Telemetrie-Broker-Identitätszertifikat ersetzen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie das Serveridentitätszertifikat auf dem Cisco Telemetry Broker (CTB) Manager-Knoten ersetzen.

Voraussetzungen

Anforderungen

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

- Administration der Cisco Telemetry Broker Appliance
- X509-Zertifikate

Verwendete Komponenten

Auf den für dieses Dokument verwendeten Appliances wird Version 2.0.1 ausgeführt.

- Cisco Telemetry Broker Manager-Knoten

- Cisco Telemetry Broker Broker-Knoten

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.

Konfigurieren

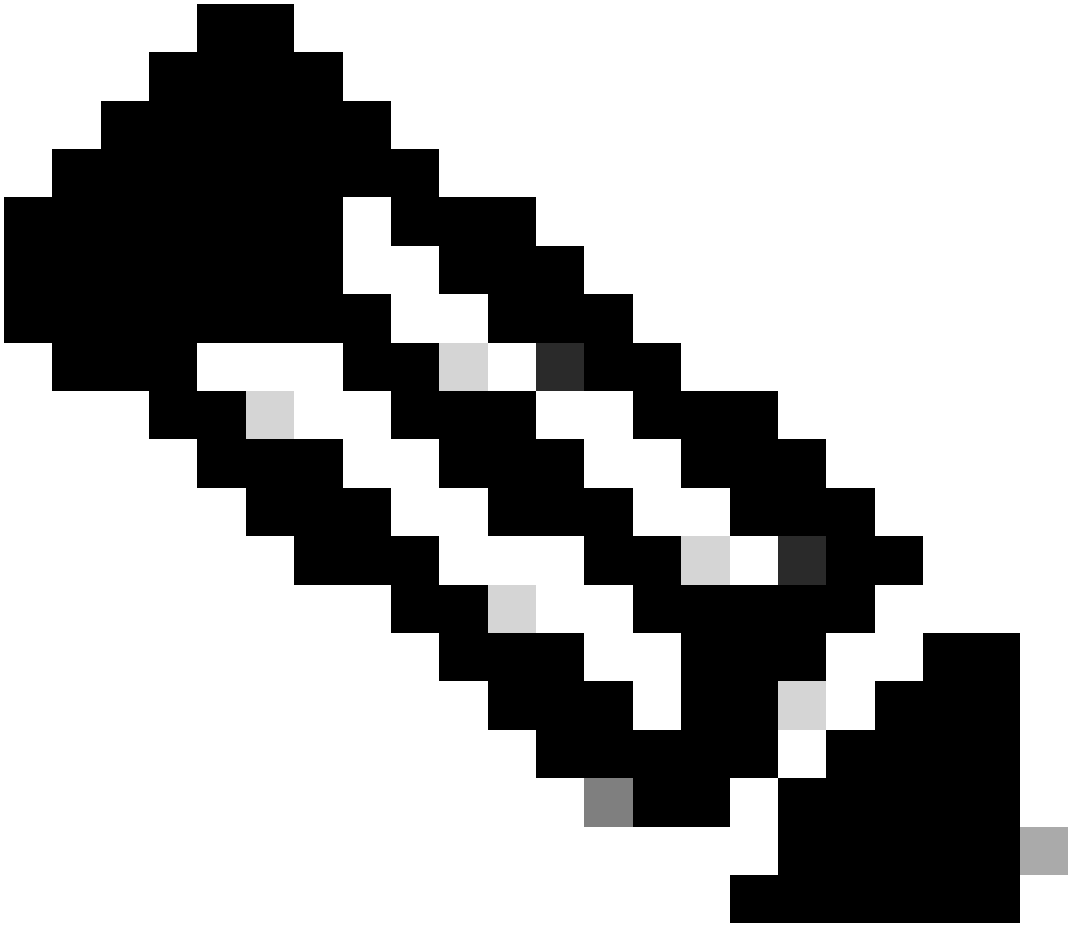
Zertifikatanforderungen

Das vom Cisco Telemetry Broker Manager verwendete x509-Zertifikat muss folgende Anforderungen erfüllen:

- Das Zertifikat und der private Schlüssel müssen übereinstimmen.
- Das Zertifikat und der private Schlüssel müssen PEM-codiert sein.
- Der private Schlüssel darf nicht durch eine Passphrase geschützt sein.

Übereinstimmendes Paar aus Zertifikat und privatem Schlüssel bestätigen

Melden Sie sich als admin-Benutzer bei der CTB Manager-Befehlszeilenschnittstelle (CLI) an.



Hinweis: Es ist möglich, dass die in diesem Abschnitt erwähnten Dateien noch nicht auf dem System vorhanden sind.

Der sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum Befehl gibt die SHA-256-Prüfsumme des öffentlichen Schlüssels aus der Zertifikatsignierungsanforderungsdatei aus.

Der sudo openssl pkey -in server_key.pem -pubout -outform pem | sha256sumBefehl gibt die SHA-256-Prüfsumme des öffentlichen Schlüssels aus der privaten Schlüsseldatei aus.

Der sudo openssl x509 -in server_cert.pem -pubkey -noout -outform pem | sha256sumBefehl gibt die SHA-256-Prüfsumme des öffentlichen Schlüssels aus der ausgegebenen Zertifikatsdatei aus.

Die Ausgabe für das Zertifikat und den privaten Schlüssel müssen übereinstimmen. Wenn keine Zertifikatsignierungsanforderung verwendet wurde, ist die Datei server_cert.pem nicht vorhanden.

```
admin@ctb-manager:~$ sudo openssl req -in server.csr -pubkey -noout -outform pem | sha256sum 3e8e6b0d39
```

Bestätigen, dass der private Schlüssel nicht durch eine Passphrase geschützt ist

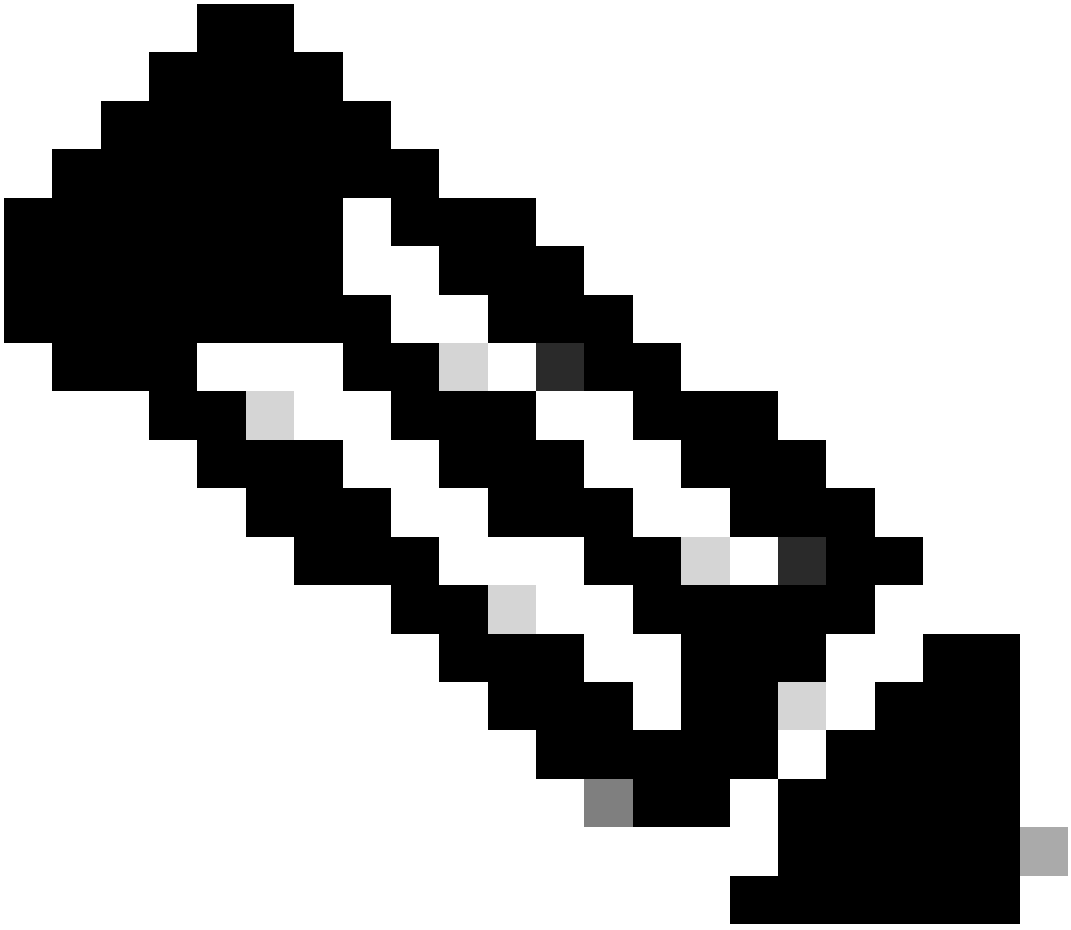
Melden Sie sich als Administrator beim CTB-Manager an. Führen Sie den ssh-keygen -yf server_key.pem Befehl aus.

Eine Passphrase wird nicht angefordert, wenn für den privaten Schlüssel keine erforderlich ist.

```
admin@ctb-manager:~$ ssh-keygen -yf server_key.pem ssh-rsa {removed for brevity} admin@ctb-manager:~$
```

Zertifikat und privaten Schlüssel bestätigen sind PEM-verschlüsselt

---



Hinweis: Diese Validierungen können vor der Installation der Zertifikate durchgeführt werden.

Melden Sie sich als Administrator beim CTB-Manager an.

Zeigen Sie den Inhalt der Datei server_cert.pem mit dem sudo cat server_cert.pem Befehl an. Passen Sie den Befehl an den Namen der Zertifikatsdatei an.

Die erste und die letzte Zeile der Datei sollten -----**BEGIN CERTIFICATE**----- bzw. sein-----END CERTIFICATE-----.

```
admin@ctb-manager:~$ sudo cat server_cert.pem -----BEGIN CERTIFICATE----- {removed_for_brevity} -----EN
```

Zeigen Sie die Datei server_key.pem mit dem sudo cat server_key.pem Befehl an. Passen Sie den Befehl an den Dateinamen der privaten Schlüssel an.

Die erste und die letzte Zeile der Datei sollten -----**BEGIN PRIVATE KEY**----- bzw. sein-----END PRIVATE KEY-----.

```
admin@ctb-manager:~$ sudo cat server_key.pem -----BEGIN PRIVATE KEY----- {removed_for_brevity} -----END
```

Selbstsigniertes Zertifikat

Selbstsigniertes Zertifikat generieren

- Melden Sie sich über eine SSH (Secure Shell) beim CTB Manager an, wie dies bei der Installation vom Benutzer konfiguriert wurde. Hierbei handelt es sich in der Regel um den Benutzer "admin".

- Geben Sie den sudo openssl req -x509 -newkey rsa:{key_len} -nodes -keyout server_key.pem -out server_cert.pem -sha256 -days 3650 -subj /CN={ctb_manager_ip} Befehl ein.

  - Ändern Sie die rsa:{key_len} mit einem privaten Schlüssel Ihrer Wahl, z. B. 2048, 4096 oder 8192.

  - Ändern Sie die {ctb_manager_ip}mit der IP des CTB-Manager-Knotens

```
admin@ctb-manager:~$ sudo openssl req -x509 -newkey rsa:4096 -nodes -keyout server_key.pem -
[sudo] password for admin:
Generating a RSA private key
.....................................................................................++++
.....................................................................++++
writing new private key to 'server_key.pem'
-----
```

```
admin@ctb-manager:~$
```

- Zeigen Sie die Datei server_cert.pem mit dem cat server_cert.pem Befehl an, und kopieren Sie den Inhalt in den Puffer, sodass er auf der lokalen Workstation in einen beliebigen Texteditor eingefügt werden kann. Speichern Sie die Datei. Sie können diese Dateien auch aus dem /home/admin Verzeichnis per SCP entfernen.

```
admin@ctb-manager:~$ cat server_cert.pem
-----BEGIN CERTIFICATE-----
{removed_for_brevity}
-----END CERTIFICATE-----
admin@ctb-manager:~$
```

- Zeigen Sie die Datei server_key.pem mit dem sudo cat server_key.pem Befehl an, und kopieren Sie den Inhalt in den Puffer, sodass er auf der lokalen Workstation in einen beliebigen Texteditor eingefügt werden kann. Speichern Sie die Datei. Sie können diese Datei auch mithilfe der SCP aus dem /home/admin Verzeichnis entfernen.

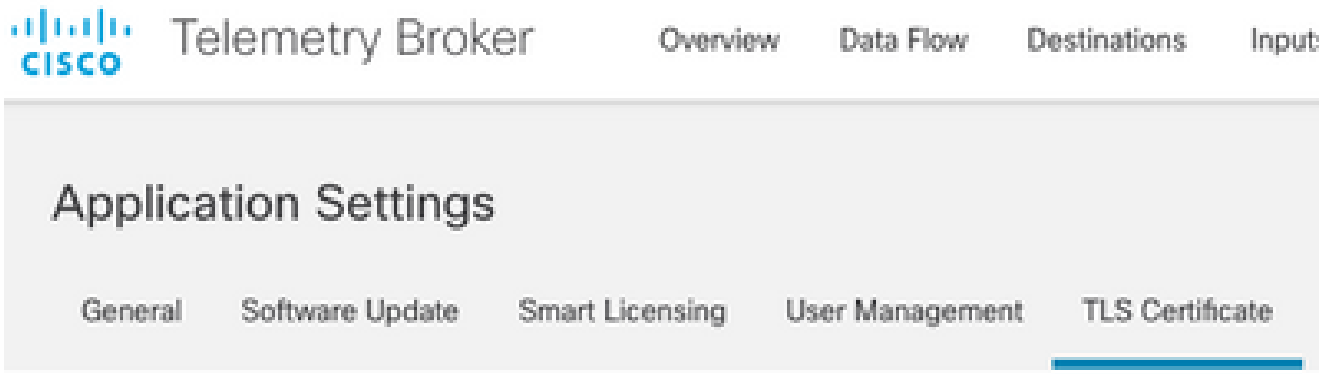
```
admin@ctb-manager:~$ sudo cat server_key.pem
-----BEGIN PRIVATE KEY-----
{removed_for_brevity}
-----END PRIVATE KEY-----
admin@ctb-manager:~$
```

Selbstsigniertes Zertifikat hochladen

1. Navigieren Sie zur CTB Manager Web UI, melden Sie sich als Administrator an, und klicken Sie auf das Zahnrad-Symbol, um auf "Settings" zuzugreifen.

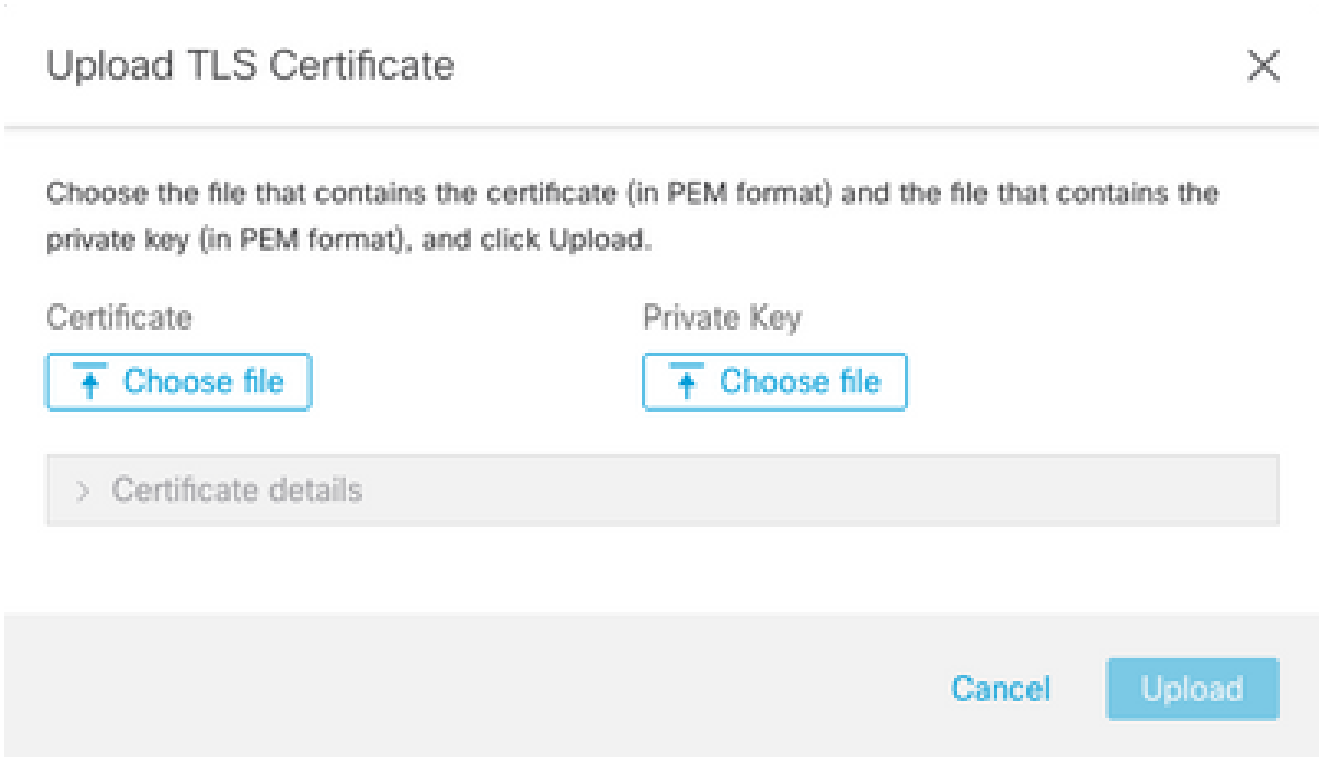
Symbol für CTB-Einstellung

- Navigieren Sie zur Registerkarte "TLS-Zertifikat".

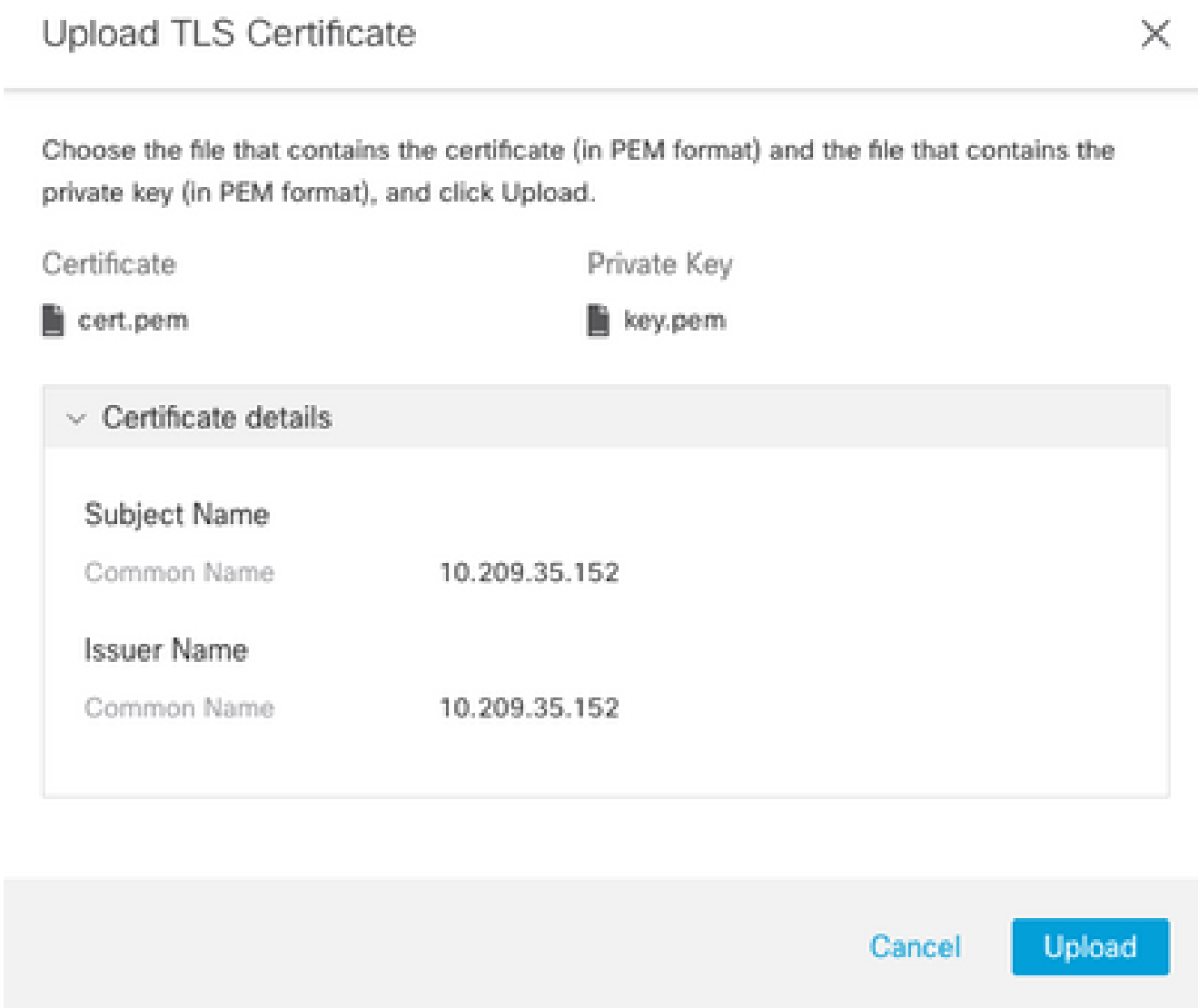


Registerkarte CTB-Zertifikate

- Upload TLS Certificate Wählen Sie im Dialogfeld "TLS-Zertifikat hochladen" die Option server_cert.pem und die Option server_key.pem für das Zertifikat und den privaten Schlüssel aus. Wenn die Dateien ausgewählt wurden, wählen Sie Hochladen aus.



• Nachdem die Dateien ausgewählt wurden, bestätigt ein Überprüfungsprozess die Kombination aus Zertifikat und Schlüssel und zeigt den allgemeinen Namen des Ausstellers und des Betreffs wie dargestellt an.



CTB-Zertifikat-Upload

- Klicken Sie auf die Schaltfläche "Hochladen", um das neue Zertifikat hochzuladen. Die Webbenutzeroberfläche startet in wenigen Augenblicken selbstständig neu, und melden Sie sich nach dem Neustart erneut beim Gerät an.

- Melden Sie sich bei der CTB Manager Node Web Console an, und navigieren Sie zu, Settings > TLS Certificate um Zertifikatsdetails anzuzeigen, z. B. ein neues Ablaufdatum, oder zeigen Sie die Zertifikatsdetails über den Browser an, um detailliertere Informationen anzuzeigen, z. B. Seriennummern.

Broker-Knoten aktualisieren

Sobald der CTB Manager Node über ein neues Identitätszertifikat verfügt, muss jeder CTB Broker Node manuell aktualisiert werden.

1. Melden Sie sich über SSH bei jedem Broker-Knoten an, und führen Sie den sudo ctb-manage Befehl aus.

```
admin@ctb-broker:~$ sudo ctb-manage

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for admin:
```

- Wählen Sie Option cbei Aufforderung aus.

```
== Management Configuration

A manager configuration already exists for 10.209.35.152
Options:

(o) Associate this node with a new manager
(c) Re-fetch the manager's certificate but keep everything else
(d) Deactivate this node (should be done after removing this node on the manager UI)
(a) Abort

How would you like to proceed? [o/c/d/a] c
```

- Überprüfen Sie die Zertifikatdetails, wenn sie mit den Werten für das signierte Zertifikat übereinstimmen, und wählen Sie diese Option aus, **y** um das Zertifikat zu akzeptieren. Die Dienste werden automatisch gestartet, und nach dem Start des Diensts wird die Eingabeaufforderung zurückgegeben. Der Servicestart kann bis zu 15 Minuten in Anspruch nehmen.

```
== Testing connection to server exists

== Fetching certificate from 10.209.35.152
Subject Hash
3fcbcd3c
subject=CN = 10.209.35.152
issuer=CN = 10.209.35.152
Validity:
notBefore=Mar 28 13:12:43 2023 GMT
notAfter=Mar 27 13:12:43 2024 GMT
X509v3 Subject Alternative Name:
IP Address:10.209.35.152

Do you accept the authenticity of the server? [y/n] y

== Writing /var/lib/titan/titanium_proxy/ssl/titanium.pem
```

```
done

== Starting service
```

Von der Zertifizierungsstelle (Certificate Authority, CA) ausgestellte Zertifikate

Erstellen einer Zertifikatssignaturanforderung (Certificate Signing Request, CSR) für die Ausstellung durch eine Zertifizierungsstelle

- Melden Sie sich über eine SSH (Secure Shell) beim CTB Manager an, wie dies bei der Installation vom Benutzer konfiguriert wurde. Hierbei handelt es sich in der Regel um den Benutzer "admin".

- Geben Sie den openssl req -new -newkey rsa:{key_len} -nodes -addext "subjectAltName = DNS:{ctb_manager_dns_name},IP:{ctb_manager_ip}" -keyout server_key.pem -out server.csr Befehl ein. Die zusätzlichen Attribute für die letzten beiden Zeilen können bei Bedarf leer gelassen werden.

  - Ändern Sie den {ctb_manager_dns_name} mit dem DNS-Namen des CTB-Manager-Knotens

    - Ändern Sie die {ctb_manager_ip}mit der IP des CTB-Manager-Knotens

    - Ändern Sie die {key_len} mit einer privaten Schlüssellänge Ihrer Wahl, z. B. 2048, 4096 oder 8192.

```
admin@ctb-manager:~$ openssl req -new -newkey rsa:4096 -nodes -addext "subjectAltName = DNS:
Generating a RSA private key
.....................++++
.....................................++++
writing new private key to 'server_key.pem'
-----
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.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:North Carolina
Locality Name (eg, city) []:RTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems Inc
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ctb-manager
Email Address []:noreply@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

- SCP stellt die CSR- und Schlüsseldateien für einen lokalen Computer bereit und stellt die CSR-Datei für die Zertifizierungsstelle bereit. Die Ausgabe der CSR-Anfrage durch die Zertifizierungsstelle im PEM-Format wird in diesem Dokument nicht behandelt.

Zertifikat mit Kette erstellen

Die Zertifizierungsstelle stellt das Serveridentitätszertifikat im PEM-Format aus. Es muss eine Kettendatei erstellt werden, die alle Kettenzertifikate und das Serveridentitätszertifikat für den CTB Manager-Knoten enthält.

Erstellen Sie in einem Texteditor eine Datei, indem Sie das im vorherigen Schritt signierte Zertifikat kombinieren und alle Zertifikate in der Kette, einschließlich der vertrauenswürdigen Zertifizierungsstelle, in der angegebenen Reihenfolge in einer einzigen Datei im PEM-Format anhängen.

```
– BEGIN CERTIFICATE – {CTB Manager Issued Certificate} – END CERTIFICATE – – BEGIN CERTIFICATE – {Issui
```

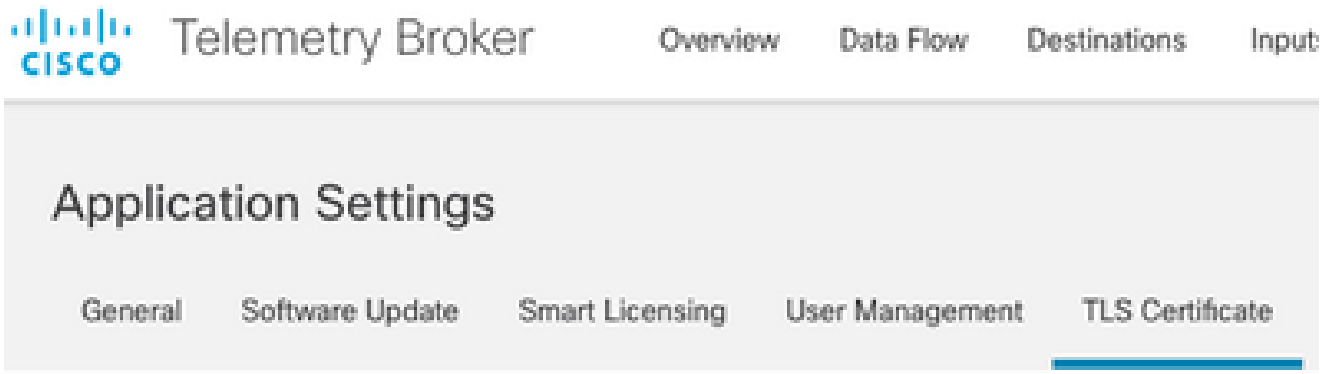
Stellen Sie sicher, dass diese neue Zertifikatsdatei mit der Kettendatei keine Leerzeichen am Anfang oder am Ende hat und keine Leerzeilen enthält und in der oben angegebenen Reihenfolge angeordnet ist.

Von der Zertifizierungsstelle ausgestelltes Zertifikat hochladen

1. Navigieren Sie zur CTB Manager Web UI, melden Sie sich als admin an, und klicken Sie auf das Zahnrad-Symbol, um auf "Settings" zuzugreifen.

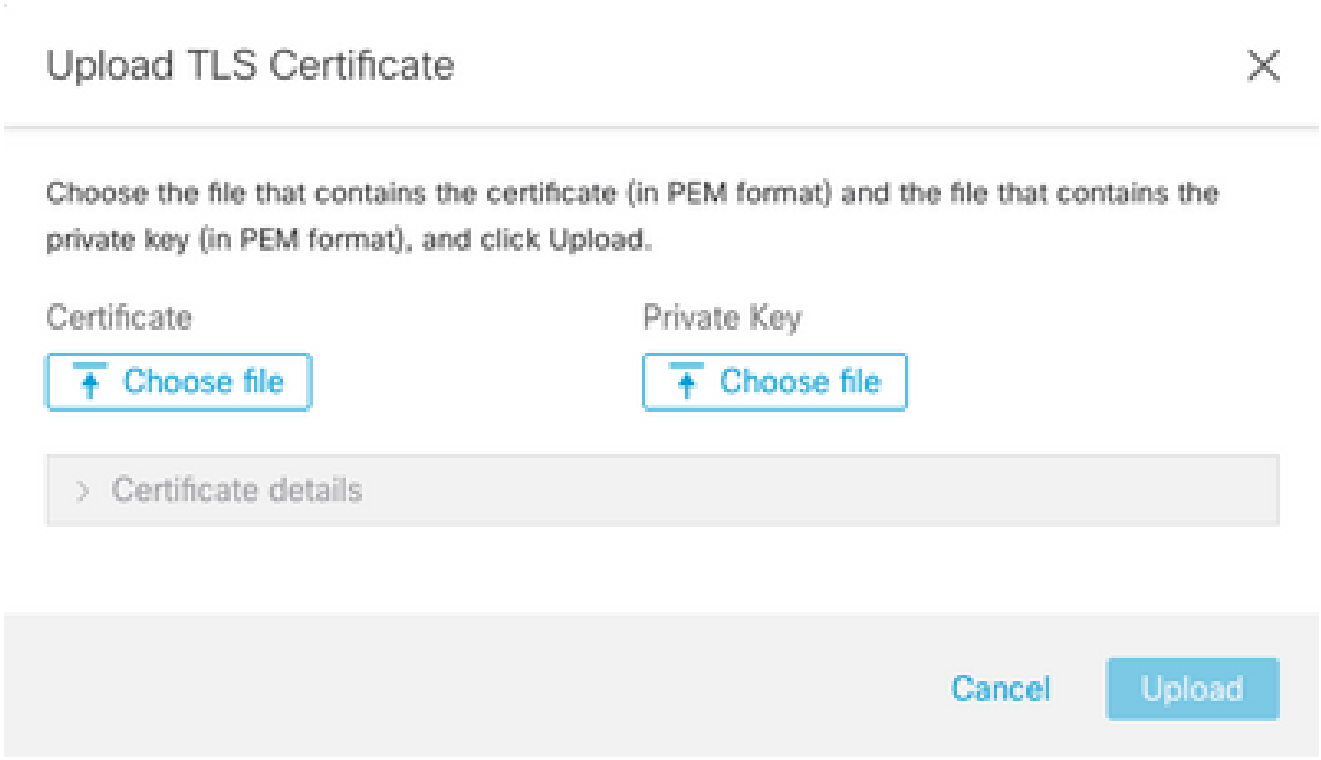
Symbol für CTB-Einstellung

- Navigieren Sie zur Registerkarte "TLS-Zertifikat".

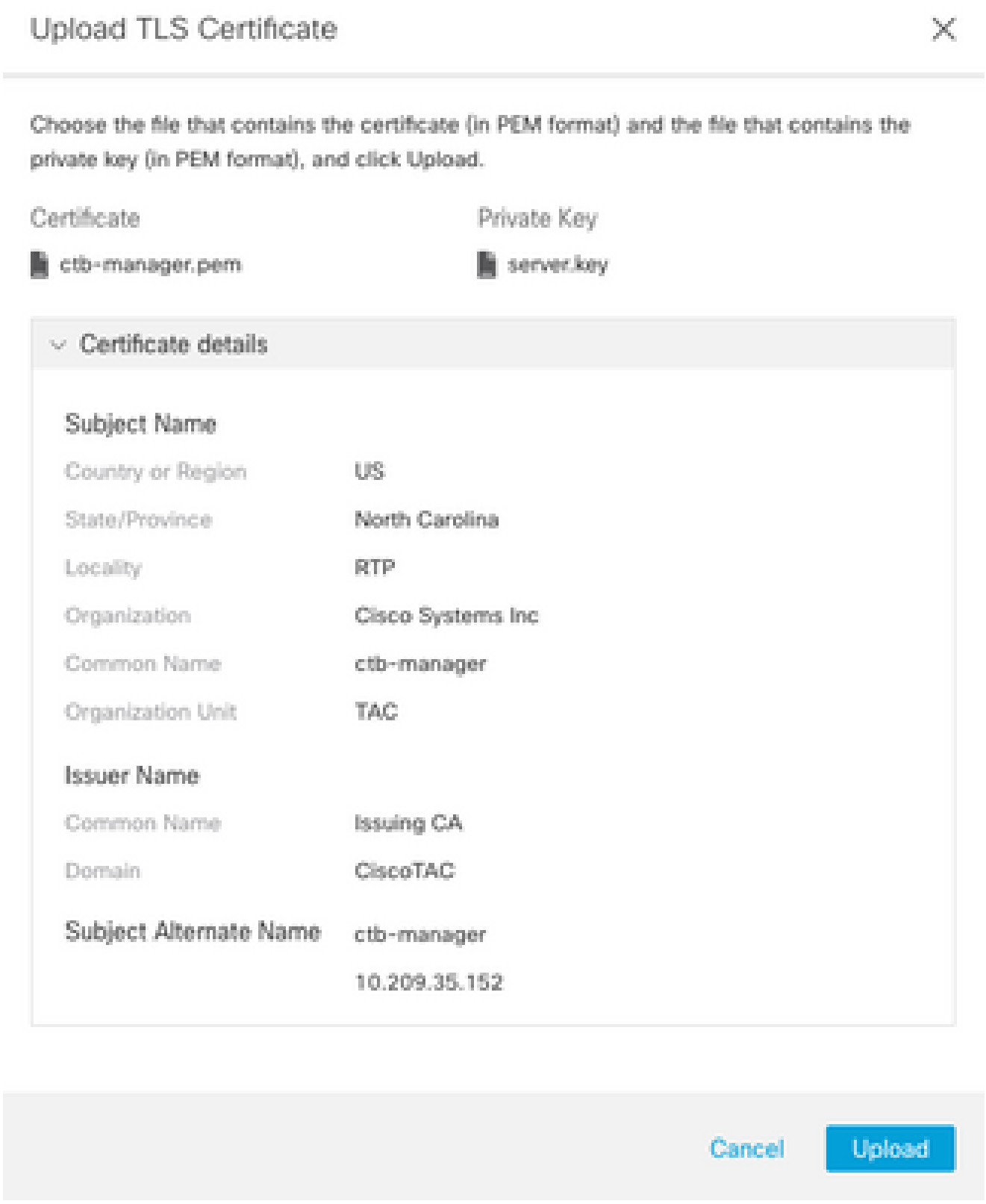


Registerkarte CTB-Zertifikate

- Wählen Sie Upload TLS Certificate und anschließend das Zertifikat mit der Kettendatei aus, die im letzten Abschnitt erstellt wurde, und den CTB-Manager, der server_key.pem für das Zertifikat bzw. den privaten Schlüssel im Dialogfeld "TLS-Zertifikat hochladen" generiert wurde. Wenn die Dateien ausgewählt wurden, wählen Sie Hochladen aus.



• Nachdem die Dateien ausgewählt wurden, bestätigt ein Verifizierungsprozess die Kombination aus Zertifikat und Schlüssel und zeigt den allgemeinen Namen des Ausstellers und des Betreffs an, wie unten gezeigt.



Zertifizierungsprüfung für CTB-CA

- Klicken Sie auf die Schaltfläche "Hochladen", um das neue Zertifikat hochzuladen. Die Webbenutzeroberfläche startet selbstständig in etwa 60 Sekunden neu und meldet sich nach dem Neustart bei der Webbenutzeroberfläche an.

- Melden Sie sich bei der CTB Manager Node Web Console an, und navigieren Sie zu, Settings > TLS Certificate um

Zertifikatsdetails anzuzeigen, z. B. ein neues Ablaufdatum, oder zeigen Sie die Zertifikatsdetails über den Browser an, um detailliertere Informationen anzuzeigen, z. B. Seriennummern.

Broker-Knoten aktualisieren

Sobald der CTB Manager Node über ein neues Identitätszertifikat verfügt, muss jeder CTB Broker Node manuell aktualisiert werden.

1. Melden Sie sich über SSH bei jedem Broker-Knoten an, und führen Sie den sudo ctb-manage Befehl aus.

```
admin@ctb-broker:~$ sudo ctb-manage

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for admin:
```

- Wählen Sie Option cbei Aufforderung aus.

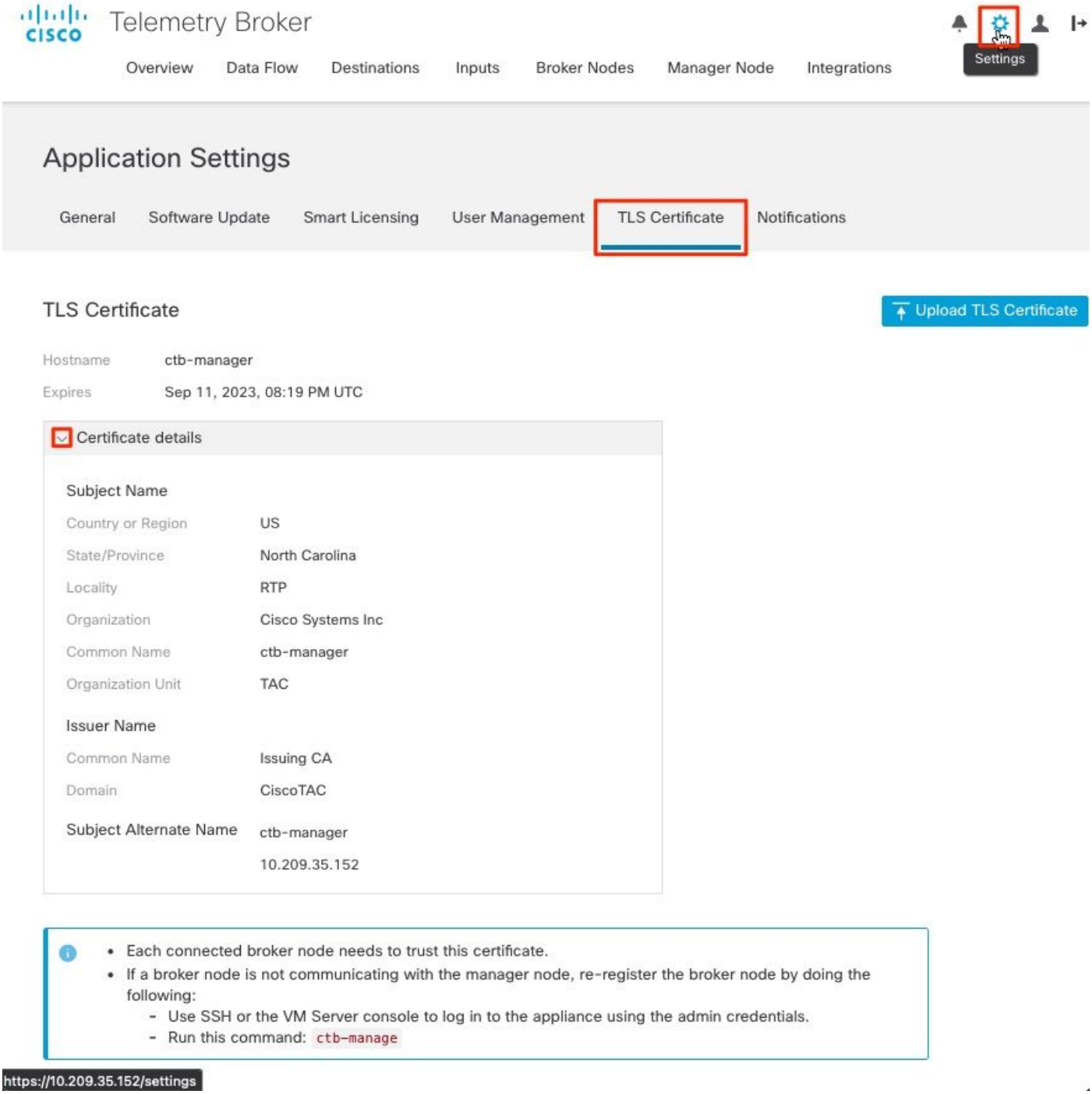
```
== Management Configuration

A manager configuration already exists for 10.209.35.152
Options:

(o) Associate this node with a new manager
(c) Re-fetch the manager's certificate but keep everything else
(d) Deactivate this node (should be done after removing this node on the manager UI)
(a) Abort

How would you like to proceed? [o/c/d/a] c
```

- Überprüfen Sie die Zertifikatdetails, wenn sie mit den Werten für das signierte Zertifikat übereinstimmen, und wählen Sie y aus, ob das Zertifikat akzeptiert werden soll. Die Dienste werden automatisch gestartet, und nach dem Start des Dienstes wird die Eingabeaufforderung zurückgegeben. Der Servicestart kann bis zu 15 Minuten in Anspruch nehmen.

```
== Testing connection to server exists

== Fetching certificate from 10.209.35.152
Subject Hash
fa7fd0fb
subject=C = US, ST = North Carolina, L = RTP, O = "Cisco Systems Inc", OU = TAC, CN = ctb-manager,
issuer=DC = CiscoTAC, CN = Issuing CA
Validity:
notBefore=Jun 13 16:09:29 2023 GMT
notAfter=Sep 11 16:19:29 2023 GMT
X509v3 Subject Alternative Name:
DNS:ctb-manager, IP Address:10.209.35.152

Do you accept the authenticity of the server? [y/n] y

== Writing /var/lib/titan/titanium_proxy/ssl/titanium.pem
done

== Starting service
```

Überprüfung

Melden Sie sich bei der CTB Manager Node Web Console an, und navigieren Sie zu, Settings > TLS Certificate um Zertifikatsdetails anzuzeigen, z. B. ein neues Ablaufdatum, oder zeigen Sie die Zertifikatsdetails über den Browser an, um detailliertere Informationen anzuzeigen, z. B. Seriennummern.



Details zum CTB-Zertifikat

Überprüfen Sie, ob der CTB-Broker-Knoten in der CTB-Manager-Knoten-Webbenutzeroberfläche keine Alarme anzeigt.

Fehlerbehebung

Wenn das Zertifikat unvollständig ist, z. B. wenn es an den Kettenzertifikaten fehlt, kann der CTB-Broker-Knoten nicht mit dem Manager-Knoten kommunizieren und zeigt in der Statusspalte in der Liste der Broker-Knoten "Not Seen Since" an.
Der Broker-Knoten wird weiterhin Datenverkehr in diesem Zustand replizieren und verteilen.

Melden Sie sich bei der CLI des CTB Manager-Knotens an, und geben Sie den sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem Befehl ein, um zu sehen, wie viele Zertifikate in der Datei cert.pem enthalten sind.

```
admin@ctb-manager:~$ sudo grep -ic begin /var/lib/titan/titanium_frontend/ssl/cert.pem [sudo] password
```

Der zurückgegebene Ausgabewert muss der Anzahl der CA-Geräte in der Kette plus dem CTB-Manager entsprechen.

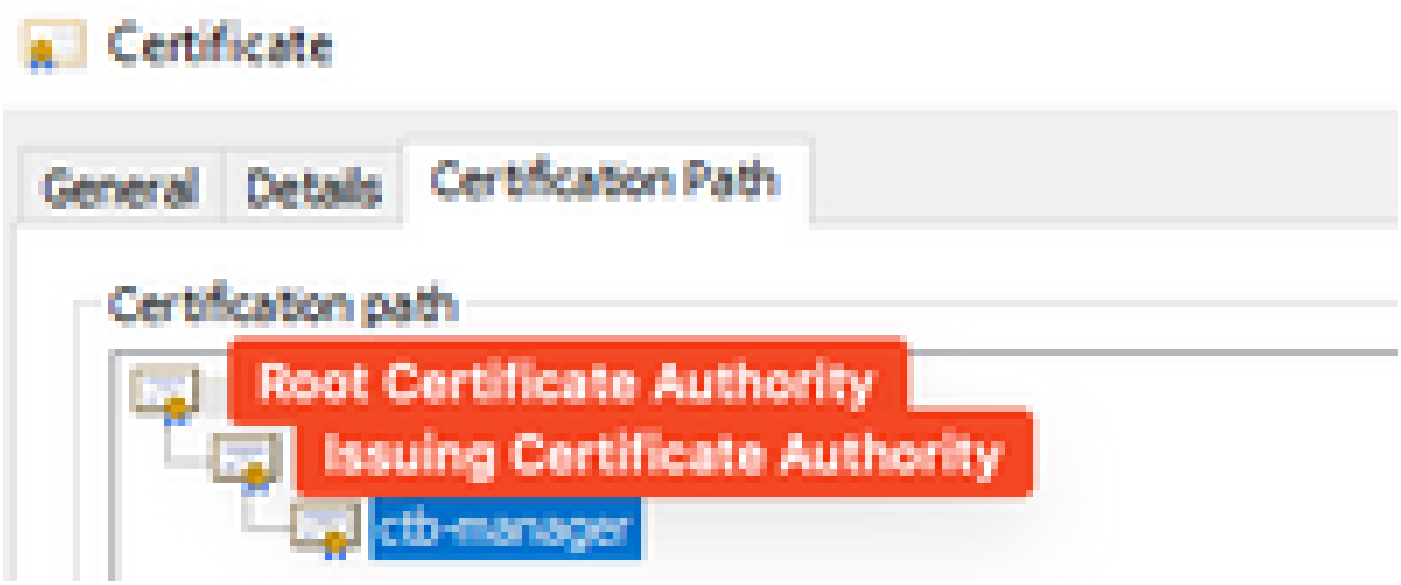
Die Ausgabe von 1 wird erwartet, wenn ein selbstsigniertes Zertifikat verwendet wird.

Die Ausgabe von 2 wird erwartet, wenn die PKI-Infrastruktur aus einer einzelnen Stammzertifizierungsstelle besteht, die auch die ausstellende Zertifizierungsstelle ist.

Die Ausgabe von 3 wird erwartet, wenn die PKI-Infrastruktur aus einer Stammzertifizierungsstelle und der ausstellenden Zertifizierungsstelle besteht.

Die Ausgabe von 4 wird erwartet, wenn die PKI-Infrastruktur aus einer Stammzertifizierungsstelle, einer untergeordneten Zertifizierungsstelle und der ausstellenden Zertifizierungsstelle besteht.

Vergleichen Sie die Ausgabe mit der aufgelisteten PKI, wenn Sie das Zertifikat in einer anderen Anwendung anzeigen, z. B. Microsoft Windows Crypto Shell Extensions.



PKI-Infrastruktur

In diesem Image enthält die PKI-Infrastruktur eine Stammzertifizierungsstelle und die ausstellende Zertifizierungsstelle.

Der Ausgabewert des Befehls sollte in diesem Szenario 3 sein.

Wenn die Ausgabe nicht den Erwartungen entspricht, überprüfen Sie die Schritte im Abschnitt **Zertifikat mit Kette erstellen,** um festzustellen, ob ein Zertifikat nicht vorhanden war.

Beim Anzeigen eines Zertifikats in ist Microsoft Windows Crypto Shell Extensions es möglich, dass nicht alle Zertifikate angezeigt werden, wenn der lokale Computer nicht über genügend Informationen verfügt, um das Zertifikat zu überprüfen.

Geben Sie den sudo ctb-mayday Befehl aus der CLI aus, um ein tägliches Paket zu generieren, das vom TAC überprüft werden soll.

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.