

# Konfigurieren der sicheren Kommunikation zwischen Finesse und CTI-Server

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[CCE CTI-Server - sicher](#)

[Finesse Secure Configuration](#)

[Agenten-PG-Zertifikat generieren \(CTI-Server\)](#)

[CSR-Zertifikat von einer Zertifizierungsstelle signieren lassen](#)

[Importieren der signierten CCE PGs CA-Zertifikate](#)

[Finesse-Zertifikat generieren](#)

[Finesse-Zertifikat von einer Zertifizierungsstelle signieren](#)

[Importieren von Finesse-Anwendungen und von Root signierten Zertifikaten](#)

[Überprüfung](#)

[Fehlerbehebung](#)

## Einführung

In diesem Dokument wird beschrieben, wie Zertifikate, die von der Zertifizierungsstelle (Certificate Authority, CA) signiert wurden, zwischen Cisco Finesse und dem Computer Telephony Integration (CTI) Server in der Cisco Contact Center Enterprise (CCE)-Lösung implementiert werden.

## Voraussetzungen

### Anforderungen

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

- CCE Version 12.0(1)
- Finesse Version 12.0(1)
- CTI-Server

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Packaged CCE (PCCE) 12.0(1)

- Finesse 12.0(1)

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 potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

In der CCE-Version 11.5 hat Cisco die Unterstützung von Transport Layer Security (TLS) Version 1.2 eingeführt, mit der Session Initiation Protocol (SIP)- und Real-Time Transport Protocol (RTP)-Nachrichten sicher über TLS 1.2 übertragen werden können. Ab CCE 12.0 und als Teil der Sicherung der übertragenen Daten startete Cisco die Unterstützung von TLS 1.2 für die meisten Callflows im Contact Center: Eingangs- und Ausgangssprachübertragung, Multichannel und Dip für externe Datenbanken. Der Schwerpunkt dieses Dokuments liegt auf der eingehenden Sprachkommunikation, insbesondere der Kommunikation zwischen Finesse und CTI Server.

Der CTI-Server unterstützt die folgenden Verbindungsmodi:

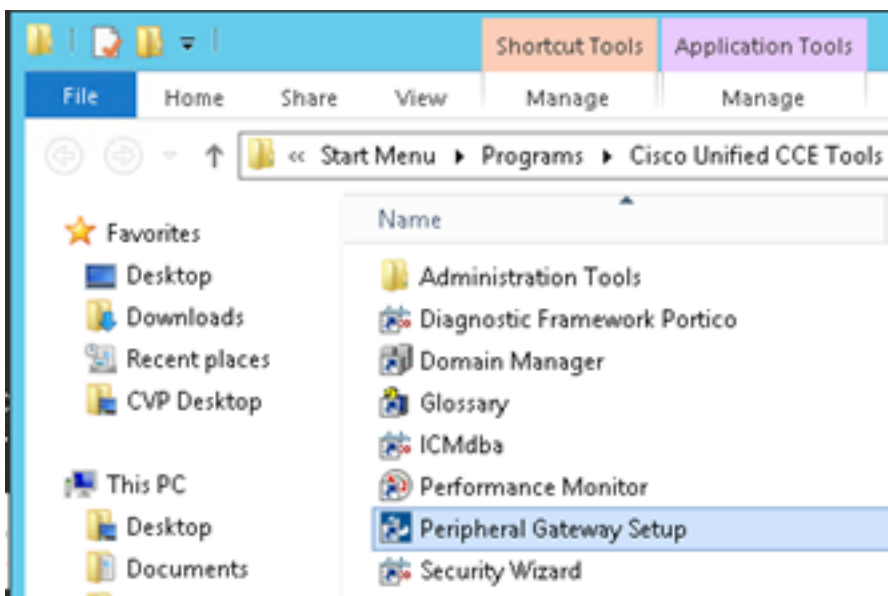
- **Sichere Verbindung:** Ermöglicht sichere Verbindungen zwischen dem CTI-Server und den CTI-Clients (Finesse, Dialer, CTIOS und ctitest).
- **Sichere und nicht gesicherte Verbindung (Mixed-Mode):** Ermöglicht gesicherte sowie nicht sichere Verbindungen zwischen dem CTI-Server und den CTI-Clients. Dies ist der Standardverbindungsmodus. Dieser Modus wird konfiguriert, wenn Sie ältere Versionen auf CCE 12.0(1) aktualisieren.

**Hinweis:** Der ungesicherte Modus wird nicht unterstützt.

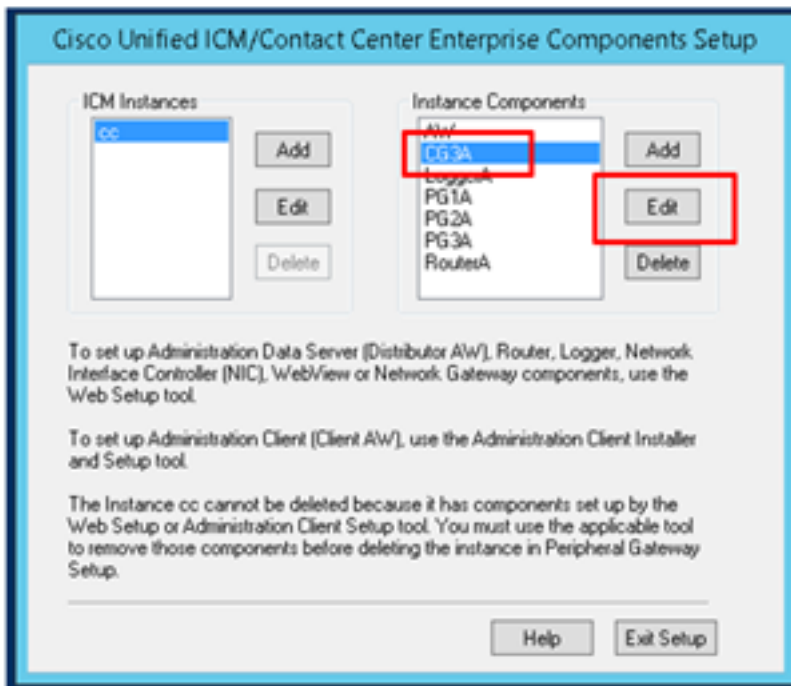
## Konfiguration

### CCE CTI-Server - sicher

Schritt 1: Öffnen Sie auf der PCCE Administrative Workstation (AW) den Ordner **Unified CCE Tools**, und doppelklicken Sie auf **Peripheral Gateway Setup**.

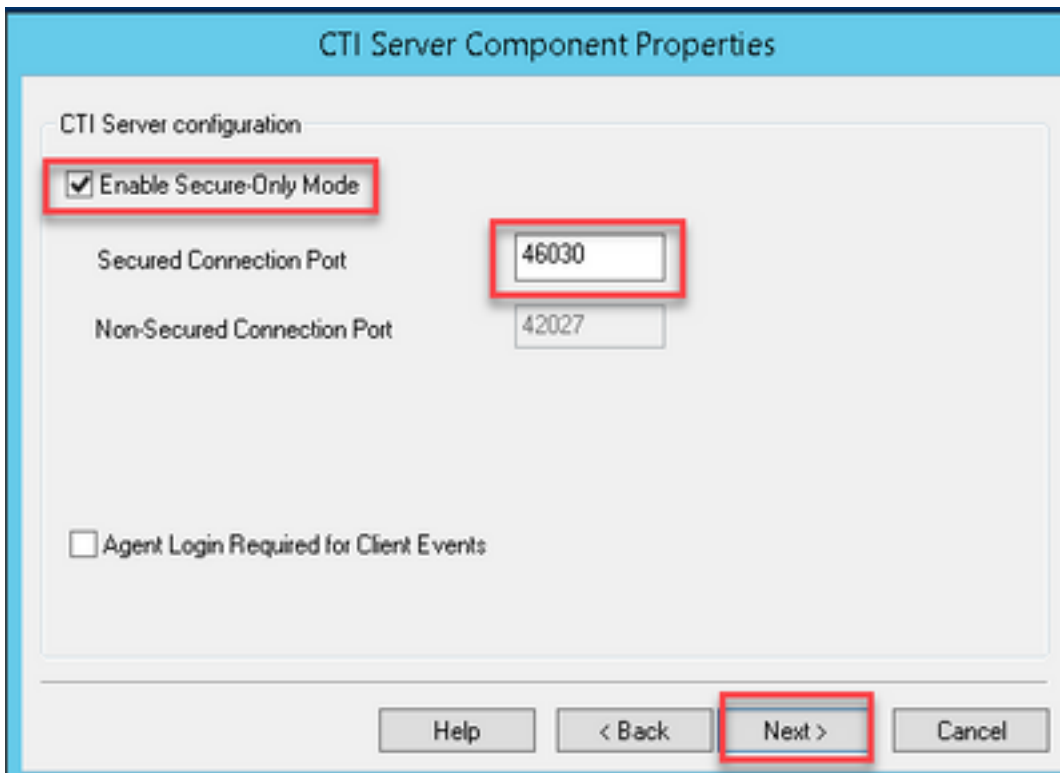


Schritt 2: Wählen Sie **CG3A** und klicken Sie auf **Bearbeiten**.



Schritt 3: Klicken Sie in den CTI-Servereigenschaften auf **Weiter**. Bei der Frage, ob der **CG3A**-Dienst durch Setup beendet werden soll, wählen Sie **Yes (Ja)** aus.

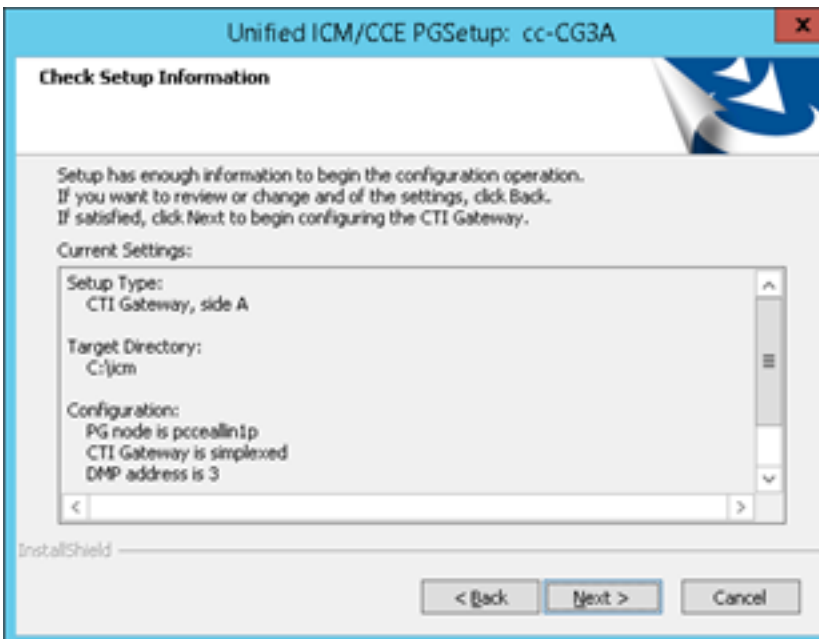
Schritt 4: Wählen Sie in den **Eigenschaften der CTI-Serverkomponenten** die Option **Sicherer Modus aktivieren** aus. Beachten Sie den **geschützten Verbindungsport (46030)**, da Sie in der nächsten Übung denselben Port in Finesse konfigurieren müssen. Klicken Sie auf **Weiter**.



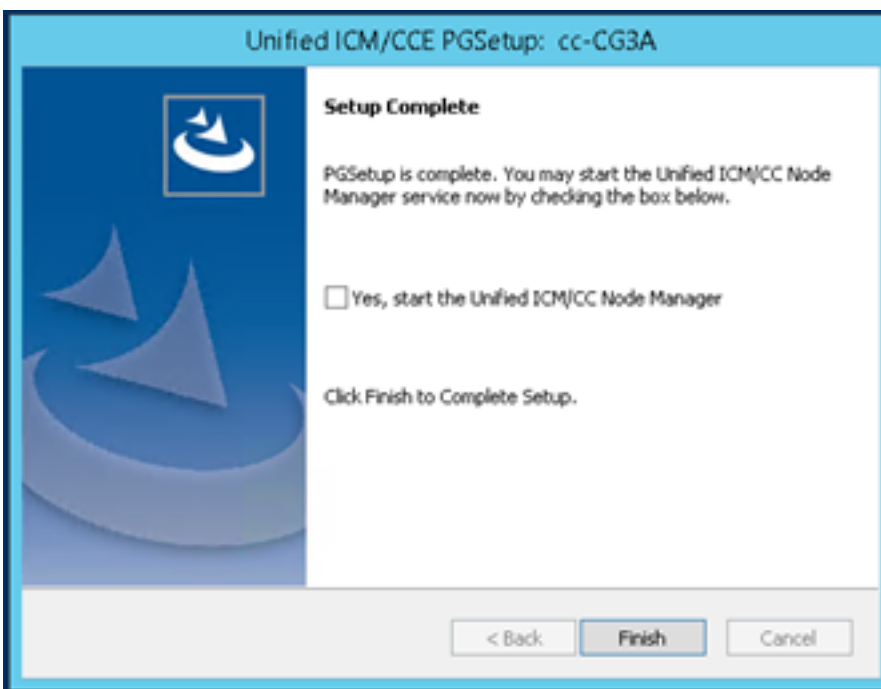
**Hinweis:** Der Standardwert für die sichere Kommunikation ist 42030. Die für dieses Dokument verwendete Übung ist 40630. Die Portnummer ist Teil einer Formel, die die ICM-System-ID enthält. Wenn die System-ID 1 (CG1a) lautet, lautet die Standardportnummer im

Allgemeinen 42030. Da die System-ID im Labor 3 (CG3a) lautet, lautet die Standard-Portnummer 46030.

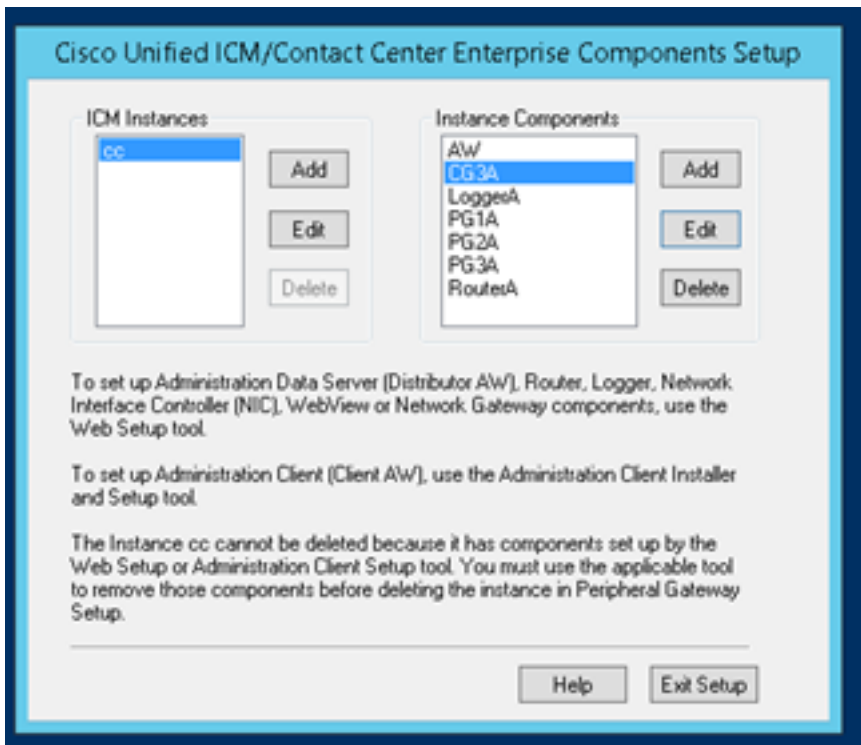
Schritt 5: Klicken Sie in den **CTI-Netzwerkschnittstelleneigenschaften** auf **Weiter**. Überprüfen Sie die **Setup-Informationen**, und klicken Sie auf **Weiter**.



Schritt 6: Klicken Sie auf **Fertig stellen** wie im Bild gezeigt.



Schritt 7: Klicken Sie auf **Setup beenden** und warten Sie, bis das Setup-Fenster wie im Bild gezeigt geschlossen wird.



Schritt 8: Doppelklicken Sie auf dem Desktop PCCEAllin1 auf **Unified CCE Service Control**.

Schritt 9: Wählen Sie Cisco ICM cc CG3A aus, und klicken Sie auf **Start**.

## Finesse Secure Configuration

Schritt 1: Öffnen Sie einen Webbrowser, und navigieren Sie zu **Finesse Administration**.

Schritt 2: Blättern Sie nach unten zum Abschnitt **Contact Center Enterprise CTI Server Settings** wie im Bild gezeigt.

Schritt 3: Ändern Sie den A-seitigen Port für den sicheren Kommunikationsport, der in der vorherigen Übung auf CG3A konfiguriert wurde: **46030**. Aktivieren Sie **SSL-Verschlüsselung aktivieren** und klicken Sie auf **Speichern**.

Contact Center Enterprise CTI Server Settings

Note: Any changes made to the settings on this gadget require a restart of Cisco Finesse Tomcat to take effect.

Contact Center Enterprise CTI Server Settings

A Side Host/IP Address\*  B Side Host/IP Address

A Side Port\*  B Side Port

Peripheral ID\*

Enable SSL encryption

**Hinweis:** Um die Verbindung zu testen, müssen Sie den Finesse Tomcat Service zuerst neu starten oder den Finesse-Server neu starten.

Schritt 4: Melden Sie sich von der Finesse Administration-Seite ab.

Schritt 5: Öffnen Sie eine SSH-Sitzung mit Finesse.

Schritt 6: Führen Sie in der FINESSEA SSH-Sitzung den folgenden Befehl aus:

**utils system restart**

Geben Sie **yes** ein, wenn Sie gefragt werden, ob Sie das System neu starten möchten.

```

Using username "administrator".
Command Line Interface is starting up, please wait ...

Welcome to the Platform Command Line Interface

VMware Installation:
 2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
 Disk 1: 146GB, Partitions aligned
 8192 Mbytes RAM

admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? yes

Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...

```

## Agenten-PG-Zertifikat generieren (CTI-Server)

CiscoCertUtils ist ein neues Tool, das auf der CCE-Version 12 veröffentlicht wurde. Sie verwenden dieses Tool, um alle CCE-Zertifikate für eingehende Sprachanrufe zu verwalten. In

diesem Dokument verwenden Sie diese CiscoCertUtils, um CSRs (Peripheral Gateways) zu generieren.

Schritt 1: Führen Sie diesen Befehl aus, um ein CSR-Zertifikat zu generieren: **CiscoCertUtil /generateCSR**

```
C:\Users\Administrator.CC>
C:\Users\Administrator.CC>CiscoCertUtil /generateCSR

Key already exists at C:\nicm\ssl\keys\host.key. It will be used to generate the
CSR.

SSL config path = C:\nicm\ssl\cfg\openssl.cfg
SYSTEM command is C:\nicm\ssl\bin\openssl.exe req -new -key C:\nicm\ssl\keys\host.
key -out C:\nicm\ssl\certs\host.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value.
If you enter '.', the field will be left blank.

-----
```

Stellen Sie die angeforderten Informationen bereit, z. B.:

Ländername: USA

Bundesland/Region Name: MA

Ortsname: BXB

Name der Organisation: Cisco

Organisationseinheit: CX

Common Name: PCCEAllin1.cc.la

E-Mail: [jdoe@cc.lab](mailto:jdoe@cc.lab)

Ein Challenge-Kennwort: Zug 1ng!

Optionaler Firmenname: Cisco

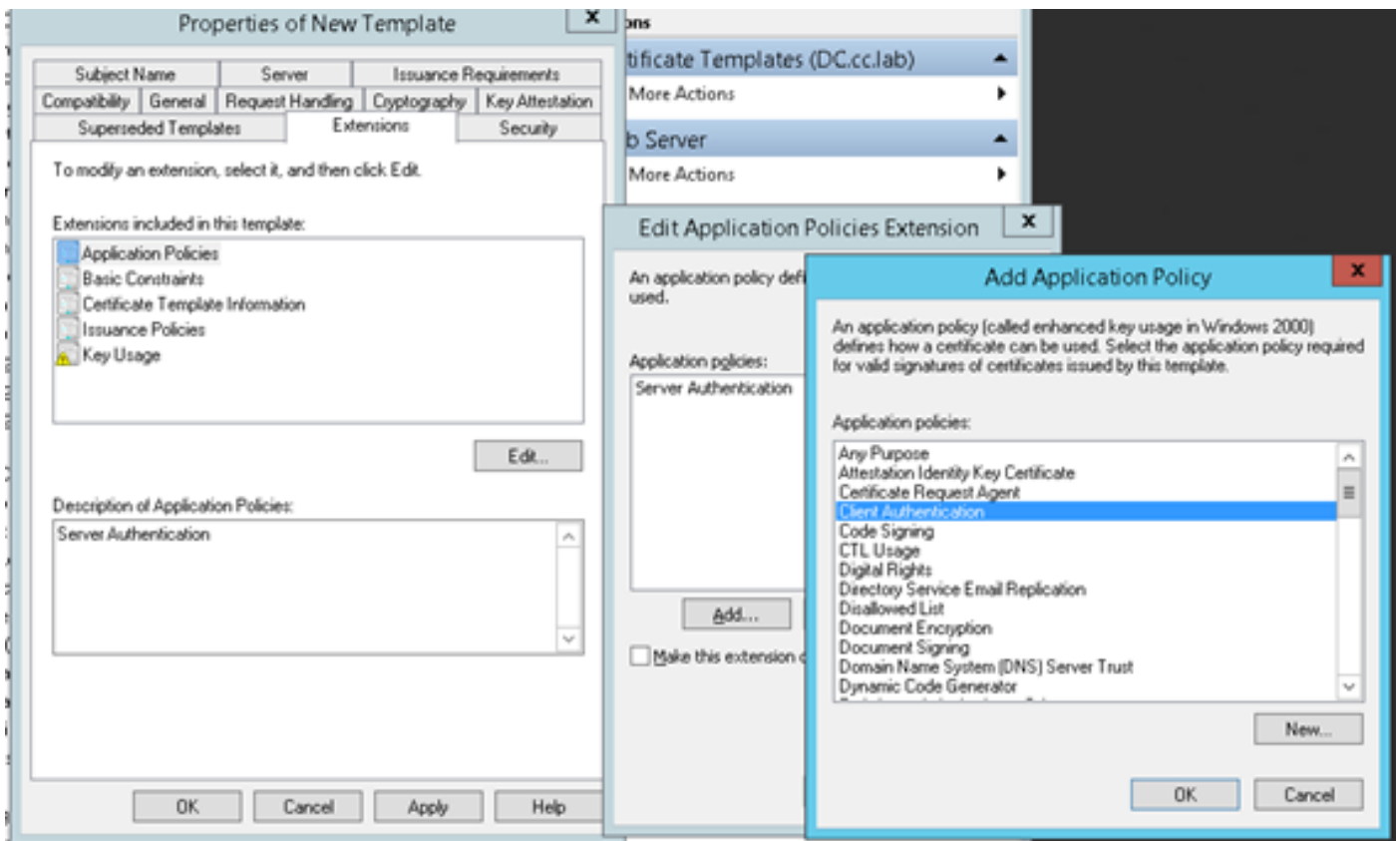
Das Hostzertifikat und der Hostschlüssel werden in **C:\nicm\ssl\certs** und **C:\nicm\ssl\keys** gespeichert.

Schritt 2: Navigieren Sie zum Ordner **C:\nicm\ssl\certs**, und stellen Sie sicher, dass die Datei **host.csr** generiert wurde.

## CSR-Zertifikat abrufen Unterzeichnet durch eine Zertifizierungsstelle

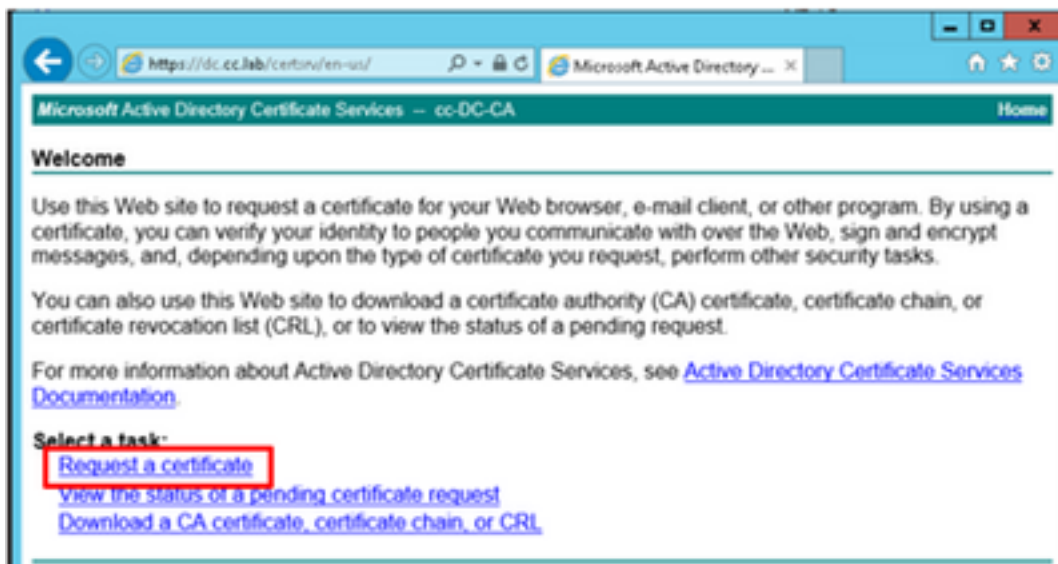
Nachdem die CSR-Zertifikate generiert wurden, müssen sie von einer Zertifizierungsstelle eines Drittanbieters signiert werden. In dieser Übung wird die im Domänencontroller installierte Microsoft CA als Drittanbieter-CA verwendet.

Stellen Sie sicher, dass die von der CA verwendete Zertifikatsvorlage die Client- und Serverauthentifizierung enthält, wie im Bild gezeigt, wenn die Microsoft CA verwendet wird.



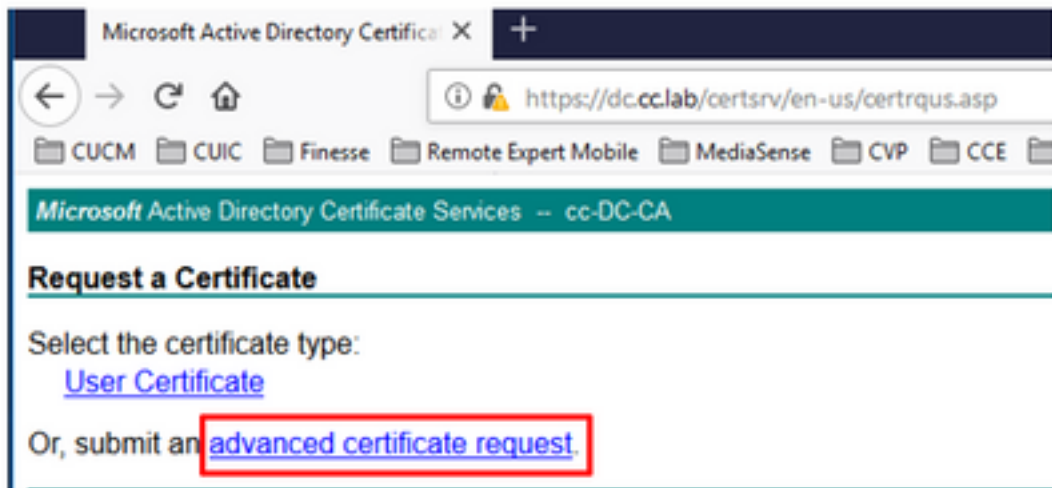
Schritt 1: Öffnen Sie einen Webbrowser, und navigieren Sie zur CA.

Schritt 2: Wählen Sie in den **Microsoft Active Directory-Zertifikatsdiensten** die Option **Zertifikat anfordern aus**.



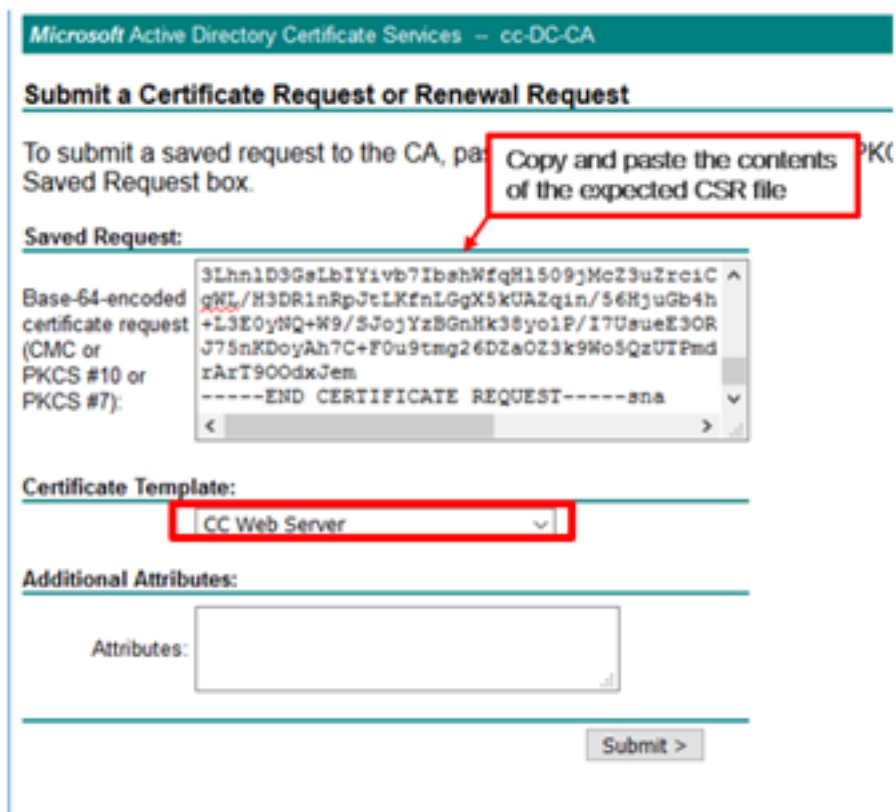
Schritt 3: Wählen Sie die Option **Erweiterte Zertifikatsanforderung** aus.





Schritt 4: Kopieren Sie auf die **erweiterte Zertifikatsanforderung** den Inhalt des PG Agent CSR-Zertifikats und fügen Sie ihn in das Feld **Gespeicherte Anforderung** ein.

Schritt 5: Wählen Sie die **Webserver**-Vorlage mit Client- und Serverauthentifizierung aus. In der Übung wurde die CC-Webserver-Vorlage mit Client- und Serverauthentifizierung erstellt.



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

Schritt 7: Wählen Sie **Base 64-verschlüsselt aus** und klicken Sie auf **Zertifikat herunterladen** wie im Bild gezeigt.

## Certificate Issued

---

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download certificate](#)

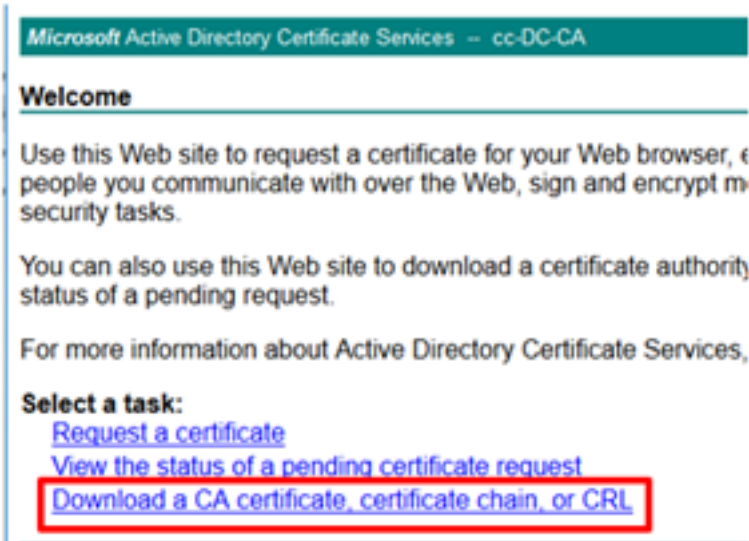
[Download certificate chain](#)

---

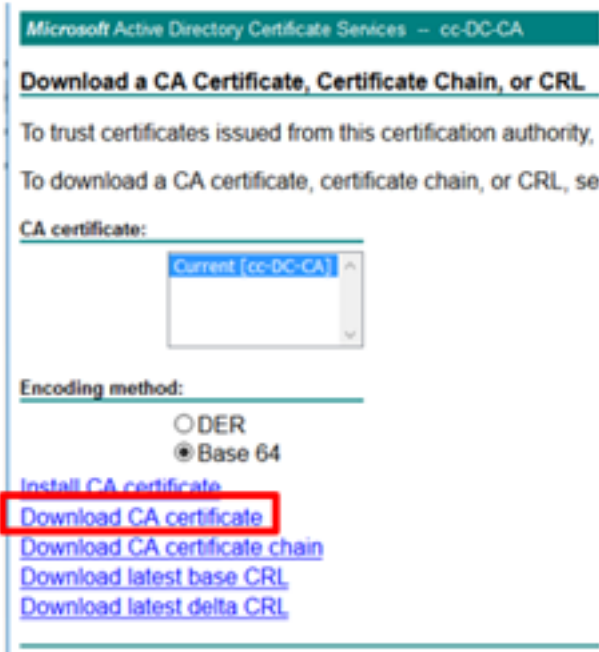
Schritt 8: Speichern Sie die Datei, und klicken Sie auf **OK**. Die Datei wird im Ordner **Downloads** gespeichert.

Schritt 9: Benennen Sie die Datei in **host.cer um** (optional).

Schritt 10: Sie müssen auch ein Stammzertifikat generieren. Rufen Sie die Zertifizierungsstellenseite des Zertifizierungsstellers auf, und wählen Sie dann **Zertifizierungsstellenkette, Zertifikatskette oder CRL herunterladen aus**. Sie müssen diesen Schritt nur einmal durchführen, da das Root-Zertifikat für alle Server (PG Agent und Finesse) gleich sein wird.

A screenshot of the Microsoft Active Directory Certificate Services website. The page has a teal header with the text "Microsoft Active Directory Certificate Services -- cc-DC-CA". Below the header is a "Welcome" section with a horizontal line. The main content area contains three paragraphs of text. The first paragraph explains the purpose of the site. The second paragraph mentions downloading a certificate authority status. The third paragraph provides more information. Below the text is a "Select a task:" section with three blue links: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL". The third link is highlighted with a red rectangular box.

Schritt 11: Klicken Sie auf **Base 64** und wählen Sie **Zertifizierungsstellenzertifikat herunterladen aus**.



Schritt 12: Klicken Sie auf "Datei speichern" und wählen Sie **OK aus**. Die Datei wird im Standardspeicherort **Downloads** gespeichert.

## Importieren der signierten CCE PGs CA-Zertifikate

Schritt 1: Navigieren Sie auf dem PG-Agenten zu **C:\icm\ssl\certs** und fügen Sie den Stamm und die PG-Agent signierten Dateien hier ein.

Schritt 2: Benennen Sie das **host.pem**-Zertifikat auf **c:\icm\ssl\certs** als **selfhost.pem** um.

Schritt 3: Umbenennen Sie **host.cer** in **host.pem** im Ordner **c:\icm\ssl\certs** .

Schritt 4: Installieren Sie das Stammzertifikat. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein: **CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer**

```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer
Install String is certutil -enterprise -addstore -f Root C:\icm\ssl\certs\rootAll.cerRoot "Trusted Root Certification Authorities"
Signature matches Public Key
Related Certificates:

Exact match:
Element 0:
Serial Number: 480a8f1b836a50b54c66a65f5298faae
Issuer: CN=cc-DC-CA, DC=cc, DC=lab
NotBefore: 2/8/2017 3:43 PM
NotAfter: 2/8/2020 3:53 PM
Subject: CN=cc-DC-CA, DC=cc, DC=lab
CA Version: 00.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): ec 49 6e f7 cb 9a c8 3a f5 46 2b ae 4f 1f 1b 15 fd 38 81 5f
Certificate "cc-DC-CA" already in store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

Schritt 5: Installieren Sie das von der Anwendung signierte Zertifikat, das denselben Befehl ausführt: **CiscoCertUtil /install C:\icm\ssl\certs\host.pem**

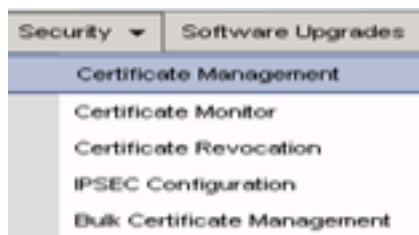
```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\nic\nssl\certs\host.pem
Install String is certutil -enterprise -addstore -f Root C:\nic\nssl\certs\host.p
enRoot "Trusted Root Certification Authorities"
Certificate "PCCALLini.cc.lab" added to store.
CertUtil: -addstore command completed successfully.
C:\Users\Administrator.CC>
```

Schritt 6: Schalten Sie den PG aus. Öffnen Sie die Unified CCE Service Control, und starten Sie den Cisco ICM Agent PG aus.

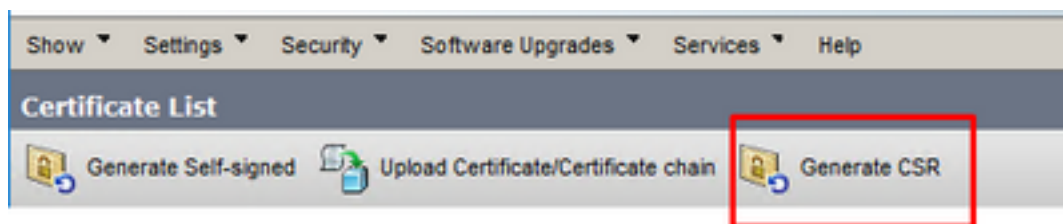
## Finesse-Zertifikat generieren

Schritt 1: Öffnen Sie den Webbrowser, und navigieren Sie zu **Finesse OS Admin**.

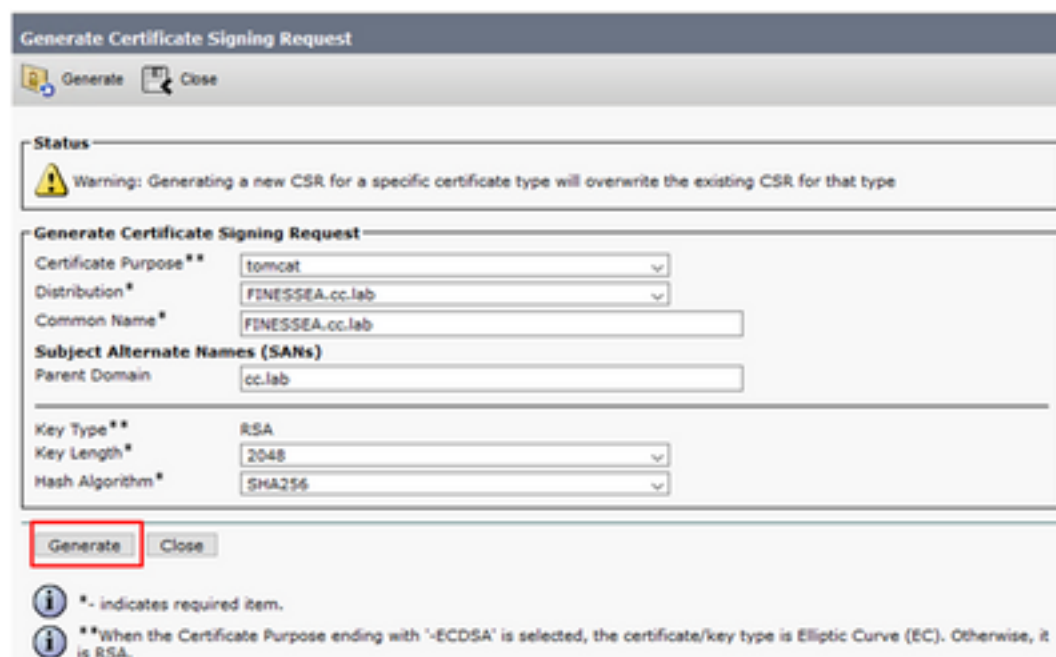
Schritt 2: Melden Sie sich mit den Anmeldeinformationen für OS Admin an, und navigieren Sie zu **Security > Certificate Management** (Verwaltung des Zertifikats), wie im Bild gezeigt.



Schritt 3: Klicken Sie auf **CSR erstellen** wie im Bild gezeigt.

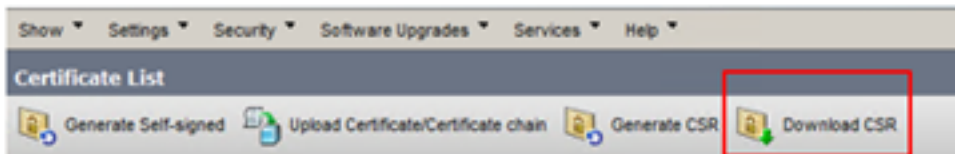


Schritt 4: Verwenden Sie auf der **Anforderung zur Signierung von Zertifikaten generieren** die Standardwerte, und klicken Sie auf **Generieren**.

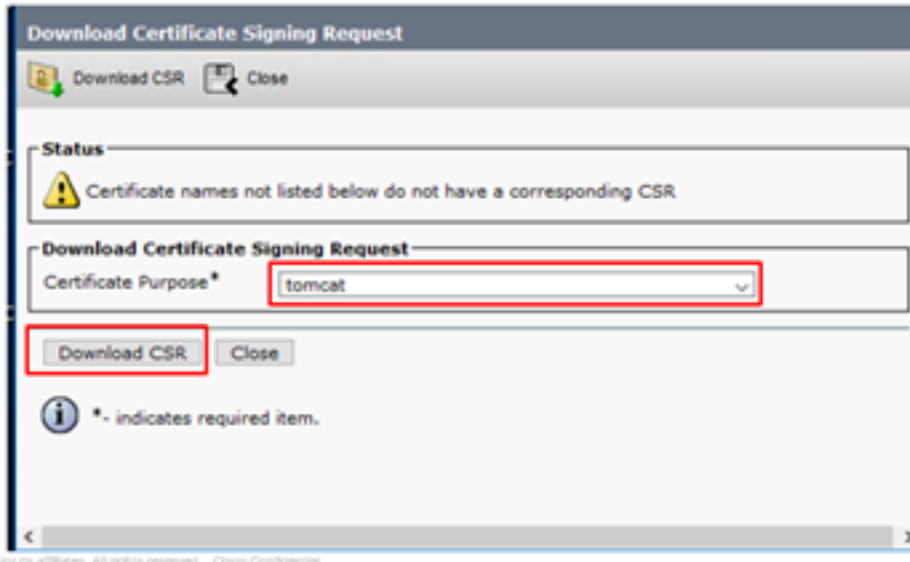
A screenshot of the 'Generate Certificate Signing Request' dialog box. The dialog has a 'Generate' button and a 'Close' button. Below the buttons is a warning message: 'Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type'. The main form contains several fields: 'Certificate Purpose\*\*' (dropdown menu with 'tomcat' selected), 'Distribution\*' (dropdown menu with 'FINESSEA.cc.lab' selected), 'Common Name\*' (text input with 'FINESSEA.cc.lab'), 'Subject Alternate Names (SANs)' section with 'Parent Domain' (text input with 'cc.lab'), 'Key Type\*\*' (dropdown menu with 'RSA' selected), 'Key Length\*' (dropdown menu with '2048' selected), and 'Hash Algorithm\*' (dropdown menu with 'SHA256' selected). At the bottom, there are 'Generate' and 'Close' buttons. A red box highlights the 'Generate' button. Below the form, there are two information icons with text: '\*- indicates required item.' and '\*\*When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.'

Schritt 5: Schließen Sie das Fenster **Signaturanforderung für Zertifikat generieren**, und wählen Sie

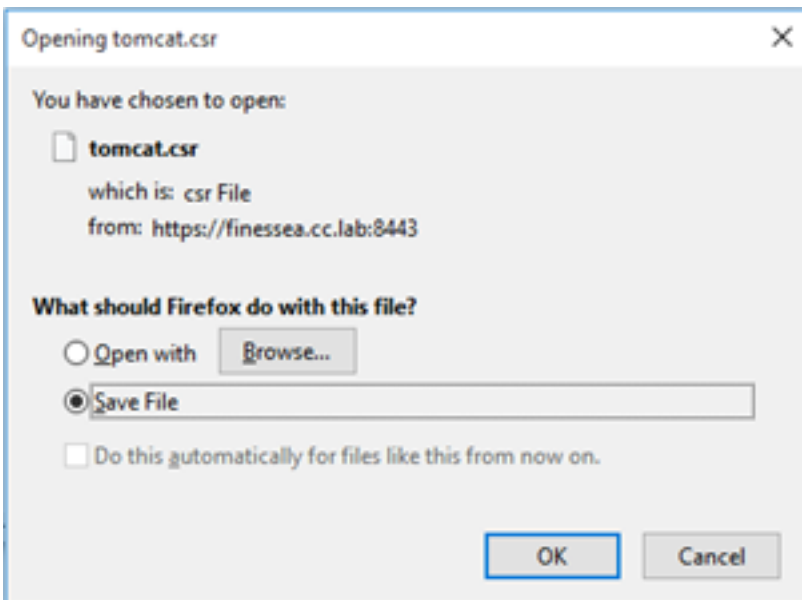
CSR herunterladen aus.



Schritt 6: Wählen Sie im Feld Zertifikatzweck die Option **tomcat** aus, und klicken Sie auf **CSR herunterladen**.



Schritt 7: Wählen Sie **Datei speichern** und klicken Sie auf **OK**, wie im Bild gezeigt.



Schritt 8: Schließen Sie das Fenster **Download Certificate Signing Request**. Das Zertifikat wird im Standardspeicherort gespeichert (**Dieser PC > Downloads**).

Schritt 9: Öffnen Sie Windows Explorer, und navigieren Sie zu diesem Ordner. Klicken Sie mit der rechten Maustaste auf dieses Zertifikat, und benennen Sie es um: **finessetomcat.csr**

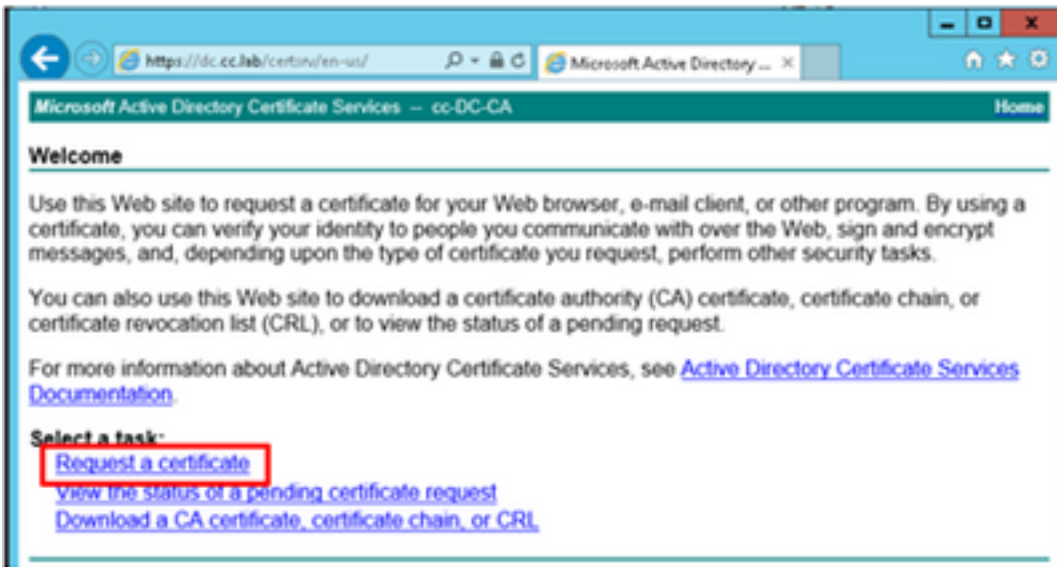
**Finesse-Zertifikat von einer Zertifizierungsstelle signieren**

In diesem Abschnitt wird dieselbe Microsoft-CA verwendet, die im vorherigen Schritt verwendet wurde, wie die Drittanbieter-CA.

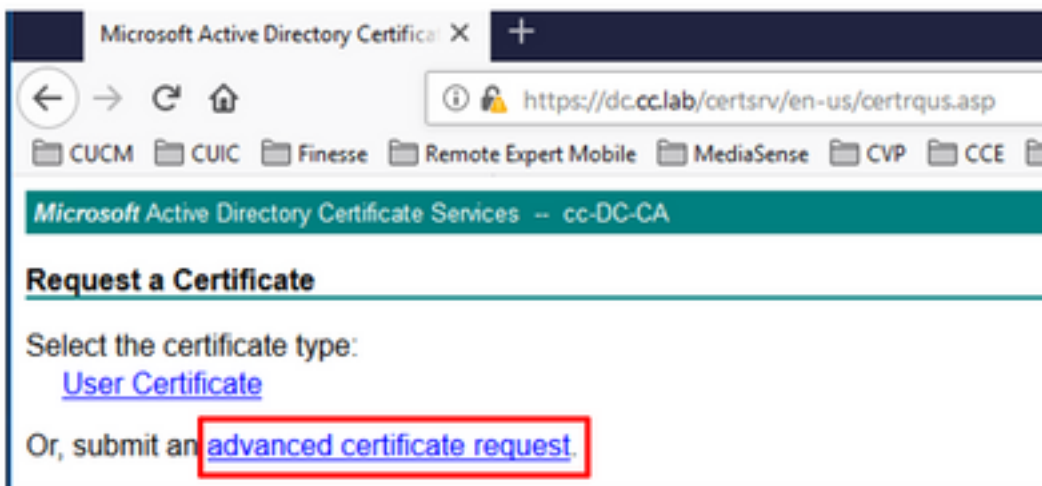
**Hinweis:** Stellen Sie sicher, dass die von der CA verwendete Zertifikatsvorlage die Client- und Serverauthentifizierung enthält.

Schritt 1: Öffnen Sie einen Webbrowser, und navigieren Sie zur CA.

Schritt 2: Wählen Sie in den **Microsoft Active Directory-Zertifikatsdiensten** die Option **Zertifikat anfordern** aus.



Schritt 3: Wählen Sie die Option **Erweiterte Zertifikatsanforderung** wie im Bild gezeigt aus.



Schritt 4: Kopieren Sie auf die **erweiterte Zertifikatsanforderung** den Inhalt des Finesse CSR-Zertifikats und fügen Sie ihn in das Feld **Gespeicherte Anforderung** ein.

Schritt 5: Wählen Sie die Webservervorlage mit Client- und Serverauthentifizierung aus. In dieser Übung wurde die CC-Webserver-Vorlage mit Client- und Serverauthentifizierung erstellt.

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste the contents of the Saved Request box. **Copy and paste the contents of the expected CSR file**

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
3Lhn1D3GgEbIY1vb7IbshWfqH1509jMcZ3uZrciC  
gKLE/H3DR1nRpJcLKfnLGgX5kUAZqin/56HjuGb4h  
+L3E0yNQ+W9/SJoJYzBGnHk38yo1P/I7UaueE3OR  
J75nKDoyAh7C+F0u9tmq26DZa0Z3k9No5QzUTPmd  
rArT900dxJem  
-----END CERTIFICATE REQUEST-----sna
```

Certificate Template:

Additional Attributes:

Attributes:

Submit >

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

Schritt 7: Wählen Sie **Base 64-verschlüsselt** aus, und klicken Sie auf **Zertifikat herunterladen**, wie im Bild gezeigt.

### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

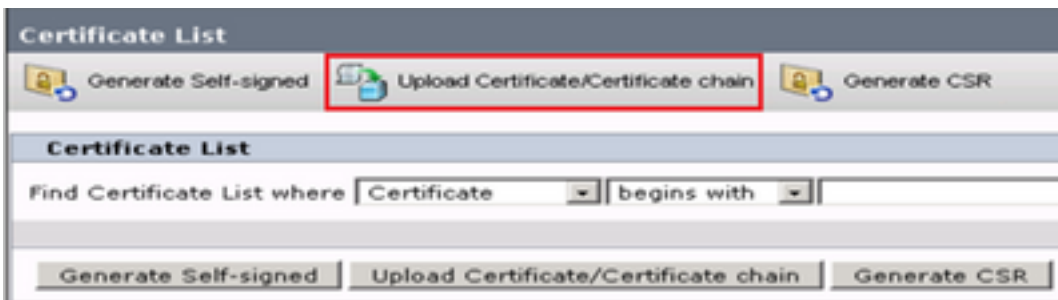
Schritt 8: Speichern Sie die Datei, und klicken Sie auf **OK**. Die Datei wird im Ordner **Downloads** gespeichert.

Schritt 9: Benennen Sie die Datei in **finesse.cer** um.

### Importieren von Finesse-Anwendungen und von Root signierten Zertifikaten

Schritt 1: Öffnen Sie auf einem Webbrowser die **Finesse OS Admin**-Seite, und navigieren Sie zu **Security > Certificate Management**.

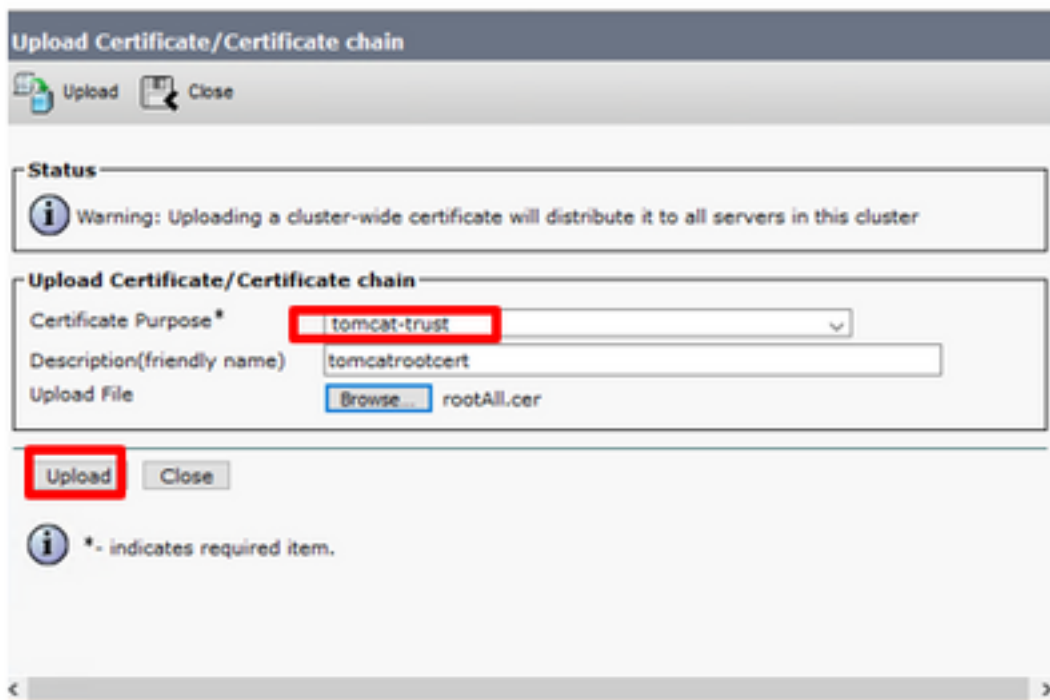
Schritt 2: Klicken Sie auf die Schaltfläche **Zertifikat/Zertifikat hochladen**, wie im Bild gezeigt.



Schritt 3: Wählen Sie im Popup-Fenster **tomcat-trust** für **Zertifikatzweck** aus.

Schritt 4: Klicken Sie auf die Schaltfläche **Durchsuchen**, und wählen Sie die zu importierende Stammzertifikatdatei aus. Klicken Sie anschließend auf die Schaltfläche **Öffnen**.

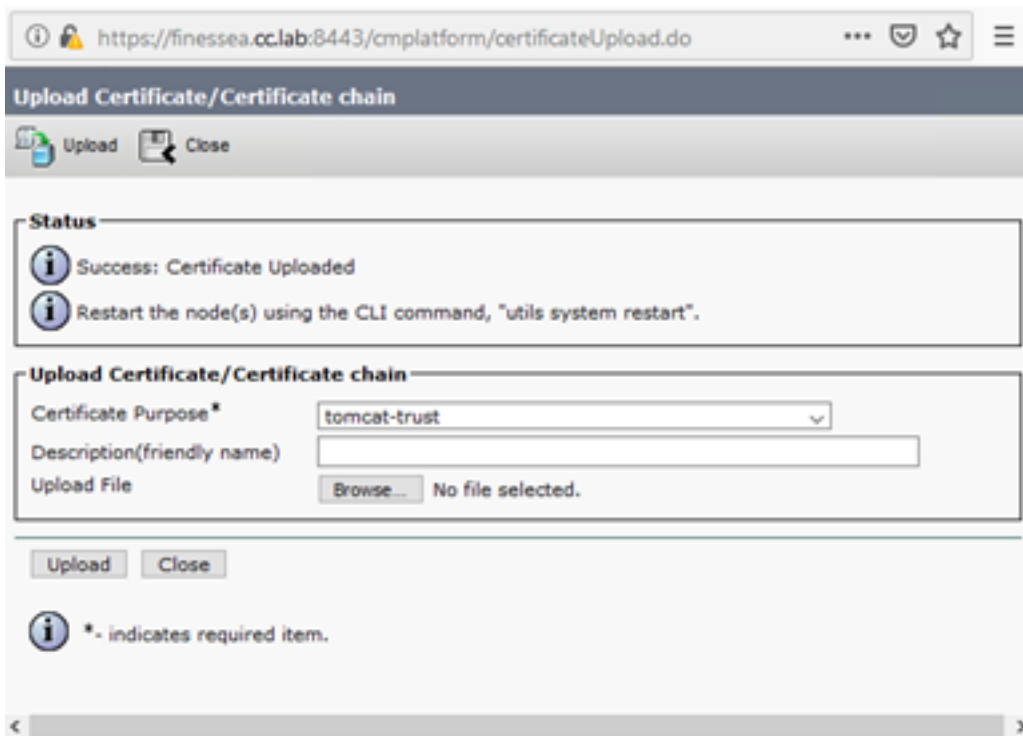
Schritt 5: In der Beschreibung schreiben Sie etwas wie **tomcatrootcert** und klicken Sie auf **Upload** Schaltfläche wie im Bild gezeigt.



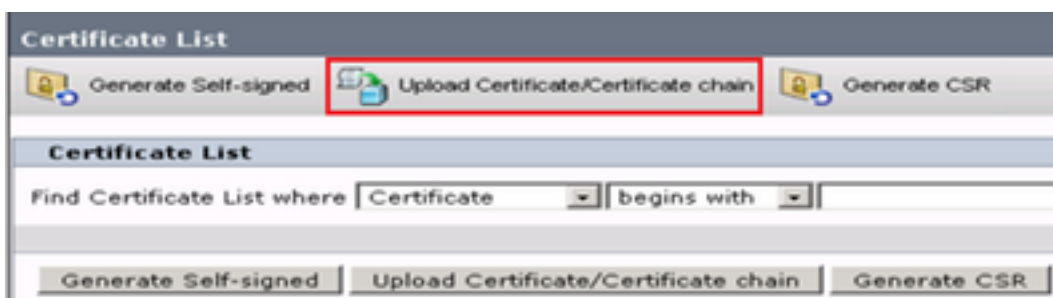
Schritt 6: Warten Sie, bis Sie den **Erfolg** sehen: Meldung **hochgeladenes Zertifikat** zum Schließen des Fensters

Sie werden gebeten, das System neu zu starten, aber fahren Sie zuerst mit dem Hochladen des Zertifikats der Finesse-Anwendung fort, und dann können Sie das System neu starten.





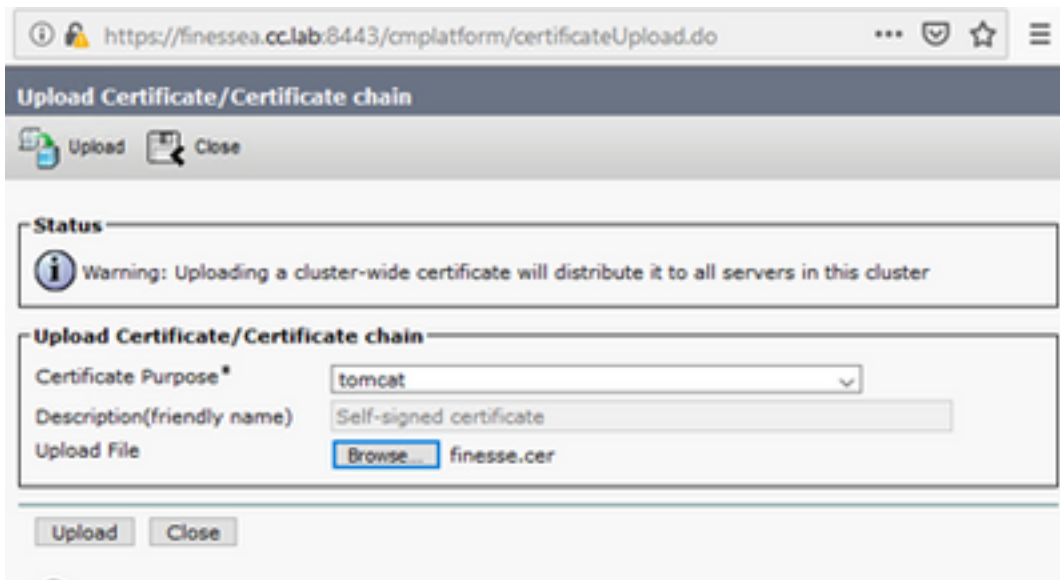
Schritt 7: Klicken Sie auf die Schaltfläche **Zertifikat/Zertifikatskette hochladen**, um das Finesse-Anwendungszertifikat zu importieren.



Schritt 8: Wählen Sie im Popup-Fenster **tomcat** für **Certificate Purpose** (Tomcat für **Zertifikatszwecke**) aus.

Schritt 9: Klicken Sie auf die Schaltfläche **Browse...** und wählen Sie die von Finesse CA signierte Datei **finesse.cer** aus. Klicken Sie anschließend auf die Schaltfläche **Öffnen**.

Schritt 10: Klicken Sie auf die Schaltfläche **Hochladen**.



Schritt 11: Warten Sie, bis Sie den **Erfolg** sehen: **Hochgeladenes Zertifikat**.

Sie werden erneut aufgefordert, das System neu zu starten. Schließen Sie das Fenster, und fahren Sie mit dem Neustart des Systems fort.

## Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Fehlerbehebung

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