

# Crea nuovi certificati da certificati CA firmati

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Informazioni pre-controllo](#)

[Configurazione e rigenerazione di certificati](#)

[Certificato Tomcat](#)

[Certificato CallManager](#)

[Certificato IPsec](#)

[Certificato CAPF](#)

[Certificato TV](#)

[Risoluzione dei problemi relativi ai messaggi di errore dei certificati caricati comuni](#)

[Il certificato CA non è disponibile nell'archivio attendibile](#)

[Il file /usr/local/platform/security/tomcat/keys/tomcat.csr non esiste](#)

[Chiave pubblica CSR e chiave pubblica del certificato non corrispondenti](#)

[Il nome alternativo del soggetto \(SAN\) CSR e la SAN del certificato non corrispondono](#)

[Certificati di attendibilità con lo stesso CN non sostituiti](#)

---

## Introduzione

In questo documento viene descritto come rigenerare i certificati firmati da un'Autorità di certificazione (CA) in Cisco Unified Communications Manager (CUCM).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Strumento di monitoraggio in tempo reale (RTMT)
- Certificati CUCM

### Componenti usati


- CUCM release 10.x, 11.x e 12.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

## Informazioni pre-controllo

---

-  Nota: per la rigenerazione dei certificati autofirmati, vedere la [Guida alla rigenerazione dei certificati](#). Per la rigenerazione di certificati multi-SAN con firma CA, consultare la [Guida alla rigenerazione di certificati multi-SAN](#)
- 

Per informazioni sull'impatto di ogni certificato e sulla sua rigenerazione, consultare la [Guida alla rigenerazione autofirmata](#).

Ogni tipo di richiesta di firma del certificato (CSR) ha utilizzi chiave diversi e quelli sono richiesti nel certificato firmato. La [Security Guide](#) include una tabella con gli utilizzi chiave richiesti per ogni tipo di certificato.

Per modificare le impostazioni dell'oggetto (Località, Stato, Unità organizzativa e così via), eseguire questo comando:

- `set web-security orgunit orgname locality state [country] [alternatehostname]`

Il certificato Tomcat viene rigenerato automaticamente dopo l'esecuzione del `set web-security` comando. Il nuovo certificato autofirmato non viene applicato a meno che il servizio Tomcat non venga riavviato. Per ulteriori informazioni sul comando, consultare le seguenti guide:


- [Guida di riferimento per la riga di comando](#)
- [Link alle fasi della Cisco Community](#)
- [Video](#)

## Configurazione e rigenerazione di certificati

Per ogni tipo di certificato vengono elencati i passaggi per la rigenerazione dei certificati a nodo singolo in un cluster CUCM firmato da una CA. Non è necessario rigenerare tutti i certificati nel cluster se non sono scaduti.

### Certificato Tomcat

---

-  **Attenzione:** verificare che SSO sia disabilitato nel cluster (**CM Administration > System > SAML Single Sign-On**). Se SSO è abilitato, deve essere disabilitato e quindi abilitato una volta completato il processo di rigenerazione dei certificati Tomcat.
- 

In tutti i nodi (CallManager e IM&P) del cluster:

Passaggio 1. Passare alla **Cisco Unified OS Administration > Security > Certificate Management > Find data di scadenza del certificato Tomcat** e verificarla.

Passaggio 2. Fare clic su **.Generate CSR > Certificate Purpose: tomcat** Selezionare le impostazioni desiderate per il certificato, quindi fare clic su **Generate**. Attendere che venga visualizzato il messaggio di operazione riuscita e fare clic su **Close**.

**Generate Certificate Signing Request**

Generate Close

**Status**

Success: Certificate Signing Request Generated

**Generate Certificate Signing Request**

Certificate Purpose\* tomcat

Distribution\* 115pub

Common Name\* 115pub

**Subject Alternate Names (SANs)**

Parent Domain

Key Type\* RSA

Key Length\* 2048

Hash Algorithm\* SHA256

Generate Close

\*- indicates required item.

\*- \*When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Passaggio 3. Scaricare il CSR. Fare clic su **Download CSR**, selezionare **Certificate Purpose: tomcat**, e fare clic su **Download**.

**Download Certificate Signing Request**

Download CSR Close

**Status**

Warning: Certificate names not listed below do not have a corresponding CSR

**Download Certificate Signing Request**

Certificate Purpose\* tomcat

Download CSR Close


\*- indicates required item.

Passaggio 4. Inviare il CSR all'autorità di certificazione.

Passaggio 5. L'autorità di certificazione restituisce due o più file per la catena di certificati firmata. Carica i certificati nell'ordine seguente:

- Certificato CA radice come tomcat-trust. Passare a **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Imposta la descrizione del certificato e sfogliare il file del certificato radice.
- Certificato intermedio come tomcat-trust (facoltativo). Passare a **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Impostare la descrizione del certificato ed esplorare il file del certificato intermedio.


---

 Nota: alcune CA non forniscono un certificato intermedio. Se è stato fornito solo il certificato radice, questo passaggio può essere omesso.

---

- Certificato firmato dalla CA come tomcat. Passare a **Certificate Management > Upload certificate > Certificate Purpose: tomcat**. Impostare la descrizione del certificato e sfogliare il file del certificato firmato dalla CA per individuare il nodo CUCM corrente.

---

 Nota: a questo punto, CUCM confronta il CSR e il certificato CA firmato caricato. Se le informazioni corrispondono, il CSR scompare e il nuovo certificato firmato dall'autorità di certificazione viene caricato. Se viene visualizzato un messaggio di errore dopo il caricamento del certificato, consultare la sezione relativa **Upload Certificate Common Error Messages a**.

---

Passaggio 6. Per applicare il nuovo certificato al server, è necessario riavviare il servizio Cisco Tomcat tramite CLI (iniziare con Publisher, quindi gli abbonati, uno alla volta). Utilizzare il comando `utils service restart Cisco Tomcat`.

Per verificare che il certificato Tomcat sia ora utilizzato da CUCM, passare alla pagina Web del nodo e selezionare **Site Information** (Icona di blocco) nel browser. Fare clic sull'opzione **certificate** e verificare la data del nuovo certificato.



Cis  
For

### Connection is secure



Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

[Learn more](#)



Certificate (Valid)



Cookies (1 in use)



Site settings

General

Details

Certification Path

**Certificate Information**

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer

**Issued to:** 115pub[REDACTED]


**Issued by:** [REDACTED]

**Valid from 9/16/2020 to 9/16/2022**

Issuer Statement

OK


## Certificato CallManager

 **Attenzione:** non rigenerare contemporaneamente i certificati CallManager e TVS. Ciò causa una mancata corrispondenza irreversibile con l'ITL installato sugli endpoint che richiede la rimozione dell'ITL da TUTTI gli endpoint nel cluster. Completare l'intero processo di

---

 CallManager e, una volta registrati nuovamente i telefoni, avviare il processo per la TV.

---

 Nota: per determinare se il cluster è in modalità mista, passare a Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non sicuro; 1 == Modalità mista).

---

Per tutti i nodi CallManager del cluster:

Passaggio 1. Passare Cisco Unified OS Administration > Security > Certificate Management > Find a e verificare la data di scadenza del certificato di CallManager.

Passaggio 2. Fare clic su .Generate CSR > Certificate Purpose: CallManager Selezionare le impostazioni desiderate per il certificato, quindi fare clic suGenerate. Attendere che venga visualizzato il messaggio di operazione riuscita e fare clic suClose.


Passaggio 3. Scaricare il CSR. Fare clic su .Download CSR. Select Certificate Purpose: CallManager and click Download

Passaggio 4. Inviare il CSR alla Certificate Authority .

Passaggio 5. L'autorità di certificazione restituisce due o più file per la catena di certificati firmata. Carica i certificati nell'ordine seguente:

- Certificato CA radice come CallManager-trust. Passare aCertificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Impostare la descrizione del certificato e sfogliare il file del certificato radice.
- Certificato intermedio come CallManager-trust (facoltativo). Passare aCertificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Impostare la descrizione del certificato ed esplorare il file del certificato intermedio.


---

 Nota: alcune CA non forniscono un certificato intermedio. Se è stato fornito solo il certificato radice, questo passaggio può essere omesso.

---

- Certificato firmato da CA come CallManager. Passare aCertificate Management > Upload certificate > Certificate Purpose: CallManager. Impostare la descrizione del certificato e sfogliare il file del certificato firmato dalla CA per individuare il nodo CUCM corrente.

---

 Nota: a questo punto, CUCM confronta il CSR e il certificato CA firmato caricato. Se le informazioni corrispondono, il CSR scompare e il nuovo certificato firmato dall'autorità di certificazione viene caricato. Se viene visualizzato un messaggio di errore dopo il caricamento del certificato, vedere la sezione Carica messaggi di errore comuni del certificato.

---

Passaggio 6. Se il cluster è in modalità mista, aggiornare l'elenco di certificati attendibili prima di riavviare i servizi: [Token](#) o [Token](#). Se il cluster è in modalità non protetta, ignorare questo

passaggio e procedere con il riavvio dei servizi.


Passaggio 7. Per ottenere il nuovo certificato applicato al server, è necessario riavviare i servizi richiesti (solo se il servizio è in esecuzione e attivo). Accedere a:

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager

Passaggio 8. Reimposta tutti i telefoni:

- Passare a Cisco Unified CM Administration > System > Enterprise Parameters > Reset. Viene visualizzata una finestra popup con l'istruzione, Si sta per ripristinare tutte le periferiche del sistema. L'operazione non può essere annullata. Continuare? selezionare OK , quindi fare clic su Reset .


---

 Nota: monitorare la registrazione del dispositivo tramite RTMT. Una volta che tutti i telefoni si sono registrati di nuovo si può procedere con il successivo tipo di certificato.

---

## Certificato IPsec

---

 Attenzione: un'attività di backup o ripristino non deve essere attiva quando il certificato IPsec viene rigenerato.

---

Per tutti i nodi (CallManager e IM&P) del cluster:

Passaggio 1. Passare a Cisco Unified OS Administration > Security > Certificate Management > Find alla data di scadenza del certificato IPsec e verificarla.

Passaggio 2. Fare clic su Genera CSR > Scopo certificato: ipsec. Selezionare le impostazioni desiderate per il certificato, quindi fare clic su Genera. Attendere che venga visualizzato il messaggio di operazione riuscita, quindi fare clic su Chiudi.

Passaggio 3. Scaricare il CSR. Fare clic su Download CSR. Selezionare Certificate Purpose ipsec e fare clic su Download.

Passaggio 4. Inviare il CSR all'autorità di certificazione.


Passaggio 5. L'autorità di certificazione restituisce due o più file per la catena di certificati firmata. Carica i certificati nell'ordine seguente:

- Certificato CA radice come attendibilità ipsec. Passare a Gestione certificati > Carica certificato > Scopo certificato: ipsec-trust. Impostare la descrizione del certificato e sfogliare il file del certificato radice.
- Certificato intermedio come trust IPsec (facoltativo). Passare a Gestione certificati > Carica certificato > Scopo certificato: tomcat-trust. Impostare la descrizione del certificato ed



esplorare il file del certificato intermedio.


---

 Nota: alcune CA non forniscono un certificato intermedio. Se è stato fornito solo il certificato radice, questo passaggio può essere omesso.

---

- Certificato firmato da CA come ipsec. Passare a Gestione certificati > Carica certificato > Scopo certificato: ipsec. Impostare la descrizione del certificato e sfogliare il file del certificato firmato dalla CA per individuare il nodo CUCM corrente.

---

 Nota: a questo punto, CUCM confronta il CSR e il certificato CA firmato caricato. Se le informazioni corrispondono, il CSR scompare e il nuovo certificato firmato dall'autorità di certificazione viene caricato. Se viene visualizzato un messaggio di errore dopo il caricamento del certificato, vedere la sezione Caricamento dei messaggi di errore comuni dei certificati < /strong>.


---

Passaggio 6. Per ottenere il nuovo certificato applicato al server, è necessario riavviare i servizi richiesti (solo se il servizio è in esecuzione e attivo). Accedere a:

- Cisco Unified Serviceability > Strumenti > Control Center - Servizi di rete > Cisco DRF Master(Publisher)
- Cisco Unified Serviceability > Strumenti > Control Center - Servizi di rete > Cisco DRF Local (autore e abbonati)


## Certificato CAPF

---

 Nota: per determinare se il cluster è in modalità mista, passare a Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non sicuro; 1 == Modalità mista).

---

---

 Nota: il servizio CAPF viene eseguito solo nel server di pubblicazione e questo è l'unico certificato utilizzato. Non è necessario ottenere i nodi del Sottoscrittore firmati da una CA perché non vengono utilizzati. Se il certificato è scaduto nei Sottoscrittori e si desidera evitare gli avvisi relativi ai certificati scaduti, è possibile rigenerare i certificati CAPF sottoscrittori come autofirmati. Per ulteriori informazioni, vedere [Certificato CAPF autofirmato](#).

---

Nel server di pubblicazione:

Passaggio 1. Passare a Cisco Unified OS Administration > Security > Certificate Management > Find e verificare la data di scadenza del certificato CAPF.

Passaggio 2. Fare clic su Genera CSR > Scopo certificato: CAPF. Selezionare le impostazioni desiderate per il certificato, quindi fare clic su Genera. Attendere che venga visualizzato il messaggio di operazione riuscita e fare clic su Chiudi.


Passaggio 3. Scaricare il CSR. Fare clic su Download CSR. Selezionare Certificate Purpose CAPF e fare clic su Download.

Passaggio 4. Inviare il CSR all'autorità di certificazione.

Passaggio 5. L'autorità di certificazione restituisce due o più file per la catena di certificati firmata. Carica i certificati nell'ordine seguente:

- Certificato CA radice come trust CAPF. Passare a Gestione certificati > Carica certificato > Scopo certificato: CAPF-trust. Impostare la descrizione del certificato e sfogliare il file del certificato radice.
- Certificato intermedio come CAPF-trust (facoltativo). Passare a Gestione certificati > Carica certificato > Scopo certificato: CAPF-trust. Impostare la descrizione del certificato ed esplorare il file del certificato intermedio.


---

 Nota: alcune CA non forniscono un certificato intermedio. Se è stato fornito solo il certificato radice, questo passaggio può essere omesso.

---

- Certificato firmato da CA come CAPF. Passare a Gestione certificati > Carica certificato > Scopo certificato: CAPF. Impostare la descrizione del certificato e sfogliare il file del certificato firmato dalla CA per individuare il nodo CUCM corrente.

---

 Nota: a questo punto, CUCM confronta il CSR e il certificato CA firmato caricato. Se le informazioni corrispondono, il CSR scompare e il nuovo certificato firmato dall'autorità di certificazione viene caricato. Se viene visualizzato un messaggio di errore dopo il caricamento del certificato, consultare la sezione Carica messaggi di errore comuni del certificato.

---

Passaggio 6. Se il cluster è in modalità mista, aggiornare l'elenco di certificati attendibili prima di riavviare i servizi: [Token](#) o [Token](#). Se il cluster è in modalità non protetta, ignorare questo passaggio e procedere con il riavvio del servizio.

Passaggio 7. Per ottenere il nuovo certificato applicato al server, è necessario riavviare i servizi richiesti (solo se il servizio è in esecuzione e attivo). Accedere a:


- Cisco Unified Serviceability > Strumenti > Control Center - Servizi di rete > Cisco Trust Verification Service (tutti i nodi in cui viene eseguito il servizio).
- Cisco Unified Serviceability > Strumenti > Control Center - Feature Services > Cisco TFTP (tutti i nodi in cui viene eseguito il servizio).
- Cisco Unified Serviceability > Strumenti > Control Center - Servizi funzionalità > Funzione proxy Cisco Certificate Authority (Publisher)

Passaggio 8. Reimposta tutti i telefoni:

- Passare a Cisco Unified CM Administration > System > Enterprise Parameters > Reset (Amministrazione Cisco Unified CM > Sistema > Parametri aziendali > Reimposta). Viene

visualizzata una finestra popup con l'istruzione, Si sta per ripristinare tutte le periferiche del sistema. L'operazione non può essere annullata. Continuare? Selezionare OK, quindi fare clic su Reset (Reimposta).


---

 Nota: monitorare la registrazione del dispositivo tramite RTMT. Una volta che tutti i telefoni si sono registrati di nuovo si può procedere con il successivo tipo di certificato.

---

## Certificato TV

---

 Attenzione: non rigenerare contemporaneamente i certificati CallManager e TVS. Ciò causa una mancata corrispondenza irreversibile con l'ITL installato sugli endpoint che richiede la rimozione dell'ITL da TUTTI gli endpoint nel cluster. Completare l'intero processo per CallManager e, una volta registrati i telefoni, avviare il processo per il televisore.

---

Per tutti i nodi TVS del cluster:

Passaggio 1. Passare a Cisco Unified OS Administration > Security > Certificate Management > Find e verificare la data di scadenza del certificato del televisore.

Passaggio 2. Fare clic su Generate CSR > Certificate Purpose: TVS. Selezionare le impostazioni desiderate per il certificato, quindi fare clic su Genera. Attendere che venga visualizzato il messaggio di operazione riuscita e fare clic su Chiudi.


Passaggio 3. Scaricare il CSR. Fare clic su Download CSR. Selezionare Certificate Purpose TVS e fare clic su Download.

Passaggio 4. Inviare il CSR all'autorità di certificazione.

Passaggio 5. L'autorità di certificazione restituisce due o più file per la catena di certificati firmata. Carica i certificati nell'ordine seguente:

- Certificato CA radice come TVS-trust. Passare a Gestione certificati > Carica certificato > Scopo certificato: TVS-trust. Impostare la descrizione del certificato e sfogliare il file del certificato radice.
- Certificato intermedio come TVS-trust (facoltativo). Passare a Gestione certificati > Carica certificato > Scopo certificato: TVS-trust. Impostare la descrizione del certificato ed esplorare il file del certificato intermedio.

---

 Nota: alcune CA non forniscono un certificato intermedio. Se è stato fornito solo il certificato radice, questo passaggio può essere omesso.

---

- Certificato firmato dall'autorità di certificazione come TV. Passare a Gestione certificati > Carica certificato > Scopo certificato: TV. Impostare la descrizione del certificato e sfogliare il file del certificato firmato dalla CA per individuare il nodo CUCM corrente.



---

Nota: a questo punto, CUCM confronta il CSR e il certificato CA firmato caricato. Se le informazioni corrispondono, il CSR scompare e il nuovo certificato firmato dall'autorità di certificazione viene caricato. Se viene visualizzato un messaggio di errore dopo il caricamento del certificato, vedere la sezione Carica messaggi di errore comuni del certificato.

---

Passaggio 6. Per ottenere il nuovo certificato applicato al server, è necessario riavviare i servizi richiesti (solo se il servizio è in esecuzione e attivo). Accedere a:

- Cisco Unified Serviceability > Strumenti > Control Center - Feature Services > Cisco TFTP (tutti i nodi in cui viene eseguito il servizio).
- Cisco Unified Serviceability > Strumenti > Control Center - Servizi di rete > Cisco Trust Verification Service (tutti i nodi in cui viene eseguito il servizio).

Passaggio 7. Reimposta tutti i telefoni:

- Passare a Cisco Unified CM Administration > System > Enterprise Parameters > Reset (Amministrazione Cisco Unified CM > Sistema > Parametri aziendali > Reimposta). Viene visualizzata una finestra popup con l'istruzione, Si sta per ripristinare tutte le periferiche del sistema. L'operazione non può essere annullata. Continuare? Selezionare OK, quindi fare clic su Reset (Reimposta).



---

Nota: monitorare la registrazione del dispositivo tramite RTMT. Una volta registrati tutti i telefoni, si può procedere con il successivo tipo di certificato.

---

## Risoluzione dei problemi relativi ai messaggi di errore dei certificati caricati comuni

In questa sezione sono elencati alcuni dei messaggi di errore più comuni quando viene caricato un certificato firmato dalla CA.

### Il certificato CA non è disponibile nell'archivio attendibile

Questo errore indica che il certificato radice o intermedio non è stato caricato in CUCM. Verificare che i due certificati siano stati caricati come attendibilità prima di caricare il certificato del servizio.

### Il file `/usr/local/platform/.security/tomcat/keys/tomcat.csr` non esiste

Questo errore viene visualizzato quando non esiste un CSR per il certificato (tomcat, callmanager, ipsec, capf, tvs). Verificare che il CSR sia stato creato in precedenza e che il certificato sia stato creato in base a tale CSR. Punti importanti da tenere a mente:

- Può esistere un solo CSR per server e tipo di certificato. Ciò significa che se viene creata una nuova RSI, quella precedente viene sostituita.
- I certificati jolly non sono supportati da CUCM.

- Non è possibile sostituire un certificato di servizio attualmente in uso senza un nuovo CSR.
- Un altro possibile errore per lo stesso problema è "Impossibile caricare il file /usr/local/platform/upload/certs//tomcat.der". Dipende dalla versione CUCM.

## Chiave pubblica CSR e chiave pubblica del certificato non corrispondenti

Questo errore viene visualizzato quando il certificato fornito dalla CA ha una chiave pubblica diversa da quella inviata nel file CSR. Le possibili cause sono:

- È stato caricato il certificato errato (forse da un altro nodo).
- Il certificato CA è stato generato con un altro CSR.
- Il CSR è stato rigenerato e ha sostituito il precedente CSR utilizzato per ottenere il certificato firmato.

Per verificare la corrispondenza tra CSR e chiave pubblica del certificato, sono disponibili diversi strumenti in linea, ad esempio [SSL](#).


## What to Check


- Check if a Certificate and a Private Key match
- Check if a CSR and a Certificate match

### Enter your Certificate:

```
TjT13aW4zMiXDTj1DRFAzQ049UHVbGjThwS2V5jTiwU2VydMjZOMsQ049U2Vy
dmjZOMsQ049Q29uZmIndGh4GhvbixQ21jB2xYwWkREM96Xg/r2VydGImawWwh
dQvS2ZQvY2f0awWjuTGzddD9mXNIP29awvjdENsY0NzPWNSTERpc3RyaWw1dGlv
bllBvaW50MIG7BgggrBgEFBQcBAQ5BnjCBqrCBqAYKwYBBQUHMAKGZicsZGFwO18v
LONOPUHVbGahYyIyMENBLENDPUFjQ5xDTj1QdVjsawWMMjBLZxXdmjBTZQj2awWl
cyxDTj1TZQj2awWlcyxDTj1Db25maWwd1cmF0awW9uLERDPWwvbgxhYxEQz1teD9j
QUwlcncRmZmYyRFP2jnc2urb2jgZWN0Q2xhc3M9Y2VydGImawWwhdGwkaF1dGhv
cm0leTAhBgkrBgEAAy13FAIEFB4SAFA2QBIAFMAZQByAHYA2QByMA0GCSqGSIb3
DQEBEwUAA4BAQCfaj2BkZ8CMxkunQavdYauIeDfDpMLSA7fHhIsqW55x/bEQs
9LyqfmidCmkoMFP6K4I2vMle4oTpKBYAQvbrApG001mWV5u+flie9PvrygWtYl
D+ve7rMp8srVo1Tmhe/26in3lcm+Qfwe5NuvCx3wN/dLRR3904KcaPCxvLQ6Aw
PtnWz/KK2GRHzqacd9fvUJuoWTKDj2Qsladcgsl5cvFMz3BBf0MjGBNX16jGjQ
yZzBr6Gm4pa4yKj6sUrcXohYslomecYeRheKu5kuPusDaeEwWwszj0QMT7P4/Ww
Z8pT2TrkQdQDAZHjGujP+yBa75QGQTZWVng1
-----END CERTIFICATE-----
```

 The certificate and CSR do NOT match!

 Certificate Hash:  
684ad486131856ce0015d4b3e615e1ed  
3b3bef6b8f590a493921661a4c4f62e9

 CSR Hash:  
635f45c1ebcd876526a3133d1ee73d9a8  
4544876fdbc8dc3a4d8fed377dcc635

### Enter your CSR:

```
q+hjgokSx+ogqYavFSNRdqTh0Glrts1ga0pJ5sGxOOLCqAtQHEARnEcGyanZzrk
g5jTQHfBJSD2vDnyD3wg5YhfwvliqkMUl3RD5qcSDYfLGLs8hB9ySHqADA3
1llWj5Q4RXZ188ESclIB3BA0ZegZ05vW4h05fP8r09h/CTW5XZtBLGytWCDGk
O0rdW2xLuuUv2u2jYWTmLD79HCN/XCM89XypLj6uLyMUf0DFh+s0F1M7gaI5b
hXXS4Zj0FIM0XYBWSFDwexH7x0D+HQaPeM4Y50N4YqhxAgMBAAQgBzBt8gkqhkiG
9w0BCQ4xYDBeMBOGA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjALBgNVHQ8E
BAMCBLAwMAYDR0RBCkx4IQY3VjB55jB2x5YwIubXCFTEsXKB1Y15jdWNLmNv
bGxhY5teDANBgkqhkiG9w0BAQsIAA0CAQEAAh8gll76T59rWxOFjsg7hsj36vf
ubcW7HGPrNyx6/pl9UyduN8XXDxQTlzZWWc9IDA3/Fpcjrz+8LdHr1FnnwBWCV
YcA9soNIWZsmU1+clbTH1HSg8FFcHADg+FR3+1AE7GNfGK0CA0RipRihZPGzQ6dO
62TRSfQ45LubCwxe4EZO5xjEQW7Zrkjfwby1GQKyj3CuXCETy3UunMCZnWjmnXkG0
n7B1nNdX7Ybgf21hY+ZozPHWgbu2HwChuH1bOAMUpkwIPebQZn9H+R7drjBAZR
leXEYWL739M7B7veNmHoOnR65kwhYrb7iq0jnhXx5y9R05052vUhhj7Hw==
-----END CERTIFICATE REQUEST-----
```

Un altro possibile errore per lo stesso problema è "Impossibile caricare il file /usr/local/platform/upload/certs/tomcat.der". Dipende dalla versione CUCM.

Il nome alternativo del soggetto (SAN) CSR e la SAN del certificato non corrispondono

Le SAN tra il CSR e il certificato devono essere identiche. Ciò impedisce la certificazione per i domini non consentiti. Per verificare la mancata corrispondenza SAN, procedere come segue:

1. Decodificare il CSR e il certificato (base 64). Ci sono diversi decoder disponibili online, come il [Decoder](#).

2. Confrontare le voci SAN e verificare che corrispondano tutte. L'ordine non è importante, ma tutte le voci nel CSR devono essere identiche nel certificato.

Ad esempio, al certificato firmato dall'autorità di certificazione vengono aggiunte due voci SAN aggiuntive, il Nome comune del certificato e un indirizzo IP aggiuntivo.

| CSR Summary              |   |
|--------------------------|---|
| Subject: domain.com      |   |
| RDN                      | Value   |
| Common Name (CN)         | pub-ms.domain.com   |
| Organizational Unit (OU) | Collaboration   |
| Organization (O)         | Cisco   |
| Locality (L)             | CUCM  |
| State (ST)               | CDMX  |
| Country (C)              | MX  |
| Properties: domain.com   |   |
| Property                 | Value   |
| Subject                  | CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX |
| Key Size                 | 2048 bits   |
| Fingerprint (SHA-1)      | C3:87:05:C8:79:FE:88:4A:86:96:77:0A:C5:88:63:27:55:3C:A4:84                   |
| Fingerprint (MD5)        | CE:5C:9D:59:3F:8E:E3:26:C5:21:9D:A2:F1:CA:68:B6                               |
| SANS                     | domain.com, sub.domain.com, pub.domain.com, imp.domain.com                    |

| Certificate Summary      |   |
|--------------------------|---|
| Subject                  |   |
| RDN                      | Value   |
| Common Name (CN)         | pub-ms.domain.com   |
| Organizational Unit (OU) | Collaboration   |
| Organization (O)         | Cisco   |
| Locality (L)             | CUCM  |
| State (ST)               | CDMX  |
| Country (C)              | MX  |
| Properties               |   |
| Property                 | Value   |
| Issuer                   | CN = Collab CA,DC = collab,DC = mx  |
| Subject                  | CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX                         |
| Valid From               | 17 Sep 2020, 1:24 a.m.  |
| Valid To                 | 17 Sep 2022, 1:24 a.m.  |
| Serial Number            | 69:00:00:00:2D:5A:92:EB:EA:9A:85:65:C4:00:00:00:00:2D(2341578246081205845683969935281333946237893677) |
| CA Cert                  | No  |
| Key Size                 | 2048 bits   |
| Fingerprint (SHA-1)      | 4E:15:F7:F3:9C:37:A9:8D:52:1A:6C:6D:4D:7D:AF:FE:08:EB:8D:0F   |
| Fingerprint (MD5)        | D8:22:33:92:5D:F7:70:2A:05:28:90:2D:57:C0:F7:EC   |
| SANS                     | sub-ms.domain.com, domain.com, sub.domain.com, pub.domain.com, imp.domain.com, 10.xx.xx.xx            |

3. Una volta identificata la mancata corrispondenza della SAN, sono disponibili due opzioni per risolvere il problema:

1. Richiedere all'amministratore della CA di rilasciare un certificato con le stesse voci SAN inviate nel CSR.
2. Creare un CSR in CUCM che soddisfi i requisiti della CA.

Per modificare il CSR creato da CUCM:

1. Se la CA rimuove il dominio, è possibile creare un CSR in CUCM senza il dominio. Durante la creazione di CSR, rimuovere il dominio popolato per impostazione predefinita.
2. Se viene creato un [certificato multisito](#), alcune CA non accettano -ms nel nome comune. I -ms possono essere rimossi dal CSR al momento della creazione.

**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 <sup>Ⓜ</sup> tomcat

Distribution <sup>Ⓜ</sup> Multi-server(SAN)

Common Name <sup>Ⓜ</sup> 115pub.ms

Subject Alternate Names (SANs)

Auto-populated Domains

115imp.  
115pub.  
115sub.

Parent Domain

Other Domains

---

Key Type <sup>Ⓜ</sup> RSA

Key Length <sup>Ⓜ</sup> 2048

Hash Algorithm <sup>Ⓜ</sup> SHA256

Generate Close

3. Per aggiungere un nome alternativo oltre a quelli completati automaticamente da CUCM:

1. Se si utilizza un certificato multisSAN, è possibile aggiungere più FQDN. (gli indirizzi IP non sono accettati).



**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 <sup>*</sup>      | <input type="text" value="tomcat"/>  |
| Distribution <sup>*</sup>             | <input type="text" value="Multi-server(SAN)"/>   |
| Common Name <sup>*</sup>              | <input type="text" value="115pub-ms-██████████"/>  |
| <b>Subject Alternate Names (SANs)</b> |  |
| Auto-populated Domains                | <input type="text" value="115imp.██████████"/><br><input type="text" value="115pub.██████████"/><br><input type="text" value="115sub.██████████"/>                               |
| Parent Domain                         | <input type="text"/>   |
| Other Domains                         | <input type="text" value="extrahostname.domain.com"/> <span style="float: right; border: 1px solid #ccc; padding: 2px 5px;">Choose File</span><br><small>For more inform</small> |
|                                       | <input type="text"/> <span style="float: right; border: 1px solid #ccc; padding: 2px 5px;">+ Add</span>  |
| Key Type <sup>*</sup>                 | <input type="text" value="RSA"/>   |
| Key Length <sup>*</sup>               | <input type="text" value="2048"/>  |
| Hash Algorithm <sup>*</sup>           | <input type="text" value="SHA256"/>  |

Generate Close

b. Se il certificato è a nodo singolo, utilizzare il `set web-security` comando. Questo comando è valido anche per i certificati multi-SAN. (È possibile aggiungere qualsiasi tipo di dominio, ma sono consentiti anche indirizzi IP).

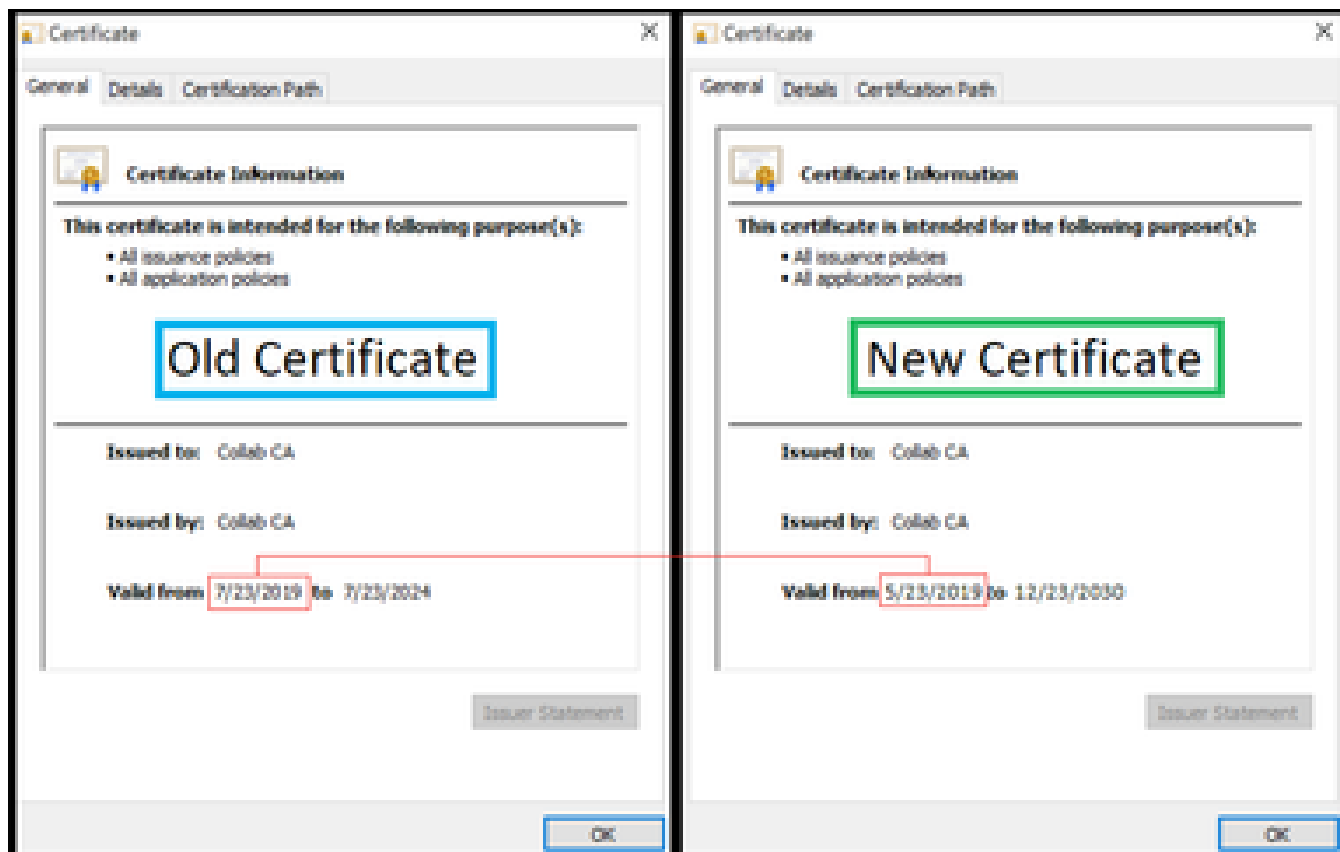
Per ulteriori informazioni, vedere la [Guida di riferimento per la riga di comando](#).

### Certificati di attendibilità con lo stesso CN non sostituiti

CUCM è stato progettato per archiviare un solo certificato con lo stesso nome comune e lo stesso tipo di certificato. Questo significa che se un certificato che è un tomcat-trust esiste già nel database e deve essere sostituito con uno recente con la stessa CN, CUCM rimuove il vecchio certificato e lo sostituisce con quello nuovo.

In alcuni casi, il certificato precedente non viene sostituito da CUCM:

1. Il certificato caricato è scaduto: CUCM non consente di caricare un certificato scaduto.
2. La data FROM del certificato precedente è più recente di quella del nuovo certificato. In CUCM viene mantenuto il certificato più recente e la data FROM precedente viene catalogata come precedente. Per questo scenario, è necessario eliminare il certificato indesiderato e quindi caricare quello nuovo.



## 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).