Contents

[Introduction](#)
[Overview](#)
[Components Used](#)
[When to Regenerate Certificates](#)
[Service Impact by the Certificate Store](#)
[Create a DRS Backup](#)
[Determine if the Cluster is in Mixed-Mode](#)
[If the Cluster is in Mixed-Mode](#)
[Verify Security by Default on the Cluster](#)
[Utilize the "Prepare Cluster for Rollback to pre 8.0" Feature](#)
[Regenerate Certificates in Specific Order](#)
[Remove and Regenerate Certificates in CUCM](#)
[Regenerate Certificates via the CLI](#)
[Remove Certificates via the CLI](#)
[Regenerate Certificates via the Web GUI](#)
[Remove Certificates via the Web GUI](#)
[After Regeneration/Removal of Certificates](#)
[Install/Update LSC on Phone](#)
[Conclusion](#)
[Related Cisco Support Community Discussions](#)

Introduction

This document provides a recommended, step-by-step procedure to regenerate certificates used in Cisco Unified Communications Manager (CUCM) Release 8.x and later. The security by default feature (ITL) and Mixed-Mode (CTL) are also be covered in order to avoid any undesired outages. For example, how to avoid phone registration issues or phones that do not accept configuration changes or firmwares.

> **Caution**: It is always recommended to complete certificate regeneration in a maintenance window.

Overview

This document discusses the certificate regeneration process for these services:

- CallManager
- CAPF (Certificate Authority Proxy Function)
- IPsec
- Tomcat
- TVS (Trust Verification Service)
- ITLRecovery (only for CUCM 10.X and later)

- phone-vpn-trust
- phone-sast-trust
- phone-trust
- phone-ctl-trust

As well as these phone certificates:

- LSCs (Locally Significant Certificates)
- MICs (Manufacturer Installed Certificates)

Components Used

All of the outputs and screenshots shown in this document are based on CUCM Release 9.1(2)SU2a, however the presented procedure can be used with CUCM Release 8.x and later. Differences that are release specific are mentioned in the appropriate sections.

The information in this document was based on devices in a lab environment which started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command and action taken.

When to Regenerate Certificates

Most of the certificates used in CUCM after a fresh installation are self-signed certificates issued, by default, for five years. Note that the five year time range currently cannot be modified to be a shorter range of time on CUCM. However, a Certificate Authority (CA) can issue certificates for nearly any range of time.

There are also some trusted certificates (such as CAPF-trust and CallManager-trust) that are preloaded and have a longer validity period. For example, the "Cisco Manufacturing CA" certificate is provided on CUCM trust stores to specific features and will not expire until the year 2029.

Certificates should be regenerated before they expire. When the certificates are about to expire you will receive warnings in RTMT (Syslog Viewer) and an email with notification will be sent if configured.

An example of a certificate expiration notification that details the "CUCM01.der" certificate will expire on "Mon May 19 14:46" on server CUCM02 on the trust store "tomcat-trust"is shown here:

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
SyslogSeverityMatchFound events generated:

SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent

ClusterID :
```

```
NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

If the service certificates (certificate stores that are not labeled with "-trust") are already expired it is still possible to regenerate them. Keep in mind that expired certificates might have an impact on your CUCM functionality, dependent upon the cluster's configuration. Considerations are discussed in the next sections.

Service Impact by the Certificate Store

It is critical for good functionality of the system to have all certificates updated across the CUCM cluster. If your certificates are expired or invalid they might significantly affect normal functionality of the system. A list of potential issues you might have when any of the specific certificates is invalid or expired is shown here. The impact might differ dependent upon your system setup.

CallManager.pem

- Encrypted/authenticated phones do not register.
- TFTP not trusted (phones do not accept signed configuration files and/or ITL files).
- Phone services might be affected.
- Secure Session Initiation Protocol (SIP) trunks or media resources (Conference bridges, Media Termination Point (MTP), Xcoders, and so on) will not register or work.
- The AXL request fails.

Tomcat.pem

- Phones are not able to access HTTPs services hosted on the CUCM node, such as Corporate Directory.
- CUCM's web GUI issues, such as unable to access service pages from other nodes in the cluster.
- Extension Mobility or Extension Mobility Cross Cluster issues.

CAPF.pem

- Phones do not authenticate for Phone VPN, 802.1x, or Phone Proxy.
- Cannot issue LSC certificates for the phones.
- Encrypted configuration files do not work.

IPSec.pem

- Disaster Recovery System (DRS)/Disaster Recovery Framework (DRF) might not function properly.
- IPsec tunnels to Gateway (GW) to other CUCM clusters do not work.

TVS (Trust Verification Service)

- The phone cannot authenticate HTTPS service. The p configuration files (this can affect nearly everything on CUCM).

phone-vpn-trust

- The phone VPN will not work, because the VPN's HTTPS URL cannot be authenticated.

  Note: If this does not exist do not worry. This is only for specific configurations.

phone-sast-trust

- Previous CTL/eTokens will not be able to update or modify CTL.

  Note: If this does not exist do not worry. This is only for specific configurations.

phone-trust and phone-ctl-trust

- Visual Voicemail with Unity or Unity Connection will not work.

  Note: If this does not exist do not worry. This is only for specific configurations.

LSCs and MICs

- Phones do not register, phone does not authenticate to Phone VPN, Phone Proxy, or 802.1x.

  Note: MICs are on most phone models by default. LSCs are signed by CAPF and last five years by default. Software clients such as CIPC (Cisco IP Communicator) and Jabber do not have a MIC installed.

Create a DRS Backup

It is recommended to create a DRS backup before you perform any major changes like this. CUCM DRF backups will back up all certificates in the cluster. All DRS backup/restore procedures can be found in the Cisco "

Caution: CSCtn50405, CUCM DRF Backup does not backup certificates

Determine if the Cluster is in Mixed-Mode

In order to determine if you run a CTL/Secure/Mixed-Mode cluster, choose **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure; 1 == Mixed Mode)**.

If the Cluster is in Mixed-Mode

If you run a CUCM cluster in Mixed-Mode, this means that the CTL file needs to be updated after all certificate changes. The procedure on how to do this is within Cisco's Security Guide Documentation. However, be sure that you have at least one eToken from the original initiation of Mixed-Mode feature and the eToken password is known.

Note: An update of the CTL does not happen automatically (as it does in case of the ITL file). It needs to be completed manually by the administrator with either the CTL Client or the CLI command.

In CUCM 10.X and later you can put the cluster into Mixed-Mode in two ways:

- CLI command - if this method is used then your CTL file is signed with the CallManager.pem certificate of the Publisher server. `admin:show ctl`
  `The checksum value of the CTL file:`

```
0c05655de63fe2a042cf252d96c6d609(MD5)
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1156
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 694 E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
A5 A3 8C 9C (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

- CTL client - if this method is used then your CTL file is signed with one of the hardware eTokens. `admin:show ctl`

```
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Note: You can move between the method used with CUCM Mixed Mode with Tokenless CTL.

Dependent upon the method used to secure your cluster, an appropriate CTL update procedure needs to be used. Either rerun the CTL client or enter the **utils ctl update CTLfile** command from the CLI.

Verify Security by Default on the Cluster

Avoidance of ITL issues is important, because ITL issues can cause many features to fail or the phone will refuse to abide by any changes to configurations. ITL issues can be avoided in these two ways.

Utilize the "Prepare Cluster for Rollback to pre 8.0" Feature

This feature "blanks" out your ITL on all servers, so the phones will trust any TFTP server. Phone services (for example, extension mobility) will NOT work when this parameter is set to True. However, users will be able to continue to make and receive basic phone calls.

> **Note**: A change to this parameter causes ALL PHONES TO RESET.

Once this feature is set, all TFTP servers need to be restarted (in order to supply the new ITL) and all phones need to be reset in order to force them to request the new "blank" ITL. Once the certificate changes are completed and all necessary services have been restarted, this feature can be set back to "False", TFTP service restarted, and the phone reset (so the phone can obtain the valid ITL file). Then all features will continue to work as they did previously.

Regenerate Certificates in Specific Order

This procedure provides a TFTP server with a valid/updated ITL file from a trusted TFTP server that is available.

1. Stop TFTP service on the Primary TFTP server.
2. Make changes on the Primary TFTP server's certificates (as needed).
3. Reset the phones (in order to get a new ITL file from the Secondary TFTP server) - dependent upon which certificates are regenerated, this might happen automatically.
4. Once phones have returned, start the Primary TFTP server's TFTP service.
5. Make certificate changes on the Secondary TFTP server.
6. Reset the phones (in order to get a new ITL file from the Primary TFTP server).

> **Caution**: Do NOT edit certificates on both TFTP servers at the same time. This gives the phones no TFTP server to trust and requires the local administrator to manually remove the ITL from all phones.

Remove and Regenerate Certificates in CUCM

Only service certificates (certificate stores that are not labeled with "-trust") can be regenerated. Certificates in the trust stores (certificate stores that are labeled with "-trust") need to be deleted, as they cannot be regenerated.

> **Caution**: Be aware of Cisco bug ID CSCut58407 - Devices shouldn't restart when CAPF / CallManager / TVS-trust is removed.

After all certificate modifications, the respective service needs to be restarted to take on the change. This is covered in the After Regeneration/Removal of Certificates section.

> **Caution**: Be aware of Cisco bug ID CSCto86463 - Deleted certificates reappear, unable to

remove certificates from CUCM. This is an issue where deleted certificates continue to reappear after removal. Follow the workaround in the defect.

Regenerate Certificates via the CLI

Caution: Regenerations of certificates triggers an automatic update of the ITL files within the cluster, which triggers a cluster-wide soft phone reset to allow phones to trigger an update of their local ITL. This is focused on CAPF and CallManager certificate regenerations, but can occur with other certificate stores within CUCM, such as Tomcat.

Regenerate CAPF

Upon regeneration, the CAPF certificate automatically uploads itself to CAPF-trust and CallManager-trust. Also, CAPF always has a unique Subject Name header, thus previously used CAPF certificates will be retained and used for authentication.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Note: If a CAPF certificate gets expired, phones that use LSC will not be able to register to CUCM because CUCM rejects their certificate. However, you can still generate a new LSC for the phone with the new CAPF certificate. When you reboot the phone it downloads the configuration and then contacts CAPF in order to update LSC. After LSC is updated, the phone registers as it should. This works as long as a new CAPF certificate is in the ITL file and the phone downloaded and trusted the certificate that signed it (callmanager.pem).

Regenerate CallManager

Upon regeneration, the CallManager automatically uploads itself to CallManager-trust.

```
admin:show ctl
The checksum value of the CTL file:
```

```
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Regenerate IPsec

Upon regeneration, the IPsec certificate automatically uploads itself to ipsec-trust.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Regenerate Tomcat

Upon regeneration, the Tomcat certificate automatically uploads itself to tomcat-trust.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015
```

```
[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Regenerate TVS

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

What to Expect

When you regenerate certificates via the CLI, you are requested to verify this change. Type **yes** and press **Enter**.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
```

```
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Remove Certificates via the CLI

Remove CAPF-trust Certificates

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Remove CallManager-trust Certificates

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
```

```
10 IPADDRESS 4
```
This etoken was used to sign the CTL file.

Remove ipsec-trust Certificates

```
admin:show ctl
The checksum value of the CTL file:
```
256a661f4630cd86ef460db5aad4e91c(MD5)
```
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
```
This etoken was used to sign the CTL file.

Remove Tomcat-trust Certificates

```
admin:show ctl
The checksum value of the CTL file:
```
256a661f4630cd86ef460db5aad4e91c(MD5)
```
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
```
This etoken was used to sign the CTL file.

Remove TVS-trust Certificates

```
admin:show ctl
The checksum value of the CTL file:
```
256a661f4630cd86ef460db5aad4e91c(MD5)
```
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
```

```
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Regenerate Certificates via the Web GUI

Regenerate CAPF

Upon regeneration, the CAPF certificate automatically uploads itself to CAPF-trust and CallManager-trust. Also, the CAPF certificate always has a unique Subject Name header, thus previously used CAPF certificates are retained and used for authentication.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Regenerate CallManager

Upon regeneration, the CAPF certificate automatically uploads itself to CallManager-trust.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
```

```
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Regenerate IPsec

Upon regeneration, the IPsec certificate automatically uploads itself to ipsec-trust.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Regenerate Tomcat

Upon regeneration, the Tomcat certificate automatically uploads itself to tomcat-trust.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
```

```
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Regenerate TVS

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Remove Certificates via the Web GUI

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
```

```
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
```
This etoken was used to sign the CTL file.

After Regeneration/Removal of Certificates

After you remove or regenerate a certificate from a certificate store, the respective service needs to be restarted in order to take on the change.

Store	Service to Restart	How (C == CLI; W == Web GUI)
Tomcat	Tomcat	C: utils service restart Cisco Tomcat G: Cisco Unified Serviceability > Tools > Control Center - Feature Services > (Select Server) > select "Cisco CallMana > Restart AND G: Cisco Unified Serviceability > Tools > Control Center - Feature Services > (Select Server) > select "Cisco Tftp" > R
CallManager	CallManager; TFTP	
CAPF	CAPF (On Publisher only)	G: Cisco Unified Serviceability > Tools > Control Center - Feature Services > (Select Server) > select "Cisco Certificat Authority Proxy Function" > Restart
TVS	Trust Verification Service (on respective server)	G: Cisco Unified Serviceability > Tools > Control Center - Network Services > (Select Server) > select "Cisco Trust Verification Service" > Restart
ipsec	Cisco DRF Local (on all nodes); Cisco DRF Master (on Publisher)	C: utils service restart Cisco DRF Local AND C: utils service restart Cisco DRF Master

Install/Update LSC on Phone

If the CAPF certificate has been regenerated, then LSC certificates for all the phones in the cluster need to be updated with LSC signed by the new CAPF certificate.

1. Choose **CUCM Serviceability > Service Activation**. Activate the Cisco CTL Provider and Cisco Certificate Authority Proxy Function on the publisher server.
2. From CUCM CCMAdmin, choose **Device > Phone.** Pick the IP Phone you want to provision an LSC on.
3. In the Device configuration page under Certificate Operation, choose **Install / Upgrade > By Null String**.
4. Save the phone configuration in CCMAdmin and choose **Apply Config**.

If the phone has trouble with the installation of the LSC, complete these actions on the phone:

When the phone resets, go to the physical phone and choose **Settings > (6) Security Configuration > (4) LSC > **#** (this operation unlocks the GUI and allows us to continue to the next step) **> Update** (update will not be visible until you perform the previous step) > **Submit**.

Do not assign any certificates to a phone unless it is a wireless phone (7921/25). Wireless phones use 3rd party Certificate Authorities (CA) in order to authenticate themselves.

Conclusion

Should you run into an issue or need assistance with this procedure, contact the Cisco Technical

Assistance Center (TAC) for assistance. In this case, keep your DRF Backup available as it will be used as a last resort in order to restore service if TAC is unable to do so through other methods.