Webbeheercertificaten installeren op Catalyst 9000-Switches

Inhoud

Inleiding

In dit document wordt beschreven hoe u certificaten kunt genereren, downloaden en installeren op switches uit de Catalyst 9000-reeks.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe te configureren Catalyst 9000-serie switches
- Certificaten ondertekenen met Microsoft Windows Server
- Public Key Infrastructure (PKI) en digitale certificaten

Gebruikte componenten

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

- Cisco Catalyst 9300 Switch, Cisco IOS® XE versie 17.12.4
- Microsoft Windows Server 2022

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

Dit document biedt een stapsgewijze handleiding voor het genereren van een Certificate Signing Request (CSR), het laten ondertekenen door een certificeringsinstantie (CA) en het installeren van het resulterende certificaat (samen met het CA-certificaat) op een Catalyst 9000-switch.

Het doel is om veilig webbeheer (HTTPS) van de switch mogelijk te maken met behulp van een betrouwbaar certificaat, zodat de compatibiliteit met moderne webbrowsers en de naleving van het beveiligingsbeleid van de organisatie worden gewaarborgd.

Configureren

Deze sectie biedt een uitgebreide workflow voor het genereren, ondertekenen en installeren van een webbeheercertificaat op een Catalyst 9000-switch. Elke stap bevat relevante CLI-opdrachten, uitleg en voorbeelduitvoer.

Stap 1: Een sleutel definiëren

Genereer een RSA-sleutelpaar voor algemene doeleinden en gebruik het om het certificaat te beveiligen. De sleutel moet exporteerbaar zijn en kan worden aangepast aan de beveiligingsbehoeften (1024 tot 4096 bits).

<#root>

```
device(config)#
```

crypto key generate rsa general-keys label csr-key exportable

Voorbeeld van uitvoer wanneer om modulusgrootte wordt gevraagd:

<#root>

```
The name for the keys will be:
```

csr-key

```
Choose the size of the key modulus in the range of 512 to 4096 for your  General Purpose Keys. Choosing
How many bits in the modulus [1024]:
```

4096

```
% Generating 4096 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 4 seconds)
```

Stap 2: Genereer een aanvraag voor certificaatondertekening (CSR)

Configureer een vertrouwenspunt op de switch voor het webbeheercertificaat, specificeer de inschrijving via terminal, schakel de herroepingscontrole uit en geef identificatiegegevens op (naam van het onderwerp, sleutel en alternatieve namen van het onderwerp).

<#root>

```
device(config)#
crypto pki trustpoint webadmin-TP
device(ca-trustpoint)#
enrollment terminal pem
device(ca-trustpoint)#
revocation-check none
device(ca-trustpoint)#
subject-name C=SJ, ST=CA, L=CA, O=TAC, OU=LANSW, CN=myc9300.local-domain
device(ca-trustpoint)#
rsakeypair csr-key
device(ca-trustpoint)#
subject-alt-name mywebadmin.com
device(ca-trustpoint)#exit
```

Meld je aan bij het trustpoint om de CSR te genereren. U moet worden gevraagd om verschillende opties; het verstrekken van "ja" of "nee" als dat nodig is. De certificaataanvraag moet op de terminal worden weergegeven.

```
device(config)#crypto pki enroll webadmin-TP
```

Voorbeeld van uitvoer:

<#root>

```
% Start certificate enrollment ..
% The subject name in the certificate will include:
C=SJ, ST=CA, L=CA, O=TAC, OU=LANSW, CN=myc9300.local-domain
```

```
% The subject name in the certificate will include: C9300.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:
```

no

Beschikbare parameters voor de configuratie van de onderwerpnaam:

- C: Land, alleen twee hoofdletters (VS)
- ST: Provincie- of provincienaam
- L: Locatienaam (stad)
- O: Naam organisatie (bedrijf)
- OU: naam van de organisatorische eenheid (afdeling/sectie)
- GN: Algemene naam (FQDN- of IP-adres dat moet worden geopend)

Stap 3: Dien de MVO in bij de certificeringsinstantie (CA)

Kopieer de volledige CSR-tekenreeks (inclusief de begin- en eindlijnen) en dien deze in bij uw CA voor ondertekening.

```
-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----
```

Als u een Microsoft Windows Server-CA gebruikt, downloadt u het ondertekende certificaat in Base64-indeling. U ontvangt meestal het ondertekende apparaatcertificaat en mogelijk een Root CA-certificaat.

Stap 4: CA Base64-certificaat voor hoofdmap verifiëren

Installeer het CA-certificaat (in Base64-indeling) op de switch om het vertrouwen te vestigen in de CA die uw apparaatcertificaat heeft uitgegeven.

<#root>

```
device(config)#
```

crypto pki authenticate webadmin-TP

Plak het CA-certificaat (inclusief de begin- en eindregels) wanneer daarom wordt gevraagd. Voorbeeld:

<#root>

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
Certificate has attributes:
      Fingerprint MD5: C7224F3A A9B0426A FDCC50E6 8A04583E
      Fingerprint SHA1: 9B31C319 A515AC41 0114EA43 33716E8B 472A4EF5
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
%
```

Certificate successfully imported

Stap 5: certificaat Device Base64 verifiëren

Het ondertekende certificaat van het apparaat verifiëren aan de hand van het geïnstalleerde CA-certificaat.

<#root>

```
device(config)#
```

crypto pki trustpoint webadmin-TP

```
device(ca-trustpoint)#
```

chain-validation stop

```
device(ca-trustpoint)#
```

crypto pki authenticate webadmin-TP

Plak desgevraagd in het apparaatcertificaat:

<#root>

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
Certificate has the following attributes:
Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

Stap 6: Import Device Signed Certificate op de Catalyst 9000-Switch

Importeer het ondertekende Base64-apparaatcertificaat in het trustpoint.

<#root>

```
device(config)#
crypto pki import webadmin-TP certificate
```

Plak het certificaat wanneer daarom wordt gevraagd:

<#root>

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
< 9300 device certificate >
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

Op dit moment wordt het apparaatcertificaat samen met alle bijbehorende CA's in de switch geïmporteerd en is het certificaat klaar voor gebruik, inclusief GUI-toegang (HTTPS).

Stap 7: Gebruik het nieuwe certificaat

Koppel het trustpoint aan de HTTP-beveiligde server en schakel HTTPS-toegang in op de switch.

<#root>

```
device(config)#
ip http secure-trustpoint webadmin-TP
```

<#root>

```
device(config)#
no ip http secure-server
```

<#root>

```
device(config)#
```

ip http secure-server

Stap 8: Hoe ervoor te zorgen dat het certificaat wordt vertrouwd door webbrowsers

- De Common Name (CN) van het certificaat of een Subject Alternative Name (SAN) moet overeenkomen met de URL waartoe de browser toegang heeft.
- Het certificaat moet binnen de geldigheidsperiode zijn.
- Het certificaat moet worden uitgegeven door een CA (of keten van CA's) waarvan de root door de browser wordt vertrouwd. De switch moet de volledige certificaatketen leveren (behalve de root-CA, die meestal al aanwezig is in de winkel van de browser).
- Als het certificaat intrekkingslijsten bevat, moet u ervoor zorgen dat de browser deze kan downloaden en dat de CN van het certificaat niet in een intrekkingslijst wordt vermeld.

Verifiëren

U kunt deze opdrachten gebruiken om de certificaatconfiguratie en de huidige status te controleren:

Bekijk de geïnstalleerde certificaten en hun status voor een trustpoint:

<#root>

```
device#
```

show crypto pki certificate webadmin-TP

Voorbeeld van uitvoer:

<#root>

```
Certificate  Status:
```

Available

```
Certificate Serial Number (hex): 4700000129584BB4BAFA13EABB000000000129
Certificate Usage: General Purpose
Issuer:
```

cn=mitch-DC02-CA   dc=mitch   dc=local

```
Subject:    Name:
```

C9300.cisco.com

```
            Serial Number: XXXXXXXXXX
            cn=
```

myc9300.local-domain

```
            ou=LANSW
            o=TAC
            l=CA
            st=CA
            c=SJ
```

hostname=C9300.cisco.com

```
Validity Date:
    start date: 05:09:42 UTC Jun 12 2025
    end   date: 07:25:06 UTC Dec 16 2026
Associated Trustpoints:
```

webadmin-TP

```
CA Certificate  Status: Available
Certificate Serial Number (hex): 101552448B9C2EBB488C40034C129F4A
Certificate Usage: Signature
Issuer:     cn=mitch-DC02-CA    dc=mitch    dc=local
Subject:     cn=mitch-DC02-CA    dc=mitch    dc=local
```

Validity Date:

```
    start date: 07:15:06 UTC Dec 16 2021
```

end   date: 07:25:06 UTC Dec 16 2026

```
Associated Trustpoints: webadmin-TP RootCA
```

Controleer de status van de HTTPS-server en het bijbehorende trustpoint:

<#root>

```
device#
```

show ip http server secure status

Voorbeeld van uitvoer:

<#root>

HTTP secure server status: Enabled

```
HTTP secure server port: 443
HTTP secure server ciphersuite:  rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
                                 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2
                                 ecdhe-rsa-aes-cbc-sha2
```

```
                                ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2
HTTP secure server TLS version:  TLSv1.2 TLSv1.1
HTTP secure server client authentication: Disabled
HTTP secure server PIV authentication: Disabled
HTTP secure server PIV authorization only: Disabled

HTTP secure server trustpoint: webadmin-TP

HTTP secure server peer validation trustpoint:
HTTP secure server ECDHE curve: secp256r1
HTTP secure server active session modules: ALL
```

Problemen oplossen

Als u problemen ondervindt tijdens het installatieproces van het certificaat, gebruikt u deze opdrachten om foutopsporing van PKI-transacties in te schakelen. Dit is vooral handig voor het diagnosticeren van fouten tijdens het importeren of registreren van certificaten.

<#root>

```
device#

debug crypto pki transactions
```

Voorbeeld van een succesvolle debug-uitvoer voor scenario's:

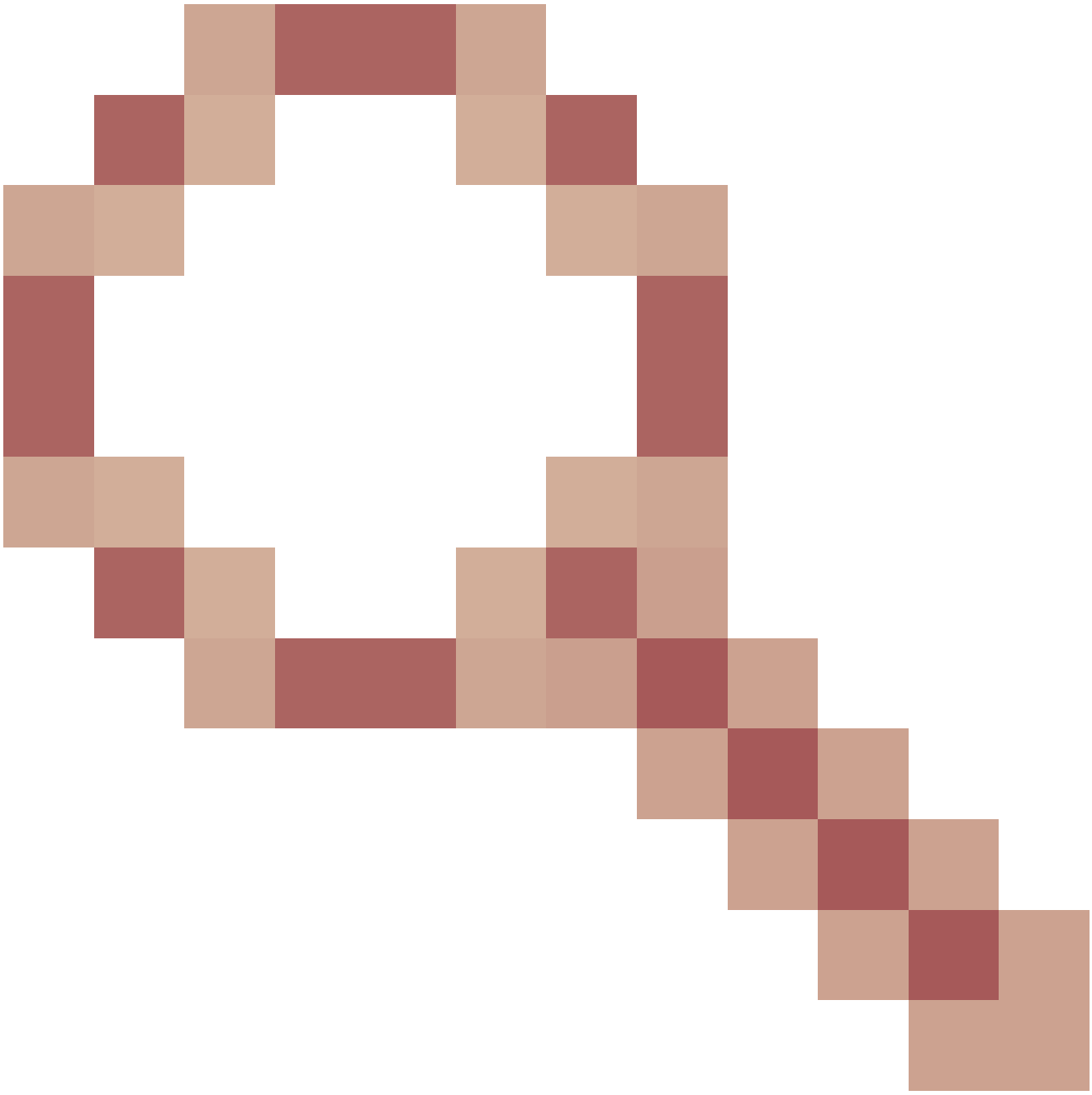
<#root>

```
*Jun 12 05:16:03.531: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named C9300.cisco.com has been generated or
*Jun 12 05:16:03.534:

 %CRYPTO-6-AUTOGEN: Generated new 2048 bit key pair

*Jun 12 05:16:03.556: CRYPTO_PKI: unlocked trustpoint RootCA, refcount is 0
*Jun 12 05:16:03.556: CRYPTO_PKI: using private key C9300.cisco.com for enrollment
*Jun 12 05:16:04.489: CRYPTO_PKI: Adding myc9300.local-domain to subject-alt-name field
*Jun 12 05:16:17.463: CRYPTO_PKI: using private key csr-key for enrollment
*Jun 12 05:18:32.378: CRYPTO_PKI: locked trustpoint webadmin-TP, refcount is 1
*Jun 12 05:19:15.464: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:19:15.470: CRYPTO_PKI: trustpoint webadmin-TP authentication status = 0
*Jun 12 05:19:15.472: CRYPTO_PKI: (A018E) Session started - identity not specified
*Jun 12 05:19:15.473: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
*Jun 12 05:19:15.473: CRYPTO_PKI: Found a subject match
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Check for identical certs
*Jun 12 05:19:15.473: CRYPTO_PKI: Found a issuer match
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Suitable trustpoints are: RootCA,
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Attempting to validate certificate using RootCA policy
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E)

Using RootCA to validate certificate

*Jun 12 05:19:15.474: CRYPTO_PKI(make trusted certs chain)
*Jun 12 05:19:15.474: CRYPTO_PKI:

Added 1 certs to trusted chain.
```

```
*Jun 12 05:20:05.555: CRYPTO_PKI: locked trustpoint webadmin-TP, refcount is 1
*Jun 12 05:20:25.734: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:20:25.735: CRYPTO_PKI(Cert Lookup)

issuer="cn=mitch-DC02-CA,dc=mitch,dc=local"

 serial number= 10 15 52 44 8B 9C 2E BB 48 8C 40 03 4C 12 9F 4A
*Jun 12 05:20:25.735: CRYPTO_PKI: crypto_pki_get_cert_record_by_cert()
*Jun 12 05:20:25.735: CRYPTO_PKI:

Found a cert match

*Jun 12 05:20:25.735: CRYPTO_PKI: crypto_pki_authenticate_tp_cert()
*Jun 12 05:20:25.735: CRYPTO_PKI: trustpoint webadmin-TP authentication status = 0
*Jun 12 05:20:32.094: PKI: Cert key-usage: Digital-Signature , Certificate-Signing , CRL-Signing
*Jun 12 05:20:32.096: CRYPTO_PKI:

Notify subsystem about new certificate.

*Jun 12 05:20:32.097: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:21:50.789: CRYPTO_PKI:

using private key csr-key for enrollment

*Jun 12 05:22:12.947: CRYPTO_PKI:

make trustedCerts list for webadmin-TP
```

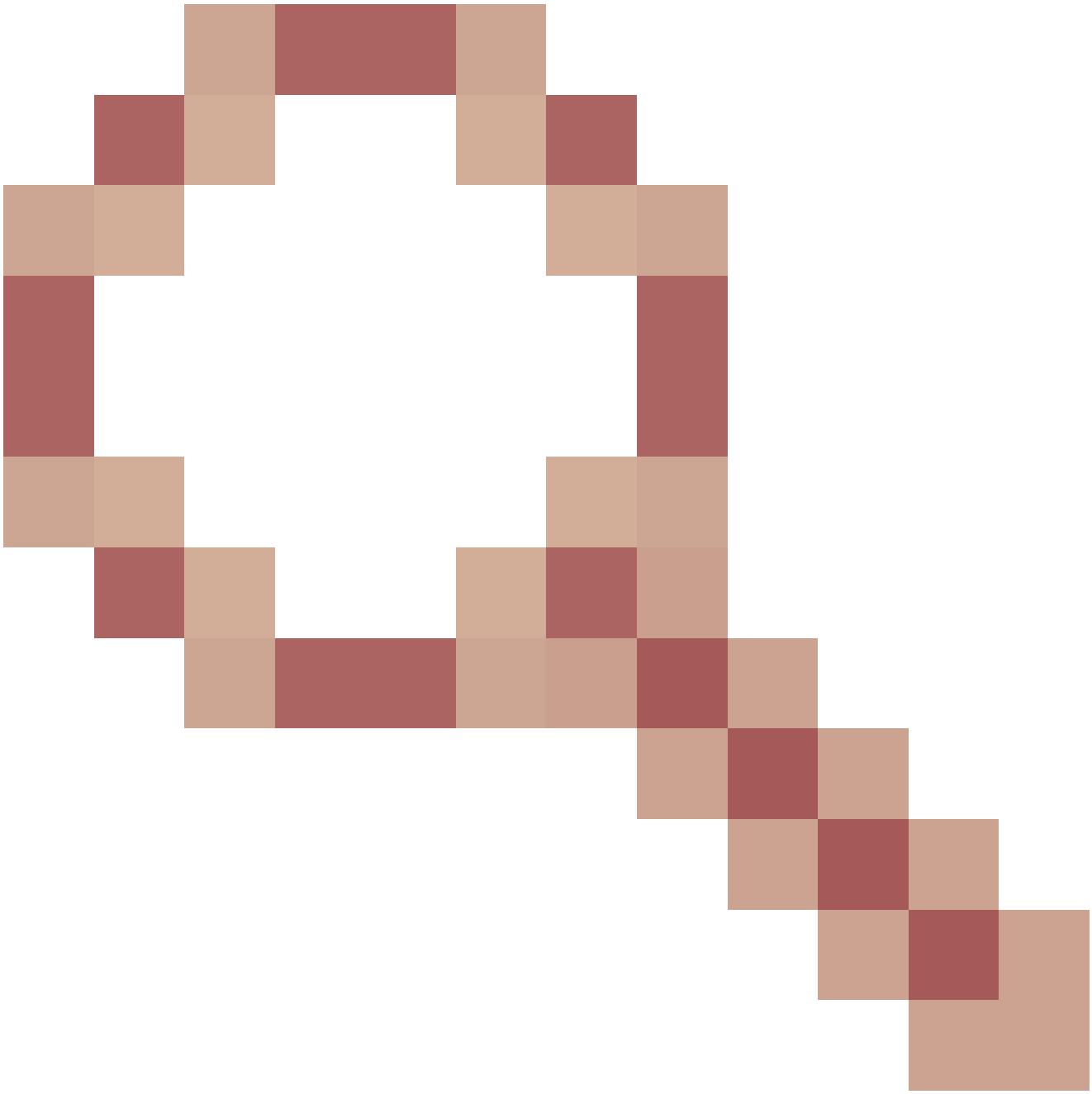
Opmerkingen en beperkingen

- Cisco IOS® XE biedt geen ondersteuning voor CA-certificaten die na 2099 geldig zijn (Cisco bug ID CSCvp64208



).

- Cisco IOS® XE biedt geen ondersteuning voor SHA256 message digest PKCS 12-bundels (SHA256-certs worden ondersteund, maar niet als de PKCS12-bundel zelf is ondertekend met SHA256) (Cisco bug ID CSCvz41428



). Dit probleem is opgelost in 17.12.1.

Gerelateerde informatie

- Cisco Technical Support en downloads

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.