

# ISE 2.0: ASA CLI-configuratievoorbeeld voor TACACS+ verificatie en opdracht

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[ISE configureren voor verificatie en autorisatie](#)

[Netwerkkapparaat toevoegen](#)

[Gebruikersidentiteitsgroepen configureren](#)

[Gebruikers configureren](#)

[Apparaatbeheerservice inschakelen](#)

[TACACS-opdrachtsets configureren](#)

[TACACS-profiel configureren](#)

[Het TACACS-machtigingsbeleid configureren](#)

[Configureer de Cisco ASA firewall voor verificatie en autorisatie](#)

[Verifiëren](#)

[Cisco ASA-firewallverificatie](#)

[ISE 2.0 Verificatie](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Gerelateerde Cisco Support Community-discussies](#)

## Inleiding

Dit document beschrijft hoe u TACACS+ verificatie en geautoriseerde commando's kunt configureren op Cisco adaptieve security applicatie (ASA) met Identity Services Engine (ISE) 2.0 en hoger. ISE gebruikt lokale identiteitsopslag om resources zoals gebruikers, groepen en endpoints op te slaan.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ASA Firewall is volledig operationeel
- Connectiviteit met ASA en ISE
- ISE Server is geblokkeerd

## Gebruikte componenten

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

- Cisco Identity Services Engine 2.0
- Cisco ASA-software release 9.5(1)S

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 de potentiële impact van elke opdracht begrijpen.

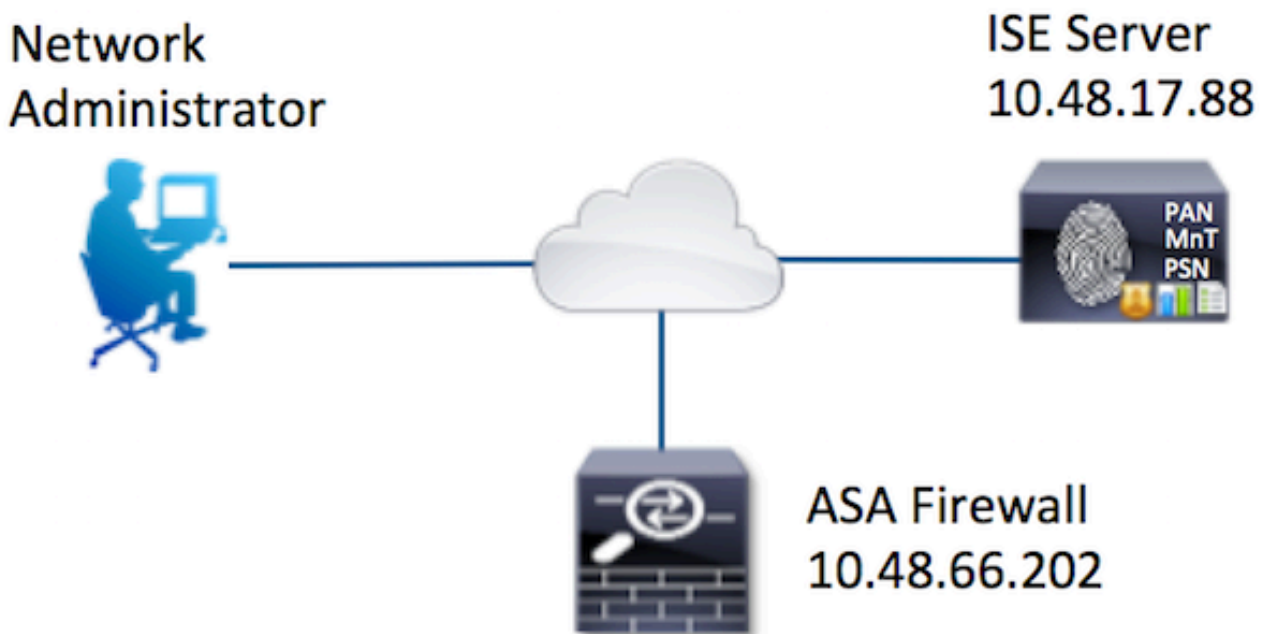
Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies.](#)

## Configureren

Het doel van de configuratie is:

- Verifieer de gebruiker via Interne Identity Store
- autorisatie van de ssh-gebruiker zodat deze in de bevoorrechte EXEC-modus wordt geplaatst na de inlognaam
- Controleer en stuur elke uitgevoerde opdracht naar ISE ter verificatie

## Netwerkdigram



## Configuraties

## ISE configureren voor verificatie en autorisatie

Er worden twee gebruikers gemaakt. Gebruiker **beheerder** is een deel van **Network Admins Local Identity Group** op ISE. Deze gebruiker heeft volledige CLI privileges. Gebruiker maakt deel uit van ISE-groep voor **netwerkonderhoud**. Deze gebruiker mag alleen opdrachten tonen en pingelen.

### Netwerkapparaat toevoegen

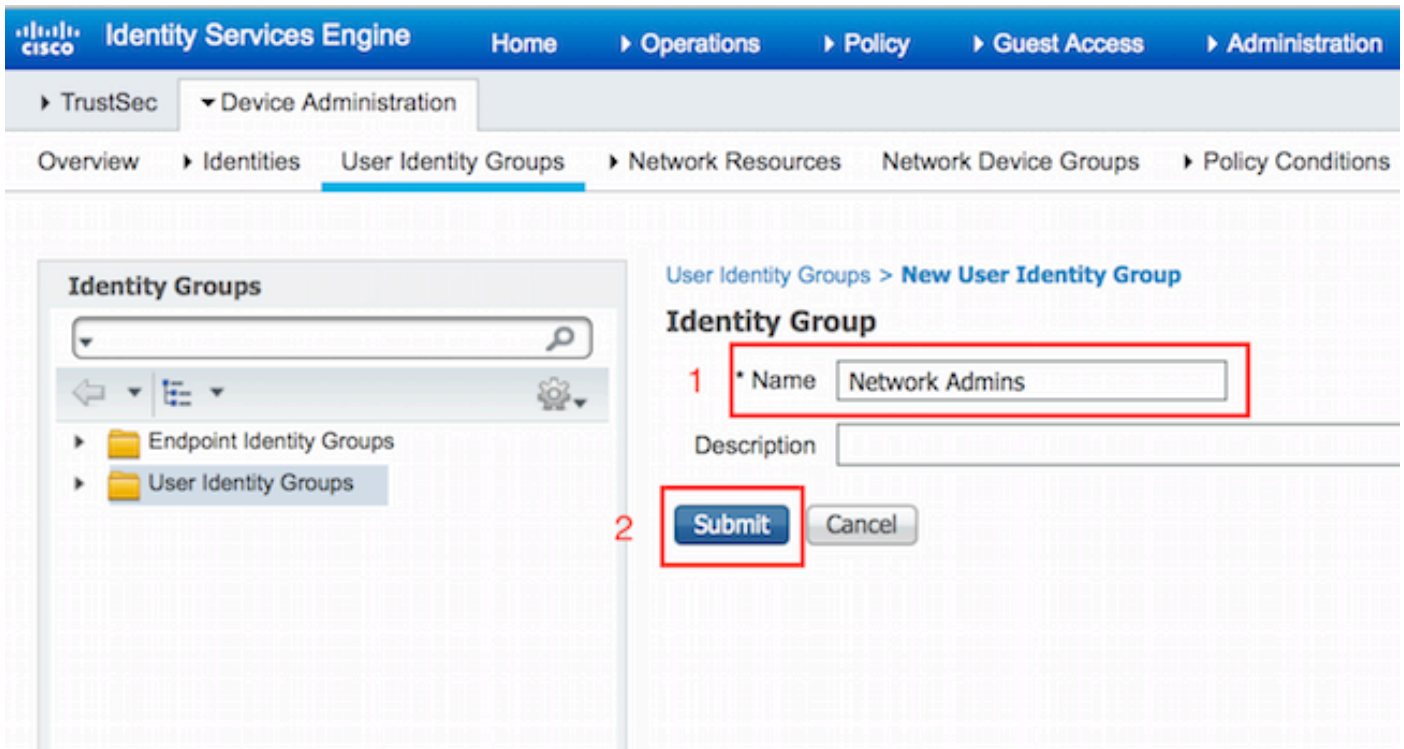
Blader naar **werkcentra > Apparaatbeheer > Netwerkbronnen > Netwerkapparaten**. Klik op **Toevoegen**. Geef naam, IP-adres, selecteer het selectieteken **TACACS+ verificatie-instellingen** en specificeer **gedeelde** beveiligingstoets. U kunt desgewenst het type/de locatie van het apparaat instellen.

The screenshot shows the 'New Network Device' configuration page in the Cisco Identity Services Engine (ISE) web interface. The page is titled 'Network Devices List > New Network Device'. The left sidebar shows 'Network Devices' with sub-items: 'Default Devices', 'TACACS External Servers', and 'TACACS Server Sequence'. The main content area is titled 'Network Devices' and contains the following fields and sections:

- Name:** A text input field containing 'ASA', highlighted with a red box and labeled '1'.
- Description:** An empty text input field.
- IP Address:** A text input field containing '10.48.66.202' and a dropdown menu set to '32', highlighted with a red box and labeled '2'.
- Device Profile:** A dropdown menu set to 'Cisco'.
- Model Name:** An empty dropdown menu.
- Software Version:** An empty dropdown menu.
- Network Device Group:** A section with two dropdown menus: 'Location' set to 'All Locations' and 'Device Type' set to 'Firewall'. Both have 'Set To Default' buttons.
- RADIUS Authentication Settings:** A section with a checkbox that is unchecked.
- TACACS+ Authentication Settings:** A section with a checkbox that is checked, highlighted with a red box and labeled '3'. Below it is a 'Shared Secret' field with a masked value '\*\*\*\*\*' and a 'Show' button.
- Enable Single Connect Mode:** A checkbox that is unchecked.

### Gebruikersidentiteitsgroepen configureren

Blader naar **werkcentra > Apparaatbeheer > Gebruikersgroepen**. Klik op **Toevoegen**. Geef naam op en klik op **Indienen**.



Herhaal dezelfde stap om de gebruikersgroep van het Netwerk Onderhoudsteam te configureren.

### Gebruikers configureren

Navigeer naar **werkcentra > Apparaatbeheer > Identificaties > Gebruikers**. Klik op **Toevoegen**. Geef naam op, inlogwachtwoord specificeert gebruikersgroep en klik op **Indienen**.

**Network Access User**

\* Name  1

Status  Enabled

Email

**Passwords** 2

	Password	Re-Enter Password	
* Login Password	<input type="password" value="....."/>	<input type="password" value="....."/>	<input type="button" value="i"/>
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="i"/>

**User Information**

First Name

Last Name

**Account Options**

Description

Change password on next login

3

**User Groups**

Herhaal de stappen om **gebruiker** te configureren en wijs **de** gebruikersgroep **van het** Netwerk Onderhoudsteam toe.

### Apparaatbeheerservice inschakelen

Navigeer naar **Administratie > Systeem > Plaatsing**. Selecteer het gewenste knooppunt. Selecteer het selectieteken **Apparaatbeheer inschakelen** en klik op **Opslaan**.

Opmerking: Voor TACACS moet er een afzonderlijke licentie zijn geïnstalleerd.

## TACACS-opdrachtsets configureren

Er worden twee opdrachtsets ingesteld. Eerst **PermitAllCommands** voor de **beheerder** gebruiker die alle opdrachten op het apparaat toestaat. Tweede **PermitPingShowCommands** voor **gebruiker** die alleen opdrachten tonen en pingen toestaat.

1. Blader naar **werkcentra > Apparaatbeheer > Beleidsuitkomsten > TACACS-opdrachtsets**. Klik op **Toevoegen**. Typ de **opdracht Naam** **toestaanAllCommands**, selecteer **Geef een opdracht toe die niet hieronder weergegeven is** en klik op **Indienen**.

TACACS Command Sets > New

### Command Set

1

Name \*

PermitAllCommands

Description

2

Permit any command that is not listed below



+ Add    🗑️ Trash ▼    ✎ Edit    ↑ Move Up    ↓ Move Down			
<input type="checkbox"/>	Grant	Command	Arguments
No data found.			

2. Blader naar **werkcentra > Apparaatbeheer > Beleidsuitkomsten > TACACS-opdrachtsets**. Klik op **Toevoegen**. Geef de opdrachten voor de naam **PingShowCommands** op, klik op **Add** en laat **show** toe, **ping** en **exit**. Standaard als Argumenten blanco blijven, worden alle argumenten opgenomen. Klik op **Inzenden**.

## Command Set

1 Name \* PermitPingShowCommands

Description

Permit any command that is not listed below 

Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	exit
<input type="checkbox"/>	PERMIT	show
<input type="checkbox"/>	PERMIT	ping

2

Cancel Save

## TACACS-profiel configureren

Eén TACACS-profiel wordt ingesteld. De eigenlijke opdrachtregel wordt uitgevoerd via opdrachtsets. Navigeer naar **werkcentra > Apparaatbeheer > Beleidsresultaten > TACACS profielen**. Klik op **Toevoegen**. Geef een naam op **ShellProfile**, selecteer het selectieteken **Default Priviool** en voer de waarde van 15 in. Klik op **Indienen**.

Identity Services Engine Home > Operations > Policy > Guest Access > Administration > Work Centers

TrustSec > Device Administration

Overview > Identities > User Identity Groups > Network Resources > Network Device Groups > Policy Conditions > Policy Results > Policy Sets > Reports > Settings

TACACS Command Sets

TACACS Profiles

TACACS Profiles > New

TACACS Profile

1 Name \* ShellProfile

Description

Task Attribute View Raw View

Common Tasks

2  Default Privilege 15 (Select 0 to 15)

Maximum Privilege (Select 0 to 15)

Access Control List

Auto Command

No Escape (Select true or false)

Timeout

Idle Time

## Het TACACS-machtigingsbeleid configureren



Verificatiebeleid door standaard punten naar All\_User\_ID\_Stores, die ook de Local Store bevat, dus deze blijft ongewijzigd.

Navigeer naar **werkcentra > Apparaatbeheer > Beleidsformaten > Standaard > autorisatiebeleid > Bewerken > Nieuwe regel hierboven invoegen.**

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular  Proxy Sequence

► Authentication Policy

▼ Authorization Policy

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	DenyAllCommands	

Er worden twee goedkeuringsregels ingesteld. De eerste regel wijst TACACS-profiel **ShellProfile** toe en de opdracht Set **PermitAllCommands** toe op basis van **Network Admins** User Identity Group lidmaatschap. Tweede regel toegewezen TACACS-profiel **ShellProfile** en opdrachtset **PermitPingShowCommands** op basis van het lidmaatschap van de Gebruiker van het Team van de Onderhoud.

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	ASAPermitAllCommands	if <b>Network Admins</b> then	PermitAllCommands AND ShellProfile	
<input checked="" type="checkbox"/>	ASAPermitShowPingComm ands	if <b>Network Maintenance Team</b> then	PermitPingShowCommands AND ShellProfile	

## Configureer de Cisco ASA firewall voor verificatie en autorisatie

1. Maak een lokale gebruiker met volledig privilege voor back-up met de gebruikersnaam, zoals hier wordt getoond

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. Definieer TACACS server ISE, specificeer interface, protocol ip adres en **tacacs** toets.

```
aaa-server ISE protocol tacacs+
aaa-server ISE (mgmt) host 10.48.17.88
key cisco
```

Opmerking: De servertoets dient overeen te komen met die welke eerder op ISE Server is gedefinieerd.

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

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

De uitvoer van de vorige opdracht toont aan dat de TACACS-server bereikbaar is en dat de gebruiker geauthentiseerd is.

4. Het configureren van de authenticatie voor ssh, exec autorisatie en commando vergunningen zoals hieronder wordt getoond. Met **een autorisatie exec authenticatie-server** kunt u automatisch in bevoorrechte EXEC modus worden geplaatst.

```
aaa authentication ssh console ISE
aaa authorization command ISE
aaa authorization exec authentication-server auto-enable
```

Opmerking: Met de bovenstaande opdrachten wordt verificatie uitgevoerd op ISE, wordt de gebruiker direct in de bevoorrechtingsmodus geplaatst en wordt de opdrachtautorisatie uitgevoerd.

5. Laat ssh op de mgmt-interface staan.

```
ssh 0.0.0.0 0.0.0.0 mgmt
```

## Verifiëren

### Cisco ASA-firewallverificatie

1. Schakel over naar de ASA Firewall als **beheerder** die deel uitmaakt van de gebruikersgroep met volledige toegang. De groep **Network Admins** is in kaart gebracht aan **ShellProfile** en Commands **All Commands** in ISE. Probeer elke opdracht uit te voeren om volledige toegang te garanderen.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
```

```
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
ciscoasa#
```

2. Stap naar de ASA Firewall als **gebruiker** die tot de gebruikersgroep met beperkte toegang behoort. De groep van het **Netwerk van Onderhoud** wordt in kaart gebracht aan **ShellProfile** en **PermitPingShowCommands** die op ISE is ingesteld. Probeer om het even welke opdracht uit te voeren om ervoor te zorgen dat slechts tonen en pingopdrachten kunnen worden afgegeven.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

## ISE 2.0 Verificatie

1. Navigeer naar **bewerkingen > TACACS-loggen**. Zorg ervoor dat de hierboven aangehaalde pogingen zijn gezien.

Generated Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy	ISE N
2015-08-19 13:47:24.135	✘		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:47:15.139	✘		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:47:07.452	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:56.816	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:49.961	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:35.595	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:35.581	✔		user	Authentication	Tacacs_Default >> Default >> Default	Joey	
2015-08-19 13:46:20.209	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	
2015-08-19 13:42:05.838	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	
2015-08-19 13:42:04.886	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	
2015-08-19 13:42:02.575	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	

2. Klik op de details van een van de rode rapporten, de mislukte opdracht die eerder is uitgevoerd, is zichtbaar.

## Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229297775/274
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> ASAPermitShowPingCommands
Shell Profile	
Matched Command Set	
Command From Device	traceroute 8.8.8.8

## Problemen oplossen

Fout: Poging mislukt: Opdrachtautorisatie mislukt

Controleer de eigenschappen SelectedCommisionSet om te controleren of de verwachte commantiesets door het autorisatiebeleid zijn geselecteerd

## Gerelateerde informatie

[Technische ondersteuning en documentatie – Cisco Systems](#)

[ISE 2.0 Releaseopmerkingen](#)

[ISE 2.0 hardwareinstallatiehandleiding](#)

[ISE 2.0 upgrade-gids](#)

[Handleiding ACS naar ISE-migratietool](#)

[ISE 200 Active Directory Integration Guide](#)

[ISE 2.0 Engine Administrator-gids](#)