

# Hoge beschikbaarheid op FMC configureren

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Voordat u begint](#)

[Configureren](#)

[Secundair VCC configureren](#)

[Primair VCC configureren](#)

[Verificatie](#)

---

## Inleiding

Dit document beschrijft een configuratievoorbeeld van High Availability (HA) op een Firewall Management Center (FMC).

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op het beveiligde FMC voor VMware v7.2.5.

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

Specifieke eisen voor dit document zijn onder meer:

- Beide FMC-peers moeten op dezelfde softwareversie, inbraakregelupdate, kwetsbaarheidsdatabase en lichtgewicht security pakket staan
- Beide FMC-peers moeten dezelfde capaciteit of hardwareversie hebben
- Beide VCC's hebben een afzonderlijke vergunning nodig

Voor een volledige reeks vereisten kunt u de [beheershandleiding](#) bezoeken.

---



Waarschuwing: Als de vereisten niet overeenkomen, kunt u HA niet configureren.

---

Deze procedure wordt op alle hardwareapparatuur ondersteund.

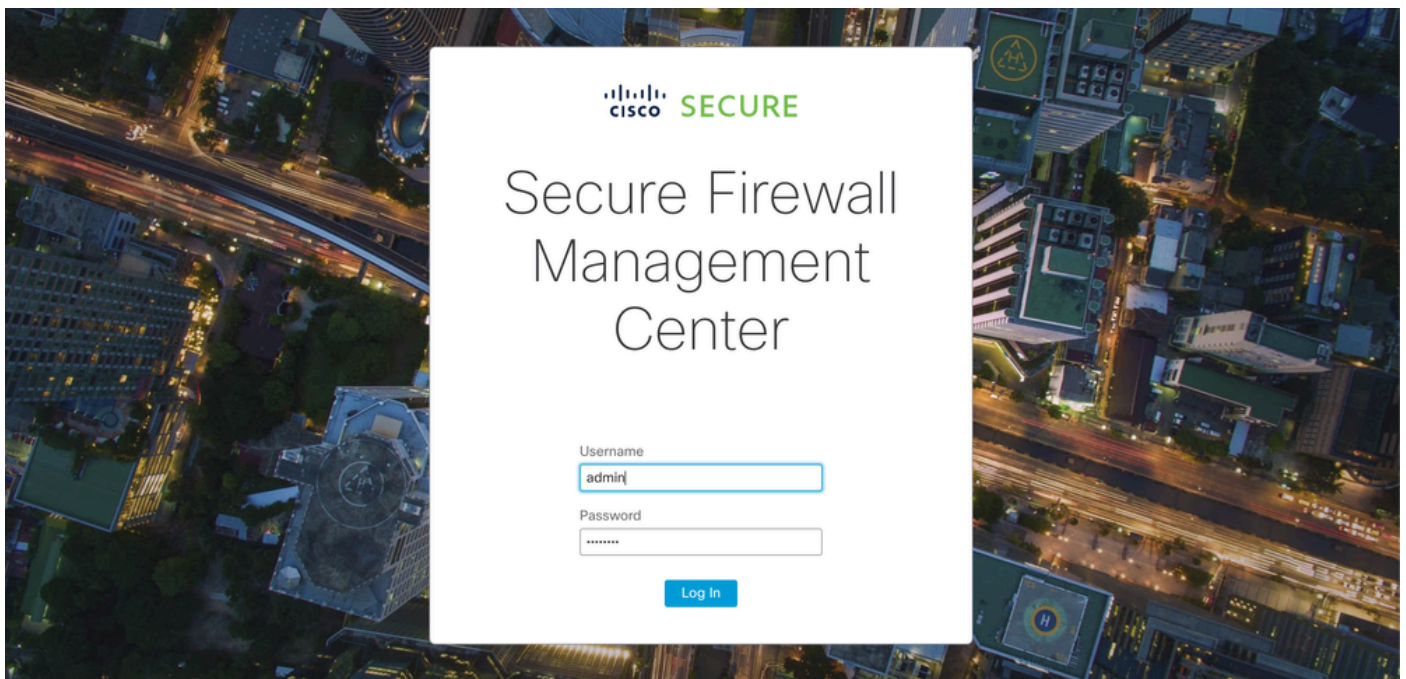
## Voordat u begint

- Ervoor zorgen dat de beheerder toegang heeft tot beide VCC's
- Zorg voor connectiviteit tussen beheerinterfaces
- Neem even de tijd om de softwareversies te bekijken en zorg ervoor dat alle benodigde upgrades uitgevoerd worden

## Configureren

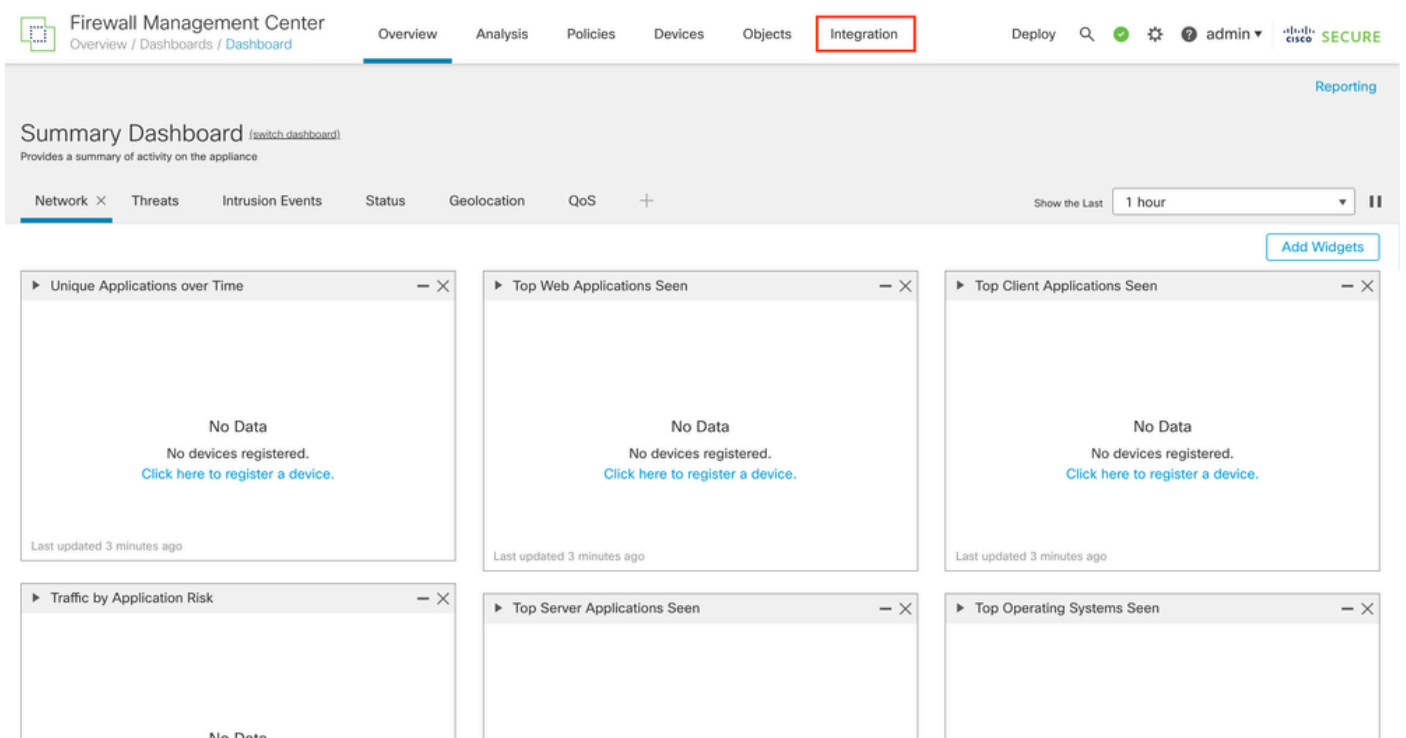
Secundair VCC configureren

Stap 1. Log in op de grafische gebruikersinterface (GUI) van het apparaat van het VCC dat de rol van Secundair/Standby zal vervullen.



Inloggen bij VCC

Stap 2. Navigeer naar het tabblad Integratie.



Naar integratie navigeren

Stap 3. Klik op Overige integraties.

## SecureX

## Security Analytics &amp; Logging

## Other Integrations

## AMP

## AMP Management

## Dynamic Analysis Connections

## Intelligence

## Incidents

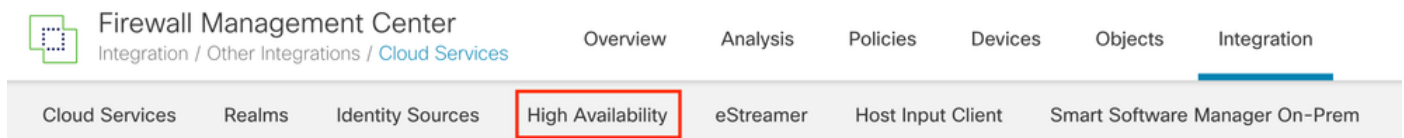
## Sources

## Elements

## Settings

Naar andere integraties navigeren

Stap 4. Navigeer naar het tabblad Hoge beschikbaarheid.



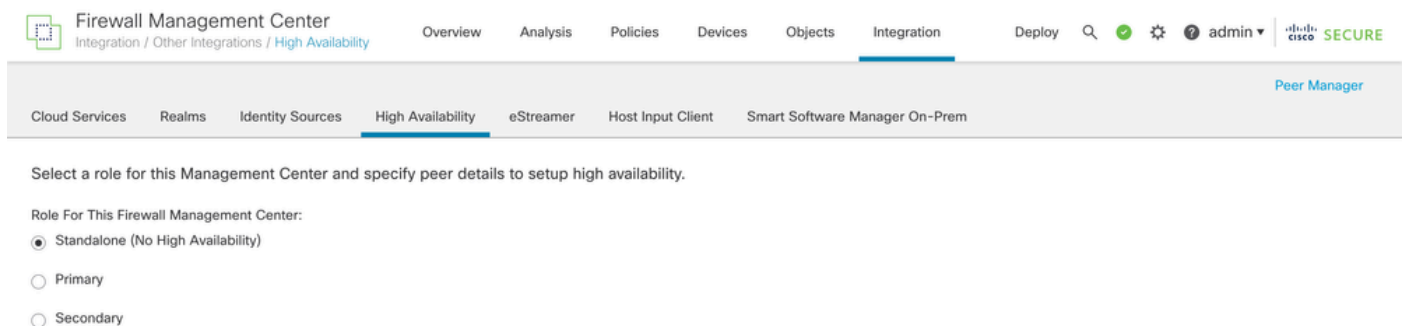
Firewall Management Center  
Integration / Other Integrations / Cloud Services

Overview Analysis Policies Devices Objects Integration

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Naar hoge beschikbaarheid navigeren

Stap 5. Klik op Secundair.



Firewall Management Center  
Integration / Other Integrations / High Availability

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ✔ ⚙️ ❓ admin ▾ cisco SECURE

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem Peer Manager

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Invoer informatie en selecteer de gewenste rol voor het huidige VCC

Stap 6. Voer informatie in van de primaire/actieve peer en klik op **Register**.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Primary Firewall Management Center Host:

Registration Key\*:

Unique NAT ID:

Register

† Either host or NAT ID is required.

Opmerking: Neem nota van de registratiesleutel, aangezien deze op het actieve VCC zal worden gebruikt.

Stap 7. Met deze waarschuwing kunt u dit bevestigen door te klikken op **Yes**.

## Warning

This operation may affect critical processes running in the background. Do you want to continue?

No

Yes



Opmerking: Zorg ervoor dat er geen andere taak wordt uitgevoerd terwijl HA wordt gemaakt, de GUI wordt opnieuw gestart.

---

Stap 8. Bevestig dat u de primaire peer wilt registreren.

## Warning

---

Do you want to register primary peer:  
10.18.19.31?

No

Yes





Waarschuwing: Alle informatie over de Apparaten/Beleid/Configuratie zal worden verwijderd uit Secundair FMC zodra HA wordt gemaakt.

Stap 9. Controleer of de status van het secundaire VCC hangende is.

Host	Last Modified	Status	State	
10.18.19.31	2023-09-28 13:53:56	Pending Registration	<input checked="" type="checkbox"/>	

Primair VCC configureren

Herhaal stap 1 t/m 4 op het primaire/actieve VCC.

Stap 5. Klik op Primair.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Secondary Firewall Management Center Host:

Registration Key\*:

Unique NAT ID:

[Register](#)

† Either host or NAT ID is required.

## Stap 6. Voer de informatie over het secundaire VCC in en klik op Registreren.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Secondary Firewall Management Center Host:

Registration Key\*:

Unique NAT ID:

[Register](#)

† Either host or NAT ID is required.



Opmerking: Gebruik dezelfde registratiesleutel die als secundair VCC wordt gebruikt.

---

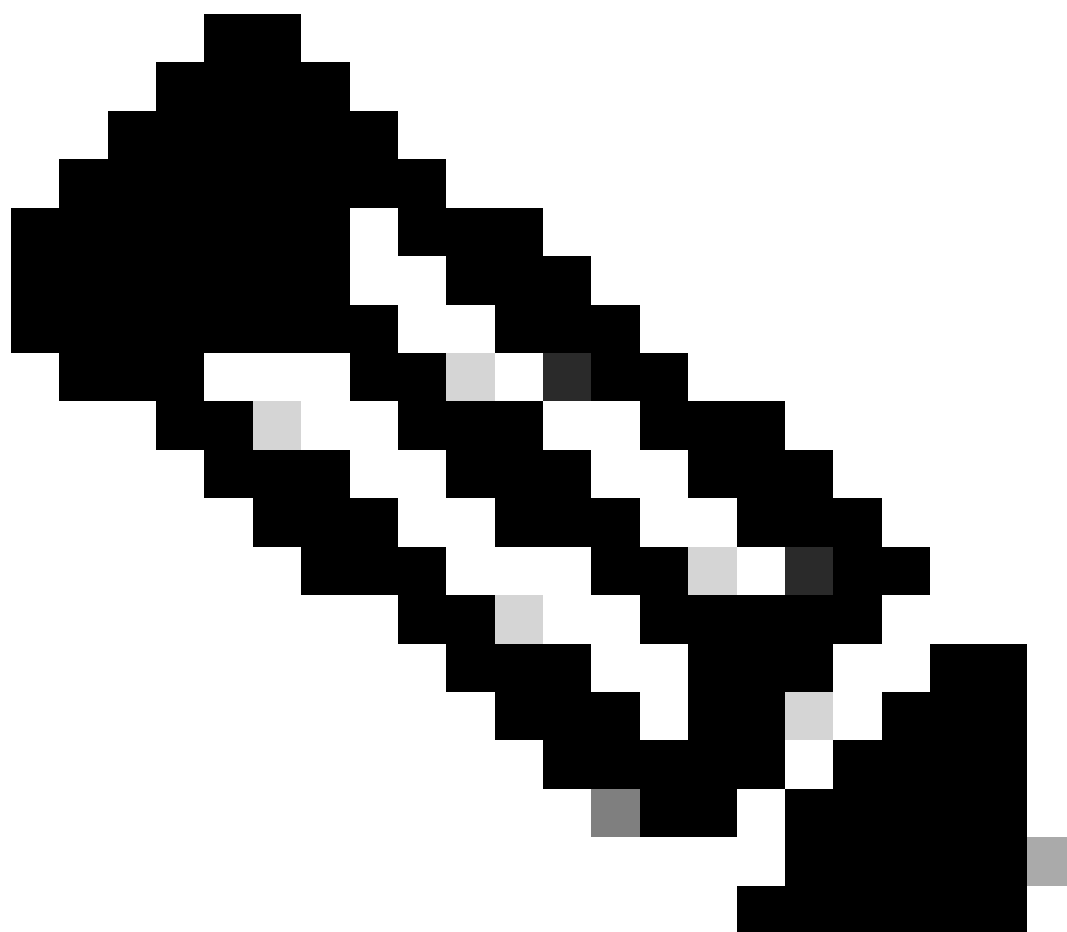
Stap 7. Met deze waarschuwing kunt u dit bevestigen door te klikken op **Yes**.

## Warning

This operation may affect critical processes running in the background. Do you want to continue?

No

Yes



---

Opmerking: Zorg ervoor dat er geen andere taak wordt uitgevoerd.

---

Stap 8. Bevestig dat u zich wilt registreren voor secundair FMC.

## Warning

Secondary peer configuration and policies will be removed. After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license. Do you want to register secondary peer:  
10.18.19.32?

No

Yes



Opmerking: Zorg ervoor dat er geen kritieke informatie over het secundaire VCC is, aangezien het aanvaarden van deze prompt alle configuraties uit het VCC verwijdert.

---

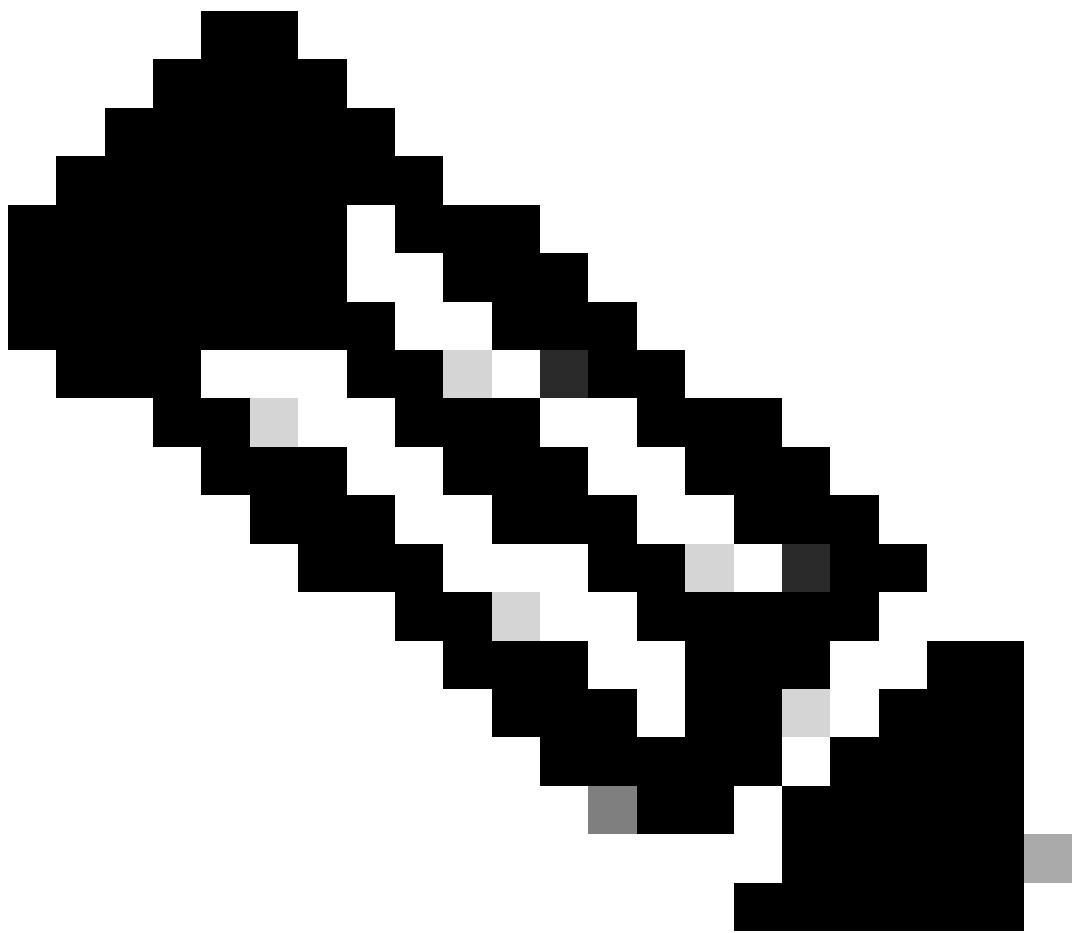
synchronisatie tussen primaire en secundaire start; de duur hangt af van de configuratie en de apparaten. Dit proces kan vanaf beide eenheden worden gevolgd.

[Switch Peer Roles](#) [Break HA](#) [Pause Synchronization](#)

High availability operations are in progress. The status messages and alerts on this page are temporary. Please check after high availability operations are complete. These operations include file copy which may take time to complete. Database files synchronization: 100% of 379MB transferred

Summary	
Status	▲ Temporarily degraded- high availability operations are in progress.
Synchronization	▲ Failed
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	Active - Primary (10.18.19.31)	Standby - Secondary (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware



Opmerking: Terwijl de synchronisatie plaatsvindt, verwacht dat de status Mislukt en Tijdelijk gedegradeerd wordt. Deze status wordt weergegeven totdat het proces is voltooid.

# Verificatie

Zodra de synchronisatie is voltooid, is de verwachte uitvoer Status Gezond en Synchronisatie OK.

The screenshot shows the Firewall Management Center interface for High Availability. The 'Summary' section indicates a healthy status with synchronization OK. The 'System Status' table shows the local system as Active - Primary and the remote system as Standby - Secondary.

Summary	
Status	Healthy
Synchronization	OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	<b>Active - Primary</b> (10.18.19.31)	<b>Standby - Secondary</b> (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

De primaire en secundaire synchronisatie behouden; dit is normaal.

The screenshot shows the Firewall Management Center interface for High Availability. The 'Summary' section indicates that a synchronization task is in progress. The 'System Status' table shows the local system as Standby - Secondary and the remote system as Active - Primary.

Summary	
Status	Synchronization task is in progress
Synchronization	OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	<b>Standby - Secondary</b> (10.18.19.32)	<b>Active - Primary</b> (10.18.19.31)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Neem even de tijd om te bekijken of uw apparaten correct worden weergegeven op zowel Primair als Secundair.



## 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.