Installation von Web Admin-Zertifikaten auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

Dieses Dokument beschreibt den Prozess zum Generieren, Herunterladen und Installieren von Zertifikaten auf Catalyst Switches der Serie 9000.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfigurieren von Catalyst Switches der Serie 9000
- Signieren von Zertifikaten mit Microsoft Windows Server
- Public Key Infrastructure (PKI) und digitale Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

- Cisco Catalyst Switch der Serie 9300, Cisco IOS® XE Version 17.12.4
- Microsoft Windows Server 2022

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dieses Dokument enthält eine schrittweise Anleitung zum Generieren einer CSR-Anforderung (Certificate Signing Request), zum Abrufen der Signatur durch eine Zertifizierungsstelle (Certification Authority, CA) und zum Installieren des resultierenden Zertifikats (zusammen mit dem CA-Zertifikat) auf einem Catalyst 9000-Switch.

Das Ziel besteht darin, die sichere Web-Administration (HTTPS) des Switches über ein vertrauenswürdiges Zertifikat zu ermöglichen und so die Kompatibilität mit modernen Webbrowsern und die Einhaltung von Sicherheitsrichtlinien im Unternehmen sicherzustellen.

Konfigurieren

Dieser Abschnitt enthält detaillierte Workflows zum Generieren, Signieren und Installieren eines Web-Admin-Zertifikats auf einem Catalyst 9000-Switch. Jeder Schritt umfasst relevante CLI-Befehle, Erläuterungen und Beispielausgaben.

Schritt 1: Definieren eines Schlüssels

Generieren Sie ein RSA-Schlüsselpaar für allgemeine Zwecke, und verwenden Sie es zum Sichern des Zertifikats. Der Schlüssel muss exportierbar sein und kann entsprechend den Sicherheitsanforderungen (1024 bis 4096 Bit) dimensioniert werden.

<#root>

```
device(config)#
```

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

Beispielausgabe bei Aufforderung zur Angabe der Modulgröße:

<#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)
```

Phase 2: Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR)

Konfigurieren Sie auf dem Switch einen Vertrauenspunkt für das Web-Admin-Zertifikat, und geben Sie die Registrierung über das Terminal an, deaktivieren Sie die Sperrprüfung, und geben Sie Identifizierungsinformationen an (Antragstellername, Schlüssel und alternative Antragstellernamen).

<#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
```

Registrieren Sie den Trustpoint, um die CSR-Anfrage zu erstellen. Sie müssen nach verschiedenen Optionen gefragt werden. bei Bedarf mit "Ja" oder "Nein". Die Zertifikatsanforderung muss auf dem Terminal angezeigt werden.

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

Beispiel:

<#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

Verfügbare Parameter für die Konfiguration des Betreffnamens:

- C: Land, nur zwei Großbuchstaben (USA)
- ST: Bundesland Name
- L: Standortname (Ort)
- E: Name der Organisation (Firma)
- OU: Name der Organisationseinheit (Abteilung/Bereich)
- KN: Common Name (FQDN oder IP-Adresse, auf die zugegriffen werden soll)

Schritt 3: Übermitteln Sie den CSR an die Zertifizierungsstelle.

Kopieren Sie die vollständige CSR-Zeichenfolge (einschließlich der Zeilen BEGIN und END), und senden Sie sie zur Signatur an Ihre Zertifizierungsstelle.

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

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

Wenn Sie eine Microsoft Windows Server-CA verwenden, laden Sie das signierte Zertifikat im Base64-Format herunter. In der Regel erhalten Sie das signierte Gerätezertifikat und möglicherweise ein Root-Zertifizierungsstellenzertifikat.

Schritt 4: Authentifizierung des Base64-Zertifikats der Stammzertifizierungsstelle

Installieren Sie das Zertifikat der Zertifizierungsstelle (im Base64-Format) auf dem Switch, um die Vertrauenswürdigkeit der Zertifizierungsstelle herzustellen, die das Gerätezertifikat ausgestellt hat.

<#root>

```
device(config)#
```

crypto pki authenticate webadmin-TP

Fügen Sie das Zertifizierungsstellenzertifikat (einschließlich der BEGIN- und END-Zeile) ein, wenn Sie dazu aufgefordert werden. Beispiel:

<#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

Schritt 5: Authentifizierung des Base64-Zertifikats des Geräts

Authentifiziert das signierte Zertifikat des Geräts anhand des installierten Zertifizierungsstellenzertifikats.

<#root>

```
device(config)#
```

crypto pki trustpoint webadmin-TP

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

chain-validation stop

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

crypto pki authenticate webadmin-TP

Wenn Sie dazu aufgefordert werden, fügen Sie das Gerätezertifikat ein:

<#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
```

Schritt 6: Import des vom Gerät signierten Zertifikats auf den Catalyst Switch der Serie 9000

Importieren Sie das mit Base64 signierte Gerätezertifikat in den Vertrauenspunkt.

<#root>

```
device(config)#

crypto pki import webadmin-TP certificate
```

Fügen Sie das Zertifikat ein, wenn Sie aufgefordert werden:

<#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
```

Zu diesem Zeitpunkt wird das Gerätezertifikat zusammen mit allen relevanten Zertifizierungsstellen auf den Switch importiert, und das Zertifikat ist einsatzbereit, einschließlich des GUI-Zugriffs (HTTPS).

Schritt 7: Neues Zertifikat verwenden

Verknüpfen Sie den Trustpoint mit dem sicheren HTTP-Server, und aktivieren Sie den HTTPS-Zugriff auf dem 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

Schritt 8: Sicherstellen, dass das Zertifikat von Webbrowsern als vertrauenswürdig eingestuft wird

- Der Common Name (CN) oder ein Subject Alternative Name (SAN) des Zertifikats muss mit der URL übereinstimmen, auf die der Browser zugreift.
- Das Zertifikat muss innerhalb seiner Gültigkeitsdauer sein.
- Das Zertifikat muss von einer Zertifizierungsstelle (oder einer Kette von Zertifizierungsstellen) ausgestellt werden, deren Root vom Browser als vertrauenswürdig eingestuft wird. Der Switch muss die gesamte Zertifikatskette bereitstellen (mit Ausnahme der Stammzertifizierungsstelle, die in der Regel bereits im Browser-Speicher vorhanden ist).
- Wenn das Zertifikat Sperrlisten enthält, stellen Sie sicher, dass der Browser diese herunterladen kann und dass die CN des Zertifikats in keiner Sperrliste aufgeführt ist.

Überprüfung

Mit diesen Befehlen können Sie die Zertifikatskonfiguration und den aktuellen Status überprüfen:

Anzeigen der installierten Zertifikate und ihres Status für einen Vertrauenspunkt:

<#root>

```
device#
```

show crypto pki certificate webadmin-TP

Beispiel:

<#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
```

Überprüfen Sie den HTTPS-Serverstatus und den zugehörigen Vertrauenspunkt:

<#root>

```
device#
```

show ip http server secure status

Beispiel:

<#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
```

Fehlerbehebung

Wenn während der Zertifikatinstallation Probleme auftreten, verwenden Sie diese Befehle, um das Debuggen von PKI-Transaktionen zu aktivieren. Dies ist besonders nützlich, um Fehler beim Importieren oder Registrieren von Zertifikaten zu diagnostizieren.

<#root>

```
device#

debug crypto pki transactions
```

Beispiel für eine erfolgreiche Fehlerbehebungsausgabe:

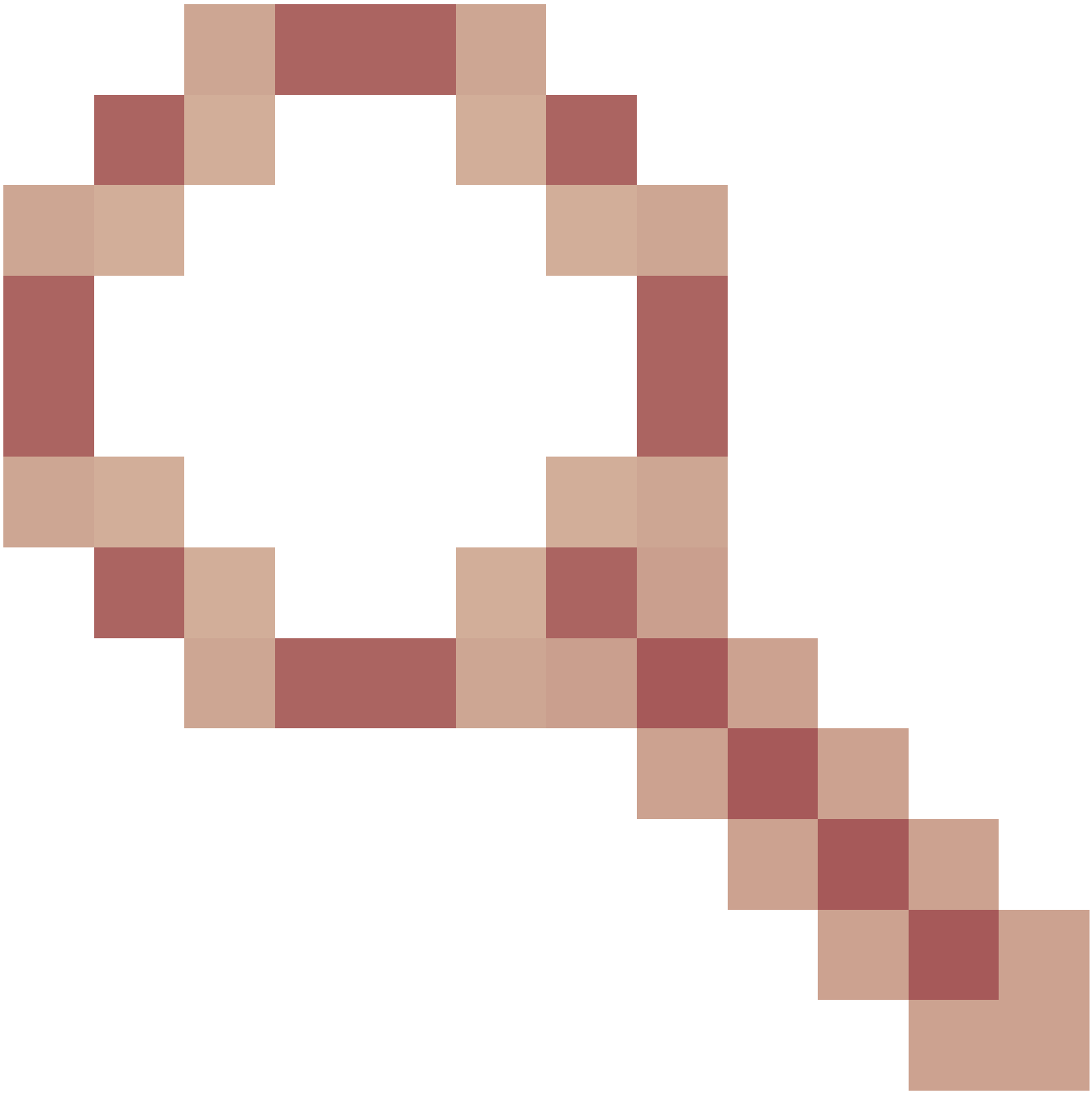
<#root>

```
*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
```

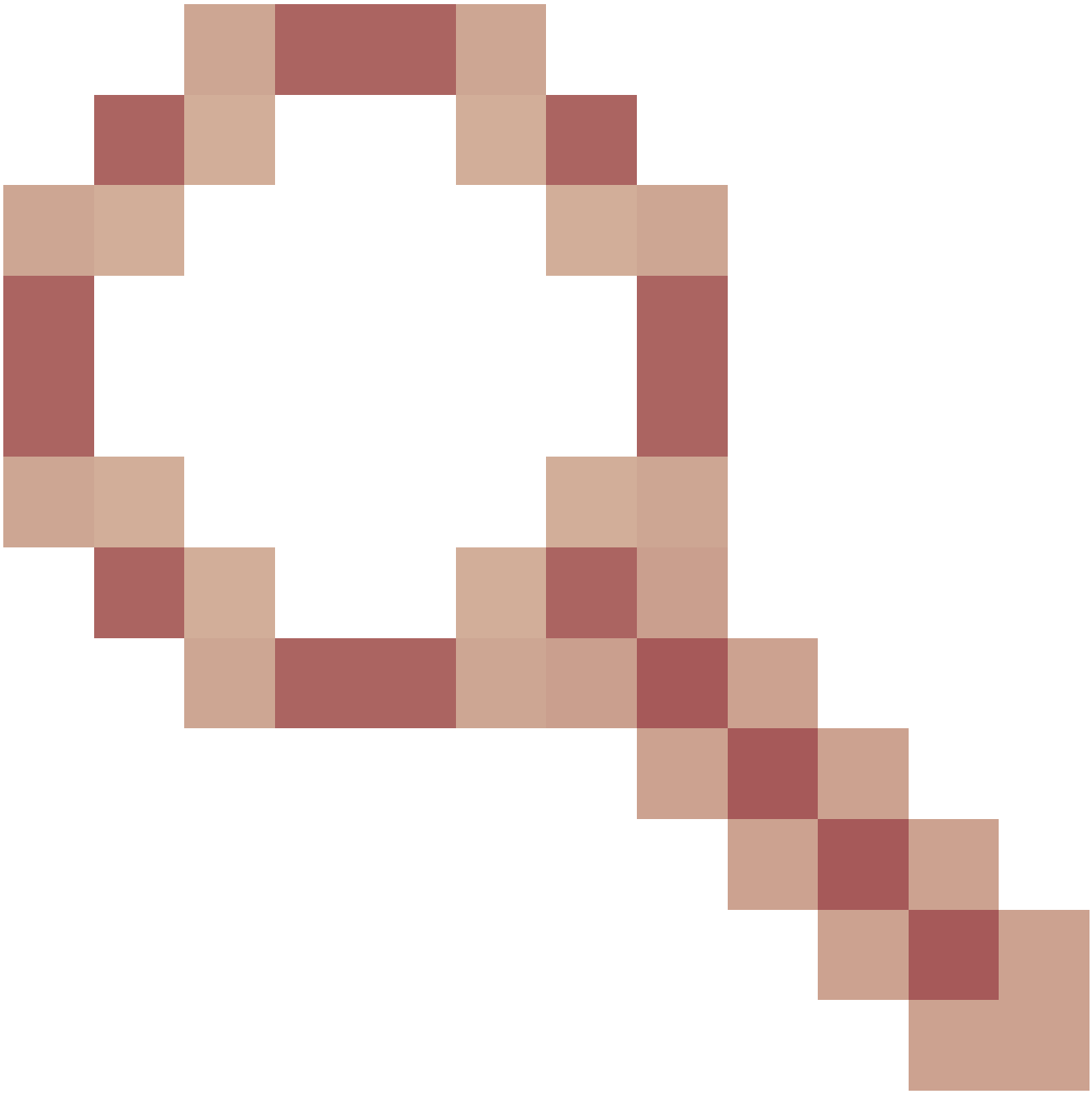
Hinweise und Einschränkungen

- Cisco IOS® XE unterstützt keine CA-Zertifikate mit einer Gültigkeit über 2099 hinaus (Cisco Bug-ID CSCvp64208)



).

- Cisco IOS® XE unterstützt keine SHA256 Message Digest PKCS 12-Pakete (SHA256-Zertifikate werden unterstützt, jedoch nicht, wenn das PKCS12-Paket selbst mit SHA256 signiert ist) (Cisco Bug-ID CSCvz41428)



). Dieses Problem wurde in Version 17.12.1 behoben.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.