

Configurare Tomcat Certificate Reuse per CallManager in CUCM 14

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[1. Impostare il certificato Tomcat come Multi-SAN](#)

[Autofirmato](#)

[Con firma CA](#)

[2. Riutilizzare il certificato Tomcat per CallManager](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come riutilizzare il certificato Multi-SAN Tomcat per CallManager su un server Cisco Unified Communications Manager (CUCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- certificati CUCM
- Strumento di monitoraggio in tempo reale (RTMT)
- ITL (Identity Trust List)

Componenti usati

Il riferimento delle informazioni contenute in questo documento è CUCM 14.0.1.13900-155.







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.

Premesse

I due servizi principali per CUCM sono Tomcat e CallManager. Nelle versioni precedenti per il cluster completo erano necessari certificati diversi per ogni servizio. In CUCM versione 14 è stata aggiunta una nuova funzionalità per riutilizzare il certificato Multi-SAN Tomcat anche per il servizio CallManager. L'utilizzo di questa funzione offre i seguenti vantaggi:

- Riduce i costi per ottenere due certificati firmati da un'Autorità di certificazione pubblica (CA) per un cluster di certificati firmati da CA.
- Questa funzione riduce le dimensioni del file ITL, riducendo in tal modo il sovraccarico.

 Low Impact  Medium Impact.  High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat		-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec		-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF		CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager		CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS		ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery		CTL + ITL	Signer or SAST backup for ITL/CTL	All	

Configurazione



Attenzione: Prima di caricare un certificato Tomcat, verificare che Single Sign-On (SSO) sia disabilitato. Se è attivata, l'SSO deve essere disattivato e riattivato al termine del processo di rigenerazione dei certificati Tomcat.

 Low Impact

1. Impostare il certificato Tomcat come Multi-SAN

In CUCM 14, il certificato Tomcat Multi-SAN può essere autofirmato o firmato dalla CA. Se il certificato Tomcat è già Multi-SAN, ignorare questa sezione.

Autofirmato

Passaggio 1. Accedere a Publisher > Operating System (OS) Administration e passare a Security > Certificate Management > Generate Self-Signed.

Passaggio 2. Scegliere Certificate Purpose: tomcat > Distribution: Multi-Server SAN. I domini SAN e il dominio padre vengono popolati automaticamente.

Generate New Self-signed Certificate

Generate

Close

Status

Generating a new certificate will overwrite any existing certificate information. When generating Call Manager, CAPF, or TVS, all devices will be reset automatically.

Generate Self-signed

Certificate Purpose**tomcat

Distribution*Multi-server(SAN)

Common Name*14pub.

Subject Alternate Names (SANs)

Auto-populated Domains

14pub.

14sub.

Key Type**RSA

Key Length*2048

Hash Algorithm*SHA256

Validity Period (in years)*5

Generate

Close

i

*- indicates required item.

i

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

Schermata Genera certificato Tomcat multifirma autografato

Passaggio 3. Fare clic su Generate e verificare che tutti i nodi siano elencati nel Certificate upload operation successful messaggio. Fare clic su .Close

Generate New Self-signed Certificate

Generate

Close

Status

i

Certificate upload operation successful for the nodes 14sub. ,14pub. .

i

Restart Cisco Tomcat Service for the nodes 14sub. ,14pub. using the CLI "utils service restart Cisco Tomcat". Restart the Cisco DRF Master and Cisco DRF Local services on the publisher node. Restart ONLY the Cisco DRF Local service on the subscriber node(s).

i

If SAML SSO is enabled, please disable and re-enable it. Also re-provision the SP metadata on the IDP.

Genera messaggio di completamento Tomcat multiSAN con firma automatica

Passaggio 4. Riavviare il servizio Tomcat, aprire una sessione CLI in tutti i nodi del cluster ed eseguire ilutils service restart Cisco Tomcatcomando.

Passaggio 5. Passare alla Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services e riavviare Cisco DRF Master Service e Cisco DRF Local Service.



Passaggio 6. Passare a ciascuna Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services finestra e riavviare Cisco DRF Local Service.


Con firma CA

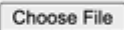





Passaggio 1. Accedere a Publisher > Operating System (OS) Administration e passare a Security > Certificate Management > Generate CSR.

Passaggio 2. Scegliere Certificate Purpose: tomcat > Distribution: Multi-Server SAN. I domini SAN e il dominio padre vengono popolati automaticamente.

Generate Certificate Signing Request

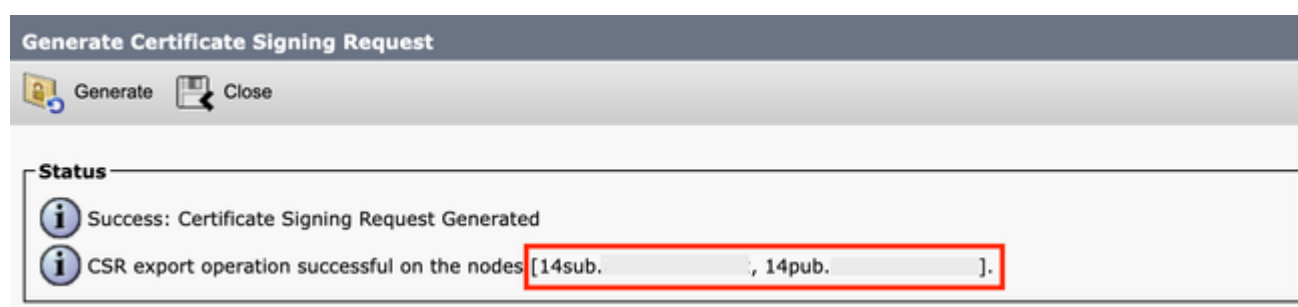
 Generate  Close

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** tomcat
Distribution* Multi-server(SAN)
Common Name* 14pub-ms.
Include OU in CSR ☐
Subject Alternate Names (SANs)
Auto-populated Domains
14pub.
14sub.
Parent Domain
Other Domains
 No file chosen
Please import .TXT file only.

Key Type** RSA
Key Length* 2048
Hash Algorithm* SHA256
 
 *- indicates required item.
 **When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

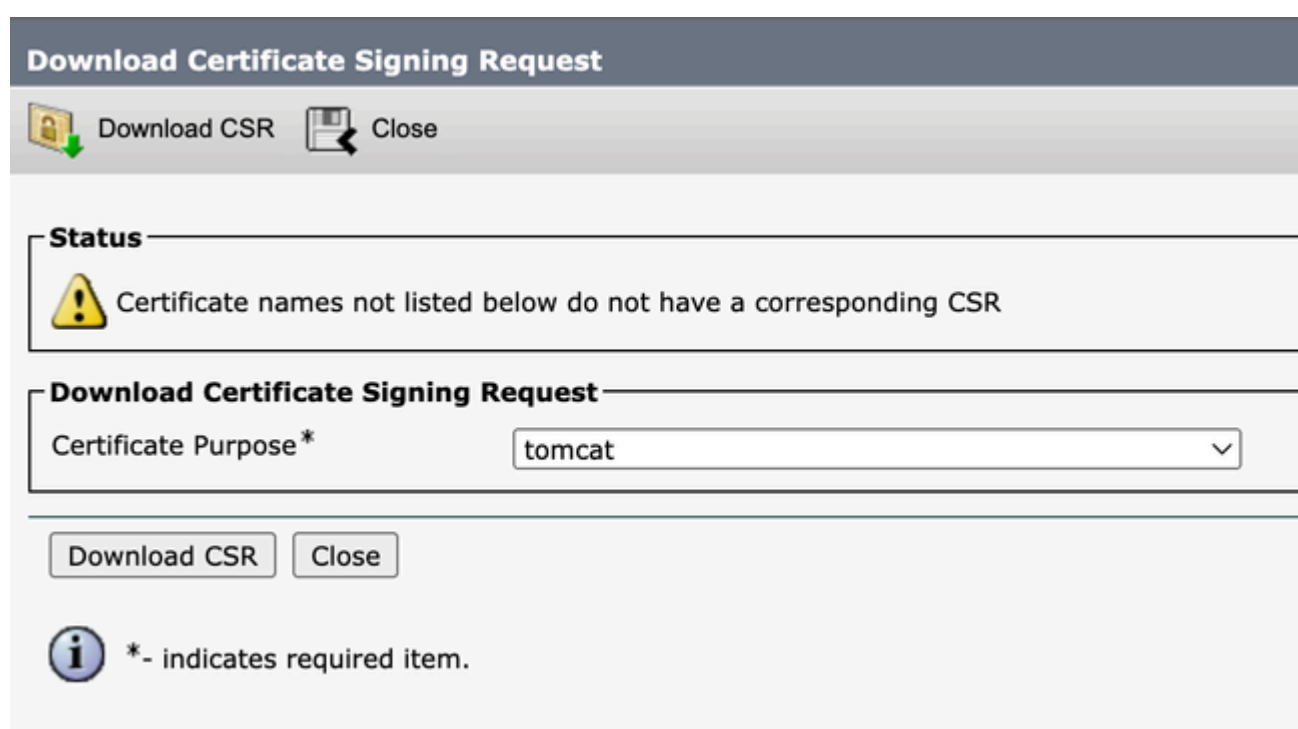
Schermata Genera CSR multi-SAN per certificato Tomcat

Passaggio 3. Fare clic su **Generate** e verificare che tutti i nodi siano elencati nel **CSR export operation successful** messaggio. Fare clic su **. Close**



Genera messaggio di riuscita CSR multi-SAN Tomcat

Passaggio 4. Fare clic su **Download CSR > Certificate Purpose: tomcat > Download.**



Schermata Download CSR Tomcat

Passaggio 5. Inviare il CSR alla CA per la firma.

Passaggio 6. Per caricare la catena di attendibilità CA, passare a **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust.** Impostare la descrizione del certificato ed esplorare i file della catena di attendibilità.

Passaggio 7. Caricare il certificato firmato dall'autorità di certificazione, passare a **Certificate Management > Upload certificate > Certificate Purpose: tomcat.** Impostare la descrizione del certificato e sfogliare il file del certificato firmato dalla CA.

Passaggio 8. Riavviare il servizio Tomcat, aprire una sessione CLI in tutti i nodi del cluster ed eseguire il **utils service restart Cisco Tomcat** comando.

Passaggio 9. Passare alla **Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services** e

riavviare Cisco DRF Master Service e Cisco DRF Local Service.

Passaggio 10. Passare a ciascuna Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services finestra e riavviare Cisco DRF Local Service.

2. Riutilizzare il certificato Tomcat per CallManager Medium Impact.



Attenzione: Per CUCM 14 viene introdotto un nuovo parametro `Phone Interaction on Certificate Update` enterprise. Utilizzare questo campo per reimpostare i telefoni manualmente o automaticamente in base alle esigenze quando viene aggiornato uno dei certificati TVS, CAPF o TFTP (CallManager/ITLRecovery). Per default, questo parametro è impostato su `reset the phones automatically`. Dopo la rigenerazione, l'eliminazione e l'aggiornamento dei certificati, assicurarsi che i servizi appropriati vengano riavviati.

È necessario riavviare i servizi per una normale rigenerazione del certificato di CallManager. Selezionare [Rigenera Certificati In Unified Communications Manager](#).



Passaggio 1. Passare all'editore CUCM e quindi a Cisco Unified OS Administration > Security > Certificate Management.

Passaggio 2. Fare clic su `Reuse Certificate`.



Passaggio 3. Dall'elenco a choose **Tomcat type** discesa, scegliere `tomcat`.

Passaggio 4. Dal `Replace Certificate for the following purpose` riquadro, selezionare la casella di CallManager controllo.

Use Tomcat Certificate For Other Services

 Finish  Close

Status

 Tomcat-ECDSA Certificate is Not Multi-Server Certificate
 Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type*

Replace Certificate for the following purpose

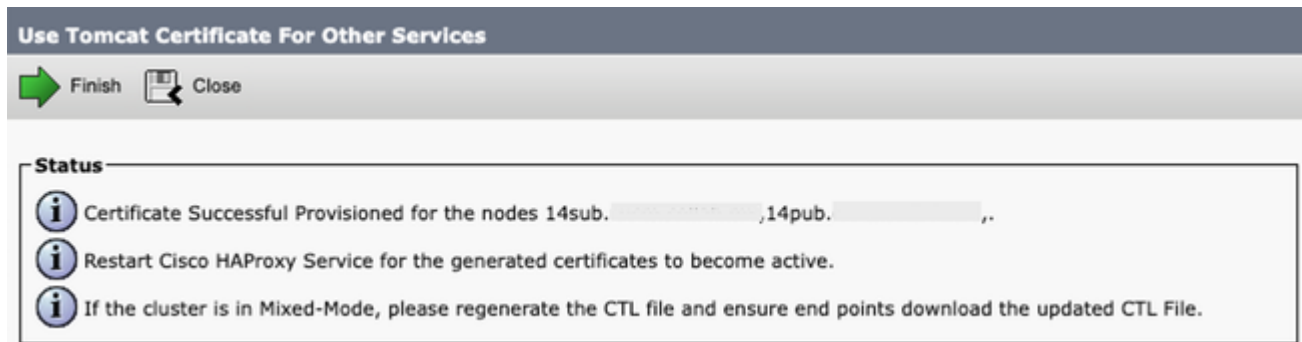
☒ CallManager
☐ CallManager-ECDSA

Finish Close



Nota: Se si sceglie Tomcat come tipo di certificato, CallManager viene abilitato come sostituto. Se si sceglie tomcat-ECDSA come tipo di certificato, CallManager-ECDSA viene abilitato come tipo sostitutivo.

Passaggio 5. Fare clic su **Finish** per sostituire il certificato CallManager con il certificato Tomcat Multi-SAN.



Riutilizza messaggio di certificato Tomcat riuscito

Passaggio 6. Riavviare il servizio Cisco HAProxy, aprire una sessione CLI in tutti i nodi del cluster ed eseguire il `utils service restart Cisco HAProxy` comando.



Nota: Per determinare se il cluster è in modalità mista, passare a **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode** (0 = Non protetto; 1 == Mixed Mode) (Gestione di Cisco Unified CM > Sistema > Parametri aziendali > Modalità di sicurezza cluster (0 = non sicuro; 1 = modalità mista)).

Passaggio 7. Se il cluster è in modalità mista, aprire una sessione CLI nel nodo Publisher ed eseguire il `utils ctl update CTLFile` comando e reimpostare tutti i telefoni del cluster per rendere effettivi gli aggiornamenti del file CTL.

Verifica

Passaggio 1. Passare all'editore CUCM e quindi a **Cisco Unified OS Administration > Security > Certificate Management**.

Passaggio 2. Filtrare per **Find Certificate List where: Usage > begins with: identity** e fare clic su **Find**.

Passaggio 3. I certificati CallManager e Tomcat devono terminare con lo stesso **Common Name_Serial Number** valore.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation
Cisco Unified OS Administration
Go

Show
Settings
Security
Software Upgrades
Services
Help

Certificate List

Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Reuse Certificate

Status
8 records found

Certificate List (1 - 8 of 8)
Rows per Page 50

Find Certificate List where Usage begins with Identity Find Clear Filter

Certificate	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
CallManager	14pub- 45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Reusing tomcat certificate for CallManager
CallManager-ECDSA	14pub-EC- 56a32bfc30d2996d5c5851a8b7e5731f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
CAPF	14pub- CAPF-02a10666	Identity	Self-signed	RSA	14pub.cucm.collab.mx	CAPF-02a10666	12/20/2027	Self-signed certificate generated by system
ipsec	14pub- 6f44af5c5cd753d5ff1538c3879b44	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
ITLRecovery	ITLRECOVERY 14pub- 727029eea3d928d999c99bee38720c89e	Identity	Self-signed	RSA	14pub.cucm.collab.mx	ITLRECOVERY_14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
tomcat	14pub- 45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Multi-server self-signed certificate for tomcat
tomcat-ECDSA	14pub-EC- 6ea1f2fedf8f6183cdf629a4a0f0447f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
TVS	14pub- 7d8022fd6eb2885c3406b77cb4126046	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system

Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Reuse Certificate

Verifica riutilizzo certificati Tomcat per CallManager



Nota: Da SU4 in poi, con il riutilizzo dei certificati abilitato, il certificato di Gestione chiamate non viene visualizzato sulla GUI, mentre entrambi i certificati sono visibili in SU2 e SU3.

Informazioni correlate

- [Guida alla sicurezza per Cisco Unified Communications Manager 14](#)
- [Supporto tecnico Cisco e download](#)

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).