Zertifikatsanforderungen für mobilen und Remote-Zugriff und ATS-Verlauf verstehen

Inhalt

Einleitung

In diesem Dokument werden die Anforderungen für das Hochladen von Zertifikaten auf CUCM für den mobilen und Remote-Zugriff beschrieben.

Hintergrundinformationen

Der Cisco Expressway verwendet den Apache Traffic Server (ATS). Der Traffic Server ist eine sehr wichtige Komponente in Traversal-Lösungen, die hauptsächlich für folgende Funktionen eingesetzt werden:

- Zertifikatsüberprüfung: Es führt eine Zertifikatverifizierung der Cisco Unified Communications Manager (CUCM)-, IM & Presence- und Unity-Serverknoten für MRA-Services durch.
- Proxyfunktion und Caching: Er fungiert als schneller, skalierbarer Caching-Proxy-Server für HTTP-/HTTPS-Datenverkehr.

Auf Expressway Version 14.0.2

Auf dem Datenverkehrsserver (ATS) wird bei der Kommunikation mit dem CUCM während der MRA-Bereitstellung eine geringfügige Durchsetzung der Zertifikatsüberprüfung erkannt.

Die Anforderung wurde unter CSCvz45074 dokumentiert, wobei die Root-Zertifikate, die Expressway Core-Serverzertifikate signiert haben, auf CUCM als Tomcat-Trust und Callmanager Trust hochgeladen werden müssen: https://cdetsng.cisco.com/summary/#/defect/CSCvz45074.

- Traffic Server erzwingt die Zertifikatsüberprüfung.

- Stellen Sie vor dem Upgrade auf die X14.0.2-Version sicher, dass diese Zertifikatanforderung erfüllt ist.

Anforderung - Die CA-Kette (Root + Intermediary), die das Expressway-C-Zertifikat signiert hat, muss zur CUCM-Liste "tomcat-trust" und "CallManager-trust" hinzugefügt werden, auch wenn sich der Unified Communications Manager (UCM) im ungesicherten Modus befindet.

Grund - Der Datenverkehrsserverdienst in Expressway sendet sein Zertifikat, wenn ein Server-UCM es anfordert. Diese Anforderungen betreffen Dienste, die auf anderen Ports als 8443 ausgeführt werden (z. B. Ports 6971, 6972 usw.). Dies erzwingt die Zertifikatsüberprüfung, auch wenn sich UCM im ungesicherten Modus befindet. Weitere Informationen finden Sie im Mobile and Remote Access Through Expressway Deployment Guide.

Verhalten bei früheren Versionen als 14.0.8

Der Datenverkehrsserver auf Expressway-C, der sichere bidirektionale HTTPS-Verbindungen zwischen Expressway-C- und Unified Communication-Knoten verarbeitet, hat das vom Remote-Ende präsentierte Zertifikat nicht überprüft. Bei der MRA-Konfiguration besteht die Option, die TLS-Zertifikatsüberprüfung durch die Konfiguration des TLS-Überprüfungsmodus auf "Ein" zu setzen, wenn entweder CUCM-, IM&P- oder Unity-Server unter Konfiguration > Unified Communications > Unified CM-Server/IM und Presence Service-Knoten/Unity Connection-Server hinzugefügt werden. Die Konfigurationsoption wird im nächsten Screenshot gezeigt, der angibt, dass sie den FQDN oder die IP im SAN sowie die Gültigkeit des Zertifikats überprüft und ob es von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.

Es gab auch ein bekanntes Problem, bei dem zwei Zertifikate mit demselben CN-Namen nicht in den Expressway-Vertrauensspeicher geladen werden können. Diese Einschränkung führte zu zwei Problemen:

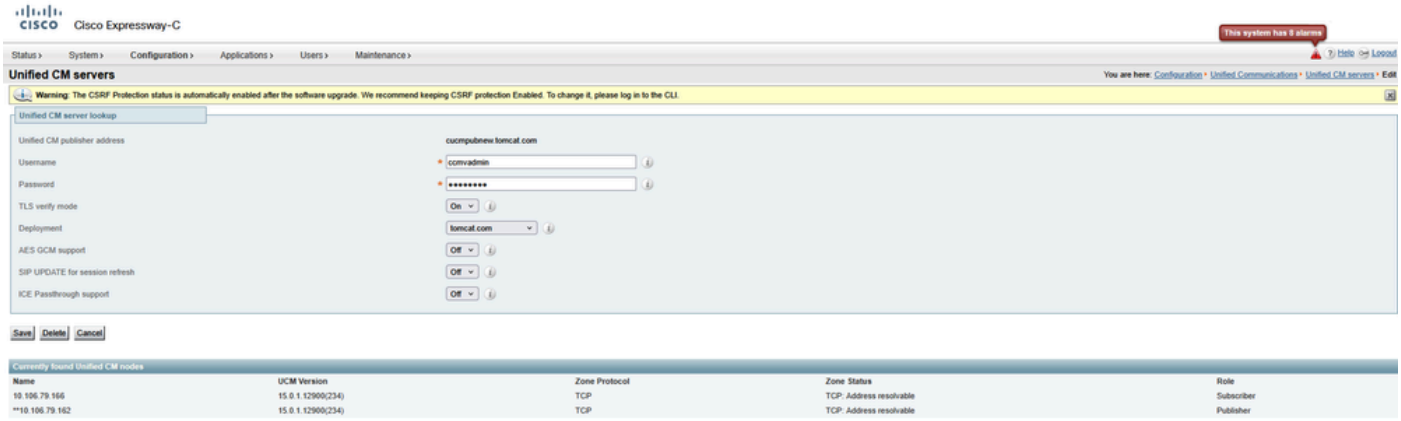
1. Wenn Sie das Call Manager-Zertifikat in den Expressway Trust Store laden, schlägt die TLS-Überprüfung "Ein" beim Hinzufügen von CUCMs fehl.

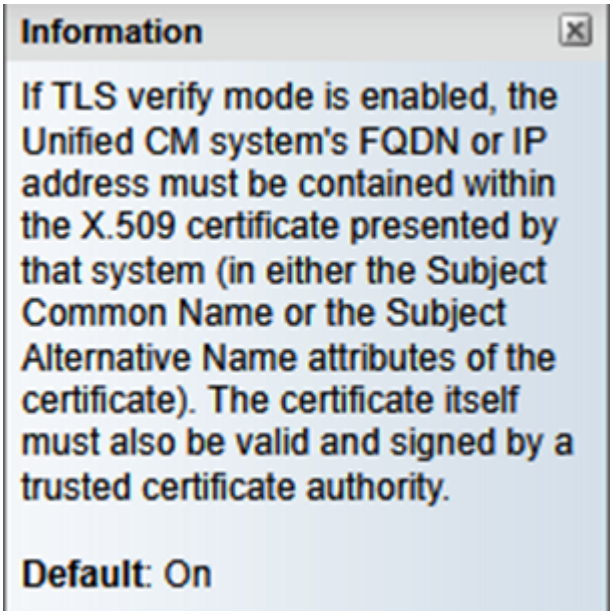
2: Wenn Sie das Tomcat-Zertifikat in den Expressway Trust-Speicher laden, schlägt die sichere SIP-Registrierung auf 5061 fehl.

Dieses Verhalten ist in CSCwa12894 dokumentiert.

Außerdem wird diese TLS-Zertifikatsüberprüfung nur bei der Erkennung der CUCM-/IM&P-/Unity-Server und nicht während der MRA-Clientbereitstellung durchgeführt.

Der Nachteil dieser Konfiguration besteht darin, dass sie nur für die Herausgeberadresse verifiziert wird, die Sie hinzufügen. Es wird nicht geprüft, ob das Zertifikat auf den Subscriber-Knoten korrekt eingerichtet wurde, da es die Subscriber-Knoten-Informationen (FQDN oder IP) aus der Datenbank des Publisher-Knotens abruft.





Verhalten bei Versionen 14.0.8 und höher

Ab der X14.0.8-Version führt der Expressway-Server für jede einzelne HTTPS-Anforderung, die über den Datenverkehrsserver erfolgt, eine TLS-Zertifikatüberprüfung durch. Dies bedeutet, dass er dies auch durchführt, wenn der TLS-Verifizierungsmodus während der Erkennung der CUCM-/IM&P-/Unity-Knoten auf "Aus" gesetzt wird. Wenn die Überprüfung nicht erfolgreich ist, wird der TLS-Handshake nicht abgeschlossen, und die Anforderung schlägt fehl. Dies kann zum Verlust von Funktionen führen, z. B. Redundanz, Failover-Probleme oder vollständige Anmeldefehler. Wenn der TLS-Verifizierungsmodus auf "Ein" gesetzt ist, ist auch nicht sichergestellt, dass alle Verbindungen ordnungsgemäß funktionieren, wie im Beispiel weiter unten beschrieben.

Die genauen Zertifikate, die Expressway gegenüber den CUCM-/IM&P-/Unity-Knoten überprüft, sind im Abschnitt des MRA-Leitfadens aufgeführt.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-0/mra/exwy_b_mra-deployment-guide-x150.pdf

Abschnitt

Zertifikatanforderungen > Zertifikataustauschanforderungen

Aufgrund dieser veränderten Kommunikationsweise zwischen Expressway-Core und CUCM muss sichergestellt werden, dass:

1. Sie empfehlen die Verwendung von CA-signierten Zertifikaten für Mobil- und Remote-Zugriff.

2. Jeder Unified CM-Cluster muss dem Expressway-C-Zertifikat vertrauen. Stellen Sie für jeden Cluster Folgendes sicher:

- Wenn der gemischte Modus aktiviert ist — Das Expressway-C-Zertifikat muss im CallManager-trust- und Tomcat-trust-Speicher des Unified CM installiert sein.
- Wenn der gemischte Modus deaktiviert ist - Das Stammzertifikat der Zertifizierungsstelle, das das Expressway-C-Zertifikat signiert, muss im CallManager-trust- und Tomcat-trust-Speicher auf dem Unified CM installiert sein. Führen Sie dann einen Neustart durch: ・ Tomcat Service ・ CallManager Service ・ HA Proxy Service (wenn TLS auf Tomcat verwendet wird).

Stellen Sie auf Expressway - Core sicher, dass folgende Maßnahmen ergriffen werden:

- Expressway-C muss den von den einzelnen Unified CM-, IM- und Presence Service-Clustern vorgelegten Zertifikaten vertrauen.

Der Vertrauensspeicher von Expressway-C muss das Zertifikat der Stammzertifizierungsstelle enthalten, das die Unified CM- und IM- und Presence Service-Zertifikate für alle UC-Cluster signiert.

Anmerkung: Stellen Sie sicher, dass Sie alle Stamm- und Zwischenzertifikate der Zertifizierungsstelle oder die vollständige Zertifizierungsstellenkette, die zum Signieren des Expressway-C-Zertifikats verwendet wird, zur Tomcat-trust- und CallManager-trust-Liste von Cisco Unified Communications Manager (UCM) hinzufügen, auch wenn der UCM im ungesicherten Modus betrieben wird.

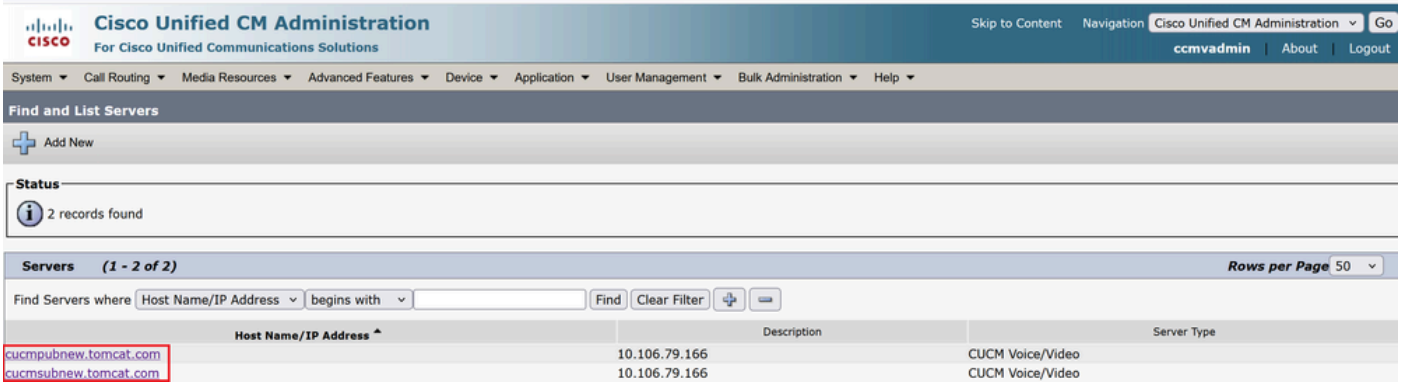
Grund - Der Datenverkehrsserver-Dienst in Expressway sendet sein Zertifikat immer dann, wenn ein Server (UCM) es anfordert. Diese Anforderungen betreffen Dienste, die auf anderen Ports als 8443 ausgeführt werden (z. B. Ports 6971, 6972 usw.). Dies erzwingt die Zertifikatsüberprüfung, auch wenn sich UCM im ungesicherten Modus befindet.

Die Art und Weise, wie die CUCM-Adresse unter System > Server hinzugefügt wird, spielt eine sehr wichtige Rolle beim Hinzufügen von CUCM/IMP zum Expressway-Core unter Configuration > Unified Communications > Unified CM-Server/IM und Presence Service-Knoten.

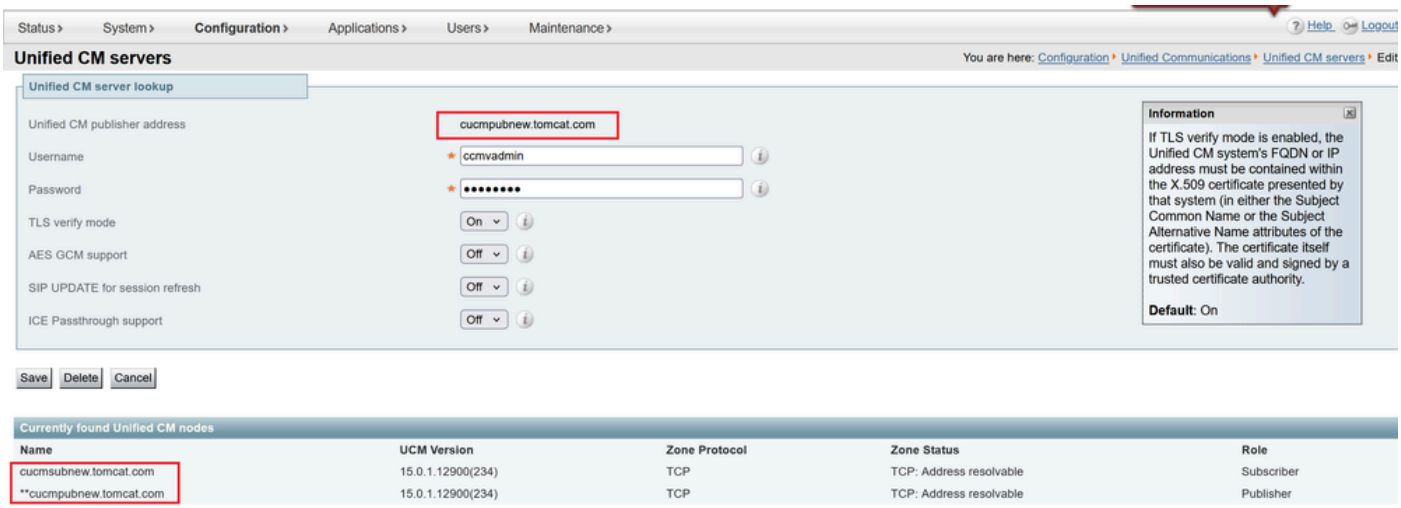
CUCM muss immer mit FQDN und nicht mit Hostname oder IP-Adresse hinzugefügt werden. Wenn er sieht, dass CUCM unter System > Server als Hostname/IP-Adresse hinzugefügt wird

Beim TLS-Handshake schlägt die TLS-Überprüfung "Ein" fehl, und das CUCM-Cluster wird auf dem Expressway-Core nicht hinzugefügt.

In der Abbildung wird CUCM als Hostname hinzugefügt:



In dieser Abbildung ist der auf dem Expressway-Core hinzugefügte CUCM mit FQDN mit TLS-Prüfmodus = EIN:



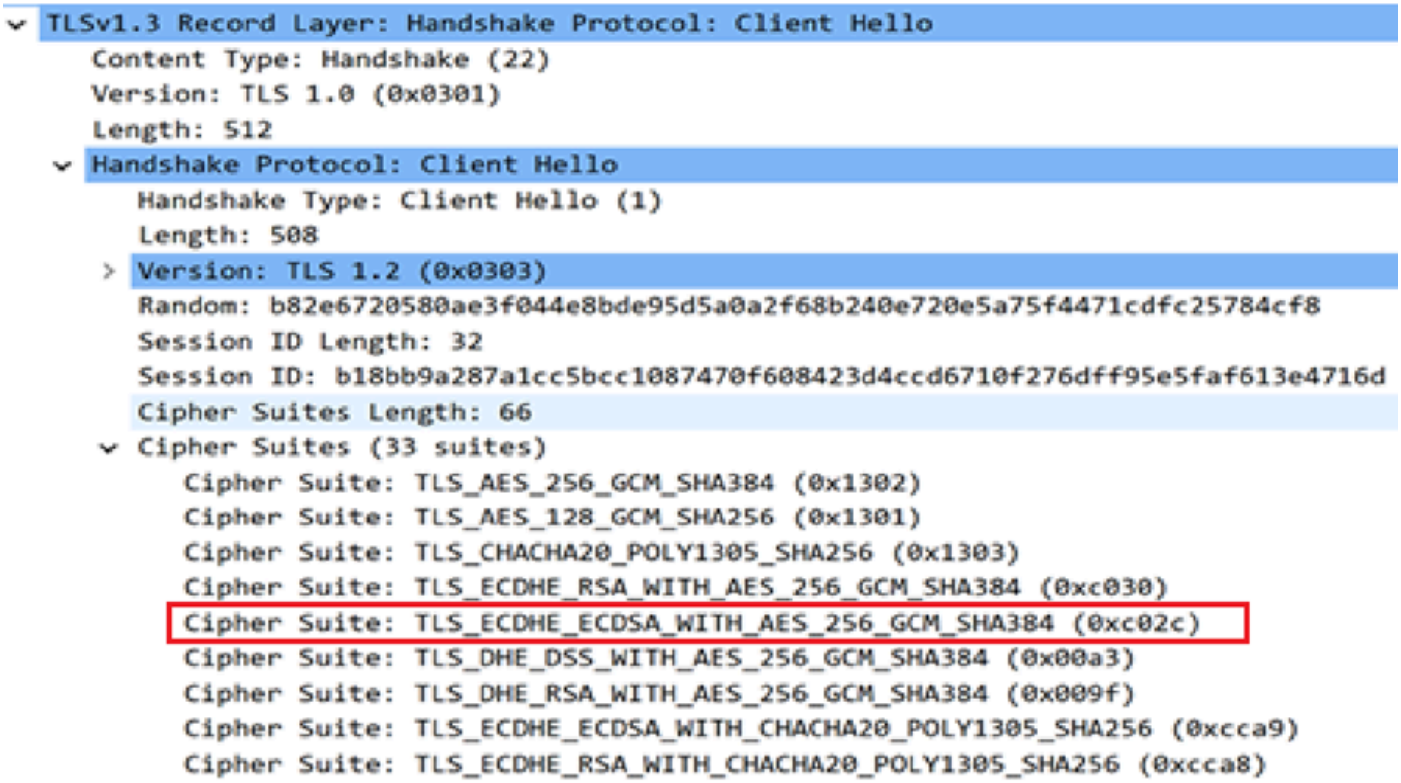
Es wurde auch eine Änderung in X14.2 eingeführt, die Chiffren während eines TLS-Handshakes (Client hello) in einer anderen Präferenzreihenfolge präsentiert. Dies war vom Upgrade-Pfad abhängig und verursachte nach einem Software-Upgrade unerwartete TLS-Verbindungen. Es kann sein, dass vor dem Upgrade während des TLS-Handshakes das Cisco Tomcat- oder Cisco CallManager-Zertifikat vom CUCM angefordert wurde. Aber dass nach dem Upgrade, es für die ECDSA-Variante (die sicherere Verschlüsselung Variante als RSA) angefordert. Die Cisco Tomcat-ECDSA- oder Cisco CallManager-ECDSA-Zertifikate können von einer anderen Zertifizierungsstelle signiert werden oder nur von selbst signierten Zertifikaten (Standard).

Diese Änderung der Reihenfolge der Verschlüsselungspräferenzen ist nicht immer relevant für Sie, da sie vom Upgrade-Pfad abhängt, wie in den Versionshinweisen zu Expressway X14.2.1 dargestellt. Kurz gesagt, Sie können aus Maintenance > Security > Ciphers für jede der Cipher-Listen sehen, ob es ECDHE-RSA-AES256-GCM-SHA384 vorausgeht oder nicht. Wenn dies nicht der Fall ist, wird die neuere ECDSA-Verschlüsselung der RSA-Verschlüsselung vorgezogen. Wenn dies der Fall ist, haben Sie das Verhalten wie zuvor bei RSA, das dann die höhere Präferenz hat.

Der nächste Screenshot zeigt in rotem Feld den ECDSA-Verschlüsselungscode, der vom Expressway-Core während der TLS-Aushandlungsmeldung in Client hello angekündigt wird: #IF

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 wird vom Remote Responder (CUCM) im Server hello ausgewählt. Die TLS-Aushandlung schlägt fehl, wenn:

ROOT-Zertifizierungsstellenzertifikate oder tatsächliche ECDSA-Zertifikate von Responder, d. h., CUCM ist in diesem Fall nicht auf dem Expressway Trust Store installiert.



Alternativ können Sie auch Expressway Ciphers so ändern, dass ECDSA keinen Vorrang hat.

1. Ändern Sie die SIP-Verschlüsselung, indem Sie eine offene SSL-Zeichenfolge von GCM-Sha384 anhängen.

"ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:.....:!MD5:!PSK:!eNULL:!aNULL:!aDH"

2. Fügen Sie + hinzu, um die Chiffre endlich zu verschieben, oder fügen Sie ! hinzu, um ECDSA dauerhaft zu deaktivieren.

Verschlüsselung: "EECDH:EDH:HIGH:-AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH:+ECDSA"

3. Fügen Sie ein Zertifikat der Stammzertifizierungsstelle und eines Zwischenzertifikats hinzu, das das ECDSA-Zertifikat auf dem CUCM signiert hat, oder fügen Sie das Tomcat-ECDSA-Zertifikat auf dem Expressway-Vertrauensspeicher hinzu (in einigen Fällen).

Aufgrund der geänderten Verschlüsselungspriorität nach dem Upgrade können MRA-Bereitstellungen jedoch abbrechen. Das TAC muss daher die zuvor erwähnte Problemumgehung durchführen, damit die Dinge wieder funktionieren.

Mit der Einführung von TLS 1.3 wird es noch schwieriger zu überprüfen, welche Zertifikate in

Wireshark ausgetauscht werden.

Verhalten bei Versionen x15.3

Nur für SIP-Schnittstellen können Sie RSA- oder ECDSA-Verschlüsselungen auswählen.

Mit X15.x wurde TLS 1.3 erzwungen. Wie vor Ort zu sehen, wird der RSA-Algorithmus vor allem über ECDSA ausgewählt. Kunden, die jetzt auf x15.2 aktualisieren, können wählen,

zwischen RSA- und ECDSA-Algorithmus mit diesem Befehlssatz:

xConfiguration SIP Advanced TlsSignatureAlgoPrefRsa: Ein/Aus

TlssignatureAlgoPrefRSA funktioniert nur, wenn die SIP-Schnittstelle über TLS 1.3 verfügt.

xConfiguration SIP - Erweiterte SipTlsVersionen: "TLSv1.3"

Anmerkung: Diese ist ab sofort nur für die SIP-Schnittstelle zulässig. Die Überlegungen zu Traffic Server und Tomcat für 8443 bleiben wie zuvor beschrieben unverändert.

Die Chiffrieranzüge, die während des Client-Begrüßungsvorgangs von Expressway an CUCM gesendet werden, werden bei Auswahl von RSA angezeigt.

- Signaturalgorithmus: rsa_pss_rsae_sha512 (0x0806)
- Signaturalgorithmus: rsa_pss_rsae_sha384 (0x0805)
- Signaturalgorithmus: rsa_pss_rsae_sha256 (0x0804)
- Signaturalgorithmus: ecdsa_secp521r1_sha512 (0x0603)
- Signaturalgorithmus: ecdsa_secp384r1_sha384 (0x0503)
- Signaturalgorithmus: ecdsa_secp256r1_sha256 (0x0403)

Die zuvor eingegebene Konfiguration funktioniert im Tandem darüber, welche Konfiguration Sie für CUCM zu TLS-Verschlüsselungen unter Enterprise Parameters (Unternehmensparameter) > Security Parameters (Sicherheitsparameter) ausgewählt haben.

Außerdem ist zu beachten, dass bei einem abgebrochenen TLS-Handshake über TLS 1.3 zwischen Expressway-C und CUCM die in Diagnoseprotokollen oder PCAP aufgedruckten Fehler nicht sehr hilfreich sind. Es lohnt sich, diese Fehlerbehebungen im Rahmen der Arbeit mit dem TAC zu aktivieren, damit die Komponente eindeutige Fehler ausgibt, um die Fehler zu beheben.

xConfiguration Logger Developer.Trafficserver.http-Ebene: "DEBUG"
xConfiguration Logger Developer.trafficServer.http_trans Ebene: "DEBUG"
xConfiguration Logger Developer.trafficServer.iocore Ebene: "DEBUG"
xConfiguration Logger Developer.trafficserver.ssl Ebene: "DEBUG"

Was ist zu erwarten, wenn Callmanager ein Zertifikat mit mehreren Diensten teilt?

Mit der Wiederverwendung des Zertifikats auf dem CUCM ändert sich die Lage geringfügig.

Ab CUCM 14.0 können Sie Tomcat- und Tomcat-ECDSA-Zertifikate als Call Manager und Call Manager ECDSA wiederverwenden.

Tomcat-Zertifikat kann als Callmanager-Zertifikat wiederverwendet werden.

Das Tomcat-ECDSA-Zertifikat kann als Callmanager-ECDSA-Zertifikat wiederverwendet werden.

Das macht das Leben einfach.

1. Mehrere Dienste auf CUCM verwenden jetzt ein Zertifikat, wodurch die Kosten für das Zertifikat sinken.

2. Weniger Verwaltung von Zertifikaten.

3. Wenn Sie das Tomcat/Callmanager- oder Tomcat-ECDSA/Callmanager-ECDSA-Zertifikat (aus irgendeinem Grund) auf den Expressway-Core Trust Store hochladen müssen, ist es nur ein Zertifikat, das Sie hochladen müssen. Es wird kein Problem mit dem gleichen CN-Namen geben (weiter oben in diesem Dokument erwähnt).

Anmerkung: Die Wiederverwendung des Zertifikats erfolgt nur, wenn Tomcat und Tomcat-ECDSA Multisan-Zertifikate sind.

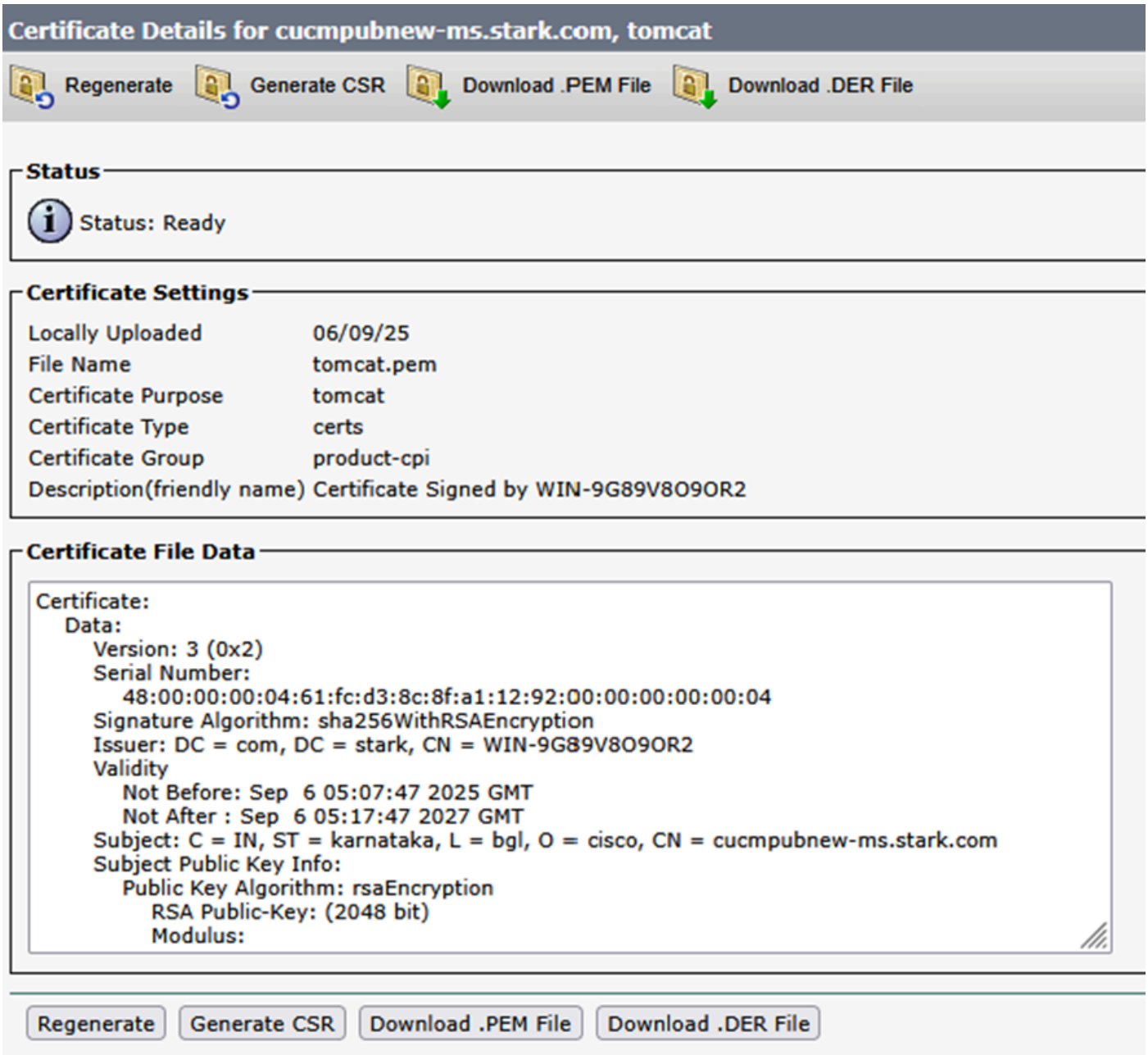
ECDSA-Serverzertifikate nach Wiederverwendung, Callmanager und Callmanager sind im CUCM-Vertrauensspeicher nicht sichtbar. Sie können die Wiederverwendung des Zertifikats in der CLI überprüfen, indem Sie die folgenden Befehle ausführen:

show cert own CallManager

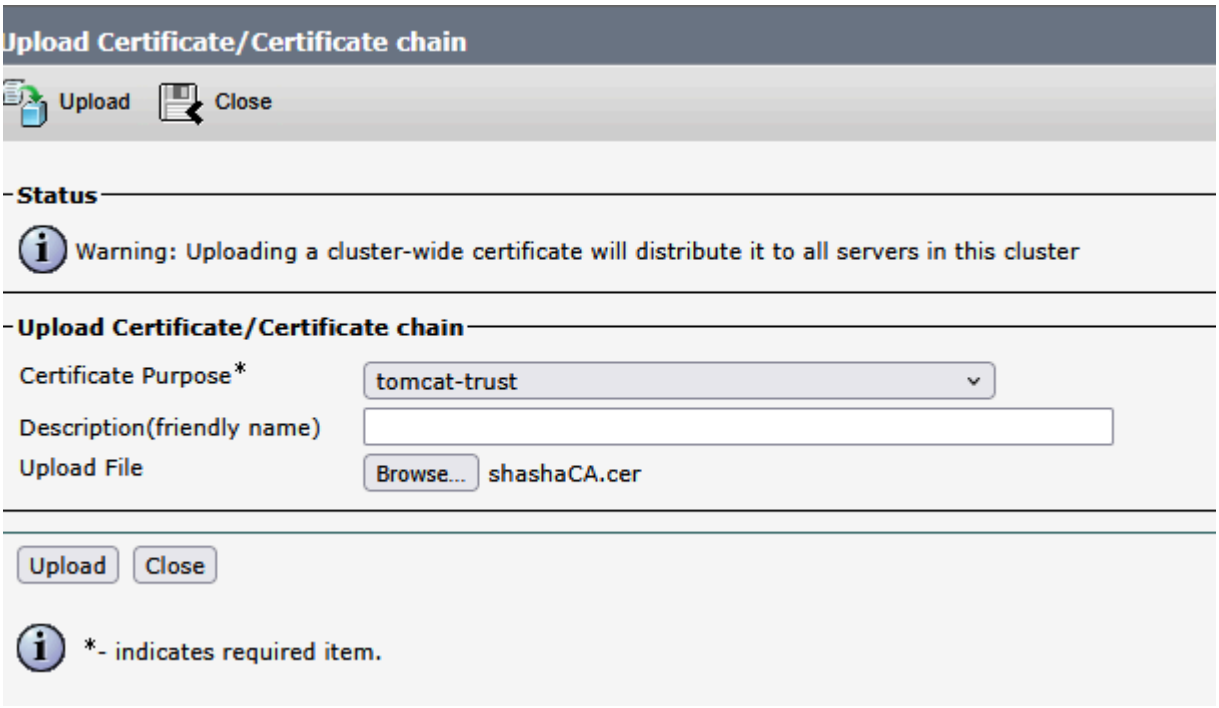
Tomatensoße

Schritte zur Wiederverwendung des Zertifikats

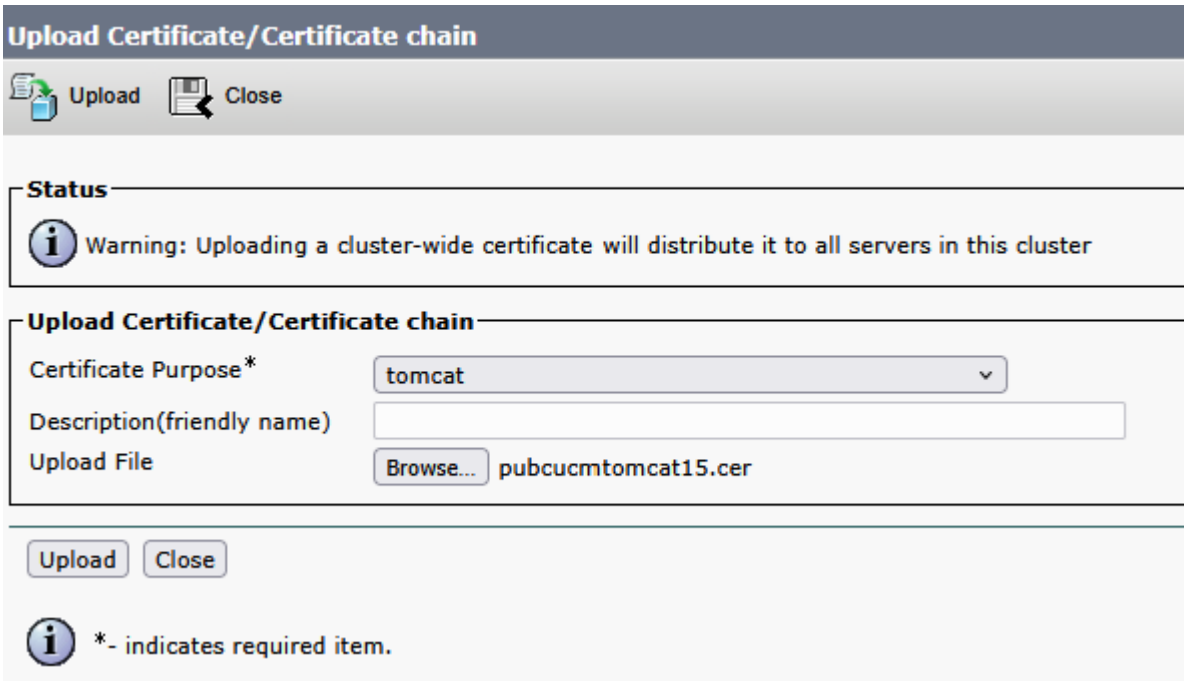
Tomcat CSR Pub wird generiert.



Laden Sie ein CA-Zertifikat hoch, das das Tomcat-Zertifikat auf dem CUCM als Tomcat-trust signiert.



Sobald das Tomcat-Zertifikat signiert ist, laden Sie es auf den Herausgeber hoch. Starten Sie die entsprechenden Services nach Aufforderung neu.



Sobald das Tomcat-Zertifikat signiert ist, laden Sie es auf den Herausgeber hoch. Starten Sie die entsprechenden Services nach Aufforderung neu.

Erfolg: Zertifikat hochgeladen. Führen Sie eine Disaster Recovery-Sicherung durch, sodass die letzte Sicherung das hochgeladene Zertifikat enthält.
Starten Sie den Cisco Tomcat-Webdienst über die CLI "utils service restart Cisco Tomcat" auf allen Clusterknoten (UCM/IMP) neu. Starten Sie die Cisco UDS Tomcat- und Cisco AXL Tomcat-

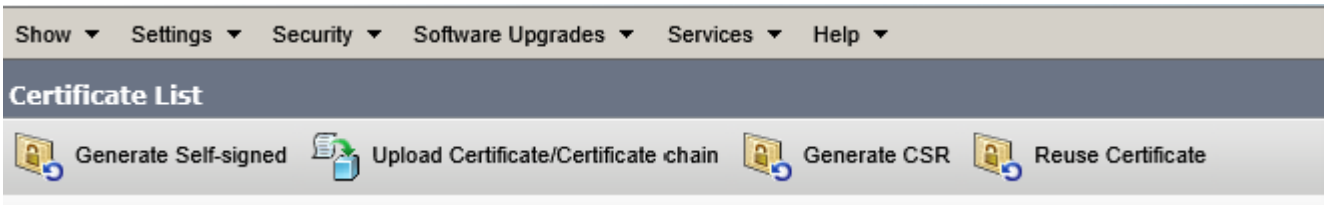
Webdienste über die CLI "utils service restart Cisco UDS Tomcat and utils service restart Cisco AXL Tomcat" auf allen UCM-Cluster-Knoten neu. Starten Sie außerdem die Cisco DRF Master- und Cisco DRF Local-Services auf dem Publisher-Knoten neu. Starten Sie nur den lokalen Cisco DRF-Dienst auf den Subscriber-Knoten neu.

Das Tomcat-Zertifikat ist jetzt von CA signiert.

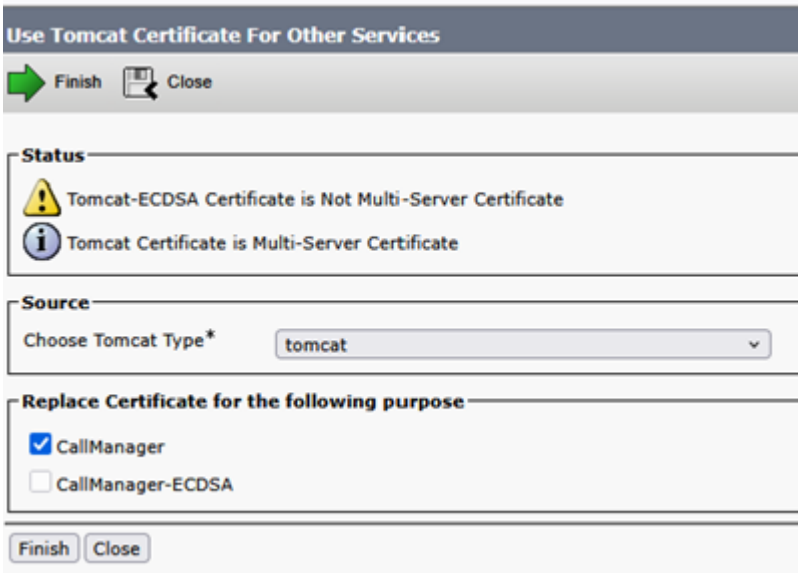
tomcat	cucmpubnew-ms.stark.com 51dc40f400000000000b	signed IdentityCA-signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/23/2027Certificate Signed by RICKY200-TMS-CA

Um das Tomcat Zertifikat jetzt als Callmanager Zertifikat wiederzuverwenden.

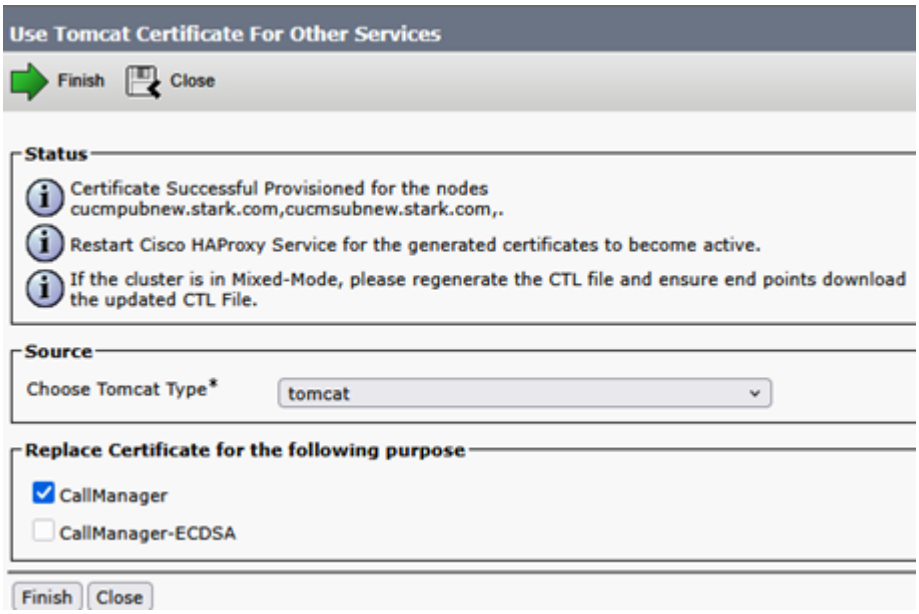
Klicken Sie auf Zertifikat wiederverwenden.



Wählen Sie Tomcat im Dropdown-Menü aus, und aktivieren Sie das Zertifikat "Callmanager".



Klicken Sie auf Beenden.



Das Tomcat-Zertifikat wird jetzt als Callmanager-Zertifikat wiederverwendet. Dies kann über die CLI validiert werden.

Seriennummer (SN) des Callmanager-Zertifikats: 56:ff:6c:71:00:00:00:00:00:0d

```
admin:show cert own CallManager
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:ff:6c:71:00:00:00:00:00:0d
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
        Validity
            Not Before: Oct 24 08:44:34 2025 GMT
            Not After : Oct 24 08:54:34 2027 GMT
        Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.
tomcat.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
                    6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
                    44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
                    10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
                    89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
                    23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
                    5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

Tomcat-Zertifikat SN: 56:ff:6c:71:00:00:00:00:00:0d

```
admin:show cert own tomcat
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:ff:6c:71:00:00:00:00:00:0d
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
        Validity
            Not Before: Oct 24 08:44:34 2025 GMT
            Not After : Oct 24 08:54:34 2027 GMT
        Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.tomcat.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
                    6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
                    44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
                    10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
                    89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
                    23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
                    5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

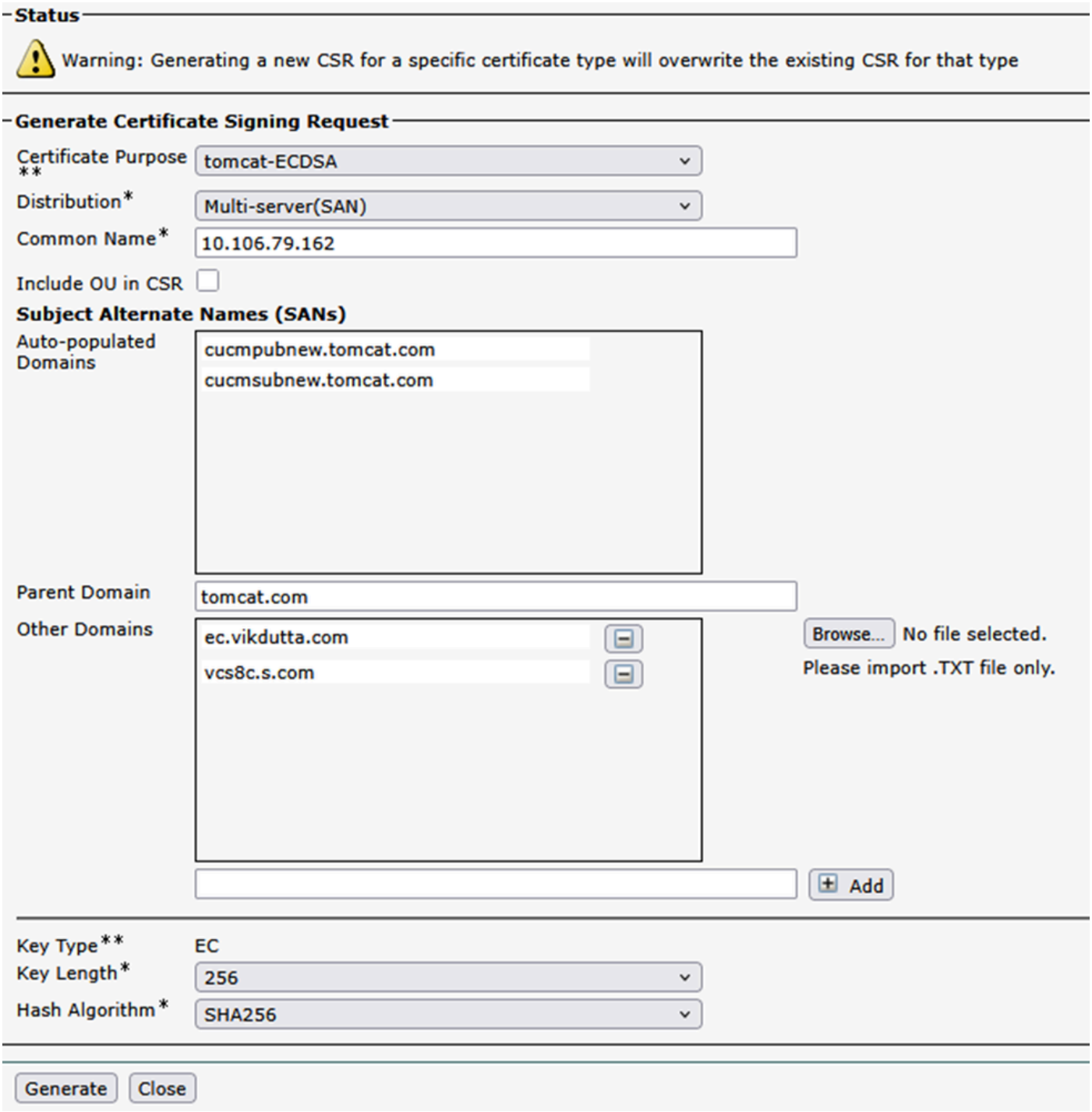
Führen Sie die gleichen Schritte für den Abonnenten aus.

Signieren Sie jetzt das ECDSA-Zertifikat, damit es als Callmanager-ECDSA wiederverwendet werden kann.

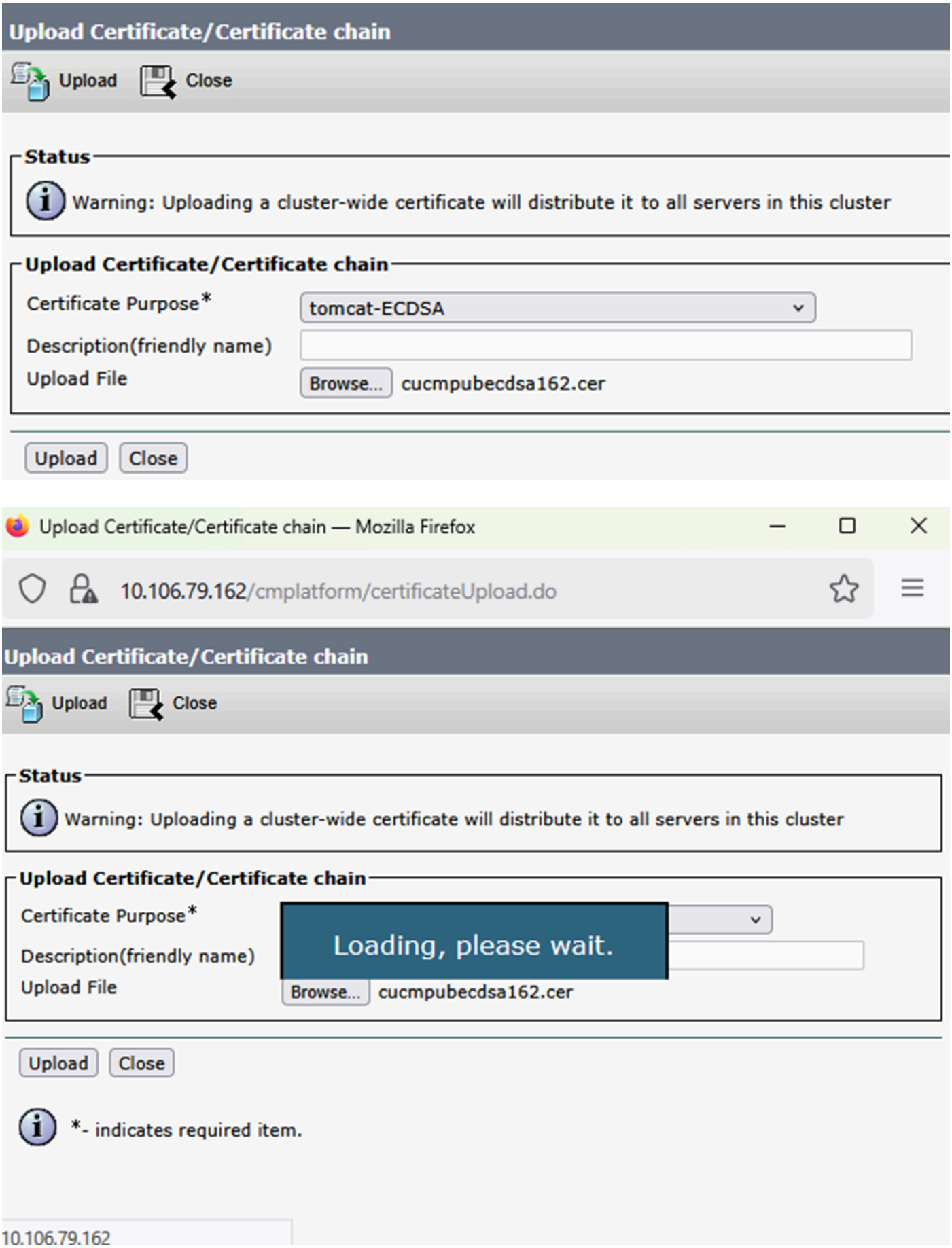
Das aktuelle Tomcat-ECDSA-Zertifikat ist selbstsigniert.

tomcat	10.106.79.162_5aceb67f00000000000f	Identity	CA-signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/25/2027	Certificate Signed by RICKY200-TMS-CA
tomcat-ECDSA	cucmpubnew-EC.tomcat.com_4b404cd202f54cabf8abdb8c15d4b	Identity	self-signed	EC	cucmpubnew.tomcat.com	cucmpubnew-EC.tomcat.com	10/23/2030	Self-signed certificate generated by system

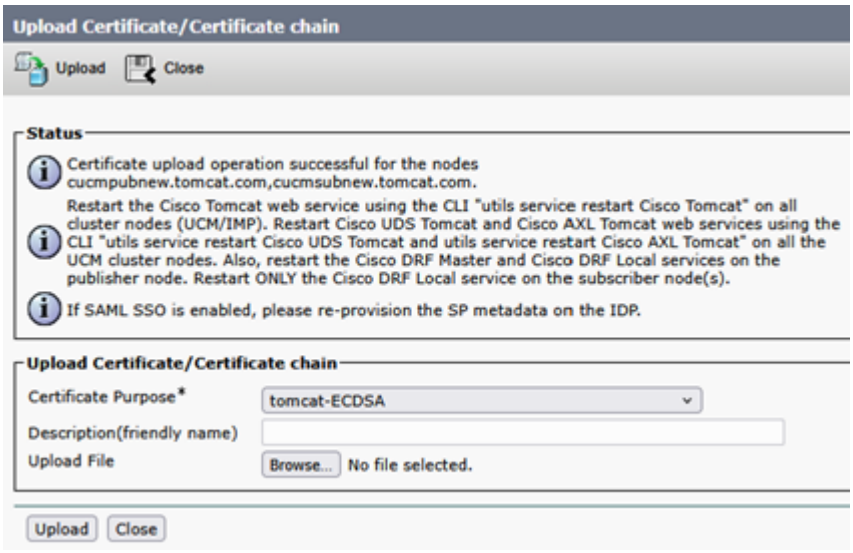
Unterzeichnen Sie das Tomcat-ECDSA-Zertifikat mit Multisan-CSR.



Signieren Sie das Zertifikat mit CSR, und laden Sie es hoch.

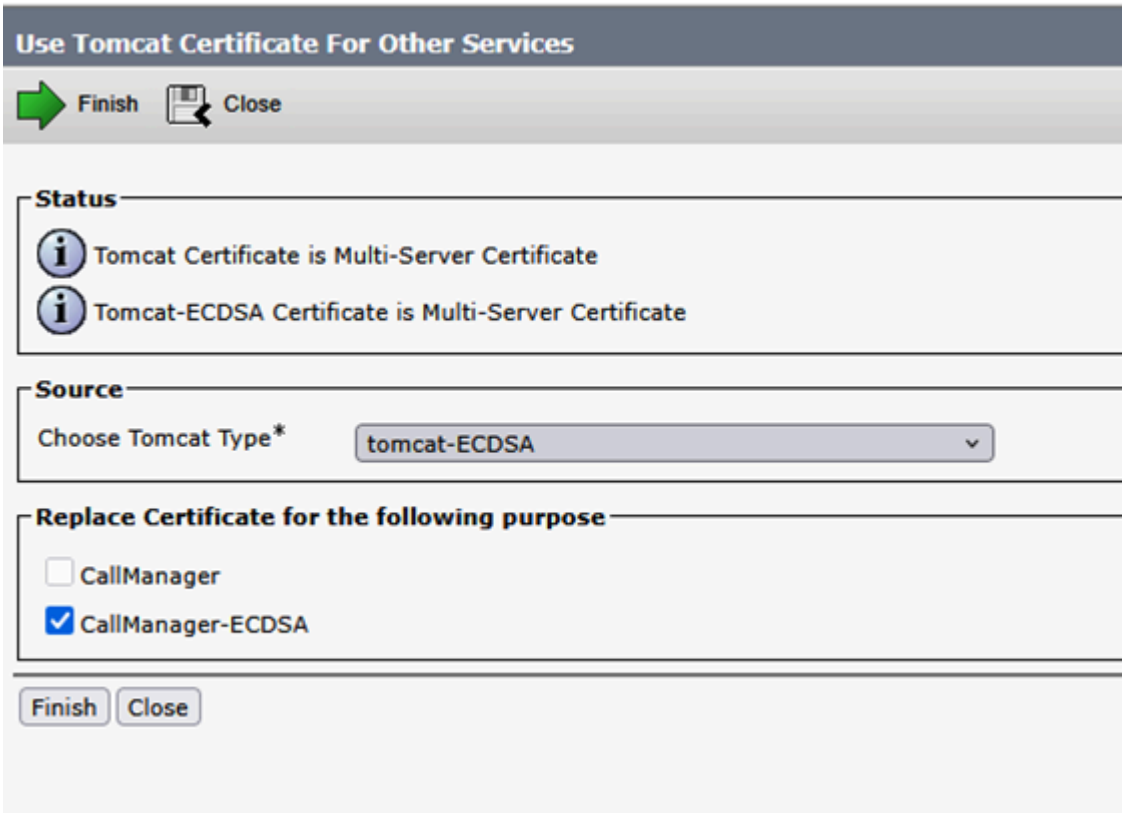


Upload erfolgreich. Starten Sie die entsprechenden Dienste nach Aufforderung neu.

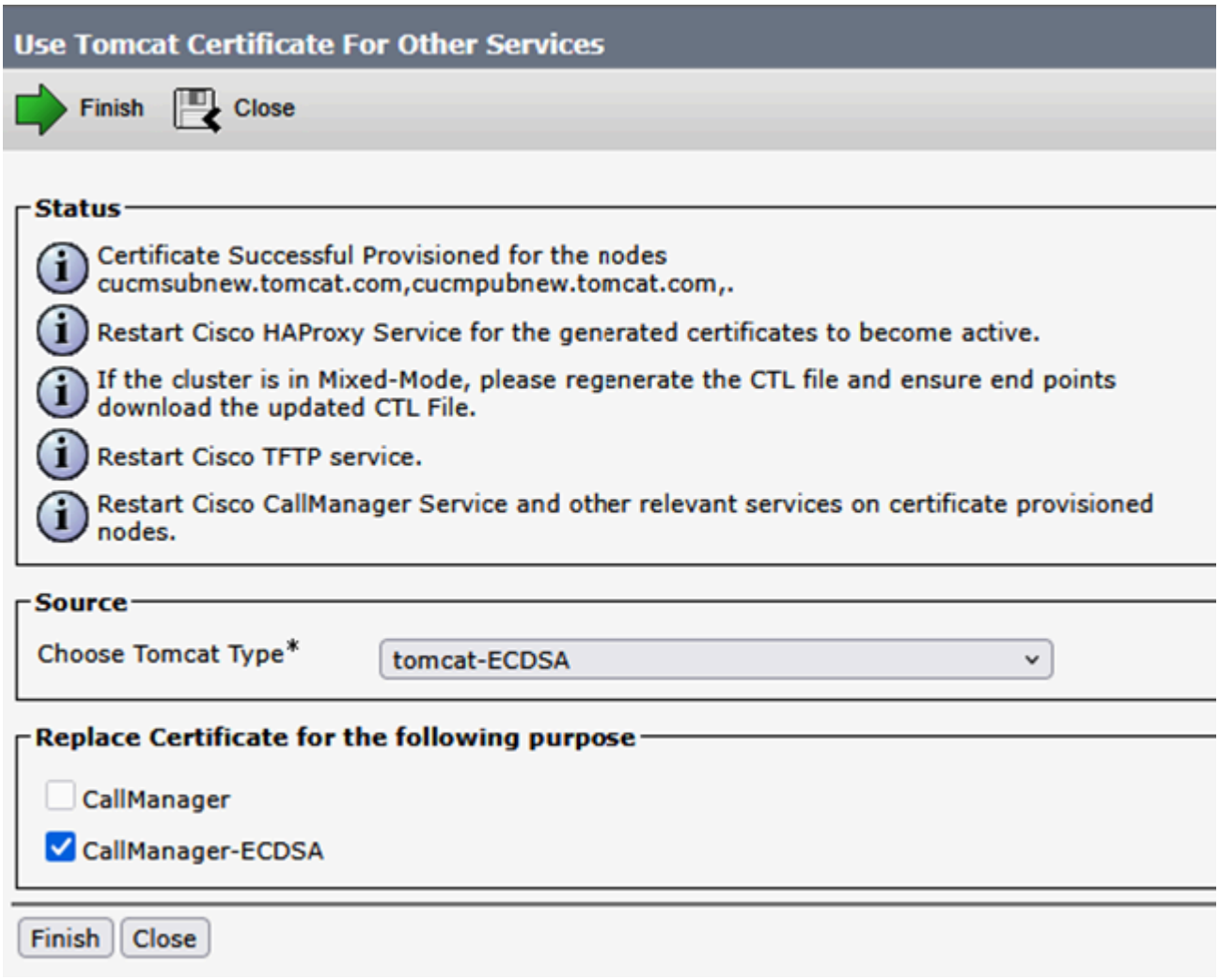


Tomcat und Tomcat-ECDSA von CA unterzeichnet.

Jetzt Tomcat-ECDSA als Callmanager-ECDSA-Zertifikat wiederverwenden.



Upload erfolgreich. Starten Sie die entsprechenden Services nach Aufforderung neu.



Überprüfen von Zertifikaten über die CLI

Callmanager-ECDSA-Zertifikat SN: 2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38

```
admin:show cert own CallManager-ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own CallManager-Ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own tomcat-ECDSA
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
        Validity
            Not Before: Oct 25 06:46:37 2025 GMT
            Not After : Oct 25 06:46:37 2026 GMT
```

Tomcat-ECDSA-Zertifikat SN: 2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38.

```
admin:show cert own tomcat-ECDSA
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
        Validity
            Not Before: Oct 25 06:46:37 2025 GMT
            Not After : Oct 25 06:46:37 2026 GMT
        Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-EC-ms.tomcat.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
```

Da Sie jetzt ein Zertifikat für zwei Dienste verwenden, d. h. Tomcat-Zertifikat für Tomcat- und Callmanager-Dienste sowie Tomcat-ECDSA für Tomcat-ECDSA- und Callmanager-ECDSA-Dienste, ist es weniger umständlich geworden, Zertifikate auf den Expressway Trust Store hochzuladen (falls hochgeladen werden muss).

TLS beim Hinzufügen von UCM zum Schnellstraßen-Core für MRA auf "On" prüfen zu lassen, war einfacher als je zuvor. Allein durch das Hinzufügen einer Tomcat-Zertifikat-CA oder eines Server-Zertifikats wird der Job erledigt (da das Zertifikat jetzt zwischen Callmanager und Tomcat-Dienst geteilt wird).

Wenn ein Upgrade auf x14.2 oder höher einen Ausfall für Mobile Remote Access verursacht hat, können Sie dieses umfassende Dokument auch zur Fehlerbehebung verwenden.

Apache Traffic Server - Versionsverlauf

Um die Version auf Ihrem Server zu überprüfen, melden Sie sich bei root an und führen ~ # /apache2/bin/httpd -v aus.

Expressway x8.11.4
Serverversion: Apache/2.4.34 (Unix)
Server erstellt: 12. November 2018 19:04:23

Expressway x12.6

Serverversion: Apache/2.4.43 (Unix)
Server erstellt: 26. Mai 2020 18:27:21 Uhr

Expressway x14.0.8

Serverversion: Apache/2.4.53 (Unix)
Server erstellt: 4. Mai 2022 08:52:57 Uhr

Expressway x15.3

Serverversion: Apache/2.4.62 (Unix)
Server erstellt: 16.07.2025 12:10:19

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.