Risoluzione dei problemi comuni relativi al rinnovo dei certificati in CUCM

Introduzione

In questo documento vengono descritti i problemi comuni successivi alla rigenerazione dei certificati in Cisco Unified Communications Manager (CUCM) e viene spiegato come risolverli.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Processo di rinnovo del certificato CUCM
- interfaccia GUI CUCM
- Server Expressway
- Registrazione del dispositivo con il processo CUCM
- Funzione proxy Autorità di certificazione
- Guida alla sicurezza per Cisco Unified Communications Manager

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM versione 15

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.

Impatto aziendale

In questa tabella viene visualizzato l'impatto aziendale di ogni rinnovo di certificato nell'operazione. Esaminate attentamente le informazioni. Rinnova i certificati richiesti dopo l'orario di ufficio o nei periodi di attesa in base al livello di rischio di ogni certificato.

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	

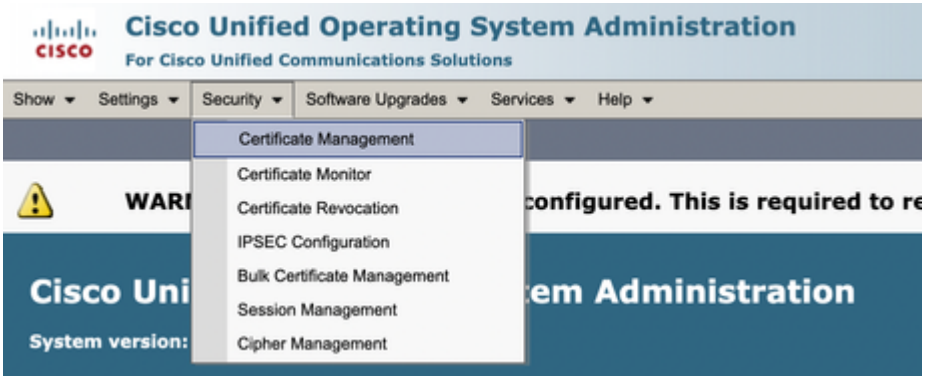
Scenario 1: Telefoni non registrati dopo il rinnovo di Call Manager, TVS e certificati ITL

Nota: Questo scenario si applica alle distribuzioni in cluster CUCM a modalità mista e non protetta, inoltre, ai certificati autofirmati e ai certificati CA.

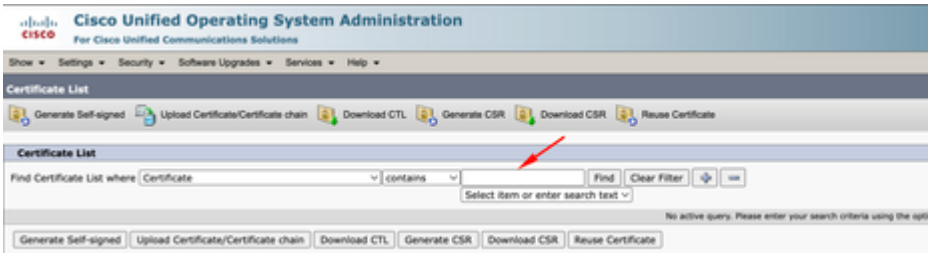
Quando i certificati Call Manager , TVS e ITL sono scaduti e sono stati rinnovati contemporaneamente, causa di avere tutti i nostri telefoni in uno stato non registrato che provoca un impatto importante sul sistema, questo è un comportamento previsto come attiviamo i telefoni di non fidarsi nel CUCM.

Verifica

1. Verificare che i certificati siano già scaduti in Cisco Unified OS Administration > Security > Certificate Management

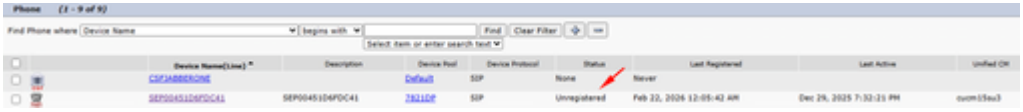


2. Cerca per Callmanager, TVS o ITL sotto il filtro nella parte superiore della pagina e usa le opzioni contiene o inizia con:



3. I certificati devono essere aggiornati e verificati nella colonna Scadenza (lo stesso vale per i certificati TV e ITL)

4. Una volta verificato che tutto è buono dopo il rinnovo del certificato, i telefoni vengono mostrati come stato Non registrato.



Soluzione

Per risolvere il problema, sono disponibili due opzioni:

1. Esegui un ripristino del telefono che consente al telefono di cancellare le impostazioni di sicurezza correnti e di acquisire i nuovi certificati
2. Aggiornare i certificati ITL e CTL dalla CLI nel nodo di pubblicazione e utilizzare il comando utilizza itl reset localkey.

Questo passaggio riguarda tutti i telefoni, compresi quelli registrati, accertarsi di eseguire questa operazione dopo ore.

Scenario 2: Single Sign-On non funziona dopo il rinnovo del certificato Tomcat

---

Nota: Questo scenario può essere applicato alle distribuzioni che utilizzano un contratto a livello di cluster o per nodo per la configurazione Single Sign-On

---

Accesso a CUCM con Single Sign-On (SSO): viene visualizzato un messaggio di errore "Errore durante l'elaborazione della risposta saml" o "Errore durante l'elaborazione della risposta saml Impossibile decrittografare la chiave segreta"

Verifica

1. Verificare che tutti i nodi contengano un certificato tomcat valido se autofirmato o se contenga il nuovo certificato tomcat multi-san associato.
2. Utilizzare il comando set samltrace level debug in tutti i nodi CUCM tramite CLI per attivare i log SSO a livello di debug
3. Ricreare il problema eseguendo nuovamente il login a CUCM e utilizzando il metodo SSO.
4. Raccogliere i log di Tomcat SSO dopo l'incidente e verificare di ricevere questo messaggio:
   -

```
2026-01-10 06:06:31,274 ERROR [http-nio-81-exec-157]  cpi.sso.saml.sp.security.authenticatio
com.sun.identity.saml2.common.SAML2Exception: Failed to decrypt the secret key.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.getEncryptionKey(FMEncProvider.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.decrypt(FMEncProvider.java:607)
              at com.sun.identity.saml2.assertion.impl.EncryptedAssertionImpl.decrypt(Encryp
...
```

Soluzione

Esportazione dei metadati CUCM dopo il rinnovo del certificato Tomcat e importazione nel server del provider di identità per assicurarsi che dispongano del nuovo certificato Tomcat per questa comunicazione.

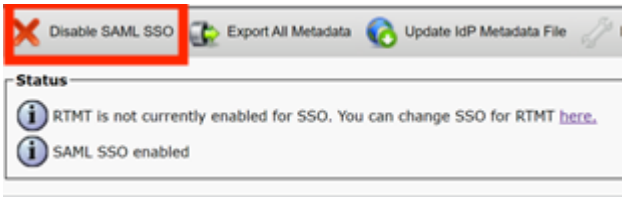
Procedura per rinnovare tomcat con la distribuzione SSO abilitata:

⚠ Attenzione: Technical Assistance Center (TAC) consiglia le fasi successive per evitare problemi dopo il rinnovo del certificato Tomcat, consigliare di eseguire questa procedura dopo ore.

1. Disabilita SSO in tutti i nodi CUCM

- Accesso all'amministrazione CM > Sistema > SAML Single Sign-On

- Selezionare Disabilita SAML SSO

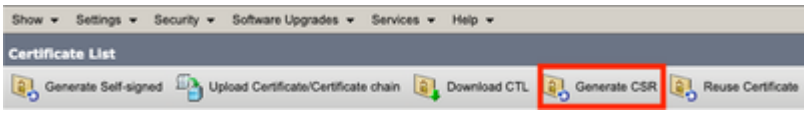


- Questo processo deve essere eseguito in tutti gli altri nodi tramite GUI se viene utilizzato il contratto per nodo.

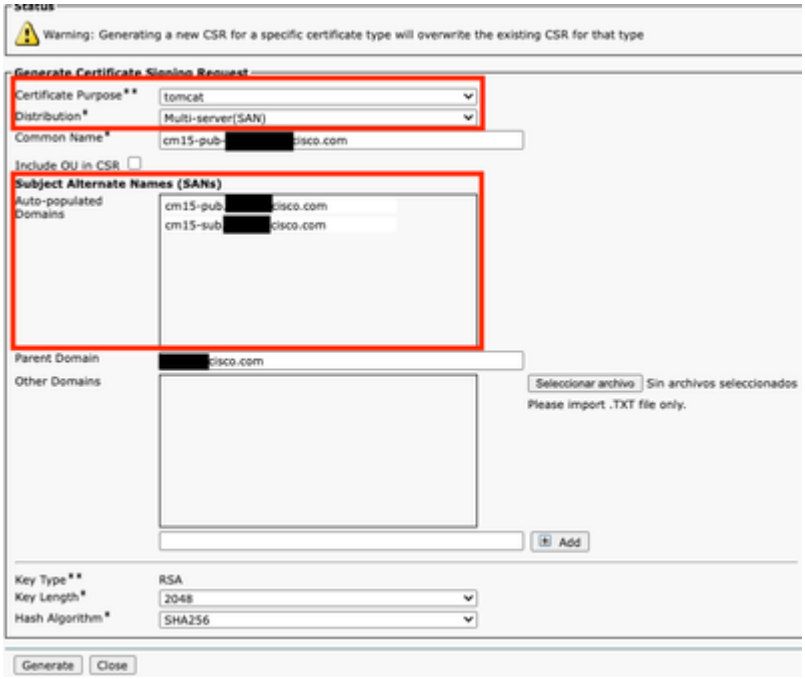
2. Rinnova certificato Tomcat nel cluster CUCM

Procedura generale per il rinnovo del certificato multi-san Tomcat nel cluster CUCM:

- Passare a Amministrazione del sistema operativo > Protezione > Gestione certificati.
- Selezionare Genera CSR



- Selezionare Tomcat in Certificate Porpuse.
- Selezionare Multi-SAN in Distribution.
- Assicurarsi che tutti i nodi nel cluster siano elencati in Domini popolati automaticamente.



- Selezionare Genera. Verificare che CSR sia stato creato in tutti i nodi del cluster.
- Scaricare il CSR generato dall'editore CUCM e firmarlo con un server CA (Certification Authority).
- Selezionare Amministrazione del sistema operativo > Protezione > Gestione certificati. Selezionare Carica catena certificati/certificati.
- Caricare i certificati CA come Tomcat-trust.
- Ripetere il passaggio 6 e caricare il certificato firmato Tomcat come Tomcat.
- Dopo aver completato e verificato che il nuovo certificato Tomcat sia applicato a tutti i nodi, riavviare il servizio Tomcat tramite CLI in tutti i nodi del cluster con questo comando utilizza il servizio per riavviare Cisco Tomcat.

Per ulteriori informazioni, consultare la seguente documentazione:

- Rigenera certificato autofirmato Tomcat
- Rigenera certificato firmato CA Tomcat.

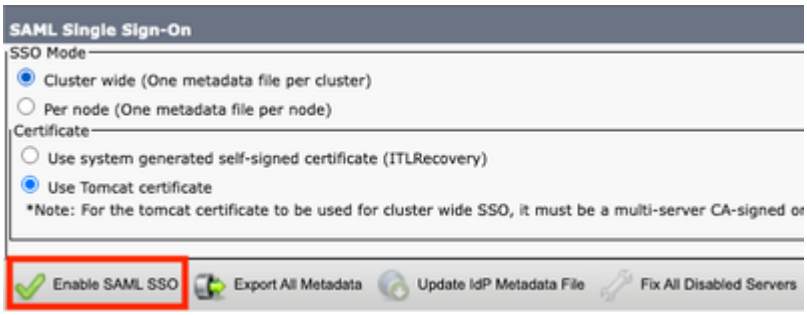
3. Esportazione dei metadati di Service Provider (SP)

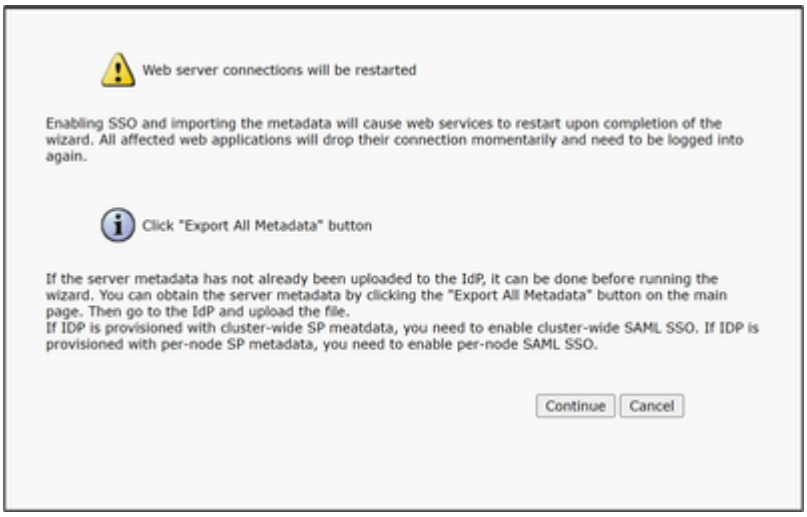
- Selezionare Amministrazione CM > Sistema > Single Sign-On
- Configurare le opzioni SSO (in questo caso, la configurazione a livello di cluster in modalità SSO e la configurazione di Usa certificato tomcat sul certificato come esempio), quindi selezionare Esporta tutti i metadati

- Importare i metadati SP nel server del provider di identità (IdP). Per ulteriori informazioni, consultare il documento sulla [configurazione di SAML SSO sul provider di identità]

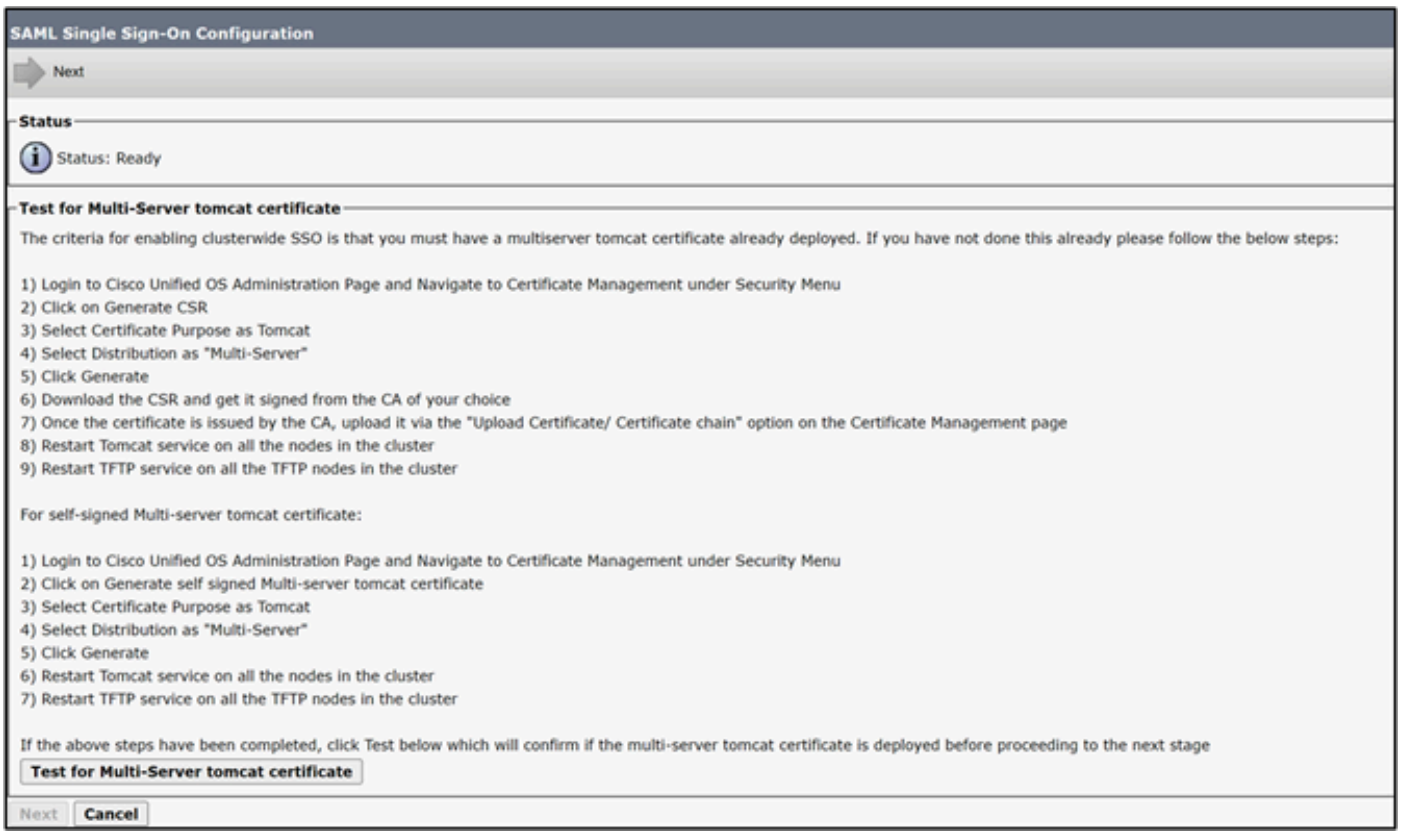
4. Abilita SSO nel cluster CUCM

- Selezionare Amministrazione CM > Sistema > Single Sign-On
- Con le stesse opzioni SSO selezionate durante l'esportazione dei metadati CUCM, selezionare Abilita SSO SAML e selezionare Continua.

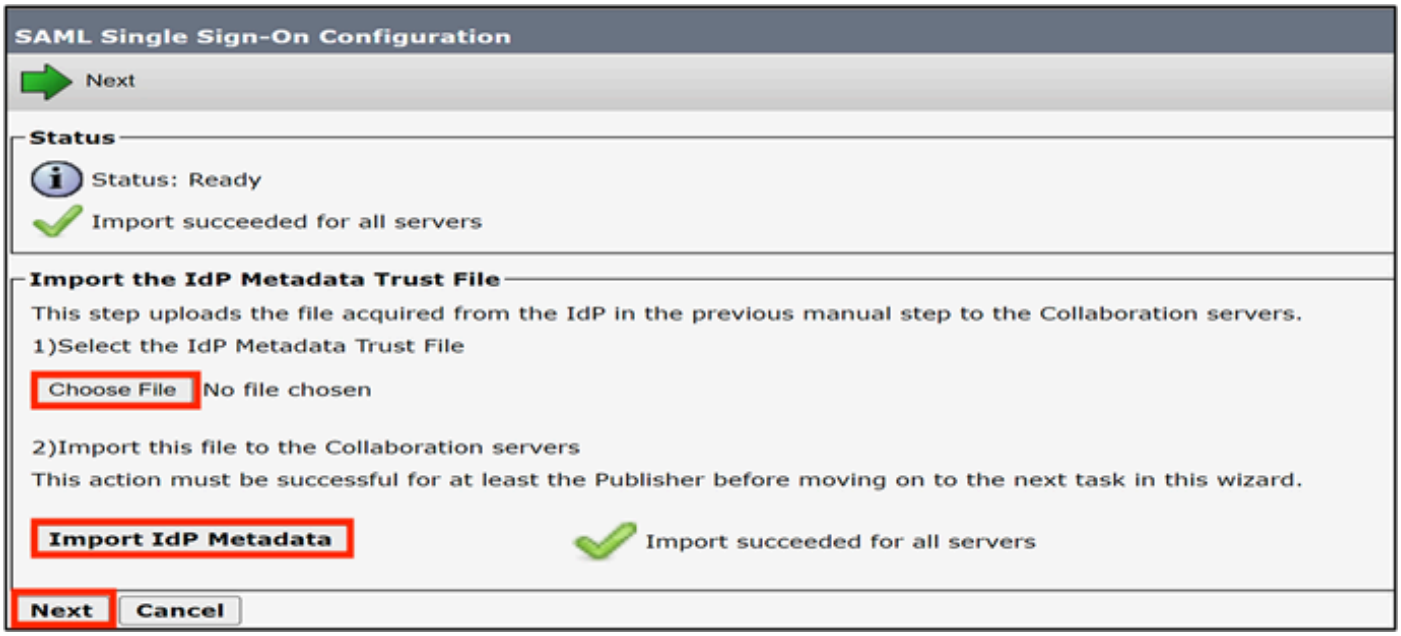




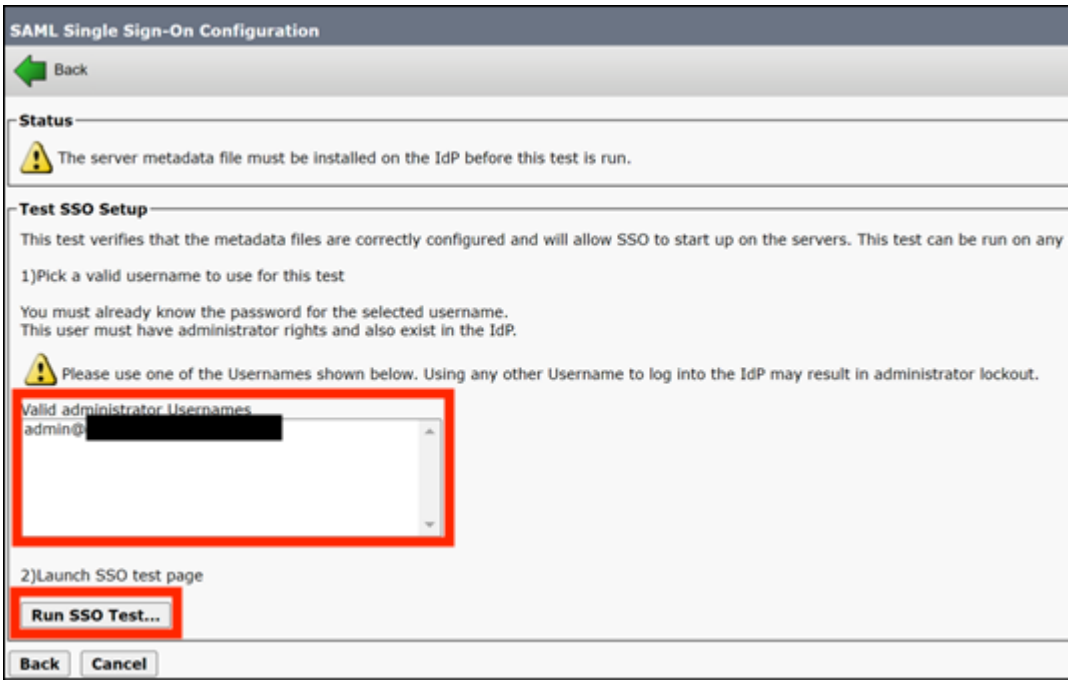
- Se a livello di cluster, questo passaggio è disponibile per controllare i certificati multi-san in tutti i nodi, selezionare Test for multi-server tomcat certificate. al termine, selezionare Avanti.

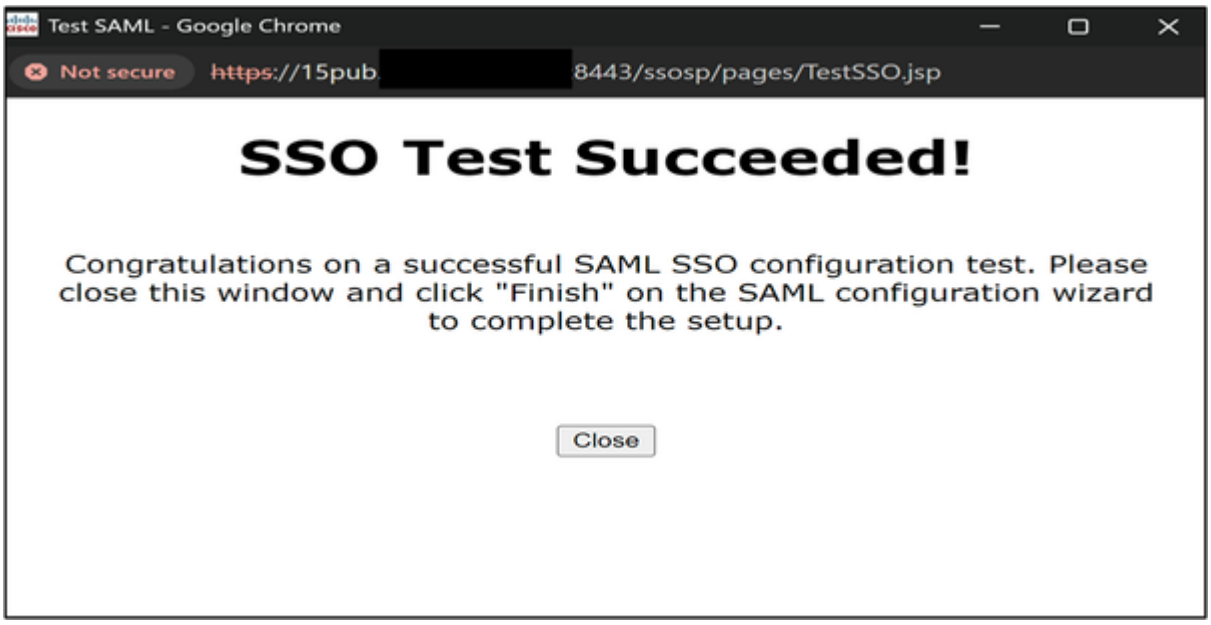


- Caricare i metadati IdP, selezionare Importa metadati IdP e al termine selezionare Avanti



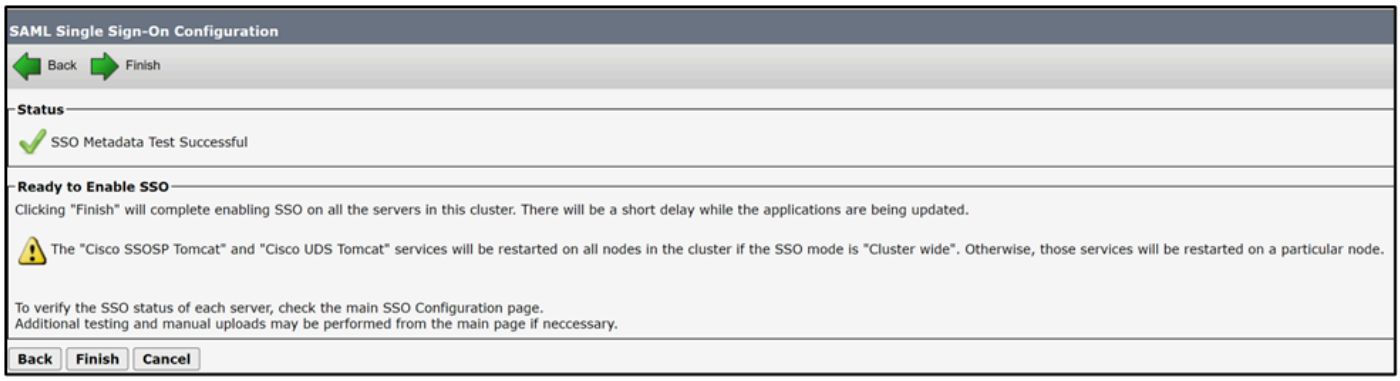
- In Test SSO Setup selezionare un utente a cui è assegnato il gruppo Standard CCM Super Users e selezionare Esegui test SSO fino al completamento dell'operazione.





4. Riavviare i servizi richiesti dopo l'abilitazione dell'SSO.

- Abilitazione di SSO per riavviare il servizio Tomcat.



Tuttavia, TAC consiglia di riavviare manualmente il servizio Tomcat (utils service restart Cisco Tomcat) e UDS Tomcat (utils service restart CiscoUDSTomcat) in tutti i nodi dopo il processo di abilitazione dell'SSO.

Scenario 3: Problemi di registrazione di mobilità e accesso remoto dopo il rinnovo del certificato

L'app Webex non è in grado di registrarsi a CUCM tramite Mobility and Remote Access (MRA) dopo il rinnovo dei certificati Call Manager, Tomcat ed Expressway C nelle distribuzioni in modalità mista.

Verifica

1. Il gestore chiamate CUCM e il certificato Tomcat sono certificati firmati dalla CA.
2. La distribuzione di CUCM e Expressway viene eseguita in modalità mista (TLS).
3. ispezionare i registri di Expressway-C viene visualizzato "SSL routines:ssl3_read_bytes:tlsv1 alert known ca".
   <#root>

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]: UTCTime="2026-01-29 19:01:16,974" Module
HTTPMSG:
|GET /CSFmarcoalh.cnf.xml HTTP/1.1
 Host: expc.cisco.com:6972
 Accept: */*
 Cookie:<CONCEALED>
 User-Agent: WebEx/0.0.0.0
 TrackingID: fxxxxxxx-86f6-4030-8259-0b768c07723e
 Client-ip: xxx.xxx.xxx.xxx
 X-Forwarded-For: xxx.xxx.xxx.xxx, 127.0.0.1
 Via: https/1.1 vcs[0fxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxx-7feb-4xxx-9

 |

2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]:[ET_NET 1]ERROR:SSL connection failed for

SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca
```

Soluzione

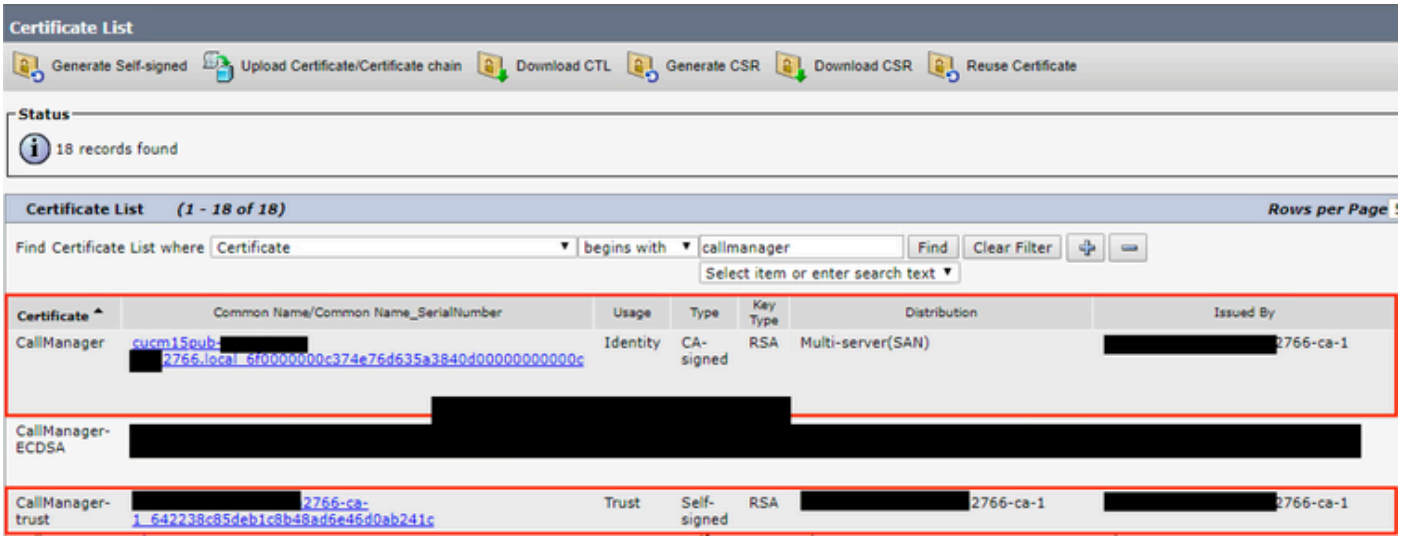
Esporta e importa certificati tra CUCM ed Expressway-C per garantire la relazione di trust.

⚠ Attenzione: TAC consiglia di eseguire questa operazione fuori orario poiché questa procedura richiede il riavvio dei servizi. L'impatto sul business è

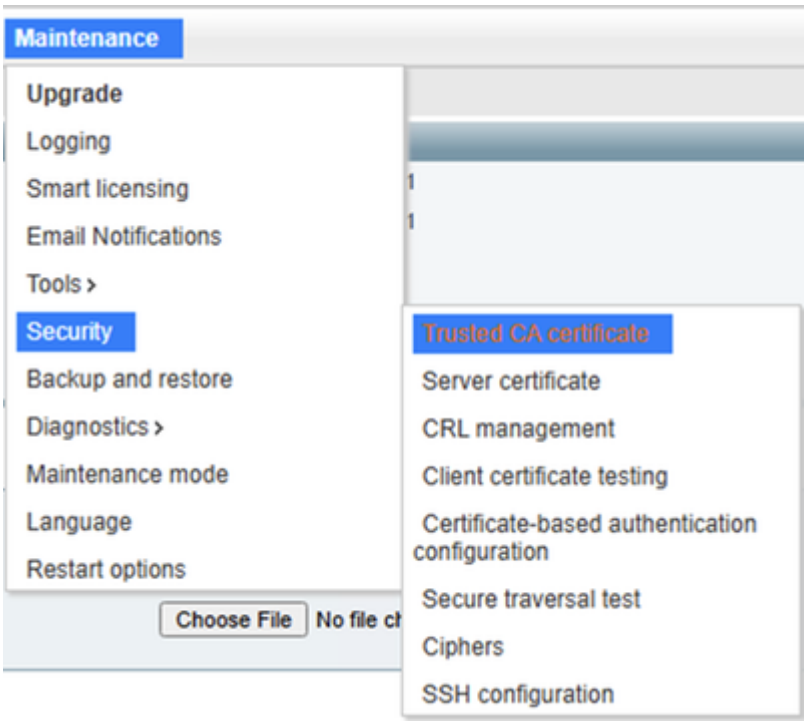

Medium Impact.

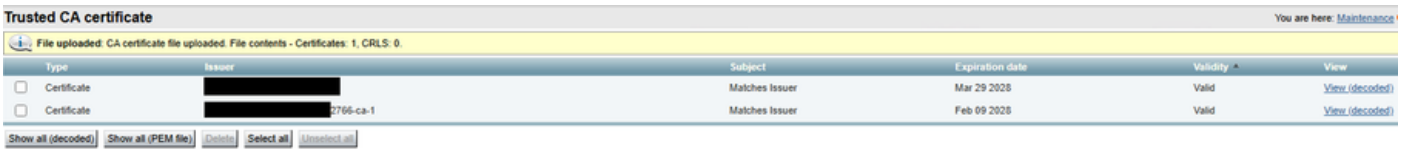
1. Procedura per completare la relazione di trust tra CUCM ed Expressway con certificati firmati da CA

Passare a Amministrazione sistema operativo > Sicurezza > Gestione certificati e scaricare il certificato CA radice e gli eventuali componenti intermedi che firmano i certificati Call Manager e Tomcat.



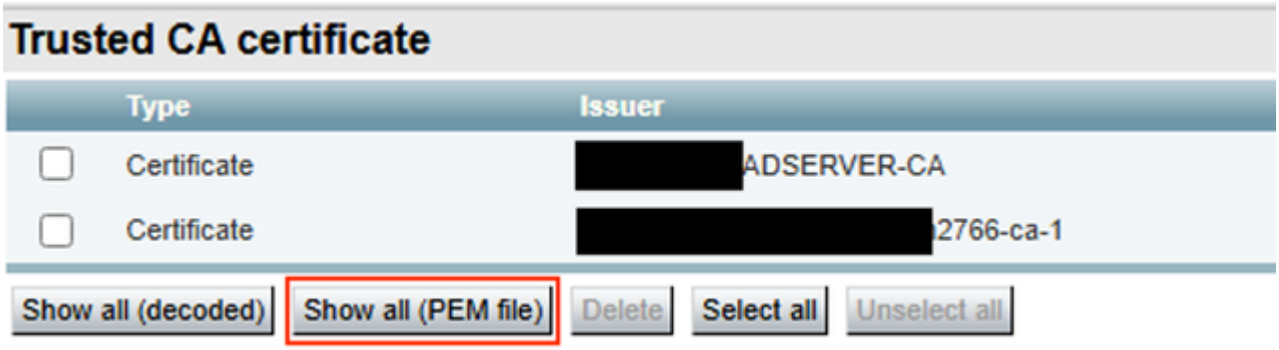
Passare quindi a Expressway-C > Manutenzione > Sicurezza > Certificato CA attendibile e caricare il certificato CA di Call Manager e il certificato Tomcat.



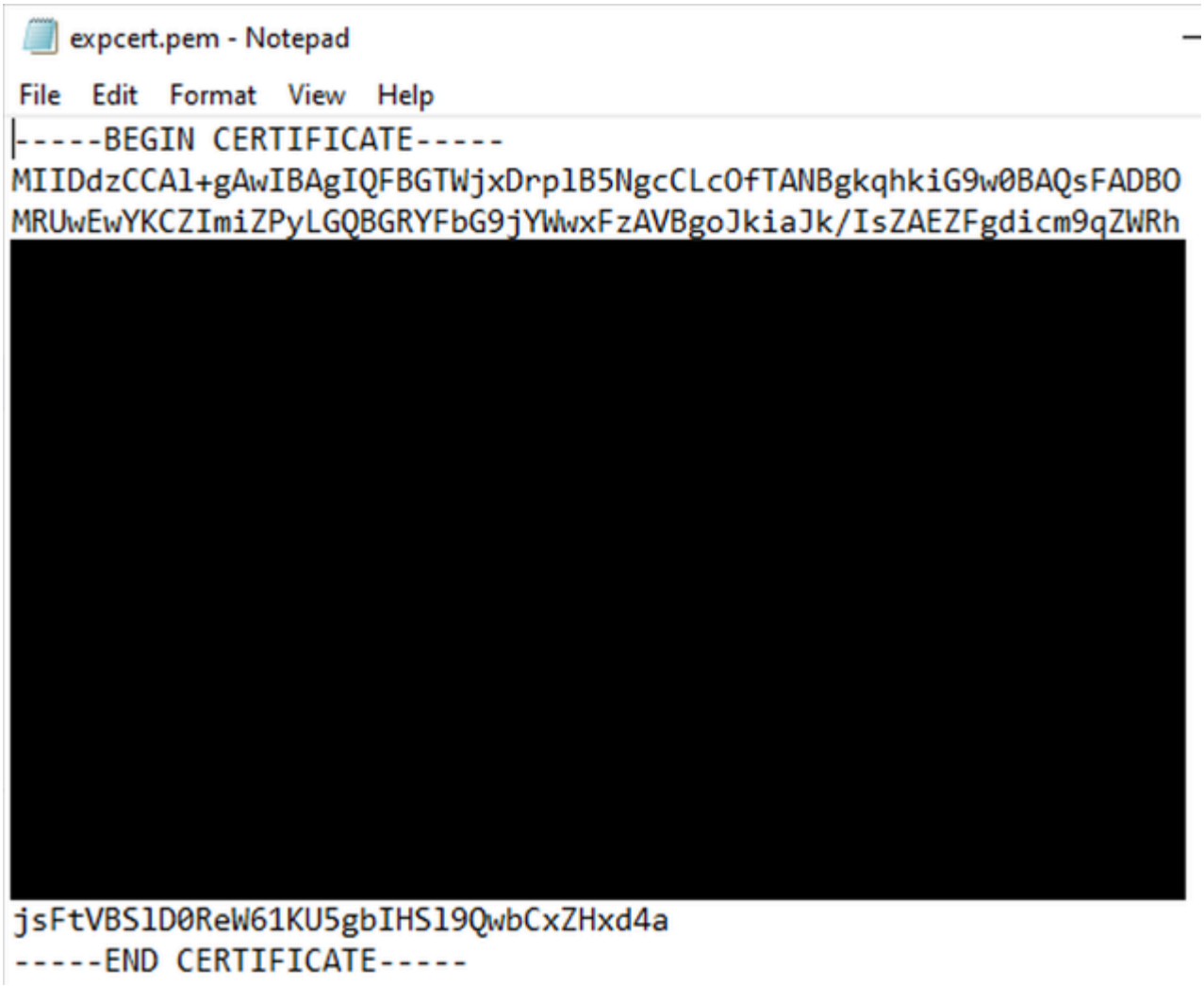


Nota: Negli scenari con il certificato Call Manager e Tomcat autofirmato, scaricare il certificato Call Manager e Tomcat e caricarlo su Expressway.

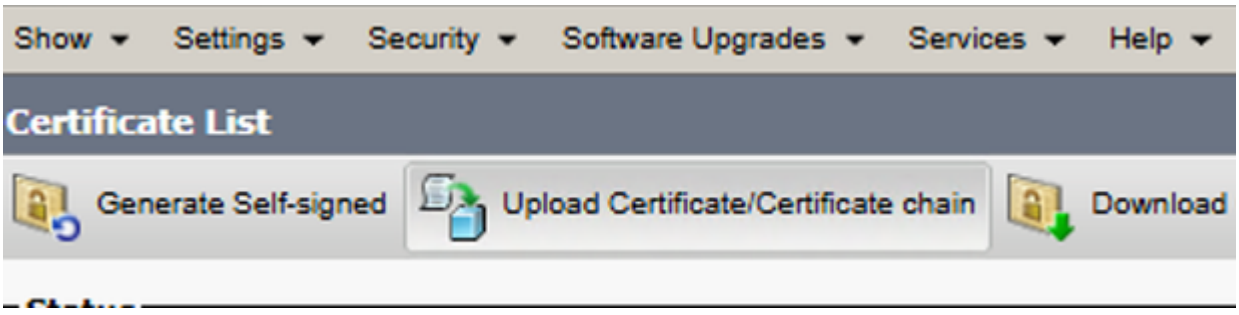
Passare a Expressway-C > Manutenzione > Sicurezza > Certificato CA attendibile > Mostra tutto (file PEM)

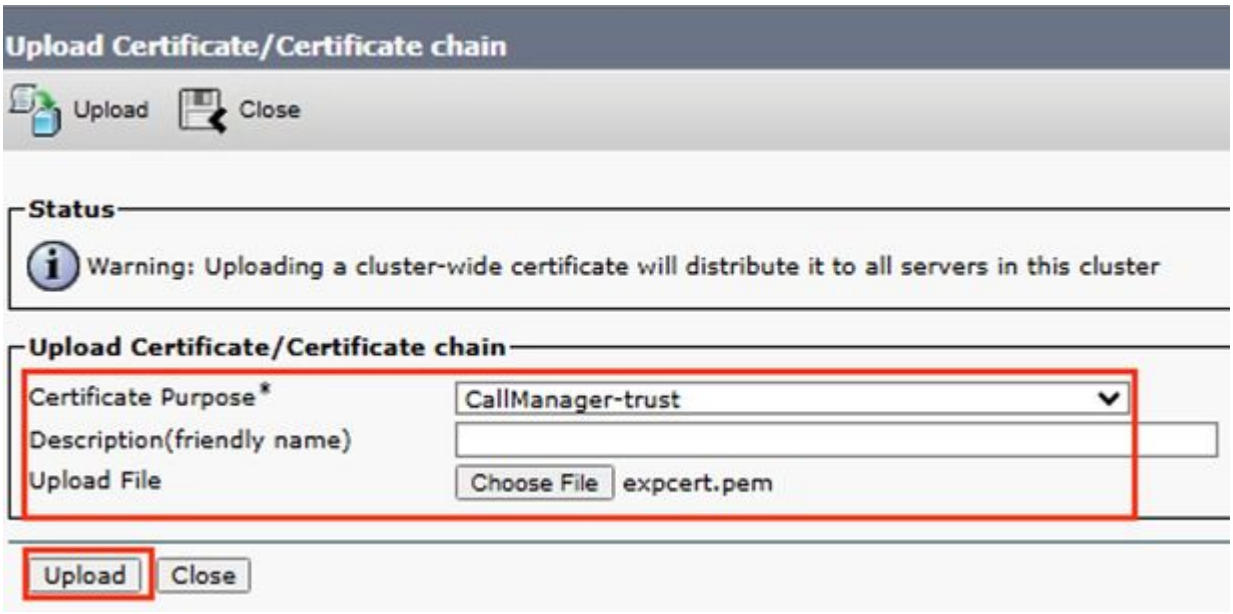


Copiare il valore PEM del certificato CA che firma Expressway-C e salvarlo in un file di testo.



Passare a Amministrazione sistema operativo > Sicurezza > Gestione certificati e selezionare Carica certificato/catena certificati e caricare il certificato CA expressway-C come Tomcat-trust e Call Manager-trust





Riavviare i servizi necessari nel cluster CUCM:

- Passare a Cisco Unified Serviceability > Tools > Control Center - Feature Services e riavviare il servizio Cisco CallManager in tutti i nodi in cui è in esecuzione.
- Passare a Cisco Unified Serviceability > Tools > Control Center - Feature Services e riavviare il servizio Cisco TFTP in tutti i nodi in cui è in esecuzione.
- Riavviare il servizio Tomcat in tutti i nodi del cluster tramite CLI con il comando utils service restart Cisco Tomcat.
- Riavviare il servizio Cisco HAproxy in tutti i nodi del cluster tramite CLI con il comando utils service restart Cisco HAPproxy.

Scenario 4: Causa del rinnovo del certificato della funzione proxy dell'autorità di certificazione

Scenario 4.1: autenticazione 802.1x non riuscita

Il telefono non viene autenticato con ASA dopo la rigenerazione del certificato CAPF (Certificate Authority Proxy Function) sull'editore CUCM.

Verifica

1. Nei messaggi di stato del telefono viene visualizzato "Autenticazione 802.1x: Non riuscito"

2. Esaminare le note telefonate del server interessato e individuare "SSL_ERROR_WANT_READ"

```
4592 NOT Feb 17 11:01:25.041733 (349-349) PAE: -Secure Connection Handshake in progress - status SSL_ER
4593 NOT Feb 17 11:01:25.041826 (349-349) PAE: -EV_REQUEST_REC, ST_AUTHENTICATING->ST_AUTHENTICATING
++ EAP-Failure
4594 NOT Feb 17 11:01:25.041898 (349-349) PAE: -send EAP-Resp/TLS - id 9
4595 NOT Feb 17 11:01:25.042032 (349-349) PAE: -authWhile timer set: 30 sec
4596 NOT Feb 17 11:01:27.061822 (349-349) PAE: -[0001-0] 08-cc-a7-1c-bb-ae vid=0xfff=4095 static=0 pri=
4597 NOT Feb 17 11:01:27.061950 (349-349) PAE: -port=0
4598 NOT Feb 17 11:01:27.062009 (349-349) PAE: -cprCdpGetPort address:  8:CC:A7:1C:BB:AE  Phyport=0 app
4599 NOT Feb 17 11:01:27.062068 (349-349) PAE: - >>>>>>>>>>>>>> port obtained = 0 for mac macAddress 08:
4600 NOT Feb 17 11:01:27.062134 (349-349) PAE: -rcvd EAP-Failure
4601 NOT Feb 17 11:01:27.062189 (349-349) PAE: -EV_FAILURE, ST_AUTHENTICATING->ST_HELD
4602 WRN Feb 17 11:01:27.062462 (349-349) PAE: -802.1X auth FAILED
4603 NOT Feb 17 11:01:27.062550 (349-349) PAE: -paeInfoToInetd: PAE info sent to NETSD
4604 NOT Feb 17 11:01:27.062717 (1786-1880) JAVA-Calling handleNetSDEvent
4605 WRN Feb 17 11:01:27.062953 (1786-1880) JAVA-Thread-11|cip.sec.Security:? - Security: Received a pr
4606 DEB Feb 17 11:01:27.063039 (1786-1880) JAVA-openQue(): que->/tmp/pae_msg_que, key->0x101019ab
4607 DEB Feb 17 11:01:27.063069 (1786-1880) JAVA-openQue(): que->/tmp/pae_rsp_que, key->0x10101c4c
4608 DEB Feb 17 11:01:27.063091 (1786-1880) JAVA-getpaeinfo: send pae info message paeCmd.mtype=1880, p
4609 DEB Feb 17 11:01:27.063121 (1786-1880) JAVA-getpaeinfo: recv pae info resp ret=-1, errno=No messag
4610 NOT Feb 17 11:01:27.063306 (349-349) PAE: -paeInfoToInetd: Netsd event NETSD_EV_PAE sent to NETSD
4611 NOT Feb 17 11:01:27.063370 (349-349) PAE: - PAE RE-AUTH, not sending SEC_DOWN Netsd event for CDP
4612 NOT Feb 17 11:01:27.063423 (349-349) PAE: -paeSetLastSupStatus: LastSupStatus 0
4613 NOT Feb 17 11:01:27.063475 (349-349) PAE: -heldWhile timer set: 60 sec
4614 NOT Feb 17 11:01:27.064074 (349-349) PAE: -paeNetsdRcvMsg(349): PAE event: status: FAIL : Resource
```

Soluzione

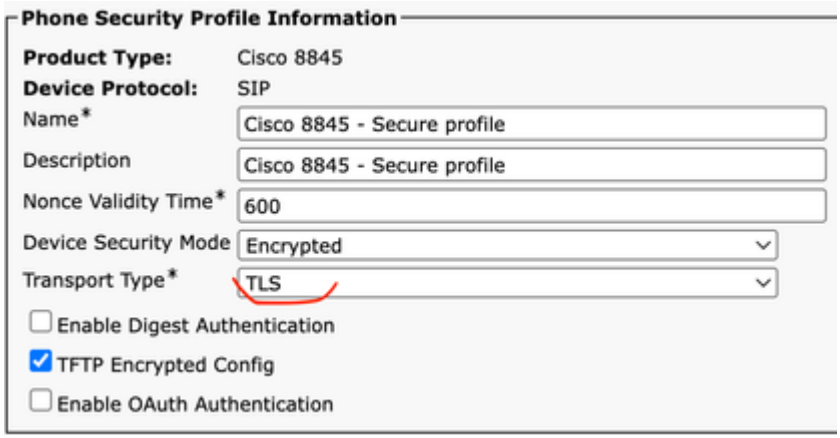
Scaricare il certificato CAPF dal publisher CUCM e caricarlo sul server di autenticazione, ignorare 802.1x per consentire la registrazione e installare il certificato LSC sui telefoni interessati.

Scenario 4.2: I telefoni non vengono registrati con CUCM che utilizza il profilo di sicurezza in modalità TLS.

I telefoni mostrano "Il telefono sta registrando" dopo la rigenerazione del certificato CAPF sull'editore CUCM.

Verifica

1. I telefoni interessati contengono il profilo di sicurezza con la modalità TLS abilitata.



2. Sui telefoni interessati è installato un certificato LSC.
3. Verificare che il certificato CAPF sia aggiornato.

4. Accedere all'editore CUCM e usare il comando show ctl che mostra il numero di serie del certificato CAPF precedente.
5. Modificare quindi il profilo di sicurezza del telefono in non protetto.

Soluzione

Rigenerare il file CTL in CUCM e riavviare i servizi necessari per assicurarsi che i telefoni ricevano il nuovo file CTL con il file CAPF.

⚠ Attenzione: TAC consiglia di eseguire questa operazione fuori orario poiché questa procedura richiede il riavvio dei servizi. L'impatto sul business è

Medium Impact.

Procedura per garantire il corretto rinnovo del CAPF.


```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n): y

Updating CTL file
CTL file Updated
Please reset all Encrypted and Authenticated phones for the CTL file updates to take effect.
```

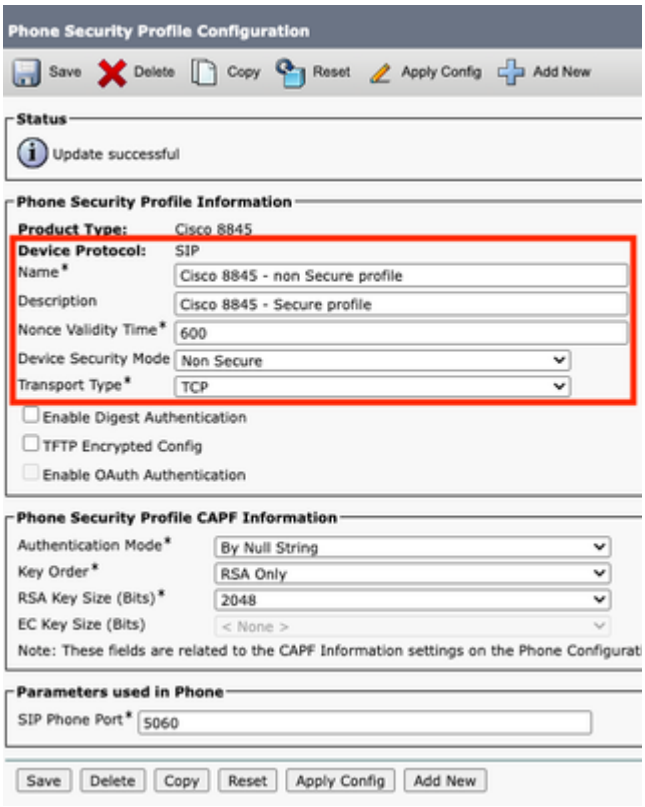
Aggiorna il file CTL dopo la rigenerazione di CAPF. Accedere alla CLI del server di pubblicazione e immettere il comando utils ctl update CTLFile.

1. Passare a Cisco Unified Serviceability > Tools > Control Center - Feature Services in CUCM publisher e riavviare il servizio CAPF.
2. Passare a Cisco Unified Serviceability > Tools > Control Center - Network Services e riavviare Cisco Trust Verification Service in tutti i nodi in cui è in esecuzione.
3. Passare a Cisco Unified Serviceability > Strumenti > Control Center - Servizi funzionalità e riavviare il servizio TFTP Cisco in tutti i nodi in cui è in esecuzione

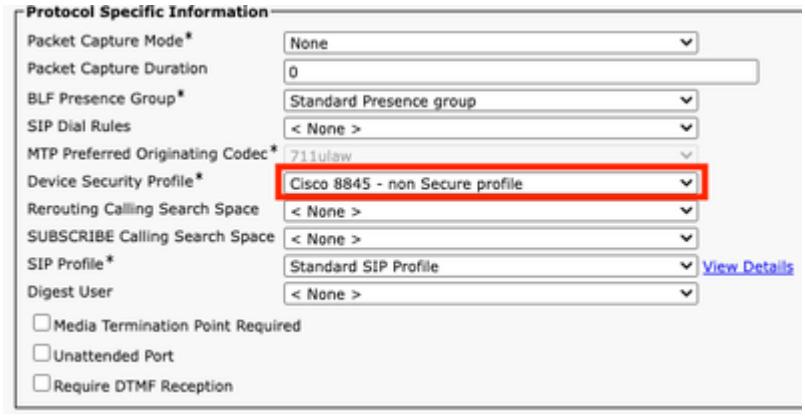
- Passare a Amministrazione CM > Sistema > Sicurezza > Profilo sicurezza telefono.

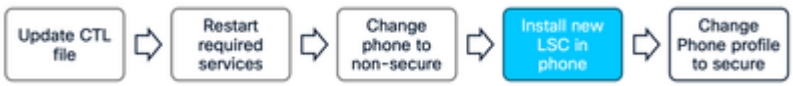
- Copia il profilo di sicurezza telefono corrente assegnato ai telefoni richiesti.

- Cambiare Nome e Modalità di protezione dispositivo in Non sicuro e selezionare Salva e applica configurazione per applicare la modifica a tutti i telefoni richiesti.



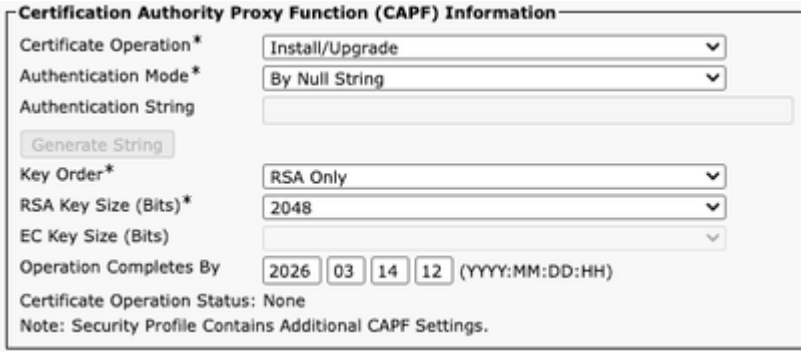
- Applicare il profilo di sicurezza del dispositivo creato alla configurazione dei telefoni richiesta, selezionare Salva e applica configurazione.





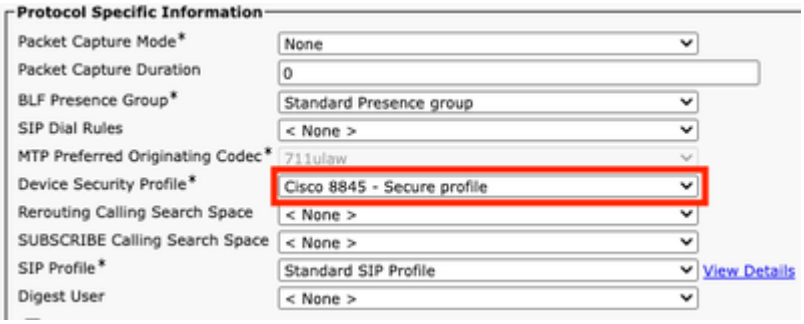
Utilizzare la sezione CAPF information (informazioni in lingua inglese) nella configurazione del dispositivo dei telefoni interessati per installare il certificato LSC nei telefoni richiesti.

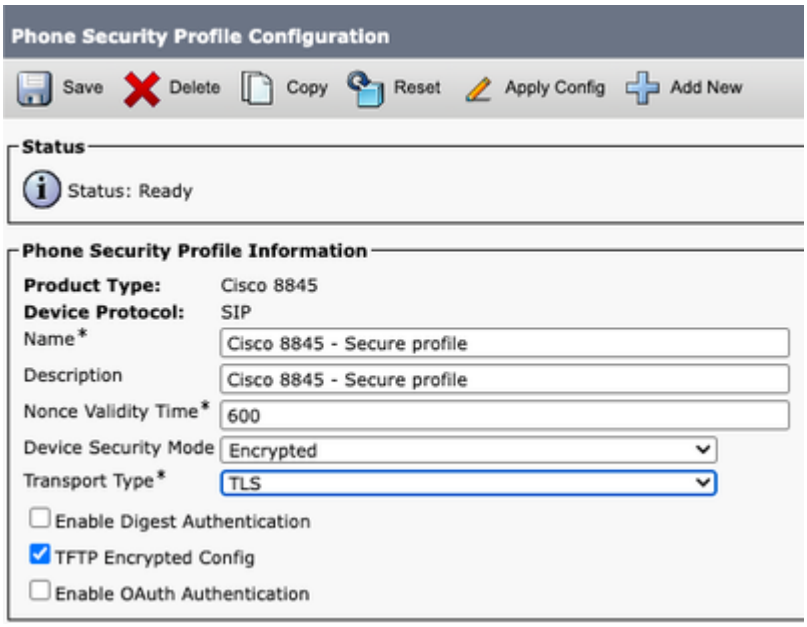
- In Informazioni CAPF, selezionare Installa/Aggiorna in Operazione certificato.



- Selezionare Save and Apply Config (Salva e applica configurazione).
- Attendere finché in Stato operazione certificato non verrà visualizzato il messaggio Operazione completata.

Nella sezione Informazioni specifiche del protocollo in Configurazione telefono, selezionare il profilo di sicurezza con TLS abilitato che è stato creato.





Informazioni correlate

- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/214231-certificate-regeneration-process-for-cis.html
- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/217138-regeneration-of-cucm-ca-signed-certifica.html
- https://www.cisco.com/c/en/us/support/docs/content-networking/certificates/213295-how-to-install-an-lsc-on-a-cisco-ip-phon.html
- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-2/mra/exwy_b_mra-deployment-guide-x152.html

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).