# CCE-Paketlösung: Verfahren zum Abrufen und Hochladen von Zertifizierungsstellenzertifikaten von Drittanbietern

## Inhalt



## Einführung

In diesem Dokument werden die Schritte zum Erwerb und zur Installation eines Zertifikats der Zertifizierungsstelle (Certificate Authority, CA) beschrieben, das von einem Drittanbieter generiert wurde, um eine HTTPS-Verbindung zwischen Finesse und den Cisco Unified Intelligence Center (CUIC)-Servern herzustellen.

Um HTTPS für die sichere Kommunikation zwischen Finesse- und CUIC-Servern zu verwenden, müssen Sicherheitszertifikate eingerichtet werden. Standardmäßig stellen diese Server selbstsignierte Zertifikate bereit, die verwendet werden, oder Kunden können Zertifizierungsstellenzertifikate beschaffen und installieren. Diese Zertifizierungsstellenzertifikate können entweder von einem Drittanbieter wie VeriSign, Thawte oder GeoTrust erworben oder intern erstellt werden.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Package Contact Center Enterprise (PCCE)
- CUIC
- Cisco Finesse
- Zertifizierungsstellenzertifikate

### Verwendete Komponenten

Die in diesem Dokument verwendeten Informationen basieren auf der Version 11.0 (1) der PCCE-Lösung.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Schritte verstehen.

## Vorgehensweise

Führen Sie die folgenden Schritte aus, um Zertifikate für die HTTPS-Kommunikation auf Finesse- und CUIC-Servern einzurichten:

- Zertifikatsanforderung (Certificate Signing Request, CSR) erstellen und herunterladen
- Sie erhalten Root-, Intermediär- (falls zutreffend) und Anwendungszertifikat von der Zertifizierungsstelle unter Verwendung von CSR.
- Zertifikate auf die Server hochladen

### CSR erstellen und herunterladen

1. Die hier beschriebenen Schritte dienen zum Generieren und Herunterladen von CSR. Diese Schritte sind für Finesse- und CUIC-Server identisch.

2. Öffnen Sie die Seite **Cisco Unified Communications Operating System Administration** (**Cisco Unified Communications-Betriebssystemverwaltung**) mit der URL, und melden Sie sich beim Administratorkonto für das Betriebssystem an, das bei der Installation erstellt wurde.
**https://hostname des primären Servers/Plattformen**

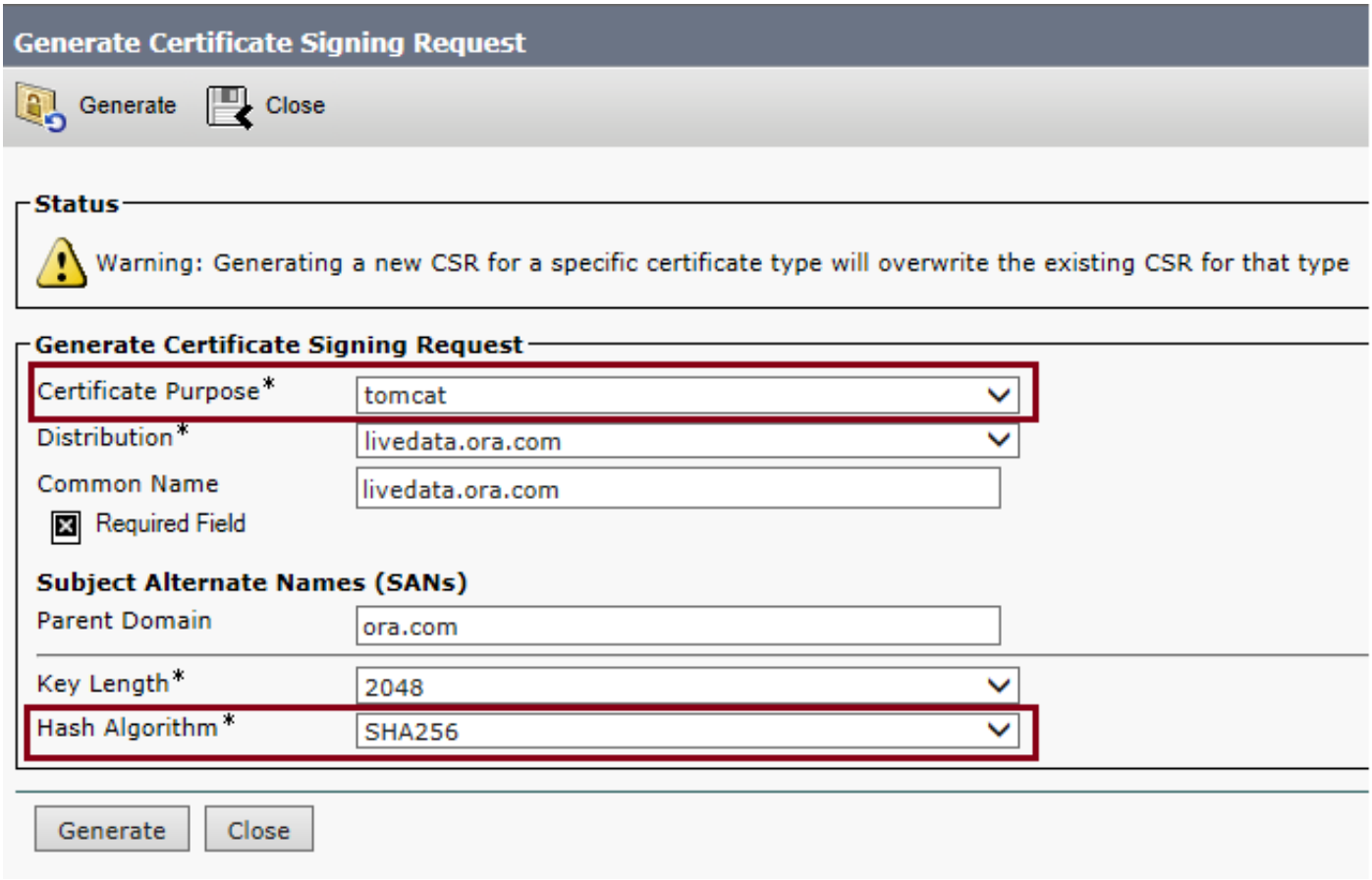
3. Erstellen einer Zertifikatssignaturanforderung.

a) Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung > CSR generieren**.

b) Wählen Sie in der Dropdownliste Zertifikatzweck* die Option **tomcat aus**.

c) Wählen Sie Hash Algorithm als **SHA256 aus**.

d) Klicken Sie auf **Generieren** wie im Bild gezeigt.

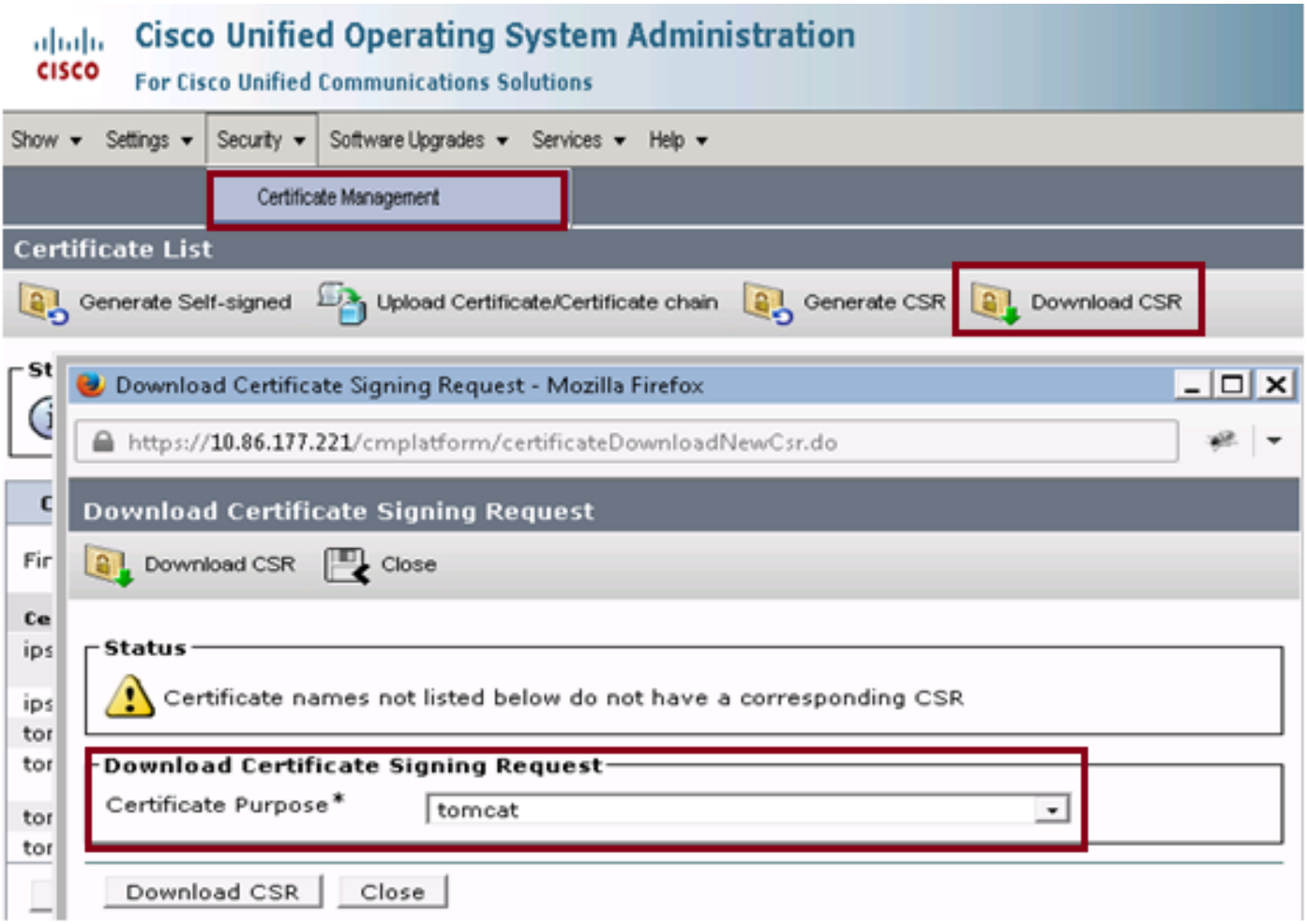



4. CSR herunterladen

a) Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung > CSR herunterladen**.

b) Wählen Sie in der Dropdownliste Zertifikatzweck* die Option **tomcat aus**.

c) Klicken Sie auf **CSR herunterladen** wie im Bild gezeigt.




**Hinweis**: Führen Sie diese Schritte auf den Sekundärservern mit der URL **https://hostname des Sekundärservers/der Compilerplattform aus**, um CSRs für CA zu erhalten.

## Zertifikat für Root, Zwischenzeit (falls zutreffend) und Anwendung von der CA abrufen

1. Stellen Sie die CSR-Informationen des primären und sekundären Servers an CAs von Drittanbietern wie VeriSign, Thawte, GeoTrust usw. bereit.

2. Von CA müssen Sie diese Zertifikatskette für die primären und sekundären Server erhalten:

- Finesse-Server: Zertifikat für Root, Zwischenstation und Anwendung
- CUIC-Server: Root- und Anwendungszertifikat

## Zertifikate auf Server hochladen

In diesem Abschnitt wird beschrieben, wie die Zertifikatskette auf Finesse- und CUIC-Servern korrekt hochgeladen wird.

### Finesse-Server

1. Primäres Finesse-Server-Stammzertifikat hochladen:

a) Navigieren Sie auf der Seite **Cisco Unified Communications Operating System Administration**

**(Verwaltung des Cisco Unified Communications-Betriebssystems) des** primären Servers zu **Security > Certificate Management > Upload Certificate (Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen)**.

b) Wählen Sie in der Dropdownliste Zertifikatzweck die Option **tomcat-trust aus**.

c) Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und durchsuchen Sie die **Stammzertifikatdatei**.

d) Klicken Sie auf **Datei hochladen**.

2. Primäres Finesse-Server-Zwischenzertifikat hochladen:

a) Wählen Sie in der Dropdownliste Zertifikatzweck die Option **tomcat-trust aus**.

b) Geben Sie im Feld Root Certificate (Stammzertifikat) den Namen des Stammzertifikats ein, das im vorherigen Schritt hochgeladen wurde. Dies ist eine **.pem**-Datei, die bei der Installation des Root-/öffentlichen Zertifikats generiert wird.

Um diese Datei anzuzeigen, navigieren Sie zu **Zertifikatsverwaltung > Suchen**. In der Zertifikatliste wird der Dateiname **.pem** mit tomcat-trust aufgeführt.

c) Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und durchsuchen Sie die **Zwischenzertifikatdatei**.

d) Klicken Sie auf **Datei hochladen**.

> **Hinweis**: Da zwischen dem primären und dem sekundären Server ein tomcat-trust store repliziert wird, muss das primäre Finesse-Server-Root- oder Zwischenzertifikat nicht auf den sekundären Finesse-Server hochgeladen werden.

3. Primäres Finesse-Serveranwendungszertifikat hochladen:

a) Wählen Sie in der Dropdownliste Zertifikatzweck die Option **tomcat aus**.

b) Geben Sie im Feld Root Certificate (Stammzertifikat) den Namen des Zwischenzertifikats ein, das im vorherigen Schritt hochgeladen wurde. Integrieren Sie die Erweiterung **.pem** (z. B. TEST-SSL-CA.pem).

c) Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und durchsuchen Sie die **Anwendungszertifikatdatei**.

d) Klicken Sie auf **Datei hochladen**.

4. Sekundäres Finesse-Server-Root- und Zwischenzertifikat hochladen:

a) Befolgen Sie die gleichen Schritte wie in den Schritten 1 und 2 für die Zertifikate des Sekundärservers.

> **Hinweis**: Da zwischen dem primären und dem sekundären Server ein tomcat-trust store repliziert wird, muss das sekundäre Finesse-Server-Root- oder Zwischenzertifikat nicht auf

den primären Finesse-Server hochgeladen werden.

5. Sekundäres Finesse-Serveranwendungszertifikat hochladen:

a) Befolgen Sie die gleichen Schritte wie in Schritt 3 beschrieben. auf dem Sekundärserver für eigene Zertifikate.

6. Server neu starten:

a) Greifen Sie auf die CLI auf den primären und sekundären Finesse-Servern zu, und führen Sie den Befehl **utils system restart aus**, um die Server neu zu starten.

### CUIC-Server

1. CUIC-Root-Zertifikat (Public Server Root) hochladen:

a) Navigieren Sie auf der Seite **Cisco Unified Communications Operating System Administration (Verwaltung des Cisco Unified Communications-Betriebssystems) des** primären Servers zu **Sicherheit > Certificate Management > Upload Certificate (Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen)**.

b) Wählen Sie in der Dropdownliste Zertifikatzweck die Option **tomcat-trust aus**.

c) Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und durchsuchen Sie die **Stammzertifikatdatei**.

d) Klicken Sie auf **Datei hochladen**.

> **Hinweis**: Da der Tomcat-Trust-Store zwischen dem primären und dem sekundären Server repliziert wird, muss das primäre CUIC-Server-Root-Zertifikat nicht auf die sekundären CUIC-Server hochgeladen werden.

2. CUIC-Zertifikat für primäre Serveranwendung (primär) hochladen:

a) Wählen Sie in der Dropdownliste Zertifikatzweck die Option **tomcat aus**.

b) Geben Sie im Feld Root Certificate (Stammzertifikat) den Namen des Stammzertifikats ein, das im vorherigen Schritt hochgeladen wurde.

Dies ist eine **.pem**-Datei, die bei der Installation des Root-/öffentlichen Zertifikats generiert wird. Um diese Datei anzuzeigen, gehen Sie zu **Zertifikatsverwaltung > Suchen**.

Der Dateiname der Zertifikatliste **.pem** wird mit tomcat-trust aufgeführt. Integrieren Sie diese .pem-Erweiterung (z. B. TEST-SSL-CA.pem).

c) Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und durchsuchen Sie die **Zertifikatsdatei der Anwendung (primär)**.

d) Klicken Sie auf **Datei hochladen**.

3. CUIC Sekundär-Server-Root-Zertifikat hochladen:

a) Befolgen Sie auf dem sekundären CUIC-Server die gleichen Schritte wie in Schritt 1 beschrieben. für das Stammzertifikat.

> **Hinweis**: Da zwischen den primären und sekundären Servern ein tomcat-trust store repliziert wird, muss das sekundäre CUIC-Server-Root-Zertifikat nicht auf den primären CUIC-Server hochgeladen werden.

4. CUIC-Zertifikat für sekundäre Serveranwendung (primär) hochladen:

a) Führen Sie den gleichen Prozess wie in Schritt 2 beschrieben aus. auf dem Sekundärserver für ein eigenes Zertifikat.

5. Server neu starten:

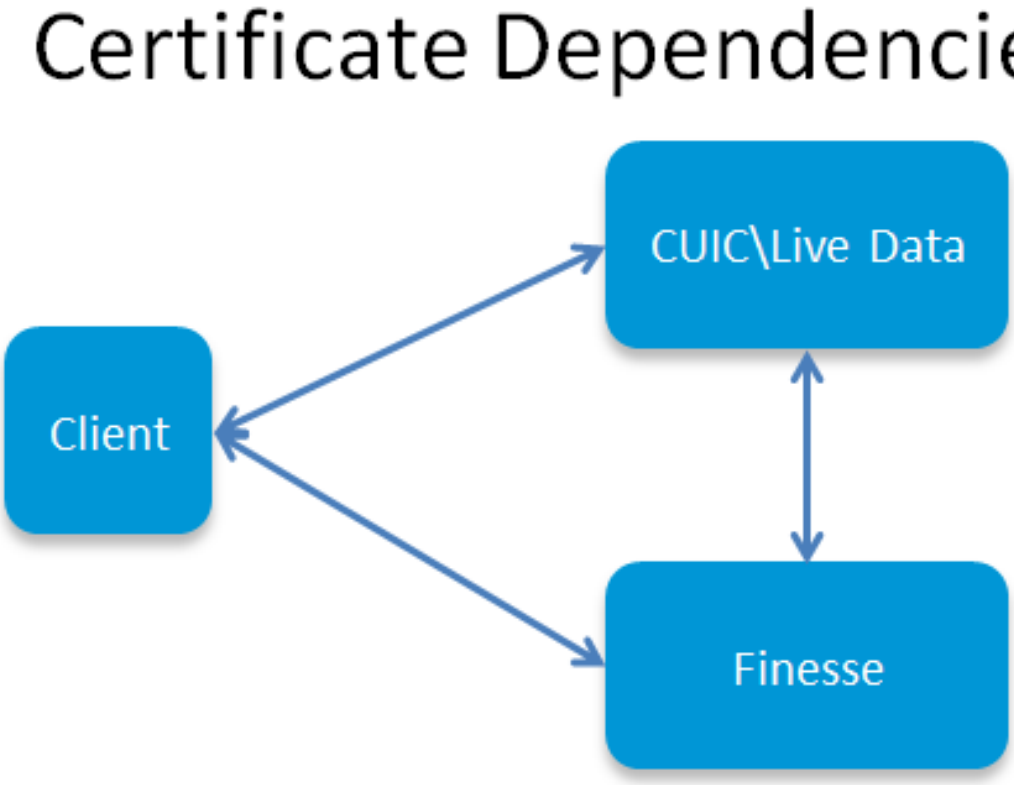
a) Greifen Sie auf die CLI auf den primären und sekundären CUIC-Servern zu, und führen Sie den Befehl **utils system restart aus**, um die Server neu zu starten.

> **Hinweis**: Um die Warnung bei Zertifikatsausnahmen zu vermeiden, müssen Sie auf die Server zugreifen, indem Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) verwenden.

## Zertifikatabhängigkeiten

Da Finesse-Agenten und -Supervisoren CUIC-Gadgets für Berichtszwecke verwenden, müssen Sie auch Root-Zertifikate dieser Server hochladen, in der hier angegebenen Reihenfolge, um Zertifikatabhängigkeiten für die HTTPS-Kommunikation zwischen diesen Servern beizubehalten, wie im Bild gezeigt.

- Hochladen des CUIC-Server-Root-Zertifikats auf dem primären Finesse-Server
- Laden Sie das Finesse Root\Intermediate-Zertifikat auf den primären CUIC-Server hoch.




**CUIC-Server-Stammzertifikat auf dem primären Finesse-Server hochladen**

1. Öffnen Sie auf dem primären Finesse-Server die Seite **Cisco Unified Communications Operating System Administration** (**Cisco Unified Communications-Betriebssystemverwaltung**) mit der URL, und melden Sie sich bei dem beim Installationsprozess erstellten Betriebssystem-Administratorkonto an:

**https://hostname des primären Finesse-Servers/-Plattformen**

2. Laden Sie das primäre CUIC-Root-Zertifikat hoch.

a) Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen**.

b) Wählen Sie in der Dropdownliste Zertifikatzweck die Option **tomcat-trust aus**.

c) Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und durchsuchen Sie die **Stammzertifikatdatei**.

d) Klicken Sie auf **Datei hochladen**.

3. Sekundäres CUIC-Root-Zertifikat hochladen.

a) Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen**.

b) Wählen Sie in der Dropdownliste Zertifikatzweck die Option **tomcat-trust aus**.

c) Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und durchsuchen Sie die **Stammzertifikatdatei**.

d) Klicken Sie auf **Datei hochladen**.

> **Hinweis**: Da der tomcat-trust store zwischen dem primären und sekundären Server repliziert wird, müssen die CUIC-Root-Zertifikate nicht auf den sekundären Finesse-Server hochgeladen werden.

4. Greifen Sie auf die CLI auf den primären und sekundären Finesse-Servern zu, und führen Sie den Befehl **utils system restart aus**, um die Server neu zu starten.

**Laden Sie das Finesse Root/Intermediate Certificate auf den CUIC Primary Server hoch.**

1. Öffnen Sie auf dem primären CUIC-Server die Seite **Cisco Unified Communications Operating System Administration (Cisco Unified Communications-Betriebssystemverwaltung) mit** der URL, und melden Sie sich beim Administratorkonto des Betriebssystems an, das zum Zeitpunkt des Installationsvorgangs erstellt wurde:

**https://hostname des primären CUIC-Servers/-Plattformen**

2. Primäres Finesse-Stammzertifikat hochladen:

a) Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen**.

b) Wählen Sie in der Dropdownliste Zertifikatzweck die Option **tomcat-trust aus**.

c) Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und durchsuchen Sie die **Stammzertifikatdatei**.

d) Klicken Sie auf **Datei hochladen**.

3. Primäres Finesse-Zwischenzertifikat hochladen:

a) Wählen Sie in der Dropdownliste Zertifikatzweck die Option **tomcat-trust aus**.

b) Geben Sie im Feld Root Certificate (Stammzertifikat) den Namen des Stammzertifikats ein, das im vorherigen Schritt hochgeladen wurde.

c) Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und durchsuchen Sie die **Zwischenzertifikatdatei**.

d) Klicken Sie auf **Datei hochladen**.

4. Führen Sie die gleichen Schritte 2 und 3 aus. für sekundäre Finesse root\Intermediate-Zertifikate auf dem primären Live-Datenserver.

> **Hinweis**: Da der tomcat-trust store zwischen den primären und sekundären Servern repliziert wird, muss das Finesse root/Intermediate-Zertifikat nicht auf die sekundären CUIC-Server hochgeladen werden.

5. Greifen Sie auf die CLI auf den primären und sekundären CUIC-Servern zu, und führen Sie den Befehl **utils system restart aus**, um die Server neu zu starten.

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.