Informazioni sulla protezione CUCM per impostazione predefinita e sul funzionamento e la risoluzione dei problemi ITL

Sommario

Introduzione

In questo documento viene descritta la funzionalità Security By Default (SBD) di Cisco Unified Communications Manager (CUCM) versione 8.0 e successive.

Premesse

CUCM versione 8.0 e successive introduce la funzionalità SBD, costituita dai file ITL (Identity Trust List) e dal servizio TVS (Trust Verification Service).

Ogni cluster CUCM utilizza ora automaticamente la protezione basata su ITL. Esiste un compromesso tra sicurezza e facilità d'uso/amministrazione di cui gli amministratori devono essere a conoscenza prima di apportare determinate modifiche a un cluster CUCM versione 8.0.

Questo documento funge da supplemento ai documenti ufficiali Protezione predefinita e fornisce informazioni operative e suggerimenti per la risoluzione dei problemi per aiutare gli amministratori e semplificare il processo di risoluzione dei problemi.

È una buona idea familiarizzare con questi concetti fondamentali di SBD: Asymmetric Key Cryptography Wikipedia article and Public Key Infrastructure Wikipedia article .

Panoramica SBD

Questa sezione fornisce una rapida panoramica di ciò che SBD fornisce. Per i dettagli tecnici completi di ciascuna funzione, vedere la sezione Dettagli SBD e informazioni sulla risoluzione dei problemi.

SBD fornisce queste tre funzioni per i telefoni IP supportati:

- Autenticazione predefinita dei file scaricati TFTP (configurazione, impostazioni internazionali, lista a anello) che utilizzano una chiave per la firma
- Crittografia facoltativa dei file di configurazione TFTP che utilizzano una chiave di firma
- Verifica certificato per connessioni HTTPS avviate telefonicamente che utilizzano un archivio certificati attendibili remoto in CUCM (TVS)

Questo documento offre una panoramica di ciascuna di queste funzioni.

Autenticazione download TFTP

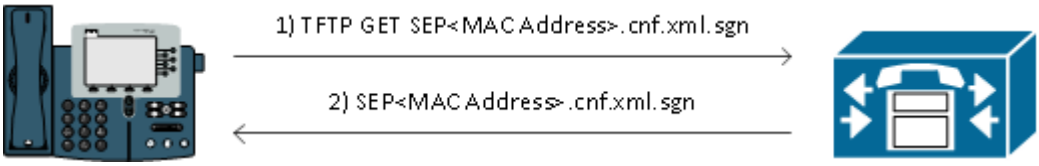
Quando è presente un elenco di certificati attendibili (CTL) o un file ITL, il telefono IP richiede un file di configurazione TFTP firmato dal server TFTP CUCM.

Questo file consente al telefono di verificare che il file di configurazione provenga da una fonte attendibile. Con i file CTL/ITL presenti sui telefoni, i file di configurazione devono essere firmati da un server TFTP attendibile.

Il file è in testo normale nella rete durante la trasmissione, ma viene fornito con una firma di verifica speciale.

Il telefono richiede **SEP<*Indirizzo MAC*>.cnf.xml.sgn** per ricevere il file di configurazione con la firma speciale.

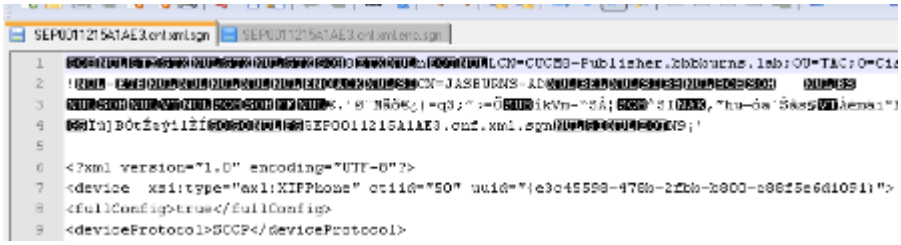
Questo file di configurazione è firmato dalla chiave privata TFTP che corrisponde a CallManager.pem nella pagina di gestione dei certificati di amministrazione del sistema operativo.



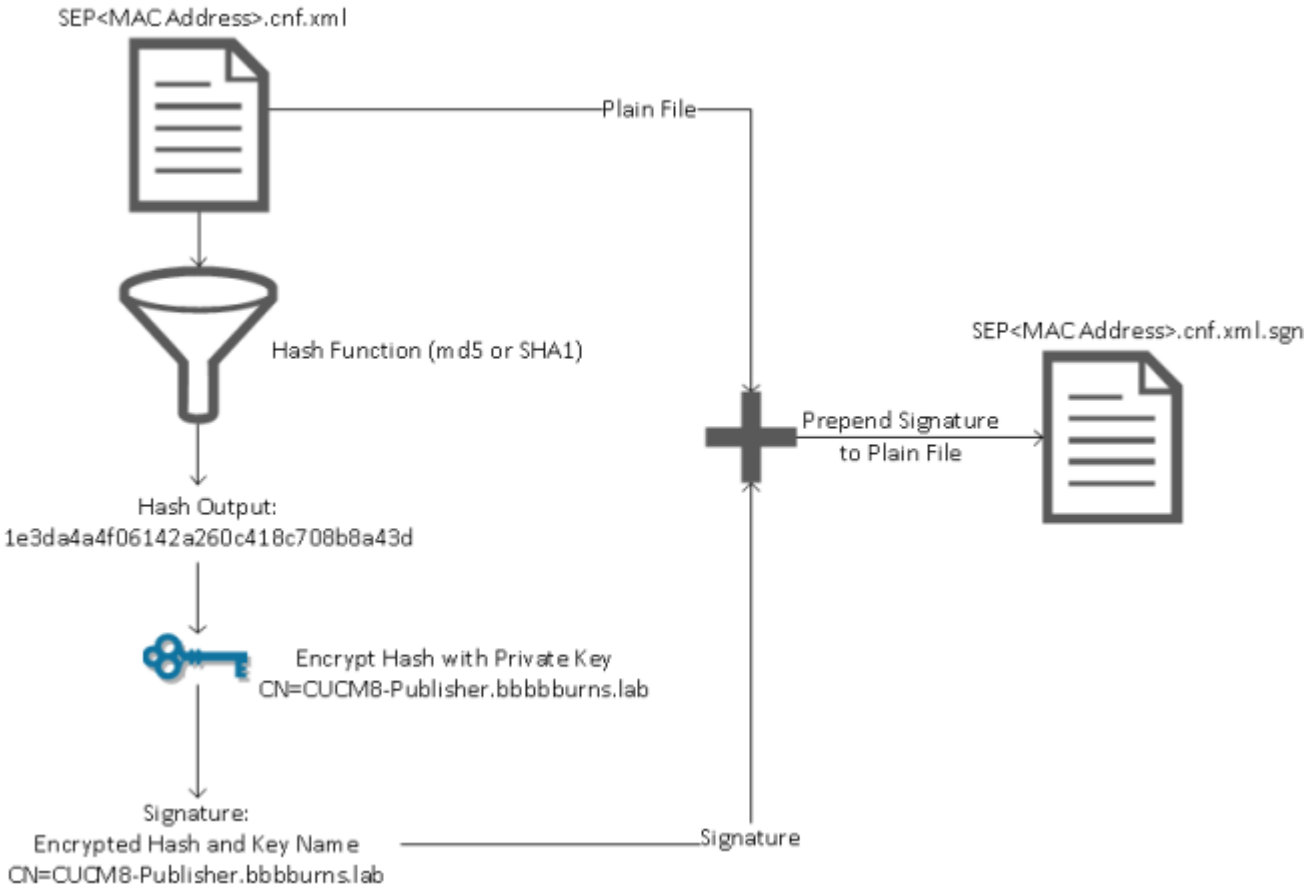
Il file firmato ha una firma nella parte superiore per l'autenticazione del file, ma è altrimenti in formato XML di testo normale.

L'immagine seguente mostra che il firmatario del file di configurazione è **CN=CUCM8-Publisher.bbbburns.lab**, a sua volta firmato da **CN=JASBURNS-AD**.

Questo significa che il telefono deve verificare la firma di **CUCM8-Publisher.bbburns.lab** rispetto al file ITL prima che questo file di configurazione venga accettato.

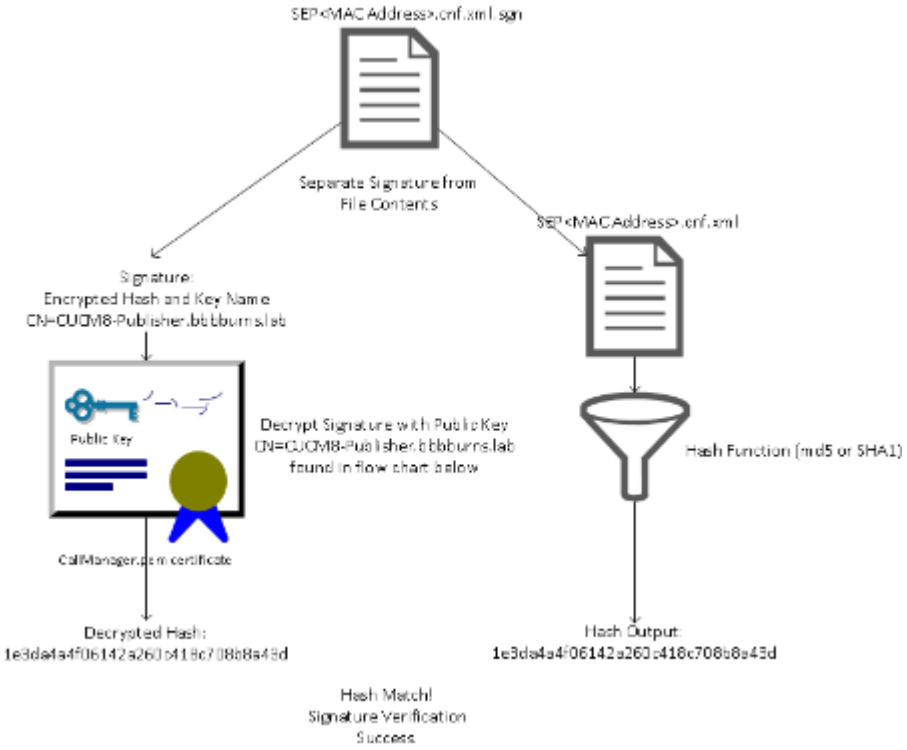


Di seguito è riportato un diagramma che mostra come la chiave privata viene utilizzata insieme a una funzione hash MD (Message Digest Algorithm)5 o SHA (Secure Hash Algorithm)1 per creare il file firmato.



La verifica della firma inverte questo processo tramite l'utilizzo della chiave pubblica corrispondente per decrittografare l'hash. Se gli hash corrispondono, viene visualizzato quanto segue:

- Il file non è stato modificato durante la trasmissione.
- Il file proviene dall'entità elencata nella firma, poiché tutti gli elementi decrittografati correttamente con la chiave pubblica devono essere stati crittografati con la chiave privata.



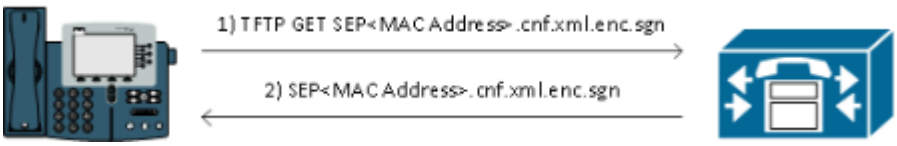
Crittografia dei file di configurazione TFTP

Se la crittografia di configurazione TFTP opzionale è abilitata nel profilo di sicurezza telefono associato, il telefono richiede un file di configurazione crittografato.

Questo file è firmato con la chiave privata TFTP e crittografato con una chiave simmetrica scambiata tra il telefono e CUCM (per ulteriori informazioni, consultare la guida alla sicurezza di Cisco Unified Communications Manager, versione 8.5(1)).

Il suo contenuto non può essere letto con uno sniffer di rete a meno che l'osservatore non abbia le chiavi necessarie.

Il telefono richiede **SEP<*Indirizzo MAC*>.cnf.xml.enc.sgn** per ottenere il file crittografato firmato.



Anche il file di configurazione crittografato presenta la firma all'inizio, ma dopo non sono presenti dati in testo normale, ma solo dati crittografati (caratteri binari alterati in questo editor di testo).

Nell'immagine è illustrato che il firmatario è lo stesso dell'esempio precedente, pertanto il firmatario deve essere presente nel file ITL prima che il telefono accetti il file.

Inoltre, le chiavi di decrittografia devono essere corrette prima che il telefono possa leggere il contenuto del file.

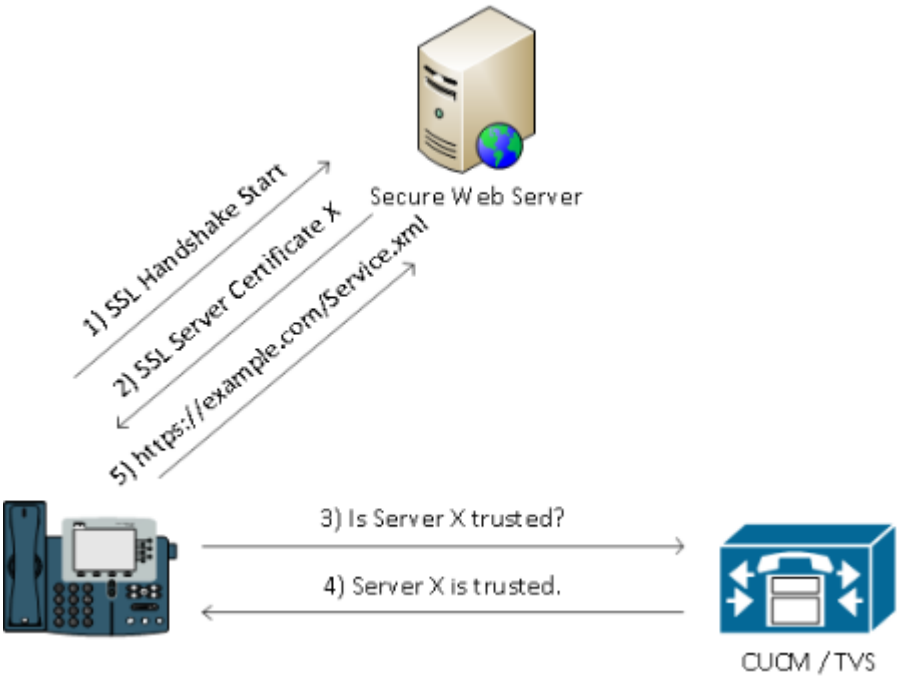
Servizio di verifica dell'attendibilità (verifica remota di certificati e firme)

I telefoni IP contengono una quantità limitata di memoria e possono anche contenere un elevato numero di telefoni da gestire in una rete.

CUCM funge da archivio di attendibilità remoto tramite il TVS in modo che non sia necessario posizionare un archivio di attendibilità completo su ogni telefono IP.

Ogni volta che il telefono non è in grado di verificare una firma o un certificato tramite i file CTL o ITL, richiede la verifica al server TVS.

Questo archivio di attendibilità centrale è più facile da gestire rispetto a quello presente su tutti i telefoni IP.



Dettagli SBD e informazioni sulla risoluzione dei problemi

In questa sezione viene descritto in dettaglio il processo SBD.

File e certificati ITL presenti in CUCM

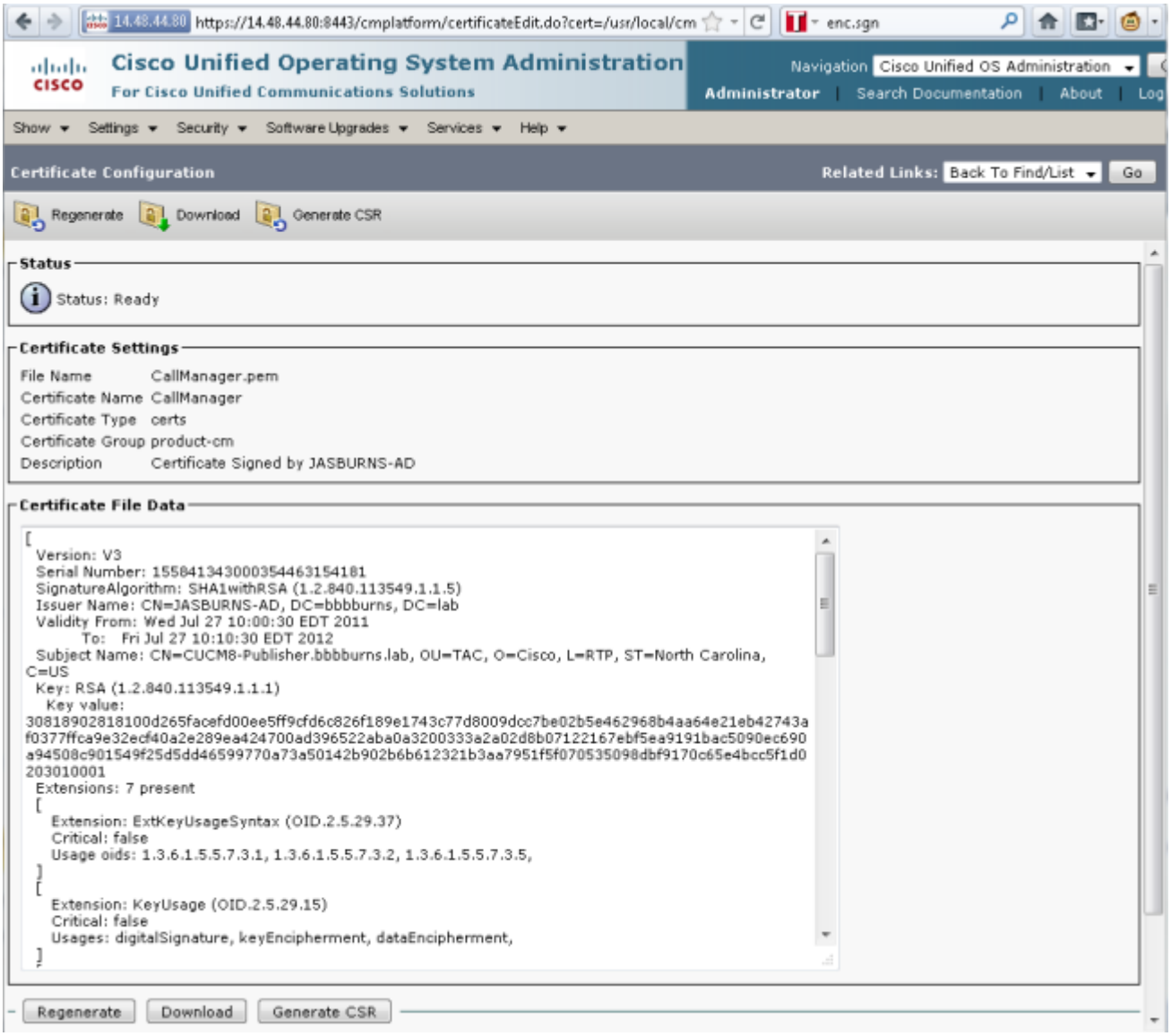
Innanzitutto, è necessario che sul server CUCM stesso siano presenti alcuni file. La parte più importante è il certificato TFTP e la chiave privata TFTP.

Il certificato TFTP si trova in **Amministrazione del sistema operativo > Protezione > Gestione certificati > CallManager.pem**.

Il server CUCM utilizza le chiavi pubbliche e private del certificato CallManager.pem per il servizio TFTP e per il servizio Cisco Call Manager (CCM).

Nell'immagine è illustrato che il certificato CallManager.pem viene rilasciato a **CUCM8-publisher.bbbburns.lab** e firmato da **JASBURNS-AD**. Tutti i file di configurazione TFTP sono firmati dalla chiave privata riportata di seguito.

Tutti i telefoni possono utilizzare la chiave pubblica TFTP nel certificato CallManager.pem per decrittografare qualsiasi file crittografato con la chiave privata TFTP, nonché per verificare qualsiasi file firmato con la chiave privata TFTP.



Oltre alla chiave privata del certificato CallManager.pem, il server CUCM memorizza anche un file ITL che viene presentato ai telefoni.

Il comando **show itl** restituisce il contenuto completo del file ITL tramite l'accesso Secure Shell (SSH) alla CLI del sistema operativo del server CUCM.

Questa sezione suddivide il file ITL pezzo per pezzo, perché ha una serie di componenti importanti che il telefono usa.

La prima parte riguarda le informazioni sulla firma. Anche il file ITL è un file firmato. Questo output mostra che è firmato dalla chiave privata TFTP associata al precedente certificato CallManager.pem.

```
admin:
```

`show itl`

```
Length of ITL file: 5438
The ITL File was last modified on Wed Jul 27 10:16:24 EDT 2011

        Parse ITL File
        ----------------

Version:        1.2
HeaderLength:   296 (BYTES)

BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
3       SIGNERID        2       110
4       SIGNERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
5       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
6       CANAME          15      CN=JASBURNS-AD
*Signature omitted for brevity*
```

Le sezioni successive contengono ognuna il proprio scopo all'interno di uno speciale parametro **Function**. La prima funzione è il token di sicurezza dell'amministratore di sistema. Firma della chiave pubblica TFTP.

```
        ITL Record #:1
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1972
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      15      CN=JASBURNS-AD
6       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
7       PUBLICKEY       140
8       SIGNATURE       256
9       CERTIFICATE     1442    0E 1E 28 0E 5B 5D CC 7A 20 29 61 F5
                                8A DE 30 40 51 5B C4 89 (SHA1 Hash HEX)
This etoken was used to sign the ITL file.
```

La funzione successiva è CCM+TFTP. Questa è di nuovo la chiave pubblica TFTP che serve per autenticare e decrittografare i file di configurazione TFTP scaricati.

```
        ITL Record #:2
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1972
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
```

```
4       FUNCTION        2       CCM+TFTP
5       ISSUERNAME      15      CN=JASBURNS-AD
6       SERIALNUMBER    10      21:00:2D:17:00:00:00:00:00:05
7       PUBLICKEY       140
8       SIGNATURE       256
9       CERTIFICATE     1442    0E 1E 28 0E 5B 5D CC 7A 20 29 61 F5
                                8A DE 30 40 51 5B C4 89 (SHA1 Hash HEX)
```

La funzione successiva è TVS. È disponibile una voce per la chiave pubblica di ciascun server TVS a cui si connette il telefono.

In questo modo il telefono può stabilire una sessione SSL (Secure Sockets Layer) con il server TVS.

```
        ITL Record #:3
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       743
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       TVS
5       ISSUERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       2E:3E:1A:7B:DA:A6:4D:84
7       PUBLICKEY       270
8       SIGNATURE       256
11      CERTHASH        20      C7 E1 D9 7A CC B0 2B C2 A8 B2 90 FB
                                AA FE 66 5B EC 41 42 5D
12      HASH ALGORITHM  1       SHA-1
```

La funzione finale inclusa nel file ITL è la funzione CAPF (Certificate Authority Proxy Function).

Questo certificato consente ai telefoni di stabilire una connessione sicura al servizio CAPF sul server CUCM in modo che il telefono possa installare o aggiornare un LSC (Locally Significant Certificate).

```
        ITL Record #:4
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       455
2       DNSNAME         2
3       SUBJECTNAME     61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       CAPF
5       ISSUERNAME      61      CN=CAPF-9c4cba7d;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       0A:DC:6E:77:42:91:4A:53
7       PUBLICKEY       140
8       SIGNATURE       128
11      CERTHASH        20      C7 3D EA 77 94 5E 06 14 D2 90 B1
                                A1 43 7B 69 84 1D 2D 85 2E
12      HASH ALGORITHM  1       SHA-1
```

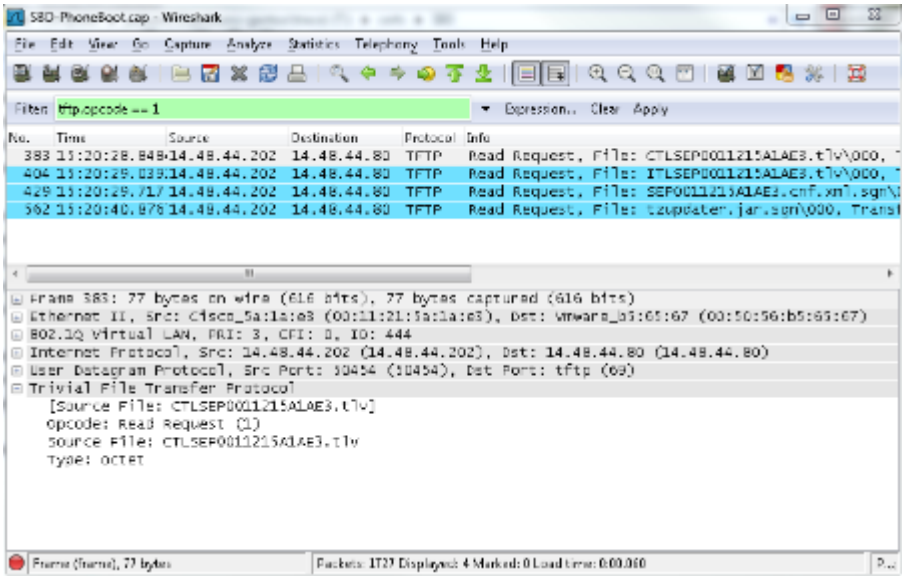
```
The ITL file was verified successfully.
```

Nella sezione successiva vengono illustrate le operazioni eseguite all'avvio di un telefono.

Download tramite telefono - ITL e file di configurazione

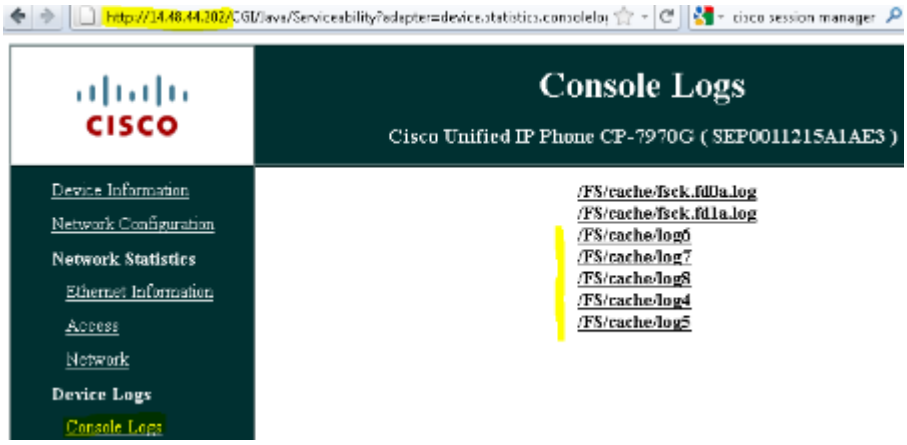
Una volta avviato il telefono e ottenuto un indirizzo IP e l'indirizzo di un server TFTP, richiede prima il CTL e i file ITL.

L'acquisizione del pacchetto mostra una richiesta telefonica per il file ITL. Se si filtra in base a **tftp.opcode == 1,** vengono visualizzate tte le richieste di lettura TFTP dal telefono:



Poiché il telefono ha ricevuto correttamente i file CTL e ITL dal TFTP, il telefono chiede un file di configurazione firmato.

I registri della console telefonica che mostrano questo comportamento sono disponibili dall'interfaccia Web del telefono:



Innanzitutto il telefono richiede un file CTL, che riesce:

```
837: NOT 09:13:17.561856 SECD: tlRequestFile: Request CTLSEP0011215A1AE3.tlv
846: NOT 09:13:17.670439 TFTP: [27]:Requesting CTLSEP0011215A1AE3.tlv from
```

```
14 . 48 . 44 . 80
847: NOT 09:13:17.685264 TFTP: [27]:Finished --> rcvd 4762 bytes
```

Poi il telefono chiede anche un file ITL:

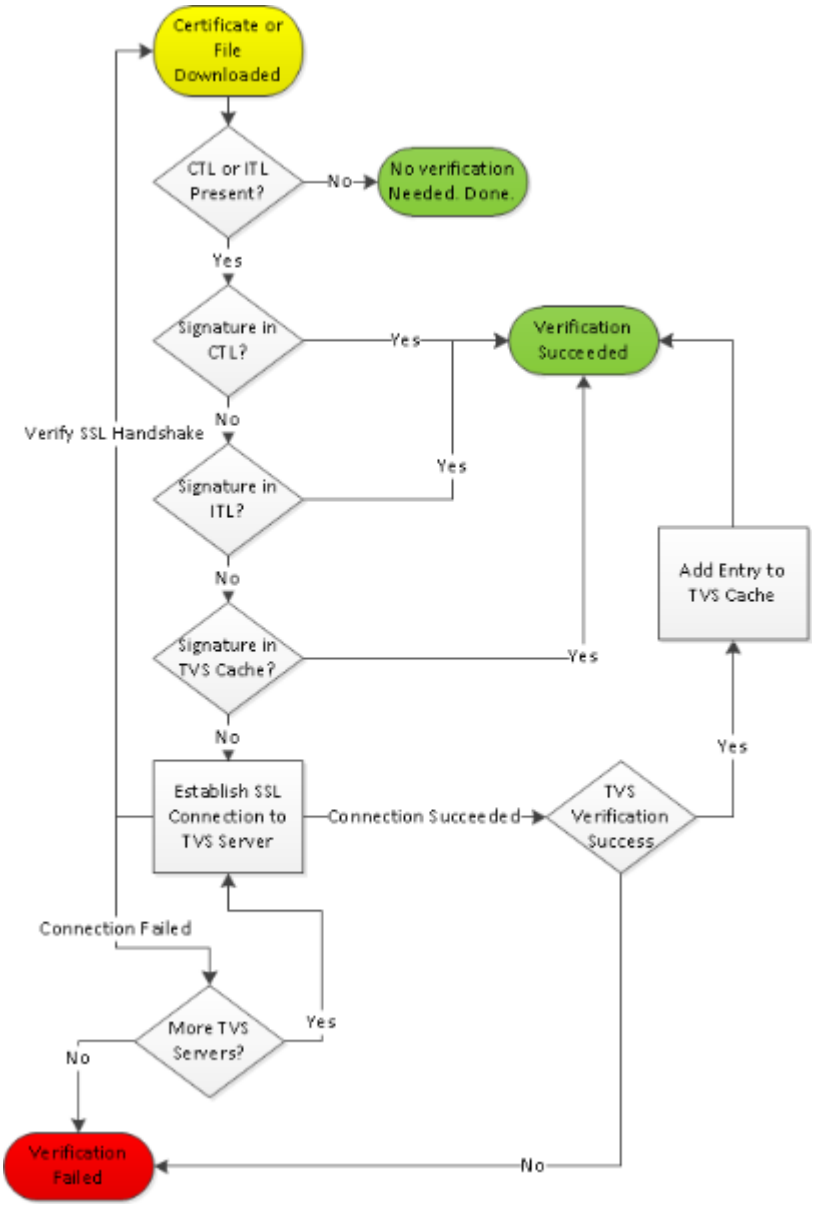
```
868: NOT 09:13:17.860613 TFTP: [28]:Requesting ITLSEP0011215A1AE3.tlv from
14 . 48 . 44 . 80
869: NOT 09:13:17.875059 TFTP: [28]:Finished --> rcvd 5438 bytes
```

Il telefono verifica ITL e file di configurazione

Dopo aver scaricato il file ITL, è necessario verificarlo. A questo punto, un telefono può trovarsi in diversi stati, quindi il presente documento li copre tutti.

- Nel telefono non è presente alcun file CTL o ITL oppure ITL è vuoto a causa del parametro **Prepara cluster per rollback a precedente alla versione 8.0**. In questo stato, il telefono considera ciecamente attendibile il successivo file CTL o ITL scaricato e usa questa firma.
- Il telefono ha già un CTL ma non un ITL. In questo stato, il telefono considera attendibile un ITL solo se può essere verificato dalla funzione CCM+TFTP nel file CTL.
- Il telefono ha già un CTL e un file ITL. In questo stato, il telefono verifica che i file scaricati di recente corrispondano alla firma nel server CTL, ITL o TVS.

Di seguito è riportato un diagramma di flusso che descrive come il telefono verifica i file firmati e i certificati HTTPS:



In questo caso, il telefono è in grado di verificare la firma nei file ITL e CTL. Il telefono ha già sia un CTL che un ITL, quindi ha semplicemente controllato rispetto a loro e ha trovato la firma corretta.

```
877: NOT 09:13:17.925249 SECD: validate_file_envelope:
File sign verify SUCCESS; header length <296>
```

Dal momento che il telefono ha scaricato i file CTL e ITL, da questo punto in esso richiede SOLO file di configurazione firmati.

Ciò dimostra che la logica del telefono consiste nel determinare che il server TFTP è sicuro, in base alla presenza di CTL e ITL, e quindi nel richiedere un file firmato:

```
917: NOT 09:13:18.433411 tftpClient: tftp request rcv'd from /usr/tmp/tftp,
srcFile = SEP0011215A1AE3.cnf.xml, dstFile = /usr/ram/SEP0011215A1AE3.cnf.xml
max size = 550001
918: NOT 09:13:18.457949 tftpClient: auth server - tftpList[0] = ::ffff:
14 . 48 . 44 . 80
```

```
919: NOT 09:13:18.458937 tftpClient: look up server - 0
920: NOT 09:13:18.462479 SECD: lookupCTL: TFTP SRVR secure
921: NOT 09:13:18.466658 tftpClient: secVal = 0x9 922: NOT 09:13:18.467762
tftpClient: ::ffff:14 . 48 . 44 . 80 is a secure server
923: NOT 09:13:18.468614 tftpClient: retval = SRVR_SECURE
924: NOT 09:13:18.469485 tftpClient: Secure file requested
925: NOT 09:13:18.471217 tftpClient: authenticated file approved - add .sgn
-- SEP0011215A1AE3.cnf.xml.sgn
926: NOT 09:13:18.540562 TFTP: [10]:Requesting SEP0011215A1AE3.cnf.xml.sgn
from 14 . 48 . 44 . 80 with size limit of 550001
927: NOT 09:13:18.559326 TFTP: [10]:Finished --> rcvd 7652 bytes
```

Una volta scaricato il file di configurazione firmato, il telefono deve autenticarlo con la Funzione per CCM+TFTP all'interno dell'ITL:

```
937: NOT 09:13:18.656906 SECD: verifyFile: verify SUCCESS
</usr/ram/SEP0011215A1AE3.cnf.xml>
```

TV contatti telefonici per certificato sconosciuto

Il file ITL fornisce una funzione TVS che contiene il certificato del servizio TVS in esecuzione sulla porta TCP 2445 del server CUCM.

TVS viene eseguito su tutti i server in cui è attivato il servizio CallManager. Il servizio TFTP CUCM utilizza il gruppo CallManager configurato per creare un elenco di server TVS che il telefono deve contattare nel file di configurazione del telefono.

Alcuni laboratori utilizzano un solo server CUCM. In un cluster CUCM a più nodi, possono essere presenti fino a tre voci TVS per telefono, una per ogni CUCM nel gruppo CUCM del telefono.

Nell'esempio viene mostrato cosa succede quando si preme il pulsante **Directories** sul telefono IP. L'URL delle directory è configurato per HTTPS, quindi al telefono viene presentato il certificato Web Tomcat dal server delle directory.

Questo certificato Web Tomcat (tomcat.pem in Amministrazione del sistema operativo) non è caricato nel telefono, quindi il telefono deve contattare TVS per autenticare il certificato.

Per una descrizione dell'interazione, fare riferimento al diagramma precedente relativo alla panoramica dei televisori. Di seguito è riportata la prospettiva del registro della console telefonica:

L'URL della directory è il seguente:

```
1184: NOT 15:20:55.219275 JVM: Startup Module Loader|cip.dir.TandunDirectories:
? - Directory url https://14 . 48 . 44 . 80:8443/ccmcip/xmldirectory.jsp
```

Questa è una sessione HTTP protetta SSL/TLS (Transport Layer Security) che richiede la verifica.

```
1205: NOT 15:20:59.404971 SECD: clpSetupSsl: Trying to connect to IPV4, IP:
14 . 48 . 44 . 80, Port : 8443
1206: NOT 15:20:59.406896 SECD: clpSetupSsl: TCP connect() waiting,
<14 . 48 . 44 . 80> c:8 s:9 port: 8443
1207: NOT 15:20:59.408136 SECD: clpSetupSsl: TCP connected,
<14 . 48 . 44 . 80> c:8 s:9
1208: NOT 15:20:59.409393 SECD: clpSetupSsl: start SSL/TLS handshake,
<14 . 48 . 44 . 80> c:8 s:9
1209: NOT 15:20:59.423386 SECD: srvr_cert_vfy: Server Certificate
Validation needs to be done
```

Il telefono verifica innanzitutto che il certificato presentato dal server SSL/TLS sia presente nell'elenco di certificati attendibili (CTL). Quindi il telefono controlla le Funzioni nel file ITL per vedere se trova una corrispondenza.

In questo messaggio di errore viene visualizzato il messaggio "HTTPS cert not in CTL", ovvero "that certification cannot be found in the CTL or the ITL" (Impossibile trovare la certificazione nel CTL o nell'ITL).

```
1213: NOT 15:20:59.429176 SECD: findByCertAndRoleInTL: Searching TL from CTL file
1214: NOT 15:20:59.430315 SECD: findByCertAndRoleInTL: Searching TL from ITL file
1215: ERR 15:20:59.431314 SECD: EROR:https_cert_vfy: HTTPS cert not in CTL,
<14 . 48 . 44 . 80>
```

Dopo aver controllato il contenuto diretto dei file CTL e ITL per il certificato, il prossimo elemento che il telefono controlla è la cache TVS.

Questa operazione viene eseguita per ridurre il traffico di rete se il telefono ha recentemente richiesto lo stesso certificato al server TVS.

Se il certificato HTTPS non viene trovato nella cache del telefono, è possibile effettuare una connessione TCP al server TVS stesso.

```
1220: NOT 15:20:59.444517 SECD: processTvsClntReq: TVS Certificate
Authentication request
1221: NOT 15:20:59.445507 SECD: lookupAuthCertTvsCacheEntry: No matching
entry found at cache
1222: NOT 15:20:59.446518 SECD: processTvsClntReq: No server sock exists,
must be created
1223: NOT 15:20:59.451378 SECD: secReq_initClient: clnt sock fd 11 bound
to </tmp/secClnt_secd>
1224: NOT 15:20:59.457643 SECD: getTvsServerInfo: Phone in IPv4 only mode
1225: NOT 15:20:59.458706 SECD: getTvsServerInfo: Retreiving IPv4 address
1230: NOT 15:20:59.472628 SECD: connectToTvsServer: Successfully started
a TLS connection establishment to the TVS server: IP:14 . 48 . 44 . 80, port:2445
(default); Waiting for it to get connected.
```

Tenere presente che la connessione alla TV stessa è SSL/TLS (HTTP protetto o HTTPS), quindi è anche un certificato che deve essere autenticato in base al CTL o all'ITL.

Se tutto funziona correttamente, il certificato del server TVS viene trovato nella funzione TVS del file ITL. Vedere il record ITL n. 3 nell'esempio precedente del file ITL.

```
1244: NOT 15:20:59.529938 SECD: srvr_cert_vfy: Server Certificate Validation
needs to be done
1245: NOT 15:20:59.533412 SECD: findByIssuerAndSerialAndRoleInTL:
Searching TL from CTL file
1246: NOT 15:20:59.534936 SECD: findByIssuerAndSerialAndRoleInTL:
Searching TL from ITL file
1247: NOT 15:20:59.537359 SECD: verifyCertWithHashFromTL: cert hash and
hash in TL MATCH
1248: NOT 15:20:59.538726 SECD: tvs_cert_vfy: TVS cert verified with hash
from TL, <14 . 48 . 44 . 80>
```

Operazione riuscita. Il telefono ora ha una connessione protetta al server TVS. Il passaggio successivo consiste nel chiedere al server TVS "Ciao, considero attendibile il certificato del server Directory?"

In questo esempio viene illustrata la risposta a tale domanda, ovvero una risposta pari a 0 che indica un esito positivo (nessun errore).

```
1264: NOT 15:20:59.789738 SECD: sendTvsClientReqToSrvr: Authenticate
Certificate : request sent to TVS server - waiting for response
1273: NOT 15:20:59.825648 SECD: processTvsSrvrResponse: Authentication Response
received, status : 0
```

Poiché è stata ricevuta una risposta positiva da parte di TV, i risultati di tale certificato vengono salvati nella cache.

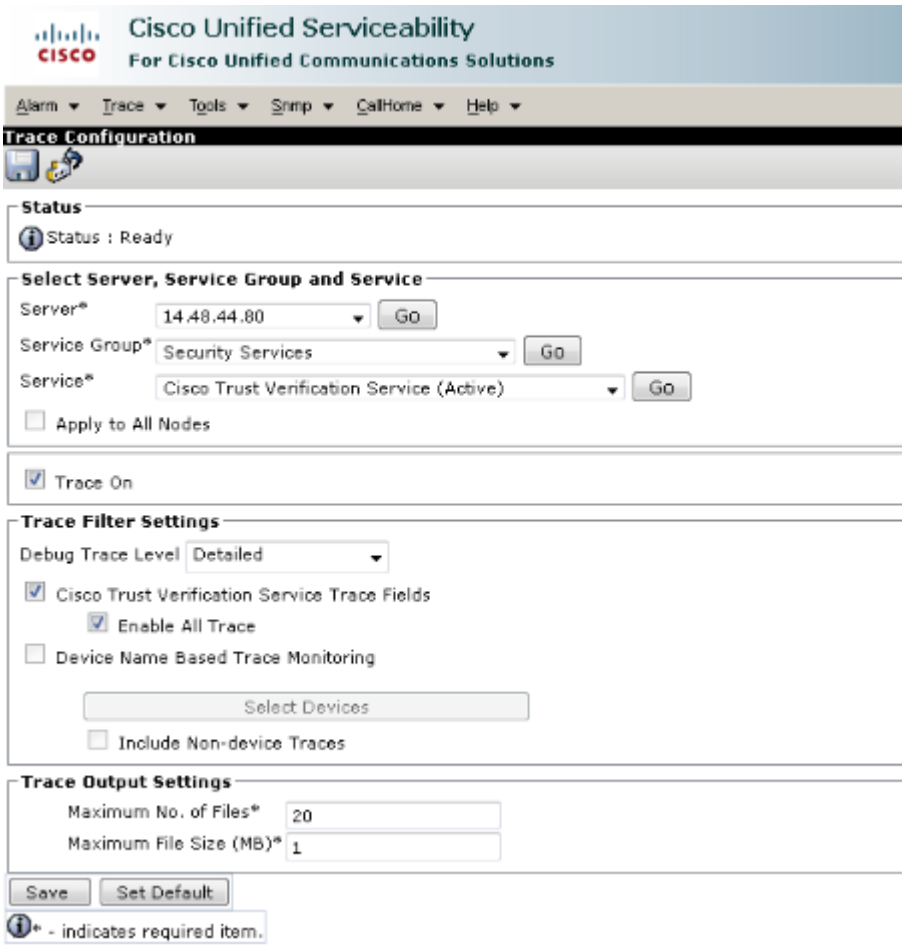
Ciò significa che, se si preme di nuovo il pulsante **Directory** entro i successivi 86.400 secondi, non sarà necessario contattare il server TVS per verificare il certificato. È sufficiente accedere alla cache locale.

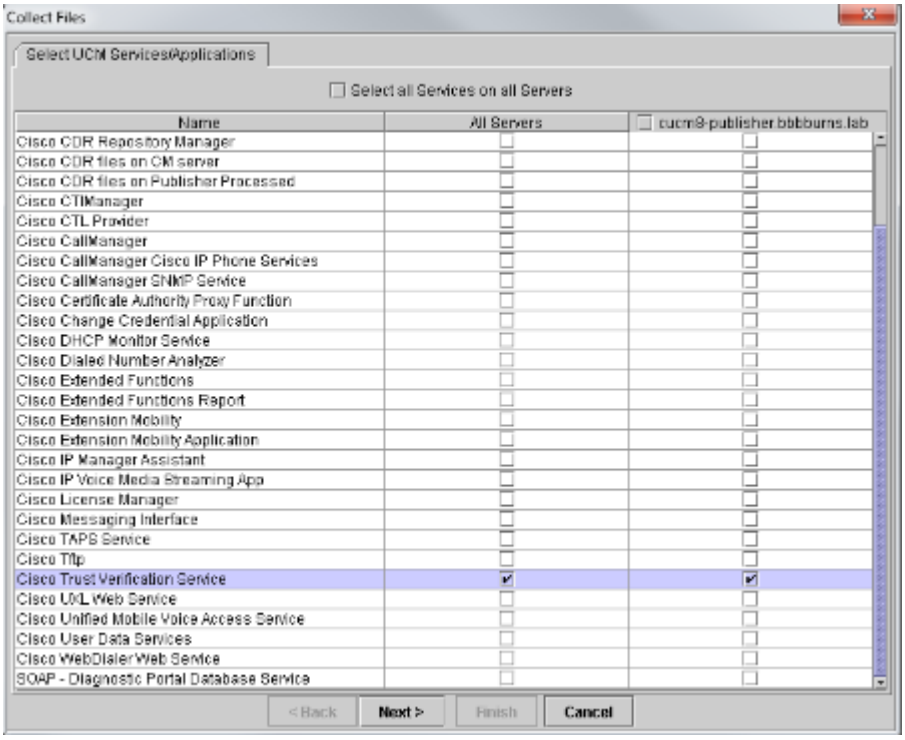
```
1279: NOT 15:20:59.837086 SECD: saveCertToTvsCache: Saving certificate
in TVS cache with default time-to-live value: 86400 seconds
1287: ERR 15:20:59.859993 SECD: Authenticated the HTTPS conn via TVS
```

Infine, verificare che la connessione al server delle directory sia stata eseguita correttamente.

```
1302: ERR 15:21:01.959700 JVM: Startup Module Loader|cip.http.ae:?
- listener.httpSucceed:  https://14 . 48 . 44 . 80:8443/ccmcip/
xmldirectoryinput.jsp?name=SEP0011215A1AE3
```

Di seguito è riportato un esempio di ciò che accade sul server CUCM in cui viene eseguito TVS. È possibile raccogliere i registri TVS con Cisco Unified Real-Time Monitoring Tool (RTMT).





I registri TVS di CUCM mostrano che l'handshake SSL viene eseguito con il telefono, il telefono chiede a TVS informazioni sul certificato Tomcat, quindi TVS risponde per indicare che il certificato corrisponde nell'archivio certificati TVS.

```
15:21:01.954 |   debug 14 . 48 . 44 . 202: tvsSSLHandShake Session ciphers - AES256-SHA
```

```
15:21:01.954 |   debug TLS HS Done for ph_conn .
15:21:02.010 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_REQ
15:21:02.011 |   debug tvsGetIssuerNameFromX509 - issuerName : CN=CUCM8-
Publisher.bbbburns.lab;OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US and Length: 75

15:21:02.011 |   debug CertificateDBCache::getCertificateInformation -
Certificate compare return =0
15:21:02.011 |   debug CertificateDBCache::getCertificateInformation -
Certificate found and equal
15:21:02.011 |   debug     MsgType               : TVS_MSG_CERT_VERIFICATION_RES
```

L'archivio certificati TVS è un elenco di tutti i certificati contenuti nella pagina Web **Amministrazione del sistema operativo > Gestione certificati**.

Verifica manualmente che l'ITL del telefono corrisponda all'ITL del CUCM

Un errore comune riscontrato durante la risoluzione dei problemi riguarda la tendenza a eliminare il file ITL con la speranza che risolva un problema di verifica dei file.

Talvolta l'eliminazione del file ITL è obbligatoria, ma il file ITL deve essere eliminato solo quando TUTTE queste condizioni sono soddisfatte.

- La firma del file ITL sul telefono non corrisponde alla firma del file ITL sul server TFTP CM.
- La firma del TVS nel file ITL non corrisponde al certificato presentato dal TVS.
- Il telefono visualizza "Verifica non riuscita" quando tenta di scaricare il file ITL o i file di configurazione.
- Nessun backup della vecchia chiave privata TFTP.

Di seguito viene riportata la procedura per verificare le prime due condizioni.

In primo luogo, è possibile confrontare il checksum del file ITL presente su CUCM con il file ITL checksum del telefono.

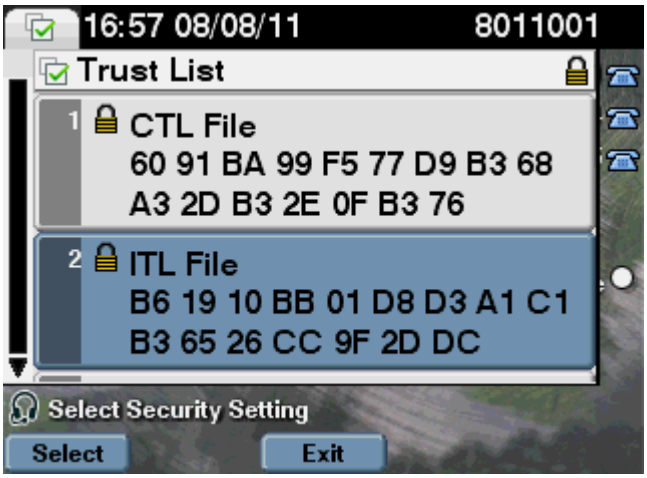
Al momento, non è possibile esaminare la somma MD5 del file ITL su CUCM direttamente da CUCM finché non si esegue una versione con la correzione per questo bug Cisco ID CSCto60209.

Nel frattempo, eseguire questa operazione con la GUI o i programmi CLI preferiti:

```
jasburns@jasburns-gentoo /data/trace/jasburns/certs/SBD $ tftp 14 . 48 . 44 . 80
tftp> get ITLSEP0011215A1AE3.tlv
Received 5438 bytes in 0.0 seconds
tftp> quit
jasburns@jasburns-gentoo /data/trace/jasburns/certs/SBD $ md5sum
ITLSEP0011215A1AE3.tlv
b61910bb01d8d3a1c1b36526cc9f2ddc  ITLSEP0011215A1AE3.tlv
```

Ciò indica che la somma MD5 del file ITL in CUCM è **b61910bb01d8d3a1c1b36526cc9f2ddc**.

Ora è possibile guardare il telefono stesso per determinare l'hash del file ITL caricato lì: **Settings > Security Configuration > Trust List**.

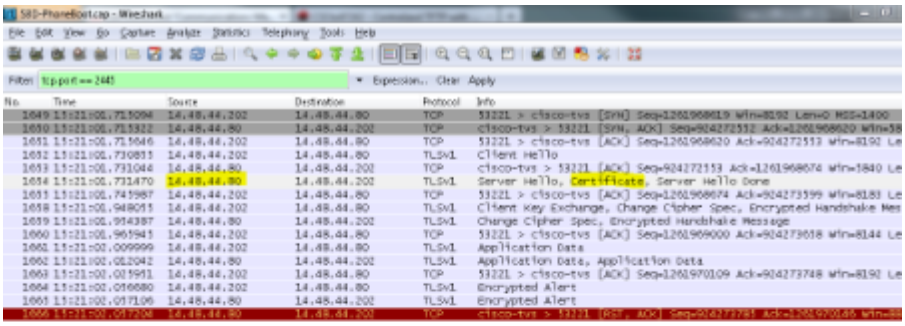


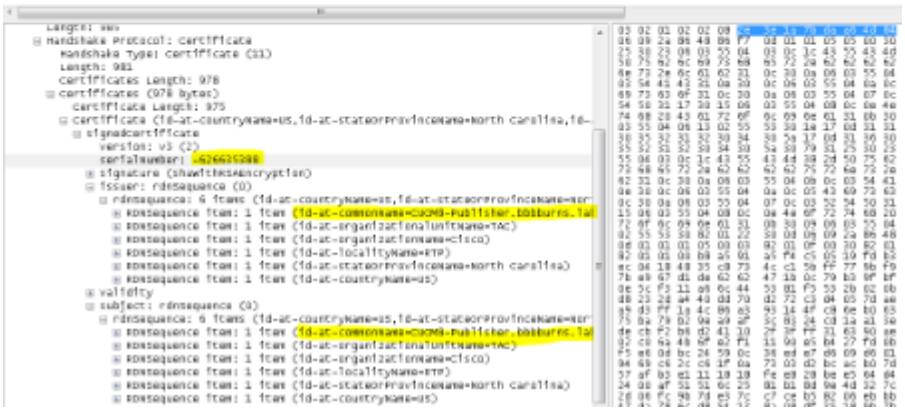
Ciò dimostra che le somme di MD5 sono uguali. Ciò significa che il file ITL sul telefono corrisponde al file sul CUCM, quindi non deve essere eliminato.

Se non corrisponde, è necessario passare all'operazione successiva, ovvero determinare se il certificato TVS nell'ITL corrisponde o meno al certificato presentato da TVS. Questa operazione è un po' più coinvolta.

Innanzitutto, è opportuno esaminare l'acquisizione dei pacchetti del telefono che si connette al server TVS sulla porta TCP 2445.

Fare clic con il pulsante destro del mouse su un pacchetto in questo flusso in Wireshark, fare clic su **Decode As** (Decodifica come), quindi selezionare **SSL**. Individuare il certificato server simile al seguente:





Esaminare il certificato TVS contenuto nel file ITL precedente. Viene quindi visualizzata una voce con il numero di serie **2E3E1A7BDAA64D84**.

<#root>

admin:

```
show itl
```

```
        ITL Record #:3
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       743
2       DNSNAME         2
3       SUBJECTNAME     76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
4       FUNCTION        2       TVS
5       ISSUERNAME      76      CN=CUCM8-Publisher.bbbburns.lab;
                                OU=TAC;O=Cisco;L=RTP;ST=North Carolina;C=US
6       SERIALNUMBER    8       2E:3E:1A:7B:DA:A6:4D:84
```

Se il file **TVS.pem** all'interno del file ITL ha esito positivo, corrisponde al certificato TVS presentato sulla rete. Non è necessario eliminare l'ITL e TVS presenta il certificato corretto.

Se l'autenticazione dei file non riesce, controllare il resto del diagramma di flusso precedente.

Restrizioni e interazioni

Rigenera certificati / Ricostruisci cluster / Scadenza certificato

Il certificato più importante è ora il certificato CallManager.pem. Questa chiave privata di certificato viene utilizzata per firmare tutti i file di configurazione TFTP, incluso il file ITL.

Se il file CallManager.pem viene rigenerato, viene generato un nuovo certificato CCM+TFTP con una nuova chiave privata. Inoltre, il file ITL è ora firmato da questa nuova chiave CCM+TFTP.

Dopo aver rigenerato CallManager.pem e riavviato il servizio TVS e TFTP, questo accade quando si avvia un telefono.

1. Il telefono tenta di scaricare il nuovo file ITL firmato dal nuovo CCM+TFTP dal server TFTP. A questo punto il telefono ha solo il vecchio file ITL e le nuove chiavi non sono nel file ITL presente sul telefono.
2. Poiché il telefono non riesce a trovare la nuova firma CCM+TFTP nel vecchio ITL, tenta di contattare il servizio TVS.

   Nota: questa parte è estremamente importante. Il certificato TVS del vecchio file ITL deve ancora corrispondere. Se i file CallManager.pem e TVS.pem vengono rigenerati contemporaneamente, i telefoni non saranno in grado di scaricare nuovi file senza eliminare manualmente l'ITL dal telefono.

   ---

3. Quando il telefono contatta il servizio TV, il server CUCM che esegue il servizio ha il nuovo certificato CallManager.pem nell'archivio certificati del sistema operativo.
4. Il server TVS restituisce un risultato positivo e il telefono carica il nuovo file ITL in memoria.
5. Il telefono ora tenta di scaricare un file di configurazione, che è stato firmato dalla nuova chiave CallManager.pem.
6. Poiché il nuovo ITL è stato caricato, il file di configurazione appena firmato viene verificato dall'ITL in memoria.

Considerazioni principali:

- Non rigenerare mai contemporaneamente i certificati CallManager.pem e TVS.pem.
- Se viene rigenerato TVS.pem o CallManager.pem, è necessario riavviare TVS e TFTP e ripristinare i telefoni per ottenere i nuovi file ITL.
- Nelle versioni più recenti di CUCM questo telefono viene reimpostato automaticamente e l'utente viene avvisato al momento della rigenerazione del certificato.
- Se esistono più server TVS (più server nel gruppo CallManager), i server aggiuntivi possono autenticare il nuovo certificato CallManager.pem.

Sposta i telefoni tra i cluster

Quando si spostano i telefoni da un cluster a un altro con ITL installati, è necessario tenere in considerazione la chiave privata ITL e TFTP.

I nuovi file di configurazione presentati al telefono DEVONO corrispondere a una firma in CTL, ITL o nel servizio TVS corrente del telefono.

Questo documento spiega come assicurarsi che il file ITL e i file di configurazione del nuovo cluster possano essere considerati attendibili dal file ITL corrente sul telefono.
https://supportforums.cisco.com/docs/DOC-15799.

Backup E Ripristino

Il certificato CallManager.pem e la chiave privata vengono sottoposti a backup tramite il sistema di ripristino di emergenza (DRS). Se un server TFTP viene ricostruito, DEVE essere ripristinato dal backup in modo che la chiave privata possa essere ripristinata.

Senza la chiave privata CallManager.pem sul server, i telefoni con ITL correnti che utilizzano la vecchia chiave non considerano attendibili i file di configurazione firmati.

Se un cluster viene ricostruito e non ripristinato dal backup, è esattamente come il documento "Spostamento di telefoni tra cluster". Questo perché un cluster con una nuova chiave è un cluster diverso per quanto riguarda i telefoni.

Esiste un grave difetto associato alle operazioni di backup e ripristino. Se un cluster è esposto all'ID bug Cisco CSCtn50405, i backup DRS non contengono il certificato CallManager.pem.

In questo modo, tutti i server ripristinati da questo backup genereranno file ITL danneggiati fino a quando non verrà generato un nuovo file CallManager.pem.

Se non ci sono altri server TFTP funzionanti che non sono passati attraverso l'operazione di backup e ripristino, probabilmente significa che tutti i file ITL devono essere eliminati dai telefoni.

Per verificare se il file CallManager.pem deve essere rigenerato, immettere il comando **show itl** seguito da:

```
run sql select c.subjectname, c.serialnumber, c.ipv4address, t.name from
certificate as c, certificatetrustrolemap as r, typetrustrole as t where  c.pkid =
r.fkcertificate and t.enum = r.tktrustrole
```

Nell'output ITL, gli errori principali da cercare sono:

```
This etoken was not used to sign the ITL file.
```

e

```
Verification of the ITL file failed.
Error parsing the ITL file!!
```

La query SQL (Structured Query Language) precedente cerca i certificati con il ruolo "Autenticazione e autorizzazione".

Il certificato CallManager.pem della query di database precedente con il ruolo Autenticazione e autorizzazione deve essere presente anche nella pagina Web Gestione certificati di amministrazione del sistema operativo.

Se viene rilevato il difetto precedente, non esiste corrispondenza tra i certificati CallManager.pem nella query e nella pagina Web del sistema operativo.

Modificare i nomi host o i nomi di dominio

Se si modifica il nome dell'host o il nome di dominio di un server CUCM, tutti i certificati vengono rigenerati contemporaneamente su tale server. La sezione di rigenerazione del certificato spiega che la rigenerazione di TVS.pem e CallManager.pem è una "cosa sbagliata".

Ci sono alcuni scenari dove un cambio di nome host non riesce, e alcuni dove funziona senza problemi. In questa sezione vengono descritti tutti gli argomenti e viene fornito un collegamento a ciò che già si sa su TVS e ITL in questo documento.

Cluster a nodo singolo con solo ITL (prestare attenzione, l'operazione si interrompe senza preparazione)

- Se si utilizza un server Business Edition o una distribuzione basata solo su server di pubblicazione, i file CallManager.pem e TVS.pem vengono rigenerati contemporaneamente quando si modificano i nomi host.
- Se il nome host viene modificato in un cluster a nodo singolo senza prima utilizzare il parametro Rollback Enterprise, i telefoni non saranno in grado di verificare il nuovo file ITL o i file di configurazione rispetto al file ITL corrente.
- I telefoni non sono in grado di connettersi a TV perché anche il certificato TV non è più considerato attendibile.
- Sui telefoni viene visualizzato un errore relativo a "Verifica dell'elenco di attendibilità non riuscita", non vengono applicate nuove modifiche alla configurazione e gli URL dei servizi protetti hanno esito negativo.
- L'unica soluzione se non si adotta la precauzione della fase 2 è eliminare manualmente l'ITL da ogni telefono.

Cluster a nodo singolo con CTL e ITL (può essere interrotto temporaneamente, ma facilmente risolto)

- Dopo aver eseguito la ridenominazione dei server, eseguire nuovamente il client CTL. Il nuovo certificato CallManager.pem viene inserito nel file CTL scaricato dal telefono.
- I nuovi file di configurazione, che includono i nuovi file ITL, possono essere considerati attendibili in base alla funzione CCM+TFTP nel file CTL.

- Questo funziona perché il file CTL aggiornato è attendibile in base a una chiave privata USB eToken che rimane la stessa.

Cluster a più nodi con solo ITL (generalmente funziona, ma può essere interrotto in modo permanente se eseguito in modo rapido)

- Poiché un cluster a più nodi dispone di più server TVS, ogni singolo server può rigenerare i propri certificati senza alcun problema. Quando il telefono riceve questa nuova firma, che non conosce, chiede a un altro dei server TVS di verificare il nuovo certificato del server.
- Ci sono due problemi principali che possono causare il fallimento di questo:
  - Se tutti i server vengono rinominati e riavviati contemporaneamente, nessuno dei server TVS sarà raggiungibile con certificati noti al riavvio dei server e dei telefoni.
  - Se un telefono dispone di un solo server nel gruppo CallManager, i server TV aggiuntivi non fanno alcuna differenza. Per risolvere il problema, vedere lo scenario "Cluster a nodo singolo" oppure aggiungere un altro server al gruppo CallManager telefonico.

Cluster a più nodi con CTL e ITL (impossibile interromperlo in modo permanente)

- Dopo aver eseguito le operazioni di ridenominazione, il servizio TVS autentica i nuovi certificati.
- Anche se tutti i server TVS non sono disponibili per qualche motivo, il client CTL può comunque essere utilizzato per aggiornare i telefoni con i nuovi certificati CallManager.pem CCM+TFTP.

TFTP centralizzato

All'avvio di un telefono con un ITL, richiede i seguenti file: CTLSEP<***Indirizzo MAC*>.*tlv***, ITLSEP<***Indirizzo MAC*>.tlv**, e **SEP<*Indirizzo MAC*>.cnf.xml.sgn**.

Se il telefono non riesce a trovare questi file, richiede **ITLFile.tlv** e **CTLFile.tlv**, che un server TFTP centralizzato fornisce a qualsiasi telefono che lo richieda.

Con il protocollo TFTP centralizzato, esiste un singolo cluster TFTP che punta a un certo numero di altri sub-cluster.

Questa operazione viene spesso eseguita perché i telefoni in più cluster CUCM condividono lo stesso ambito DHCP e quindi devono avere lo stesso server TFTP con opzione DHCP 150.

Tutti i telefoni IP puntano al cluster TFTP centrale, anche se si registrano ad altri cluster. Questo server TFTP centrale esegue una query sui server TFTP remoti ogni volta che riceve una richiesta di un file che non riesce a trovare.

A causa di questa operazione, il TFTP centralizzato funziona solo in un ambiente ITL omogeneo.

Tutti i server devono eseguire CUCM versione 8.x o successiva oppure tutti i server devono eseguire versioni precedenti alla versione 8.x.

Se il file ITLFile.tlv viene presentato dal server TFTP centralizzato, i telefoni non considerano attendibili i file del server TFTP remoto perché le firme non corrispondono.

Ciò accade in una miscela eterogenea. In una combinazione omogenea, il telefono richiede il file **ITLSEP<*MAC*>.tlv** estratto dal cluster remoto corretto.

In un ambiente eterogeneo con una combinazione di cluster precedenti alla versione 8.x e alla versione 8.x, è necessario abilitare il comando "Prepare Cluster for Rollback to Pre 8.0" sul cluster della versione 8.x come descritto nell'ID bug Cisco CSCto87262.

Configurare i "Parametri URL telefono protetto" con HTTP anziché con HTTPS. In questo modo le funzioni ITL vengono disattivate sul telefono.

Domande frequenti

È possibile disattivare la funzione SBD?

È possibile disattivare SBD solo se SBD e ITL funzionano attualmente.

SBD può essere temporaneamente disabilitato sui telefoni con il parametro Enterprise "Prepare Cluster for Rollback" precedente alla versione 8.0 e configurando i "Parametri URL telefono protetto" con HTTP anziché con HTTPS.

Quando si imposta il parametro Rollback, viene creato un file ITL firmato con voci di funzione vuote.

Il file ITL "vuoto" è ancora firmato, quindi il cluster deve essere in uno stato di sicurezza completamente funzionante prima di poter abilitare questo parametro.

Dopo aver abilitato questo parametro e aver scaricato e verificato il nuovo file ITL con voci vuote, i telefoni accettano qualsiasi file di configurazione, indipendentemente da chi lo ha firmato.

Non è consigliabile lasciare il cluster in questo stato, poiché non è disponibile alcuna delle tre funzioni precedentemente descritte (file di configurazione autenticati, file di configurazione crittografati e URL HTTPS).

È possibile eliminare facilmente il file ITL da tutti i telefoni dopo aver perso CallManager.pem?

Al momento non esiste un metodo per eliminare tutti gli ITL da un telefono fornito da Cisco in remoto. Ecco perché le procedure e le interazioni descritte nel presente documento sono così importanti da tenere in considerazione.

Su Cisco bug ID CSCto47052 è presente un miglioramento non risolto che richiede questa funzionalità, ma non è stato ancora implementato.

Nel frattempo, è stata aggiunta una nuova funzionalità tramite l'ID bug Cisco CSCts01319, che consente probabilmente al Cisco Technical Assistance Center (TAC) di ripristinare l'ITL precedentemente attendibile, se questo è ancora disponibile sul server.

Questa operazione funziona solo in alcuni casi in cui il cluster si trova in una versione con questa correzione del problema e in cui l'ITL precedente esiste in un backup archiviato in una posizione speciale sul server.

Visualizzate il difetto per verificare se la versione in uso contiene la correzione. Contattare Cisco TAC per eseguire la procedura di recupero potenziale descritta nel difetto.

Se la procedura precedente non è disponibile, i pulsanti del telefono devono essere premuti manualmente sul telefono per eliminare il file ITL. Questo è il compromesso tra sicurezza e facilità di amministrazione. Affinché il file ITL sia realmente sicuro, non deve essere rimosso facilmente in remoto.

Anche con la pressione di pulsanti tramite script con oggetti XML SOAP (Simple Object Access Protocol), l'ITL non può essere rimosso in remoto.

Ciò è dovuto al fatto che, a questo punto, l'accesso TVS (e quindi l'accesso URL di autenticazione sicura per convalidare gli oggetti Push XML SOAP in entrata) non funziona.

Se l'URL di autenticazione non è configurato come sicuro, è possibile eseguire lo script delle pressioni di tasti per eliminare un ITL, ma questo script non è disponibile da Cisco.

Altri metodi per eseguire script di pressioni di tasti remoti senza utilizzare l'URL di autenticazione possono essere disponibili da terze parti, ma queste applicazioni non sono fornite da Cisco.

Il metodo più usato per eliminare l'ITL è una trasmissione via e-mail a tutti gli utenti del telefono che indica loro la sequenza di tasti.

Se l'accesso alle impostazioni è impostato su **Limitato** o **Disabilitato**, il telefono deve essere ripristinato dal produttore perché gli utenti non hanno accesso al menu Impostazioni del telefono.

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).