

Implementieren von CA-signierten Zertifikaten in einer CCE-Lösung

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrund](#)

[Vorgehensweise](#)

[CCE Windows-basierte Server](#)

[1. CSR erstellen](#)

[2. Entgegennehmen der von der Zertifizierungsstelle signierten Zertifikate](#)

[3. Laden Sie die CA Signed Certificates hoch](#)

[4. Binden des von der Zertifizierungsstelle signierten Zertifikats an IIS](#)

[5. Binden des CA-signierten Zertifikats an das Diagnoseportal](#)

[6. Importieren Sie das Stamm- und Zwischenzertifikat in den Java-Schlüsselspeicher.](#)

[CVP-Lösung](#)

[1. Zertifikate mit FQDN generieren](#)

[2. CSR erstellen](#)

[3. Entgegennehmen der von der Zertifizierungsstelle signierten Zertifikate](#)

[4. Importieren Sie die von der Zertifizierungsstelle signierten Zertifikate](#)

[VOS-Server](#)

[1. CSR-Zertifikat generieren](#)

[2. Entgegennehmen der von der Zertifizierungsstelle signierten Zertifikate](#)

[3. Laden Sie die Anwendungs- und Stammzertifikate hoch.](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Implementierung von CA-Zertifikaten (Certificate Authority) in der CCE-Lösung (Cisco Contact Center Enterprise) beschrieben.

Beiträge von Anuj Bhatia, Robert Rogier und Ramiro Amaya, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

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

- Unified Contact Center Enterprise (UCCE) Version 12.5(1)
- Package Contact Center Enterprise Version 12.5(1)
- Customer Voice Portal (CVP) Version 12.5 (1)
- Cisco Virtualized Voice Browser (VB)
- Cisco CVP Operations and Administration Console (OAMP)

- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Communication Manager (CUCM)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- PCCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12,5
- Feinheiten 12,5
- CUIC 12.5
- Windows 2016

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.

Hintergrund

Zertifikate werden verwendet, um sicherzustellen, dass die Kommunikation mit der Authentifizierung zwischen Clients und Servern sicher ist.

Benutzer können Zertifikate von einer Zertifizierungsstelle erwerben oder selbst signierte Zertifikate verwenden.

Selbstsignierte Zertifikate (wie der Name schon sagt) werden von derselben Stelle signiert, deren Identität sie bescheinigen, während sie von einer Zertifizierungsstelle signiert werden. Selbstsignierte Zertifikate werden nicht als so sicher wie CA-Zertifikate betrachtet, werden jedoch standardmäßig in vielen Anwendungen verwendet.

In der Package Contact Center Enterprise (PCCE)-Lösung Version 12.x werden alle Komponenten der Lösung von Single Pane of Glass (SPOG) gesteuert, der auf dem Hauptserver der Admin Workstation (AW) gehostet wird.

Aufgrund von Security Management Compliance (SRC) in der PCCE 12.5(1)-Version erfolgt die gesamte Kommunikation zwischen SPOG und anderen Komponenten der Lösung über ein sicheres HTTP-Protokoll. In UCCE 12.5 erfolgt die Kommunikation zwischen den Komponenten ebenfalls über ein sicheres HTTP-Protokoll.

In diesem Dokument werden die erforderlichen Schritte zum Implementieren von CA-signierten Zertifikaten in einer CCE-Lösung für die sichere HTTP-Kommunikation detailliert beschrieben. Weitere Sicherheitsüberlegungen zu UCCE finden Sie in den [UCCE-Sicherheitsrichtlinien](#). Informationen zu zusätzlichen sicheren CVP-Verbindungen, die sich von sicheren HTTP-Verbindungen unterscheiden, finden Sie in den Sicherheitsrichtlinien im CVP-Konfigurationsleitfaden: [CVP Security Guidelines](#).

Vorgehensweise

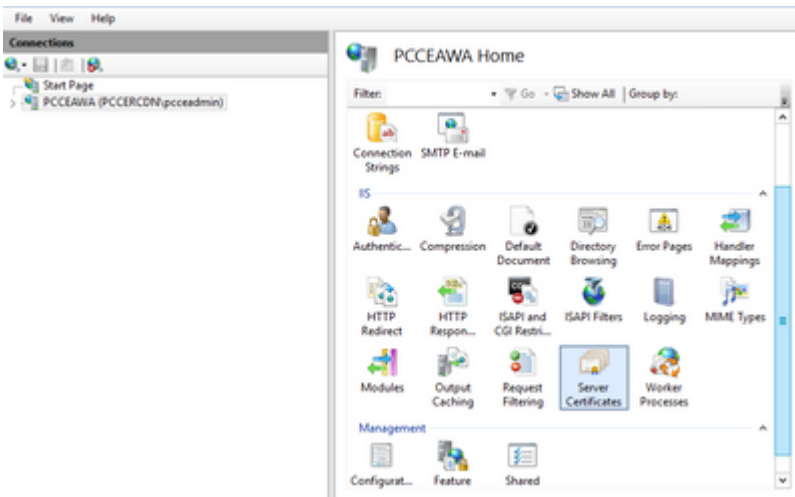
CCE Windows-basierte Server

1. CSR erstellen

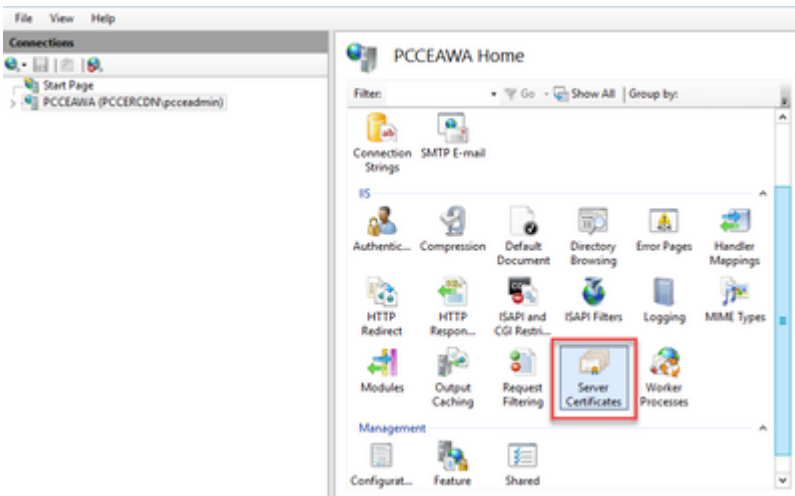
In diesem Verfahren wird erläutert, wie Sie eine CSR-Anforderung (Certificate Signing Request) vom Internetinformationsdienste-Manager (IIS-Manager) generieren.

Schritt 1: Melden Sie sich bei Windows an, und wählen Sie **Systemsteuerung > Verwaltung > Internetinformationsdienste (IIS)-Manager** aus.

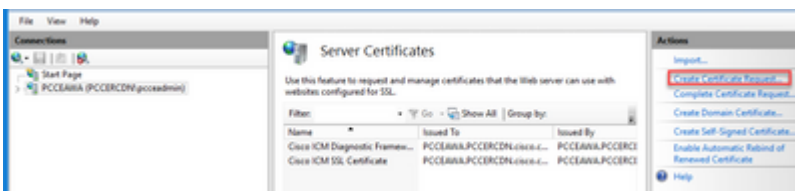
Schritt 2: Klicken Sie im Bereich Verbindungen auf den Servernamen. Der Server-Hauptbereich wird angezeigt.



Schritt 3: Doppelklicken Sie im IIS-Bereich auf Serverzertifikate.

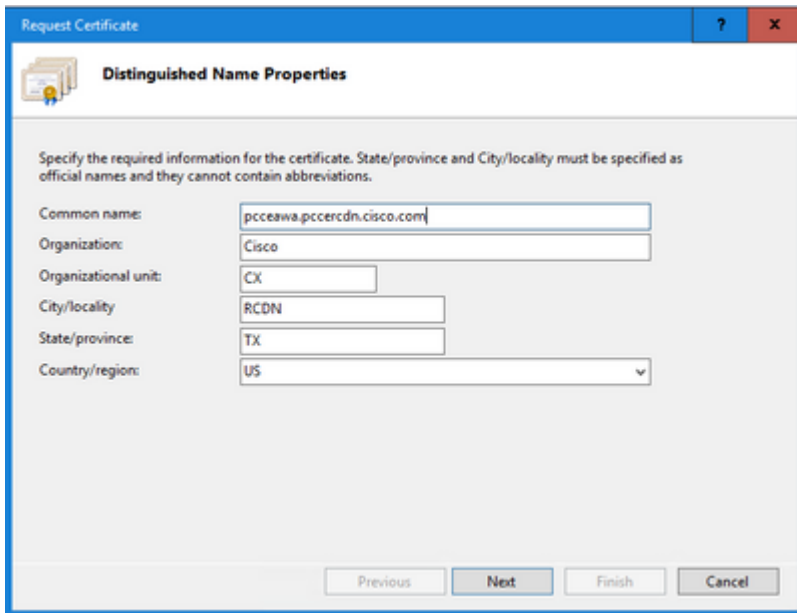


Schritt 4: Klicken Sie im Aktionsbereich auf **Zertifikatsanforderung erstellen**.



Schritt 5: Führen Sie im Dialogfeld Zertifikat anfordern die folgenden Schritte aus:

Geben Sie die erforderlichen Informationen in den angezeigten Feldern ein, und klicken Sie auf **Weiter**.



Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:

Organization:

Organizational unit:

City/locality:

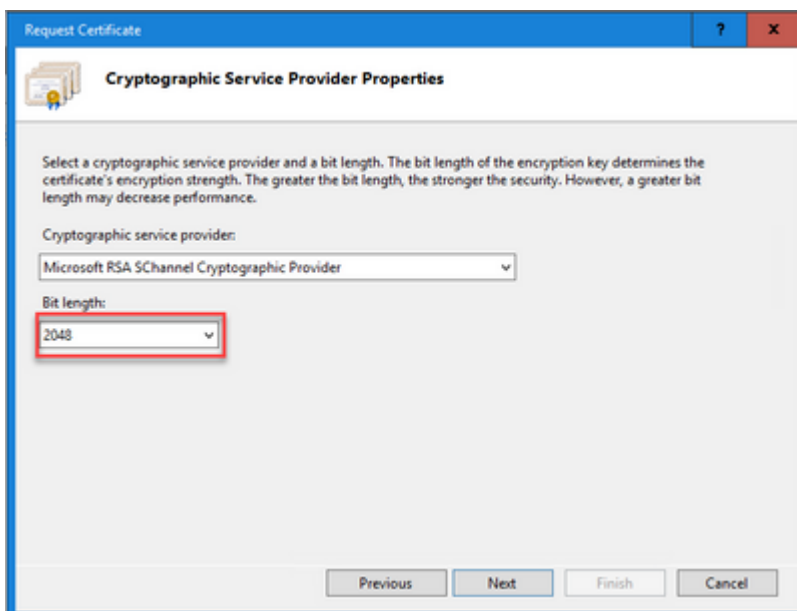
State/province:

Country/region:

Previous Next Finish Cancel

Belassen Sie in der Dropdown-Liste für den Kryptografiedienstanbieter die Standardeinstellung.

Wählen Sie in der Dropdown-Liste Bitlänge die Option **2048** aus.



Request Certificate

Cryptographic Service Provider Properties

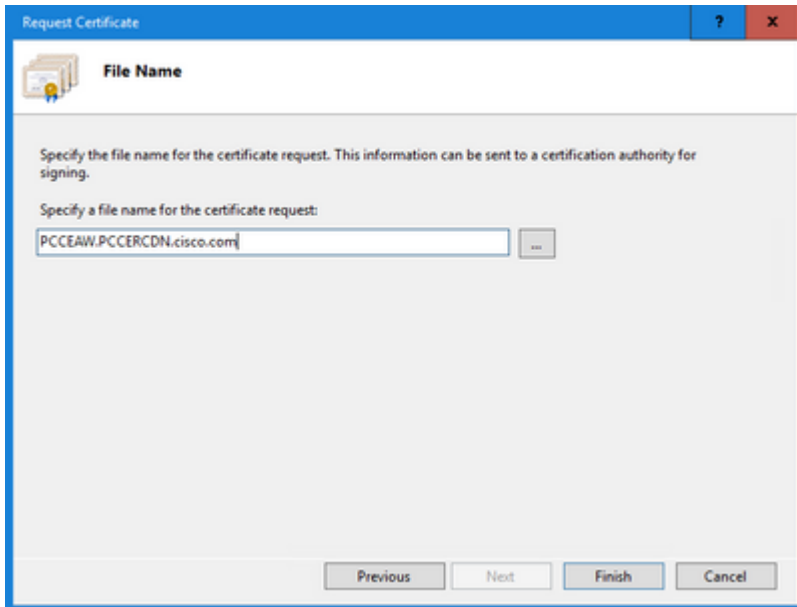
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:

Bit length:

Previous Next Finish Cancel

Schritt 6: Geben Sie einen Dateinamen für die Zertifikatanforderung an, und klicken Sie auf **Fertig stellen**.



2. Entgegennehmen der von der Zertifizierungsstelle signierten Zertifikate

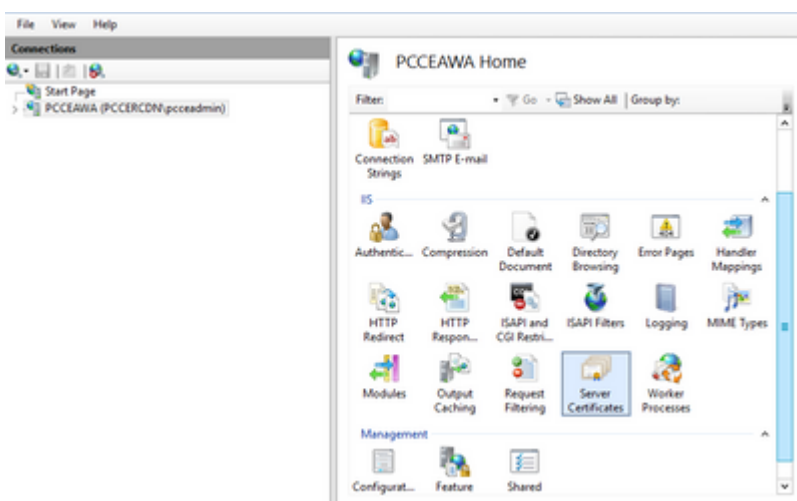
Schritt 1: Signieren des Zertifikats auf einer Zertifizierungsstelle

Hinweis: Stellen Sie sicher, dass die von der CA verwendete Zertifikatvorlage die Client- und Serverauthentifizierung enthält.

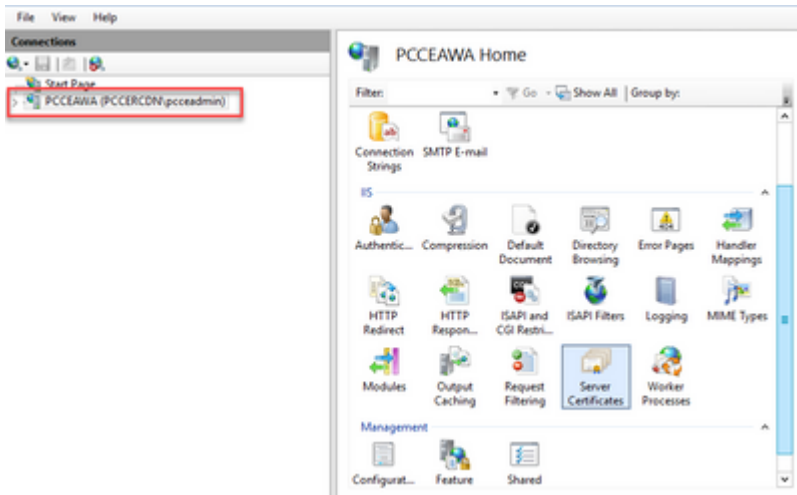
Schritt 2: Holen Sie die von der Zertifizierungsstelle signierten Zertifikate ein (Stamm, Anwendung und Zwischenprodukt, falls vorhanden).

3. Laden Sie die CA Signed Certificates hoch

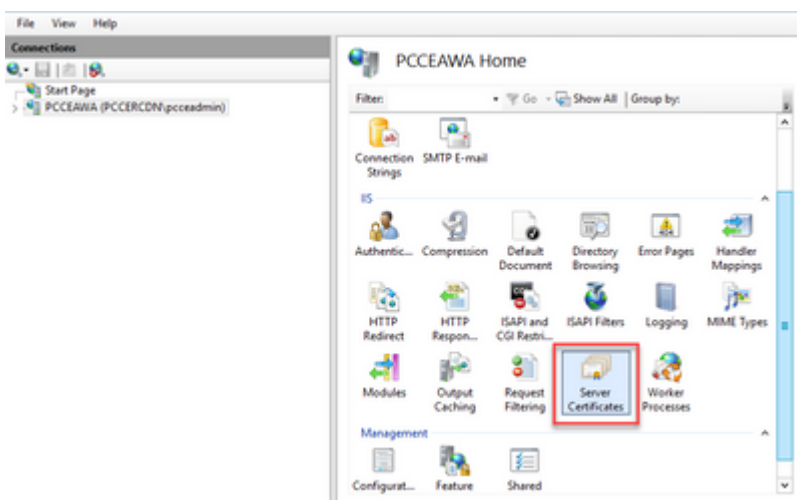
Schritt 1: Melden Sie sich bei Windows an, und wählen Sie **Systemsteuerung > Verwaltung > Internetinformationsdienste (IIS)-Manager** aus.



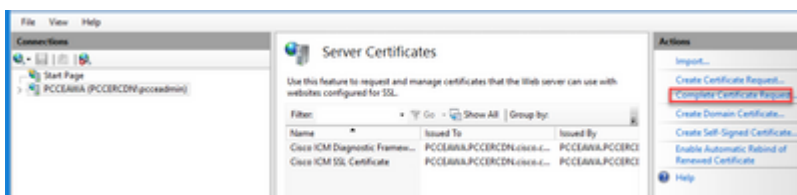
Schritt 2: Klicken Sie im Bereich Verbindungen auf den Servernamen.



Schritt 3: Doppelklicken Sie im IIS-Bereich auf **Serverzertifikate**.



Schritt 4: Klicken Sie im Aktionsbereich auf **Zertifikatsanforderung abschließen**.



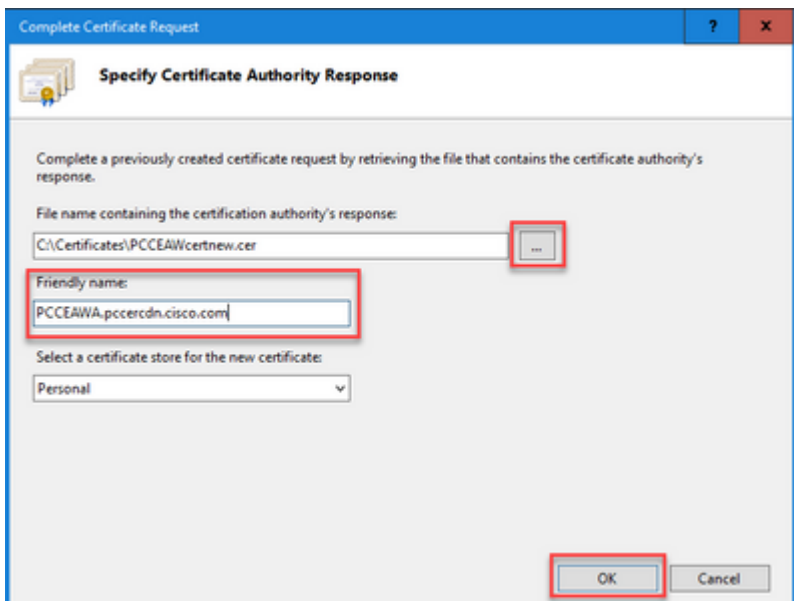
Schritt 5: Füllen Sie im Dialogfeld Complete Certificate Request (Zertifikatsanforderung abschließen) die folgenden Felder aus:

Klicken Sie im Feld Dateiname, das die Antwort der Zertifizierungsstelle enthält, auf die Schaltfläche

Navigieren Sie zu dem Speicherort, in dem das signierte Anwendungszertifikat gespeichert ist, und klicken Sie dann auf Öffnen.

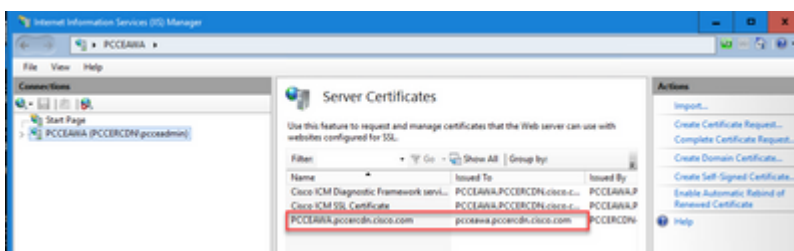
Hinweis: Wenn es sich um eine zweistufige CA-Implementierung handelt und das Stammzertifikat noch nicht im Serverzertifikatsspeicher vorhanden ist, muss der Stamm in den Windows-Speicher hochgeladen werden, bevor Sie das signierte Zertifikat importieren. Weitere Informationen zum Hochladen der Stammzertifizierungsstelle in den Windows Store finden Sie in diesem Dokument unter <https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate>.

Geben Sie im Feld Anzeigename den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) des Servers oder einen für Sie wichtigen Namen ein. Stellen Sie sicher, dass das Dropdown-Menü **Zertifikatsspeicher** auswählen für das neue Zertifikat als **Personal** angezeigt wird.



Schritt 6: Klicken Sie auf **OK**, um das Zertifikat hochzuladen.

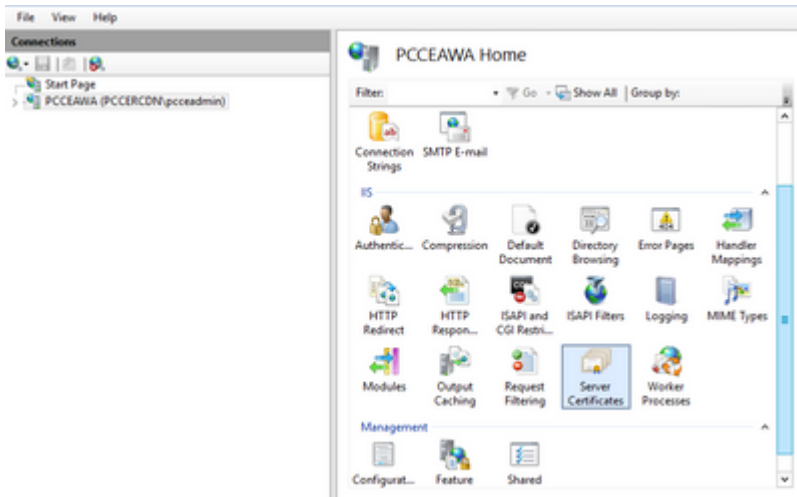
Wenn das Zertifikat erfolgreich hochgeladen wurde, wird das Zertifikat im Bereich "Serverzertifikate" angezeigt.



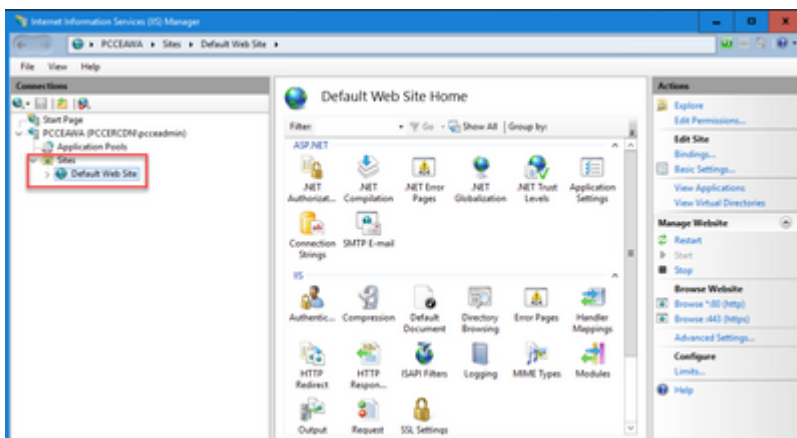
4. Binden des von der Zertifizierungsstelle signierten Zertifikats an IIS

In diesem Verfahren wird erläutert, wie ein Zertifikat mit CA-Signatur an den IIS-Manager gebunden wird.

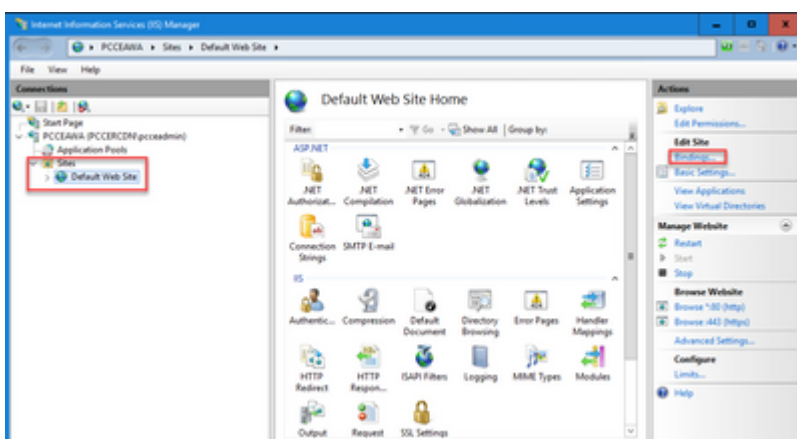
Schritt 1: Melden Sie sich bei Windows an, und wählen Sie **Systemsteuerung > Verwaltung > Internetinformationsdienste (IIS)-Manager** aus.



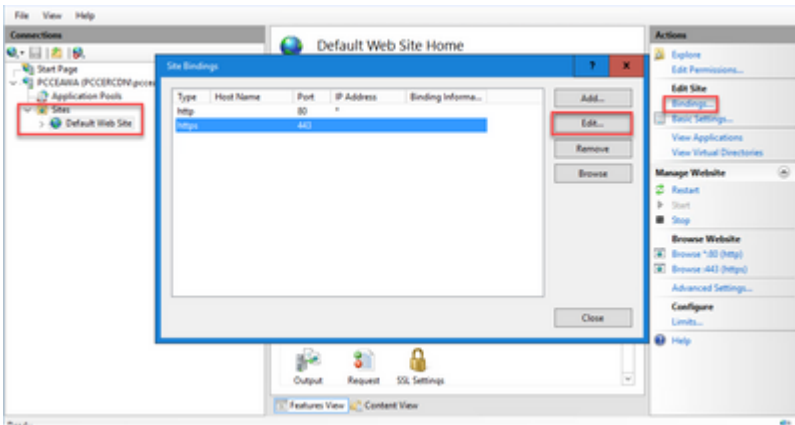
Schritt 2: Wählen Sie im Bereich Verbindungen die Option <Servername> > Sites > **Default Web Site** aus.



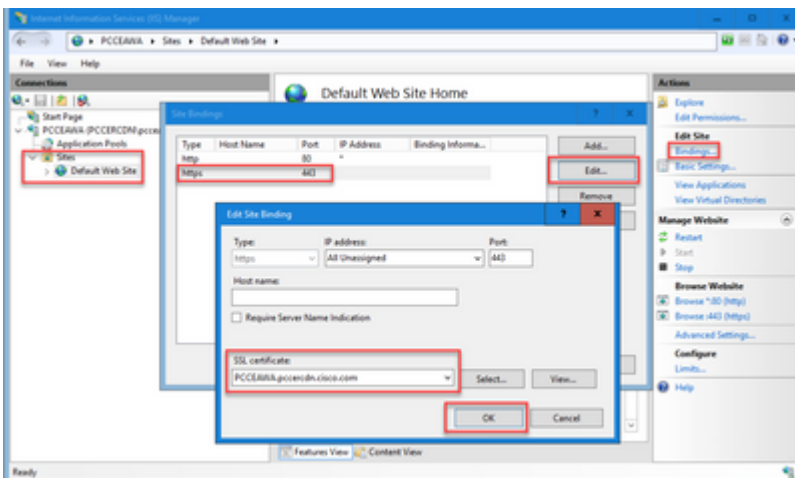
Schritt 3: Klicken Sie im Aktionsbereich auf **Bindungen...**



Schritt 4: Klicken Sie auf den Typ **https** mit Port **443**, und klicken Sie dann auf **Bearbeiten...**

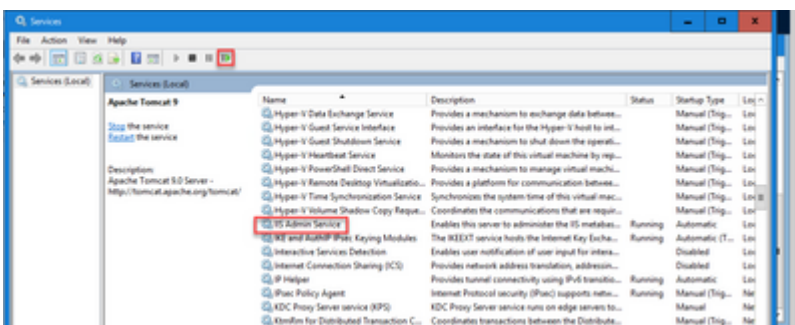


Schritt 5: Wählen Sie aus der Dropdown-Liste für das SSL-Zertifikat das Zertifikat mit dem gleichen Anzeigenamen aus, der im vorherigen Schritt angegeben wurde.



Schritt 6: Klicken Sie auf **OK**.

Schritt 7. Navigieren Sie zu **Start > Ausführen > services.msc**, und starten Sie den IIS-Administratordienst neu.



Wenn IIS erfolgreich neu gestartet wird, werden beim Starten der Anwendung keine Zertifikatfehlerwarnungen angezeigt.

5. Binden des CA-signierten Zertifikats an das Diagnoseportal

In diesem Verfahren wird erläutert, wie ein CA-signiertes Zertifikat im Diagnosebereich gebunden wird.

Schritt 1: Öffnen Sie die Eingabeaufforderung (Als Administrator ausführen).

Schritt 2: Navigieren Sie zum Startordner des Diagnoseportals. Führen Sie diesen Befehl aus:

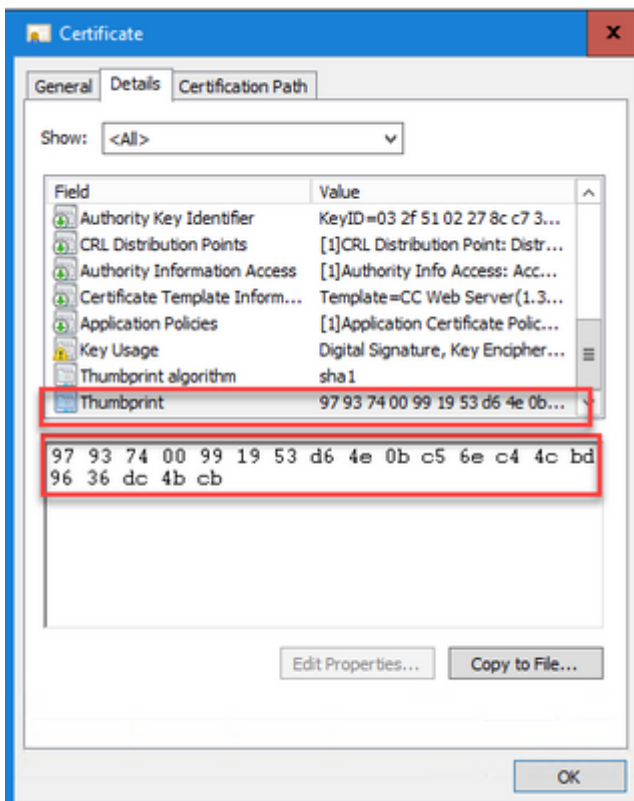
```
cd c:\vicm\serviceability\diagnostics\bin
```

Schritt 3: Entfernen Sie die aktuelle Zertifikatbindung aus dem Diagnosebereich. Führen Sie diesen Befehl aus:

```
DiagFwCertMgr /task:UnbindCert
```

```
c:\vicm\serviceability\diagnostics\bin>DiagFwCertMgr /task:UnbindCert
*****
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager
*****
Executing Task: 'UnbindCert'
Read port number from service configuration file: '7890'
ATTEMPTING TO UNBIND CERTIFICATE FROM WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to delete the existing binding on 0.0.0.0:7890
Deleted existing binding successfully
Deleted entry from the service registry
ALL TASKS FOR UNBINDING THE CERTIFICATE FROM HTTP SERVICE COMPLETED SUCCESSFULLY
c:\vicm\serviceability\diagnostics\bin>
```

Schritt 4: Öffnen Sie das signierte Zertifikat, und kopieren Sie den Hashinhalt (ohne Leerzeichen) des Felds "Fingerabdruck".



Schritt 5: Führen Sie diesen Befehl aus, und fügen Sie den Hashinhalt ein.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```

```
E:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:BindCertFromStore /certhash:97937400991953d64e0bc56ec44cb096360c48cb
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager

Executing Task: 'BindCertFromStore'
Read port number from service configuration file: '7890'
Certhash Argument Passed: '97937400991953d64e0bc56ec44cb096360c48cb'
ATTEMPTING TO BIND CERTIFICATE WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Trying to look up certificate: 97937400991953d64e0bc56ec44cb096360c48cb
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
Certificate bind with HTTP service on 0.0.0.0:7890 completed successfully
Found existing registry key for the service
Hash of certificate used stored in the service registry
ALL TASKS FOR BINDING THE CERTIFICATE WITH HTTP SERVICE COMPLETED SUCCESSFULLY

E:\icm\serviceability\diagnostics\bin>
```

Wenn die Zertifikatbindung erfolgreich war, wird die Meldung **Die Zertifikatbindung ist GÜLTIG** angezeigt.

Schritt 6: Überprüfen, ob die Zertifikatbindung erfolgreich war Führen Sie diesen Befehl aus:

```
DiagFwCertMgr /task:ValidateCertBinding
```

```
E:\icm\serviceability\diagnostics\bin>DiagFwCertMgr /task:ValidateCertBinding
Cisco Unified ICM/CCE Diagnostic Framework Certificate Manager

Executing Task: 'ValidateCertBinding'
Read port number from service configuration file: '7890'
ATTEMPTING TO VALIDATE CERTIFICATE BINDING WITH WINDOWS HTTP SERVICE
Binding IP Address: '0.0.0.0:7890'
Attempting to query HTTP service for SSL certificate binding
Found a certificate binding on 0.0.0.0:7890
Attempting to locate this certificate in the Local Computer certificate store
Trying to look up certificate: 97937400991953d64e0bc56ec44cb096360c48cb
Local Computer Personal certificate store was opened successfully
Certificate requested found in store
Certificate store was closed successfully
The certificate binding is VALID
Certificate hash stored in service registry matches certificate used by service
ALL TASKS FOR VALIDATING CERTIFICATE BINDING COMPLETED SUCCESSFULLY

c:\icm\serviceability\diagnostics\bin>
```

Hinweis: DiagFwCertMgr verwendet standardmäßig Port 7890.

Wenn die Zertifikatbindung erfolgreich war, wird die Meldung **Die Zertifikatbindung ist GÜLTIG** angezeigt.

Schritt 7. Starten Sie den Diagnose-Framework-Dienst neu. Führen Sie folgende Befehle aus:

```
net stop DiagFwSvc
net start DiagFwSvc
```

Wenn das Diagnose-Framework erfolgreich neu gestartet wird, werden beim Starten der Anwendung keine Zertifikatfehlerwarnungen angezeigt.

6. Importieren Sie das Stamm- und Zwischenzertifikat in den Java-Schlüsselspeicher.

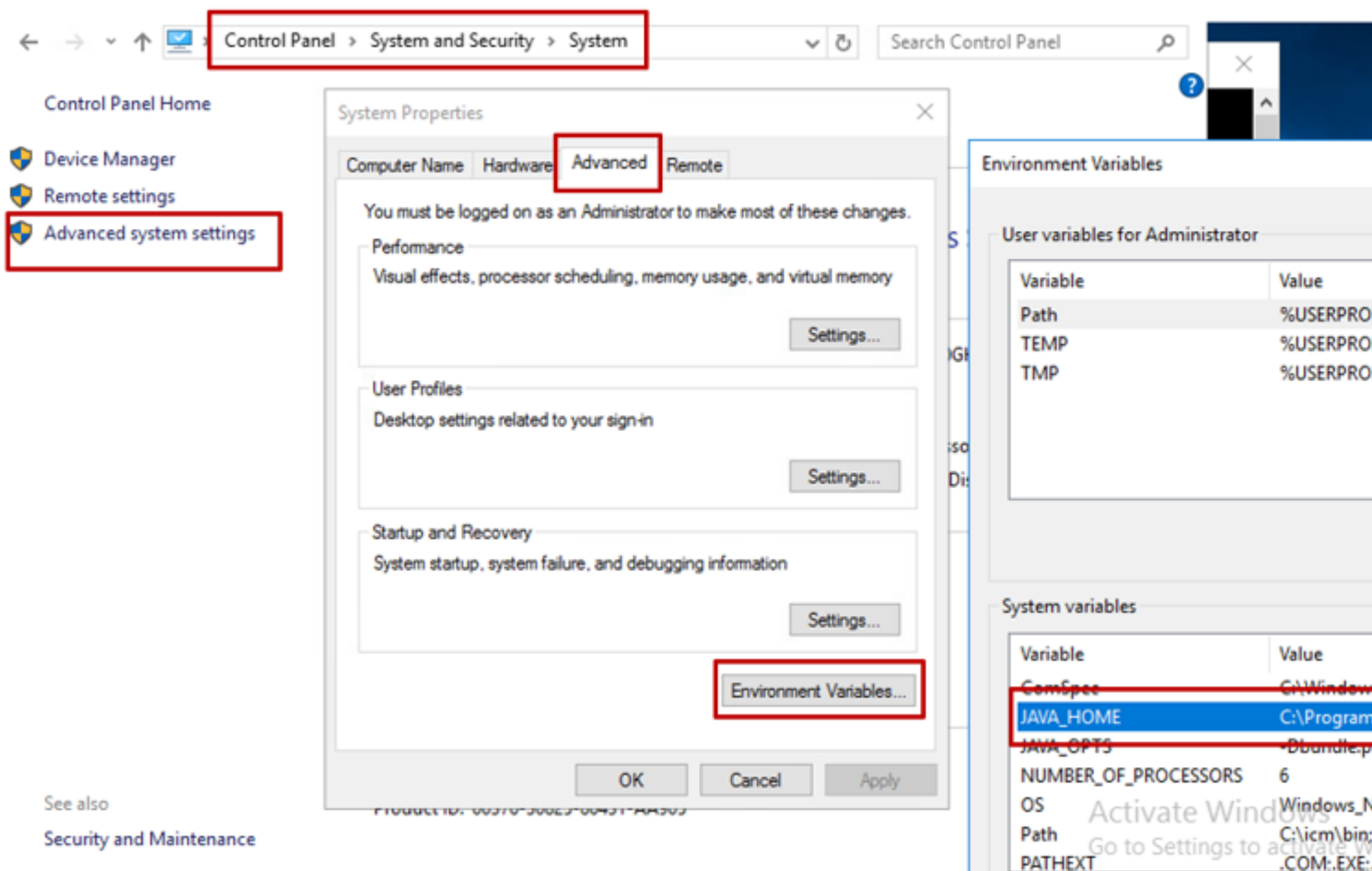
Vorsicht: Bevor Sie beginnen, müssen Sie den Schlüsselspeicher sichern und die Befehle vom Java-Home als Administrator ausführen.

Schritt 1: Kennen Sie den Java-Home-Pfad, um sicherzustellen, wo das Java-Keytool gehostet wird. Es gibt mehrere Möglichkeiten, den Java-Home-Pfad zu finden.

Option 1: CLI-Befehl: `echo %JAVA_HOME%`

```
C:\>echo %java_home%
C:\Program Files (x86)\Java\jre1.8.0_221
```

Option 2: Manuell über die erweiterte Systemeinstellung, wie im Bild dargestellt



Hinweis: Der Standardpfad für UCCE 12.5 lautet C:\Program Files (x86)\Java\jre1.8.0_221\bin. Wenn Sie jedoch das Installationsprogramm 12.5(1a) verwendet haben oder 12.5 ES55 installiert haben (obligatorisches OpenJDK ES), verwenden Sie CCE_JAVA_HOME anstelle von JAVA_HOME, da sich der Datenspeicherpfad mit OpenJDK geändert hat. Weitere Informationen zur OpenJDK-Migration in CCE und CVP finden Sie in den folgenden Dokumenten: [Install and Migrate](#)

[to OpenJDK in CCE 2.5\(1\)](#) und [Install and Migrate to OpenJDK in CVP 12.5\(1\)](#).

Schritt 2: Sichern Sie die Datei **cacerts** aus dem Ordner **C:\Program Files (x86)\Java\jre1.8.0_221\lib\security**. Sie können es an einen anderen Speicherort kopieren.

Schritt 3: Öffnen Sie ein Befehlsfenster als Administrator, um den Befehl auszuführen:

```
keytool.exe -keystore .\cacerts -import -file <path where the Root, or Intermediate certificate are st
```

Hinweis: Welche Zertifikate benötigt werden, hängt von der Zertifizierungsstelle ab, die Sie zum Signieren der Zertifikate verwenden. In einer zweistufigen Zertifizierungsstelle, die für öffentliche Zertifizierungsstellen typisch und sicherer als interne Zertifizierungsstellen ist, müssen Sie sowohl das Root- als auch das Zwischenzertifikat importieren. In einer eigenständigen Zertifizierungsstelle ohne Zwischenprodukte, die in der Regel in einer Übung oder einer einfacheren internen Zertifizierungsstelle zu finden ist, müssen Sie nur das Stammzertifikat importieren.

CVP-Lösung

1. Zertifikate mit FQDN generieren

In diesem Verfahren wird erläutert, wie Zertifikate mit FQDN für Web Service Manager (WSM)-, Voice XML (VXML)-, Anrufserver- und Operations Management (OAMP)-Dienste generiert werden.

Hinweis: Wenn Sie CVP installieren, enthält der Zertifikatsname nur den Namen des Servers und nicht den FQDN. Daher müssen Sie die Zertifikate neu generieren.

Vorsicht: Bevor Sie beginnen, müssen Sie dies tun:

1. Das Kennwort für den Schlüsselspeicher abrufen. Führen Sie den folgenden Befehl aus: `more %CVP_HOME%\conf\security.properties`. Sie benötigen dieses Kennwort, wenn Sie die Befehle `keytool` ausführen.
 2. Kopieren Sie den Ordner `%CVP_HOME%\conf\security` in einen anderen Ordner.
 3. Öffnen Sie ein Befehlsfenster als Administrator, um die Befehle auszuführen.
-

CVP-Server

Schritt 1: Führen Sie die folgenden Befehle aus, um die Zertifikate der CVP-Server zu löschen:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

Schritt 2: Führen Sie den folgenden Befehl aus, um das WSM-Zertifikat zu generieren:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

Hinweis: Standardmäßig werden die Zertifikate für zwei Jahre generiert. Verwenden Sie `-valid XXXX`, um das Ablaufdatum festzulegen, an dem Zertifikate neu generiert werden. Andernfalls sind Zertifikate 90 Tage lang gültig und müssen vor diesem Zeitpunkt von einer Zertifizierungsstelle signiert werden. Für die meisten dieser Zertifikate muss eine Validierungszeit von 3-5 Jahren angemessen sein.

Hier sind einige Standardeingaben für die Gültigkeit:

1 Jahr	365
Zwei Jahre	730
Drei Jahre	1095
Vier Jahre	1460
Fünf Jahre	1895
Zehn Jahre	3650

Achtung: Bei 12.5-Zertifikaten muss es sich um **SHA 256**, Key Size **2048** und Verschlüsselungsalgorithmus **RSA handeln**. Verwenden Sie diese Parameter, um die folgenden Werte festzulegen: `-keyalg RSA` und `-keysize 2048`. Es ist wichtig, dass die CVP-Keystore-Befehle den `-storetype`-Parameter `JCEKS` enthalten. Andernfalls kann das Zertifikat, der Schlüssel oder, schlimmer noch, der Schlüsselspeicher beschädigt werden.

Geben Sie den FQDN des Servers an, und **wie lautet Ihr Vor- und Nachname?**

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\keystore -alias -
in certificate -keysize 2048 -keyalg RSA
Enter keystore password:
What is your first and last name?
[Unknown]: cvp.bora.com
What is the name of your organizational unit?
[Unknown]:
```

Beantworten Sie die folgenden Fragen:

Wie lautet der Name Ihrer Organisationseinheit?

[Unbekannt]: <OU angeben>

Wie heißt Ihre Organisation?

[Unbekannt]: <Name der Organisation angeben>

Wie lautet der Name Ihrer Stadt oder Gemeinde?

[Unbekannt]: <Name der Stadt/des Ortes angeben>

Wie heißt Ihr Bundesland?

[Unbekannt]: <Name des Bundeslandes angeben>

Wie lautet der aus zwei Buchstaben bestehende Ländercode für diese Einheit?

[Unbekannt]: <Ländercode aus zwei Buchstaben angeben>

Geben Sie für die nächsten beiden Eingaben **yes** (Ja) an.

Schritt 3: Führen Sie für vxml_certificate und callserver_certificate die gleichen Schritte aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

CVP-Berichtsserver

Schritt 1: Führen Sie die folgenden Befehle aus, um die WSM- und Reporting Server-Zertifikate zu löschen:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -al
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -al
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

Schritt 2: Führen Sie den folgenden Befehl aus, um das WSM-Zertifikat zu generieren:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

Geben Sie den FQDN des Servers für die Abfrage an, **wie lautet Ihr Vor- und Nachname?**, und fahren Sie mit den gleichen Schritten wie bei CVP-Servern fort.

Schritt 3: Führen Sie für callserver_certificate die gleichen Schritte aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

CVP OAMP (UCCE-Bereitstellung)

Da in Version 12.x der PCCE-Lösung alle Komponenten der Lösung vom SPOG gesteuert werden und OAMP nicht installiert ist, sind diese Schritte nur für eine UCCE-Bereitstellungslösung erforderlich.

Schritt 1: Führen Sie die folgenden Befehle aus, um die WSM- und OAMP-Serverzertifikate zu löschen:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -delete -a
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

Schritt 2: Führen Sie den folgenden Befehl aus, um das WSM-Zertifikat zu generieren:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

Geben Sie den FQDN des Servers für die Abfrage an, **wie lautet Ihr Vor- und Nachname?**, und fahren Sie mit den gleichen Schritten wie bei CVP-Servern fort.

Schritt 3: Führen Sie die gleichen Schritte für oamp_certificate aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -genkeypair
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

2. CSR erstellen

Hinweis: RFC5280-kompatibler Browser erfordert, dass jedem Zertifikat ein Subject Alternative Name (SAN) hinzugefügt wird. Dies kann bei der Generierung des CSR mithilfe des Parameters -ext mit SAN erreicht werden.

Alternativer Betreffname

Mit dem Parameter -ext kann ein Benutzer auf bestimmte Durchwahlen zugreifen. Im gezeigten Beispiel

wird ein Subjekt-Alternativname (SAN) mit dem vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Servers sowie des lokalen Hosts hinzugefügt. Zusätzliche SAN-Felder können als durch Kommas getrennte Werte hinzugefügt werden.

Gültige SAN-Typen sind:

```
ip:192.168.0.1  
dns:myserver.mydomain.com  
email:name@mydomain.com
```

Beispiel: `-ext san=dns:mycvp.mydomain.com,dns:localhost`

CVP-Server

Schritt 1: Generieren Sie die Zertifikatanforderung für den Alias. Führen Sie diesen Befehl aus, und speichern Sie ihn in einer Datei (z. B. `wsm_certificate`):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

Schritt 2: Führen Sie für `vxml_certificate` und `callserver_certificate` die gleichen Schritte aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

CVP-Berichtsserver

Schritt 1: Generieren Sie die Zertifikatanforderung für den Alias. Führen Sie diesen Befehl aus, und speichern Sie ihn in einer Datei (z. B. `wsmreport_certificate`):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

Schritt 2: Führen Sie die gleichen Schritte für das `callserver_certificate`-Zertifikat aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -a
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

CVP OAMP (UCCE-Bereitstellung)

Schritt 1: Generieren Sie die Zertifikatanforderung für den Alias. Führen Sie diesen Befehl aus, und speichern Sie ihn in einer Datei (z. B. oamp_certificate):

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -a  
Ensure to replace "mycvp.mydomain.com" with your OAMP FQDN.  
Enter the keystore password when prompted.
```

Schritt 2: Führen Sie die gleichen Schritte für oamp_certificate aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -certreq -a
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein.

3. Entgegennehmen der von der Zertifizierungsstelle signierten Zertifikate

Schritt 1: Signieren Sie die Zertifikate auf einer Zertifizierungsstelle (WSM, Callserver und VXML-Server für den CVP-Server, WSM und OAMP für den CVP OAMP-Server und WSM und Callserver für den Reporting-Server).

Schritt 2: Laden Sie die Anwendungszertifikate und das Stammzertifikat von der Zertifizierungsstelle herunter.

Schritt 3: Kopieren Sie das Stammzertifikat und die von der Zertifizierungsstelle signierten Zertifikate in den Ordner %CVP_HOME%\conf\security\ jedes Servers.

4. Importieren Sie die von der Zertifizierungsstelle signierten Zertifikate

Wenden Sie diese Schritte auf alle Server der CVP-Lösung an. Nur die Zertifikate für Komponenten auf diesem Server müssen mit dem von der Zertifizierungsstelle signierten Zertifikat importiert werden.

Schritt 1: Stammzertifikat importieren Führen Sie diesen Befehl aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein. Geben Sie an der Eingabeaufforderung diesem Zertifikat vertrauen **Ja ein**.

Wenn ein Zwischenzertifikat vorhanden ist, führen Sie den folgenden Befehl aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v -trustcacerts -alias in
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein. Geben Sie an der Eingabeaufforderung diesem Zertifikat vertrauen **Ja ein**.

Schritt 2: Importieren Sie das von der Zertifizierungsstelle signierte WSM für dieses Serverzertifikat (CVP, Reporting und OAMP). Führen Sie diesen Befehl aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein. Geben Sie an der Eingabeaufforderung diesem Zertifikat vertrauen **Ja ein**.

Schritt 3: Auf den CVP-Servern und den Reporting-Servern wird das signierte Zertifikat der Callserver-CA importiert. Führen Sie diesen Befehl aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

Geben Sie auf Aufforderung das Kennwort für den Schlüsselspeicher ein. Geben Sie an der Eingabeaufforderung diesem Zertifikat vertrauen **Ja ein**.

Schritt 4: Importieren Sie auf den CVP-Servern das signierte Zertifikat des VXML-Servers für die CA. Führen Sie diesen Befehl aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

Schritt 5: Importieren Sie im CVP OAMP-Server (nur für UCCE) das OAMP-Server-CA-Signaturzertifikat. Führen Sie diesen Befehl aus:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -import -v
```

Schritt 6: Server neu starten.

Hinweis: Stellen Sie bei der UCCE-Bereitstellung sicher, dass Sie die Server (Reporting, CVP-Server usw.) in CVP OAMP mit dem FQDN hinzufügen, den Sie bei der Erstellung des CSR angegeben haben.

VOS-Server

1. CSR-Zertifikat generieren

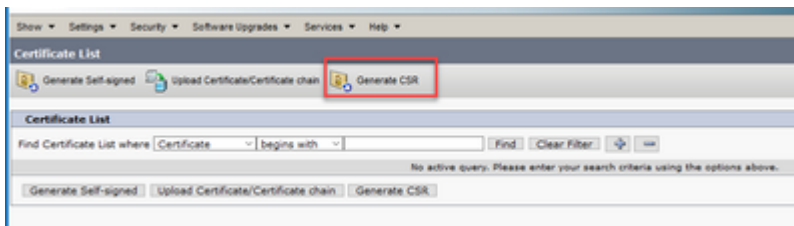
In diesem Verfahren wird erläutert, wie Sie ein Tomcat CSR-Zertifikat von einer auf dem Cisco Voice

Operating System (VOS) basierenden Plattform generieren. Dieser Prozess gilt für alle VOS-basierten Anwendungen wie:

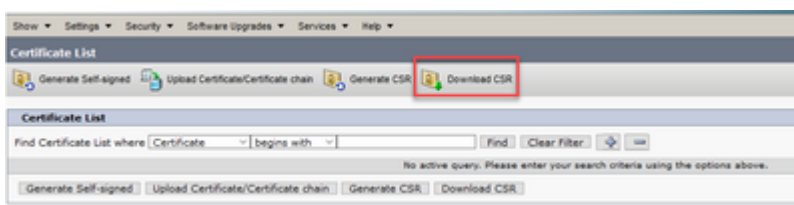
- CUCM
- Finesse
- CUIC \ Live-Daten (LD) \ Identity Server (IDS)
- Cloud Connect
- Cisco VVB

Schritt 1: Rufen Sie die Seite Cisco Unified Communications Operating System Administration (Cisco Unified Communications-Betriebssystemverwaltung) auf: <https://FQDN:<8443 oder 443>/cmplatform>.

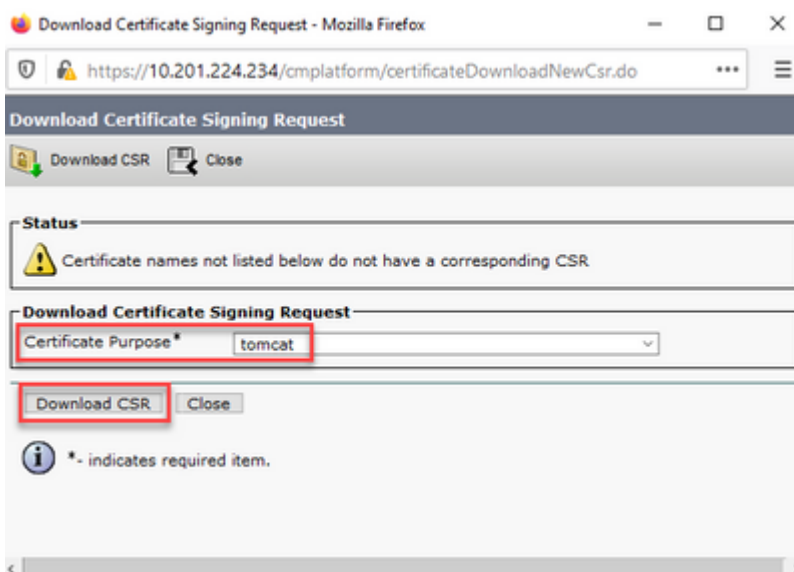
Schritt 2: Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung**, und wählen Sie **CSR generieren** aus.



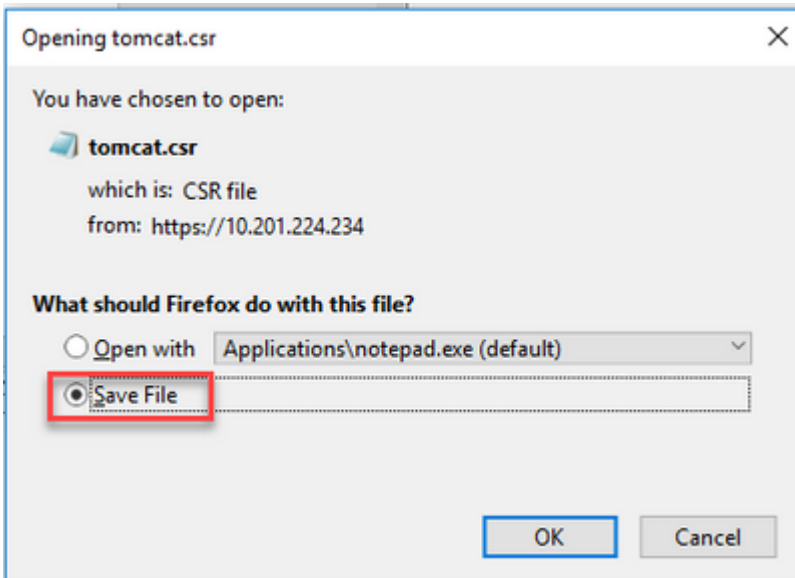
Schritt 3: Wenn das CSR-Zertifikat generiert wurde, schließen Sie das Fenster, und wählen Sie **CSR herunterladen** aus.



Schritt 4: Vergewissern Sie sich, dass das Zertifikat als Zielort festgelegt ist, und klicken Sie auf **CSR herunterladen**.



Schritt 5: Klicken Sie auf **Datei speichern**. Die Datei wird im Download-Ordner gespeichert.



2. Entgegennehmen der von der Zertifizierungsstelle signierten Zertifikate

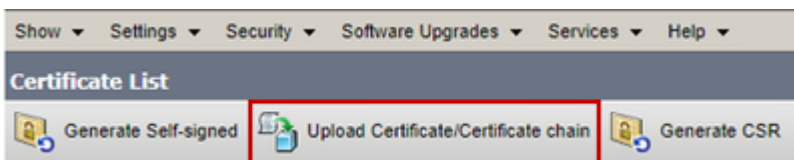
Schritt 1: Signieren Sie das auf einer Zertifizierungsstelle exportierte Tomcat-Zertifikat.

Schritt 2: Laden Sie die Anwendung und den von der Zertifizierungsstelle zertifizierten Root herunter.

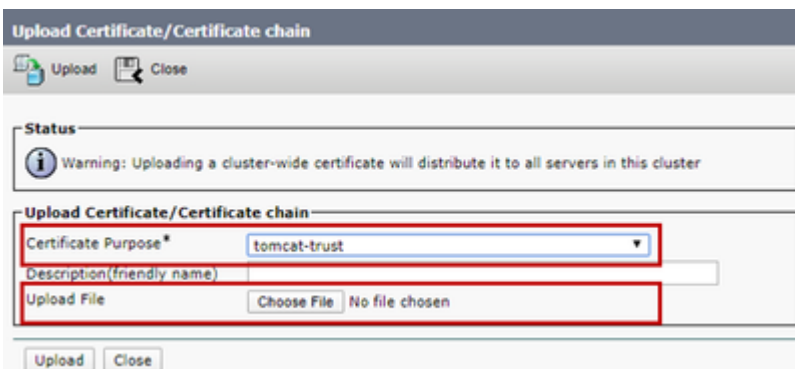
3. Laden Sie die Anwendungs- und Stammzertifikate hoch.

Schritt 1: Rufen Sie die Seite Cisco Unified Communications Operating System Administration (Cisco Unified Communications-Betriebssystemverwaltung) auf: <https://FQDN:<8443 oder 443>/cmplatform>.

Schritt 2: Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung**, und wählen Sie **Zertifikat hochladen/Zertifikatskette** aus.



Schritt 3: Wählen Sie im Fenster Zertifikat hochladen/Zertifikatskette die Option tomcat-trust in certificate purpose aus, und laden Sie das Root-Zertifikat hoch.



Schritt 4: Laden Sie ein Zwischenzertifikat (falls vorhanden) als tomcat-trust hoch.

Schritt 5: Wählen Sie im Fenster "Zertifikat hochladen/Zertifikatskette" im Feld "Zweck des Zertifikats" die Option "Kat." aus, und laden Sie das von der Anwendungszertifizierungsstelle signierte Zertifikat hoch.

The screenshot shows a dialog box titled "Upload Certificate/Certificate chain". At the top, there are "Upload" and "Close" buttons. Below is a "Status" section with a warning icon and the text: "Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster". The main section is titled "Upload Certificate/Certificate chain" and contains a "Certificate Purpose*" dropdown menu with "tomcat" selected. Below this is a "Description(friendly name)" field with the text "Self-signed certificate". There is an "Upload File" section with a "Browse..." button and the text "No file selected.". At the bottom of the dialog, the "Upload" button is highlighted with a red box, and the "Close" button is also visible. A small information icon and the text "* - indicates required item." are located at the bottom left of the dialog.

Schritt 6: Starten Sie den Server neu.

Überprüfung

Führen Sie nach dem Neustart des Servers die folgenden Schritte aus, um die von der Zertifizierungsstelle signierte Implementierung zu überprüfen:

Schritt 1: Öffnen Sie einen Webbrowser, und löschen Sie den Cache.

Schritt 2: Schließen Sie den Browser, und öffnen Sie ihn erneut.

Nun müssen Sie den Zertifikatschalter sehen, um das von der Zertifizierungsstelle signierte Zertifikat zu starten, und die Anzeige im Browserfenster, dass das Zertifikat selbst signiert und daher nicht vertrauenswürdig ist, muss verschwinden.

Fehlerbehebung

In diesem Leitfaden werden keine Schritte zur Fehlerbehebung bei der Implementierung der Zertifikate mit CA-Signatur beschrieben.

Zugehörige Informationen

- CVP-Konfigurationsleitfaden: [CVP-Konfigurationsleitfaden - Sicherheit](#)
- UCCE-Konfigurationsleitfaden: [UCCE-Konfigurationsleitfaden - Sicherheit](#)
- PCCE-Administrationshandbuch: [PCE-Administrationshandbuch - Sicherheit](#)
- UCCE-selbstsignierte Zertifikate: [Austausch von UCCE-selbstsignierten Zertifikaten](#)
- Selbstsignierte PCCE-Zertifikate: [Austausch selbstsignierter PCCE-Zertifikate](#)
- Installation und Migration auf OpenJDK in CCE 12.5(1): [CCE OpenJDK Migration](#)
- Installation und Migration auf OpenJDK in CVP 12.5(1): [CVP OpenJDK Migration](#)

[Technischer Support und Dokumentation für Cisco Systeme](#)

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.