

瞭解預設情況下的CUCM安全性以及ITL運行和故障排除

目錄

[簡介](#)

[背景資訊](#)

[SBD概述](#)

[ITFP下載驗證](#)

[ITFP組態檔加密](#)

[信任驗證服務 \(遠端證書和簽名驗證\)](#)

[SBD詳細資訊和故障排除資訊](#)

[CUCM上存在的ITL檔案和證書](#)

[電話下載ITL和配置檔案](#)

[電話驗證ITL和配置檔案](#)

[未知證書的電話聯絡人TVS](#)

[手動驗證電話ITL是否與CUCM ITL匹配](#)

[限制和互動](#)

[重新生成證書/重建群集/證書過期](#)

[在集群之間行動電話](#)

[備份和還原](#)

[更改主機名或域名](#)

[集中式ITFP](#)

[常見問題](#)

[我可以關閉SBD嗎？](#)

[CallManager.pem丟失後，能否從所有電話輕鬆刪除ITL檔案？](#)

簡介

本檔案介紹Cisco Unified Communications Manager(CUCM)8.0版及更新版本的預設安全(SBD)功能。

背景資訊

CUCM版本8.0及更高版本引入了SBD功能，包括身份信任清單(ITL)檔案和信任驗證服務(TVS)。

每個CUCM集群現在自動使用基於ITL的安全性。在安全性和易用性/管理便利性之間有一個折衷，管理員在對8.0版CUCM群集進行某些更改之前必須瞭解這一點。

本文檔是對官方[預設安全文檔](#)的補充，提供了操作資訊和故障排除提示，可幫助管理員簡化故障排除過程。

瞭解SBD的核心概念是一個好主意：非對稱金鑰加密維基百科文章[和公鑰基礎設施維基百科文章](#)。

SBD概述

本部分簡要概述了SBD提供的具體功能。有關每個功能的完整技術詳細資訊，請參見SBD詳細資訊和故障排除資訊部分。

SBD為支援的IP電話提供以下三種功能：

- 使用簽名金鑰的TFTP下載檔案（配置、區域設定、鈴聲）的預設身份驗證
- 可選加密使用簽名金鑰的TFTP配置檔案
- 使用CUCM(TVS)上的遠端證書信任儲存區的電話發起的HTTPS連線的證書驗證

本檔案將概述這些功能的每一種。

TFTP下載驗證

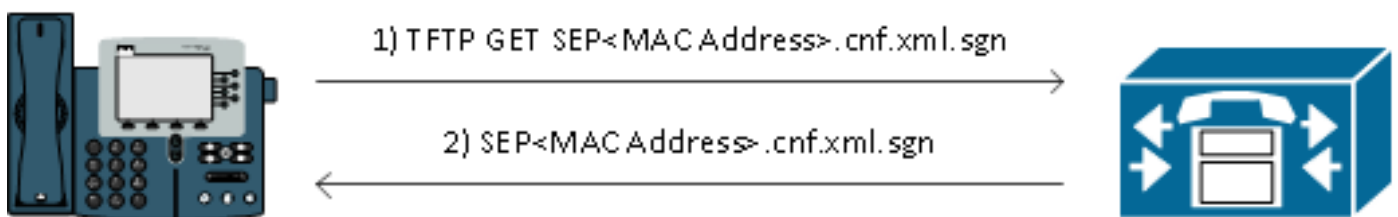
當存在證書信任清單(CTL)或ITL檔案時，IP電話會從CUCM TFTP伺服器請求已簽名的TFTP配置檔案。

此檔案允許電話驗證配置檔案是否來自受信任的來源。如果電話上存在CTL/ITL檔案，則配置檔案必須由受信任的TFTP伺服器簽名。

檔案在傳輸時是網路上的純文字檔案，但帶有特殊的驗證簽名。

電話請求SEP<MAC Address>.cnf.xml.sgn，以便接收具有特殊簽名的配置檔案。

此配置檔案由與作業系統(OS)管理證書管理(Operating System，OS)頁面上的CallManager.pem對應的TFTP私鑰簽名。



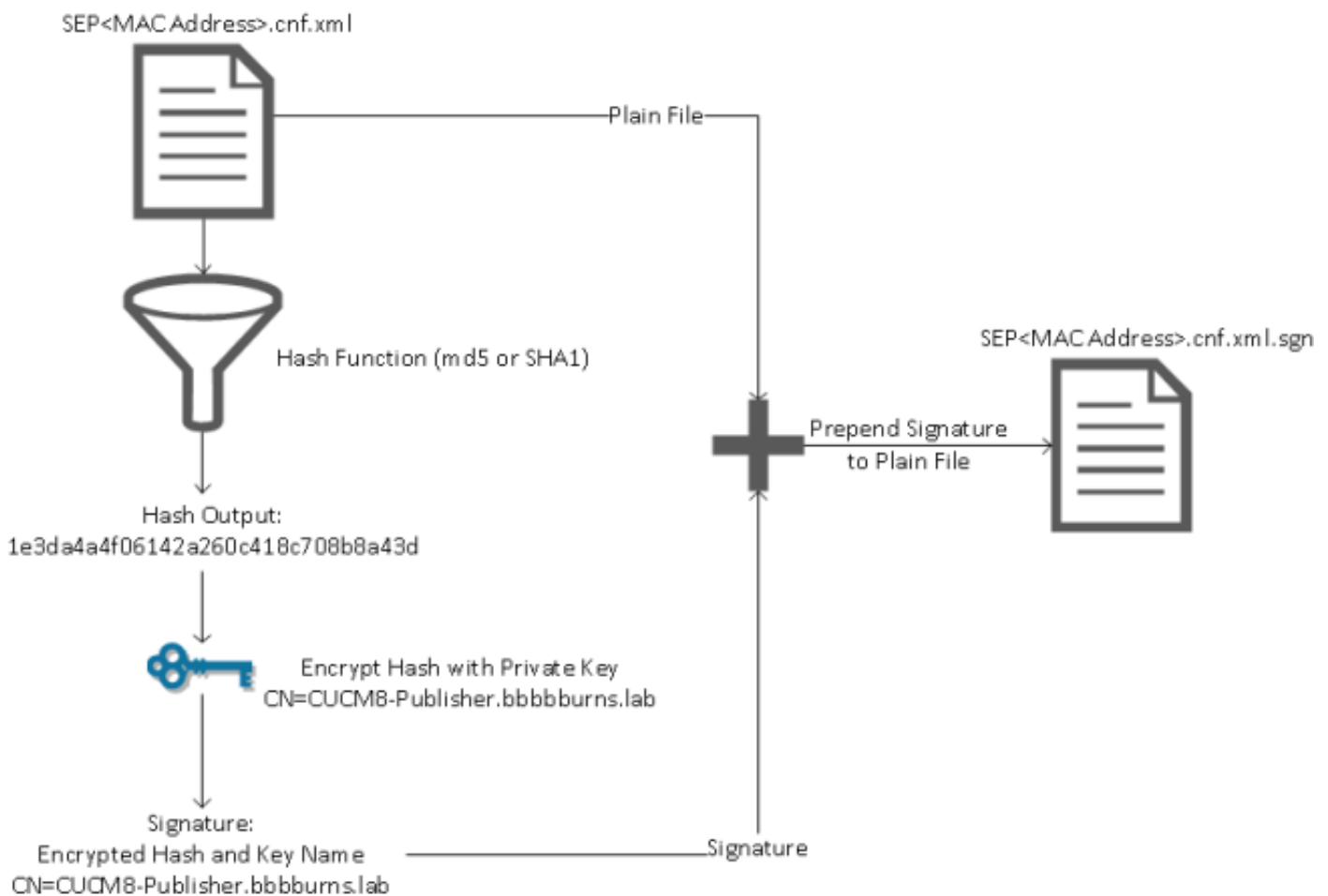
簽名檔案在頂部有一個簽名以驗證檔案，否則使用純文字檔案XML。

下圖顯示組態檔的簽署者是CN=CUCM8-Publisher.bbburns.lab，而後者是由CN=JASBURNS-AD簽署。

這意味著在接受此配置檔案之前，電話需要根據ITL檔案驗證CUCM8-Publisher.bbburns.lab的簽名。

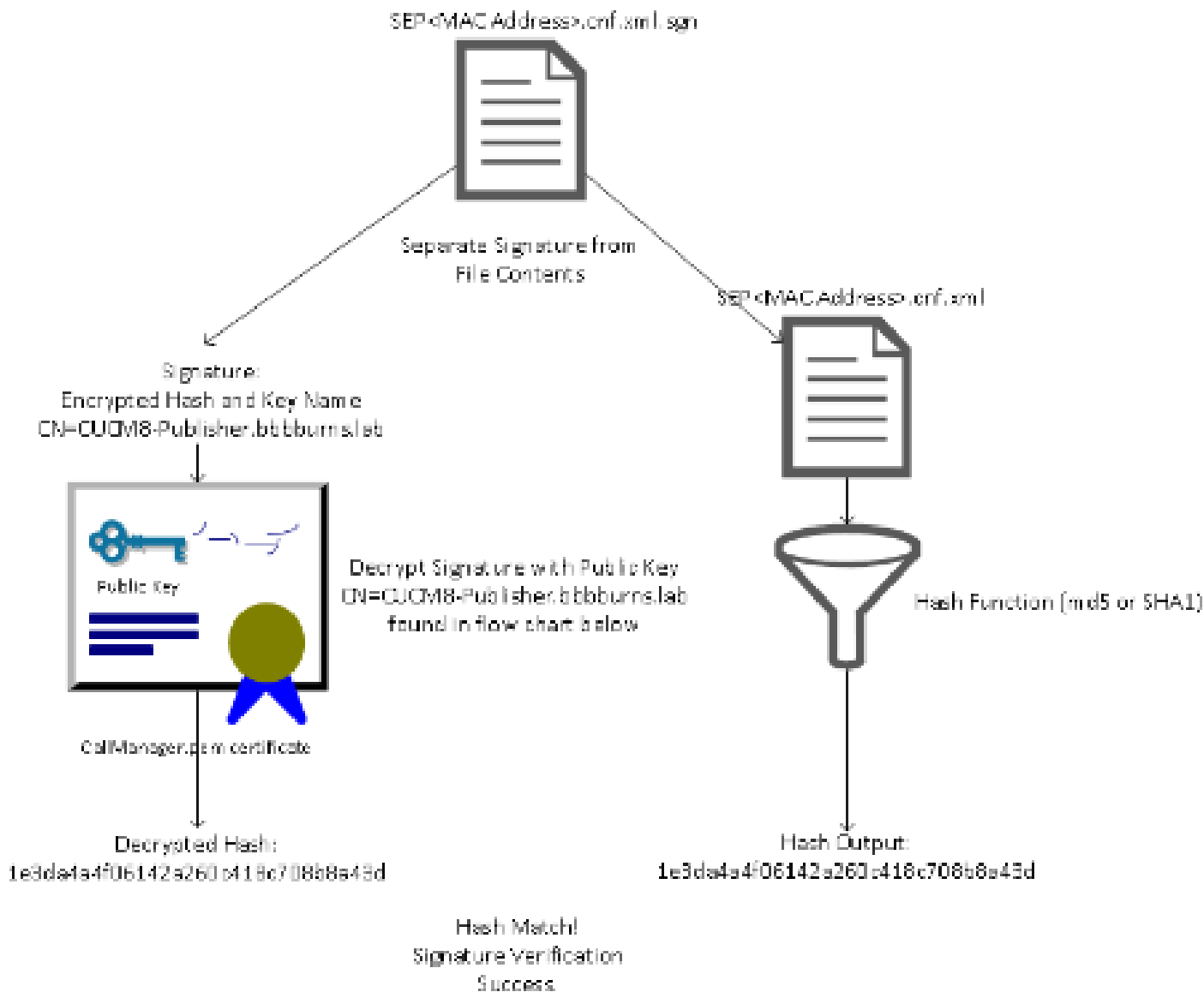
```
SEP0011215A1AE3.cnf.xml.sgn
SEP0011215A1AE3.cnf.xml.sgn
1  -----BEGIN-----
2  -----BEGIN-----
3  -----BEGIN-----
4  -----BEGIN-----
5
6  <?xml version="1.0" encoding="UTF-8"?>
7  <device xmlns:type="axl:XIPPhone" ct1id="50" uuid="{e3c45599-476b-2fbb-2800-e98f5e6d1091}">
8  <fullConfig>true</fullConfig>
9  </deviceProtocol></deviceProtocol>
```

以下圖表顯示私鑰如何與訊息摘要演算法(MD)5或安全雜湊演算法(SHA)1雜湊函式一起使用以建立簽署式檔案。



簽名驗證通過使用匹配的公鑰來解密雜湊來反轉此過程。如果雜湊匹配，則顯示：

- 傳送過程中未修改此檔案。
- 此檔案來自簽名中列出的參與方，因為使用公鑰成功解密的任何內容都必須使用私鑰進行加密。



TFTP組態檔加密

如果在關聯的電話安全配置檔案中啟用了可選的TFTP配置加密，則電話會請求加密的配置檔案。

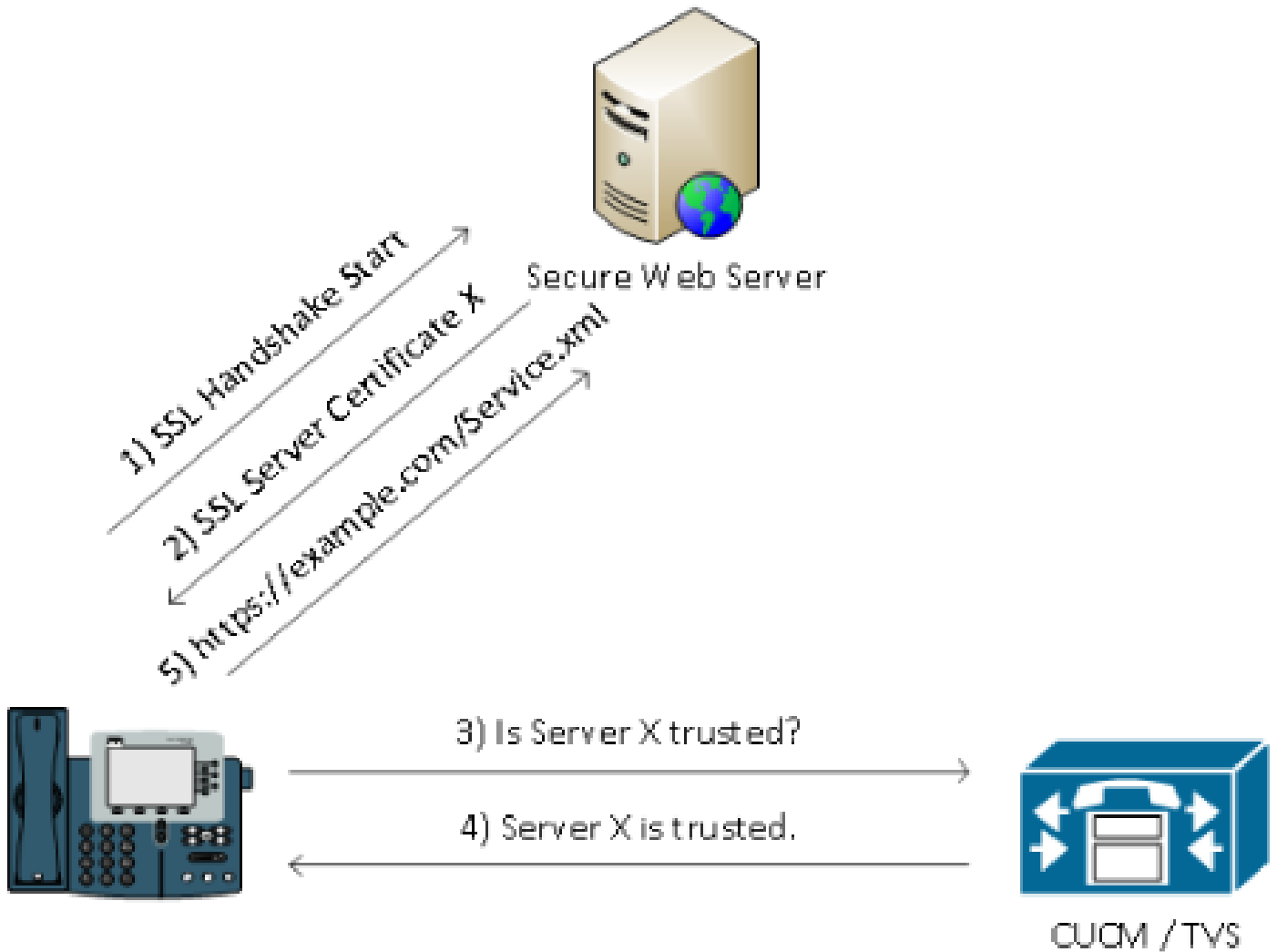
此檔案使用TFTP私鑰簽名，並使用電話和CUCM之間交換的對稱金鑰進行加密(有關詳細資訊，請參閱《[Cisco Unified Communications Manager安全指南8.5\(1\)版本](#)》)。

除非觀察者具有必要的金鑰，否則無法通過網路監聽器讀取其內容。

電話請求SEP<MAC Address>.cnf.xml.enc.sgn以獲取已簽名的加密檔案。



加密的配置檔案在開頭也有簽名，但之後沒有純文字檔案資料，只有加密資料(在此文本編輯器中被損壞的二進位制字元)。



SBD詳細資訊和故障排除資訊

本節詳細介紹SBD過程。

CUCM上存在的ITL檔案和證書

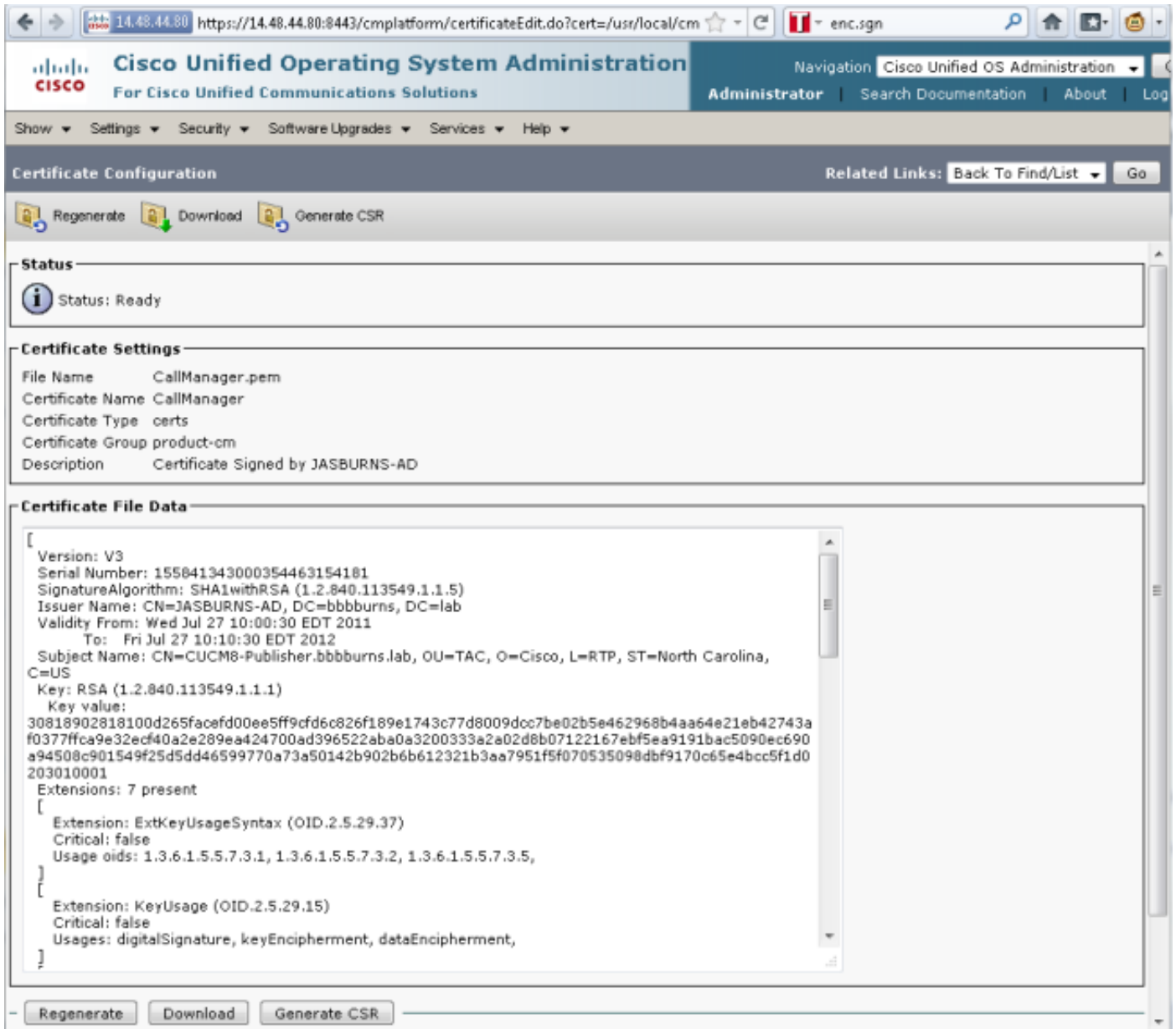
首先，CUCM伺服器本身必須存在許多檔案。最重要的部分是TFTP證書和TFTP私鑰。

TFTP證書位於OS Administration > Security > Certificate Management > CallManager.pem下。

CUCM伺服器將CallManager.pem證書私鑰和公鑰用於TFTP服務(以及Cisco Call Manager(CCM)服務)。

該圖顯示，CallManager.pem證書已頒發給CUCM8-publisher.bbburns.lab，並由JASBURNS-AD簽名。所有TFTP配置檔案均使用以下私鑰進行簽名。

所有電話都可以使用CallManager.pem證書中的TFTP公鑰解密使用TFTP私鑰加密的任何檔案，以及驗證使用TFTP私鑰簽名的任何檔案。



除了CallManager.pem證書私鑰之外，CUCM伺服器還儲存一個提供給電話的ITL檔案。

show itl命令通過對CUCM伺服器OS CLI的安全外殼(SSH)訪問顯示此ITL檔案的全部內容。

本節逐一分解國際交易日誌檔案，因為它具有電話使用的許多重要元件。

第一部分是簽名資訊。甚至國際交易日誌檔案也是已簽名的檔案。此輸出顯示，此連線埠由與先前CallManager.pem憑證關聯的TFTP私鑰簽署。

```
<#root>
```

```
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:17:00:00:00:00:05
6	CANAME	15	CN=JASBURNS-AD

Signature omitted for brevity

接下來的每個部分在特殊函式引數中包含其用途資訊。第一個功能是系統管理員安全令牌。這是 TFTP 公鑰的簽名。

```

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      ISSUENAME     15      CN=JASBURNS-AD
6      SERIALNUMBER  10      21:00:2D:17:00:00:00:00:05
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.

下一個功能是 CCM+TFTP。這再次是用於對下載的 TFTP 配置檔案進行身份驗證和解密的 TFTP 公鑰。

```

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      ISSUENAME     15      CN=JASBURNS-AD
6      SERIALNUMBER  10      21:00:2D:17:00:00:00:00:05
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)

```


下一個功能是TVS。電話所連線的每個TVS伺服器的公鑰都有一個條目。

這樣，電話就可以建立到TVS伺服器的安全套接字層(SSL)會話。

```
ITL Record #:3
-----
BYTEPOS TAG          LENGTH  VALUE
-----  ---  -----  -
```

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

國際交易日誌檔案中包含的最後一個功能是證書頒發機構代理功能(CAPF)。

此證書允許電話建立與CUCM伺服器上的CAPF服務的安全連線，以便電話可以安裝或更新本地重要證書(LSC)。

```
ITL Record #:4
-----
BYTEPOS TAG          LENGTH  VALUE
-----  ---  -----  -
```

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

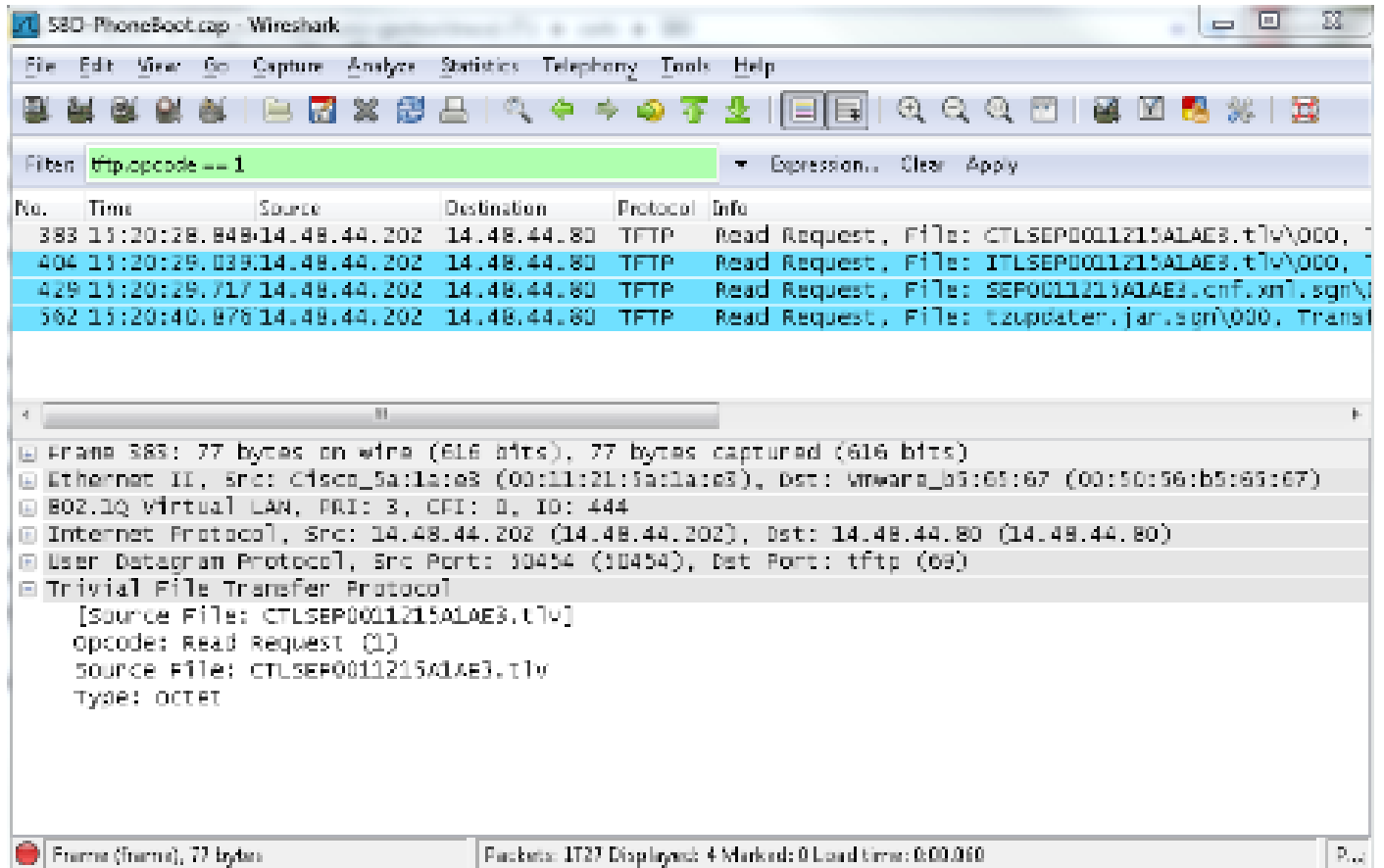
The ITL file was verified successfully.

下一節將介紹電話啟動時發生的具體情況。

電話下載ITL和配置檔案

電話啟動並獲得IP地址和TFTP伺服器地址後，首先請求CTL和ITL檔案。

此資料包捕獲顯示對ITL檔案的電話請求。如果您在tftp.opcode == 1上進行過濾，會看到電話上的每個TFTP讀取請求：



The image shows a Wireshark capture window titled "580-PhoneBoot.cap - Wireshark". The filter bar contains the expression "tftp.opcode == 1". The packet list pane shows four TFTP Read Request packets:

No.	Time	Source	Destination	Protocol	Info
383	13:20:28.848	14.48.44.202	14.48.44.80	TFTP	Read Request, File: CTLSEP0011215ALAE3.tlv\000,
404	13:20:29.039	14.48.44.202	14.48.44.80	TFTP	Read Request, File: ITLSEP0011215ALAE3.tlv\000,
429	13:20:29.717	14.48.44.202	14.48.44.80	TFTP	Read Request, File: SEP0011215ALAE3.cnf.xml.sgn\,
562	13:20:40.876	14.48.44.202	14.48.44.80	TFTP	Read Request, File: tzupdate.jar.sgn\000, Transf

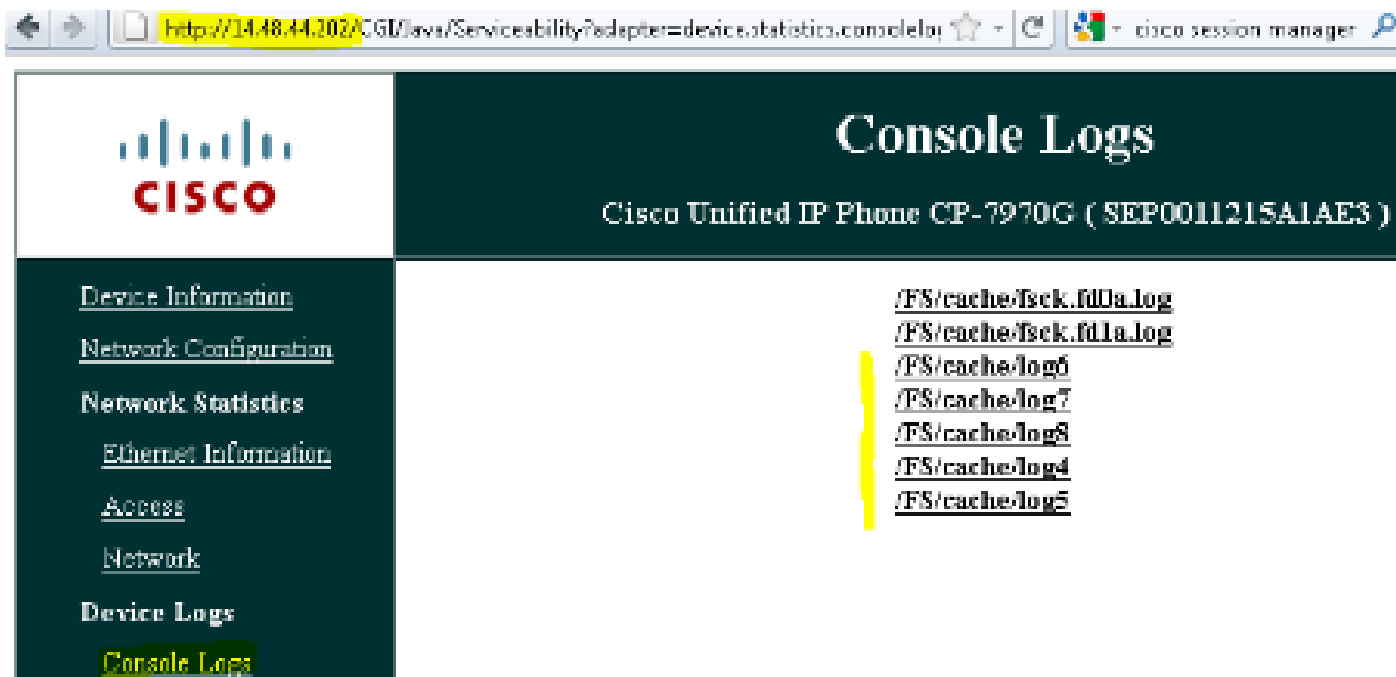
The packet details pane for the selected packet (No. 383) shows the following structure:

- Frame 383: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
- Ethernet II, Src: cisco_5a:1a:e8 (00:11:21:5a:1a:e8), Dst: vmware_b5:09:67 (00:50:56:b5:09:67)
- B02.IQ Virtual LAN, PRI: 3, CFI: 0, ID: 444
- Internet Protocol, Src: 14.48.44.202 (14.48.44.202), Dst: 14.48.44.80 (14.48.44.80)
- User Datagram Protocol, Src Port: 30454 (30454), Dst Port: tftp (69)
- Trivial File Transfer Protocol
 - [Source File: CTLSEP0011215ALAE3.tlv]
 - Opcode: Read Request (1)
 - Source File: CTLSEP0011215ALAE3.tlv
 - Type: OCTET

The status bar at the bottom indicates: Frame (frame), 77 bytes | Packets: 1727 Displayed: 4 Marked: 0 Load time: 0:00.060

由於電話成功地從TFTP接收到CTL和ITL檔案，因此電話要求輸入已簽名的配置檔案。

可以從電話Web介面獲取顯示此行為的電話控制檯日誌：



首先，電話請求一個CTL檔案，該請求成功：

```
837: NOT 09:13:17.561856 SECD: t1RequestFile: 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
```

接下來，電話還會請求一個ITL檔案：

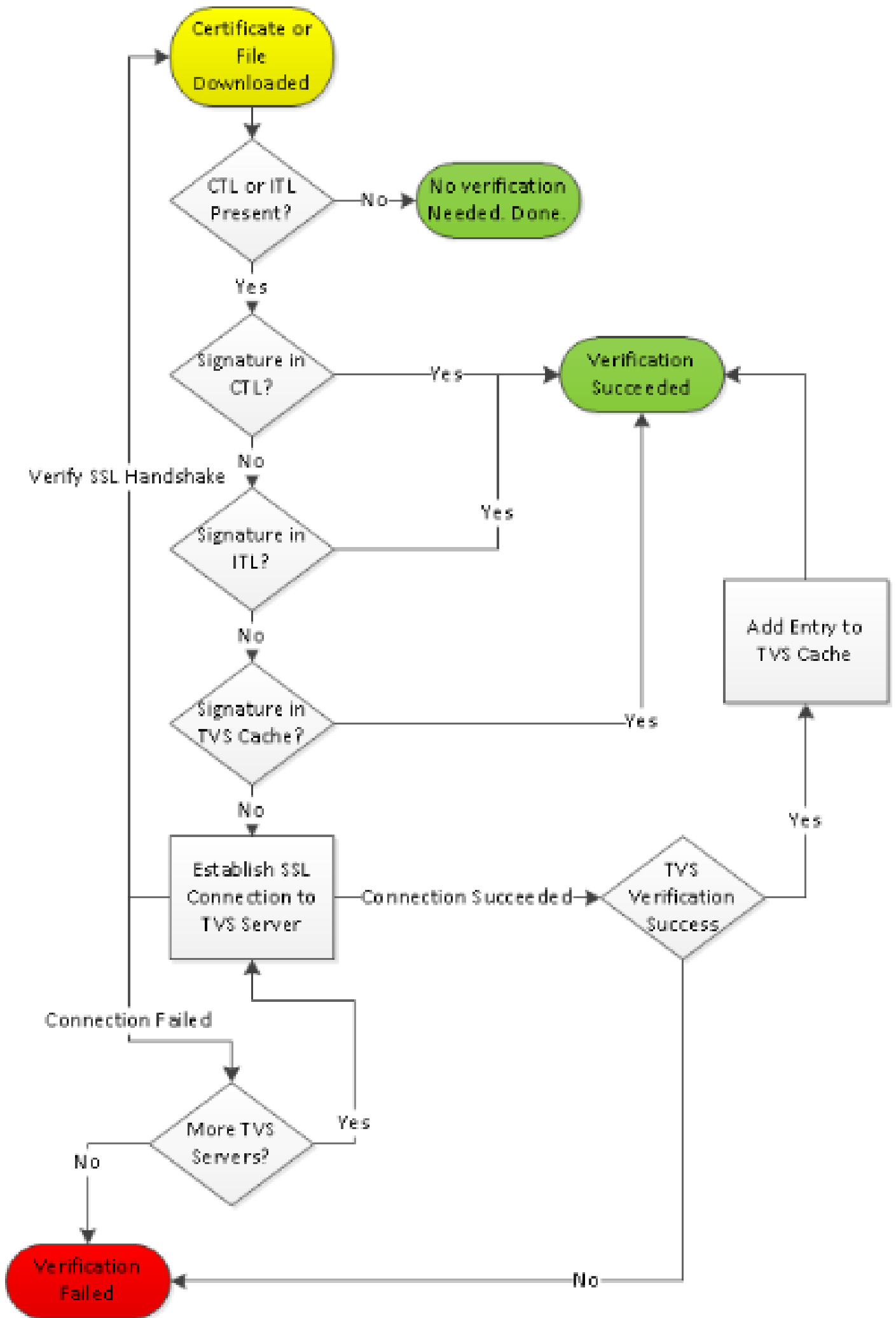
```
868: NOT 09:13:17.860613 TFTP: [28]:Requesting ITLSEP0011215A1AE3.tlv from
14 . 48 . 44 . 80
869: NOT 09:13:17.875059 TFTP: [28]:Finished --> rcvd 5438 bytes
```

電話驗證ITL和配置檔案

ITL檔案下載後，必須對其進行驗證。此時電話可以處於多種狀態，因此本文檔將介紹所有狀態。

- 電話沒有CTL或ITL檔案，或者ITL為空，因為Prepare Cluster for Rollback to Pre 8.0引數。在此狀態下，電話盲目信任下載的下一個CTL或ITL檔案，並且從此以後使用此簽名。
- 該電話已具有CTL，但沒有ITL。在此狀態下，只有在CTL檔案中的CCM+TFTP功能可以驗證某個ITL時，電話才會信任它。
- 該電話已經有一個CTL和一個ITL檔案。在此狀態下，電話會驗證最近下載的檔案是否與CTL、ITL或TVS伺服器中的簽名匹配。

以下是說明電話如何驗證簽名檔案和HTTPS證書的流程圖：



```
File sign verify SUCCESS; header length <296>
```

由於電話下載了CTL和ITL檔案，因此從此時開始，它只請求已簽名的配置檔案。

這說明，電話邏輯是根據CTL和ITL的存在來確定TFTP伺服器是否安全，然後請求簽名檔案：

```
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
```

下載已簽名的配置檔案後，電話必須根據ITL中的CCM+TFTP功能對其進行身份驗證：

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

未知證書的電話聯絡人TVS

ITL檔案提供一個TVS函式，其中包含在CUCM伺服器TCP埠2445上運行的TVS服務的證書。

TVS在啟用CallManager服務的所有伺服器上運行。CUCM TFTP服務使用配置的CallManager組來構建電話必須在電話配置檔案上聯絡的TVS伺服器清單。

某些實驗只使用一個CUCM伺服器。在多節點CUCM集群中，一個電話最多可以有三個TVS條目，該電話的CUCM組中的每個CUCM各一個。

此示例顯示了按下IP電話上的Directories按鈕時發生的情況。「目錄URL」配置為HTTPS，因此電話會顯示「目錄」伺服器的Tomcat Web證書。

此Tomcat Web證書（作業系統管理中的tomcat.pem）未載入到電話中，因此電話必須與TVS聯絡以驗證該證書。

有關互動的說明，請參閱先前的TVS概述圖。以下是電話控制檯日誌的視角：

首先找到目錄URL:

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

這是需要驗證的SSL/傳輸層安全(TLS)安全HTTP會話。

```
1205: NOT 15:20:59.404971 SECD: cIpSetupSsl: Trying to connect to IPV4, IP:  
14 . 48 . 44 . 80, Port : 8443  
1206: NOT 15:20:59.406896 SECD: cIpSetupSsl: TCP connect() waiting,  
<14 . 48 . 44 . 80> c:8 s:9 port: 8443  
1207: NOT 15:20:59.408136 SECD: cIpSetupSsl: TCP connected,  
<14 . 48 . 44 . 80> c:8 s:9  
1208: NOT 15:20:59.409393 SECD: cIpSetupSsl: 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
```

電話首先驗證SSL/TLS伺服器提供的證書是否存在CTL中。然後，電話檢視ITL檔案中的Functions，以檢視是否找到匹配項。

此錯誤消息顯示「HTTPS證書不在CTL中」，這意味著「在CTL或ITL中找不到證書」。

```
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>
```

在檢查證書的CTL和ITL檔案的直接內容之後，電話檢查的下一件事是TVS快取。

如果電話最近向TVS伺服器請求了相同的證書，則這樣做是為了減少網路流量。

如果在電話快取中找不到HTTPS證書，您可以建立與TVS伺服器本身的TCP連線。

```
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: cInt sock fd 11 bound  
to </tmp/secClnt_sec>  
1224: NOT 15:20:59.457643 SECD: getTvsServerInfo: Phone in IPv4 only mode  
1225: NOT 15:20:59.458706 SECD: getTvsServerInfo: Retrieving 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.

請記住，與TVS本身的連線是SSL/TLS (安全HTTP或HTTPS)，因此它也是需要針對CTL到ITL進行身份驗證的證書。

如果一切正常，則在ITL檔案的TVS功能中找到TVS伺服器證書。參見上一個#3例ITL檔案中的ITL記錄資訊。

```
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>
```

成功！電話現在與TVS伺服器具有安全連線。下一步是詢問TVS伺服器「Hello， Do I trust this Directories server certificate？」

此示例顯示對該問題的答案 — 值為0的響應，表示成功（無錯誤）。

```
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
```

由於TVS的響應成功，因此該證書的結果會儲存到快取中。

這表示如果您在接下來的86,400秒內再次按Directories按鈕，則無需聯絡TVS伺服器來驗證證書。您只需訪問本地快取即可。

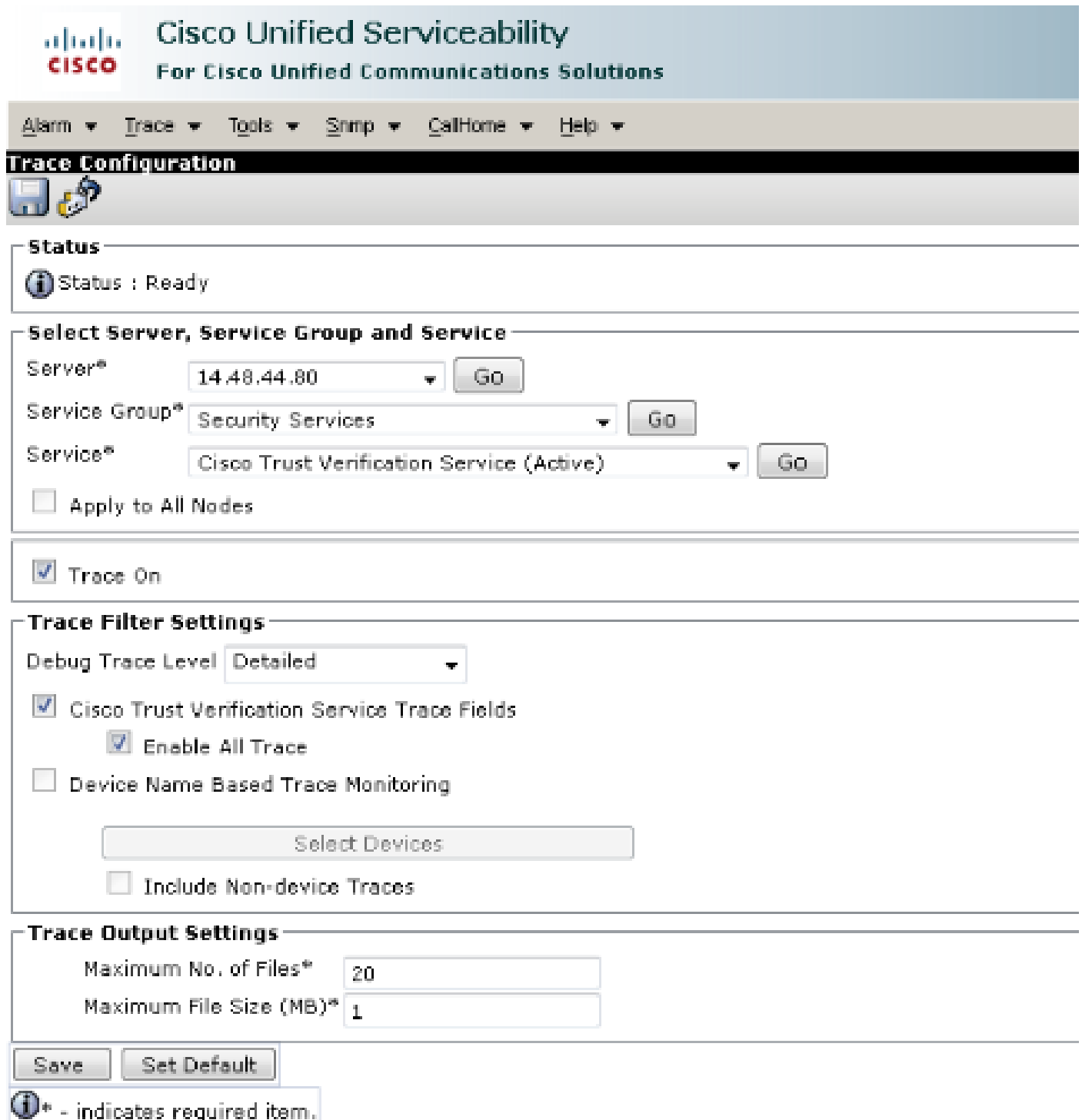
```
1279: NOT 15:20:59.837086 SECD: saveCertToTvsCache: Saving certificate
in TVS cache with default time-to-live value: 86400 seconds
1287: ERR 15:20:59.859993 SECD: Authenticated the HTTPS conn via TVS
```

最後，驗證您與目錄伺服器的連線是否成功。

```
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

以下示例說明在運行TVS的CUCM伺服器上發生的情況。您可以使用思科統一即時監控工具 (RTMT) 收集TVS日誌。



The screenshot shows the Cisco Unified Serviceability interface for configuring traces. At the top, there is a navigation menu with links for Alarm, Trace, Tools, Snmp, CallHome, and Help. The main heading is "Trace Configuration".

Status
Status : Ready

Select Server, Service Group and Service

Server* 14.48.44.80 [GO]
Service Group* Security Services [GO]
Service* Cisco Trust Verification Service (Active) [GO]

Apply to All Nodes

Trace On

Trace Filter Settings

Debug Trace Level Detailed

Cisco Trust Verification Service Trace Fields
 Enable All Trace

Device Name Based Trace Monitoring

[Select Devices]

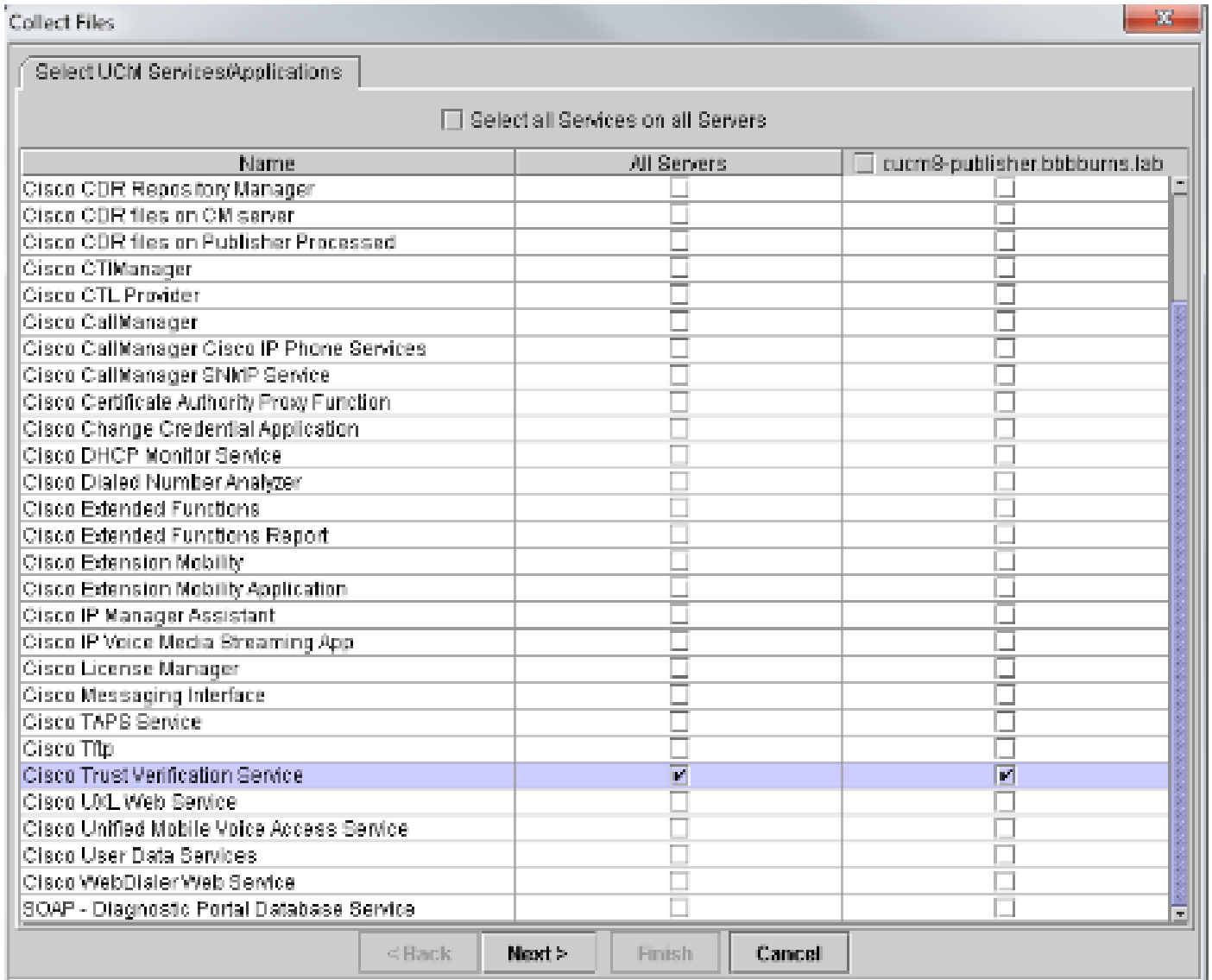
Include Non-device Traces

Trace Output Settings

Maximum No. of Files* 20
Maximum File Size (MB)* 1

[Save] [Set Default]

i* - indicates required item.



CUCM TVS日誌顯示，您與電話進行SSL握手，電話會向TVS詢問有關Tomcat證書的資訊，然後TVS會響應以指示證書在TVS證書儲存中匹配。

```

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

```

TVS證書儲存是OS管理>證書管理網頁中包含的所有證書的清單。

手動驗證電話ITL是否與CUCM ITL匹配

在故障排除時發現的一個常見誤解涉及刪除ITL檔案的趨勢，希望它解決一個檔案驗證問題。

有時需要刪除ITL檔案，但ITL檔案只有在滿足所有這些條件時才需要刪除。

- 電話上的ITL檔案的簽名與CM TFTP伺服器上的ITL檔案的簽名不匹配。
- ITL檔案中的TVS簽名與TVS提供的證書不匹配。
- 當電話嘗試下載ITL檔案或配置檔案時，顯示「驗證失敗」。
- 不存在舊TFTP私鑰的備份。

以下是檢查前兩個條件的方法。

首先，您可以將CUCM上存在的ITL檔案的校驗和與電話的ITL檔案的校驗和進行比較。

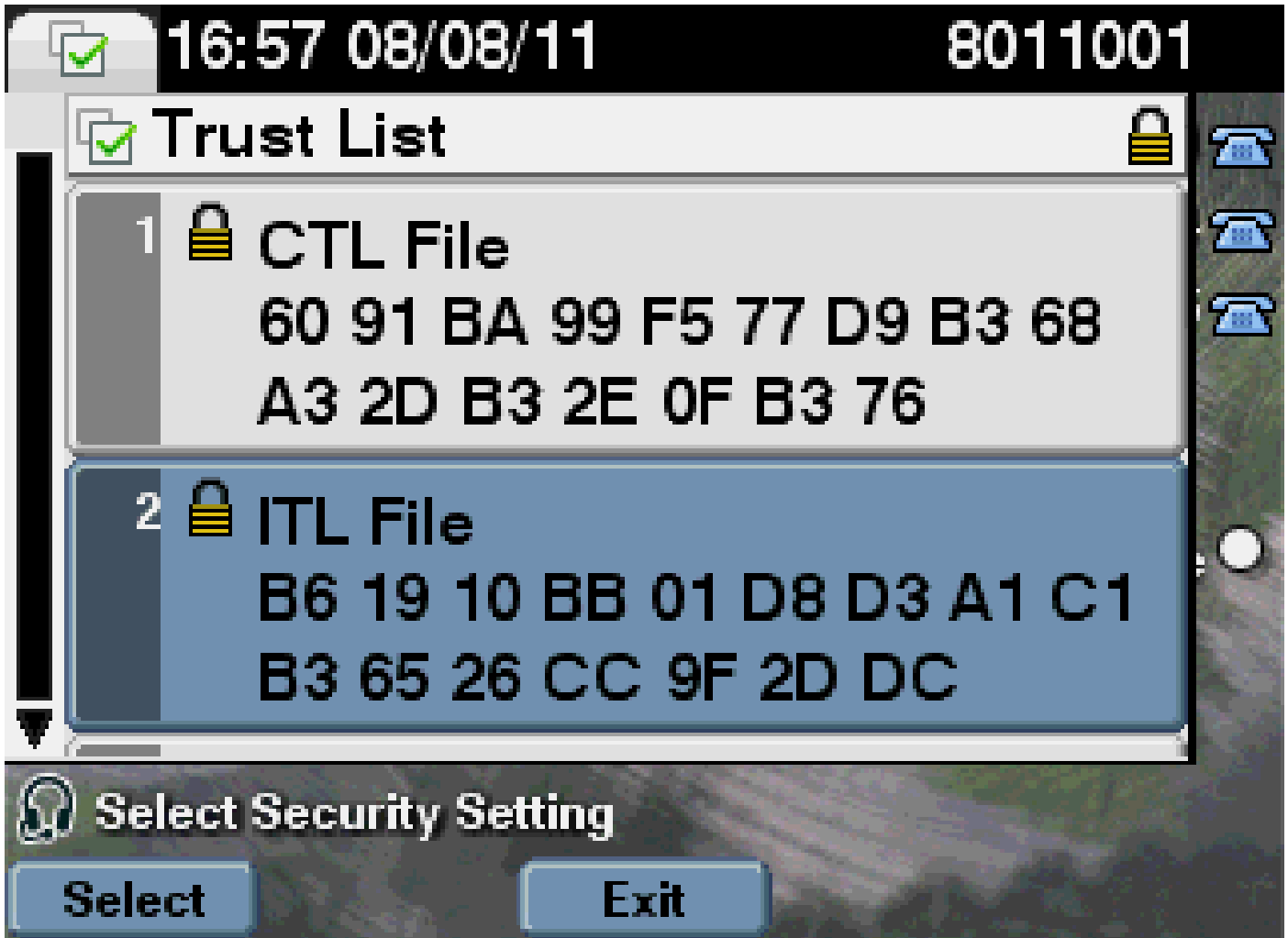
目前，無法從CUCM本身檢視CUCM上ITL檔案的MD5sum，除非您運行帶有此[Cisco錯誤ID CSCto60209](#)修復程式的版本。

在此期間，請使用您喜愛的GUI或CLI程式運行以下命令：

```
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
```

這表明CUCM中ITL檔案的MD5sum是b61910bb01d8d3a1c1b36526cc9f2ddc。

現在，您可以檢視電話本身，以確定在那裡載入的ITL檔案的雜湊：設定>安全配置>信任清單。



這顯示MD5和匹配。這意味著電話上的ITL檔案與CUCM上的檔案匹配，因此不需要將其刪除。

如果匹配，則需要轉到下一個操作 — 確定ITL中的TVS證書是否與TVS提供的證書匹配。這個操作有點複雜。

首先，檢視連線到TCP埠2445上TVS伺服器的電話的資料包捕獲。

在Wireshark中按一下右鍵此流中的任何資料包，按一下Decode As，然後選擇SSL。查詢如下所示的伺服器證書：

No.	Time	Source	Destination	Protocol	Info
1849	11:21:00.713094	14.48.44.202	14.48.44.80	TOP	51221 > cisco-tvs [SYN] Seq=1261968919 win=8192 Len=0 MSS=1400
1850	11:21:00.713121	14.48.44.80	14.48.44.202	TOP	cisco-tvs > 51221 [ACK] Seq=934273112 Ack=1261968920 win=8192
1851	11:21:00.713649	14.48.44.202	14.48.44.80	TOP	51221 > cisco-tvs [ACK] Seq=1261968920 Ack=934273112 win=8192 Len=0
1852	11:21:00.730833	14.48.44.202	14.48.44.80	TLSv1	Client Hello
1853	11:21:00.731044	14.48.44.80	14.48.44.202	TOP	cisco-tvs > 51221 [ACK] Seq=934273113 Ack=1261968924 win=8192 Len=0
1854	11:21:00.731470	14.48.44.80	14.48.44.202	TLSv1	Server Hello, Certificate, Server Hello Done
1855	11:21:00.747987	14.48.44.202	14.48.44.80	TOP	51221 > cisco-tvs [ACK] Seq=1261968974 Ack=934273159 win=8192 Len=0
1858	11:21:00.948093	14.48.44.202	14.48.44.80	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1859	11:21:00.954387	14.48.44.80	14.48.44.202	TLSv1	Change Cipher Spec, Encrypted Handshake Message
1860	11:21:00.967943	14.48.44.202	14.48.44.80	TOP	51221 > cisco-tvs [ACK] Seq=1261969000 Ack=934273618 win=8144 Len=0
1862	11:21:00.0099999	14.48.44.202	14.48.44.80	TLSv1	Application Data
1862	11:21:00.022042	14.48.44.80	14.48.44.202	TLSv1	Application Data, Application Data
1863	11:21:00.035931	14.48.44.202	14.48.44.80	TOP	51221 > cisco-tvs [ACK] Seq=1261970109 Ack=934273718 win=8192 Len=0
1864	11:21:00.046680	14.48.44.202	14.48.44.80	TLSv1	Encrypted Alert
1865	11:21:00.057106	14.48.44.80	14.48.44.202	TLSv1	Encrypted Alert
1866	11:21:00.067204	14.48.44.80	14.48.44.202	TOP	cisco-tvs > 51221 [ACK] Seq=934273791 Ack=1261970146 win=8192

```

Length: 984
  Handshake Protocol: certificate
    handshake type: certificate (31)
    Length: 984
    certificates Length: 978
    certificates (978 bytes)
      certificate Length: 975
      certificate (18-at-countryName=us,1d-at-stateOrProvInceName=north carolina,1d-at-organizationalUnitName=tac)
        signedCertificate
          version: v3 (2)
          certificate: A62E3E1A7BDAA64D84
          signature (shaWithRSAEncryption)
            issuer: rdssequence (0)
              rdssequence: 6 items (1d-at-countryName=us,1d-at-stateOrProvInceName=north carolina,1d-at-organizationalUnitName=tac)
                rdssequence item: 1 item (1d-at-commonName=CUCM8-Publisher.bbburns.lab)
                rdssequence item: 1 item (1d-at-organizationalUnitName=tac)
                rdssequence item: 1 item (1d-at-organizationalUnitName=cisco)
                rdssequence item: 1 item (1d-at-localityName=ntp)
                rdssequence item: 1 item (1d-at-stateOrProvInceName=north carolina)
                rdssequence item: 1 item (1d-at-countryName=us)
            validity
              subject: rdssequence (0)
                rdssequence: 6 items (1d-at-countryName=us,1d-at-stateOrProvInceName=north carolina,1d-at-organizationalUnitName=tac)
                  rdssequence item: 1 item (1d-at-commonName=CUCM8-Publisher.bbburns.lab)
                  rdssequence item: 1 item (1d-at-organizationalUnitName=tac)
                  rdssequence item: 1 item (1d-at-organizationalUnitName=cisco)
                  rdssequence item: 1 item (1d-at-localityName=ntp)
                  rdssequence item: 1 item (1d-at-stateOrProvInceName=north carolina)
                  rdssequence item: 1 item (1d-at-countryName=us)

```

檢視上一個ITL檔案中包含的TVS證書。然後您會看到序列號為2E3E1A7BDAA64D84的條目。

<#root>

admin:

show itl

```

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

```

成功，ITL檔案中的TVS.pem與網路上提供的TVS證書匹配。您不需要刪除ITL，並且TVS提供正確的證書。

如果檔案驗證仍失敗，請檢查前面的流程圖的其餘部分。

限制和互動

重新生成證書/重建群集/證書過期

現在最重要的證書是CallManager.pem證書。該證書私鑰用於簽署所有TFTP配置檔案，其中包括ITL檔案。

如果重新生成CallManager.pem檔案，則會使用新私鑰生成新的CCM+TFTP證書。此外，ITL檔案現在使用此新的CCM+TFTP金鑰進行簽名。

重新生成CallManager.pem並重新啟動TVS和TFTP服務後，電話啟動時會發生這種情況。

1. 電話嘗試從TFTP伺服器下載新的CCM+TFTP簽名的ITL檔案。目前該電話只有舊的國際交易日誌檔案，新金鑰不在電話上的國際交易日誌檔案中。
2. 由於電話在舊ITL中找不到新的CCM+TFTP簽名，因此它會嘗試聯絡TVS服務。



註：此部分非常重要。舊ITL檔案的TVS證書必須仍然匹配。如果同時重新生成CallManager.pem和TVS.pem，則電話不能下載任何新檔案，除非從電話上手動刪除ITL。

3. 當電話聯絡TVS時，運行TVS的CUCM伺服器在作業系統證書儲存區中具有新的CallManager.pem證書。
4. TVS伺服器返回成功，電話將新的ITL檔案載入到記憶體中。
5. 電話現在會嘗試下載已使用新CallManager.pem金鑰簽名的配置檔案。
6. 由於載入了新的ITL，新簽名的配置檔案由記憶體中的ITL成功驗證。

重點：

- 切勿同時重新生成CallManager.pem和TVS.pem證書。
- 如果重新生成TVS.pem或CallManager.pem，則必須重新啟動TVS和TFTP並重置電話，才能獲取新的ITL檔案。
- 較新版本的CUCM會自動處理此電話重置，並在證書重新生成時警告使用者。
- 如果存在多個TVS伺服器（CallManager組中有多個伺服器），則其他伺服器可以對新的CallManager.pem證書進行身份驗證。

在集群之間行動電話

在將電話從一個集群移動到另一個集群並部署了ITL時，必須考慮ITL和TFTP私鑰。

提供給電話的任何新配置檔案必須與CTL、ITL中的簽名或電話當前TVS服務中的簽名匹配。

本文檔說明如何確保新的集群ITL檔案和配置檔案受電話上當前ITL檔案的信任。

<https://supportforums.cisco.com/docs/DOC-15799>。

備份和還原

CallManager.pem證書和私鑰通過災難恢復系統(DRS)進行備份。如果重建了TFTP伺服器，則必須從備份中恢復它，以便可以恢復私鑰。

如果伺服器上沒有CallManager.pem私鑰，則具有使用舊金鑰的當前ITL的電話不信任已簽名的配置檔案。

如果重建了群集但未從備份中恢復，則與「在群集之間移動電話」文檔完全相同。這是因為對於電話而言，包含新金鑰的群集是不同的群集。

備份和還原存在一個嚴重缺陷。如果群集易受Cisco錯誤ID CSCtn50405影響，則DRS備份不包含CallManager.pem證書。

這將導致從此備份還原的任何伺服器生成損壞的ITL檔案，直到生成新的CallManager.pem。

如果沒有其他正常工作的TFTP伺服器未完成備份和還原操作，這可能意味著需要從電話中刪除所有ITL檔案。

要驗證是否需要重新生成CallManager.pem檔案，請輸入show itl命令，然後輸入：

```
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
```

在國際交易日誌輸出中，需要查詢的主要錯誤有：

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

和

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

上一個結構化查詢語言(SQL)查詢搜尋具有「身份驗證和授權」角色的證書。

具有身份驗證和授權角色的先前資料庫查詢中的CallManager.pem證書也必須出現在作業系統管理證書管理網頁中。

如果遇到上述缺陷，則查詢中的CallManager.pem證書與作業系統網頁中的CallManager.pem證書

不匹配。

更改主機名或域名

如果更改CUCM伺服器的主機名或域名，它將立即在該伺服器上重新生成所有證書。憑證再生一節說明，再生TVS.pem和CallManager.pem都是「壞事」。

有幾種情況下主機名更改會失敗，也有一些情況下會順利工作，而不會出現問題。本節涵蓋所有這些資訊，並將它們連結回您從本文檔中已經瞭解的關於電視和國際交易日誌的內容。

僅使用ITL的單節點集群（請注意，此操作會中斷，不會進行準備）

- 使用Business Edition伺服器或僅發行者部署，在您更改主機名的同時重新生成CallManager.pem和TVS.pem。
- 如果在單個節點集群上更改主機名，而未首先使用此處介紹的[Rollback Enterprise引數](#)，則電話無法根據當前ITL檔案驗證新的ITL檔案或配置檔案。
- 電話無法連線到TVS，因為TVS證書也不再受信任。
- 電話顯示有關「信任清單驗證失敗」的錯誤，新的配置更改沒有生效，安全服務URL失敗。
- 如果不首先採取步驟2中的預防措施，則唯一的解決辦法是[手動刪除每台電話的國際交易日誌](#)。

具有CTL和ITL的單節點集群（可以暫時斷開，但易於修復）

- 執行完伺服器重新命名操作後，重新運行CTL客戶端。這會將新的CallManager.pem證書放在電話下載的CTL檔案中。
- 根據CTL檔案中的CCM+TFTP功能，可以信任包含新ITL檔案的新配置檔案。
- 這工作正常，因為更新的CTL檔案基於保持不變的USB eToken私鑰受信任。

僅使用ITL的多節點集群（這通常有效，但如果匆忙完成，可能會永久中斷）

- 由於多節點群集有多個TVS伺服器，因此任何一個伺服器都可以順利重新生成其證書。當電話收到這個新的、不熟悉的簽名時，它會要求另一台TVS伺服器驗證新的伺服器證書。
- 有兩個主要問題可能導致此操作失敗：
 - 如果同時重新命名並重新引導所有伺服器，則當伺服器和電話恢復運行時，任何一台電視伺服器都無法通過已知證書訪問。
 - 如果電話的CallManager組中只有一個伺服器，則其他TVS伺服器不會產生任何影響。請參閱「單節點群集」方案以解決此問題，或將其他伺服器新增到電話CallManager組。

具有CTL和ITL的多節點集群（無法永久斷開）

- 執行完重新命名後，TVS服務會驗證新證書。
- 即使所有TVS伺服器因某種原因不可用，仍可使用CTL客戶端以使用新的CallManager.pem CCM+TFTP證書更新電話。

集中式TFTP

帶ITL的電話啟動時，會請求以下檔案：CTLSEP<MAC Address>.tlv、ITLSEP<MAC

Address>.tlv和SEP<MAC Address>.cnf.xml.sgn。

如果電話找不到這些檔案，便會請求ITLFile.tlv和CTLFile.tlv，後者是由集中式TFTP伺服器提供給任何要求它的電話的。

使用集中式TFTP時，有一個TFTP群集可以指向許多其他子群集。

這通常是因為多個CUCM集群上的電話共用相同的DHCP作用域，因此必須具有相同的DHCP選項150 TFTP伺服器。

所有IP電話都指向中央TFTP集群，即使它們註冊到其他集群也是如此。每當此中央TFTP伺服器收到其找不到檔案的請求時，都會查詢遠端TFTP伺服器。

由於這種操作，集中式TFTP只能在ITL同構環境中工作。

所有伺服器必須運行CUCM 8.x版或更高版本，或者所有伺服器必須運行8.x版之前的版本。

如果集中TFTP伺服器提供ITLFile.tlv，則電話不信任來自遠端TFTP伺服器的任何檔案，因為簽名不匹配。

這是異種混合體發生的。在同構混合中，電話請求ITLSEP<MAC>.tlv，該請求是從正確的遠端群集拉出的。

在混合使用版本8.x前版本和版本8.x群集的異構環境中，必須在8.x版本群集上啟用「準備群集以回滾到版本8.0」，如[Cisco錯誤ID CSCto87262](#)中所述。

使用HTTP而不是HTTPS配置「安全電話URL引數」。這有效地禁用了電話上的國際交易日誌功能。

常見問題

我可以關閉SBD嗎？

只有當SBD和ITL當前工作的情況下，才能關閉SBD。

在具有[Prepare Cluster for Rollback to pre 8.0"企業引數](#)以及使用HTTP而不是HTTPS配置「安全電話URL引數」的電話上，可以臨時禁用SBD。

當您設定Rollback引數時，它會建立一個帶有空函式項的帶符號的ITL檔案。

「空」ITL檔案仍被簽名，因此群集必須處於完全正常運行的安全狀態，才能啟用此引數。

啟用此引數並下載並驗證帶有空白條目的新ITL檔案後，電話接受任何配置檔案，無論其簽名者是誰。

建議不要將群集保持此狀態，因為之前提到的三個功能（經過身份驗證的配置檔案、加密的配置檔案和HTTPS URL）均不可用。

CallManager.pem丟失後，能否從所有電話輕鬆刪除ITL檔案？

目前沒有從思科遠端提供的電話中刪除所有ITL的方法。正因如此，本文檔中介紹的程式和互動作用必須加以考慮。

目前有一個未解析的[Cisco錯誤ID CSCto47052](#)增強功能來要求此功能，但尚未實作。

在過渡期間，已通過[Cisco錯誤ID CSCts01319](#)新增了一項新功能，該功能可能允許思科技術支援中心(TAC)還原到先前受信任的ITL (如果伺服器中仍可使用該功能)。

這僅在以下特定情況下起作用：集群使用具有此缺陷修復程式的版本，並且先前的ITL存在於儲存在伺服器上的特定位置的備份中。

檢視缺陷以檢視您的版本是否有修補程式。請與Cisco TAC聯絡，以便執行缺陷中說明的可能的復原程式。

如果上述程式不可用，則必須手動按下電話上的電話按鍵才能刪除國際交易日誌檔案。這是安全與易於管理之間的權衡。為了使國際交易日誌檔案真正安全，不得輕易地將其遠端刪除。

即使使用指令碼按鈕按下簡單對象訪問協定(SOAP)XML對象，也無法遠端刪除ITL。

這是因為，此時TVS訪問 (因此用於驗證傳入的SOAP XML按鈕按鈕對象的安全身份驗證URL訪問) 不起作用。

如果驗證URL未配置為安全，則有可能對按鍵進行指令碼化以刪除ITL，但思科無法提供此指令碼。

其他不使用身份驗證URL對遠端按鍵進行指令碼化的方法可能由第三方提供，但這些應用程式不是由Cisco提供的。

刪除國際交易日誌最常用的方法是向所有電話使用者傳送電子郵件廣播，指示他們輸入按鍵順序。

如果設定訪問許可權設定為Restricted或Disabled，則電話需要出廠重置，因為使用者無權訪問電話的「設定」選單。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。