Configurazione di LSC su IP Phone con CUCM

Sommario

Introduzione

In questo documento viene descritto come installare un certificato LSC (Locally Significant Certificate) su un telefono IP Cisco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Opzioni della modalità di protezione cluster di Cisco Unified Communications Manager (CUCM)
- Certificati X.509
- Certificati di produzione installati (MIC)
- LCS
- Operazioni sui certificati CAPF (Certificate Authority Proxy Function)
- Protezione predefinita (SBD)
- File dell'elenco di attendibilità iniziale (ITL)

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni di CUCM che supportano SBD, ovvero CUCM 8.0(1) e versioni successive.

> **Nota**: riguarda solo i telefoni che supportano la funzione di sicurezza predefinita (SBD, Security By Default). Ad esempio, i telefoni 7940 e 7960 non supportano SBD, né i telefoni da conferenza 7935, 7936 e 7937. Per un elenco dei dispositivi che supportano SBD nella versione di CUCM in uso, selezionare **Cisco Unified Reporting > System Reports > Unified CM Phone Feature List** (Report di sistema > Elenco funzionalità telefoniche di Unified CM) ed eseguire un report su Feature: Security

---

by Default (Funzionalità: sicurezza per impostazione predefinita).

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

MIC e LSC

Se si usa l'autenticazione basata sui certificati per le VPN telefoniche 802.1X o Anyconnect, è importante comprendere la differenza tra i MIC e gli LSC.

Ogni telefono Cisco è dotato di un microfono preinstallato in fabbrica. Questo certificato è firmato da uno dei certificati CA di Cisco Manufacturing, dal certificato CA di Cisco Manufacturing, CA SHA2 di Cisco Manufacturing, CAP-RTP-001 o CAP-RTP-002. Quando il telefono presenta questo certificato, dimostra che si tratta di un telefono Cisco valido, ma questo non convalida che il telefono appartenga a un cliente specifico o a un cluster CUCM. Potrebbe trattarsi di un telefono non autorizzato acquistato sul mercato o trasferito da un altro sito.

Le schede LSC, invece, vengono installate intenzionalmente sui telefoni da un amministratore e sono firmate dal certificato CAPF di CUCM Publisher. È possibile configurare la VPN 802.1X o Anyconnect in modo che consideri attendibili solo le licenze LSC rilasciate da autorità di certificazione CAPF note. L'autenticazione dei certificati basata su LCS anziché su MIC offre un controllo molto più granulare dei dispositivi telefonici considerati attendibili.

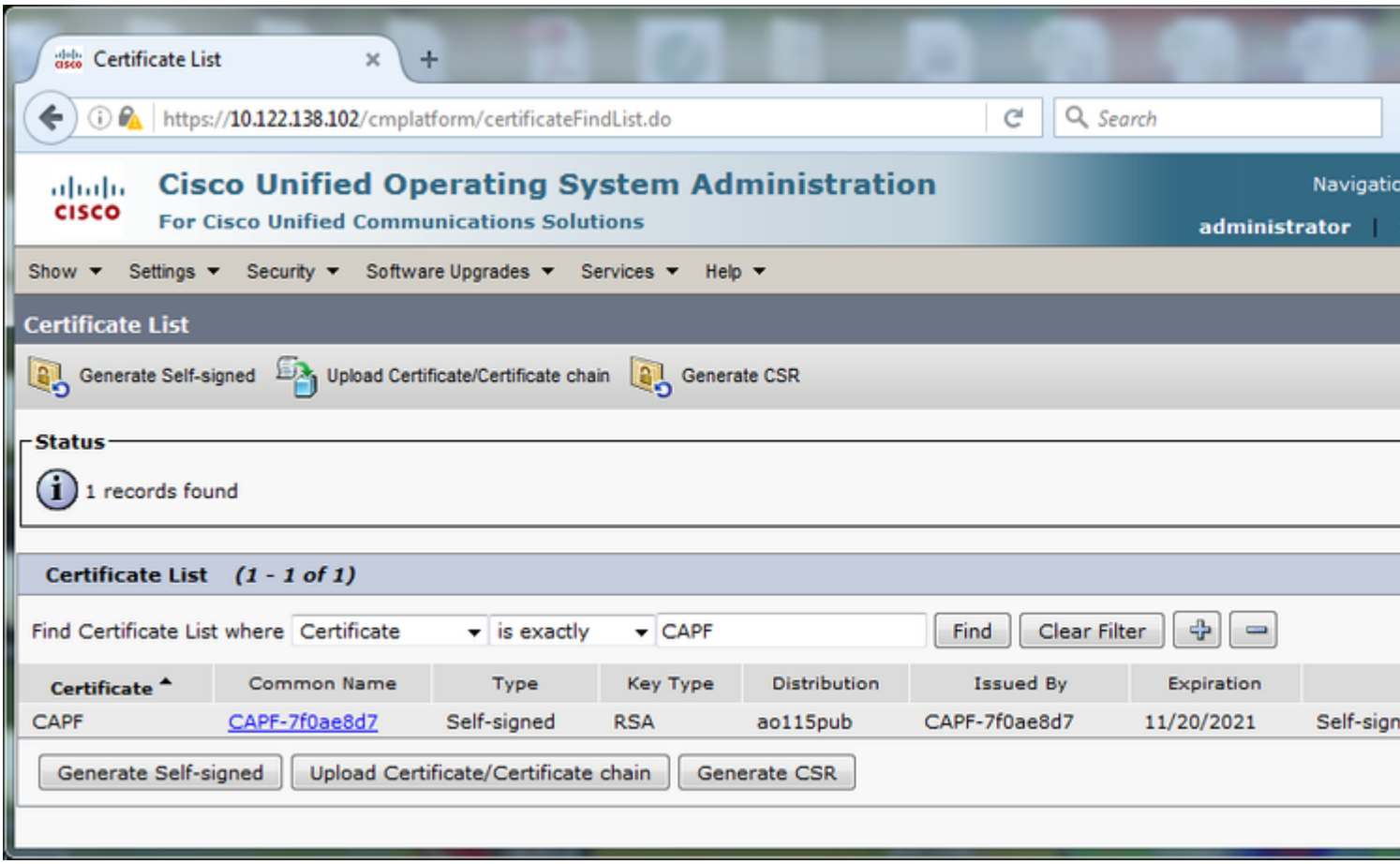
Configurazione

Topologia della rete

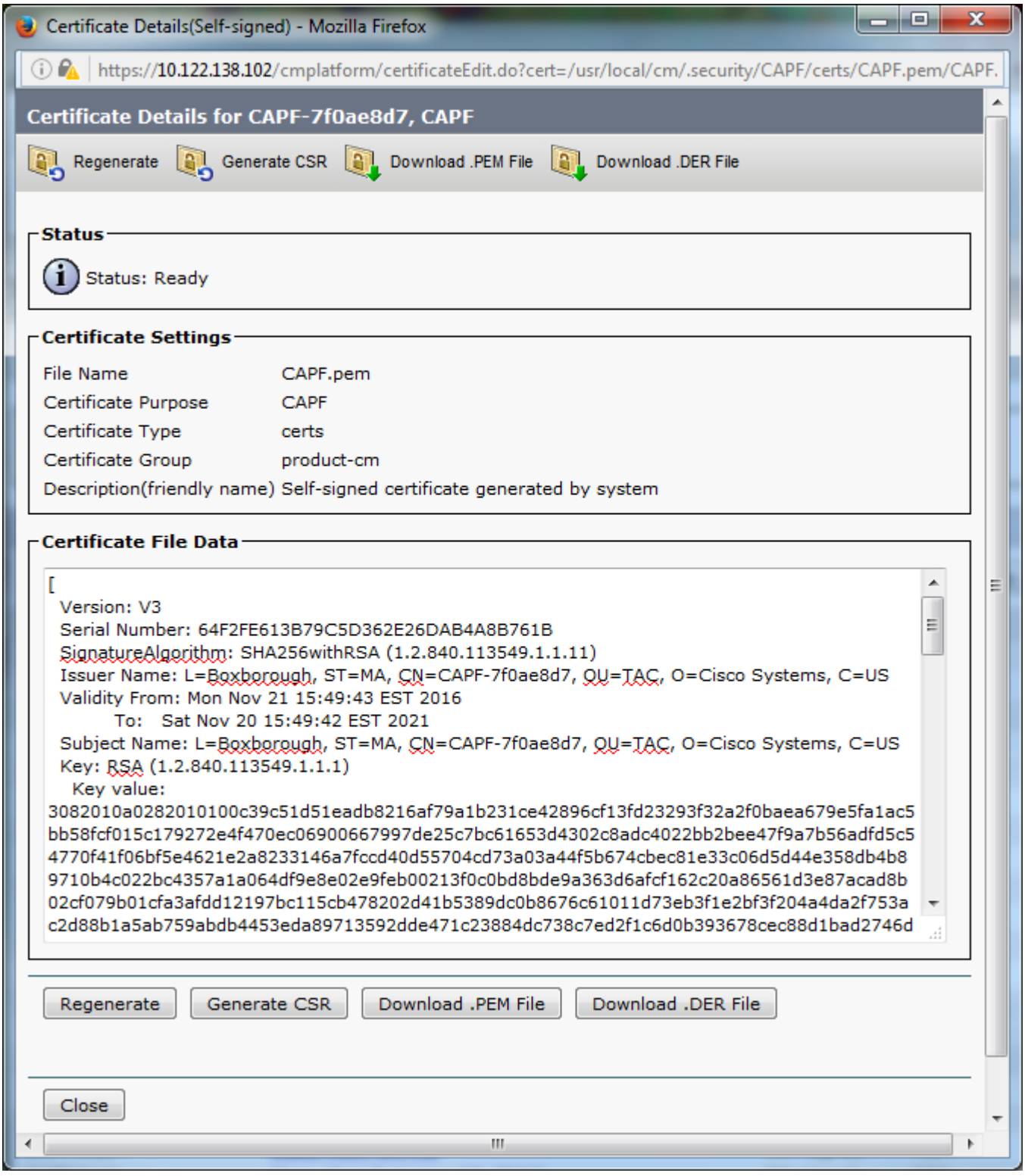
Per questo documento sono stati utilizzati i seguenti server lab CUCM:

- ao115pub - 10.12.138.102 - CUCM Publisher e server TFTP
- ao115sub - 10.122.138.103 - Sottoscrittore CUCM e server TFTP

Verificare che il certificato CAPF non sia scaduto o stia per scadere in un prossimo futuro. Passare a **Cisco Unified OS Administration > Security > Certificate Management** (Amministrazione del sistema operativo unificato Cisco > Sicurezza > Gestione certificati), quindi **Trova elenco certificati in cui Certificate è esattamente CAPF**, come mostrato nell'immagine.



Per aprire la pagina Dettagli certificato, fare clic su **Nome comune**. Controllare le date di Validità - Da: e Validità - A: nel riquadro **Dati file certificato** per determinare la data di scadenza del certificato, come illustrato nell'immagine.



Se il certificato CAPF è scaduto o sta per scadere, rigenerarlo. Non procedere con il processo di installazione di LSC con un certificato CAPF scaduto o prossimo alla scadenza. In questo modo si evita la necessità di riemettere gli LCS nel prossimo futuro a causa della scadenza dei certificati CAPF. Per informazioni su come rigenerare il certificato CAPF, fare riferimento all'articolo Processo di rigenerazione/rinnovo del certificato CUCM.

Analogamente, se è necessario che il certificato CAPF sia firmato da un'autorità di certificazione di terze parti, in questa fase è possibile scegliere di eseguire questa operazione. Completare la generazione e l'importazione del file CSR (Certificate Signing Request) del certificato CAPF firmato oppure continuare la configurazione con un LSC autofirmato per un test preliminare. Se è necessario un certificato CAPF firmato da terze parti, in genere è consigliabile configurare questa funzionalità innanzitutto con un certificato CAPF

autofirmato, testare e verificare, quindi ridistribuire gli LCS firmati da un certificato CAPF firmato da terze parti. Ciò semplifica la successiva risoluzione dei problemi, se i test con il certificato CAPF firmato da terze parti hanno esito negativo.

Avviso: se si rigenera il certificato CAPF o si importa un certificato CAPF firmato da terze parti mentre il servizio CAPF è attivato e avviato, i telefoni vengono reimpostati automaticamente da CUCM. Completare queste procedure in una finestra di manutenzione quando è possibile ripristinare i telefoni. Per riferimento, vedere l'ID bug Cisco CSCue55353 - Aggiungere un avviso durante la rigenerazione di un certificato TV/CCM/CAPF reimpostato dal telefono

---

Nota: se la versione CUCM in uso supporta SBD, questa procedura di installazione LSC verrà applicata indipendentemente dal fatto che il cluster CUCM sia impostato o meno sulla modalità mista. SBD fa parte di CUCM versione 8.0(1) e successive. In queste versioni di CUCM, i file ITL contengono il certificato per il servizio CAPF sul server di pubblicazione CUCM. In questo modo i telefoni possono connettersi al servizio CAPF per supportare operazioni sui certificati come l'installazione/l'aggiornamento e la risoluzione dei problemi.

Nelle versioni precedenti di CUCM era necessario configurare il cluster per la modalità mista per supportare le operazioni sui certificati. Poiché non è più necessario, ciò riduce le barriere all'uso di LSC come certificati di identità telefonici per l'autenticazione 802.1X o per l'autenticazione dei client VPN AnyConnect.

Eseguire il comando **show itl** su tutti i server TFTP del cluster CUCM. Il file ITL contiene un certificato CAPF.

Ad esempio, di seguito è riportato un estratto dell'output **show itl** generato dal subscriber lab CUCM ao115sub.

Nota: nel file è presente una voce ITL Record con FUNCTION (FUNZIONE) di CAPF.

Nota: se il file ITL non dispone di una voce CAPF, accedere all'editore CUCM e verificare che il servizio CAPF sia attivato. Per confermare questa condizione, selezionare **Cisco Unified Serviceability > Strumenti > Service Activation > CUCM Publisher > Security**, quindi attivare il **servizio funzione proxy di Cisco Certificate Authority**. Se il servizio è stato disattivato e lo si è appena attivato, passare a **Cisco Unified Serviceability > Strumenti > Control Center - Feature Services > Server > CM Services**, quindi riavviare il servizio TFTP Cisco su tutti i server TFTP del cluster CUCM per rigenerare il file ITL. Inoltre, verificare di non aver premuto Cisco sull'ID bug CSCuj7830.

Nota: al termine, eseguire il comando **show itl** su tutti i server TFTP nel cluster CUCM per verificare che il certificato CAPF corrente di CUCM Publisher sia ora incluso nel file.

<#root>

```
ITL Record #:1


----
```

BYTEPOS TAG LENGTH VALUE

------- --- ------ -----

1 RECORDLENGTH 2 727

2 DNSNAME 2

3 SUBJECTNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US

4 FUNCTION 2 CAPF

5 ISSUERNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US

6 SERIALNUMBER 16 64:F2:FE:61:3B:79:C5:D3:62:E2:6D:AB:4A:8B:76:1B

7 PUBLICKEY 270

8 SIGNATURE 256

11 CERTHASH 20 C3 E6 97 D0 8A E1 0B F2 31 EC ED 20 EC C5 BC 0F 83 BC BC 5E

12 HASH ALGORITHM 1 null

ITL Record #:2

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 6B:99:31:15:D1:55:5E:75:9C:42:8A:CE:F2:7E:EA:E8
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 05 9A DE 20 14 55 23 2D 08 20 31 4E B5 9C E9 FE BD 2D 55 87
12 HASH ALGORITHM 1 null

ITL Record #:3

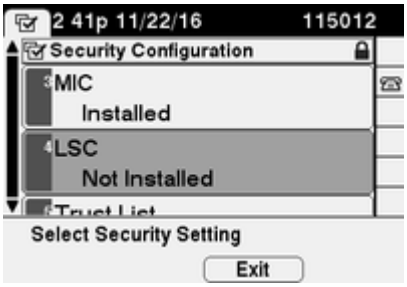
BYTEPOS TAG LENGTH VALUE

```
------- --- ------ -----
1 RECORDLENGTH 2 1680
2 DNSNAME 2
3 SUBJECTNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 51:BB:2F:1C:EE:80:02:16:62:69:51:9A:14:F6:03:7E
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 963 DF 98 C1 DB E0 61 02 1C 10 18 D8 BA F7 1B 2C AB 4C F8 C9 D5 (SHA1 Hash HEX)
This etoken was not used to sign the ITL file.

 ITL Record #:4
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 65:E5:10:72:E7:F8:77:DA:F1:34:D5:E3:5A:E0:17:41
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 00 44 54 42 B4 8B 26 24 F3 64 3E 57 8D 0E 5F B0 8B 79 3B BF
12 HASH ALGORITHM 1 null

 ITL Record #:5
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)
This etoken was used to sign the ITL file.

 ITL Record #:6
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)

 ITL Record #:7
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1031
2 DNSNAME 9 ao115sub
```

```
3 SUBJECTNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 53:CC:1D:87:BA:6A:28:BD:DA:22:B2:49:56:8B:51:6C
7 PUBLICKEY 97
8 SIGNATURE 103
9 CERTIFICATE 651 E0 CF 8A B3 4F 79 CE 93 03 72 C3 7A 3F CF AE C3 3E DE 64 C5 (SHA1 Hash HEX)

The ITL file was verified successfully.
```

Una volta confermata la voce CAPF come voce nell'ITL, è possibile completare un'operazione di certificazione su un telefono. In questo esempio viene installato un certificato RSA a 2048 bit tramite l'autenticazione di tipo String Null.

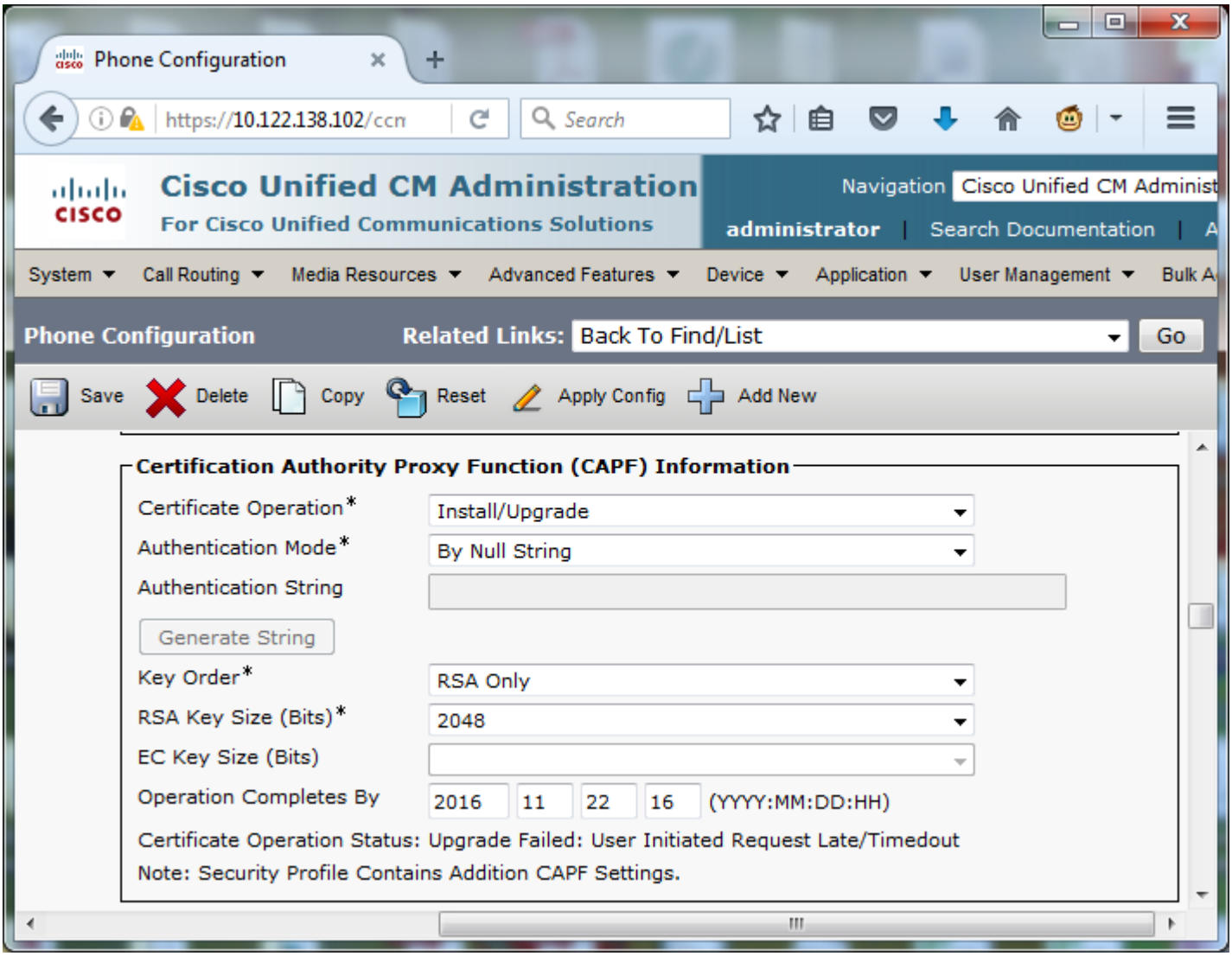
Al telefono, verificare che non sia ancora installato un LSC come mostrato nell'immagine. Ad esempio, su un telefono serie 79XX, selezionare **Settings > 4 - Security Configuration > 4 - LSC** (Impostazioni > 4 - Configurazione protezione > 4 - LSC).



Aprire la pagina di configurazione del telefono. Selezionare **Cisco Unified CM Administration > Device > Phone** (Amministrazione Cisco Unified CM > Dispositivo > Telefono).

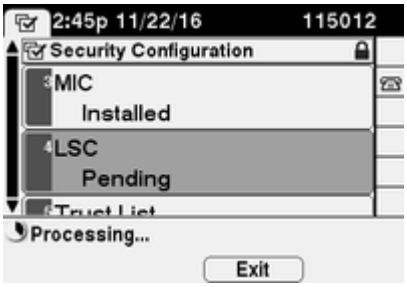
Immettere questi dettagli nella sezione CAPF Information della configurazione del telefono, come mostrato nell'immagine:

- Per Operazione certificato, scegliere **Installa/Aggiorna**
- Per Modalità di autenticazione, scegliere **Per stringa null**
- Per questo esempio, lasciare le opzioni Ordine chiavi, Dimensione chiave RSA (bit) e Dimensione chiave EC (bit) impostate sui valori predefiniti del sistema.
- Per Completamento operazione entro il, immettere una data e un'ora future di almeno un'ora.

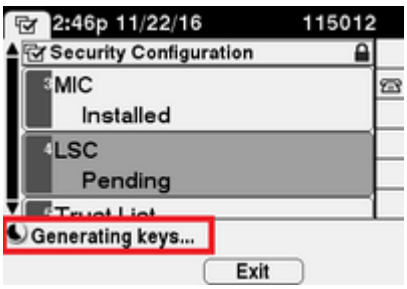


Salvare le modifiche alla configurazione, quindi **applicare la configurazione**.

Lo stato LSC sul telefono cambia in In sospeso come mostrato nell'immagine.



Il telefono genera i tasti come mostrato nell'immagine.



Il telefono viene reimpostato e al termine del ripristino, lo stato di LSC del telefono viene impostato su Installato, come mostrato nell'immagine.

Questo è visibile anche in Messaggi di stato nel telefono come mostrato nell'immagine.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per verificare l'installazione del certificato LSC su più telefoni, fare riferimento alla sezione Generate CAPF Report della Security Guide for Cisco Unified Communications Manager, release 11.0(1). In alternativa, è possibile visualizzare gli stessi dati all'interno dell'interfaccia Web di amministrazione CUCM utilizzando la procedura Trova telefoni per stato LSC o Stringa di autenticazione.

Per ottenere copie dei certificati LSC installati nei telefoni, fare riferimento all'articolo How to Retrieve Certificates from Cisco IP Phonesarticle.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Nessun server CAPF valido

Impossibile installare LSC. I messaggi di stato del telefono indicano **Nessun server CAPF valido**. Ciò indica che non esiste alcuna voce CAPF nel file ITL. Verificare che il servizio CAPF sia stato attivato, quindi riavviare il servizio TFTP. Verificare che il file ITL contenga un certificato CAPF dopo il riavvio, reimpostare il telefono per selezionare il file ITL più recente, quindi riprovare a eseguire l'operazione sul certificato. Se la voce del server CAPF nel menu delle impostazioni di sicurezza del telefono viene visualizzata come nome host o nome di dominio completo, verificare che il telefono sia in grado di risolvere la voce in un indirizzo IP.

LSC: Connessione non riuscita

Impossibile installare LSC. Nei messaggi di stato del telefono viene visualizzato **LSC: Connessione non riuscita**. Ciò può indicare una delle seguenti condizioni:

- Mancata corrispondenza tra il certificato CAPF nel file ITL e il certificato corrente. Il servizio CAPF è in uso.
- Il servizio CAPF è stato arrestato o disattivato.
- Il telefono non può raggiungere il servizio CAPF tramite la rete.

Verificare che il servizio CAPF sia attivato, riavviare il servizio CAPF, riavviare i servizi TFTP in tutto il cluster, reimpostare il telefono per selezionare l'ultimo file ITL, quindi riprovare l'operazione di certificato. Se il problema persiste, acquisire un pacchetto dal telefono e dal server di pubblicazione CUCM e analizzare per verificare se è presente una comunicazione bidirezionale sulla porta 3804, la porta predefinita del servizio CAPF. In caso contrario, è possibile che si sia verificato un problema di rete.

LSC: non riuscito

Impossibile installare LSC. Nei messaggi di stato del telefono viene visualizzato **LSC: Operazione non riuscita**. Nella pagina Web Configurazione telefono viene visualizzato **Stato operazione certificato: aggiornamento non riuscito: ritardo richiesta avviata dall'utente/timeout**. Ciò indica che l'operazione viene completata entro la data e l'ora sono scadute o sono già trascorse. Immettere una data e un'ora successive di almeno un'ora, quindi riprovare a eseguire l'operazione sul certificato.

LSC: Operazione in sospeso

Impossibile installare LSC. Nei messaggi di stato del telefono viene visualizzato **LSC: Connessione non riuscita**. La pagina Configurazione telefono mostra **Stato operazione certificato: operazione in sospeso.** Esistono diversi motivi per cui è possibile visualizzare **Stato operazione certificato:** stato **operazione in sospeso**. Alcuni di essi possono includere:

- ITL al telefono è diverso da quello attualmente utilizzato sui server TFTP configurati.
- Problemi con ITL corrotti. In questo caso, i dispositivi perdono lo stato di attendibilità e il comando **utilizza itl reset localkey** deve essere eseguito dall'editore CUCM per forzare i telefoni a usare ora il certificato ITLRecovery. Se il cluster è in modalità mista, è necessario utilizzare il comando **utils ctl reset localkey.** Successivamente, viene visualizzato un esempio di ciò che è possibile vedere quando si tenta di visualizzare un ITL danneggiato dalla CLI di CUCM. Se si verifica un errore durante il tentativo di visualizzare l'ITL e di eseguire il comando **utils itl reset localkey** ma viene visualizzato il secondo errore, è possibile che l'ID bug Cisco sia CSCus33755. Verificare se la versione di CUCM è interessata.

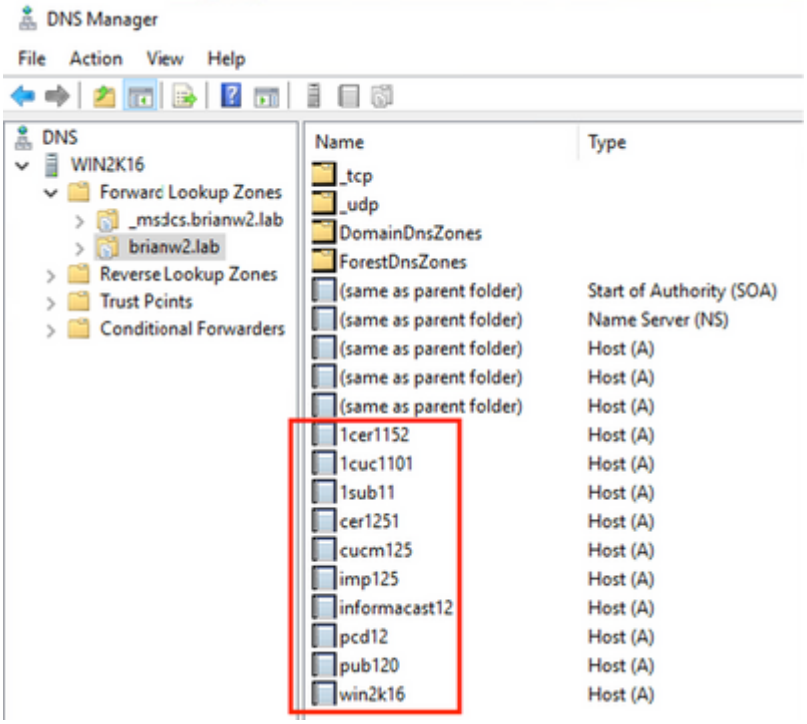
```
admin:show itl
Length of ITL file: 0
ITL File not found. To generate an ITL file, activate or restart the Cisco TFTP service as thi
servers.
Error parsing the ITL File.


admin:utils itl reset localkey
Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Unable to determine the active and running  TFTP nodes in the cluster
Ensure that the DB replication is working on all nodes and the correct Password has been en
Then retry the command

Executed command unsuccessfully
chmod: changing permissions of `/var/log/active/cm/trace/dbl/sdi/replication_scripts_output
```

- I telefoni non riescono ad autenticare la nuova LSC a causa di un errore della TV.
- Il telefono utilizza il certificato MIC, ma nella sezione Informazioni sulla funzione CAPF (Certificate Authority Proxy Function) della pagina di configurazione dei telefoni la modalità di autenticazione è impostata su Da certificato esistente (Precedenza a LSC).
- Il telefono non è in grado di risolvere l'FQDN di CUCM.

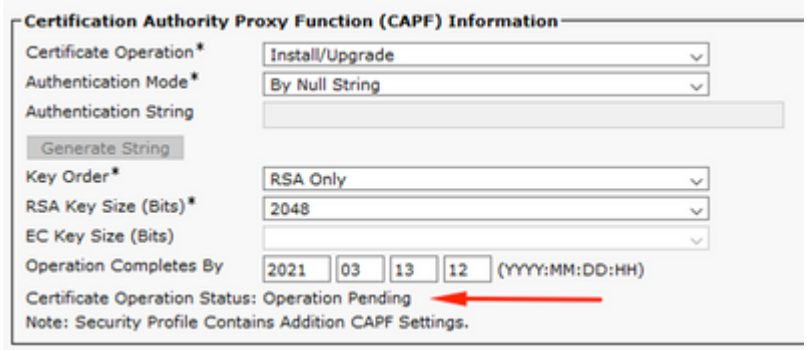
Per l'ultimo scenario, viene configurato un ambiente lab per simulare ciò che sarebbe visualizzato nei log se un telefono non fosse stato in grado di risolvere il FQDN di CUCM. Attualmente, il laboratorio è configurato con questi server:

- Server di pubblicazione e sottoscrittore CUCM con versione 11.5.1.15038-2
- Installazione di Windows 2016 Server come server DNS

Per il test, non è presente una voce DNS per il server CUCM PUB11 configurato.



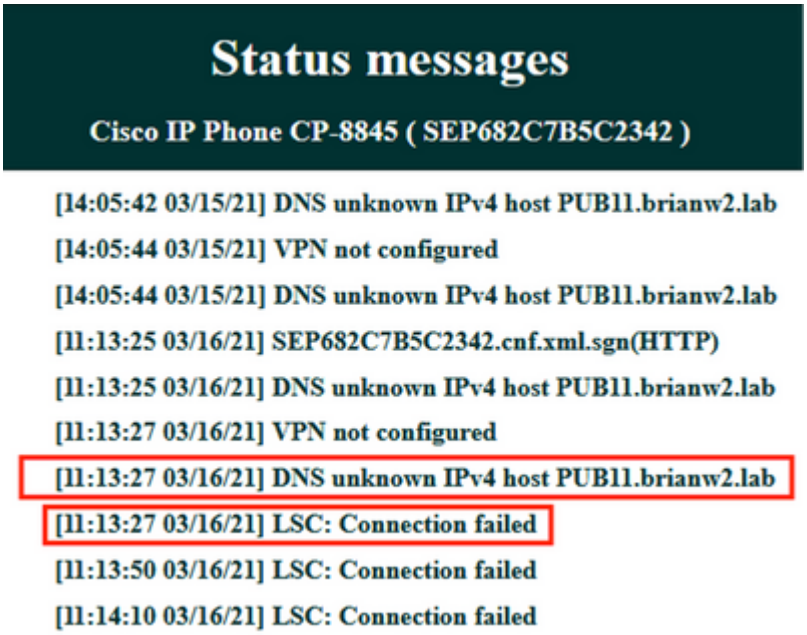
Tentativo di spingere un LSC su uno dei telefoni (8845) in laboratorio. Verificare che venga ancora visualizzato Stato operazione certificato: operazione in sospeso.



Nei registri della console telefonica, vedere il telefono tenta di eseguire una query nella cache locale (127.0.0.1) prima di inoltrare la query all'indirizzo del server DNS configurato.

```
0475 INF Mar 12 15:07:53.686410 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0476 INF Mar 12 15:07:53.686450 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
0477 INF Mar 12 15:07:53.694909 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
0478 INF Mar 12 15:07:53.695263 dnsmasq[12864]: reply PUB11.brianw2.lab is NXDOMAIN-IPv4
0479 INF Mar 12 15:07:53.695833 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0480 INF Mar 12 15:07:53.695865 dnsmasq[12864]: cached PUB11.brianw2.lab is NXDOMAIN-IPv4
0481 WRN Mar 12 15:07:53.697091 (12905:13036) JAVA-configmgr MQThread|NetUtil.traceIPv4DNSErrors:? - DNS

++ However, we see that the phone is not able to resolve the FQDN of the CUCM Publisher. This is because

0482 ERR Mar 12 15:07:53.697267 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Failed to

++ Afterwards, we see the CAPF operation fail. This is expected because we do not have a DNS mapping for

0632 NOT Mar 12 15:07:55.760715 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty:? - Ce
0633 NOT Mar 12 15:07:55.761649 (322:17812) SECUREAPP-RCAPF_START_MODE: Start CAPF - mode:[1]([NULL_STR]
0634 NOT Mar 12 15:07:55.761749 (322:17812) SECUREAPP-CAPF_CLNT_INIT:CAPF clnt initialized
0635 NOT Mar 12 15:07:55.761808 (322:17812) SECUREAPP-CAPFClnt: SetDelayTimer - set with value <0>
0636 ERR Mar 12 15:07:55.761903 (322:17812) SECUREAPP-Sec create BIO - invalid parameter.
0637 ERR Mar 12 15:07:55.761984 (322:17812) SECUREAPP-SEC_CAPF_BIO_F: CAPF create bio failed
0638 ERR Mar 12 15:07:55.762040 (322:17812) SECUREAPP-SEC_CAPF_OP_F: CAPF operation failed, ret -7
0639 CRT Mar 12 15:07:55.863826 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty$1:? -

++ What we would expect to see is something similar to the following where DNS replies with the IP addre

4288 INF Mar 12 16:34:06.162666 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
4289 INF Mar 12 16:34:06.162826 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
4290 INF Mar 12 16:34:06.164908 dnsmasq[12864]: reply PUB11.brianw2.lab is X.X.X.X
4291 NOT Mar 12 16:34:06.165024 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Resolve Tv
```

Vedere nei messaggi di stato del telefono seguenti, che il telefono non è in grado di risolvere PUB11.brianw2.lab. Vedere quindi il messaggio **LSC: Connessione non riuscita**.



Difetti da considerare:

Cisco ID bug CSCub62243 - L'installazione di LSC non riesce in modo intermittente e quindi blocca il server CAPF

Miglioramento difetto da considerare:

ID bug Cisco CSCuz18034 - Segnalazione della necessità per gli endpoint LSC installati e stato di scadenza

Informazioni correlate

Questi documenti forniscono ulteriori informazioni sull'uso degli LSC nel contesto dell'autenticazione dei client VPN AnyConnect e dell'autenticazione 802.1X.

- AnyConnect VPN Phone - Risoluzione dei problemi di telefoni IP, ASA e CUCM
- Servizi Identity-Based Networking: Guida alla distribuzione e configurazione della telefonia IP nelle reti abilitate IEEE 802.1X

Esiste anche un tipo avanzato di configurazione LSC, in cui i certificati LSC sono firmati direttamente da un'autorità di certificazione di terze parti, non dal certificato CAPF.

Per ulteriori informazioni, consultare: Esempio di generazione e importazione di schede LSC firmate da CA di terze parti CUCM

- Documentazione e supporto tecnico â€“ Cisco Systems

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).