Regeneration of Certificates for CUCM

Contents

Introduction

This document describes the procedure to regenerate certificates in Cisco Unified Communications Manager (CUCM) release 8.X and later.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- *Real Time Monitoring Tool* (RTMT)
- CUCM Certificates

Components Used

The information in this document is based on these software and hardware versions:

- CUCM release 8.X and higher

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes the step-by-step procedure on how to regenerate certificates in Cisco Unified Communications Manager (CUCM) release 8.X and newer. However, this does not reflect the changes post 12.0 to ITL recovery.

Install RTMT

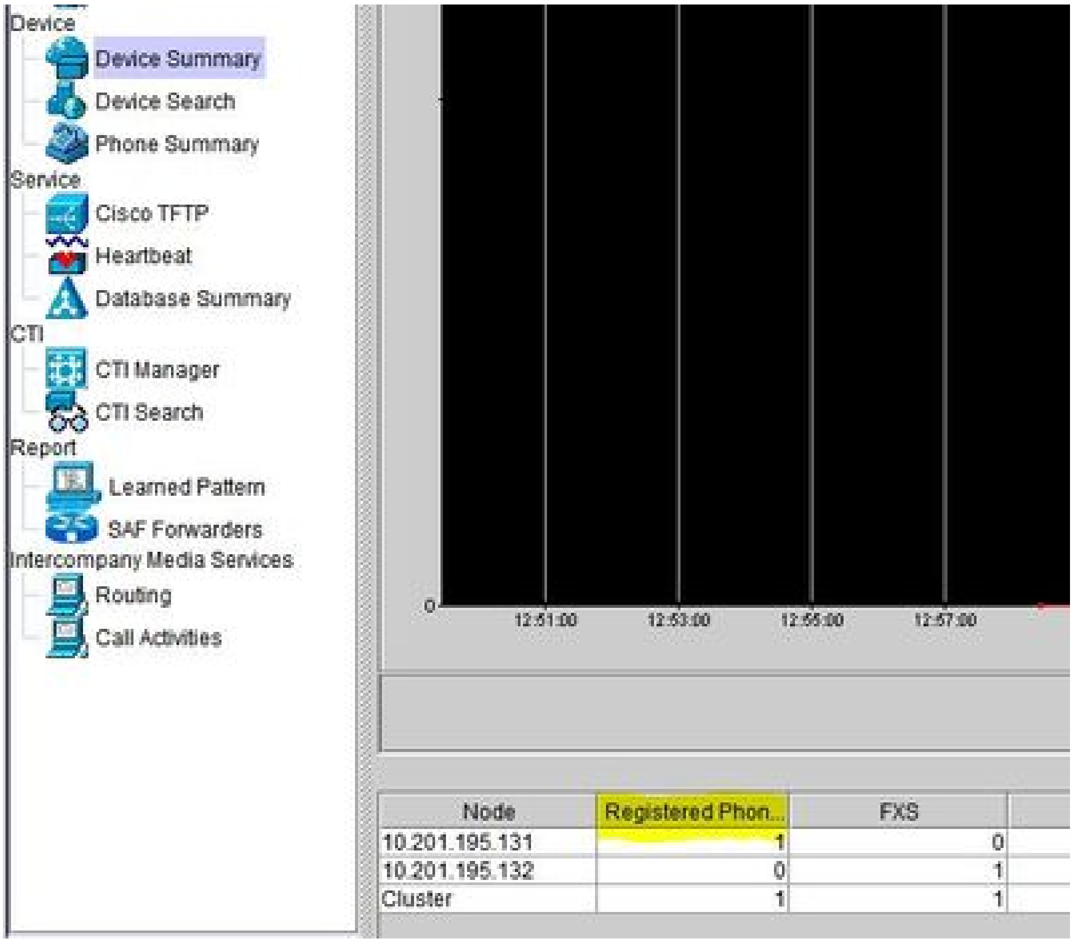
- Download and install RTMT Tool from Call Manager. Navigate to Call Manager (CM) Administration: **Application > Plugins > Find > Cisco Unified Real-Time Monitoring Tool - Windows > Download** Install And launch

Monitor Endpoints with RTMT

- Launch RTMT and enter the IP address or Fully Qualified Domain Name (FQDN), then username and password to access the tool:
- Select the **Voice/Video Tab**.Select **Device Summary**. This section identifies the total number of registered end-points and how many to each nodeMonitor while endpoint reset to ensure registration prior to the regeneration of the next certificate

Tip: The regeneration process of some certificates can impact endpoint. Consider an action plan after regular business hours due to the requirement to restart services and reboot phones. Verify phone registration via RTMT is highly recommended.

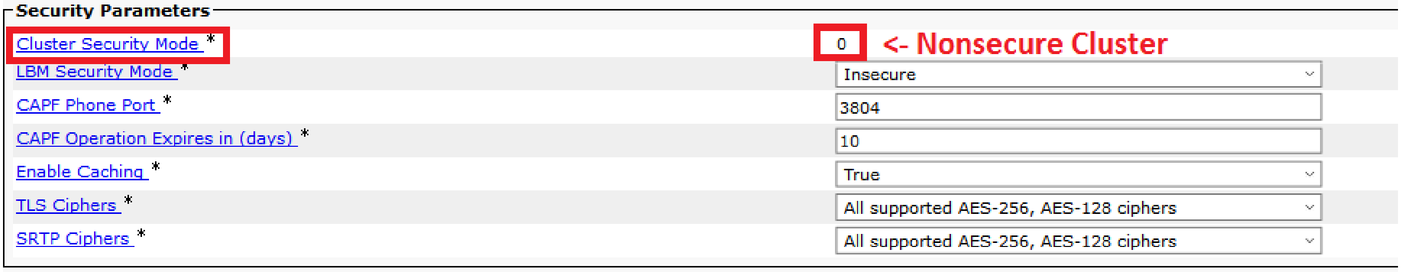
Warning: Endpoints with current ITL mismatch can have registration issues after this process. The deletion of the ITL on the endpoint is a typical best practice solution after the regeneration process is completed and all other phones have registered.



Node	Registered Phon...	FXS
10.201.195.131	1	0
10.201.195.132	0	1
Cluster	1	1

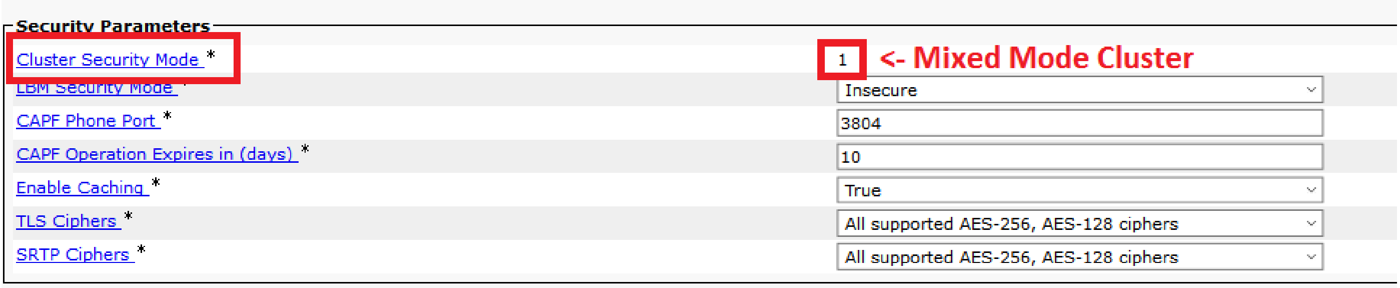
Identify if your cluster is in Mixed-Mode or Non-Secure Mode

- Navigate to CM Administration. **System > Enterprise Parameters > Security Parameters > Cluster Security Mode**



Security Parameters

Cluster Security Mode *	0 <- Nonsecure Cluster
LBM Security Mode *	Insecure
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
Enable Caching *	True
TLS Ciphers *	All supported AES-256, AES-128 ciphers
SRTP Ciphers *	All supported AES-256, AES-128 ciphers



Security Parameters

Cluster Security Mode *	1 <- Mixed Mode Cluster
LBM Security Mode *	Insecure
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
Enable Caching *	True
TLS Ciphers *	All supported AES-256, AES-128 ciphers
SRTP Ciphers *	All supported AES-256, AES-128 ciphers

Impact by the Certificate Store

It is critical for successful system functionality to have all certificates updated across the CUCM cluster. If certificates are expired or invalid they can significantly affect normal functionality of the system. The impact can differ dependent upon your system setup. A list of services for the specific certificates that are invalid or expired is shown here:

CallManager.pem

- Encrypted/authenticated phones do not register
- Trivial File Transfer Protocol (TFTP) is not trusted (phones do not accept signed configuration files and/or ITL files)
- Phone services can be affected
- Secure Session Initiation Protocol (SIP) trunks or media resources (Conference bridges, Media Termination Point (MTP), Xcoders, and so on) does 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 can have various web issues, such as unable to access service pages from other nodes in the cluster
- Extension Mobility (EM) or Extension Mobility Cross Cluster issues
- Single Sign-On (SSO)
- If UCCX (Unified Contact Center Express) is integrated, due to security change from CCX 12.5 it is required to have upload CUCM Tomcat certificate (self-signed) or the Tomcat root & intermediate certificate (for CA signed) in UCCX tomcat-trust store since it effect Finesse desktop logins.

CAPF.pem

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

IPSec.pem

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

TVS (Trust Verification Service)

Trust Verification Service (TVS) is the main component of Security by Default. TVS enables Cisco Unified IP Phones to authenticate application servers, such as EM services, directory, and MIDlet, when HTTPS is established.

TVS provides these features:

- Scalability - Cisco Unified IP Phone resources are not impacted by the number of certificates to trust.

- Flexibility - Addition or removal of trust certificates are automatically reflected in the system.
- Security by Default - Non-media and signal security features are part of the default installation and do not require user intervention.

ITL and CTL

- ITL contains the certificate role for Call Manager TFTP, all TVS certificates in the cluster, and Certificate Authority Proxy Function (CAPF) when ran.
- CTL contains entries for System Administrator Security Token (SAST), Cisco CallManager and Cisco TFTP services that are ran on the same server, CAPF, TFTP server(s), and Adaptive Security Appliance (ASA) firewall. TVS is not referenced in CTL.

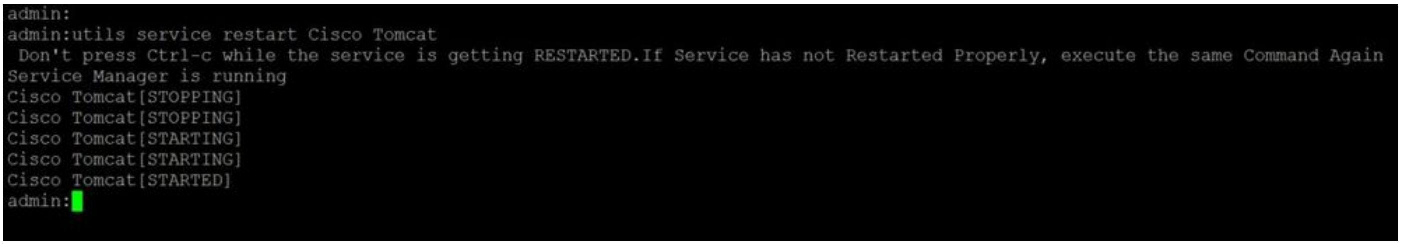
Certificate Regeneration Process

> **Note**: All the endpoints need to be powered on and registered before the certificates regeneration. Otherwise, the not connected phones require the removal of the ITL.

Tomcat Certificate

Identify if third party certificates are in use:

1. Navigate to each server in your cluster (in separate tabs of your web browser) begin with the publisher, followed by each subscriber. Navigate to **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Observe from Description column if Tomcat states Self-signed certificate generated by system. If Tomcat is third party signed, follow the link provided and perform those steps after the Tomcat regeneration.Third Party Signed certificates, refer to CUCM Uploading CCMAdmin Web GUI Certificates.
2. Select **Find** in order to show all the certificates: Select the **Tomcat pem** Certificate.Once open select **Regenerate** and wait until you see the Success pop-up then close pop-up or go back and select **Find/List**.
3. Continue with each subsequent Subscriber, follow the same procedure in step 2 and complete on all Subscribers in your cluster.
4. After all Nodes have regenerated the Tomcat certificate, restart the tomcat service on all the nodes. Begin with the publisher then followed by the subscribers. In order to restart Tomcat you need to open a CLI session for each node and execute the command **utils service restart Cisco Tomcat**.



```
admin:
admin:utils service restart Cisco Tomcat
 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

5. These steps are needed from the CCX enviroment if applicable:

- If self-signed certificate is used, upload the Tomcat certificates from all nodes of the CUCM

cluster to Unified CCX Tomcat trust store.
- If CA signed or private CA signed certificate is used, upload root CA certificate of CUCM to Unified CCX Tomcat trust store.
- Restart the servers as mentioned in the certificate regeneration document for CCX.

Additional References:

- UCCX Solution Certificate Management Guide
- Unified CCX Health Check Utility

IPSEC Certificate

Note: CUCM/Instant Messaging and Presence (IM&P) before version10.X the DRF Master Agent runs on both CUCM Publisher and IM&P Publisher. DRF Local service runs on the subscribers respectively. Versions 10.X and higher, DRF Master Agent runs on the CUCM Publisher only and DRF Local service on CUCM Subscribers and IM&P Publisher and Subscribers.

Note: The Disaster Recovery System uses an Secure Socket Layer (SSL) based communication between the Master Agent and the Local Agent for authentication and encryption of data between the CUCM cluster nodes. DRS makes use of the IPSec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSEC truststore (hostname.pem) file from the Certificate Management page, then DRS do not work as expected. If you delete the IPSEC-trust file manually, then you must ensure that you upload the IPSEC certificate to the IPSEC trust-store. For more details, refer to the certificate management help page in the Cisco Unified Communications Manager Security Guides.

1. Navigate to each server in your cluster (in separate tabs of your web browser) begin with the publisher, followed by each subscriber. Navigate to **Cisco Unified OS Administration > Security > Certificate Management > Find**:
 Select the **IPSEC pem** Certificate.Once open select **Regenerate** and wait until you see the Success pop-up then close pop-up or go back and select **Find/List**.
2. Continue with subsequent Subscribers; follow the same procedure in step 1 and complete on all subscribers in your cluster.
3. After all Nodes have regenerated the IPSEC certificate then restart services.
 Navigate to the Publisher **Cisco Unified Serviceability**. **Cisco Unified Serviceability > Tools > Control Center - Network Services**.Select **Restart** on **Cisco DRF Master**service.Once the service restart completes, select **Restart** on the **Cisco DRF Local Service** on the publisher then continue with the subscribers and select **Restart** on the **Cisco DRF Local Service**.

The IPSEC.pem certificate in the publisher must be valid and must be present in all subscribers as IPSEC truststores. The subscribers IPSEC.pem certificate not be present in the publisher as IPSEC truststore in a standard deployment. In order to verify the validity compare the serial numbers in the IPSEC.pem certificate from the PUB with the IPSEC-trust in the SUBs. They must match.

CAPF Certificate

Warning: Ensure you have identified if your Cluster is in Mixed-Mode before you proceed.

Refer to section **Identify if your cluster is in Mix-Mode or Non-secure Mode**.

1. Navigate to the **Cisco Unified CM Administration > System > Enterprise Parameters**. Check the section Security Parameters and verify if the Cluster Security Mode is set to 0 or 1. If the value if 0 then the cluster is in Non-Secure Mode. If it is 1 then the cluster is in mixed-mode and you need to update the CTL file prior to the restart of services. See Token and Tokenless links.
2. Navigate to each server in your cluster (in separate tabs of your web browser) begin with the publisher, then each subscriber. Navigate to **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Select the **CAPF pem** Certificate.Once open select **Regenerate** and wait until you see the Success pop-up then close pop-up or go back and select **Find/List**
3. Continue with subsequent subscribers; follow the same procedure in step 2 and complete on all subscribers in your cluster. If cluster is in Mixed-Mode ONLY and the CAPF has been regenerated – Update the CTL before you proceed further Token - Tokenless.If cluster is in Mixed Mode then the Call Manager service also need to be restarted prior to the restart of other services.
4. After all Nodes have regenerated the CAPF certificate, restart services.
   Navigate to publisher **Cisco Unified Serviceability**. **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.Begin with the publisher and select **Restart** on the **Cisco Certificate Authority Proxy Function Service** only where active.
5. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Begin with the publisher then continue with the subscribers, select **Restart** on **Cisco Trust Verification Service**. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.Begin with the publisher then continue with the subscribers, restart **Cisco TFTP Service** only where active.
6. Reboot all Phones: **Cisco Unified CM Administration > System > Enterprise Parameters**Select **Reset** then you see a pop-up with the statement **You are about to reset all devices in the system. This action cannot be undone. Continue?,**select **OK** and then select **Reset**.

The phones now reset. Monitor their actions via RTMT tool to ensure the reset was successful and that devices register back to CUCM. Wait for the phone registration to complete before you proceed to next certificate. This process of phones registration can take some time. Be advised, devices that had bad ITLs prior to regeneration process do not register back to the cluster until it is remove.

CallManager Certificate

Warning: Ensure you have identified if your Cluster is in Mixed-Mode before you proceed. Refer to section **Identify if your cluster is in Mix-Mode or Non-secure Mode**.

Warning: Do not regenerate CallManager.PEM and TVS.PEM certificates at the same time. This cause an unrecoverable mismatch to the installed ITL on endpoints which require the removal the ITL from ALL endpoints in the cluster. Finish the entire process for CallManager.PEM and once the phones are registered back, start the process for the TVS.PEM.

1. Navigate to the **Cisco Unified CM Administration > System > Enterprise Parameters**: Check the section Security Parameters and verify if the Cluster Security Mode is set to 0 or 1. If the value if 0 then the cluster is in Non-Secure Mode. If it is 1 then the cluster is in mixed-mode and you need to update the CTL file prior to the restart of services. See Token and Tokenless links.
2. Navigate to each server in your cluster (in separate tabs of your web browser) begin with the publisher, then each subscriber. Navigate to **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Select the CallManager pem Certificate.Once open select **Regenerate** and wait until you see the Success pop-up then close pop-up or go back and select **Find/List**.
3. Continue with subsequent subscribers; follow the same procedure in step 2 and complete on all subscribers in your cluster. If cluster is in Mixed-Mode ONLY and the CallManager certificate has been regenerated – Update the CTL before you proceed further Token - Tokenless
4. Log into Publisher Cisco Unified Serviceability: Navigate to **Cisco Unified Serviceability > Tools > Control Center - Feature Services**.Begin with the publisher then continue with the subscribers, restart **Cisco CallManager Service** where active.
5. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Feature Services** Begin with the Publisher then continue with the subscribers, restart **Cisco CTIManager Service** only where active.
6. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Network Services**. Begin with the Publisher then continue with the subscribers, restart **Cisco Trust Verification Service**.
7. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Feature Services**. Begin with the Publisher then continue with the subscribers, restart **Cisco TFTP Service** only where active.
8. Reboot all Phones: **Cisco Unified CM Administration > System > Enterprise Parameters**Select **Reset** then you see a pop-up with the statement **You are about to reset all devices in the system. This action cannot be undone. Continue?,**select **OK** and then select **Reset**

The phones now reset. Monitor their actions via RTMT tool to ensure the reset was successful and that devices register back to CUCM. Wait for the phone registration to complete before you proceed to next certificate. This process of phones registration can take some time. Be advised, devices that had bad ITLs prior to regeneration process do not register back to the cluster until ITL is remove.

TVS Certificate

> **Warning**: Do not regenerate CallManager.PEM and TVS.PEM certificates at the same time. This cause an unrecoverable mismatch to the installed ITL on endpoints which require the removal the ITL from ALL endpoints in the cluster.

> **Note**: TVS authenticates certificates on behalf of Call Manager. Regenerate this certificate last.

Navigate to each server in your cluster (in separate tabs of your web browser) begin with the publisher, then each subscriber. Navigate to **Cisco Unified OS Administration > Security >

Certificate Management > Find:

- Select the **TVS pem** Certificate.
- Once open select **Regenerate** and wait until you see the Success pop-up then close pop-up or go back and select **Find/List**.

1. Continue with subsequent subscribers; follow the same procedure in step 1 and complete on all subscribers in your cluster. After all Nodes have regenerated the TVS certificate, restart the services: Log into Publisher **Cisco Unified Serviceability**. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Network Services**.On the publisher select **Restart** on **Cisco Trust Verification Service**.Once the service restart completes, continue with the subscribers and restart the **Cisco Trust Verification Service**.
2. Begin with the Publisher then continue with the subscribers, restart **Cisco TFTP Service** only where active.
3. Reboot all Phones: **Cisco Unified CM Administration > System > Enterprise Parameters**.Select **Reset** then you see a pop-up with the statement **You are about to reset all devices in the system. This action cannot be undone. Continue?,**select **OK** and then select **Reset**.

The phones now reset. Monitor their actions via RTMT tool to ensure the reset was successful and that devices register back to CUCM. Wait for the phone registration to complete before you proceed to next certificate. This process of phones registration can take some time. Be advised, devices that had bad ITLs prior to regeneration process do not register back to the cluster until ITL is remove.

ITLRecovery Certificate

> **Note**: The ITLRecovery Certificate is used when devices lose their trusted status. The certificate appears in both the ITL and CTL (when CTL provider is active).
> If devices lose their trust status, you can use the command **utils itl reset localkey** for non-secure clusters and the command **utils ctl reset localkey** for mix-mode clusters. Read the security guide for your Call Manager version to become familiar with how the ITLRecovery certificate is used and the process required to recover trusted status.
> If the cluster has been upgraded to a version that supports a key length of 2048 and the clusters server certificates have been regenerated to 2048 and the ITLRecovery has not been regenerated and is currently 1024 key length, the ITL recovery command fails and the ITLRecovery method is not used.

1. Navigate to each server in your cluster (in separate tabs of your web browser) begin with the publisher, then each subscriber. Navigate to **Cisco Unified OS Administration > Security > Certificate Management > Find**:
   Select the **ITLRecovery pem** Certificate.Once open select **Regenerate** and wait until you see the Success pop-up then close pop-up or go back and select **Find/List**.
2. Continue with subsequent Subscribers; follow the same procedure in step 2 and complete on all subscribers in your cluster.
3. After all Nodes have regenerated the ITLRecovery certificate, services need to be restarted in the order as follows: If you are in Mixed Mode – Update the CTL before you proceed Token - Tokenless.Log into Publisher **Cisco Unified Serviceability**. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Network Services**.On the publisher select **Restart** on **Cisco Trust Verification Service**. Once the service restart

completes, continue with the subscribers and restart the **Cisco Trust Verification Service**.

4. Begin with the Publisher then continue with the subscribers, restart **Cisco TFTP Service** only where active.
5. Reboot all Phones: **Cisco Unified CM Administration > System > Enterprise Parameters**Select **Reset** then you see a pop-up with the statement **You are about to reset all devices in the system. This action cannot be undone. Continue?,**select **OK** and then select **Reset**.
6. Phones now upload the new ITL/CTL while they reset.

Delete Expired Trust Certificates

> **Note**: Identify the trust certificates that need to be deleted, no longer required, or have expired. Do not delete the five base certificates which include the CallManager.pem, tomcat.pem, ipsec.pem, CAPF.pem and TVS.pem. Trust certificates can be deleted when appropriate. The next service that restarts is designed to clear information of legacy certificates within those services.

1. Navigate to **Cisco Unified Serviceability > Tools > Control Center - Network Services**. From the drop down select the CUCM Publisher.Select **Stop Certificate Change Notification**.Repeat for every Call Manager node in your cluster.If you have an IMP Server: From the drop down menu select your IMP servers one at a time and Select **Stop Platform Administration Web Services and Cisco Intercluster Sync Agent**.
2. Navigate to **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Find the expired trust certificates. (For versions 10.X and higher you can filter by Expiration. For versions lower than 10.0 you need to identify the specific certificates manually or via the RTMT alerts if received.)The same trust certificate can appear in multiple nodes. It must be deleted individually from each node.Select the trust certificate to be deleted (dependent on your version you either get a pop-up or you navigated to the certificate on same page) Select **Delete**. (You get a pop-up that begins with "you are about to permanently delete this certificate".*)*Select **OK**.
3. Repeat the process for every trust certificate to be deleted.
4. Upon Completion, services need to be restarted that are directly related to the certificates deleted. You do not need to reboot phones in this section. Call Manager and CAPF be endpoint impacting. Tomcat-trust: restart Tomcat Service via command line (See Tomcat Section)CAPF-trust: restart Cisco Certificate Authority Proxy Function (see CAPF Section) Do not reboot endpoints.CallManager-trust: CallManager Service/CTIManager (See CallManager Section) Do not reboot endpoints. Impacts endpoints and causes restarts.IPSEC-trust: DRF Master/DRF Local (See IPSEC Section).TVS (Self-Signed) does not have trust certificates.
5. Restart Services Previously Stopped in Step 1.

Verification

Verification procedure are not available for this configuration.

Troubleshoot

Troubleshoot procedures are not available for this configuration.