Zertifikate generieren und hinzufügen, die für die Installation von Secure Endpoint Private Cloud 3.x erforderlich sind

Inhalt

Einleitung

In diesem Dokument wird das Generieren von Zertifikaten beschrieben, die bei jeder Neuinstallation von Secure Console Private Cloud hochgeladen werden müssen, oder das Erneuern der installierten Zertifikatsdienste.

Voraussetzungen

Anforderungen

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

- Windows Server 2008
- CentOS 7/8
- Secure Console Virtual Private Cloud 3.0.2 (ab)
- OpenSSL 1.1.1

Verwendete Komponenten

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

- Windows Server 2008 (ab)
- Secure Console Private Cloud-Installation
- Public-Key-Infrastruktur
- OpenSSL
- Linux-Kommandozeile

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

Mit der Einführung von Secure Console Private Cloud 3.X sind Hostnamen und Zertifikat-Schlüssel-Paare für alle folgenden Dienste erforderlich:

- Administrationsportal
- Authentifizierung (neu in Private Cloud 3.x)
- Sichere Konsole
- Dispositionsserver
- Disposition Server - Extended Protocol
- Dispositionsaktualisierungsdienst
- FirePOWER Management Center

In diesem Dokument wird eine schnelle Methode zum Generieren und Hochladen der erforderlichen Zertifikate beschrieben. Sie können die einzelnen Parameter, einschließlich des Hashing-Algorithmus, der Schlüssellänge und andere, gemäß der Richtlinie Ihrer Organisation anpassen. Der Mechanismus zum Generieren dieser Zertifikate entspricht möglicherweise nicht den hier beschriebenen Details.

> **Warnung**: Das unten beschriebene Verfahren kann je nach Konfiguration Ihres CA-Servers variieren. Es wird davon ausgegangen, dass der CA-Server Ihrer Wahl bereits bereitgestellt ist und die Konfiguration desselben abgeschlossen ist. Im folgenden technischen Hinweis wird nur ein Beispiel für die Erstellung der Zertifikate beschrieben. Das Cisco TAC ist nicht an der Fehlerbehebung von Problemen mit der Zertifikatgenerierung und/oder dem CA-Server beteiligt.

Erstellung des Zertifikats

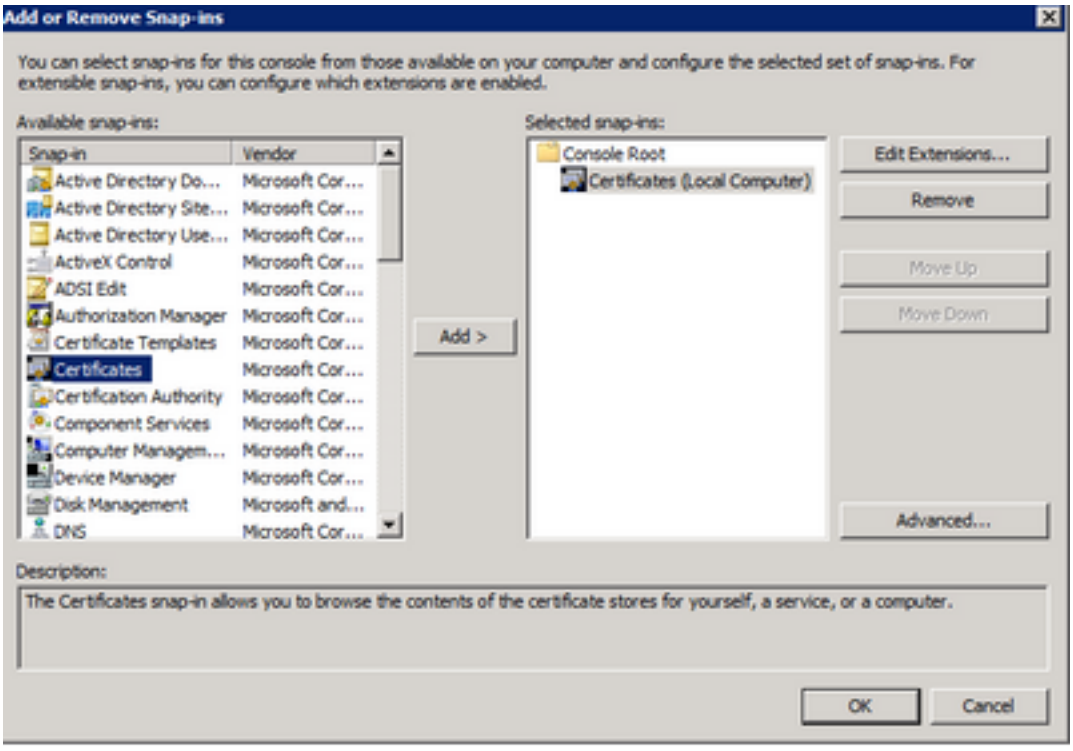
Zertifikate auf dem Windows-Server generieren

Stellen Sie sicher, dass die folgenden Rollen auf Ihrem Windows Server installiert und konfiguriert sind.

- Active Directory-Zertifikatdienste
- Zertifizierungsstelle
- Zertifizierungsstelle Web Enrollment
- Online-Responder
- Zertifikatregistrierungs-Webdienst
- Webdienst für die Zertifikatregistrierungsrichtlinie
- Active Directory Domain Services
- DNS-Server
- Webserver (IIS)

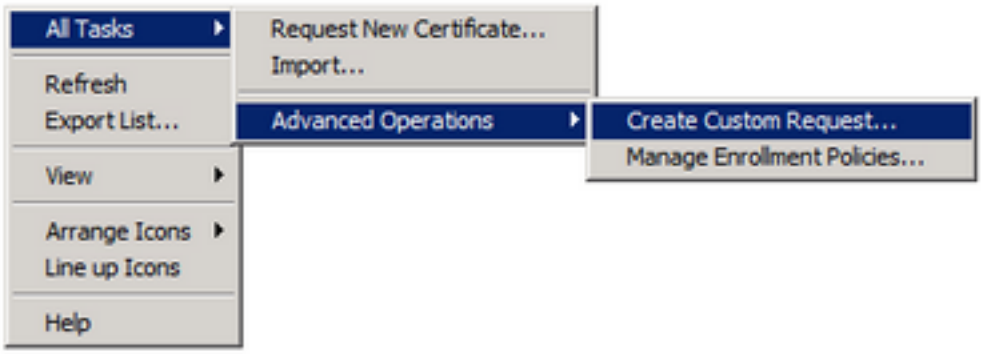
Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR)

Schritt 1: Navigieren Sie zur MMC-Konsole, und fügen Sie das Zertifikat-Snap-In für Ihr Computerkonto hinzu, wie in der Abbildung hier gezeigt.

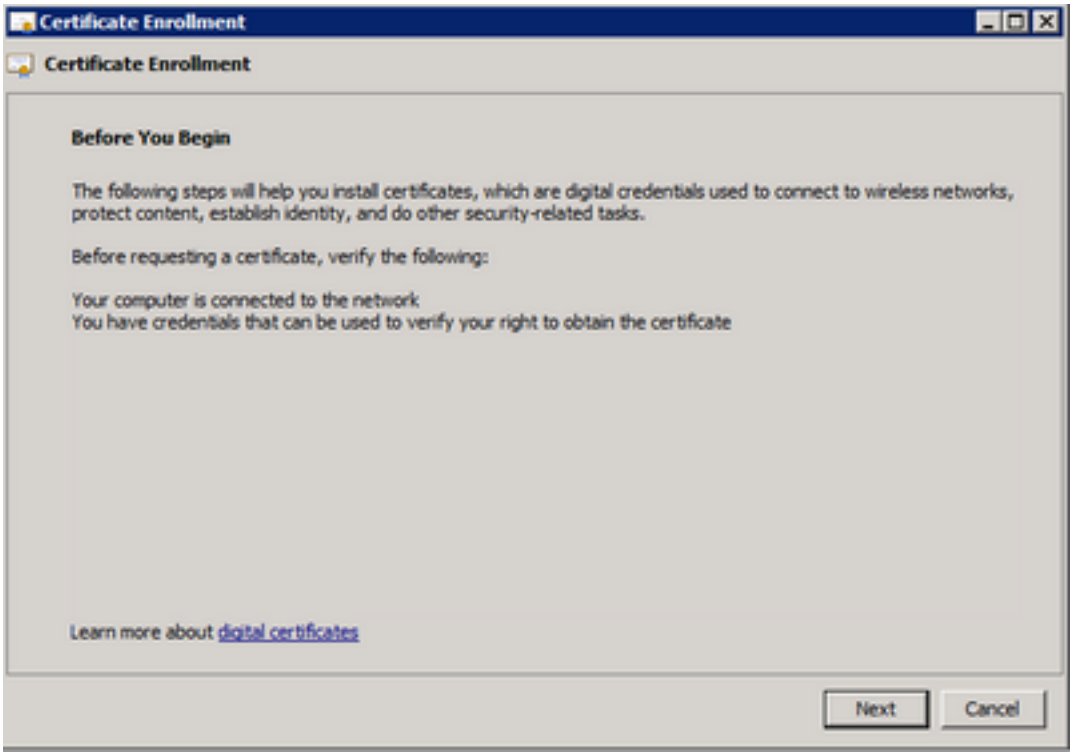


Schritt 2: Drill-Down **für Zertifikate (Lokaler Computer) > Persönlich > Zertifikate**.

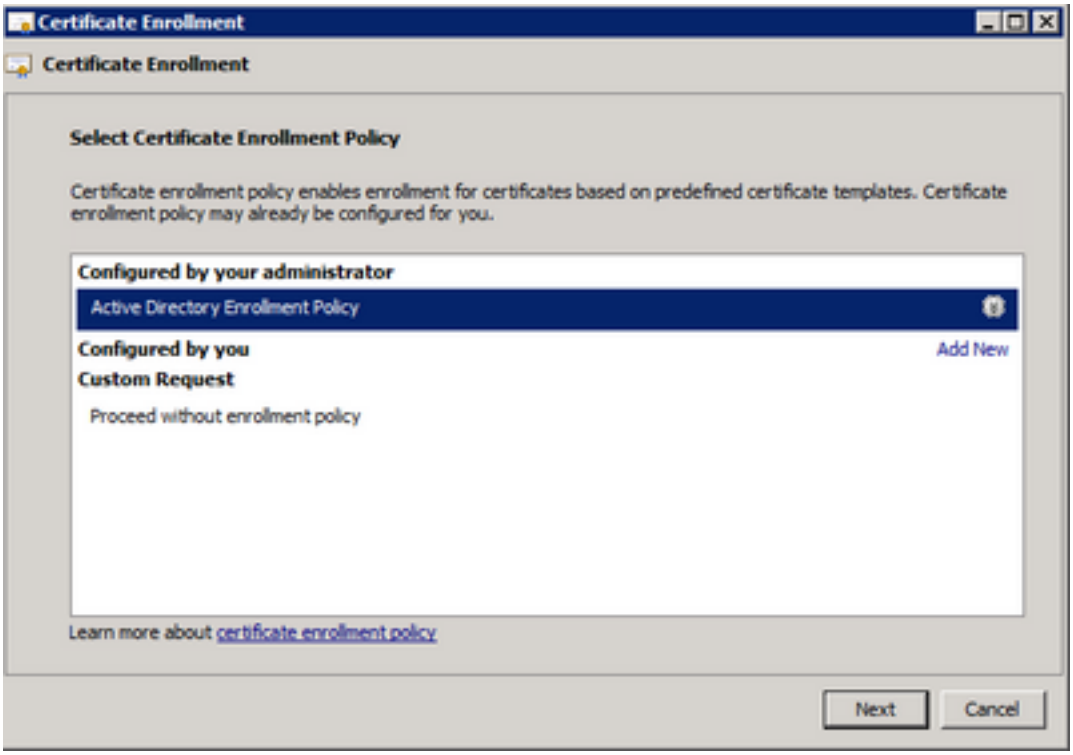
Schritt 3: Klicken Sie mit der rechten Maustaste auf den leeren Bereich, und wählen Sie **Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen aus.**



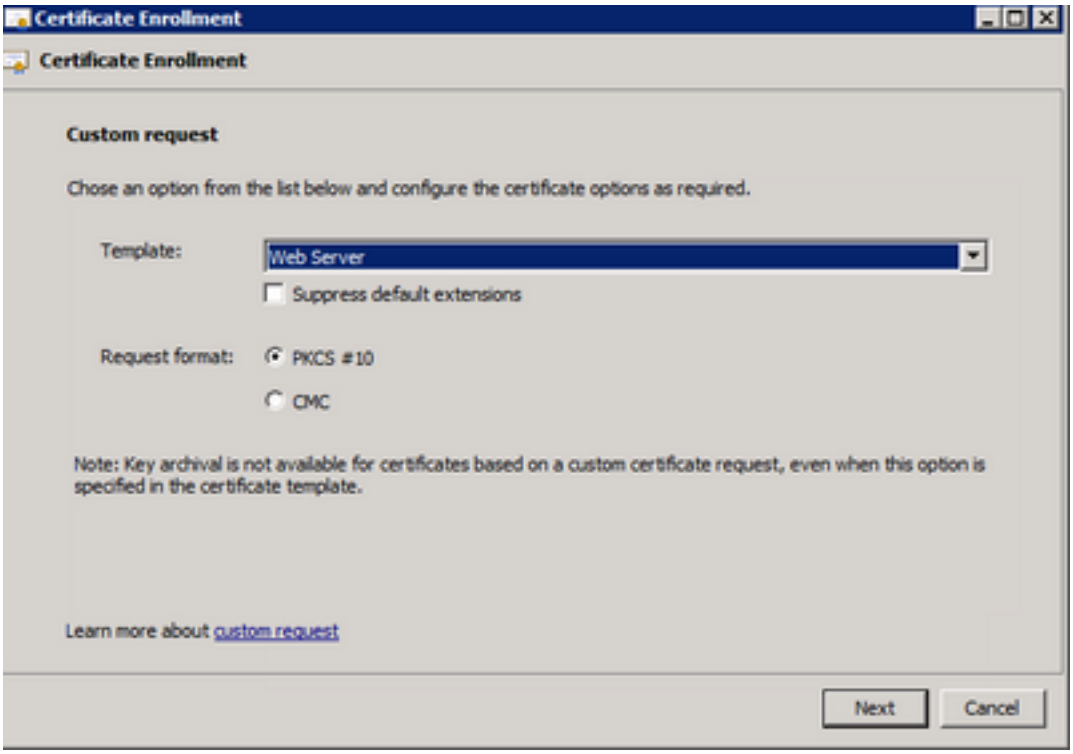
Schritt 4: Wählen Sie im Anmeldungsfenster die Option **Weiter** aus.



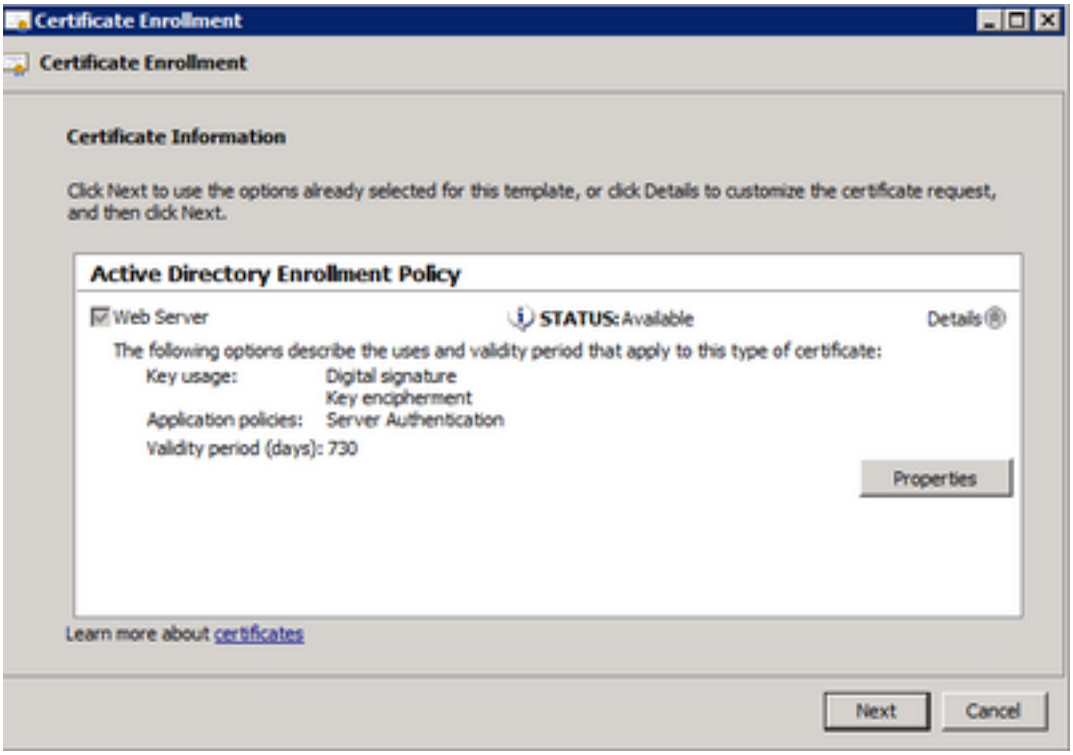
Schritt 5: Wählen Sie Ihre Zertifikatregistrierungsrichtlinie aus, und wählen Sie **Weiter aus**.



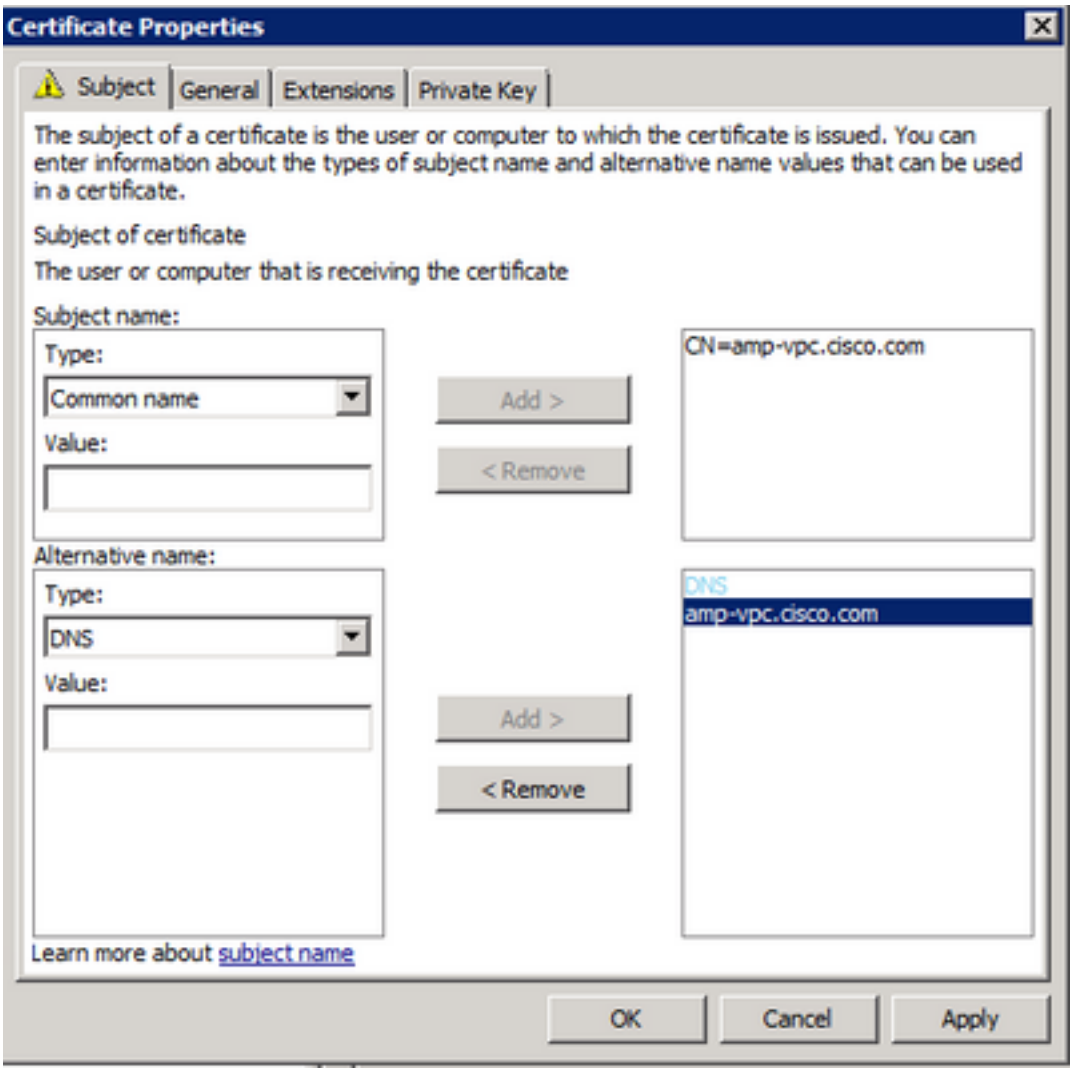
Schritt 6: Wählen Sie die Vorlage als **Webserver aus**, und wählen Sie **Weiter aus**.



Schritt 7. Wenn Ihre Webserver-Vorlage richtig konfiguriert wurde und für die Registrierung verfügbar ist, wird der Status Verfügbar angezeigt. Wählen Sie **Details** aus, um Eigenschaften zu erweitern.

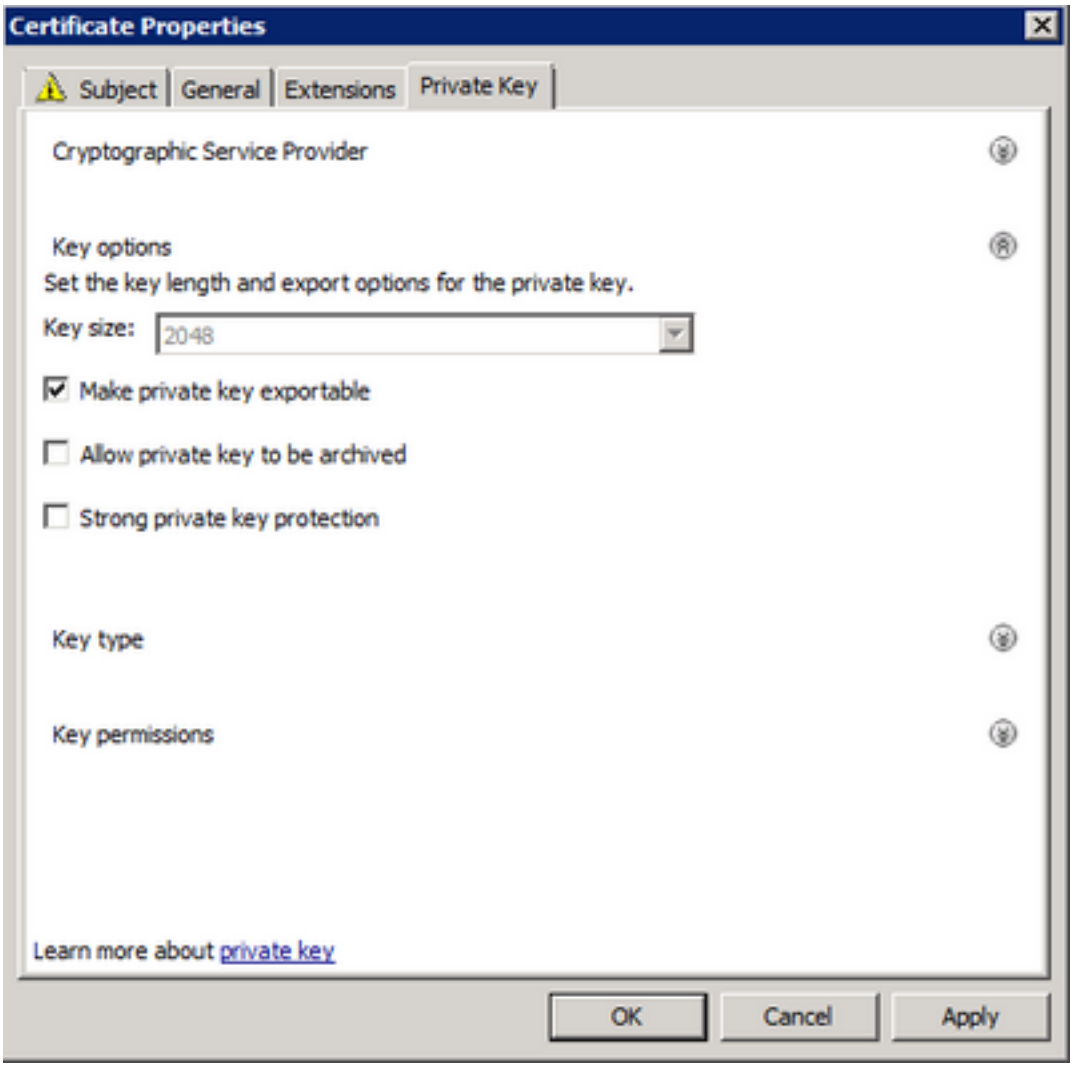


Schritt 8: Fügen Sie mindestens die CN- und DNS-Attribute hinzu. Die restlichen Attribute können entsprechend Ihren Sicherheitsanforderungen hinzugefügt werden.



Schritt 9. Geben Sie auf der Registerkarte **Allgemein** einen Anzeigenamen ein.

Schritt 10. Wählen Sie diese Option auf der Registerkarte **Privater Schlüssel aus**, und stellen Sie sicher, dass Sie im Abschnitt **Schlüsseloptionen** die Option **Privaten Schlüssel exportieren lassen** aktivieren.

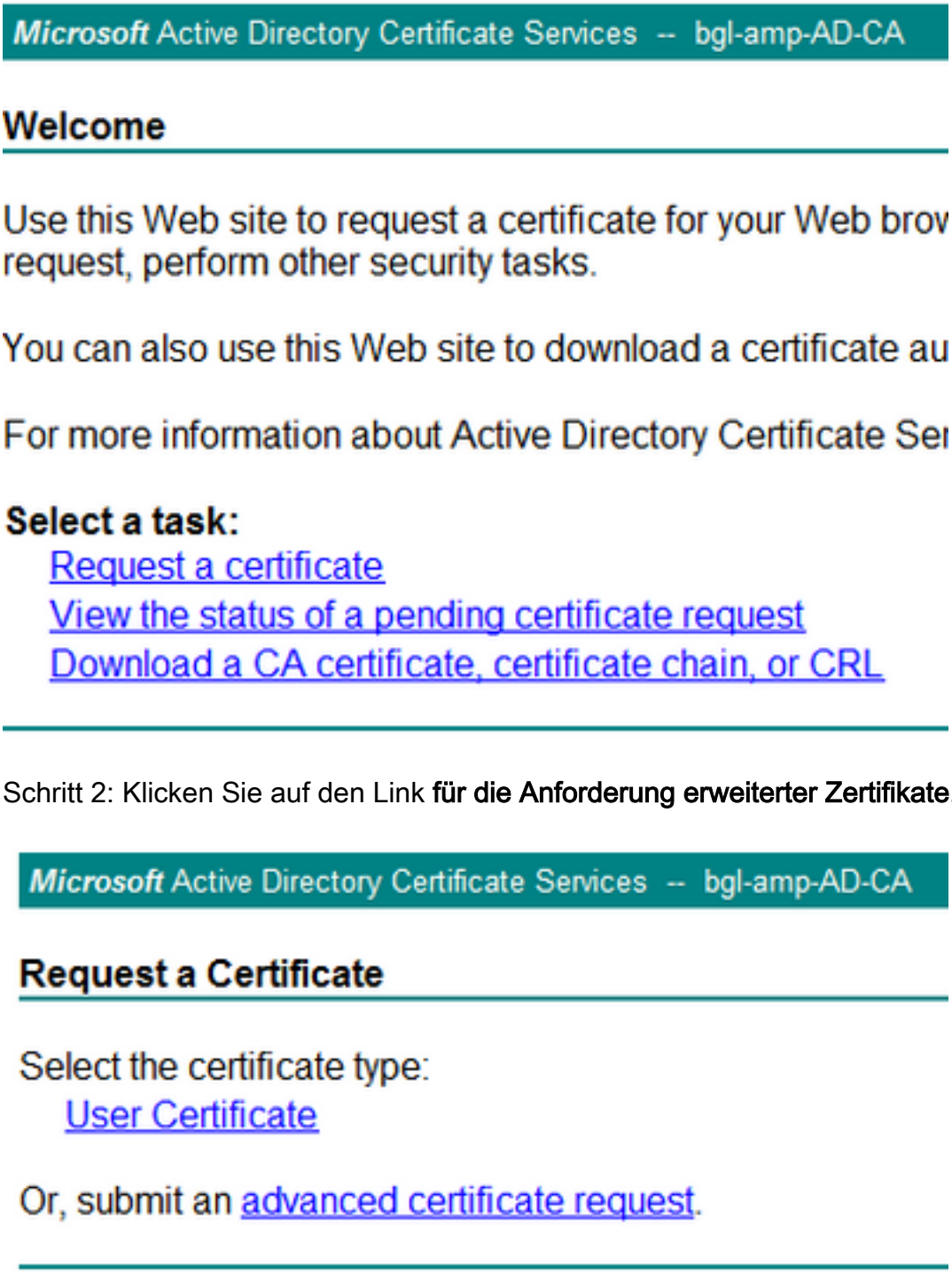


Schritt 11. Wählen Sie abschließend **OK**. Dies muss Sie zum Dialogfeld Zertifikatregistrierung führen, in dem Sie **Weiter** auswählen können.

Schritt 12: Navigieren Sie zu einem Speicherort für die REQ-Datei, die zur Signatur an den CA-Server gesendet wird.

Einreichen des CSR an die Zertifizierungsstelle und Generieren des Zertifikats

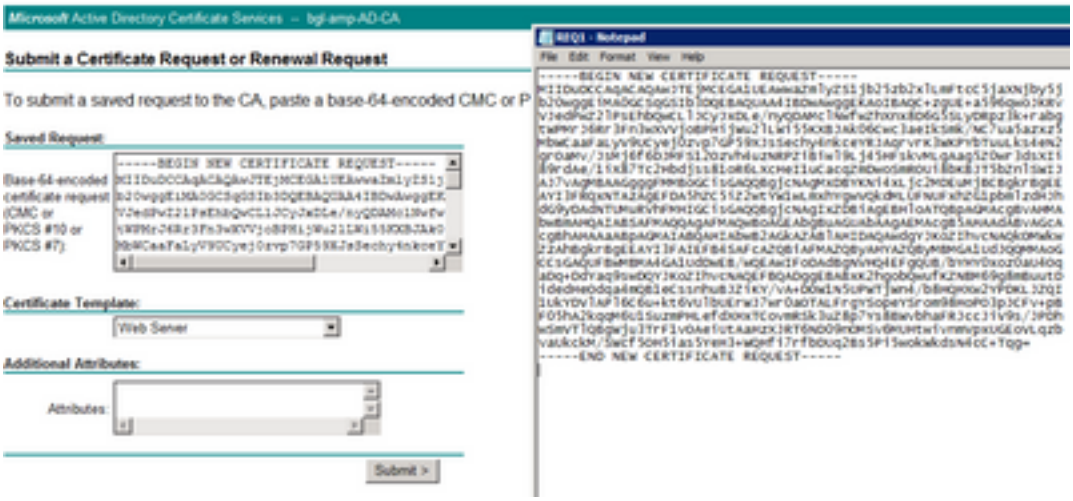
Schritt 1: Navigieren Sie wie unten zu Ihrer MS AD-Zertifikatdienste-Webseite, und wählen Sie **Zertifikat anfordern aus**.



Schritt 2: Klicken Sie auf den Link **für die Anforderung erweiterter Zertifikate**.

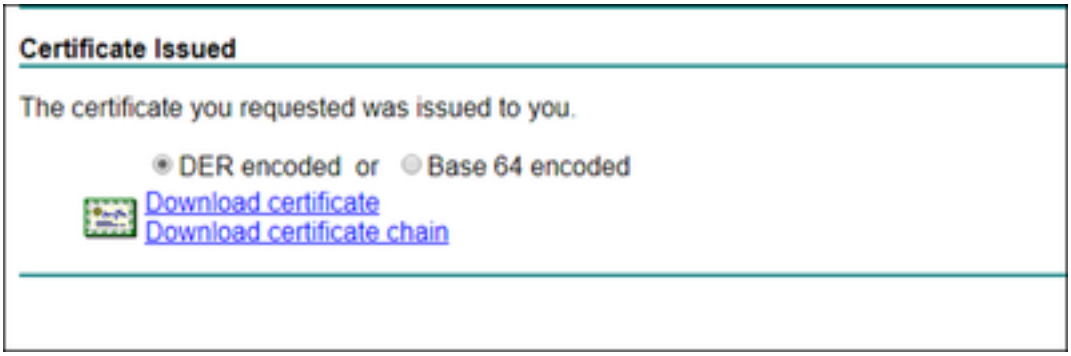
Schritt 3: Wählen Sie bei **Senden einer Zertifikatsanforderung mithilfe einer Base-64-codierten CMC- oder PKCS #10-Datei aus, oder senden Sie eine Verlängerungsanforderung mithilfe einer Base-64-codierten PKCS #7-Datei**.

Schritt 4: Öffnen Sie den Inhalt der zuvor gespeicherten REQ-Datei (CSR) über den Editor. Kopieren Sie den Inhalt, und fügen Sie ihn hier ein. Stellen Sie sicher, dass die Zertifikatvorlage als **Webserver** ausgewählt ist.



Schritt 5: Wählen Sie anschließend **Senden**.

Schritt 6: An diesem Punkt müssen Sie in der Lage sein, das Zertifikat **herunterzuladen**, wie im Bild dargestellt.



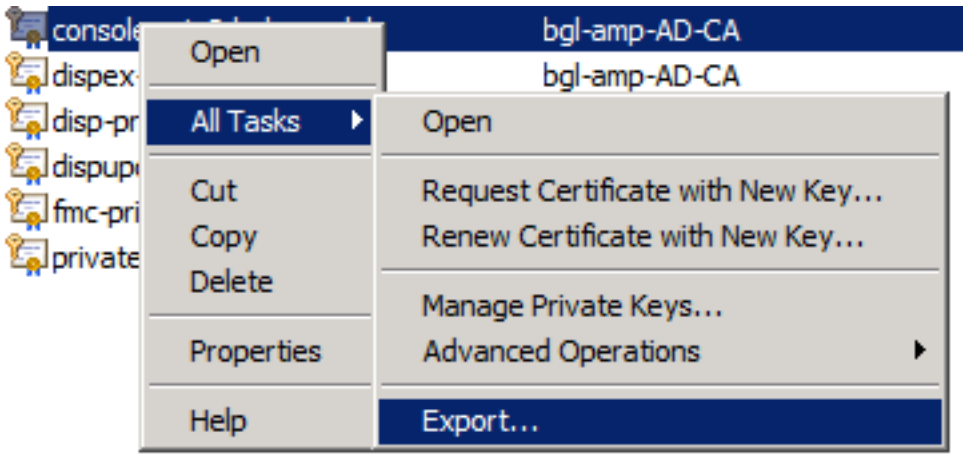
Den privaten Schlüssel exportieren und in das PEM-Format konvertieren

Schritt 1: Installieren Sie das Zertifikat in Ihrem Zertifikatspeicher, indem Sie die CER-Datei öffnen und **Zertifikat installieren** auswählen.

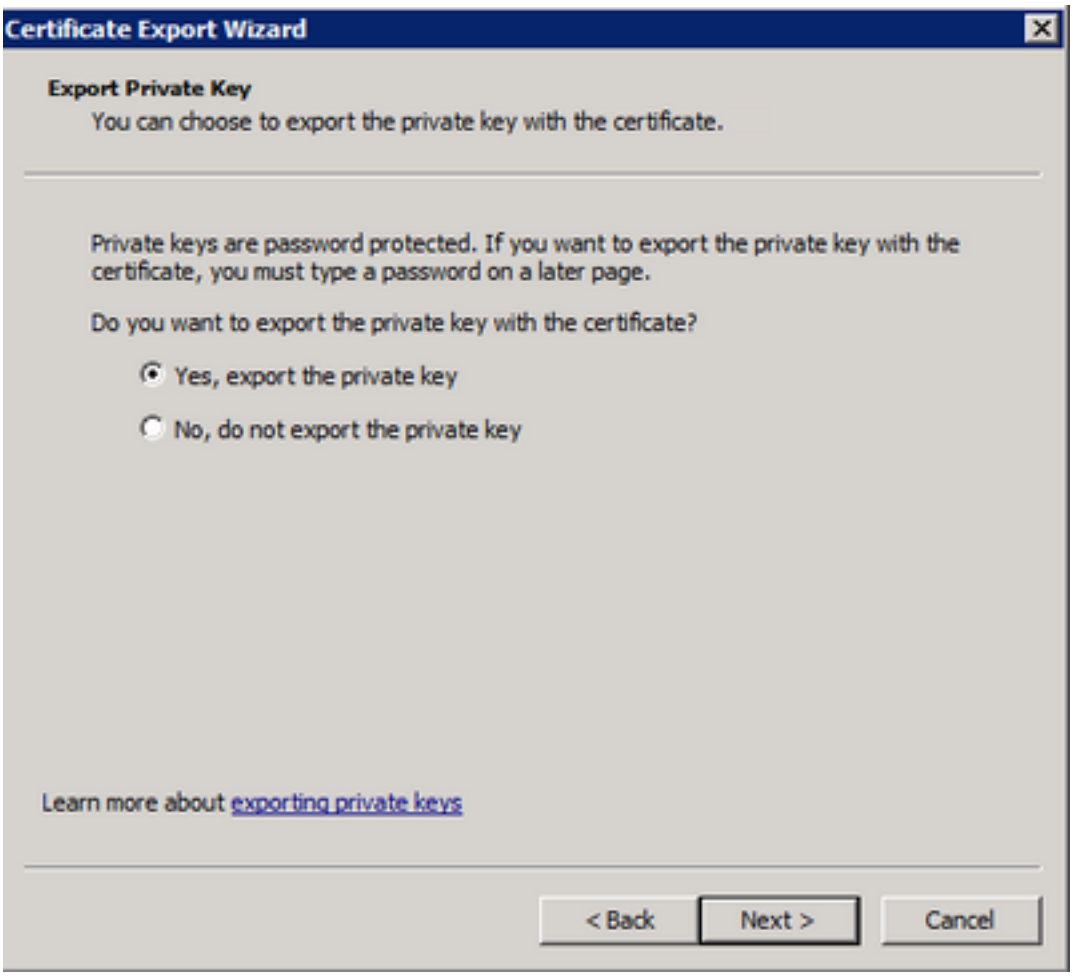
Schritt 2: Navigieren Sie zum MMC-Snap-In, das zuvor ausgewählt wurde.

Schritt 3: Navigieren Sie zu dem Speicher, in dem das Zertifikat installiert wurde.

Schritt 4: Klicken Sie mit der rechten Maustaste auf das richtige Zertifikat, und wählen Sie **Alle Aufgaben > Exportieren aus**.



Schritt 5: Bestätigen Sie im Zertifikatexport-Assistenten, dass der private Schlüssel exportiert wird, wie im Bild gezeigt.



Schritt 6: Geben Sie ein Kennwort ein, und wählen Sie **Weiter aus**, um den privaten Schlüssel auf der Festplatte zu speichern.

Schritt 7. Dadurch wird der private Schlüssel im PFX-Format gespeichert. Dies muss jedoch in das PEM-Format konvertiert werden, um ihn in Secure Endpoint Private Cloud verwenden zu können.

Schritt 8: OpenSSL-Bibliotheken installieren

Schritt 9. Öffnen Sie ein Eingabeaufforderungsfenster, und wechseln Sie in das Verzeichnis, in dem Sie OpenSSL installiert haben.

Schritt 10. Führen Sie den folgenden Befehl aus, um den privaten Schlüssel zu extrahieren und in einer neuen Datei zu speichern: (Wenn sich Ihre PFX-Datei nicht im gleichen Pfad wie die OpenSSL-Bibliothek befindet, müssen Sie den genauen Pfad zusammen mit dem Dateinamen angeben)

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes
```

Schritt 11. Führen Sie nun den folgenden Befehl aus, um auch das öffentliche Zertifikat zu extrahieren und in einer neuen Datei zu speichern:

```
openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes
```

Zertifikat auf Linux-Server generieren (SSL-Prüfung für strikte Sicherheit

DEAKTIVIERT)

> **Hinweis**: Mit der strengen TLS-Prüfung wird überprüft, ob das Zertifikat die TLS-Anforderungen von Apple erfüllt. Weitere Informationen finden Sie im Administratorhandbuch.

Stellen Sie sicher, dass die OpenSSL 1.1.1-Bibliotheken auf dem Linux-Server, auf dem Sie versuchen, die erforderlichen Zertifikate zu generieren, installiert sind. Es wird überprüft, ob dies und das unten aufgeführte Verfahren von der Linux-Distribution, die Sie ausführen, abweichen können. Dieser Abschnitt wurde dokumentiert, wie auf einem CentOS 8.4 Server.

Selbstsignierte RootCA generieren

Schritt 1: Generieren Sie den privaten Schlüssel für das Zertifikat der Stammzertifizierungsstelle.

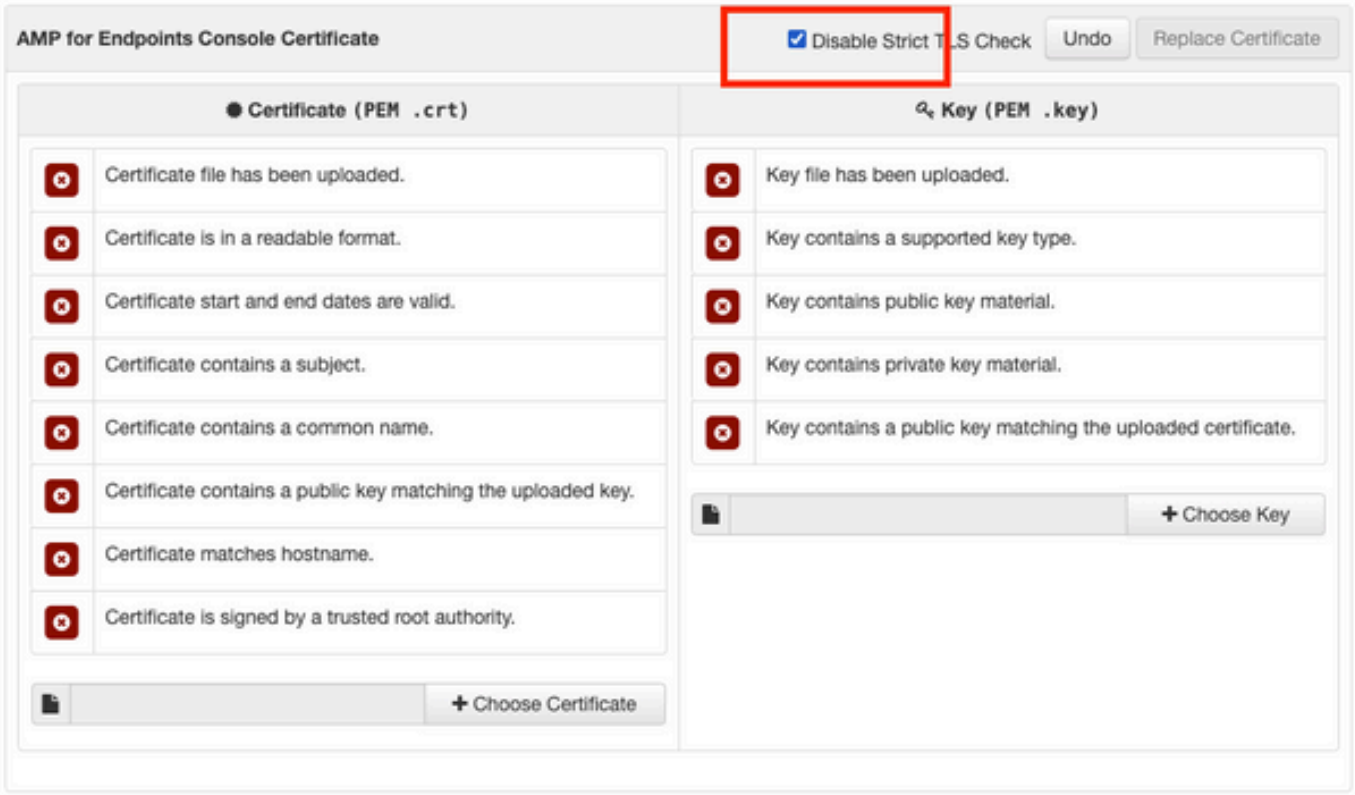
```
openssl genrsa -out
```

Schritt 2: Erstellen des Zertifizierungsstellenzertifikats

```
openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"
```

Zertifikat für jeden Dienst generieren

Erstellen Sie das Zertifikat für den Service Authentication, Console, Disposition, Disposition-Extended, Update server, FirePOWER Management Center (FMC) entsprechend dem DNS-Namenseintrag. Sie müssen den unten stehenden Zertifikatgenerierungsprozess für jeden Dienst (Authentifizierung, Konsole usw.) wiederholen.



Privaten Schlüssel generieren

```
openssl genrsa -out
```

Ersetzen Sie <YourServiceName.key> durch den neuen KEY-Dateinamen, der als Auth-Cert.key erstellt werden soll.

CSR erstellen

```
openssl req -new \
-subj '/CN=
-key
```

Ersetzen Sie <YourServiceName.key> mit der aktuellen (oder neuen) KEY-Zertifikatsdatei wie Auth-Cert.key

Ersetzen Sie <YourServiceName.csr> durch einen zu erstellenden CSR-Dateinamen wie Auth-Cert.crt.

Zertifikat generieren

```
openssl x509 -req \
-in
-CAkey
-days 397 -sha256
```

Ersetzen Sie <YourServiceName.csr> durch eine aktuelle (oder neue) Zertifikat-CSR, z. B. Auth-Cert.csr.

Ersetzen Sie <YourRootCAName.pem> durch den tatsächlichen (oder neuen) PEM-Dateinamen

RootCAName.pem.

Ersetzen Sie <YourServiceName.key> durch die aktuelle (oder neue) KEY-Zertifikatsdatei, z. B. Auth-Cert.key

Ersetzen Sie <YourServiceName.crt> durch einen zu erstellenden Dateinamen wie Auth-Cert.crt.

Zertifikat auf Linux-Server generieren (SSL-Prüfung "Strict" AKTIVIERT)

> **Hinweis**: Mit der strengen TLS-Prüfung wird überprüft, ob das Zertifikat die TLS-Anforderungen von Apple erfüllt. Weitere Informationen finden Sie im Administratorhandbuch.

Selbstsignierte RootCA generieren

Schritt 1: Generieren Sie den privaten Schlüssel für das Zertifikat der Stammzertifizierungsstelle.

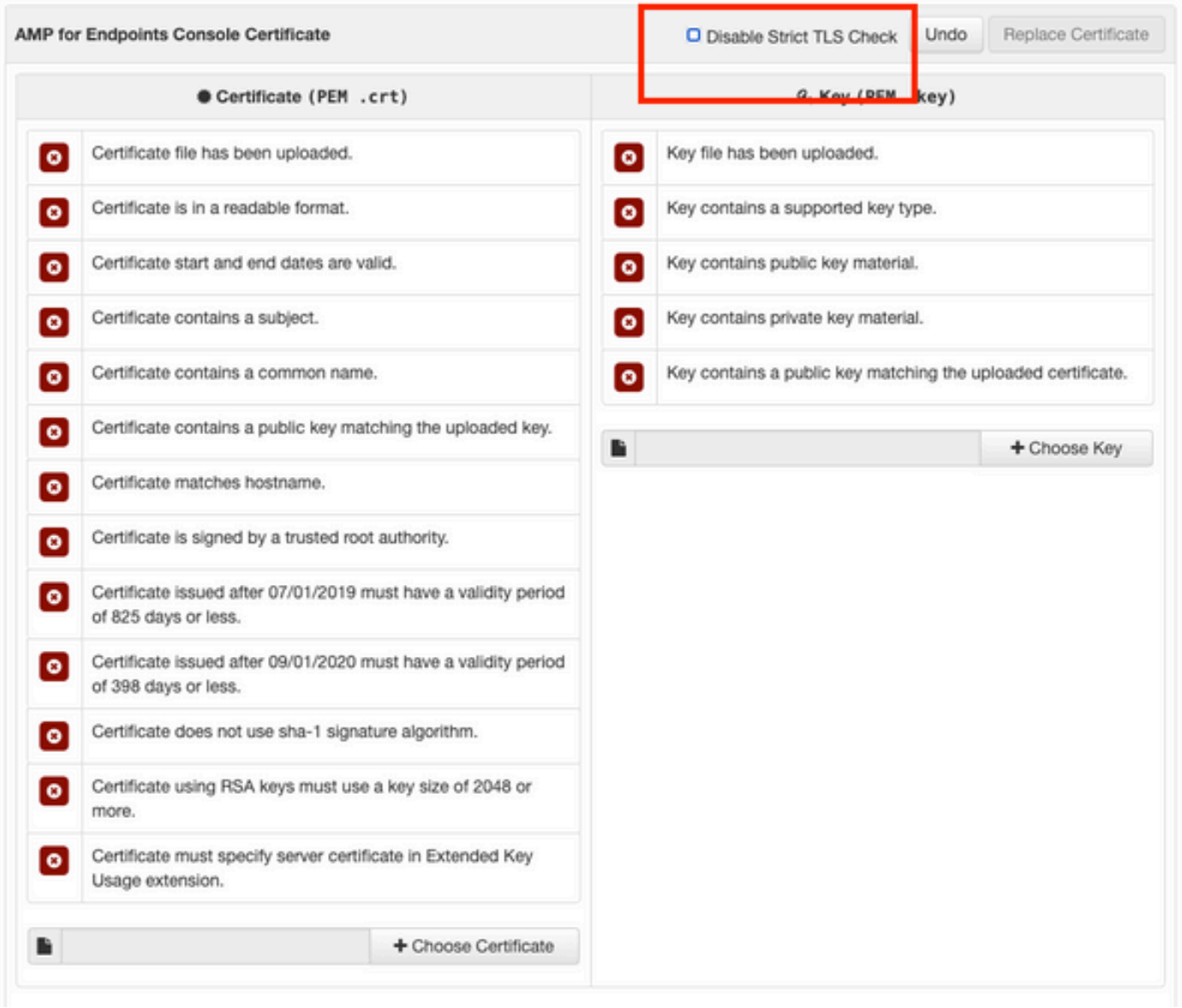
```
openssl genrsa -out
```

Schritt 2: Erstellen des Zertifizierungsstellenzertifikats

```
openssl req \
-subj '/CN=
-outform pem -out
-key
-days "1000"
```

Zertifikat für jeden Dienst generieren

Erstellen Sie das Zertifikat für den Service Authentication, Console, Disposition, Disposition-Extended, Update server, FirePOWER Management Center (FMC) entsprechend dem DNS-Namenseintrag. Sie müssen den unten stehenden Zertifikatgenerierungsprozess für jeden Dienst (Authentifizierung, Konsole usw.) wiederholen.



Erstellen und speichern Sie eine Konfigurationsdatei für die Erweiterungen (extensions.cnf).

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

Privaten Schlüssel generieren

```
openssl genrsa -out
```

Ersetzen Sie <YourServiceName.key> durch einen neuen KEY-Dateinamen, der als Auth-Cert.key erstellt werden soll.

CSR erstellen

```
openssl req -new \
-key
-subj '/CN=
-out
```

Ersetzen Sie <YourServiceName.key> mit dem aktuellen (oder neuen) Zertifikatschlüssel, z. B. Auth-Cert.key

Ersetzen Sie <YourServiceName.csr> durch den aktuellen (oder neuen) CSR für das Zertifikat, z. B. Auth-Cert.csr.

Zertifikat generieren

```
openssl x509 -req -in
-CA
-CAcreateserial -out
-extensions v3_ca -extfile extensions.cnf \
-days 397 -sha256
```

Ersetzen Sie <YourServiceName.csr> durch eine aktuelle (oder neue) Zertifikat-CSR wie Auth-Cert.csr.

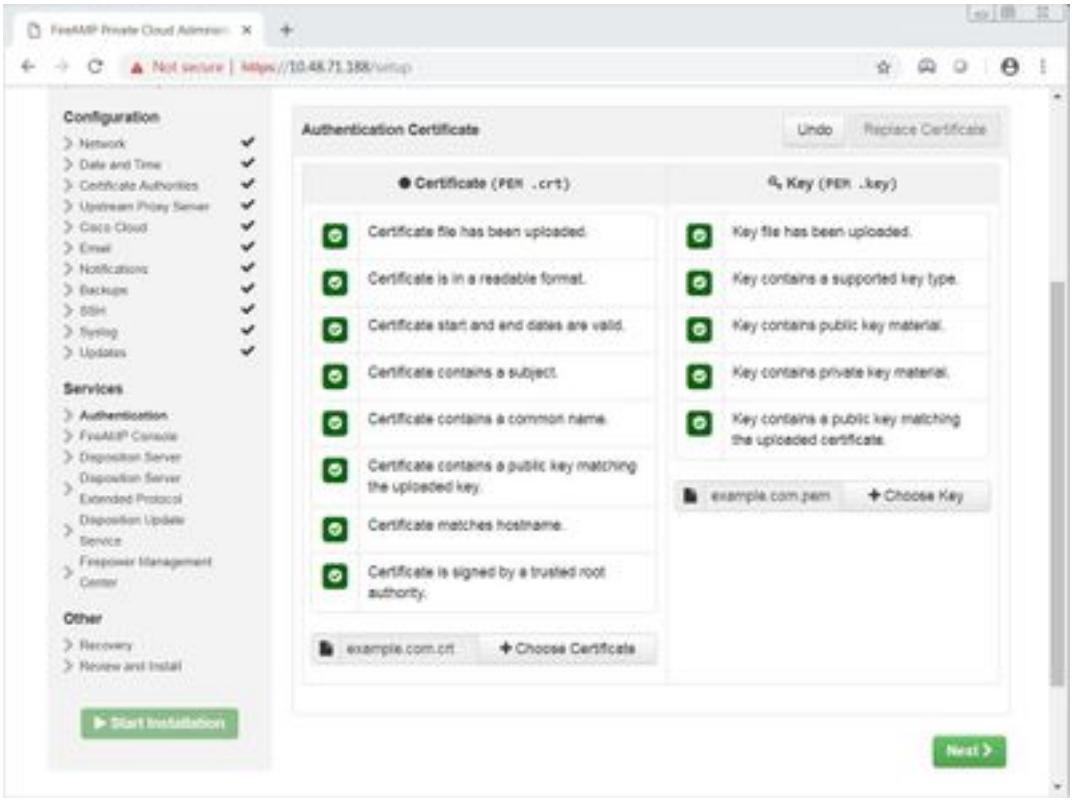
Ersetzen Sie <YourRootCAName.pem> durch den aktuellen (oder neuen) PEM-Dateinamen RootCAName.pem.

Ersetzen Sie <YourServiceName.key> durch die aktuelle (oder neue) KEY-Zertifikatsdatei, z. B. Auth-Cert.key.

Ersetzen Sie <YourServiceName.crt> durch einen zu erstellenden Dateinamen wie Auth-Cert.crt.

Hinzufügen der Zertifikate zur Secure Console Private Cloud

Schritt 1: Wenn die Zertifikate auf einer der oben genannten Methoden generiert wurden, laden Sie das entsprechende Zertifikat für jeden der Dienste hoch. Wenn sie korrekt generiert wurden, sind alle Auswahlfelder aktiviert, wie im Bild zu sehen ist.



Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

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.