

Unified CCE-Lösung: Verfahren zum Erhalt und Upload von Zertifizierungsstellenzertifikaten von Drittanbietern (Version 11.x)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Erstellen und Herunterladen von Zertifikatssignaturanträgen \(Certificate Signing Request, CSR\)](#)

[Schritt 2: Holen Sie Root, Intermediate \(falls zutreffend Schritt 5\) ein. und Anwendungszertifikat der Zertifizierungsstelle.](#)

[Schritt 3: Laden Sie Zertifikate auf die Server hoch.](#)

[Finesse-Server](#)

[CUIC-Server \(unter der Annahme, dass keine Zwischenzertifikate in der Zertifikatkette vorhanden sind\)](#)

[Live-Datenserver](#)

[Zertifikatabhängigkeiten für Live-Datenserver](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

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

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Live Data (LD)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Finesse
- CA-zertifiziert

Verwendete Komponenten

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

Hintergrundinformationen

Um HTTPS für die sichere Kommunikation zwischen Finesse-, CUIC- und Live Data-Servern zu verwenden, müssen Sicherheitszertifikate eingerichtet werden. Standardmäßig stellen diese Server selbstsignierte Zertifikate bereit, die verwendet werden, oder Kunden können Zertifikate erwerben und installieren, die von der Zertifizierungsstelle (Certificate Authority, CA) signiert wurden. Diese CA-Zertifikate können entweder von einem Drittanbieter wie VeriSign, Thawte oder GeoTrust bezogen werden oder intern hergestellt werden.

Konfigurieren

Das Einrichten eines Zertifikats für die HTTPS-Kommunikation in Finesse-, CUIC- und Live-Datenservern erfordert die folgenden Schritte:

1. Erstellen und Herunterladen von Zertifikatssignaturanträgen (Certificate Signing Request, CSR)
2. Holen Sie das Root-, Intermediär- (falls zutreffend) und Anwendungszertifikat von der Zertifizierungsstelle unter Verwendung von CSR ein.
3. Laden Sie Zertifikate auf die Server hoch.

Schritt 1: Erstellen und Herunterladen von Zertifikatssignaturanträgen (Certificate Signing Request, CSR)

1. Die hier beschriebenen Schritte zum Generieren und Herunterladen von CSR sind für Finesse-, CUIC- und Live-Datenserver identisch.
2. Öffnen Sie die Seite **Cisco Unified Communications Operating System Administration** (Cisco Unified Communications-Betriebssystemverwaltung) unter der angegebenen URL, und melden Sie sich mit dem Administratorkonto des Betriebssystems an, das während des Installationsprozesses erstellt wurde.
<https://FQDN:8443/cmplatform>
3. Generieren Sie die CSR-Anfrage (Certificate Signing Request), wie im Bild gezeigt:

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose* tomcat

Distribution* livedata.ora.com

Common Name livedata.ora.com

Required Field

Subject Alternate Names (SANs)

Parent Domain ora.com

Key Length* 2048

Hash Algorithm* SHA256

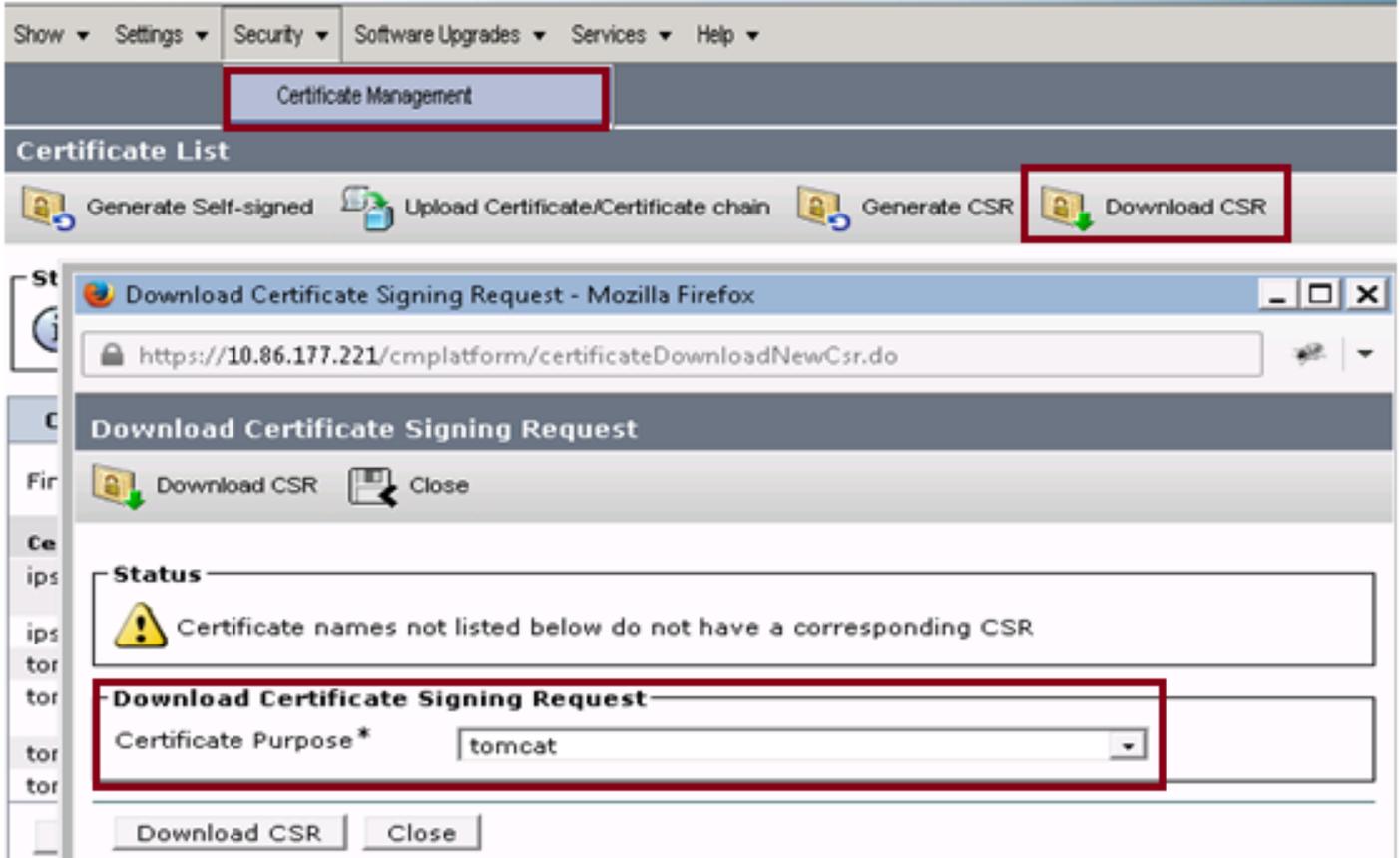
Generate Close

Schritt 1: Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung > CSR generieren**. Schritt 2: Wählen Sie in der Dropdownliste Name für Zertifikatzweck die Option tomcat aus. Schritt 3: Wählen Sie je nach Geschäftsanforderungen Hash Algorithm und Schlüssellänge aus.

- Schlüssellänge: 2048 \ Hash Algorithm: SHA256 wird empfohlen

Schritt 4: Klicken Sie auf **CSR erstellen**. **Hinweis:** Wenn für Unternehmen die Angabe des Domänennamens für das Stammdomänenfeld "Subject Alternate Names (SANs)" erforderlich ist, beachten Sie bitte die Problemadressen im Dokument ["SANs Issue with a Third Party Signed Certificate in Finesse" \(Problem mit SANs mit Signed Certificate von Drittanbietern in Finesse\)](#).

4. Laden Sie die CSR-Anfrage (Certificate Signing Request) wie im Bild gezeigt herunter:



Schritt 1: Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung > CSR herunterladen**.

Schritt 2: Wählen Sie in der Dropdownliste Zertifikatname die Option tomcat aus.

Schritt 3: Klicken Sie auf **CSR herunterladen**.

Hinweis:

Hinweis: Führen Sie die oben genannten Schritte auf den Sekundärservern durch, und verwenden Sie die URL <https://FQDN:8443/cmplatform>, um CSRs für die Zertifizierungsstelle zu erhalten.

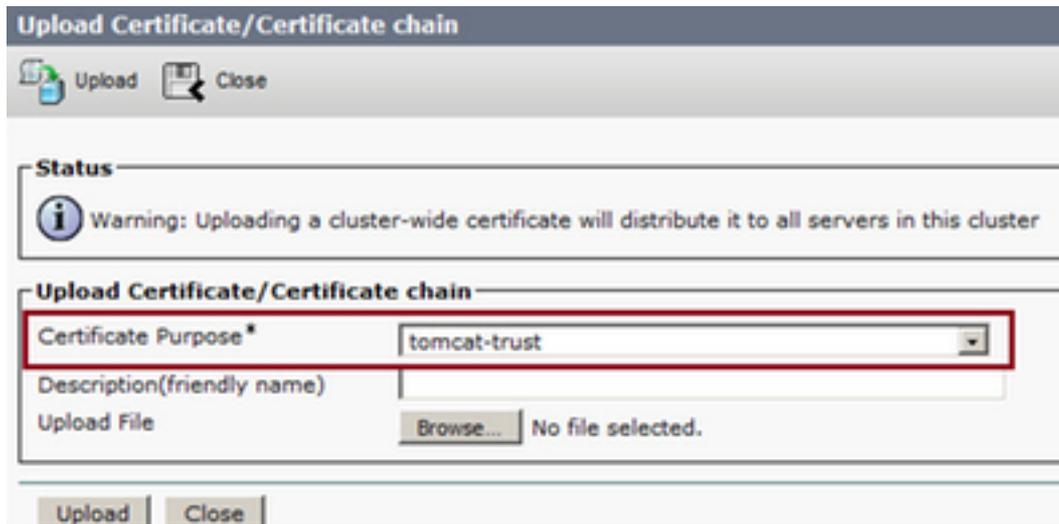
Schritt 2: Holen Sie Root, Intermediate (falls zutreffend Schritt 5) ein. und Anwendungszertifikat der Zertifizierungsstelle.

1. Stellen Sie die Informationen für die Zertifikatsanforderung (Certificate Signing Request, CSR) für den primären und sekundären Server an Zertifizierungsstellen von Drittanbietern wie VeriSign, Thawte, GeoTrust usw. bereit.
2. Von der Zertifizierungsstelle sollte man die folgende Zertifikatskette für die primären und sekundären Server erhalten.
 - Finesse-Server: Zertifikat für Root, Zwischenzeit (optional) und Anwendung
 - CUIC-Server: Zertifikat für Root, Zwischenzeit (optional) und Anwendung
 - Live-Datenserver: Zertifikat für Root, Zwischenzeit (optional) und Anwendung

Schritt 3: Laden Sie Zertifikate auf die Server hoch.

In diesem Abschnitt wird beschrieben, wie die Zertifikatskette auf Finesse-, CUIIC- und Live-Datenservern korrekt hochgeladen wird.

Finesse-Server



1. Laden Sie das Root-Zertifikat auf dem primären Finesse-Server mithilfe der folgenden Schritte hoch:

Schritt 1: Navigieren Sie auf der Seite zur Administration des Cisco Unified Communications-Betriebssystems auf dem primären Server zu **Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen**.

Schritt 2: Wählen Sie in der Dropdownliste Zertifikatname die Option tomcat-trust aus.

Schritt 3: Klicken Sie im Feld Upload File (Datei hochladen) auf Browse (Durchsuchen), und navigieren Sie zur Stammzertifikatdatei.

Schritt 4: Klicken Sie auf Datei hochladen.

2. Laden Sie das Zwischenzertifikat mithilfe der folgenden Schritte auf den primären Finesse-Server hoch:

Schritt 1: Die Schritte zum Hochladen des Zwischenzertifikats entsprechen dem Stammzertifikat in Schritt 1.

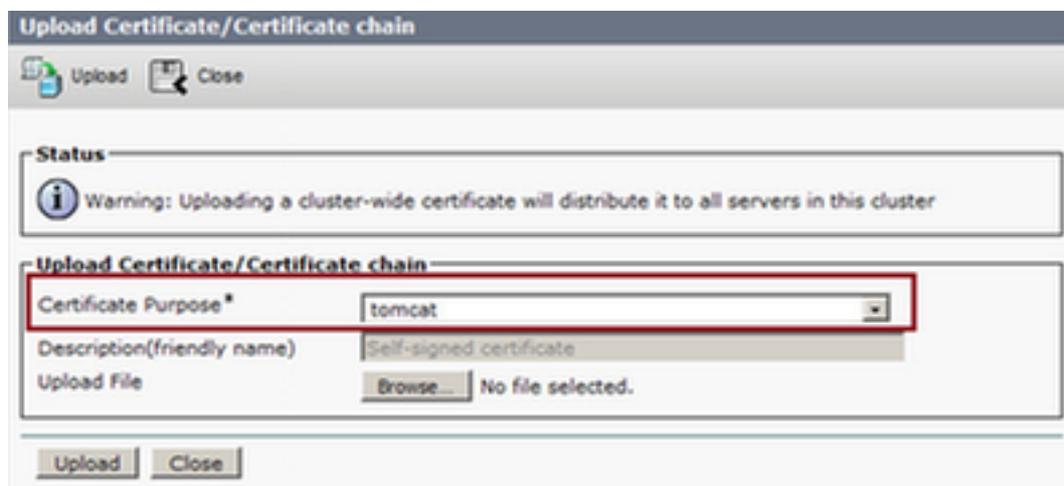
Schritt 2: Navigieren Sie auf der Seite für die Cisco Unified Communications-Betriebssystemadministration des Primärserver zu **Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen**.

Schritt 3: Wählen Sie in der Dropdownliste Zertifikatname die Option tomcat-trust aus.

Schritt 4: Klicken Sie im Feld Upload File (Datei hochladen) auf Browse (Durchsuchen), und navigieren Sie zur Zwischenzertifikatdatei.

Schritt 5: Klicken Sie auf **Hochladen**. **Hinweis:** Da Tomcat-trust Store zwischen dem primären und sekundären Server repliziert wird, muss das Root- oder Zwischenzertifikat nicht auf den sekundären Finesse-Server hochgeladen werden.

3. Laden Sie das Anwendungszertifikat des primären Finesse-Servers wie im Bild gezeigt hoch:



Schritt 1: Wählen Sie in der Dropdownliste Zertifikatname die Option tomcat aus. Schritt 2: Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und rufen Sie die Anwendungszertifikatdatei auf.
Schritt 3: Klicken Sie auf **Hochladen**, um die Datei hochzuladen.

4. Laden Sie das sekundäre finesische Serveranwendungszertifikat hoch.
In diesem Schritt führen Sie für das eigene Anwendungszertifikat auf dem Sekundärserver den gleichen Prozess wie in Schritt 3 für das eigene Anwendungszertifikat durch.
5. Jetzt können Sie die Server neu starten.
Greifen Sie auf die CLI auf den primären und sekundären Finesse-Servern zu, und geben Sie den Befehl **utils system restart** ein, um die Server neu zu starten.

CUIC-Server (unter der Annahme, dass keine Zwischenzertifikate in der Zertifikatkette vorhanden sind)

1. Root-Zertifikat auf den primären CUIC-Server hochladen.

Schritt 1: Navigieren Sie auf der Seite für die Cisco Unified Communications-Betriebssystemadministration des Primärservers zu **Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen/Zertifikatkette**.

Schritt 2: Wählen Sie in der Dropdownliste Zertifikatname die Option tomcat-trust aus.

Schritt 3: Klicken Sie im Feld Upload File (Datei hochladen) auf Browse (Durchsuchen), und navigieren Sie zur Stammzertifikatdatei.

Schritt 4: Klicken Sie auf Datei hochladen. **Hinweis:** Da der tomcat-trust store zwischen dem primären und sekundären Server repliziert wird, muss das Root-Zertifikat nicht auf den sekundären CUIC-Server hochgeladen werden.

2. Laden Sie das primäre Anwendungszertifikat des CUIC-Servers hoch.

Schritt 1: Wählen Sie in der Dropdownliste Zertifikatname die Option tomcat aus.

Schritt 2: Klicken Sie im Feld Upload File (Datei hochladen) auf Browse (Durchsuchen), und navigieren Sie zur Anwendungszertifikatdatei.

Schritt 3: Klicken Sie auf Datei hochladen.

3. Sekundäres CUIC-Serveranwendungszertifikat hochladen.

Führen Sie für das eigene Anwendungszertifikat den gleichen Prozess wie in Schritt 2 auf dem Sekundärserver durch.

4. Server neu starten

Greifen Sie auf die CLI auf den primären und sekundären CUIK-Servern zu, und geben Sie den Befehl **"utils system restart"** ein, um die Server neu zu starten.

Hinweis: Wenn die Zertifizierungsstelle die Zertifikatskette bereitstellt, die Zwischenzertifikate enthält, gelten die im Abschnitt "Finesse Servers" genannten Schritte auch für CUIK-Dienste.

Live-Datenserver

1. Die Schritte zum Hochladen der Zertifikate auf Live-Data-Servern sind je nach Zertifikatskette mit Finesse- oder CUIK-Servern identisch.

2. Laden Sie das Root-Zertifikat auf den primären Live-Datenserver hoch.

Schritt 1: Navigieren Sie auf der Seite für die Cisco Unified Communications-Betriebssystemadministration des Primärserver zu **Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen**.

Schritt 2: Wählen Sie in der Dropdownliste Zertifikatname die Option tomcat-trust aus.

Schritt 3: Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und navigieren Sie zur Stammzertifikatdatei.

Schritt 4: Klicken Sie auf **Hochladen**.

3. Zwischenzertifikat auf den primären Live-Datenserver hochladen.

Schritt 1: Die Schritte zum Hochladen des Zwischenzertifikats entsprechen dem Stammzertifikat in Schritt 1.

Schritt 2: Navigieren Sie auf der Seite für die Cisco Unified Communications-Betriebssystemadministration des Primärserver zu **Sicherheit > Zertifikatsverwaltung > Zertifikat hochladen**.

Schritt 3: Wählen Sie in der Dropdownliste Zertifikatname die Option tomcat-trust aus.

Schritt 4: Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und navigieren Sie zur Zwischenzertifikatdatei.

Schritt 5: Klicken Sie auf **Hochladen**.

Hinweis: Da Tomcat-trust Store zwischen dem primären und sekundären Server repliziert wird, muss das Root- oder Zwischenzertifikat nicht auf den sekundären Live-Datenserver hochgeladen werden.

4. Upload des primären Live-Data-Server-Anwendungszertifikats.

Schritt 1: Wählen Sie in der Dropdownliste Zertifikatname die Option tomcat aus.

Schritt 2: Klicken Sie im Feld Upload File (Datei hochladen) auf **Browse (Durchsuchen)** und rufen Sie die Anwendungszertifikatdatei auf.

Schritt 3: Klicken Sie auf **Hochladen**.

5. Laden Sie das sekundäre Anwendungszertifikat des Live-Data-Servers hoch.

Befolgen Sie die gleichen Schritte wie oben in (4) für das eigene Anwendungszertifikat auf

dem zweiten Server.

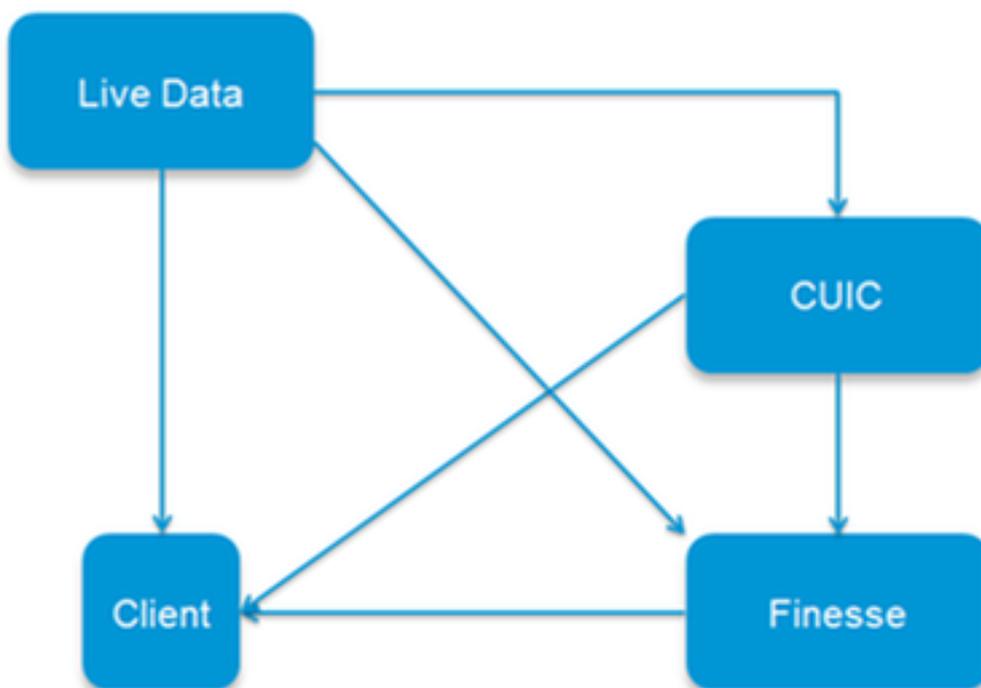
6. Server neu starten

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

Zertifikatabhängigkeiten für Live-Datenserver

Wenn Live-Datenserver mit CUIC- und Finesse-Servern interagieren, gibt es Zertifikatabhängigkeiten zwischen diesen Servern, wie im Bild gezeigt:

Certificate Dependencies



In Bezug auf die Zertifizierungsstellenkette von Drittanbietern sind die Root- und Zwischenzertifikate für alle Server in der Organisation identisch. Damit der Live-Datenserver ordnungsgemäß funktioniert, müssen Sie sicherstellen, dass die Finesse- und CUIC-Server die Root- und Zwischenzertifikate ordnungsgemäß in den Tomcat-Trust-Containern laden.

Überprüfen

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.