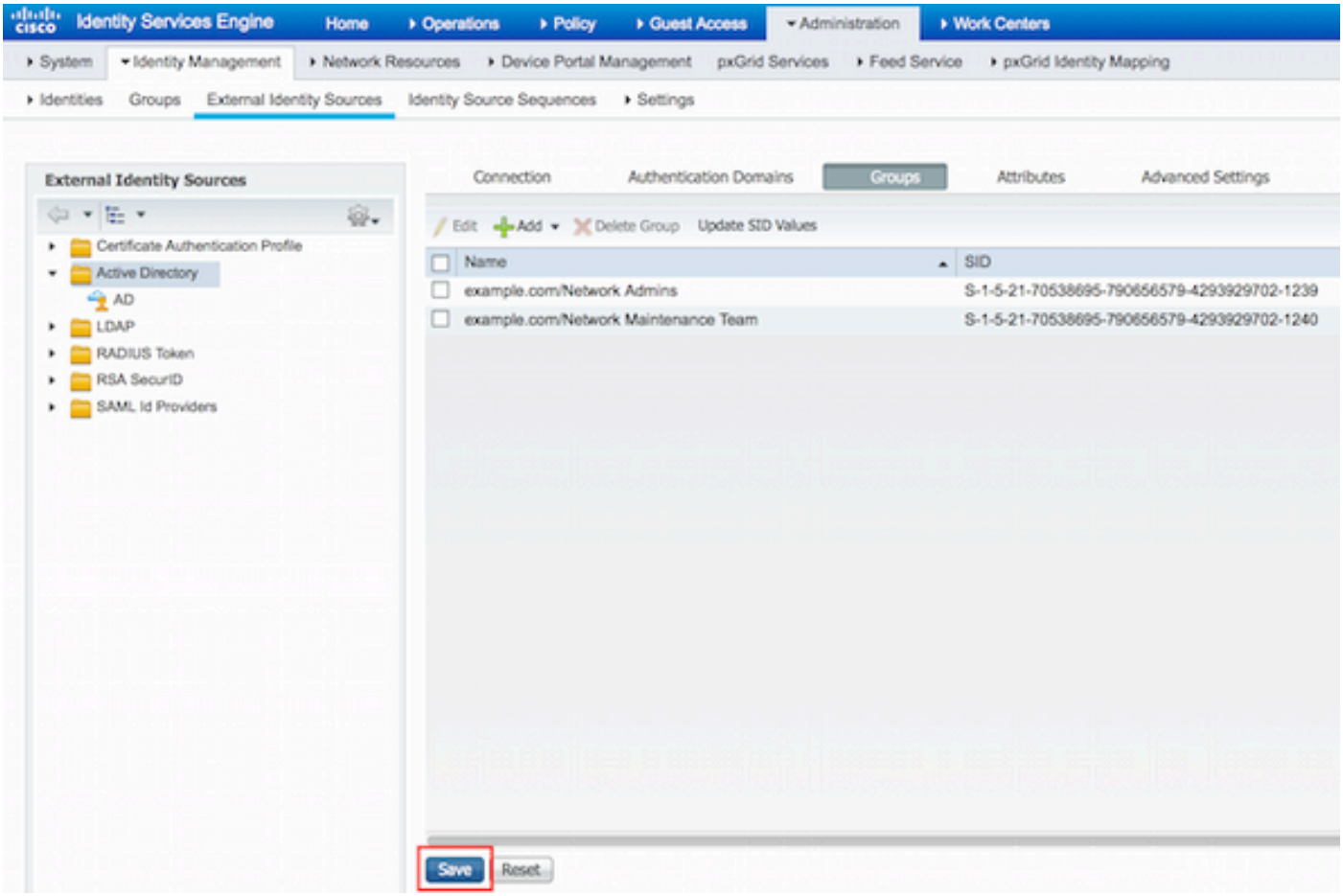
6. Navigeer naar **Groepen > Toevoegen > Groepen selecteren uit map > Groepen ophalen.** Selecteer selectievakjes **Netwerkbeheerders** AD-groep en **Netwerkonderhoudsteam** AD-groep, zoals in deze afbeelding.

> **Opmerking:** Gebruikersbeheerder is lid van de AD-groep Netwerkbeheerders. Deze gebruiker heeft volledige toegangsrechten. Deze gebruiker is lid van Network Maintenance

Team AD Group. Deze gebruiker kan alleen uitvoeren toont opdrachten.

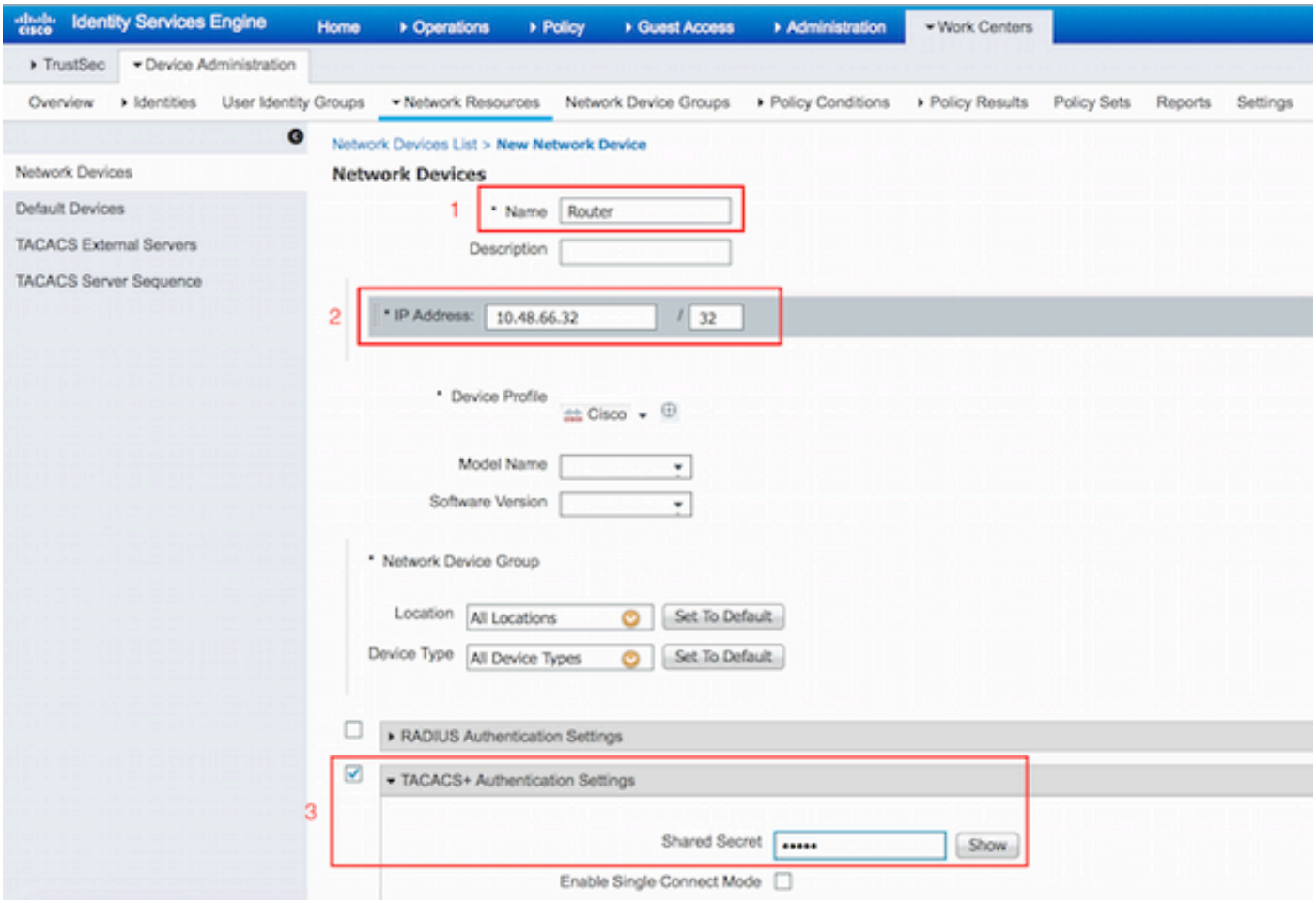


7. Klik op **Opslaan** om teruggewonnen AD-groepen op te slaan.



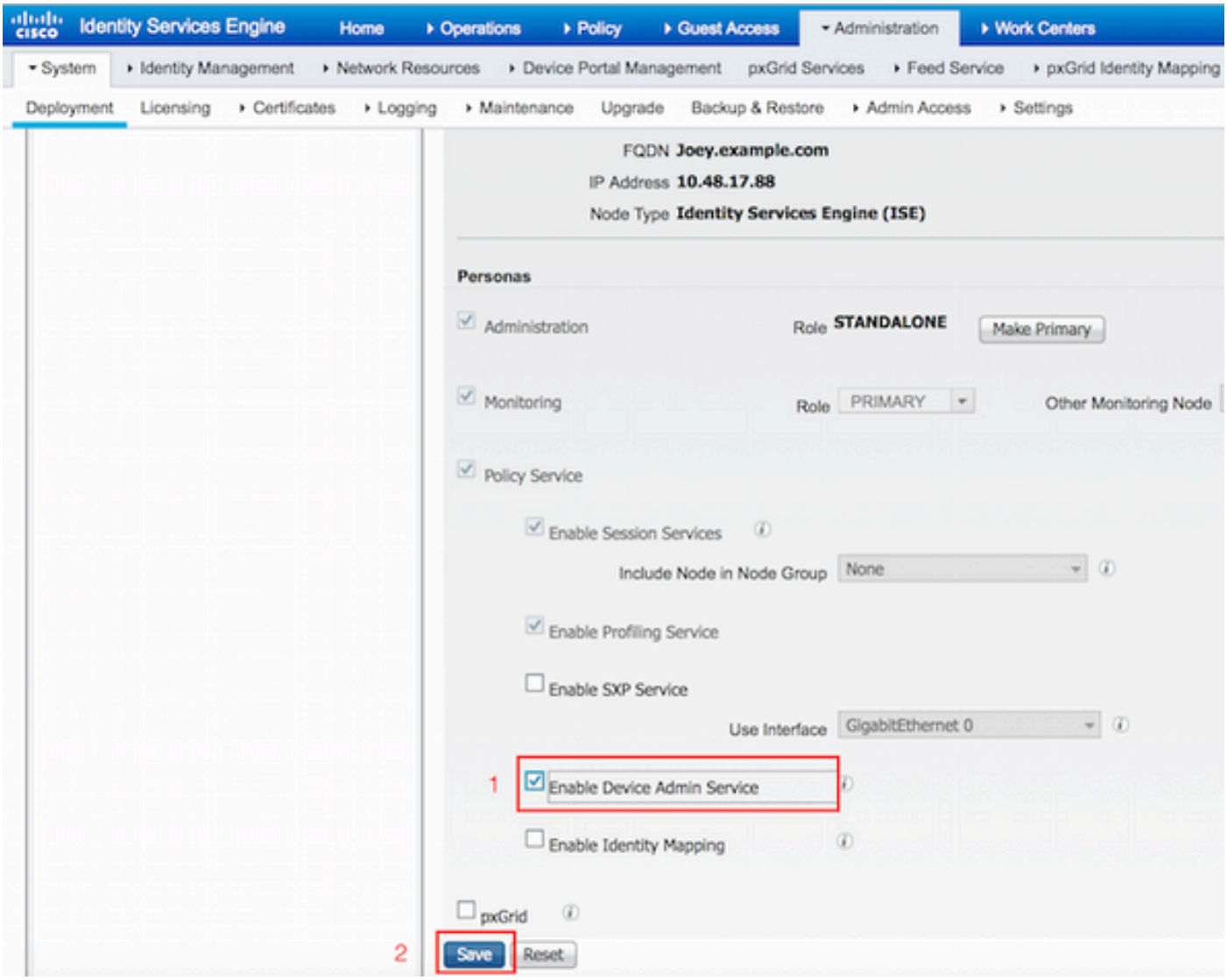
Netwerkapparaat toevoegen

Navigeren naar **werkcentra > Apparaatbeheer > Netwerkbronnen > Netwerkapparaten**. Klik op **Add** (Toevoegen). Geef naam, IP-adres, selecteer het aanvinkvakje **TACACS+ verificatie-instellingen** en geef gedeelde geheime sleutel op.



Service voor apparaatbeheer inschakelen

Ga naar **Beheer > Systeem > Implementatie.** Kies vereist knooppunt. Kies selectievakje **Apparaatbeheer** inschakelen en klik op **Opslaan.**

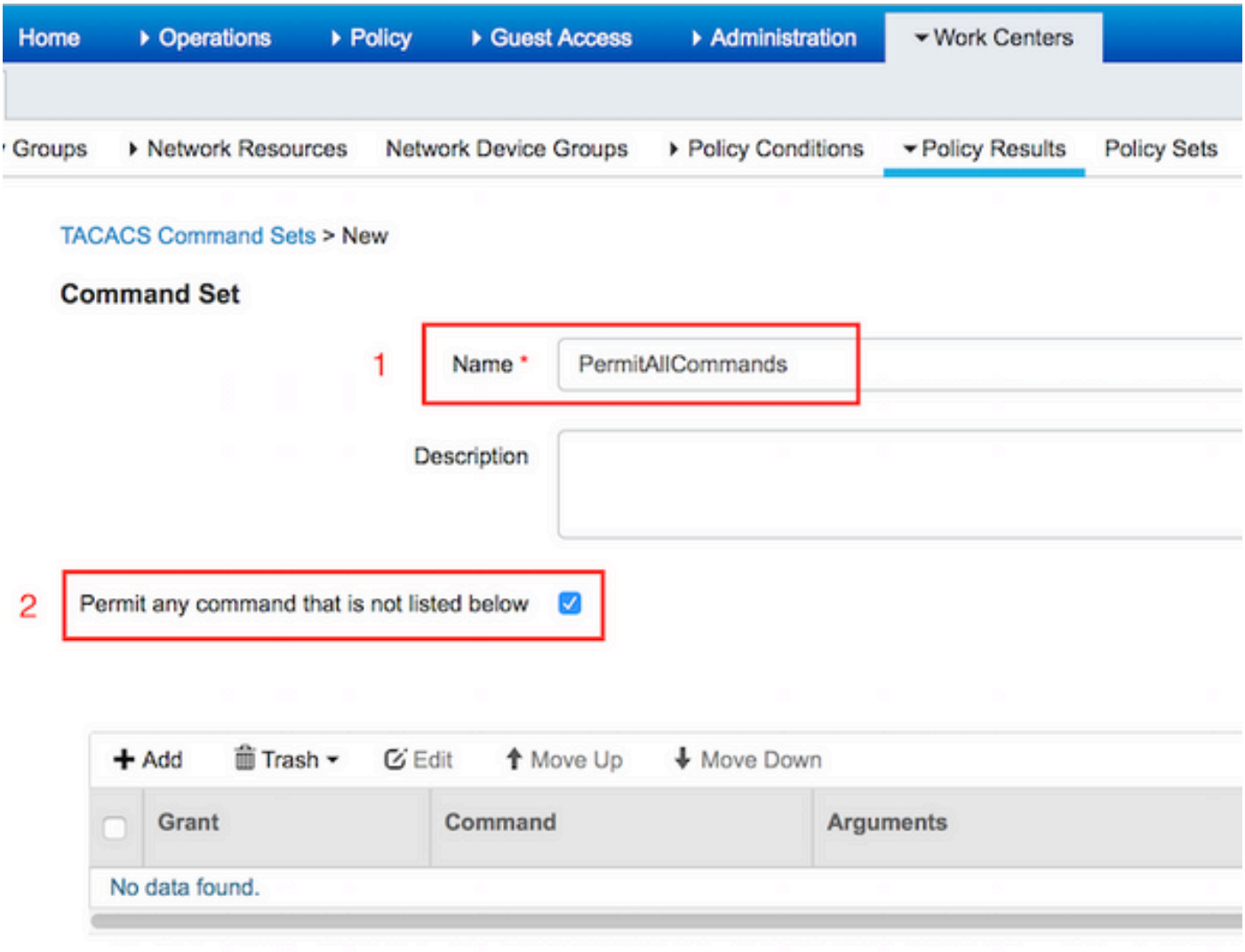


Opmerking: Voor TACACS moet u afzonderlijke licenties hebben geïnstalleerd.

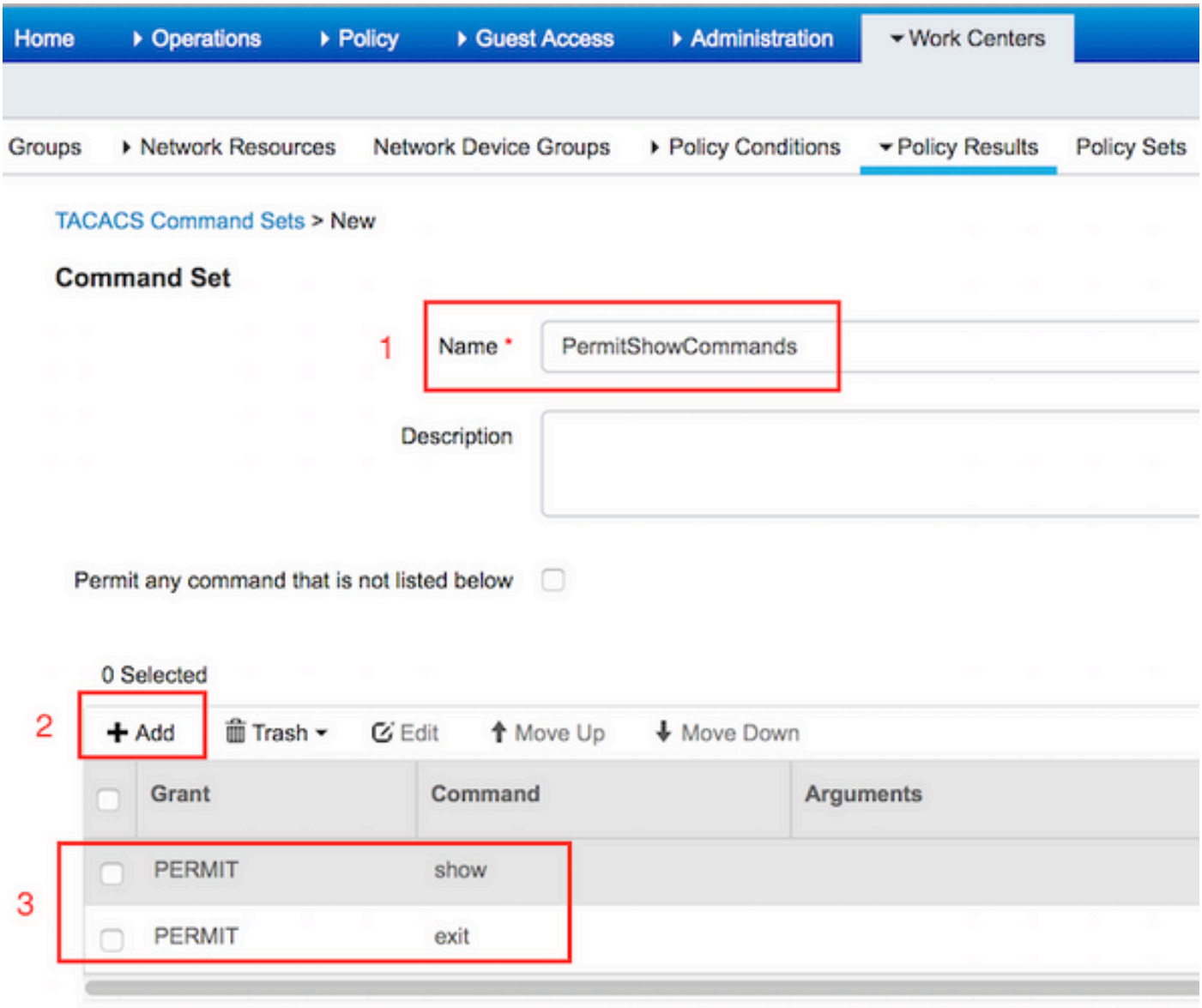
Opdrachtsets voor TACACS configureren

Er worden twee opdrachtsets geconfigureerd. Eerste **PermitAllCommands** voor de gebruikersbeheerder die alle opdrachten op het apparaat toestaat. Tweede **PermitShowCommands** voor gebruiker die alleen opdrachten laat zien.

1. Navigeer naar **werkcentra > Apparaatbeheer > Beleidsresultaten > Tacacs-opdrachtsets.** Klik op **Add (Toevoegen).** Vermeld de Naam **PermitAllCommands**, kies **Permit een opdracht** checkbox die niet vermeld is en klik op **Indienen.**

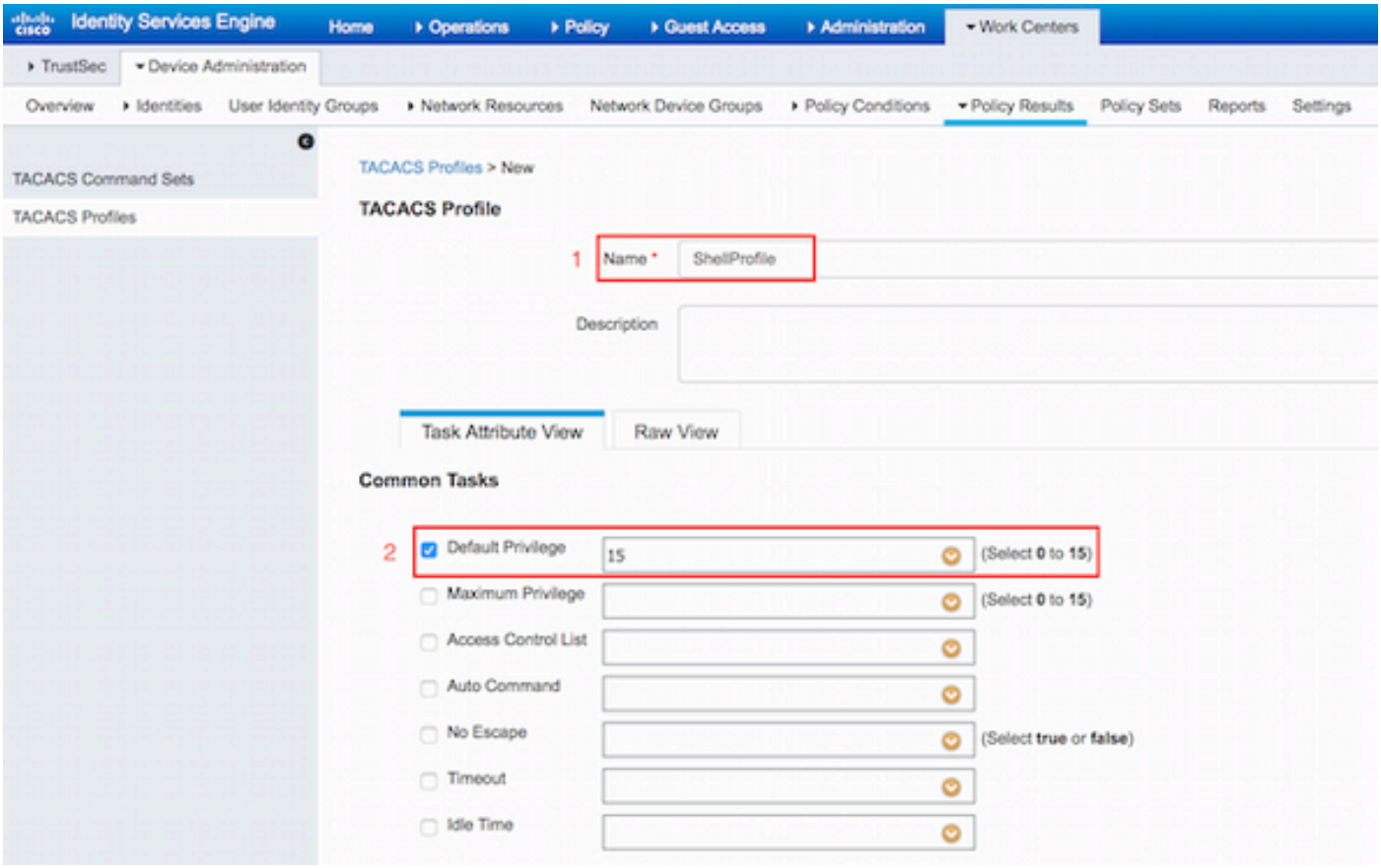


2. Navigeren naar **werkcentra > Apparaatbeheer > Beleidsresultaten > Tacacs-opdrachtsets.** Klik op **Add (Toevoegen).** Geef de naam **PermitShowCommands op**, klik op **Add** en laat opdrachten **tonen** en **afsluiten** toe. Als Argumenten standaard leeg blijven, worden alle argumenten opgenomen. Klik op **Verzenden.**



TACACS-profiel configureren

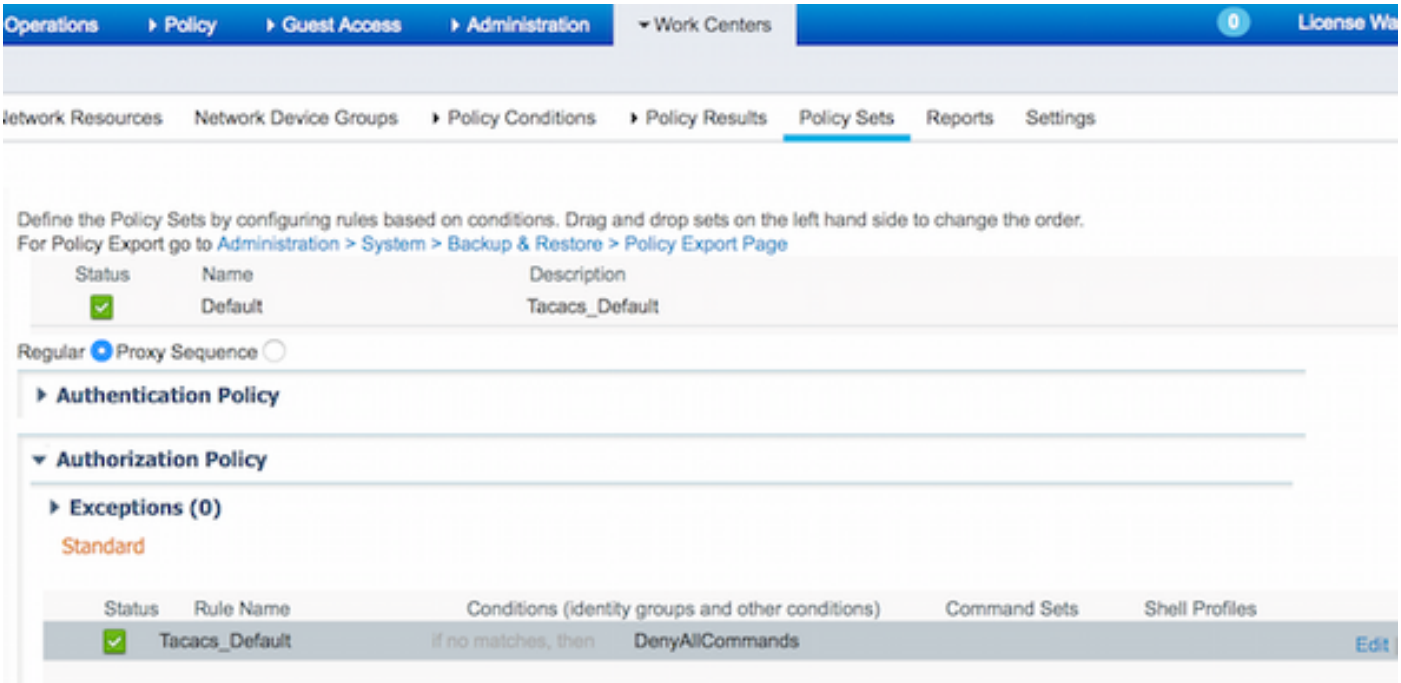
Eén TACACS-profiel is geconfigureerd. Het TACACS-profiel is hetzelfde concept als Shell Profile op ACS. De daadwerkelijke opdrachthandhaving gebeurt via opdrachtsets. Ga naar **Werkcentra > Apparaatbeheer > Beleidsresultaten > TACACS-profielen.** Klik op **Add (Toevoegen).** Geef Naam ShellProfile, selecteer **Default Privilege** checkbox en voer de waarde van 15 in. Klik op **Indienen.**



Toepassingsbeleid TACACS configureren

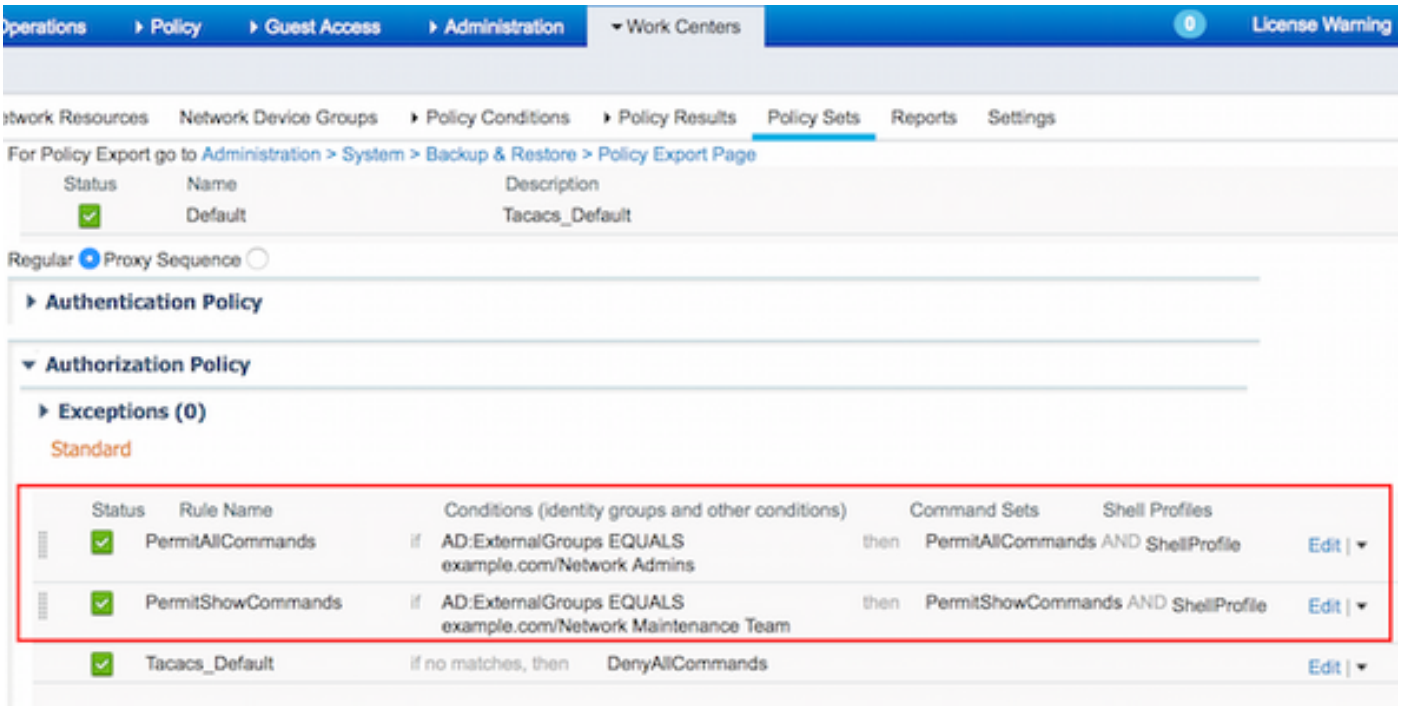
Verificatiebeleid verwijst standaard naar All_User_ID_Stores, die AD bevat, zodat deze ongewijzigd blijft.

Navigeer naar **Werkcentra > Apparaatbeheer > Beleidssets > Standaard > Autorisatiebeleid > Bewerken > Nieuwe regel invoegen hierboven.**



Er worden twee machtigingsregels ingesteld; eerste regel wijst TACACS profiel ShellProfile en commando Set PermitAllCommands toe gebaseerd op Network Admins AD Group lidmaatschap.

De tweede regel wijst een TACACS-profiel toe ShellProfile en de opdracht Set PermitShowCommands gebaseerd op het lidmaatschap van de AD-groep van het Onderhoudsteam van het Netwerk.



Configureer de Cisco IOS-router voor verificatie en autorisatie

Voltooi deze stappen om Cisco IOS router voor verificatie en autorisatie te configureren.

1. Maak een lokale gebruiker met volledige rechten voor fallback met de **gebruikersnaam** opdracht zoals hier getoond.

```
username cisco privilege 15 password cisco
```

2. Schakel een nieuw model in. Definieer de TACACS-server ISE en plaats deze in de groep ISE_GROUP.

```
aaa new-model

tacacs server ISE
 address ipv4 10.48.17.88
 key cisco
aaa group server tacacs+ ISE_GROUP
 server name ISE
```

> **Opmerking:** De servertoets komt overeen met de toets die eerder op ISE Server is gedefinieerd.

3. Test de bereikbaarheid van de TACACS-server met de test **aaa** opdracht zoals getoond.

```
Router#test aaa group tacacs+ admin Krakow123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

De output van het vorige bevel toont aan dat de server TACACS bereikbaar is en de gebruiker

met succes voor authentiek is verklaard.

4. Configureer de login en schakel authenticaties in en gebruik vervolgens de exec- en opdrachtautorisaties zoals aangegeven op de afbeelding.

```
aaa authentication login AAA group ISE_GROUP local
aaa authentication enable default group ISE_GROUP enable
aaa authorization exec AAA group ISE_GROUP local
aaa authorization commands 0 AAA group ISE_GROUP local
aaa authorization commands 1 AAA group ISE_GROUP local
aaa authorization commands 15 AAA group ISE_GROUP local
aaa authorization config-commands
```

> **Opmerking:** De gemaakte methodelijst wordt AAA genoemd, die later wordt gebruikt, wanneer deze aan line vty wordt toegewezen.

5. Wijs methodelijsten toe aan regel vty 0 4.

```
line vty 0 4
 authorization commands 0 AAA
 authorization commands 1 AAA
 authorization commands 15 AAA
 authorization exec AAA
 login authentication AAA
```

Verifiëren

Cisco IOS-routerverificatie

1. Telnet naar de Cisco IOS-router als beheerder die tot de volledige toegangsgroep in AD behoort. Network Admins-groep is de groep in AD die is toegewezen aan ShellProfile en PermitAllCommands Command die op de ISE zijn ingesteld. Probeer om het even welk bevel in werking te stellen om volledige toegang te verzekeren.

```
Username:admin
Password:

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes
Router(config-isakmp)#exit
Router(config)#exit
Router#
```

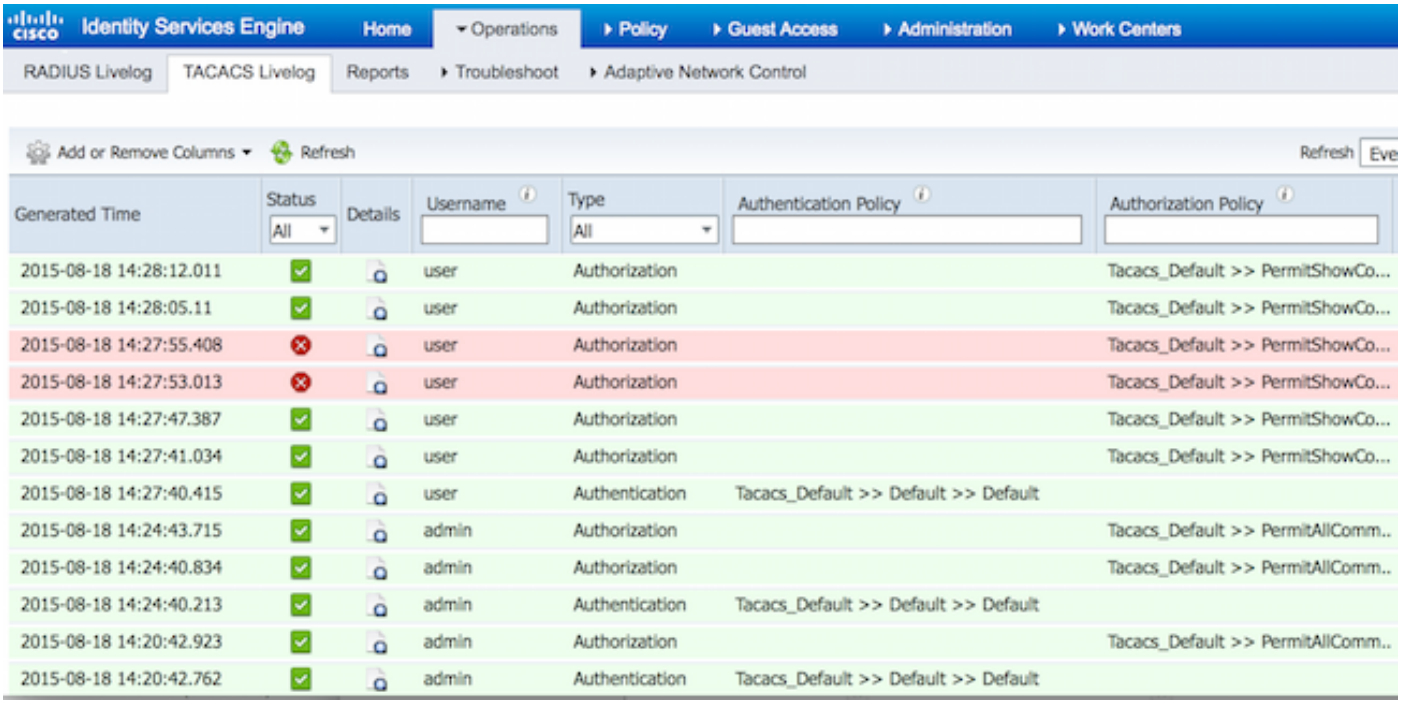
2. Telnet naar de Cisco IOS-router als gebruiker die tot de beperkte toegangsgroep in AD behoort. Network Maintenance Team is de groep in AD die wordt toegewezen aan **ShellProfile** en **PermitShowCommands** Command op de ISE. Probeer om het even welk bevel in werking te stellen om ervoor te zorgen dat slechts toont de bevelen kunnen worden uitgegeven.

```
Username:user
Password:

Router#show ip interface brief | exclude unassigned
```

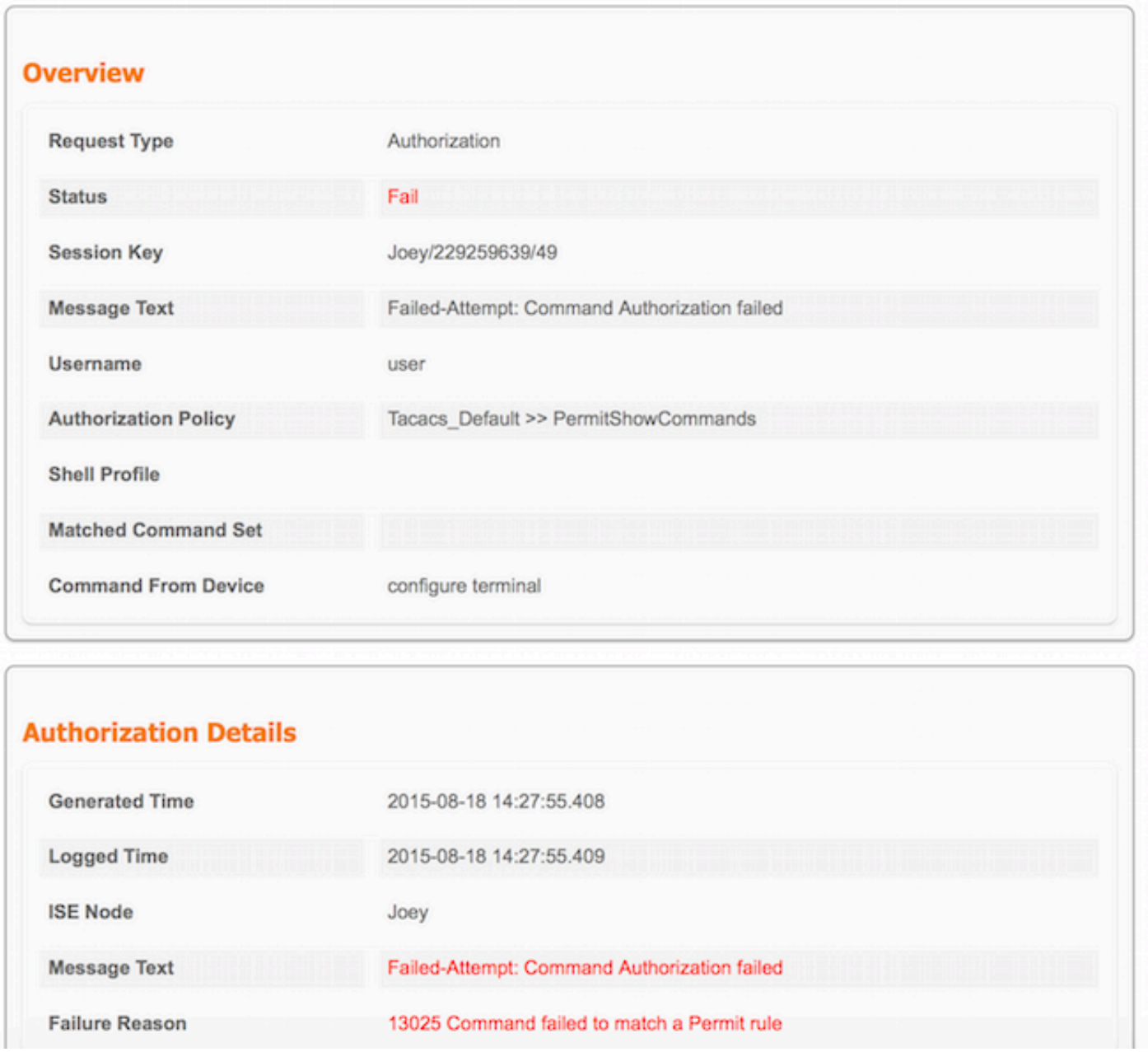
```
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.48.66.32     YES NVRAM  up                    up

Router#ping 8.8.8.8
Command authorization failed.

Router#configure terminal
Command authorization failed.

Router#show running-config | include hostname
hostname Router
Router#
```

ISE 2.0-verificatie

1. Ga naar **Operations > TACACS Livelog.** Zorg ervoor dat de pogingen zichtbaar zijn.



2. Klik op de details van een van de rode rapporten. Mislukte opdracht eerder uitgevoerd kan worden gezien.



Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Matched Command Set	
Command From Device	configure terminal

Authorization Details

Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

Problemen oplossen

Fout: 13025-opdracht voldoet niet aan permit-regel

Controleer de eigenschappen SelectedCommandSet om te verifiëren dat de verwachte Opdrachtsets zijn geselecteerd door het Autorisatiebeleid.

Gerelateerde informatie

[Technische ondersteuning en documentatie – Cisco Systems]

[Releaseopmerkingen van ISE 2.0]

[ISE 2.0 hardware-installatiehandleiding]

[ISE 2.0 upgrade-handleiding]

Handleiding ACS naar ISE-migratietool

ISE 2.0 Active Directory-integratiegids

ISE 2.0 Engine beheerdershandleiding

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.