

TLS-/SSL-certificaten configureren in ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Servercertificaten](#)

[ISE-certificaten](#)

[Systeemcertificaten](#)

[Trusted Certificates Store](#)

[Basis taken](#)

[Een zelfondertekend certificaat genereren](#)

[Verleng een zelfondertekend certificaat](#)

[Een betrouwbaar certificaat installeren](#)

[Een door CA ondertekend certificaat installeren](#)

[Reserve-certificaten en privésleutels](#)

[Problemen oplossen](#)

[Controleer de geldigheid van het certificaat](#)

[Een certificaat verwijderen](#)

[Supplicant vertrouwt niet op het ISE-servercertificaat bij een 802.1x-verificatie](#)

[ISE-certificaatketen is correct maar endpoint weigert ISE-servercertificaat tijdens verificatie](#)

[Veelgestelde vragen](#)

[Wat te doen als ISE een waarschuwing geeft dat het certificaat al bestaat?](#)

[Waarom geeft de browser een waarschuwing dat de portal pagina van ISE wordt gepresenteerd door een onbetrouwbare server?](#)

[Wat te doen wanneer een upgrade mislukt vanwege ongeldige certificaten?](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft TLS-/SSL-certificaten in Cisco ISE, de soorten en rollen van ISE-certificaten, hoe u veelvoorkomende taken en probleemoplossing kunt uitvoeren, en beantwoordt veelgestelde vragen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

1. Cisco Identity Services Engine (ISE)
2. De terminologie die wordt gebruikt om verschillende typen ISE- en AAA-implementaties te beschrijven.

3. RADIUS-protocol en AAA-basisgegevens
4. SSL/TLS- en x509-certificaten
5. Basis publieke sleutelinfrastructuur (PKI)

Gebruikte componenten

De informatie in dit document is gebaseerd op de software en hardwareversies van Cisco ISE, releases 2.4 - 2.7. Het dekt ISE van versie 2.4 tot 2.7, maar het moet vergelijkbaar of identiek zijn met andere ISE 2.x-software-releases, tenzij anders vermeld.

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.

Servercertificaten

Servercertificaten worden door servers gebruikt om de identiteit van de server aan de clients voor te stellen voor authenticiteit en om een veilig kanaal voor communicatie te bieden. Deze kunnen zelf worden ondertekend (waarbij de server het certificaat aan zichzelf afgeeft) of worden afgegeven door een certificeringsinstantie (hetzij intern binnen een organisatie of van een bekende verkoper).

Servercertificaten worden doorgaans afgegeven aan hostnamen of FQDN (Fully Qualified Domain Name) van de server, of ze kunnen ook een wildcard-certificaat zijn (*.domain.com). De host(s), het domein of het subdomein(en) waaraan het wordt uitgegeven, worden doorgaans vermeld in de velden algemene naam (CN) of alternatieve naam (SAN) voor onderwerpgebied.

Wildcard-certificaten zijn SSL-certificaten die gebruikmaken van een wildcard-notatie (een asterisk in plaats van hostnaam) en dus het mogelijk maken dat hetzelfde certificaat wordt gedeeld door meerdere hosts in een organisatie. Bijvoorbeeld, kan de waarde van CN of van SAN voor een vervangingscertificaten Onderwerpnaam gelijkaardig kijken aan *.company.com en kan worden gebruikt om alle hosts van dit domein zoals server1.com, server2.com en ga zo maar door.

De certificaten gebruiken typisch Public-Key cryptografie of asymmetrische encryptie.

- Openbare sleutel: De openbare sleutel is aanwezig in het certificaat in een van de velden, en wordt openbaar gedeeld door een systeem wanneer een apparaat probeert te communiceren met het.
- Privé Sleutel: De privé sleutel is privé aan het eindstelsel en is gekoppeld met de Openbare Sleutel. Gegevens die met een openbare sleutel zijn versleuteld, kunnen alleen worden gedecodeerd met de specifieke gekoppelde privé-sleutel en omgekeerd.

ISE-certificaten

Cisco ISE vertrouwt op Public Key Infrastructure (PKI) om beveiligde communicatie te bieden met endpoints, gebruikers, beheerders enzovoort, en tussen Cisco ISE-knooppunten in een multinode-implementatie. PKI vertrouwt op x.509 digitale certificaten om openbare sleutels voor de encryptie en de decryptie van berichten over te brengen, en de authenticiteit van andere certificaten te verifiëren die door gebruikers en apparaten worden voorgesteld. Cisco ISE heeft twee categorieën certificaten die doorgaans worden gebruikt:

- **Systeemcertificaten:** dit zijn servercertificaten die een Cisco ISE-knooppunt voor clients identificeren. Elk Cisco ISE-knooppunt heeft zijn eigen lokale certificaten, die elk samen met de respectieve persoonlijke sleutel op het knooppunt zijn opgeslagen.
- **Trusted Certificates Store Certificates:** Dit zijn certificaten van de certificeringsinstantie (CA) die worden gebruikt om de certificaten te valideren die voor verschillende doeleinden aan de ISE worden voorgelegd. Deze certificaten in de Certificate Store worden beheerd op het knooppunt voor primair beheer en worden gerepliceerd naar alle andere knooppunten in een gedistribueerde Cisco ISE-implementatie. Het certificaatarchief bevat ook certificaten die voor de ISE-knooppunten worden gegenereerd door de interne certificeringsinstantie van ISE die voor BYOD is bestemd.

Systemcertificaten

Systemcertificaten kunnen worden gebruikt voor een of meer rollen. Elke rol dient een ander doel en wordt hier uitgelegd:

- **Admin:** Dit wordt gebruikt om alle communicatie via 443 (Admin GUI) te beveiligen, evenals voor replicatie en voor elke poort/elk gebruik dat hier niet wordt vermeld.
- **Portal:** Dit wordt gebruikt om de communicatie van HTTP over de portals zoals het Gecentraliseerde Poorten van de Verificatie van het Web (CWA), Gast, BYOD, Clientlevering, de portalen van de Native Supplicant Provisioning, etc. te beveiligen. Elke Portal moet worden toegewezen aan een Portal Group Tag (standaard is Default Portal Group Tag) die de portal instrueert op het specifiek gelabelde certificaat dat moet worden gebruikt. In het vervolkeuzemenu Portal Group Tag name in de opties Bewerken van het certificaat kunt u een nieuwe tag maken of een bestaande tag kiezen.
- **EAP:** Dit is een rol die het certificaat specificeert dat aan clients wordt aangeboden voor 802.1x-verificatie. Certificaten worden gebruikt met vrijwel alle mogelijke EAP-methoden, zoals EAP-TLS, PEAP, EAP-FAST, enzovoort. Met EAP-methoden met tunnels zoals PEAP en FAST wordt TLS (Transport Layer Security) gebruikt om de uitwisseling van referenties te beveiligen. De client aanmeldingsgegevens worden pas naar de server verzonden nadat deze tunnel is gemaakt om een veilige uitwisseling te garanderen.
- **RADIUS-DTLS:** met deze rol wordt het certificaat gespecificeerd dat moet worden gebruikt voor een DTLS-verbinding (TLS-verbinding via UDP) om RADIUS-verkeer tussen een netwerktoegangsapparaat (NAD) en de ISE te versleutelen. En u moet beschikken over DTLS-encryptie die deze functie kan gebruiken.
- **SAML:** Het servercertificaat wordt gebruikt voor de beveiligde communicatie met de SAML Identity Provider (IDP). Een certificaat dat bedoeld is voor gebruik door SAML kan niet worden gebruikt voor andere services, zoals Admin, EAP-verificatie enzovoort.
- **ISE Messaging Service:** sinds 2.6 maakt ISE gebruik van ISE Messaging Service in plaats

van het legacy Syslog protocol om gegevens te registreren. Dit wordt gebruikt om deze communicatie te versleutelen.

- PxGrid: Dit certificaat wordt gebruikt voor PxGrid-services op ISE.

Wanneer ISE wordt geïnstalleerd, genereert het een Default Self-Signed Server Certificate. Dit wordt standaard toegewezen voor EAP-verificatie, Admin, Portal en RADIUS DTLS. Het wordt aanbevolen om deze rollen te verplaatsen naar een interne CA of een bekend CA-ondertekend certificaat.

Friendly Name	Used By	Portal group tag	Valid From	Valid To	
hongkongise					
OU=Certificate Services System Certificate, CN=hongkongise.riverdale.local\Certificate Services Endpoint Sub CA - hongkongise#00002	pxGrid	hongkongise.riverdale.local	Certificate Services Endpoint Sub CA - hongkongise	Mon, 13 Apr 2020	Sun, 14 Apr 2030
OU=ISE Messaging Service, CN=hongkongise.riverdale.local\Certificate Services Endpoint Sub CA - hongkongise#00001	ISE Messaging Service	hongkongise.riverdale.local	Certificate Services Endpoint Sub CA - hongkongise	Mon, 13 Apr 2020	Sun, 14 Apr 2030
Default self-signed saml server certificate - CN=SAML_hongkongise.riverdale.local	SAML	SAML_hongkongise.riverdale.local	SAML_hongkongise.riverdale.local	Tue, 14 Apr 2020	Wed, 14 Apr 2021
Default self-signed server certificate	EAP, Administration, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	hongkongise.riverdale.local	hongkongise.riverdale.local	Tue, 14 Apr 2020

Tip: het is een goede werkwijze om ervoor te zorgen dat zowel de FQDN- als IP-adressen van de ISE-server worden toegevoegd aan het SAN-veld van het ISE-systeemcertificaat. In het algemeen kunt u, om ervoor te zorgen dat de certificaatverificatie in Cisco ISE niet wordt beïnvloed door kleine verschillen in de op certificaat gebaseerde verificatiefuncties, in kleine letters hostnamen gebruiken voor alle Cisco ISE-knooppunten die in een netwerk worden geïmplementeerd.

Opmerking: het formaat van een ISE-certificaat moet zijn: Privacy Enhanced Mail (PEM) of Distinguished Encoding Rules (DER).

Trusted Certificates Store

Certificaatcertificaten moeten worden opgeslagen op: Administration > System > Certificates > Certificate Store en moeten beschikken over Trust for client authentication use-case om ervoor te zorgen dat ISE deze certificaten gebruikt om de certificaten te valideren die worden aangeboden door de eindpunten, apparaten of andere ISE-knooppunten.

System Certificates	Trusted Certificates	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
<input type="checkbox"/>	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...	Baltimore CyberTrust Ro...	Fri, 12 May 2000	Mon, 12 May 2025
<input type="checkbox"/>	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029
<input type="checkbox"/>	Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2053
<input type="checkbox"/>	Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 2038
<input type="checkbox"/>	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA ...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
<input type="checkbox"/>	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029
<input type="checkbox"/>	Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 CE ...	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016	Sun, 9 Aug 2099
<input type="checkbox"/>	Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 D3 ...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 2033
<input type="checkbox"/>	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037
<input type="checkbox"/>	Cisco RXC-R2	Enabled	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034
<input type="checkbox"/>	Default self-signed server certificate	Enabled	Endpoints Infrastructure	5E 95 93 55 00 00 ...	hongkongise.inverdale.local	hongkongise.inverdale.local	Tue, 14 Apr 2020	Wed, 14 Apr 2021
<input type="checkbox"/>	DigCert Global Root CA	Enabled	Cisco Services	08 3B E0 56 90 42 ...	DigCert Global Root CA	DigCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov 2031
<input type="checkbox"/>	DigCert root CA	Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 0B ...	DigCert High Assurance ...	DigCert High Assurance ...	Fri, 10 Nov 2006	Mon, 10 Nov 2031
<input type="checkbox"/>	DigCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC 5C ...	DigCert SHA2 High Assu...	DigCert High Assurance ...	Tue, 22 Oct 2013	Sun, 22 Oct 2028
<input type="checkbox"/>	DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3 ...	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021
<input type="checkbox"/>	HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0 ...	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2023
<input type="checkbox"/>	QuoVadis Root CA 2	Enabled	Cisco Services	05 09	QuoVadis Root CA 2	QuoVadis Root CA 2	Fri, 24 Nov 2006	Mon, 24 Nov 2031
<input type="checkbox"/>	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5 ...	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Wed, 16 Jul 2036
<input type="checkbox"/>	VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D ...	VeriSign Class 3 Public Pr...	VeriSign Class 3 Public Pr...	Wed, 8 Nov 2006	Wed, 16 Jul 2036
<input type="checkbox"/>	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03 ...	VeriSign Class 3 Secure ...	VeriSign Class 3 Public Pr...	Mon, 8 Feb 2010	Fri, 7 Feb 2020

Basis taken

Het certificaat heeft een vervaldatum en kan op een bepaald moment worden ingetrokken of vervangen. Als het ISE-servercertificaat verloopt, kunnen er ernstige problemen ontstaan, tenzij ze worden vervangen door een nieuw, geldig certificaat.

Opmerking: als het certificaat dat wordt gebruikt voor het EAP (Extensible Verification Protocol) verloopt, kunnen clientverificaties mislukken omdat de client niet meer vertrouwt op het ISE-certificaat. Als een certificaat dat gebruikt wordt voor portals verloopt, kunnen klanten en browsers weigeren om verbinding te maken met de portal. Als het Administratiecertificaat verloopt, is het risico nog groter, waardoor een beheerder niet meer kan inloggen op de ISE en de gedistribueerde implementatie kan ophouden te functioneren zoals het moet.

Een zelfondertekend certificaat genereren

Om nieuwe zelfondertekende certificaten te genereren, navigeer naar Administration > System > Certificates > System Certificates. Klik op de Generate Self Signed Certificate.

System Certificates ⚠️ For disaster recovery it is recommended to export certificate and private key pairs

Friendly Name	Used By	Portal group tag	Issued To
hongkongise	pxGrid		hongkongis

Deze lijst beschrijft de velden op de pagina Generate Self Signed Certificate.

Zelfondertekende certificaatinstellingen Richtlijnen voor het gebruik van veldnamen:

- Selecteer Knooppunt: (verplicht) Het knooppunt waarvoor het nodig is om het systeemcertificaat te genereren.
- CN: (Vereist als SAN niet is gespecificeerd) Standaard is de CN de FQDN van het ISE-knooppunt waarvoor het zelfondertekende certificaat wordt gegenereerd.
- Organisatorische eenheid (OU): Organisatorische Eenheidsnaam, bijvoorbeeld Engineering.
- Organisatie (O): naam van de organisatie, bijvoorbeeld Cisco.
- Stad (L): (Niet afkorten) Naam van de stad, bijvoorbeeld, San Jose.
- State (ST): (Niet afkorten) State name, bijvoorbeeld, California.
- Land (C): Landnaam. De tweeletterige ISO-landencode is vereist. Bijvoorbeeld de VS.
- SAN: een IP-adres, DNS-naam of Uniform Resource Identifier (URI) dat aan het certificaat is gekoppeld.
- Sleuteltype: Geef aan welk algoritme moet worden gebruikt om de openbare sleutel te maken: RSA of ECDSA.
- Key Lengte: Geef de bitgrootte op voor de openbare sleutel. Deze opties zijn beschikbaar voor RSA: 512 1024 2048 4096 en deze opties zijn beschikbaar voor ECDSA: 256 384.
- Digest to Sign With: Kies een van deze hash algoritmen: SHA-1 of SHA-256.
- Certificaatbeleid: Voer het certificaatbeleid of de lijst van OID's in waaraan het certificaat moet voldoen. Gebruik komma's of spaties om de OID's te scheiden.
- Vervaldatum: Geef het aantal dagen op waarna het certificaat vervalt.
- Vriendelijke Naam: Voer een vriendelijke naam in voor het certificaat. Als er geen naam is opgegeven, maakt Cisco ISE automatisch een naam in de indeling aan waarbij is een uniek vijf-cijferig getal.
- Wildcard Certificaten toestaan: Schakel dit selectievakje in om een zelfondertekend wildcard-certificaat te genereren (een certificaat dat een sterretje (*) bevat in elke CN in het onderwerp en/of de DNS-naam in het SAN. De DNS-naam die aan het SAN is toegewezen, kan bijvoorbeeld *.domain.com.
- Gebruik: Kies de service waarvoor dit systeemcertificaat moet worden gebruikt. De beschikbare opties zijn:
BeheerderEAP-verificatieRADIUS-DTLSPXGridSAMLPortal



Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

Generate Self Signed Certificate

* Select Node

Subject

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)

* Key type

* Key Length

* Digest to Sign With

Certificate Policies

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

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

System Certificates

Trusted Certificates

OCSF Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

Subject Alternative Name (SAN) IP Address 10.127.196.248

* Key type RSA

* Key Length 2048

* Digest to Sign With SHA-256

Certificate Policies

* Expiration TTL 10 years

Friendly Name

Allow Wildcard Certificates

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- SAML: Use certificate for SAML Signing
- Portal: Use for portal

Submit Cancel

Opmerking: openbare RSA- en ECDSA-sleutels kunnen verschillende lengtes hebben voor hetzelfde beveiligingsniveau. Kies 2048 als het de bedoeling is om een openbaar CA-ondertekend certificaat te verkrijgen of Cisco ISE te implementeren als een FIPS-compatibel beleidsbeheersysteem.

Verleng een zelfondertekend certificaat

Om de zelfondertekende certificaten te bekijken die bestaan, bladert u naar Administration > System > Certificates > System Certificates in de ISE-console. Elk certificaat met de 'Afgegeven aan' en 'Afgegeven door' indien vermeld in dezelfde ISE-server FQDN, dan is het een zelfondertekend certificaat. Kies dit certificaat en klik op Edit.

Onder Renew Self Signed Certificate, controleer Renewal Period Draai het vakje aan en stel de verloopdatumnotatie naar wens in. Klik tot slot op Save.

Een betrouwbaar certificaat installeren

Verkrijg de Base 64 encoded certificate(s) van de Root CA, Intermediate CA(s) en/of de Hosts die moeten worden vertrouwd.

1. Log in op het ISE-knooppunt en navigeer naar Administration > System > Certificate > Certificate Management > Trusted Certificates en klik op Import, zoals in deze afbeelding wordt getoond.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. Below this, a breadcrumb trail shows 'System' > 'Identity Management' > 'Network Resources' > 'Device Portal Management' > 'pxGrid Services'. The main navigation menu is open, showing 'Certificates' selected. Under 'Certificates', the 'Trusted Certificates' option is highlighted. The main content area displays the 'Trusted Certificates' page with a toolbar containing 'Edit', 'Import' (highlighted in yellow), 'Export', 'Delete', and 'View'. Below the toolbar is a table of certificates:

<input type="checkbox"/>	Friendly Name	Status
<input type="checkbox"/>	Baltimore CyberTrust Root	✓
<input type="checkbox"/>	Cisco CA Manufacturing	⊘
<input type="checkbox"/>	Cisco ECC Root CA	✓
<input type="checkbox"/>	Cisco Licensing Root CA	✓

2. Upload op de volgende pagina de CA-certificaten die zijn verkregen (in dezelfde volgorde als eerder beschreven). Geef ze een vriendelijke naam en een beschrijving die uitlegt waar het certificaat voor is om te volgen.

Afhankelijk van de behoeften van het gebruik kruist u de vakjes aan naast:

- Vertrouwen voor verificatie binnen ISE - Dit is om nieuwe ISE-knooppunten toe te voegen wanneer ze hetzelfde vertrouwde CA-certificaat hebben geladen in hun Trusted Certificate Store.
- Vertrouwen voor clientverificatie en Syslog - Schakel deze optie in om het certificaat te gebruiken voor het verifiëren van eindpunten die verbinding maken met ISE met EAP- en/of trust Secure Syslog-servers.
- Vertrouwen voor verificatie van Cisco-services - Dit is alleen nodig om externe Cisco-services zoals een feed-service te vertrouwen.

3. Klik tot slot Submit. Het certificaat moet nu zichtbaar zijn in de Trusted Store en worden gesynchroniseerd met alle secundaire ISE-knooppunten (indien in een implementatie).

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu on the left includes 'Certificate Management' with sub-items: System Certificates, Trusted Certificates, OSCP Client Profile, Certificate Signing Requests, and Certificate Periodic Check Settings. The main content area is titled 'Import a new Certificate into the Certificate Store'. It contains the following fields and options:

- * Certificate File: CA certificate.cer
- Friendly Name:
- Trusted For: Trust for authentication within ISE, Trust for client authentication and Syslog, Trust for authentication of Cisco Services, Validate Certificate Extensions
- Description:
- Buttons:

Een door CA ondertekend certificaat installeren

Zodra de Root- en Intermediate CA(s)-certificaten zijn toegevoegd aan het Trusted Certificate Store, kan een certificaatondertekeningaanvraag worden afgegeven en kan het op basis van de CSR ondertekende certificaat worden gebonden aan het ISE-knooppunt.

1. Hiervoor bladert u naar **Administration > System > Certificates > Certificate Signing Requests** en klik op **Generate Certificate Signing Requests (CSR)** een MVO genereren.

2. Kies in het gedeelte **Gebruik** de rol die u wilt gebruiken in het vervolgkeuzemenu op de pagina die wordt weergegeven.

Als het certificaat voor meerdere rollen wordt gebruikt, kies dan **Meervoudig gebruik**. Zodra het certificaat is gegenereerd, kunnen de rollen indien nodig worden gewijzigd. In de meeste gevallen kan het certificaat worden ingesteld om te worden gebruikt voor meervoudig gebruik in de vervolgkeuzelijst **Gebruikt voor**; dit maakt het mogelijk dat het certificaat bruikbaar is voor alle ISE-webportalen.

3. Vink het vakje naast de ISE-knooppunten aan om de knooppunten te kiezen waarvoor het certificaat wordt gegenereerd.

4. Als het doel is een wildcard-certificaat te installeren/genereren, controleert u het **Allow Wildcard Certificates** doos.

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

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:


ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - This is not a signing request, but an ability to generate a brand new Messaging certificate.

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for  You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).


Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input type="checkbox"/> hongkongise	hongkongise#Multi-Use

Usage

Certificate(s) will be used for  You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input type="checkbox"/> hongkongise	hongkongise#Multi-Use

5. Vul de onderwerpregel in op basis van gegevens over de host of organisatie (organisatie, organisatie, stad, staat en land).

6. Klik om dit te voltooien op **Generate** en klik vervolgens op **Export** op de pop-up die verschijnt.

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

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

▼ Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

► Certificate Authority

hongkongise hongkongise#Multi-Use

Subject

Common Name (CN) \$FQDN\$ ⓘ

Organizational Unit (OU) Security ⓘ

Organization (O) IT ⓘ

City (L) Kolkata

State (ST) West Bengal

Country (C) IN

Subject Alternative Name (SAN) IP Address 10.127.196.248 - + ⓘ

* Key type RSA ⓘ

* Key Length 2048 ⓘ

* Digest to Sign With SHA-256

Certificate Policies

Generate Cancel

Country (C) IN

Subject Alternative Name (SAN) | | - + ⓘ

- DNS Name
- IP Address
- Uniform Resource Identifier
- Directory Name

* Key type RSA

* Key Length 2048 ⓘ

* Digest to Sign With SHA-256

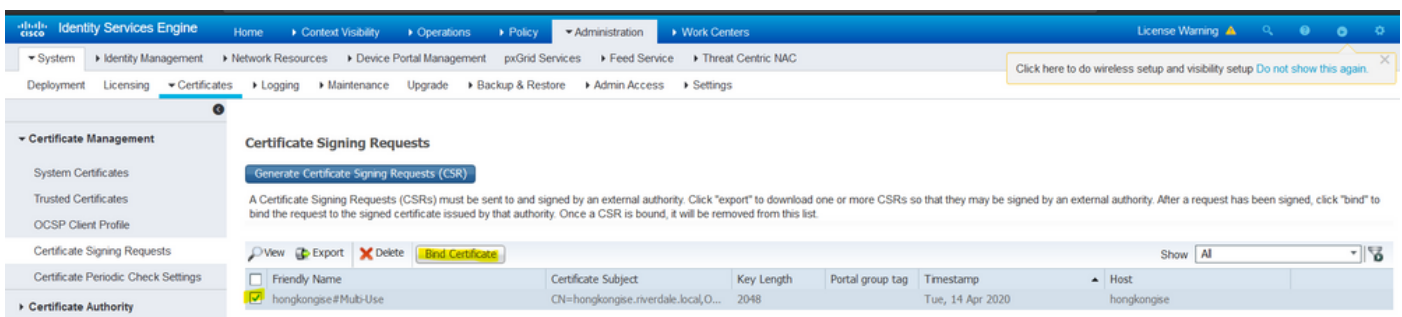
Dit downloadt het Base-64-encoded certificaatverzoek dat net is gemaakt - dit PEM-bestand moet naar CA worden verzonden voor ondertekening, en het resulterende ondertekende certificaat CER-bestand verkrijgen (Base 64 encoded).

Opmerking: onder de GN-velden vult ISE automatisch de knooppunten FQDN.

Opmerking: in ISE 1.3 en 1.4 was het verplicht om twee CSR's uit te geven om ten minste pxGrid te gebruiken. De ene is gewijd aan pxGrid en de andere aan de rest van de diensten. Sinds 2.0 en later staat dit allemaal op één MVO.

Opmerking: als het certificaat wordt gebruikt voor EAP-verificaties, mag het '*'-symbool niet in het veld Onderwerp GN staan, omdat Windows-aanvragers het servercertificaat afwijzen. Zelfs als Validate Server Identity is uitgeschakeld op de aanvrager, kan de SSL handdruk mislukken als de '*' in het CN veld staat. In plaats daarvan kan een generieke FQDN worden gebruikt in het veld CN, en vervolgens in de *.domain.com Kan worden gebruikt in het veld SAN DNS-naam. Sommige certificeringsinstanties (CA) kunnen de wildcard (*) automatisch toevoegen in de GN van het certificaat, ook als deze niet in de CSR voorkomt. In dit scenario moet een speciaal verzoek worden ingediend om deze actie te voorkomen.

7. Nadat het certificaat is ondertekend door de CA (dat is gegenereerd vanuit de CSR zoals in de video wordt getoond, [hier](#) als Microsoft CA wordt gebruikt), gaat u terug naar ISE GUI en navigeer naar **Beheer > Systeem > Certificaatbeheer > Certificaatondertekeningaanvraag**; controleer het vakje naast de CSR die eerder is gemaakt en klik op de knop **Bindcertificaat**.



The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The navigation path is: Administration > Work Centers > Certificates. The page title is "Certificate Signing Requests". There is a "Generate Certificate Signing Requests (CSR)" button. Below it, a text box explains that CSRs must be sent to and signed by an external authority. A table lists the CSR requests with the following columns: Friendly Name, Certificate Subject, Key Length, Portal group tag, Timestamp, and Host. The first entry has a checked checkbox in the Friendly Name column.

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input checked="" type="checkbox"/> hongkongse# Multi-Use	CN=hongkongse.rverdale.local,O=...	2048		Tue, 14 Apr 2020	hongkongse

8. Upload vervolgens het ondertekende certificaat dat zojuist is ontvangen en geef het een vriendschappelijke naam voor ISE. Kies vervolgens de vakjes naast het gebruik naar behoefte voor het certificaat (zoals Admin- en EAP-verificatie, Portal, enzovoort) en klik op Submit, zoals getoond in deze afbeelding:

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

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Trusted Certificates
- OCSF Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Bind CA Signed Certificate

* Certificate File certnew(1).cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal

* Portal group tag ⓘ

Portal(s) using this tag

BYOD Portal (default)	Blacklist Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	MDM Portal (default)
My Devices Portal (default)	Self-Registered Guest Portal (default)
Sponsor Portal (default)	Sponsored Guest Portal (default)

Als de Admin Role voor dit certificaat is gekozen, moet het ISE-knooppunt de services opnieuw opstarten. Op basis van de versie en de bronnen die aan de VM zijn toegewezen, kan dit 10 tot 15 minuten duren. Om de status van de toepassing te controleren, opent u de ISE-opdrachtregel en geeft u de `show application status ise` uit.

next visibility Operations Policy Administration Work Centers

es Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Maintenance

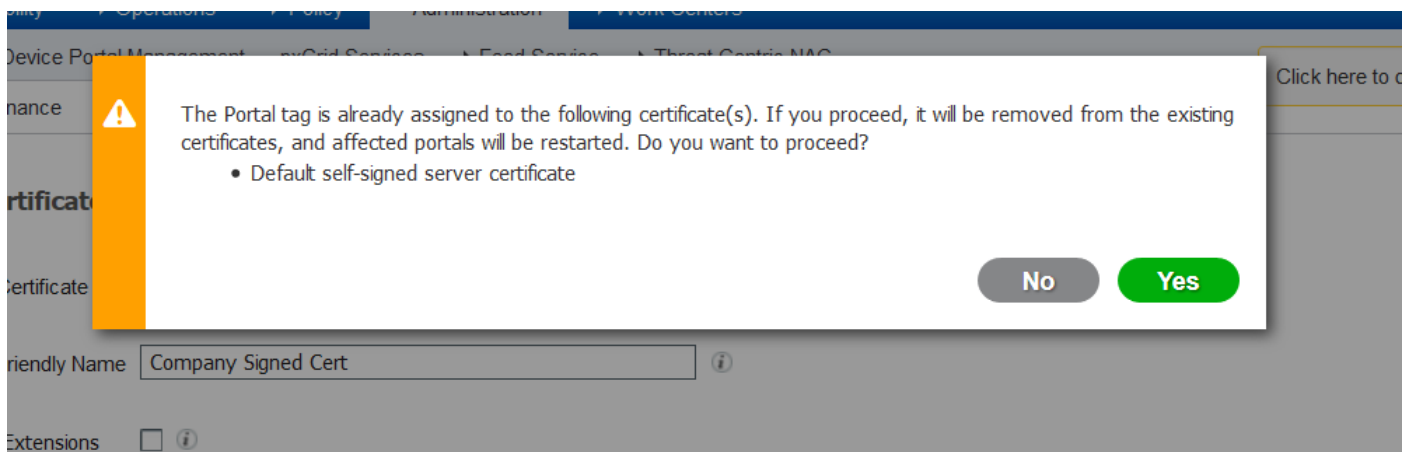
Bind CA Signed Certificate

* Certificate

Friendly Name ⓘ

Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates



Als de admin of portal rol is gekozen bij het importeren van het certificaat, kan worden geverifieerd dat het nieuwe certificaat aanwezig is wanneer de admin of de portal pagina's in de browser worden benaderd. Kies het slotsymbool in de browser en onder het certificaat, verifieert het pad dat de volledige keten aanwezig is en door de machine wordt vertrouwd. De browser moet vertrouwen op het nieuwe admin of portal certificaat zolang de keten correct is gebouwd en als de certificaat ketting wordt vertrouwd door de browser.

Opmerking: om een geldig CA-ondertekend systeemcertificaat te verlengen, genereert u een nieuw CSR en bindt u het ondertekende certificaat aan het certificaat met dezelfde opties. Aangezien het mogelijk is om een nieuw certificaat op de ISE te installeren voordat het actief is, moet u het nieuwe certificaat installeren voordat het oude certificaat verloopt. Deze overlappende periode tussen de oude verloopdatum van het certificaat en de nieuwe begindatum van het certificaat geeft tijd om certificaten te verlengen en hun swap te plannen met weinig of geen downtime. Ontvang een nieuw certificaat met een begindatum die voorafgaat aan de verloopdatum van het oude certificaat. De tijdsperiode tussen deze twee data is het wijzigingsvenster. Zodra het nieuwe certificaat zijn geldige datumbereik heeft, schakelt u de benodigde protocollen in (Admin/EAP/Portal). Vergeet niet dat als het gebruik van Admin is ingeschakeld, er opnieuw service wordt gestart.

Tip: het is raadzaam om de Company Internal CA voor Admin en EAP-certificaten te gebruiken, en een publiekelijk ondertekend certificaat voor Guest/Sponsor/Hotspot/etc portals. De reden hiervoor is dat als een gebruiker of gast op het netwerk komt en de ISE portal een persoonlijk ondertekend certificaat gebruikt voor de Guest Portal, ze certificaatfouten krijgen of mogelijk hun browser blokkeert hen van de portal pagina. Om dit alles te voorkomen, gebruik een openbaar ondertekend certificaat voor het gebruik van Portal om een betere gebruikerservaring te verzekeren. Bovendien moet elk IP-adres voor implementatieknooppunten worden toegevoegd aan het SAN-veld om een certificaatwaarschuwing te voorkomen wanneer de server via het IP-adres wordt benaderd.

Reserve-certificaten en privésleutels

Aanbevolen wordt:

1. Alle systeemcertificaten (van alle knooppunten in de implementatie) samen met hun privésleutels (dit is nodig om ze opnieuw te installeren) naar een beveiligde locatie. Noteer de configuratie van het certificaat (voor welke dienst het certificaat is gebruikt).

2. Alle certificaten van de Trusted Certificates Store van het knooppunt voor primaire toediening. Noteer de configuratie van het certificaat (voor welke dienst het certificaat is gebruikt).

3. Alle certificaten van de certificeringsinstantie.

Hier toe

1. Naar navigeren Administration > System > Certificates > Certificate Management > System Certificates. Kies het certificaat en klik op Export. Kiezen Export Certificates en het keuzerondje Private Keys. Voer het wachtwoord voor de persoonlijke sleutel in en bevestig het wachtwoord. Klik Export.
2. Naar navigeren Administration > System > Certificates > Certificate Management > Trusted Certificates. Kies het certificaat en klik op Export. Klik Save File om het certificaat uit te voeren.
3. Naar navigeren Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. Kies het certificaat en klik op Export. Kiezen Export Certificates en het keuzerondje Private Keys. Voer het wachtwoord voor de persoonlijke sleutel in en bevestig het wachtwoord. Klik Export. Klik Save File om het certificaat uit te voeren.

Problemen oplossen

Controleer de geldigheid van het certificaat

Het upgradeproces mislukt als een certificaat in de winkel Cisco ISE-vertrouwde certificaten of systeemcertificaten is verlopen. Zorg ervoor dat u de geldigheid controleert in het veld Vervaldatum van het venster Betrouwbare certificaten en systeemcertificaten (Administration > System > Certificates > Certificate Management), en deze, indien nodig, vóór de upgrade te verlengen.

Controleer ook de geldigheid in het veld Verloopdatum van de certificaten in het venster CA-certificaten (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates), en deze, indien nodig, vóór de upgrade te verlengen.

Een certificaat verwijderen

Als een certificaat in de ISE is verlopen of niet wordt gebruikt, moet het worden verwijderd. Zorg ervoor dat de certificaten worden geëxporteerd (met hun persoonlijke sleutels, indien van toepassing) voordat ze worden gewist.

Als u een verlopen certificaat wilt verwijderen, navigeer dan naar Administration > System > Certificates > Certificate Management. Klik op de System Certificates Store. Kies de verlopen certificaten en klik op Delete. Raadpleeg hetzelfde voor de opslag van Trusted Certificates en Certificaatinstanties.

Supplicant vertrouwt niet op het ISE-servercertificaat bij een 802.1x-verificatie

Controleer of ISE de volledige certificaatketen voor het SSL-handshake proces verstuurt.

Met EAP-methoden waarvoor een servercertificaat (d.w.z. PEAP) en Validate Server Identity is geselecteerd in de client OS-instellingen, valideert de aanvrager de certificaatketen met de certificaten die hij in zijn lokale vertrouwensopslag heeft als onderdeel van het verificatieproces. Als onderdeel van het SSL-handshake-proces presenteert ISE haar certificaat en ook alle Root-en/of tussencertificaten in haar keten. De aanvrager kan de identiteit van de server niet valideren

als de keten onvolledig is of als deze keten ontbreekt in zijn vertrouwensarchief.

Om te controleren of de certificaatketen aan de client is doorgegeven, neemt u een pakketopname van ISE (Operations > Diagnostic Tools > General Tools > TCP Dump) of Wireshark Capture op het eindpunt op het moment van de verificatie. Open de opname en pas het filter toe `ssl.handshake.certificates` in Wireshark en vind een access challenge.

Nadat u deze hebt gekozen, navigeert u naar `Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates`.

Als de ketting onvolledig is, navigeer dan naar ISE `Administration > Certificates > Trusted Certificates` en controleert of de basiscertificaten en/of de tussenliggende certificaten aanwezig zijn. Indien de certificaatketen met succes is doorlopen, moet de keten zelf volgens de hier beschreven methode als geldig worden gecontroleerd.

Open elk certificaat (server, tussenpersoon en wortel) en controleer de vertrouwensketen om de Onderwerp Key Identifier (SKI) van elk certificaat te matchen met de Autoriteit Key Identifier (AKI) van het volgende certificaat in de keten.

ISE-certificaatketen is correct maar endpoint weigert ISE-servercertificaat tijdens verificatie

Als ISE haar volledige certificaatketting voor de SSL-handdruk presenteert en de aanvrager de certificaatketting nog steeds heeft afgewezen; de volgende stap is te verifiëren dat de Root- en/of Intermediate-certificaten in de lokale vertrouwenswinkel van de klanten zijn.

Om dit vanaf een Windows-apparaat te verifiëren, start u `mmc.exe`(Microsoft Management Console), navigeer naar `File > Add-Remove Snap-in`. Kies in de kolom beschikbare invoegtoepassingen `Certificates` en klik op `Add`. Kies één van beide `My user account` of `Computer account` op basis van het gebruikte verificatietype (Gebruiker of Machine) en klik vervolgens op `OK`.

Kies onder de consoleweergave voor `Trusted Root Certification Authorities` en `Intermediate Certification Authorities` om de aanwezigheid van Root en Intermediate Certificates in het lokale vertrouwensarchief te verifiëren.

Een eenvoudige manier om te verifiëren dat dit een probleem is met de Server Identity Check, vinkt u het Servercertificaat uit onder de profielconfiguratie van de aanvrager en test u het opnieuw.

Veelgestelde vragen

Wat te doen als ISE een waarschuwing geeft dat het certificaat al bestaat?

Dit bericht betekent dat ISE een systeemcertificaat heeft gedetecteerd met exact dezelfde OU-parameter en dat er geprobeerd is een duplicaat van het certificaat te installeren. Aangezien het dubbele systeemcertificaat niet wordt ondersteund, is het raadzaam om de waarden van de Stad/Staat/Afdeling eenvoudig te wijzigen in een iets andere waarde om er zeker van te zijn dat het nieuwe certificaat anders is.

Waarom geeft de browser een waarschuwing dat de portal pagina van ISE wordt

gepresenteerd door een onbetrouwbare server?

Dit gebeurt wanneer de browser het identiteitsbewijs van de server niet vertrouwt.

Zorg er eerst voor dat het portaalcertificaat dat zichtbaar is op de browser, is wat er verwacht werd en dat het op ISE is geconfigureerd voor de portal.

Ten tweede, zorg voor toegang tot het portaal via FQDN - in het geval van het IP adres in gebruik, zorg ervoor dat zowel het FQDN als IP adres in de SAN en/of CN velden van het certificaat zijn.

Zorg er tot slot voor dat de portal certificaatketen (ISE portal, Intermediate CA(s), Root CA-certificaten) wordt geïmporteerd op/vertrouwd door de client-OS/browser-software.

Opmerking: Sommige latere versies van iOS-, Android OS- en Chrome/Firefox-browsers hebben strikte beveiligingsverwachtingen van het certificaat. Zelfs als aan deze punten wordt voldaan, kunnen ze weigeren verbinding te maken als de Portal en Tussentijdse CA's minder zijn dan SHA-256.

Wat te doen wanneer een upgrade mislukt vanwege ongeldige certificaten?

Het upgradeproces mislukt als een certificaat in de winkel Cisco ISE-vertrouwde certificaten of systeemcertificaten is verlopen. Zorg ervoor dat u de geldigheid controleert in het veld Vervaldatum van het venster Betrouwbare certificaten en systeemcertificaten (Administration > System > Certificates > Certificate Management), en deze, indien nodig, vóór de upgrade te verlengen.

Controleer ook de geldigheid in het veld Verloopdatum van de certificaten in het venster CA-certificaten (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates), en deze, indien nodig, vóór de upgrade te verlengen.

Zorg er vóór de ISE-upgrade voor dat de interne CA-certificaatketen geldig is.

Naar navigeren Administration > System > Certificates > Certificate Authority Certificates. Voor elke knoop in de plaatsing, kies het certificaat met SubCA van de Diensten van het Certificaat in de Vriendelijke kolom van de Naam. Klik View Controleer of de certificaatstatus een goed bericht is en zichtbaar is.

Als een certificaatketen is verbroken, zorg er dan voor dat het probleem wordt opgelost voordat het Cisco ISE-upgradeproces begint. Ga naar om het probleem op te lossen Administration > System > Certificates > Certificate Management > Certificate Signing Requests, en genereert een client voor de ISE-basiscoderingsoptie.

Gerelateerde informatie

- [ISE 2.7 Certificaten en certificaatopslag beheren](#)
- [Digitale certificaten implementeren in ISE](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

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.