Informazioni sui requisiti dei certificati di accesso remoto e mobile e sulla cronologia ATS

Sommario

Introduzione

In questo documento vengono descritti i requisiti di caricamento dei certificati in CUCM per l'accesso remoto e mobile.

Premesse

Cisco Expressway utilizza Apache Traffic Server (ATS). Il server del traffico è un componente molto importante nelle soluzioni traversal, utilizzato principalmente per queste funzionalità:

- Verifica certificato: Esegue la verifica dei certificati dei nodi server Cisco Unified Communications Manager (CUCM), IM & Presence e Unity per i servizi MRA.
- Proxy e memorizzazione nella cache: Funge da server proxy di cache veloce e scalabile per il traffico HTTP/HTTPS.

On Expressway versione 14.0.2

Traffic Server (ATS) inizia a vedere una leggera applicazione della 'verifica del certificato' quando parla con CUCM durante il provisioning MRA.

Il requisito è stato documentato in CSCvz45074 dove i certificati radice che hanno firmato i certificati del server Expressway Core devono essere caricati in CUCM come Tomcat-Trust e Callmanager Trust: https://cdetsng.cisco.com/summary/#/defect/CSCvz45074.

- Verifica certificato imposto dal server traffico.
- Prima di eseguire l'aggiornamento alla release X14.0.2, verificare che questo requisito del

certificato sia soddisfatto.

Requisito - La catena di Autorità di certificazione (CA) (radice + intermediario) che ha firmato il certificato Expressway-C deve essere aggiunta all'elenco di attendibilità tomcat-trust e CallManager-trust di CUCM, anche se Unified Communications Manager (UCM) è in modalità non protetta.

Motivo: il servizio server traffico di Expressway invia il proprio certificato ogni volta che un server UCM lo richiede. Queste richieste riguardano servizi in esecuzione su porte diverse da 8443 (ad esempio, porte 6971, 6972 e così via). In questo modo viene applicata la verifica del certificato anche se UCM è in modalità non protetta. Per ulteriori informazioni, vedere Mobile and Remote Access Through Expressway Deployment Guide.

Comportamento nelle versioni precedenti alla 14.0.8

Il server di traffico su Expressway-C che gestisce connessioni bidirezionali HTTPS sicure tra i nodi Expressway-C e Unified Communications non ha verificato il certificato presentato dall'estremità remota. Nella configurazione MRA è possibile impostare la verifica del certificato TLS impostando la modalità di verifica TLS su 'Attivata' quando si aggiungono server CUCM, IM&P o Unity in Configurazione > Unified Communications > Unified CM servers/IM and Presence Service nodes/Unity Connection servers. L'opzione di configurazione è mostrata nella schermata successiva, che indica che verifica il nome di dominio completo o l'indirizzo IP nella SAN, nonché la validità del certificato e se è firmato da una CA attendibile.

Si è inoltre verificato un problema noto in cui non è possibile caricare due certificati con lo stesso nome CN nell'archivio attendibilità di Expressway. Questa limitazione ha causato due problemi:

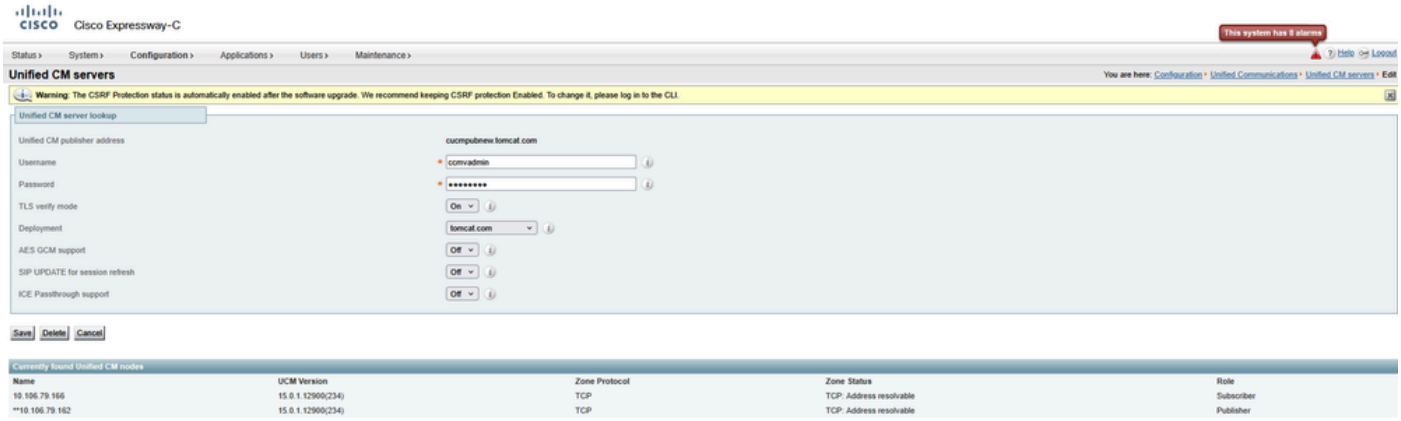
1. Se si sceglie di caricare il certificato del gestore chiamate nell'archivio attendibile di Expressway, la verifica TLS su 'On' non riuscirà durante l'aggiunta di CUCM.

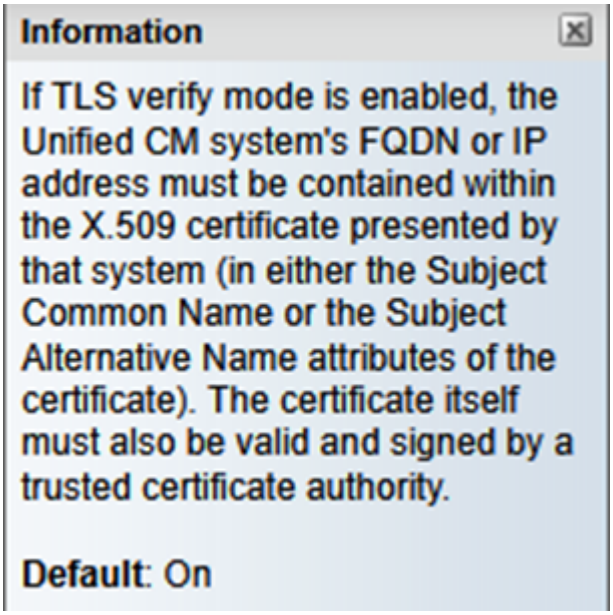
2: Se si sceglie di caricare il certificato Tomcat nell'archivio di Expressway Trust, le registrazioni sip sicure su 5061 avranno esito negativo.

Questo comportamento è documentato in CSCwa12894.

Inoltre, questo controllo di verifica del certificato TLS viene eseguito solo al rilevamento dei server CUCM/IM&P/Unity e non al momento del provisioning del client MRA.

Lo svuotamento di questa configurazione, è che la verifica solo per l'indirizzo dell'autore aggiunto. Non verifica se il certificato nei nodi del sottoscrittore è stato impostato correttamente in quanto recupera le informazioni sul nodo del sottoscrittore (FQDN o IP) dal database del nodo del server di pubblicazione.





Comportamento delle versioni 14.0.8 e successive

A partire dalla versione X14.0.8, il server Expressway esegue la verifica del certificato TLS per ogni singola richiesta HTTPS effettuata tramite il server di traffico. Ciò significa che viene eseguito anche quando la modalità di verifica TLS è impostata su 'Off' durante il rilevamento dei nodi CUCM/IM&P/Unity. Se la verifica non ha esito positivo, l'handshake TLS non viene completato e la richiesta non riesce. Ciò può causare, ad esempio, la perdita di funzionalità quali ridondanza, problemi di failover o errori di accesso completi. Inoltre, se la modalità di verifica TLS è impostata su 'On', non è possibile garantire che tutte le connessioni funzionino correttamente come descritto nell'esempio seguente.

I certificati esatti che Expressway controlla verso i nodi CUCM/IM&P/Unity sono indicati nella sezione della guida MRA.

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

Sezione

Requisiti certificato > Requisiti per lo scambio di certificati

A causa di questi cambiamenti nelle modalità di comunicazione tra Expressway-Core e CUCM, è necessario garantire che:

1. È consigliabile utilizzare certificati firmati dall'autorità di certificazione per l'accesso remoto e mobile.

2. Ogni cluster di Gestione certificati unificata deve considerare attendibile il certificato Expressway-C. Per ogni cluster, verificare quanto segue:

- Se è attivata la modalità mista, il certificato Expressway-C deve essere installato nell'archivio CallManager-trust e Tomcat-trust in Unified CM.
- Se la modalità mista è disattivata, il certificato CA radice che firma il certificato Expressway-C deve essere installato nell'archivio CallManager-Trust e Tomcat-trust in Unified CM. Quindi, riavviare quanto segue: · Servizio Tomcat · Servizio CallManager · Servizio proxy HA (se si utilizza TLS su Tomcat).

Su Expressway - Core, assicurarsi che vengano intraprese le seguenti azioni:

- Expressway-C deve considerare attendibili i certificati presentati da ogni cluster di Gestione certificati unificata, Messaggistica immediata e Servizio presenza.

L'archivio di attendibilità di Expressway-C deve includere il certificato CA radice che firma i certificati dei servizi di messaggistica unificata, di messaggistica immediata e di presenza per tutti i cluster UC.

Nota: Accertarsi di aggiungere tutti i certificati CA radice e intermedi o la catena di CA completa utilizzata per firmare il certificato Expressway-C all'elenco di attendibilità Tomcat e CallManager di Cisco Unified Communications Manager (UCM), anche se UCM funziona in modalità non protetta.

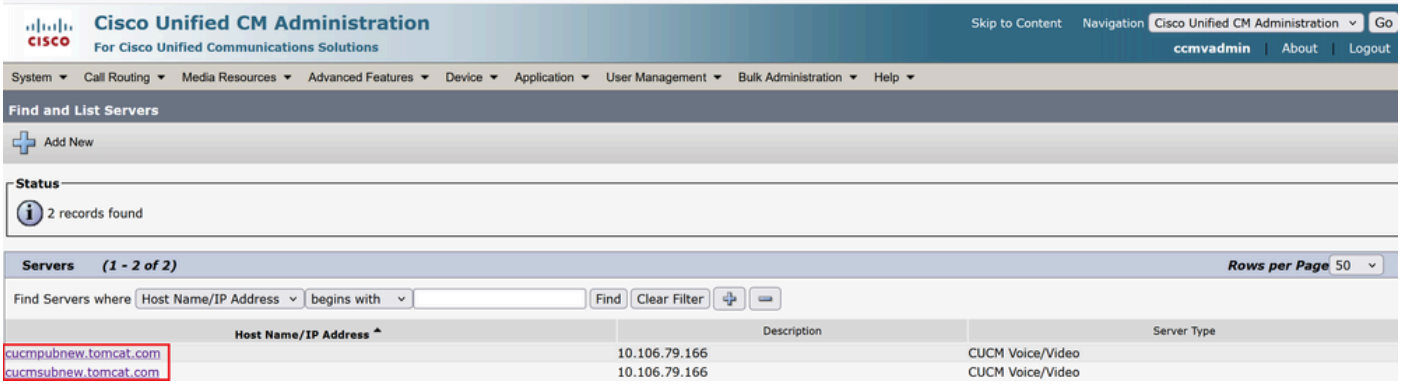
Motivo: il servizio server traffico di Expressway invia il proprio certificato ogni volta che un server (UCM) lo richiede. Queste richieste riguardano servizi in esecuzione su porte diverse da 8443 (ad esempio, porte 6971, 6972 e così via). In questo modo viene applicata la verifica del certificato anche se UCM è in modalità non protetta.

Il modo in cui l'indirizzo CUCM viene aggiunto in Sistema > Server svolge un ruolo molto importante nell'aggiunta di CUCM/IMP sul core Expressway in Configurazione > Unified Communications > Unified CM servers/IM e nodi del servizio di presenza.

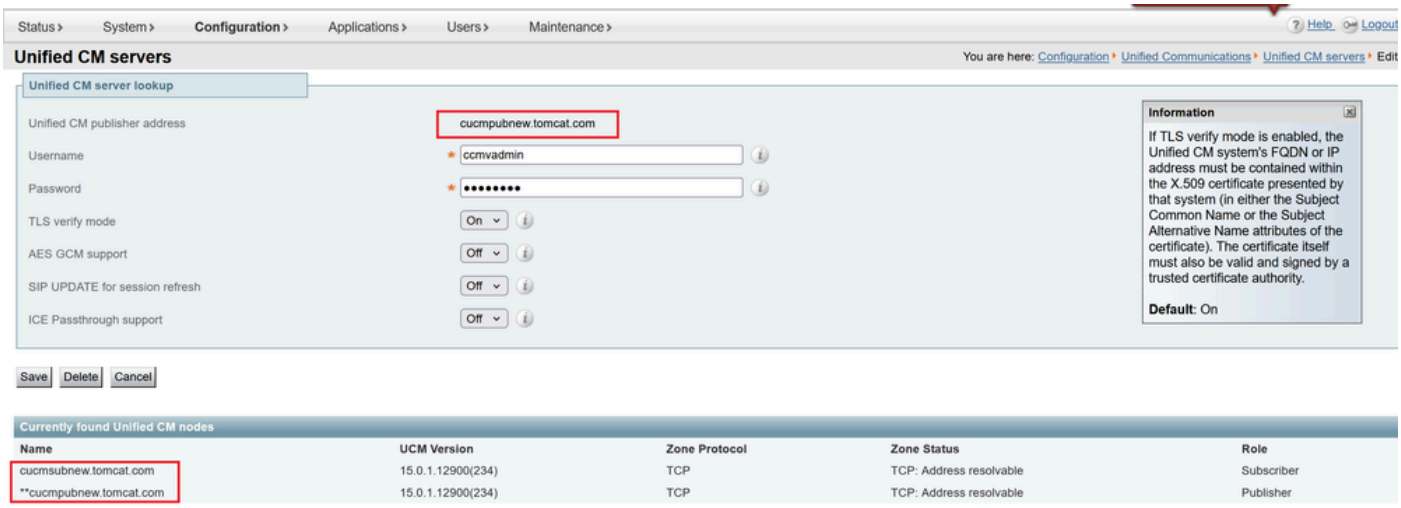
CUCM deve essere sempre aggiunto con FQDN e non con nome host o indirizzo IP. Se viene visualizzato che CUCM è stato aggiunto in Sistema > Server come nome host/indirizzo IP

durante l'handshake TLS, la verifica TLS 'On' non riuscirà e il cluster CUCM non verrà aggiunto in Expressway-Core.

La figura mostra CUCM aggiunto come nome host:



Nella figura viene illustrato il CUCM aggiunto in Expressway-Core con FQDN con modalità di verifica TLS = ON:

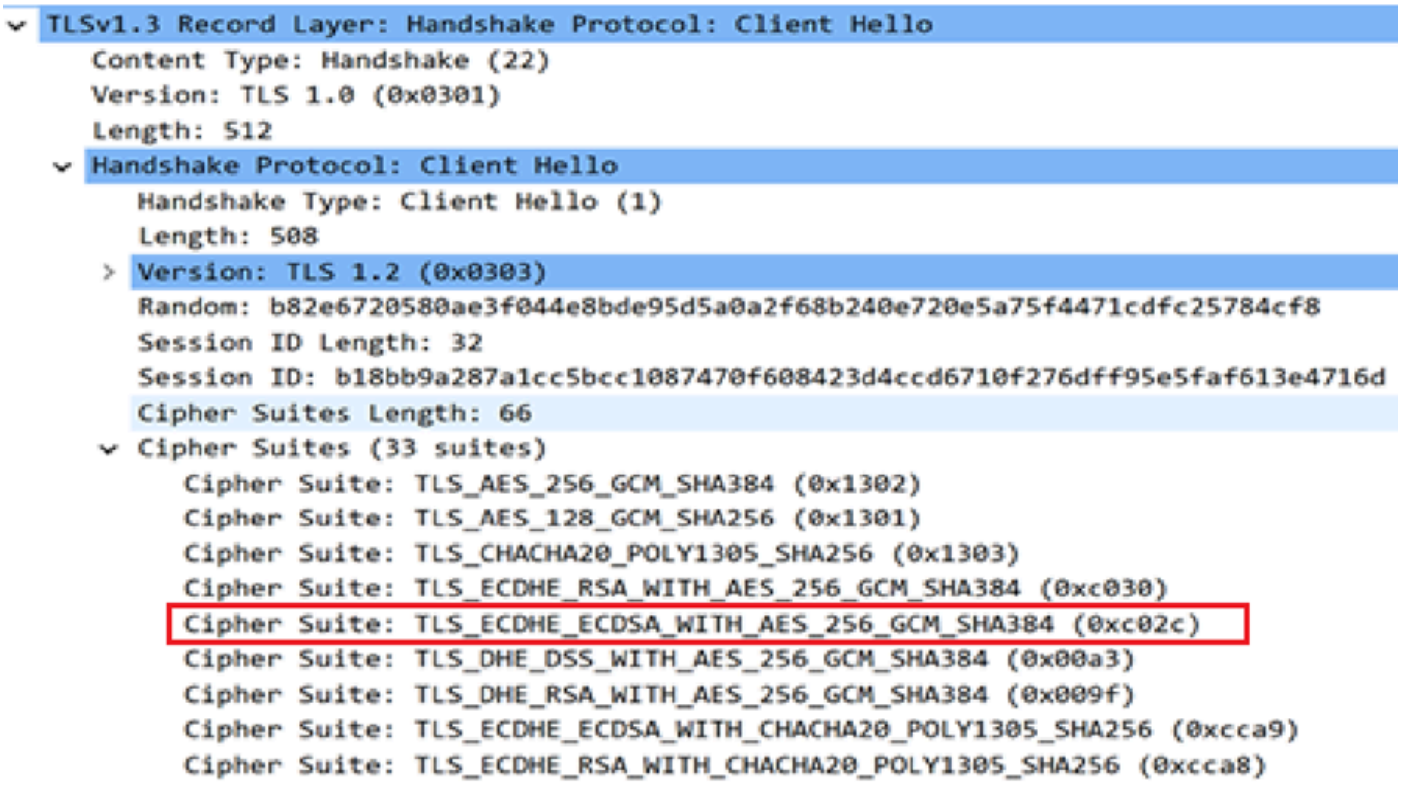


C'è stata anche una modifica introdotta in X14.2 che presenterà i cifrari durante un handshake TLS (saluto client) in ordine di preferenza diverso. Ciò dipende dal percorso di aggiornamento e ha causato connessioni TLS impreviste dopo un aggiornamento del software. È possibile che prima dell'aggiornamento durante l'handshake TLS, sia stato richiesto il certificato Cisco Tomcat o Cisco CallManager da CUCM. Tuttavia, dopo l'upgrade, ha richiesto la variante ECDSA (che è la variante più sicura di RSA). I certificati Cisco Tomcat-ECDSA o Cisco CallManager-ECDSA possono essere firmati da un'autorità di certificazione diversa o solo da certificati autofirmati (impostazione predefinita).

La modifica dell'ordine delle preferenze di cifratura non è sempre rilevante in quanto dipende dal percorso di aggiornamento, come illustrato nelle note di rilascio di Expressway X14.2.1. In breve, è possibile vedere da Manutenzione > Sicurezza > Cifre per ciascuno degli elenchi di cifratura se precede o meno ECDHE-RSA-AES256-GCM-SHA384. In caso contrario, preferisce la cifratura ECDSA più recente a quella RSA. In caso affermativo, si avrà il comportamento precedente di RSA che ha la preferenza più alta.

La schermata successiva mostra in rosso la cifratura ECDSA annunciata da Expressway core durante il messaggio di negoziazione TLS in Salve client, #IF TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 viene scelto da CUCM (Remote responder) in Salve server, quindi la negoziazione TLS avrà esito negativo se:

In questo caso, i certificati CA RADICE o i certificati effettivi ECDSA del risponditore, ovvero CUCM non è installato nell'archivio di Expressway Trust.



In alternativa, è possibile modificare i cifrari Expressway in modo che ECDSA non abbia la precedenza.

1. Modificare la cifratura SIP aggiungendo la stringa SSL aperta GCM-Sha384.

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

2. Aggiungere + per spostare la cifratura all'ultima preferenza o aggiungere ! per disabilitare l'ECDSA in modo permanente.

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

3. Aggiungere il certificato CA radice e intermedio che ha firmato il certificato ECDSA in CUCM o aggiungere il certificato Tomcat-ECDSA nell'archivio di attendibilità di Expressway (in alcuni casi).

Tuttavia, a causa della modifica nella precedenza delle cifrature, dopo l'aggiornamento, le distribuzioni MRA possono interrompersi, quindi TAC dovrà eseguire la soluzione descritta in precedenza per far funzionare di nuovo le cose.

Con l'introduzione di TLS 1.3, diventa ancora più difficile controllare quali certificati vengono scambiati in wireshark.

Comportamento delle versioni x15.3

Solo per l'interfaccia SIP, è possibile scegliere di utilizzare la cifratura RSA o ECDSA.

Con X15.x è stato applicato TLS 1.3. Come visto sul campo, l'algoritmo RSA è scelto principalmente su ECDSA. I clienti che eseguono l'aggiornamento a x15.2 possono scegliere

tra l'algoritmo RSA e l'algoritmo ECDSA con questo set di comandi:

xConfiguration SIP Advanced TlsSignatureAlgoPrefRsa: On/Off

TlssignatureAlgoPrefRSA funziona solo se l'interfaccia SIP ha TLS 1.3

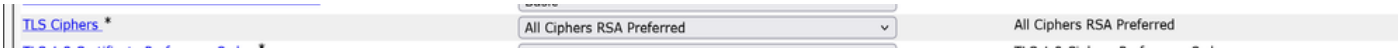
xConfiguration SIP Advanced SipTlsVersioni: "TLSv1.3"

Nota: Questa funzionalità è disponibile per l'interfaccia SIP solo a partire da ora. Le considerazioni su Traffic Server e Tomcat su 8443 rimangono invariate come documentato in precedenza.

Le tute da cifratura inviate da Expressway a CUCM durante il "saluto del cliente" saranno quelle mostrate quando si sceglie RSA.

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

La configurazione precedente funzionerà in tandem sulla configurazione scelta da CUCM a cifratura TLS in Parametri Enterprise > Parametri di sicurezza.



Inoltre, è importante notare che durante un handshake TLS interrotto su TLS 1.3 tra Expressway-C e CUCM, gli errori stampati nei log diagnostici o PCAP non sono molto utili. È opportuno attivare questi debug durante l'utilizzo di TAC, in modo che il componente stampi gli errori chiari per la risoluzione dei problemi.

Developer Developer.trafficserver.http Livello: "DEBUG"
Sviluppatore xConfiguration Logger.trafficserver.http_trans Livello: "DEBUG"
Sviluppatore xConfiguration Logger.trafficserver.iocore Livello: "DEBUG"
Sviluppatore xConfiguration Logger.trafficserver.ssl Livello: "DEBUG"

Cosa aspettarsi quando Callmanager condivide un certificato con più servizi

Le cose cambiano leggermente con il riutilizzo del certificato su CUCM.

A partire dalla versione 14.0 di CUCM, è possibile riutilizzare i certificati Tomcat e Tomcat ECDSA come Call Manager e Call Manager ECDSA.

Il certificato Tomcat può essere riutilizzato come certificato di Callmanager.

Il certificato Tomcat-ECDSA può essere riutilizzato come certificato Callmanager-ECDSA.

Questo rende la vita facile.

1. Più servizi su CUCM ora utilizzano un solo certificato, che riduce il costo del certificato.

2. Minore gestione dei certificati.

3. Se è necessario caricare un certificato Tomcat/Callmanager o Tomcat-ECDSA/Callmanager-ECDSA (per qualsiasi motivo) su un trust store Expressway-Core, si tratta di un unico certificato da caricare. Non vi saranno problemi relativi allo stesso problema con il nome CN (descritto in precedenza in questo documento).

Nota: Il riutilizzo del certificato verrà eseguito solo quando Tomcat e Tomcat-ECDSA sono certificati multisan.

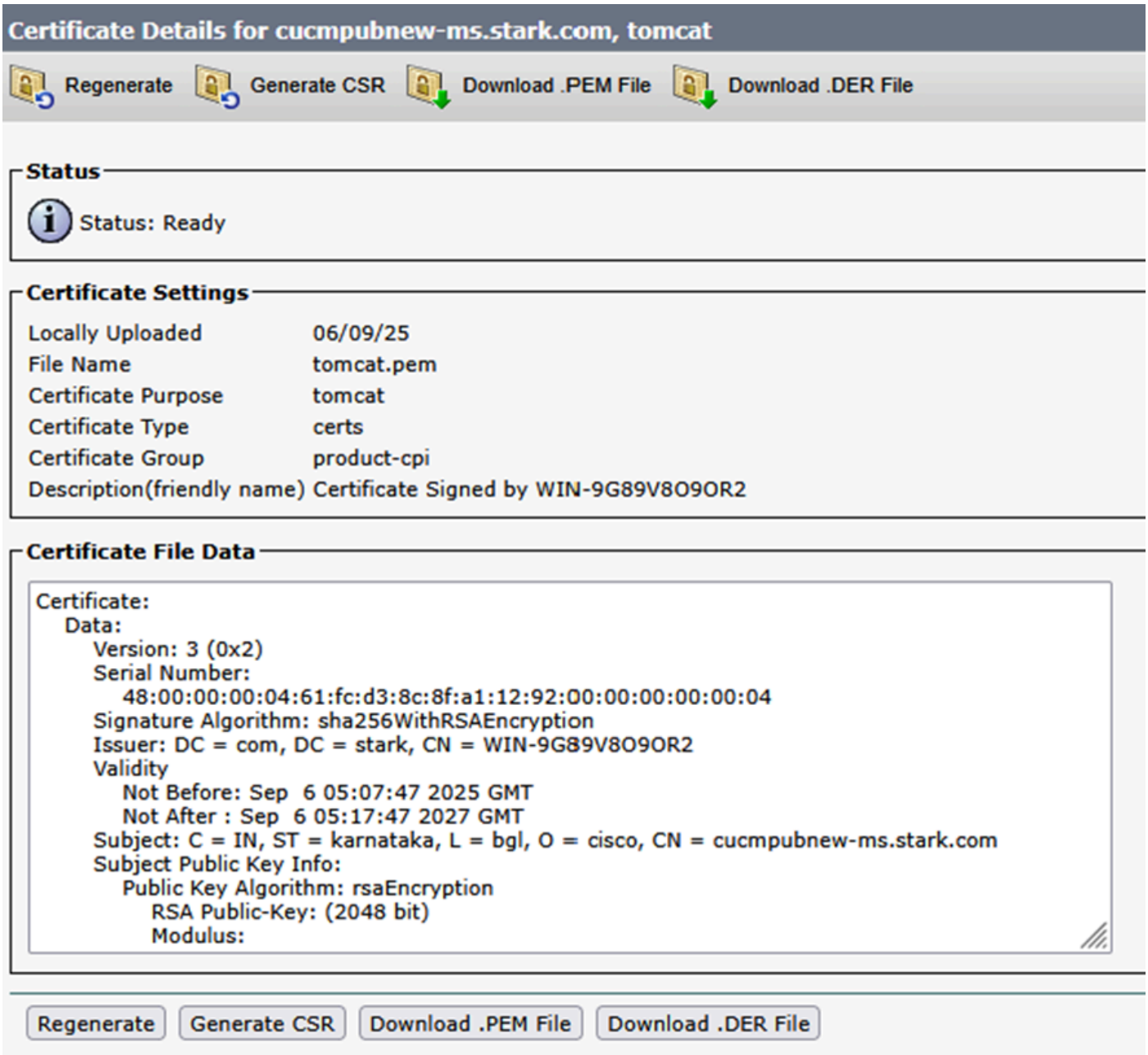
I certificati server ECDSA Post-Reuse, Callmanager e Callmanager non sono visibili nell'archivio di attendibilità CUCM. È possibile convalidare il riutilizzo dei certificati dalla CLI eseguendo i seguenti comandi:

mostra certificato proprio CallManager

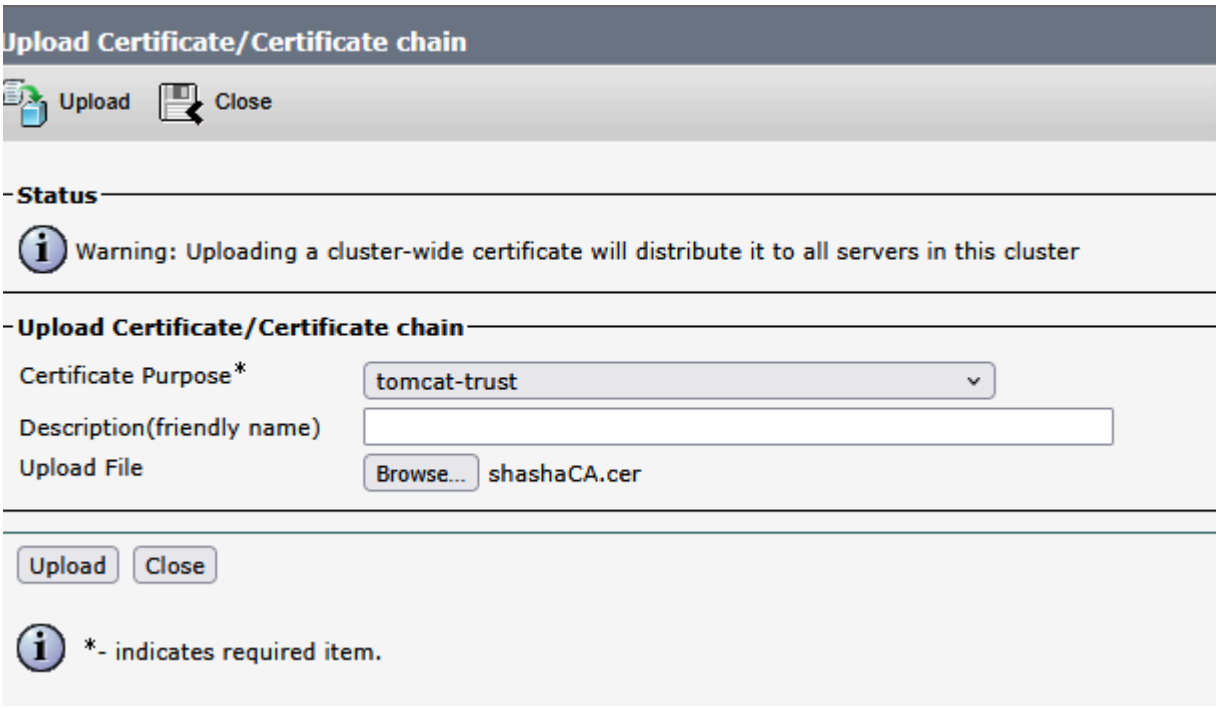
mostra il proprio gatto

Passaggi per il riutilizzo del certificato

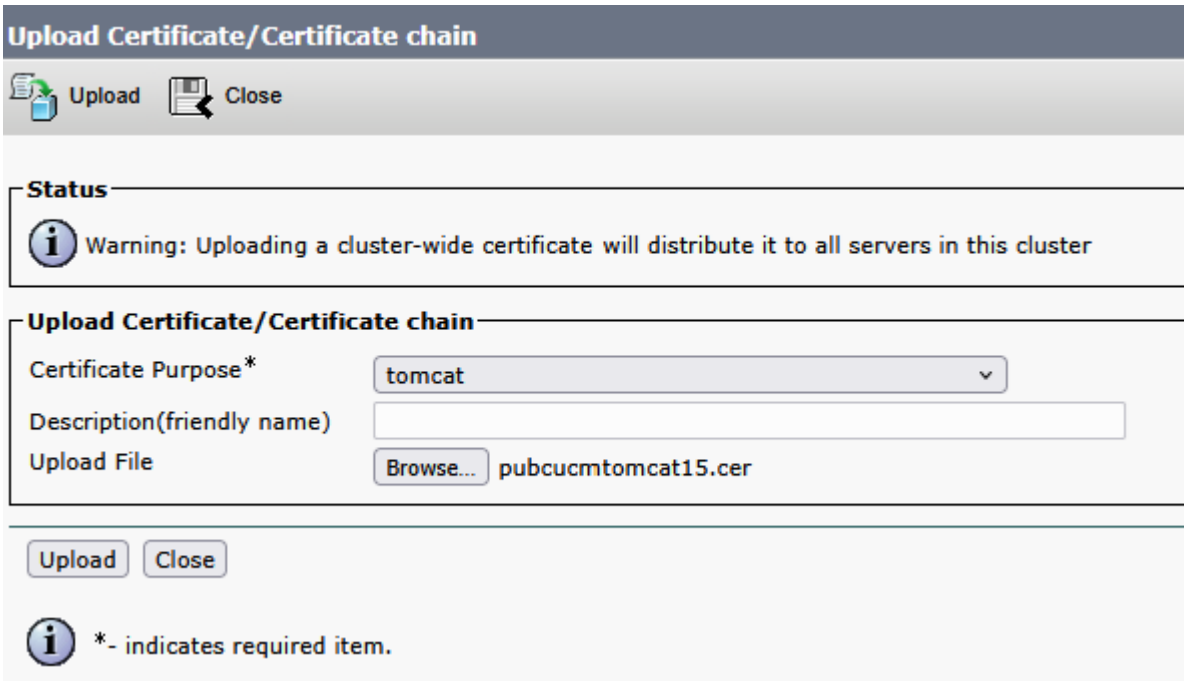
Generazione di Tomcat CSR pub add.



Caricare il certificato CA che firmerà il certificato Tomcat su CUCM come Tomcat-trust.



Una volta firmato il certificato Tomcat, caricalo sul publisher. Riavviare i servizi pertinenti come richiesto.



Una volta firmato il certificato Tomcat, caricalo sul publisher. Riavviare i servizi pertinenti come richiesto.

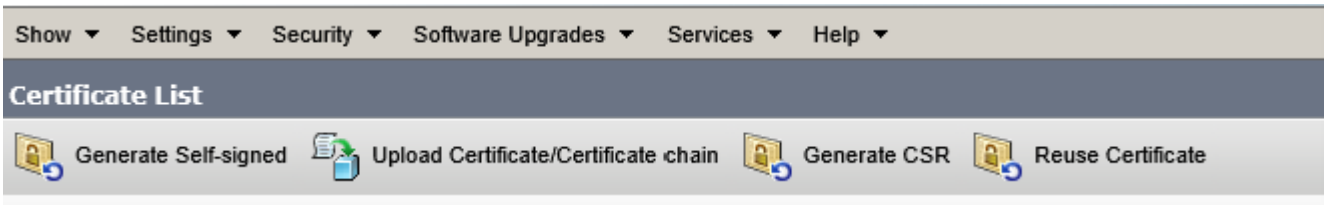
Operazione completata: Certificato caricato. Eseguire un backup di ripristino di emergenza in modo che l'ultimo backup contenga il certificato caricato.
Riavviare il servizio Web Cisco Tomcat usando il comando 'utils service restart Cisco Tomcat' su tutti i nodi del cluster (UCM/IMP) della CLI. Riavviare i servizi Web Cisco UDS Tomcat e Cisco

AXL Tomcat utilizzando il comando CLI 'utils service restart Cisco UDS Tomcat and utils service restart Cisco AXL Tomcat' su tutti i nodi del cluster UCM. Inoltre, riavviare i servizi Cisco DRF Master e Cisco DRF Local sul nodo del server di pubblicazione. Riavviare solo il servizio Cisco DRF Local sui nodi del sottoscrittore.

Certificato Tomcat firmato dalla CA.

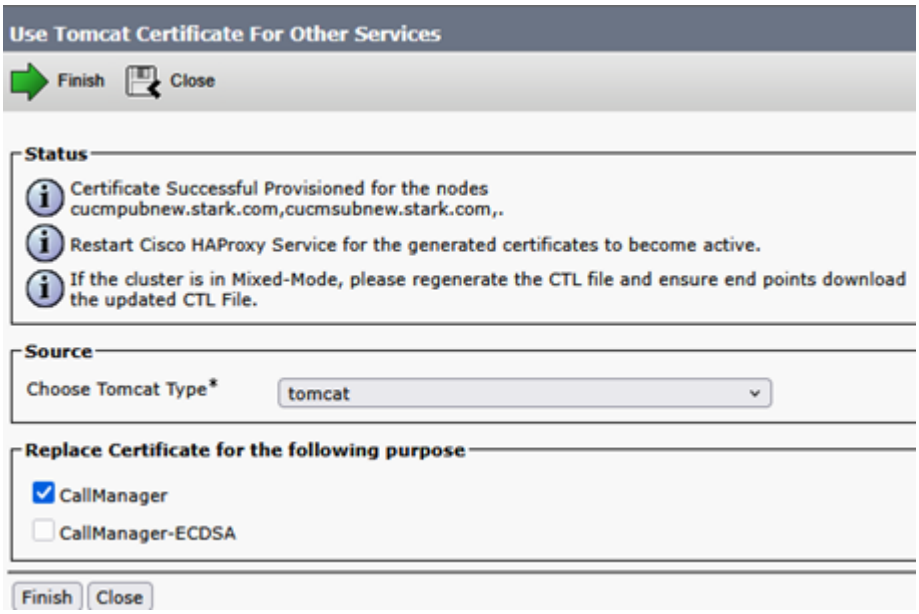
Per riutilizzare il certificato Tomcat come certificato del gestore chiamate.

Fare clic su Riutilizza certificato.



Scegliere Tomcat nell'elenco a discesa e controllare il certificato di Callmanager.

Fare clic su Finish (Fine).



Il certificato Tomcat è ora riutilizzato come certificato di Callmanager. È possibile convalidare questa condizione dalla CLI.

Numero di serie (SN) del certificato del gestore chiamate: 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
```

Numero di serie certificato Tomcat: 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
```

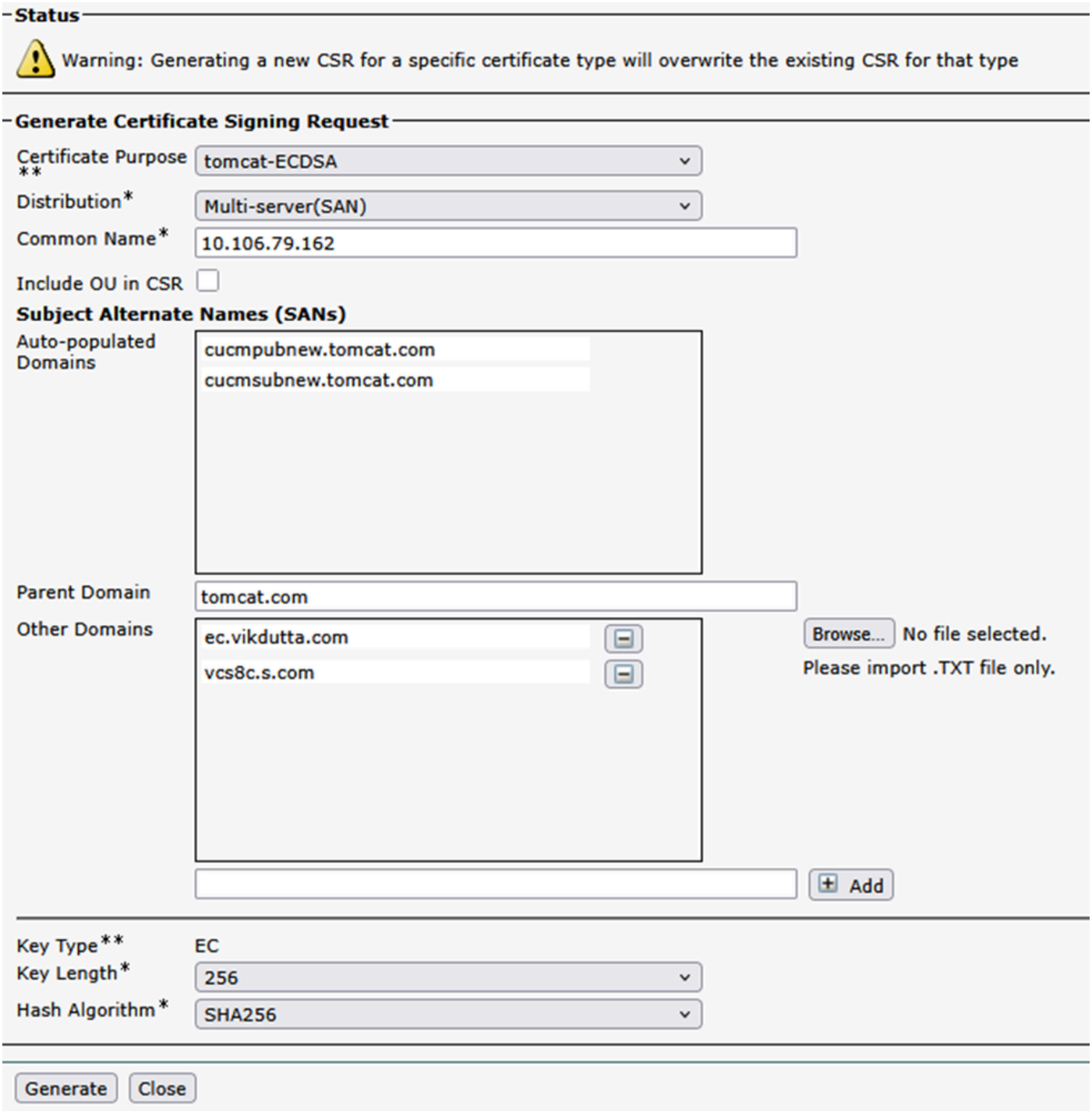
Eseguire la stessa procedura nel Sottoscrittore.

Firma ora il certificato ECDSA in modo che possa essere riutilizzato come Callmanager-ECDSA.

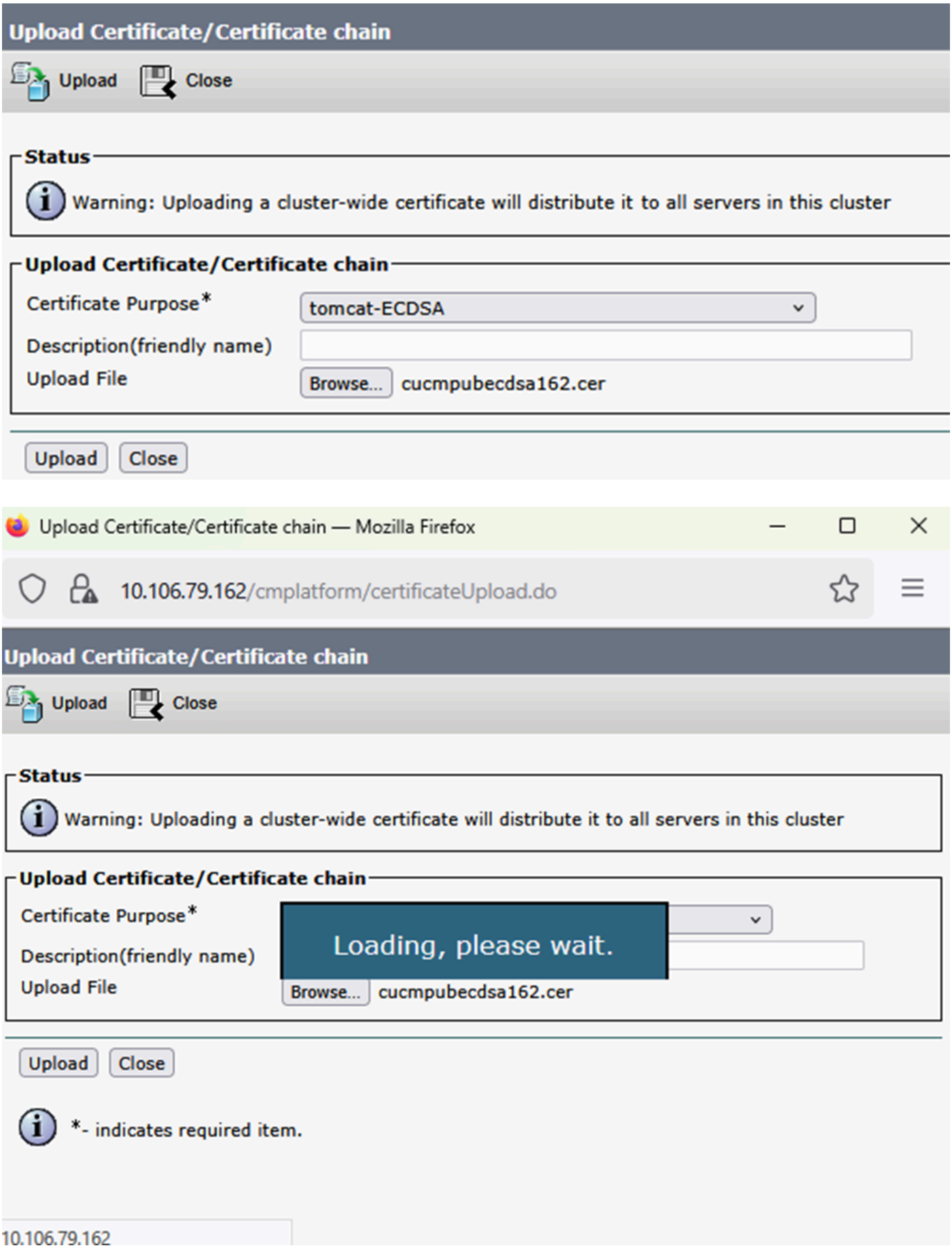
Il certificato Tomcat-ECDSA corrente è autofirmato.

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_4b404cd202f547cabf8a6db78c715d46	Identity	self-signed	EC	cucmpubnew.tomcat.com	cucmpubnew-EC.tomcat.com	10/23/2030	Self-signed certificate generated by system

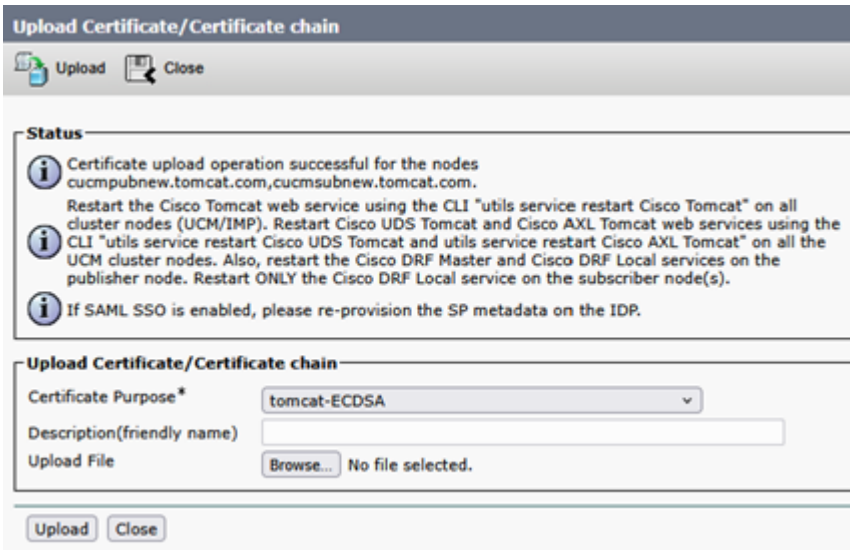
Firma CSR multisan per certificato Tomcat-ECDSA.



Firmare il certificato utilizzando CSR e caricarlo.

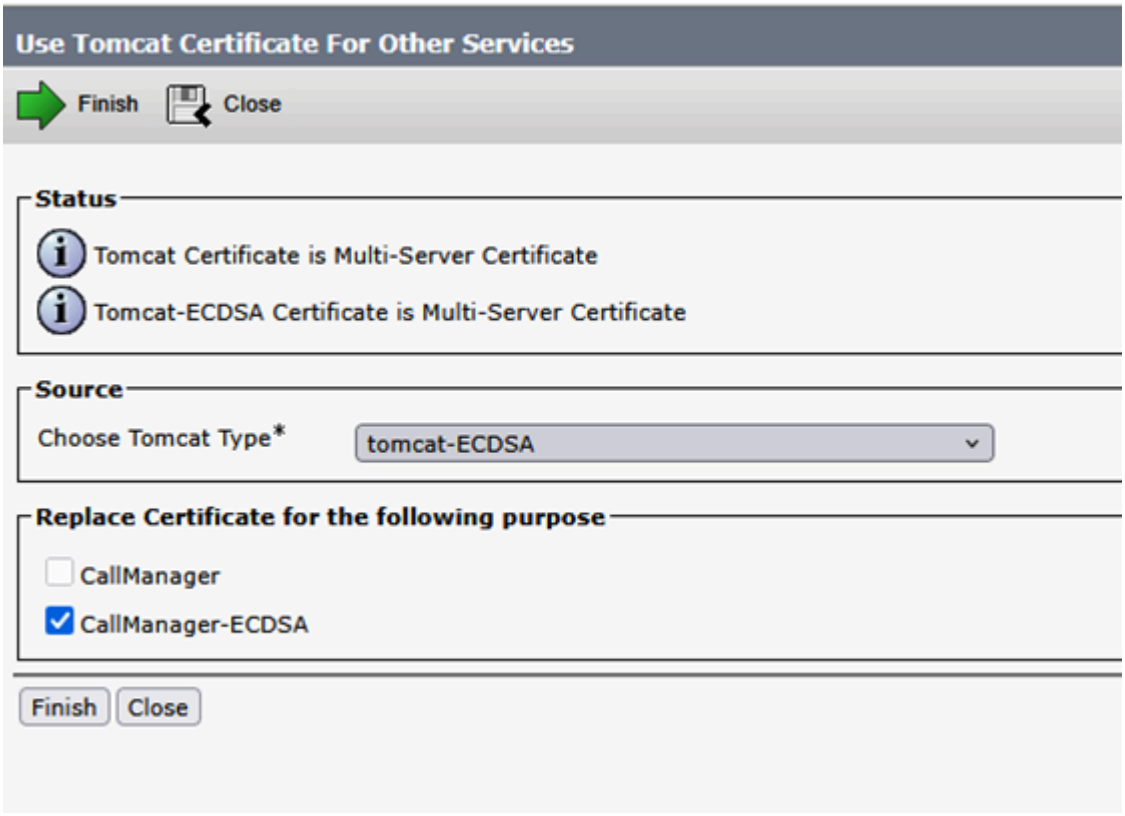


Caricamento completato. Riavviare i servizi pertinenti come richiesto.

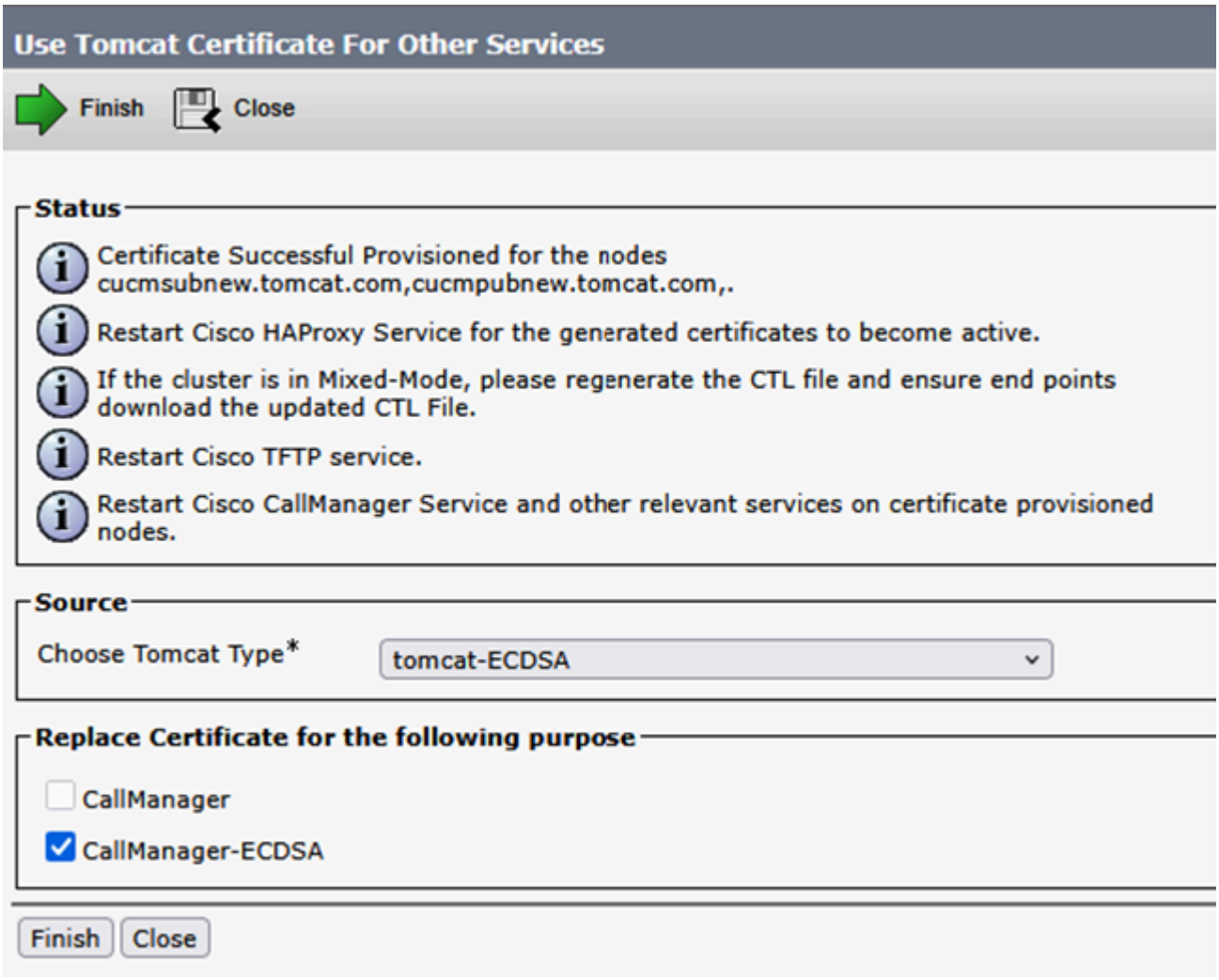


Tomcat e Tomcat-ECDSA firmati da CA.

Ora riutilizzare Tomcat-ECDSA come certificato Callmanager-ECDSA.



Caricamento completato. Riavviare i servizi pertinenti come richiesto.



Verificare i certificati dalla CLI.

Numero di serie certificato Callmanager-ECDSA:
2f: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
```

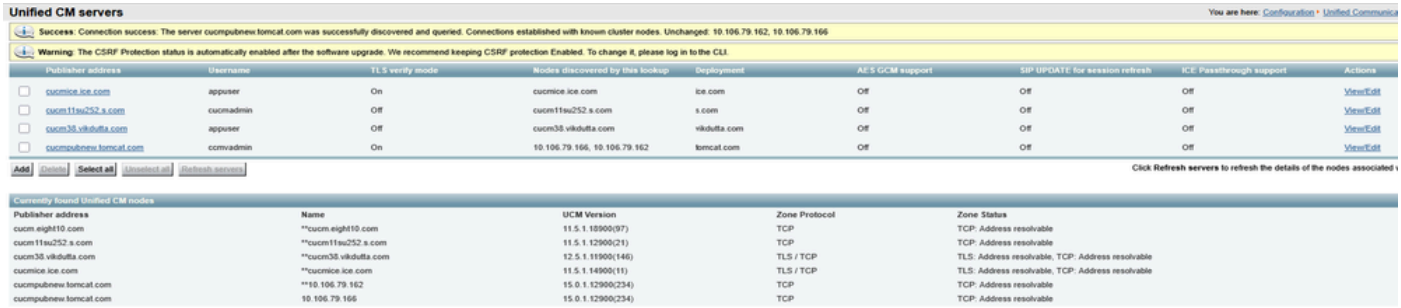
Numero di serie del certificato Tomcat-ECDSA:

2f: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)
```

Poiché si sta utilizzando un certificato per due servizi, ovvero il certificato Tomcat per i servizi Tomcat e Callmanager e il certificato Tomcat-ECDSA per i servizi Tomcat-ECDSA e Callmanager-ECDSA, è diventato meno complicato caricare i certificati nell'archivio attendibile di Expressway (se necessario, caricarli).

Avere TLS verificato 'On' durante l'aggiunta di UCM su expressway-core per MRA, è stato più facile che mai. Solo aggiungendo un certificato Tomcat CA o un certificato server eseguirà il processo (perché il certificato è ora condiviso tra Callmanager e il servizio Tomcat).



Se l'aggiornamento a x14.2 o versioni successive ha causato un'interruzione dell'accesso remoto mobile, è inoltre possibile consultare questo documento completo per la risoluzione del problema.

Cronologia versioni server traffico Apache

Per controllare la versione presente sul server di accesso alla directory principale ed eseguire ~ # /apache2/bin/httpd -v.

Expressway x8.11.4
Versione server: Apache/2.4.34 (Unix)
Creazione server: 12 nov 2018 19:04:23

Expressway x12.6

Versione server: Apache/2.4.43 (Unix)
Creazione server: 26 mag 2020 18:27:21

Expressway x14.0.8

Versione server: Apache/2.4.53 (Unix)
Creazione server: 4 maggio 2022 08:52:57

Expressway x15.3

Versione server: Apache/2.4.62 (Unix)
Creazione server: 16 lug 2025 12:10:19

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).