

# Configuratie van SWA Second Factor-verificatie met ISE als RADIUS-server

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerktopologie](#)

[Configuratiestappen](#)

[ISE-configuratie](#)

[Configuratie SWA](#)

[Verifiëren](#)

[Referenties](#)

---

## Inleiding

Dit document beschrijft hoe u verificatie van tweede factoren kunt configureren op een beveiligde web-applicatie met Cisco Identity Service Engine als een RADIUS-server.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis in SWA.
- Kennis van de configuratie van het authenticatie- en autorisatiebeleid op ISE.
- Basiskennis van RADIUS.

Cisco raadt u ook aan het volgende te hebben:

- Beveiligde toegang voor beheer van Web Appliance (SWA) en Cisco Identity Service Engine (ISE).
- Uw ISE is geïntegreerd in Active Directory of LDAP.
- Active Directory of LDAP is geconfigureerd met een gebruikersnaam 'admin' om SWA standaard 'admin' account te authenticeren.
- Compatibele WSA en ISE versies.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- SWA 14.0.2-012
- ISE 3.0.0

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

Wanneer u de tweede factorverificatie voor administratieve gebruikers op SWA inschakelt, verifieert het apparaat de gebruikersreferenties met de RADIUS-server voor de tweede keer nadat de referenties zijn geverifieerd die in SWA zijn geconfigureerd.

## Netwerktopologie



Afbeelding - Netwerktopologiediagram

Administratieve gebruikers hebben toegang tot SWA op poort 443 met hun referenties. SWA verifieert de referenties met de RADIUS-server voor verificatie van de tweede factor.

## Configuratiestappen

### ISE-configuratie

Stap 1. Voeg een nieuw netwerkapparaat toe. Ga naar Beheer > Netwerkbronnen > Netwerkapparaten > +Add.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices

Default Device

Device Security Settings

**Network Devices**

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type
No data available				

SWA als netwerkkapparaat toevoegen in ISE

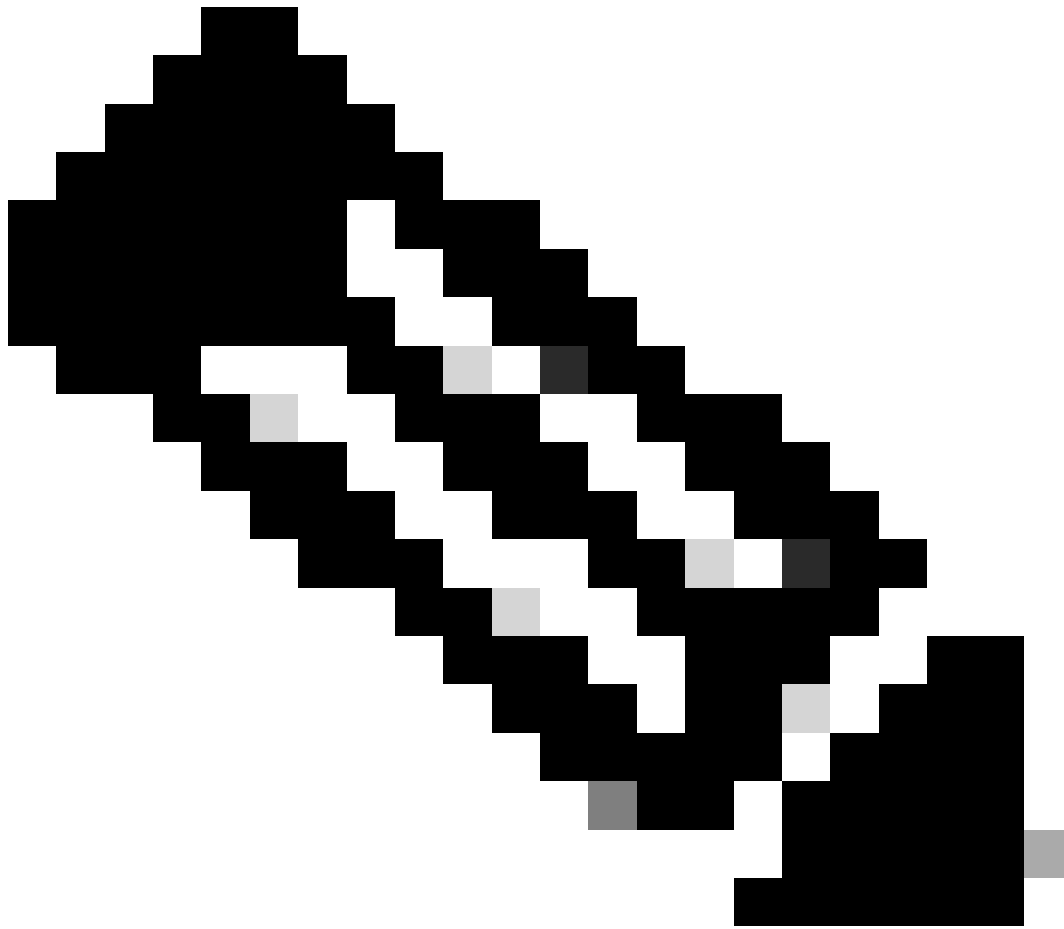
Stap 2. Configureer het netwerkkapparaat in ISE.

Stap 2.1. Wijs een naam toe aan het object van het netwerkkapparaat.

Stap 2.2. Plaats het SWA IP-adres.

Stap 2.3. Controleer het aanvinkvakje RADIUS.

Stap 2.4. Definieer een gedeeld geheim.



Opmerking: dezelfde toets moet later worden gebruikt om de SWA te configureren.

---

Network Devices

Default Device

Device Security Settings

[Network Devices List > SWA](#)

### Network Devices

\* Name

Description

IP Address  \* IP :  /

\* Device Profile  Cisco

Model Name

Software Version

\* Network Device Group

Location

IPSEC

Device Type

**RADIUS Authentication Settings**

#### RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret

gedeelde sleutel voor netwerkkapparaat configureren

Stap 2.5. Klik op Verzenden.

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol: **RADIUS**

\* Shared Secret:

Use Second Shared Secret:  ⓘ

CoA Port:

**RADIUS DTLS Settings ⓘ**

DTLS Required:  ⓘ

Shared Secret:  ⓘ

CoA Port:

Issuer CA of ISE Certificates for CoA:  ⓘ

DNS Name:

**General Settings**

Enable KeyWrap:  ⓘ

\* Key Encryption Key:

\* Message Authenticator Code Key:

Key Input Format:  ASCII  HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Configuratie van netwerkapparaat verzenden

Stap 3. U moet Netwerktogangsgebruikers maken die overeenkomen met de gebruikersnaam die in de SWA is geconfigureerd. Navigeren naar Administratie > Identiteitsbeheer > Identiteiten > + Toevoegen.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Users

Latest Manual Network Scan Results

**Network Access Users**

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address
No data available					

Voeg lokale gebruikers toe in ISE

Stap 3.1. Wijs een naam toe.

Stap 3.2. (optioneel) Voer het e-mailadres van de gebruiker in.

Stap 3.3. Wachtwoord instellen.

Stap 3.4. Klik op Save (Opslaan).

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

**Network Access User**

\* Name:

Status:  Enabled

Email:

**Passwords**

Password Type:

Password: 
 Re-Enter Password: 
 ⓘ

\* Login Password: 
 ⓘ

Enable Password: 
 ⓘ

Voeg een lokale gebruiker toe in ISE

Stap 4. Maak een beleidsset die overeenkomt met het SWA IP-adres. Dit is om toegang tot andere apparaten met deze gebruikersreferenties te voorkomen.

Navigeer naar Policy > PolicySets en klik op +pictogram in de linkerbovenhoek.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

**Policy Sets**

+	Status	Policy Set Name	Description	Conditions
Search				

Beleidsset toevoegen in ISE

Stap 4.1. Een nieuwe regel wordt bovenaan uw Policy Sets geplaatst. Voer een naam in voor nieuw beleid.

Stap 4.2. Voeg een voorwaarde voor RADIUS NAS-IP-Adres attribuut toe om het SWA IP-adres aan te passen.

Stap 4.3. Klik op Gebruik om de wijzigingen te bewaren en de editor te verlaten.







Opmerking: in dit voorbeeld is de lijst met standaardprotocollen voor netwerktoegang toegestaan. U kunt een nieuwe lijst maken en deze indien nodig beperken.

---

Stap 5. Als u de nieuwe beleidssets wilt weergeven, klikt u op het pictogram ">" in de kolom Bekijken.

Stap 5.1. Breid het menu Autorisatiebeleid uit en klik op het + pictogram om een nieuwe regel toe te voegen om de toegang tot alle geverifieerde gebruikers mogelijk te maken.

Stap 5.2. Stel een naam in.

Stap 5.3. Stel de voorwaarden in om de netwerktoegang voor woordenboeken met de verificatiestatus van kenmerken af te stemmen op de doorgegeven verificatie en klik op Gebruik.



# Configuratie SWA

Stap 1. Van SWA GUI navigeer aan Systeembeheer en klik Gebruikers.

Stap 2. Klik op Inschakelen in Second Factor Verification Settings.

**Cisco Secure Web Appliance S100V**

Reporting | Web Security Manager | Security Services | Network | System Administration | Secure We

## Users

Add User...

<input type="checkbox"/> All Accounts	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	

Enforce Passphrase Changes

### Local User Account & Passphrase Settings

Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. Additional rules configured...

Edit Settings...

### External Authentication

External Authentication is disabled.

Enable...

### Second Factor Authentication Settings

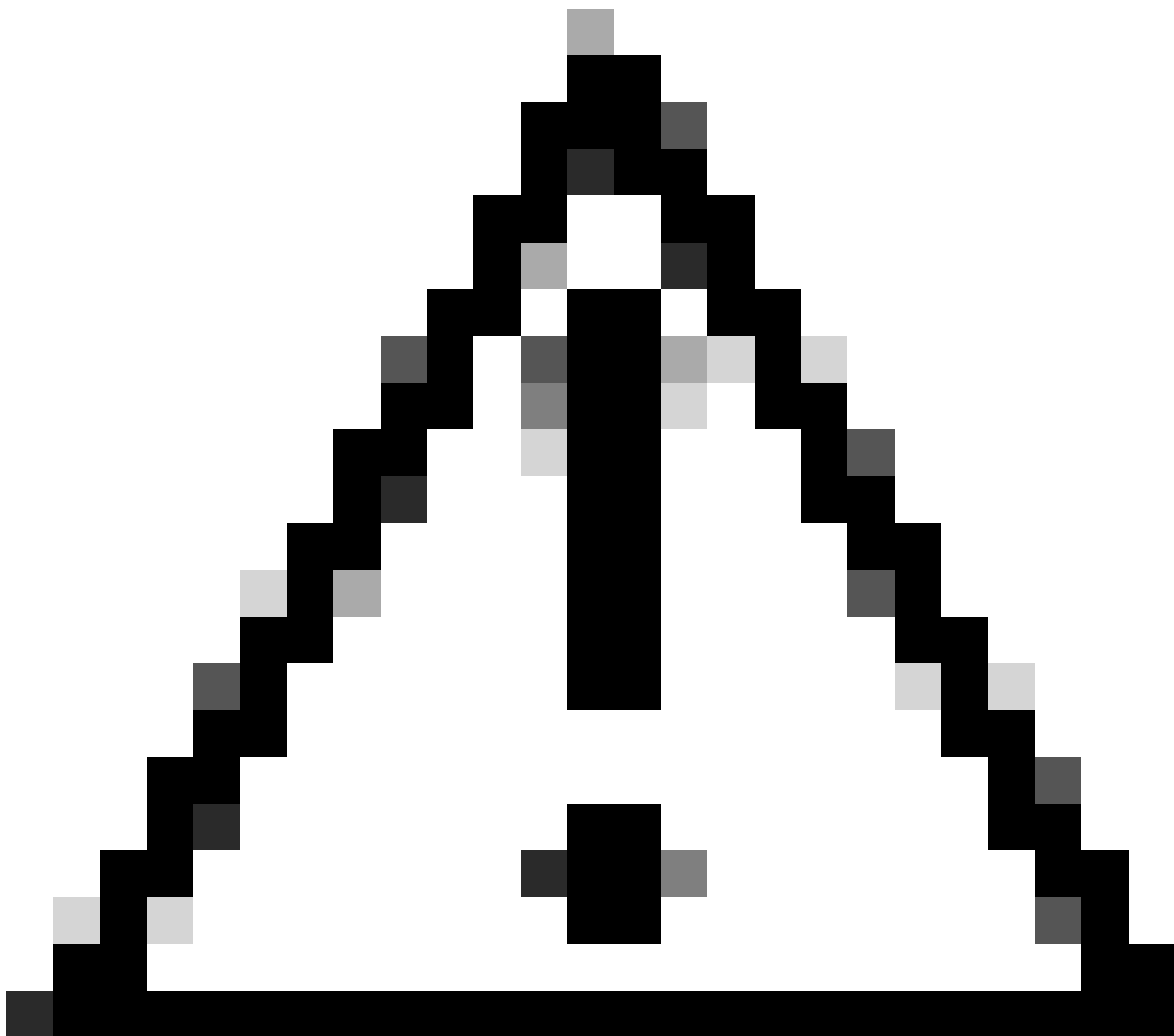
Two Factor Authentication is disabled.

Enable...

Tweede factor verificatie in SWA inschakelen

Stap 3. Voer het IP-adres van de ISE in het veld RADIUS Server Hostname in en voer het gedeelde geheim in dat is geconfigureerd in stap 2 van ISE-configuratie.

Stap 4. Selecteer de gewenste vooraf gedefinieerde rollen die Tweede Factor-handhaving moet worden ingeschakeld.



Waarschuwing: als u authenticatie van een tweede factor in SWA inschakelt, wordt de standaard 'admin' account ook ingeschakeld met handhaving van de tweede factor. U moet ISE integreren met LDAP of Active Directory (AD) om 'admin' referenties te verifiëren, omdat ISE u niet toestaat om 'admin' te configureren als een Network Access Gebruiker.

---



## Users

### Users

[Add User...](#)

All  
 Accounts

User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
admin	Administrator	Administrator	Active	n/a	

[Enforce Passphrase Changes](#)

### Local User Account & Passphrase Settings

Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. <i>Additional rules configured...</i>

[Edit Settings...](#)

### External Authentication

*External Authentication is disabled.*

[Enable...](#)

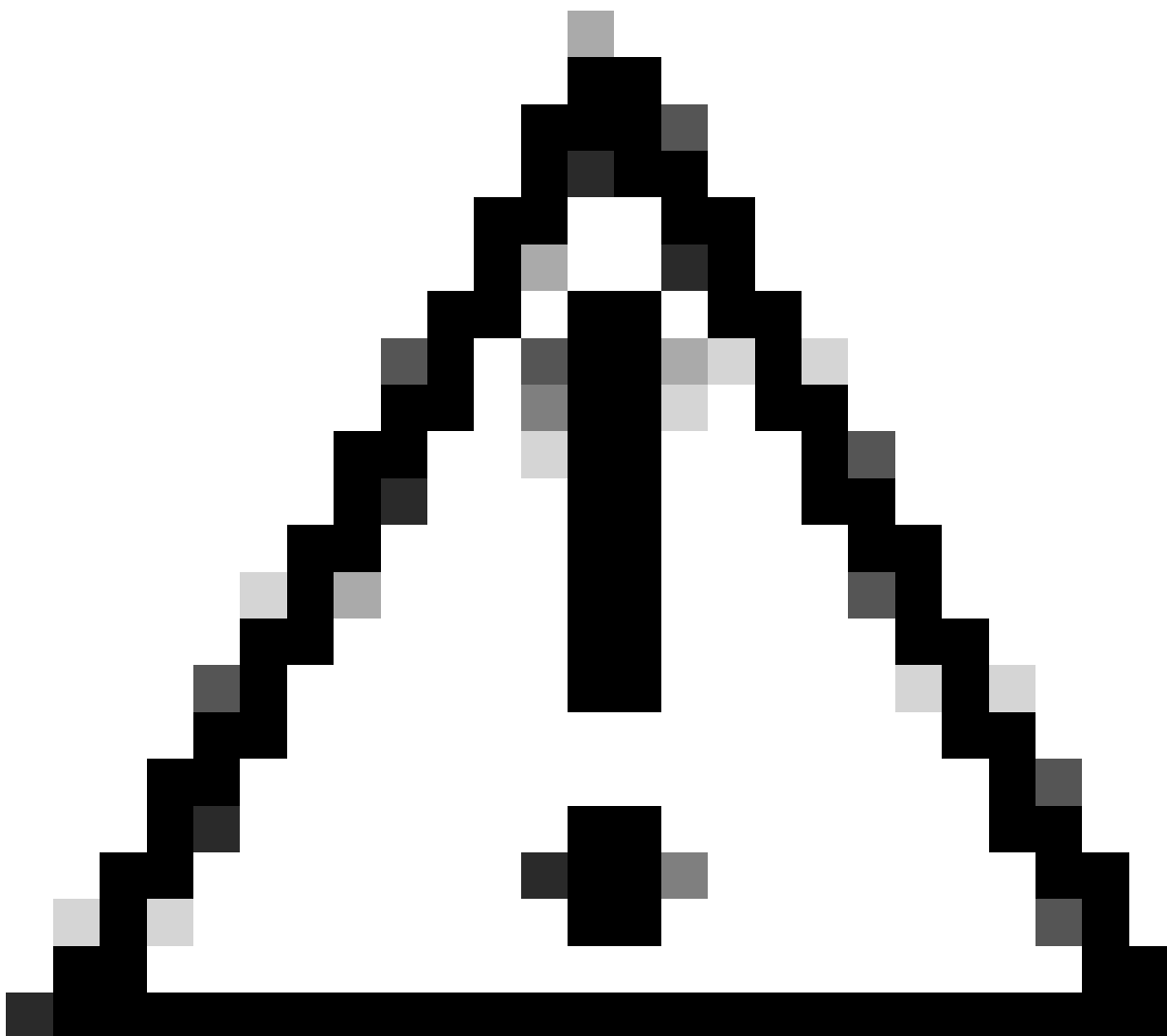
### Second Factor Authentication Settings

*Two Factor Authentication is disabled.*

[Enable...](#)



Tweede factor verificatie in SWA inschakelen



Waarschuwing: als u authenticatie van een tweede factor in SWA inschakelt, wordt de standaard 'admin' account ook ingeschakeld met handhaving van de tweede factor. U moet ISE integreren met LDAP of Active Directory (AD) om 'admin' referenties te verifiëren, omdat ISE u niet toestaat om 'admin' te configureren als een Network Access Gebruiker.

---

## Second Factor Authentication

**Second Factor Authentication Settings**

**Enable Second Factor Authentication**

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:	RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Add Row
	<span style="border: 1px solid #ccc; padding: 2px;">10.106.38.150</span>	<span style="border: 1px solid #ccc; padding: 2px;">1812</span>	<span style="border: 1px solid #ccc; padding: 2px;">*****</span>	<span style="border: 1px solid #ccc; padding: 2px;">5</span>	<span style="border: 1px solid #ccc; padding: 2px;">PAP</span>	

**User Role Privileges**

Configure user roles for Second Factor Authentication

Second Factor Authentication is enforced to:

Predefined Roles

- Administrator
- Operator
- Read-Only Operator
- Guest

**Two Factor Login Page**

Appearance:

Current Logo:

Use Current Logo

Upload Custom Logo from Local Computer: Browse... No file selected.

Company Name:   
(Max 150 characters only)

Custom text Information:   
(Max 500 characters only)

Login help Information:   
(Examples: For login trouble Please contact, Contact Name ,123-1234-123,admin@example.com or help URL. Note:Max 500 characters only)

[View Existing Two Factor Login Page](#)

Cancel
Submit

Tweede factorverificatie configureren

Stap 5: Klik op Add User om Gebruikers in SWA te configureren. Voer een gebruikersnaam in en selecteer het gebruikerstype dat vereist is voor de gewenste rol. Voer wachtwoordgroep in en typ deze opnieuw.

## Users

**Users**

Add User...

\* When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.

All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	adminuser	Admin User	Administrator	Active	n/a	
<input type="checkbox"/>	rouser	RO User	Read-Only Operator	Active	n/a	

Gebruikersconfiguratie in SWA

Stap 6: Klik op Indienen en Wijzigingen vastleggen.

## Verifiëren

Open de SWA GUI met de geconfigureerde gebruikersreferenties. Na succesvolle verificatie wordt u omgeleid naar de secundaire verificatiepagina. Hier moet u de secundaire verificatiereferenties invoeren die in ISE zijn geconfigureerd.



Passcode:

Login

Copyright © 2003-2022 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

Controleer het inloggen op tweede factor

## Referenties

- [Gebruikershandleiding voor AsyncOS 14.0 voor Cisco Secure Web applicatie](#)
- [ISE 3.0 beheerdershandleiding](#)
- [ISE-compatibiliteitsmatrix voor beveiligde web applicatie](#)
- [Geïntegreerde AD voor ISE GUI en CLI-aanmelding](#)



## 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.