Ondersteuning van SHA-256 voor UCCX

Inhoud

Inleiding

Dit document beschrijft SHA-256-ondersteuning voor Cisco Unified Contact Center Express (UCCX). De SHA-1-encryptie zal snel worden afgebroken en alle ondersteunde webbrowsers voor UCCX zullen beginnen webpagina's te blokkeren van servers die certificaten met de SHA-1-encryptie aanbieden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Contact Center Express (UCCX)
- certificaatbeheer

Aankondigingen van Microsoft en Mozilla

[SHA-1 Deprectificatie](#)

[SHA-1-certificaten blijven uitfaseren](#)

In deze mededelingen hebben de browser fabrikanten aangegeven dat de browsers bypassable waarschuwingen zullen tonen voor de aangetroffen SHA-1-certificaten die met **ValidFrom** datums

na 1 januari 2016 worden uitgegeven.

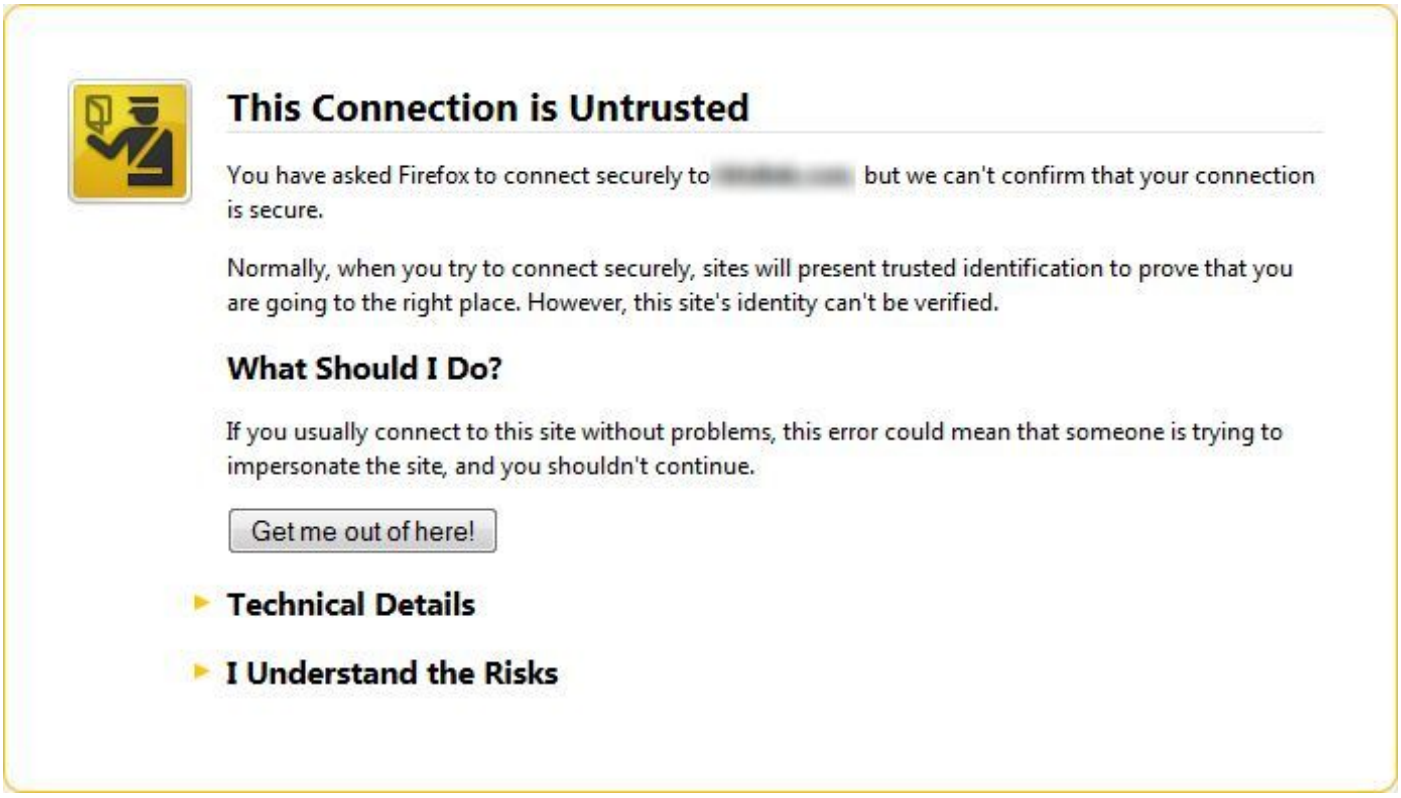
Bovendien is het huidige plattegronden bedoeld om websites te blokkeren die SHA-1-certificaten gebruiken na 1 januari 2017, ongeacht de ValidFrom-vermelding in het certificaat. Maar met recente aanvallen die zich op SHA-1-certificaten richten, kunnen deze browsers deze tijdlijn wel omhoog verplaatsen en websites blokkeren die SHA-1-certificaten gebruiken na 1 januari 2017, ongeacht de datum van uitgifte van het certificaat.

Cisco adviseert klanten om de aankondigingen in detail te lezen en op verdere aankondigingen van Microsoft en Mozilla over dit onderwerp bij te blijven.

Sommige versies van UCCX genereren SHA-1-certificaten. Als u toegang hebt tot UCCX-webpagina's die zijn beschermd door SHA-1-certificaten, genereren ze een waarschuwing of worden ze geblokkeerd volgens de datums en regels die eerder zijn vermeld.

Gebruikershandleiding

Wanneer een SHA-1-certificaat wordt gedetecteerd, afhankelijk van de ValidFrom-datum en de eerder genoemde regels, kan de gebruiker een vergelijkbaar bericht zien:



Afhankelijk van de genomen beslissingen kan een gebruiker deze waarschuwing al dan niet omzeilen.

UCCX-overwegingen

In deze tabellen worden de "SHA-1"-strategieën voor het effect en de verzachting van de effecten van certificaten beschreven voor elke versie van UCCX die momenteel onder softwareonderhoud valt.

Aanwijzingen in dit document

Opmerking	Beschrijving
✅	Reeds ondersteund. Geen verdere actie vereist.
⚠	Er is steun beschikbaar, maar er is behoefte aan regeneratie van certificaten.
⛔	Ondersteuning is niet beschikbaar.

UCCX 11.5

	UCCX-beheer	CUIC-beheer Live Data#	Finesse beheerdesktop#	Agent-e-mail en - Chat met socialMiner*	UCCX REST-scripts
Vers installeren	✅	✅	✅	✅	✅
upgrade vanaf vorige versie	⚠ De UCCX certificaten behouden het algoritme van oudere versies. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	⚠ De UCCX Cisco Unified Intelligence Center (CUIC) certificaten behouden het algoritme van oudere releases. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	⚠ De UCCX Finesse certificaten behouden het algoritme van oudere releases. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	⚠ De SocialMiner **en** UCCX certificaten behouden het algoritme van oudere versies. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	⚠ UCCX wijst een externe webserver die SHA-1-certificaten gebruikt niet af als onderdeel van de Representational State Transfer (REST) communicatie. De REST-stappen worden uitgevoerd nadat de certificaten opnieuw op UCCX zijn gegenereerd.

Opmerking: *De gegenereerde MediaSense en SocialMiner-certificaten moeten opnieuw worden geïmporteerd in UCCX.

Opmerking: er zijn geen afzonderlijke handelingen nodig voor Finse en CUIC. De certificaten worden slechts eenmaal gegenereerd op de pagina van het UCCX-platform beheer.

UCCX 11.0(1)

	UCCX-beheer	CUIC-beheer met actieve gegevens#	Finesse beheerdesktop#	Agent-e-mail en - Chat met social Miner**	UCCX RE
Vers installeren	⚠ Standaard zijn alle	⚠ Standaard zijn alle	⚠ Standaard zijn alle	⚠ Standaard zijn alle	⚠ UCCX v

	zelf getekende nieuwe installatiecertificaten SHA-1-certificaten en moeten deze opnieuw worden gegenereerd.	zelf getekende nieuwe installatiecertificaten SHA-1-certificaten en moeten deze opnieuw worden gegenereerd.	zelf getekende nieuwe installatiecertificaten SHA-1-certificaten en moeten deze opnieuw worden gegenereerd.	zelf getekende nieuwe installatiecertificaten SHA-1-certificaten en moeten deze opnieuw worden gegenereerd.	externe w die S certificate niet af als van de commun REST-s worden u nadat de c opnieuw zijn gege
upgrade vanaf vorige versie	De UCCX certificaten behouden het algoritme van oudere versies. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	De UCCX CUIC certificaten behouden het algoritme van oudere versies. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	De UCCX Finesse certificaten behouden het algoritme van oudere releases. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	De SocialMiner **en** UCCX certificaten behouden het algoritme van oudere versies. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	UCCX v externe w die S certificate niet af als van de commun REST-s worden u nadat de c opnieuw zijn gege

Opmerking: *Er wordt een Speciaal technische ontwerp (ES) vrijgegeven om MediaSense 10.5 en 11.0 toe te staan om SHA-256-certificaten te genereren en te accepteren.

Opmerking: **Het(de) geregenereerde MediaSense en SocialMiner-certificaat(s) moet/moeten opnieuw worden ingevoerd in UCCX.

Opmerking: #Er zijn geen afzonderlijke acties nodig voor Finse en CUIC. De certificaten worden slechts eenmaal gegenereerd op de pagina van het UCCX-platform beheer.

UCCX 10.5 en 10.6

	UCCX-beheer	**CUIC-beheer met actieve gegevens#**	**Finesse beheerdesktop#**	**Agent-e-mail en -Chat met socialMiner***	**UCCX REST-sc**
Vers installeren	Standaard zijn alle zelf getekende nieuwe installatiecertificaten SHA-1-certificaten	Standaard zijn alle zelf getekende nieuwe installatiecertificaten SHA-1-certificaten	Standaard zijn alle zelf getekende nieuwe installatiecertificaten SHA-1-certificaten	SHA-256 ondersteuning voor agent-e-mail en chat is alleen	UCCX wijst e externe webser die SHA-1- certificaten geb niet af als onder

	en moeten deze opnieuw worden gegenereerd.	en moeten deze opnieuw worden gegenereerd.	en moeten deze opnieuw worden gegenereerd.	beschikbaar in SocialMiner (SM) v11 en SM v11 is niet compatibel met UCCX v10.x.	van de REST communicatie. REST-stappe worden uitgevo nadat de certific opnieuw op UC zijn gegeneree
upgrade vanaf vorige versie	De certificaten behouden het algoritme van oudere versies. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	De certificaten behouden het algoritme van oudere versies. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	De certificaten behouden het algoritme van oudere versies. Als het gegenereerd wordt met een SHA-11-toets in oudere releases zijn de zelf-ondertekende certificaten op SHA-1 gebaseerd en moeten ze opnieuw worden gegenereerd.	SHA-256 ondersteuning voor agent-e-mail en chat is alleen beschikbaar in SM v11 en SM v11 is niet compatibel met UCCX v10.x.	UCCX wijst ee externe webser die SHA-1-certificaten gebr niet af als onder van de REST communicatie. REST-stappe worden uitgevo nadat de certific opnieuw op UC zijn gegeneree

Opmerking: *Er wordt een Speciaal technisch ontwerp vrijgegeven om SocialMiner 10.6 toe te staan om SHA-256-certificaten te genereren en te accepteren.

Opmerking: **Er wordt een Engineering Special (ES) vrijgegeven om MediaSense 10.0 en 10.5 te laten genereren en accepteren van SHA-256-certificaten.

Opmerking: ***De regenereerde MediaSense en SocialMiner-certificaten moeten opnieuw worden ingevoerd in UCCX.

Opmerking: #Er zijn geen afzonderlijke acties nodig voor Finse en CUIC. De certificaten worden slechts eenmaal gegenereerd op de pagina van het UCCX-platform beheer.

UCCX 10.0

	UCS-beheer*	CUIC-beheer met actieve gegevens#	Finesse beheerdesktop#	Agent Chat met SocialMiner*	UC
Vers installeren	Het standaard zelfgetekende certificaat is SHA-1. Het regeneratiecertificaat biedt geen optie voor SHA-256.	Het standaard zelfgetekende certificaat is SHA-1. Het regeneratiecertificaat biedt geen optie voor SHA-256.	Het standaard zelfgetekende certificaat is SHA-1. Het regeneratiecertificaat biedt geen optie voor SHA-256.	SHA-256-ondersteuning voor gespreksfuncties is alleen beschikbaar in SM v11 en SM v11 is niet compatibel met UCCX v10.x.	U ext cer niet v co

upgrade vanaf vorige versie	Het standaard zelfgetekende certificaat is SHA-1. Het regeneratiecertificaat biedt geen optie voor SHA-256.	Het standaard zelfgetekende certificaat is SHA-1. Het regeneratiecertificaat biedt geen optie voor SHA-256.	Het standaard zelfgetekende certificaat is SHA-1. Het regeneratiecertificaat biedt geen optie voor SHA-256.	SHA-256-ondersteuning voor gespreksfuncties is alleen beschikbaar in SM v11 en SM v11 is niet compatibel met UCCX v10.x.	R wo nad opr zij U ext cer niet v co R wo nad opr zij

Opmerking: *Er wordt een Speciaal technisch ontwerp vrijgegeven om SocialMiner 10.6 toe te staan om SHA-256-certificaten te genereren en te accepteren.

Opmerking: **Er wordt een Engineering Special (ES) vrijgegeven om MediaSense 10.0 te laten genereren en accepteren van SHA-256-certificaten.

Opmerking: ***De regenereerde MediaSense en SocialMiner-certificaten moeten opnieuw worden ingevoerd in UCCX.

Opmerking: #Er zijn geen afzonderlijke acties nodig voor Finse en CUIC. De certificaten worden slechts eenmaal gegenereerd op de pagina van het UCCX-platform beheer.

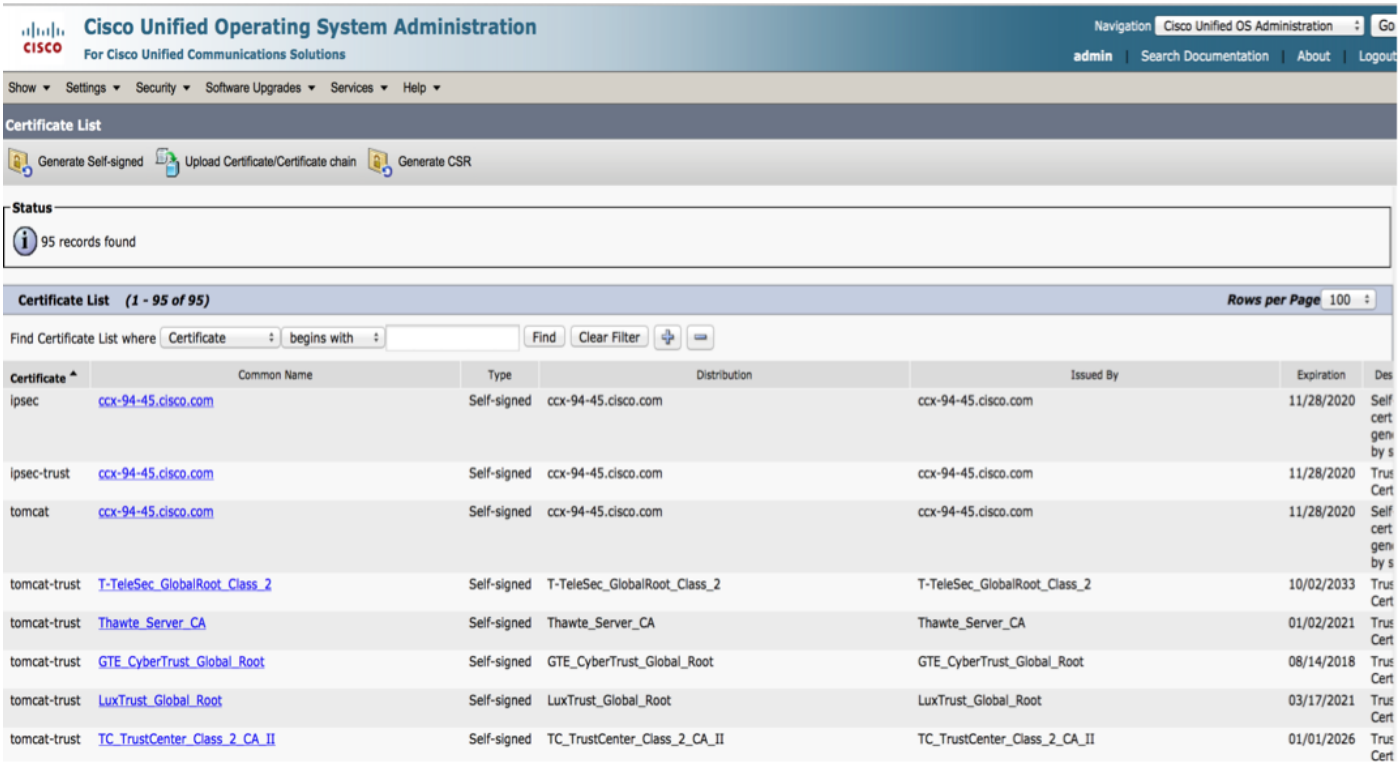
Instructies voor certificaatbeheer

Er zijn drie soorten certificaten die moeten worden gecontroleerd en mogelijk moeten worden geregenereerd:

- Zelfgetekende certificaten
- Trusted wortelcertificaten
- Door derden ondertekende certificaten

Zelfondertekende certificaten

Navigeer naar de pagina OS-beheer. Kies **Beveiliging > Navigeren in naar certificaatbeheer**. Klik op **Zoeken**.



Merk de vier categorieën certificaten op:

- ipsec
- ipsec-trust
- tomcat
- kat-trust

De certificaten in de categorie **tomcat** en type **zelfgetekend** zijn de certificaten die regeneratie vereisen. In de vorige afbeelding is het derde certificaat het certificaat dat moet worden gerestaureerd.

Voltooi deze stappen om certificaten te regenereren:

Stap 1. Klik op de Gemeenschappelijke naam van het certificaat.

Stap 2. Klik vanuit het popupvenster op **Opnieuw genereren**.

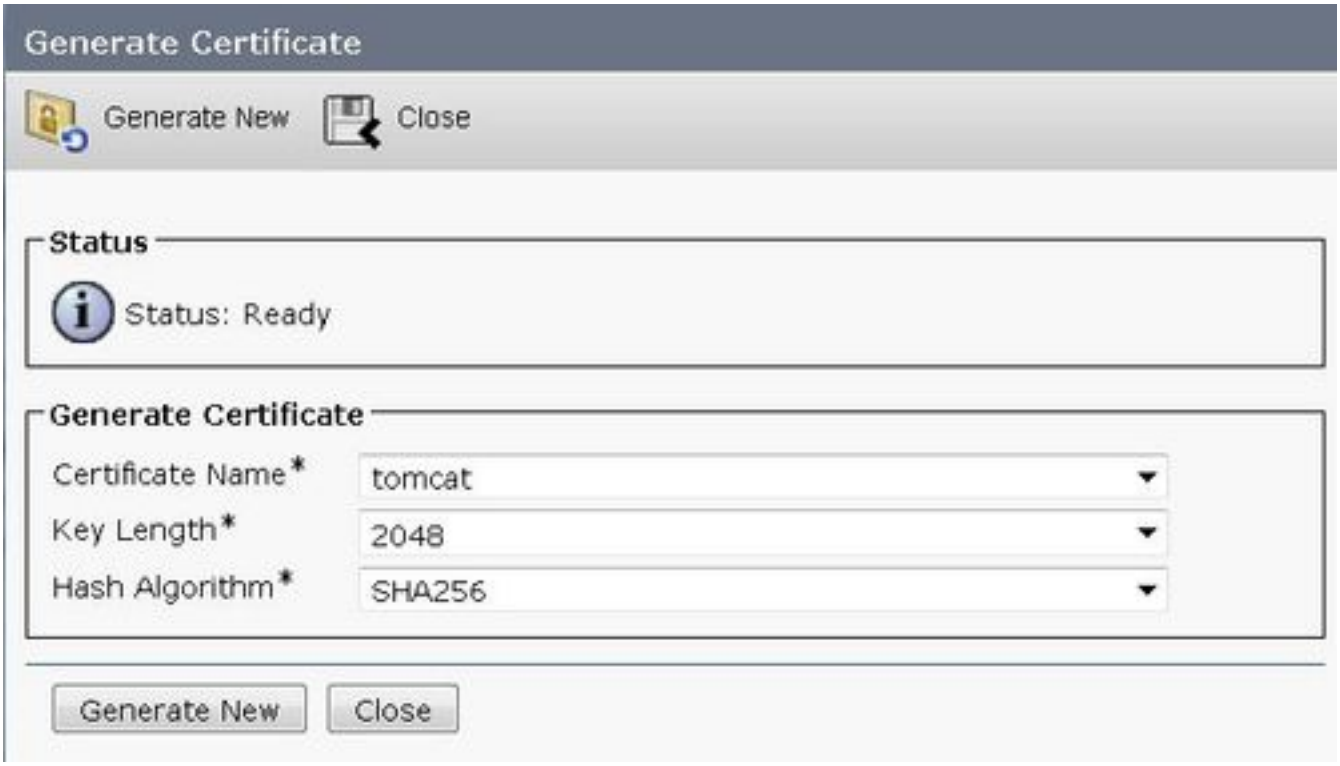
Stap 3. Kies het encryptiealgoritme van SHA-256.

Voltooi de volgende stappen voor UCCX versie 10.6 om certificaten te regenereren:

Stap 1. Klik op **Generate New**.

Stap 2. Selecteer *certificaatnaam* als **zodanig**, *toetslang* als **2048** en *algoritme* **Hash** als SHA256.

Stap 3. Klik op **Generate New.**



Trusted Root-certificaten

Dit zijn de certificaten die door het platform worden verstrekt. Op SHA-1 gebaseerde handtekeningen voor deze certificaten zijn geen probleem, omdat deze certificaten worden vertrouwd door de cliënten van de Transport Layer Security (TLS) op basis van hun identiteit, in plaats van door de ondertekening van hun hash.

Door derden ondertekende certificaten

Certificaten die door een certificeringsinstantie van een derde partij met het SHA-1-algoritme zijn ondertekend, moeten opnieuw worden ingevoerd met de SHA-256 ondertekende certificaten. Alle certificaten in een certificeringsketen moeten worden afgevoerd met SHA-256.

Extra opmerkingen

De nieuwste technische specificaties worden indien beschikbaar op cisco.com geplaatst. Controleer de corresponderende productpagina's regelmatig op speciale downloads van technische apparatuur.

- Open een Cisco TAC-case voor ondersteuning van certificeringsregeneratie of verwante problemen.
- Klanten die op UCCX versies 8.x of 9.x draaien, moeten van plan zijn om te upgraden naar de nieuwste ondersteunde releases om Cisco- en browser-ondersteuning te behouden.

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.