Laden Sie die Root-/Intermediate-Zertifikate von Expressway-Core auf CUCM hoch.

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die Stamm- und Zwischenzertifikate von Zertifizierungsstellen, die Expressway-C-Zertifikate signiert haben, in den CUCM-Publisher hochgeladen werden.

Hintergrundinformationen

Aufgrund von Verbesserungen beim Datenverkehrsserverdienst auf Expressway in X14.0.2 sendet Expressway-C sein Clientzertifikat immer dann, wenn ein Server (CUCM) es nach Diensten anfordert, die auf anderen Ports als 8443 ausgeführt werden (z. B. 6971,6972), selbst wenn CUCM sich im ungesicherten Modus befindet. Aufgrund dieser Änderung ist es erforderlich, dass die Zertifizierungsstelle für die Expressway-C-Zertifikatssignatur in CUCM sowohl als "tomcat-trust" als auch als "callmanager-trust" hinzugefügt wird.

Wenn die CA zum Signieren von Expressway-C nicht auf CUCM hochgeladen wird, schlägt die MRA-Anmeldung nach einem Upgrade von Expressways auf X14.0.2 oder höher fehl.

Damit der CUCM dem von Expressway-C gesendeten Zertifikat vertraut, müssen "tomcat-trust" und "callmanager-trust" die Stammzertifizierungsstelle und alle zwischengeschalteten Zertifizierungsstellen enthalten, die an der Signierung des Expressway-C-Zertifikats beteiligt sind.

Konfiguration

Schritt 1: Abrufen der Stamm- und Zwischenzertifikate, die das Expressway-C-Serverzertifikat signiert haben

Wenn Sie das Serverzertifikat ursprünglich von einer Zertifizierungsstelle erhalten haben, die dieses Serverzertifikat signiert hat, verfügen Sie auch über das Root- und Zwischenzertifikat für

dieses Serverzertifikat und speichern es an einem sicheren Ort. Wenn Sie diese Dateien noch haben oder erneut von Ihrer Zertifizierungsstelle herunterladen können, fahren Sie mit Schritt 2 fort, wo Sie Anweisungen zum Hochladen der Dateien auf CUCM finden.

Wenn Sie diese Dateien nicht mehr haben, können Sie sie von der Expressway-C-Webschnittstelle herunterladen. Dies ist etwas kompliziert. Es wird daher dringend empfohlen, die Zertifizierungsstelle zu kontaktieren, um den Trust Store von dieser herunterzuladen, wenn möglich.

Navigieren Sie auf dem Expressway-C zu Maintenance > Security > Server certificate, und klicken Sie auf die Schaltfläche Show (decoding) neben Server certificate. Es wird ein neues Fenster/Register mit dem Inhalt des Expressway-C-Serverzertifikats geöffnet. Sie finden dort das Feld "Issuer":

<#root>

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            55:00:00:02:21:bb:2d:41:60:55:d7:b2:27:00:01:00:00:02:21
    Signature Algorithm: sha256WithRSAEncryption


 Issuer: O=DigiCert Inc, CN=DigiCert Global CA-1

        Validity
            Not Before: Dec  8 10:36:57 2021 GMT
            Not After : Dec  8 10:36:57 2023 GMT
        Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab
        Subject Public Key Info:
...
```

In diesem Beispiel wird das Expressway-C-Serverzertifikat von einer Organisation, DigiCert Inc. mit dem gemeinsamen Namen DigiCert Global CA-1, ausgestellt.

Navigieren Sie nun zu Maintenance > Security > Trusted CA certificate, und überprüfen Sie in der Liste, ob dort ein Zertifikat mit dem gleichen Wert im Feld Subject (Betreff) vorhanden ist. In diesem Beispiel ist dies O=DigiCert Inc, CN=DigiCert Global CA-1 im Feld Betreff. Wenn Sie eine Übereinstimmung finden, bedeutet dies, dass es sich um eine zwischengeschaltete Zertifizierungsstelle handelt. Sie benötigen diese Datei und müssen weiter suchen, bis Sie die Stammzertifizierungsstelle gefunden haben.

Wenn Sie keine Übereinstimmung finden können, suchen Sie im Feld "Aussteller" nach einem Zertifikat mit diesem Wert und einem Aussteller für den Betreff der Übereinstimmung. Wenn Sie eine Übereinstimmung finden, bedeutet dies, dass es sich um die Stammdatei der Zertifizierungsstelle handelt, und dies ist die einzige Datei, die wir benötigen.

	Type	Issuer	Subject
☐	Certificate	CN=vngtp-ACTIVE-DIR-CA	Matches Issuer
☐	Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer
☐	Certificate	O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root	Matches Issuer
☐	Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	Matches Issuer
☐	Certificate	O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority	Matches Issuer
☐	Certificate	O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2	Matches Issuer
☐	Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer
☐	Certificate	O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA	Matches Issuer
☐	Certificate	O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5	Matches Issuer
☐	Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	O=DigiCert Inc, CN=DigiCert Global CA-1

Show all (decoded) | Show all (PEM file) | Delete | Select all | Unselect all

Expressway Trust Store

In diesem Beispiel stellen Sie nach dem Suchen des Zertifikats fest, dass das Feld Betreff nicht mit dem Feld Aussteller übereinstimmt. Dies bedeutet, dass es sich um ein CA-Zwischenzertifikat handelt. Sie benötigen dieses Zertifikat zusätzlich zum Stammzertifikat. Wenn der Betreff "Matches Issuer" (Aussteller von Übereinstimmungen) angegeben hat, wissen Sie, dass dies die Stammzertifizierungsstelle ist und das einzige Zertifikat ist, dem Sie vertrauen müssen.

Wenn Sie über ein Zwischenzertifikat verfügen, müssen Sie fortfahren, bis wir das Stammzertifikat gefunden haben. Schauen Sie dazu im Feld "Aussteller" nach Ihrem Zwischenzertifikat. Suchen Sie dann im Feld Betreff nach einem Zertifikat mit dem gleichen Wert. In unserem Fall ist dies O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA - Sie suchen ein Zertifikat mit diesem Wert im Feld Betreff. Wenn Sie kein passendes Zertifikat finden, suchen Sie diesen Wert im Feld "Aussteller" mit dem Betreff des Ausstellers für Übereinstimmungen.

In diesem Beispiel sehen Sie, dass unser Expressway-C-Serverzertifikat von der zwischengeschalteten CA O=DigiCert Inc, CN=DigiCert Global CA-1 signiert wurde, die von der Stamm-CA O=DigiCert Inc. OU=www.digicert.com, CN=DigiCert Global Root CA signiert wurde. Da Sie die Stammzertifizierungsstelle gefunden haben, sind Sie fertig. Wenn Sie jedoch eine andere zwischengeschaltete Zertifizierungsstelle gefunden haben, müssen Sie diesen Prozess fortsetzen, bis Sie jede zwischengeschaltete Zertifizierungsstelle und die Stamm-Zertifizierungsstelle identifiziert haben.

Um die Stamm- und Zwischenzertifikatdateien herunterzuladen, klicken Sie unter der Liste auf die Schaltfläche Alle anzeigen (PEM-Datei). Hier sehen Sie alle Stamm- und Zwischenzertifikate im PEM-Format. Blättern Sie nach unten, bis Sie ein Zertifikat finden, das mit einem Ihrer Zwischenzertifikate oder dem Stammzertifikat übereinstimmt. In diesem Beispiel ist das erste, das Sie finden, O=DigiCert Inc, CN=DigiCert Global Root CA - Sie kopieren dieses Zertifikat in eine Datei und speichern es lokal.

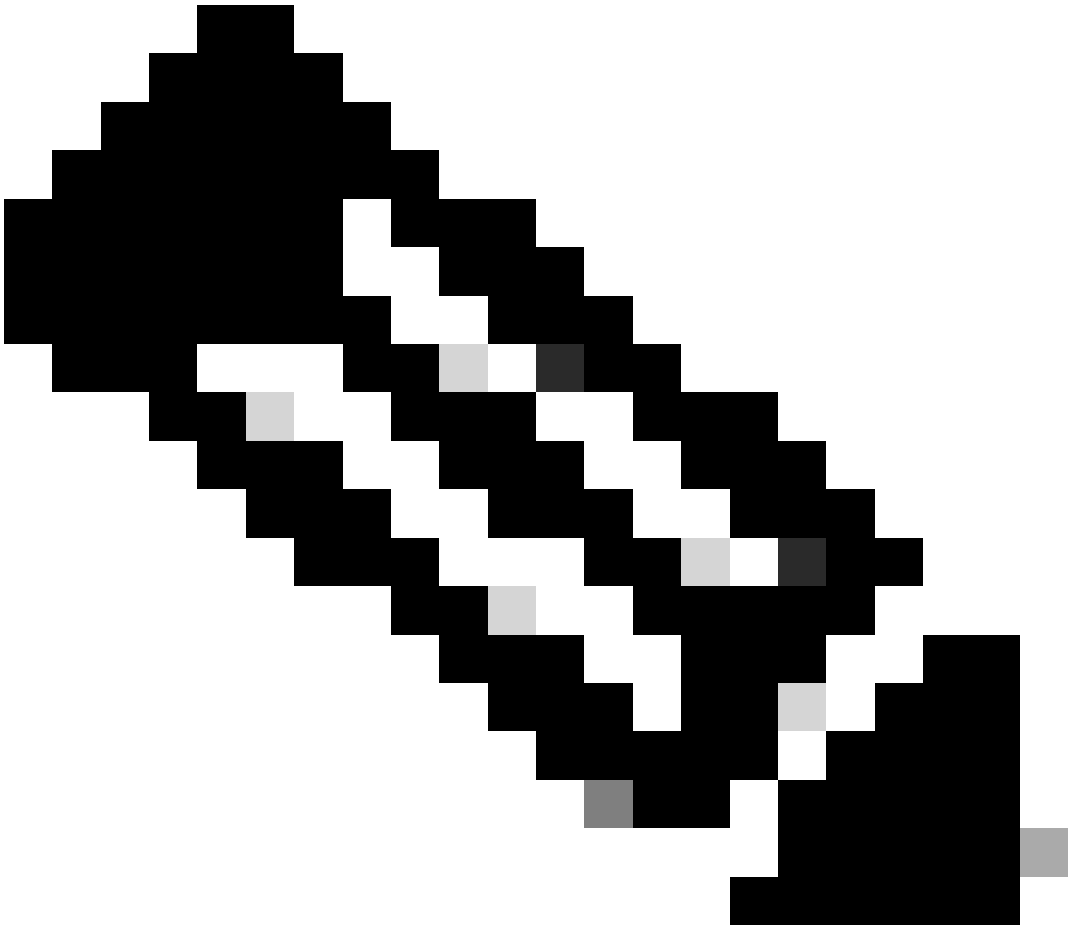
```
...
Epn3o0WC4zxe9Z2etiefC7IpJ5OCBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz
```

```
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah617jzV/OeBHRnDJELqYzmp
-----END CERTIFICATE-----

O=DigiCert Inc, CN=DigiCert Global Root CA
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----

O=The Go Daddy Group, Inc.
-----BEGIN CERTIFICATE-----
MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh
MB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE
...
```

Kopieren Sie für jedes Stamm- und eventuelle Zwischenzertifikat alles, was mit (enthalten) -----BEGIN CERTIFICATE----- beginnt und mit (enthalten) -----END CERTIFICATE----- endet. Legen Sie jeden Text in eine eigene Textdatei und fügen Sie am Ende (nach der Zeile mit -----END CERTIFICATE-----) eine zusätzliche leere Zeile hinzu. Speichern Sie diese Dateien mit der Erweiterung .pem: root.pem, intermediär1.pem, intermediär2.pem, ... Sie benötigen eine separate Datei für jedes Stamm-/Zwischenzertifikat. Im vorherigen Beispiel enthält die Datei root.pem Folgendes:

```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
```

```
TLtm8KPiGxvDl7I9OVUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I9OVUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+OtKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```

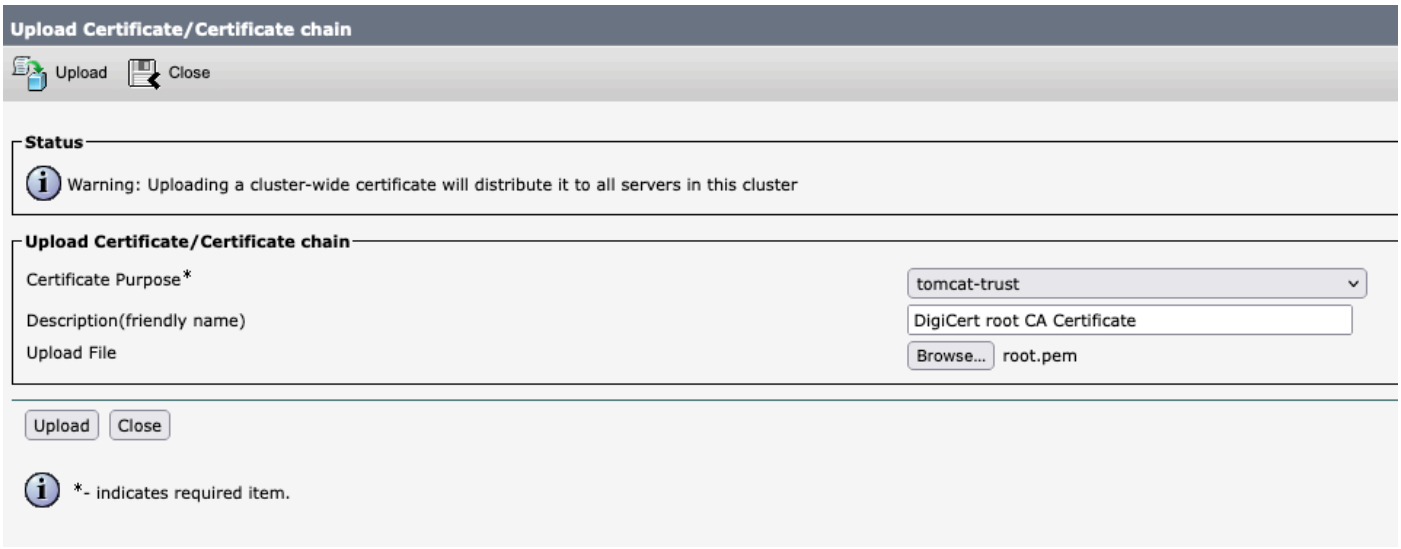


Hinweis: Unten muss eine einzige leere Zeile stehen.

Schritt 2: Laden Sie ggf. die Stamm- und Zwischenzertifikate auf den CUCM hoch.

- Melden Sie sich bei der Seite "Cisco Unified OS Administration" Ihres CUCM Publisher an.
- Navigieren Sie zu Sicherheit > Zertifikatsverwaltung.
- Klicken Sie auf die Schaltfläche Zertifikat hochladen/Zertifikatskette.
- Starten Sie im neuen Fenster, um das Stammzertifikat aus Schritt 1 hochzuladen. Laden Sie

es in tomcat-trust hoch.



- Klicken Sie auf die Schaltfläche Hochladen, und als Nächstes müssen Sie Success: Certificate Uploaded (Erfolg: Zertifikat hochgeladen) sehen. Ignorieren Sie die Meldung, dass Sie Tomcat jetzt neu starten sollen.
- Laden Sie dieselbe Stammdatei jetzt mit CallManager-trust für den Zertifikatzweck hoch.
- Wiederholen Sie die vorherigen Schritte (Hochladen in tomcat-trust und CallManager-trust) für alle Zwischenzertifikate, die auf dem Expressway-C verwendet werden.

Schritt 3: Starten Sie die erforderlichen Dienste auf CUCM neu.

Diese Dienste müssen auf jedem CUCM-Knoten in Ihrem CUCM-Cluster neu gestartet werden:

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat

Cisco CallManager und Cisco TFTP können über die Cisco Unified Serviceability-Seiten des CUCM neu gestartet werden:

- Melden Sie sich bei der Cisco Unified Service-Seite Ihres CUCM Publisher an.
- Navigieren Sie zu Extras > Control Center - Feature Services.
- Wählen Sie Ihren Publisher als Server aus.
- Wählen Sie den Cisco CallManager-Service aus, und klicken Sie auf die Schaltfläche Neu starten.
- Nachdem der Cisco CallManager-Dienst neu gestartet wurde, wählen Sie den Cisco TFTP-Dienst aus, und klicken Sie auf die Schaltfläche Neu starten.

Cisco Tomcat kann nur über die Kommandozeile neu gestartet werden:

- Öffnen Sie eine Befehlszeilenverbindung zu Ihrem CUCM Publisher.
- Verwenden Sie den Befehl utils service restart Cisco Tomcat.

Zugehörige Informationen

Technischer Support und Dokumentation - Cisco Systems

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.