Regenerate CUCM IM/P Service Self-Signed Certificates

Contents

Introduction

This document describes a recommended step-by-step procedure on how to regenerate certificates in CUCM IM/P 8.x and later.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the IM & Presence (IM/P) Service certificates.

Components Used

The information in this document is based on the IM/P release 8.x and later.

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

Certificate Store Utilization

Cisco Unified Presence (CUP) Certificate

Used for secure SIP connections for SIP Federation, Microsoft Remote Call Control for Lync/OCS/LCS, secure connection between Cisco Unified Certificate Manager (CUCM) and IM/P, and so on.

Cisco Unified Presence - Extensible Messaging and Presence Protocol (CUP-XMPP) Certificate

Used to validate secure connections for XMPP clients when an XMPP session is created.

Cisco Unified Presence - Extensible Messaging and Presence Protocol - Server to Server (CUP-XMPP-S2S) Certificate

Used to validate secure connections for XMPP interdomain federations with an externally federated XMPP system.

IP Security (IPSec) Certificate

Used to:
• Validate secure connection for Disaster Recovery System (DRS)/Disaster Recovery Framework (DRF)
• Validate secure connection for IPsec tunnels to Cisco Unified Communications Manager (CUCM) and IM/P nodes in the cluster

Tomcat Certificate

Used to:

• Validate various web access such as access to service pages from other nodes in the cluster and Jabber Access.
• Validate secure connection for SAML Single Sign-On (SSO).

• Validate secure connection for Intercluster Peer.

⚠ **Caution**: If you use the SSO feature on your Unified Communication servers and the Cisco Tomcat certificates are regenerated, the SSO must be reconfigured with the new certificates. The link to configure SSO on CUCM and ADFS 2.0 is: https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html.

Note: The link to CUCM Certificate Regeneration/Renewal Process is: https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html.

Certificate Regeneration Process

CUP Certificate

Step 1. Open a Graphical User Interface (GUI) for each server in your cluster. Start with the IM/P publisher, then open a GUI for each IM/P subscriber server in turn and navigate to Cisco Unified OS Administration > Security > Certificate Management.

Step 2. Begin with the publisher GUI, and choose Find to show all the certificates. Choose the cup.pem certificate. Once open, choose Regenerate and wait until you see success before the pop-up is closed.

Step 3. Continue with subsequent subscribers, refer to the same procedure as in Step 2. and complete all subscribers in your cluster.

Step 4. After the CUP certificate has been regenerated on all nodes, the services must be restarted.

Note: If the Presence Redundancy Group configuration has Enable High Availability checked, Uncheck it before the services are restarted. Presence Redundancy Group configuration can be accessed at CUCM Pub Administration > System > Presence Redundancy Group. A restart of the services causes a temporary outage of IM/P and must be done outside production hours.

Restart the services in this order:

• Log into the Cisco Unified Serviceability of the Publisher:

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco SIP Proxy service.

c. Once the service restart completes, continue with the subscribers and Restart Cisco SIP Proxy service.

d. Begin with the publisher and then continue with the subscribers. Restart Cisco SIP Proxy service (also, from Cisco Unified Serviceability > Tools > Control Center - Feature Services).

• Log into the Cisco Unified Serviceability of the Publisher:

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco Presence Engine service.

c. Once the service restart completes, continue with Restart of Cisco Presence EngineService on the subscribers.

Note: If configured for SIP Federation, Restart Cisco XCP SIP Federation Connection Manager service (located at Cisco Unified Serviceability > Tools > Control Center - Feature Services). Begin with the publisher and then continue with the subscribers.

CUP-XMPP Certificate

Note: Since Jabber utilizes the CUCM and IM/P Tomcat and the CUP-XMPP server certificates to validate the connections for Tomcat and the CUP-XMPP services, these CUCM and IM/P certificates are in most cases CA-signed. Suppose the Jabber device does not have the root and an intermediate certificate that is part of the CUP-XMPP certificate installed in its certificate trust store, in that case, the Jabber client displays a security warning popup for the untrusted certificate. If not already installed in the certificate of the Jabber device trust store, the root and any intermediate certificate must be pushed to the Jabber device through group policy, MDM, email, and so on, which depends on

---

the Jabber client.

Note: If the CUP-XMMP certificate is self-signed, the Jabber client displays a security warning popup for the untrusted certificate if the CUP-XMPP certificate is not installed in the trust store of the Jabber device certificate. If it is not already installed, the self-signed CUP-XMPP certificate must be pushed to the Jabber device through group policy, MDM, email, and so on, which depends on the Jabber client.

Step 1. Open a GUI for each server in your cluster. Start with the IM/P publisher, then open a GUI for each IM/P subscriber server in turn and navigate to **Cisco Unified OS Administration > Security > Certificate Management.**

Step 2. Begin with the publisher GUI, and choose Find to show all the certificates. From the type column for the cup-xmpp.pem certificate, determine whether it is self-signed or CA-signed. If the cup-xmpp.pem certificate is a third-party signed (type CA-signed) distribution multi-SAN, review this link when you generate a multi-SAN CUP-XMPP CSR and submit to CA for CA-signed CUP-XMPP certificate; Unified Communication Cluster Setup with CA-Signed Multi-Server Subject Alternate Name Configuration Example.

If the cup-xmpp.pem certificate is a third-party signed (type CA-signed) distribution single node (distribution name equals the common name for the certificate), review this link when you generate a single-node CUP-XMPP CSR and submit to CA for CA-signed CUP-XMPP certificate; Jabber Complete How-To Guide for Certificate Validation. If the cup-xmpp.pem certificate is self-signed, continue to Step 3.

Step 3. Choose Find in order to show all the certificates and then choose the cup-xmpp.pem certificate. Once open, choose Regenerate and wait until you see success before the pop-up is closed.

Step 4. Continue with subsequent subscribers; refer to the same procedure in Step 2, and complete it for all subscribers in your cluster.

Step 5. After the CUP-XMPP certificate has been regenerated on all nodes, the Cisco XCP Router service must be restarted on the IM/P nodes.

Note: If the Presence Redundancy Group Configuration has Enable High Availability checked, Uncheck this before the service is restarted. Presence Redundancy Group Configuration can be accessed at CUCM Pub Administration > System > Presence Redundancy Group. A restart of the service causes a temporary outage of IM/P and must be done outside production hours.

• Log into the Cisco Unified Serviceability of the Publisher:

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart the Cisco XCP Router service.

c. Once the service restart completes, continue with Restart Cisco XCP Router service on the subscribers.

CUP-XMPP-S2S Certificate

Step 1. Open a GUI for each server in your cluster. Start with the IM/P publisher, then open a GUI to each IM/P subscriber server in turn and navigate to Cisco Unified OS Administration > Security > Certificate Management.

Step 2. Begin with the publisher GUI, choose Find to show all the certificates, and choose the cup-xmpp-s2s.pem certificate. Once open, choose Regenerate and wait until you see success before the pop-up is closed.

Step 3. Continue with subsequent subscribers and refer to the same procedure in Step 2, and complete for all subscribers in your cluster.

Step 4. After the CUP-XMPP-S2S certificate has been regenerated on all nodes, the services must be restarted in the order mentioned.

Note: If the Presence Redundancy Group Configuration has Enable High Availability checked,Uncheck this before these services are restarted. Presence Redundancy Group Configuration can be accessed on CUCM Pub Administration > System > Presence Redundancy Group. A restart of the services causes a temporary outage of IM/P and must be done outside production hours.

• Log into the Cisco Unified Serviceability of the Publisher:

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.
b. Restart the Cisco XCP Router service.
c. Once the service restart completes, continue with Restart of the Cisco XCP Router service on the subscribers.

• Log into the Cisco Unified Serviceability of the Publisher:

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart the Cisco XCP XMPP Federation Connection Manager service.

c. Once the service restart completes, continue with Restart of the Cisco XCP XMPP Federation Connection Manager service on the subscribers.

IPSec Certificate

Note: The ipsec.pem certificate in the CUCM publisher must be valid and present in all subscribers (CUCM and IM/P nodes) in the IPSec trust store. The ipsec.pem certificate of the subscriber is not present in the publisher as the IPSec trust store in a standard deployment. In order to verify the validity, compare the serial numbers in the ipsec.pem certificate from the CUCM-PUB with the IPSec-trust in the subscribers. They must match.

Note: The DRS uses a Secure Socket Layer (SSL) based communication between the Source Agent and the Local Agent for authentication and encryption of data between the CUCM cluster nodes (CUCM and IM/P nodes). DRS makes use of the IPSec certificates for its Public/Private Key encryption. Be aware that if you delete the IPSEC trust store (hostname.pem) file from the Certificate Management page, then DRS does 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 CUCM Security Guides.

Step 1. Open a GUI for each server in your cluster. Start with the IM/P publisher, then open a GUI to each IM/P subscriber server in turn and navigate to Cisco Unified OS Administration > Security > Certificate Management.

Step 2. Begin with the publisher GUI, and choose Find to show all the certificates.Choose the ipsec.pem certificate. Once open, choose Regenerate and wait until you see success before the pop-up is closed.

Step 3. Continue with subsequent subscribers and refer to the same procedure in Step 2, and complete for all

subscribers in your cluster.

Step 4. After all the nodes have regenerated the IPSEC certificate, then Restart these services. Navigate to the Cisco Unified Serviceability of the Publisher; Cisco Unified Serviceability > Tools > Control Center - Network Services.
a. Choose Restart on the Cisco DRF primary service.
b. Once the service restart completes, choose Restart of Cisco DRF Local service on the publisher then continue with Restart of the Cisco DRF Local service on each subscriber.

Tomcat Certificate

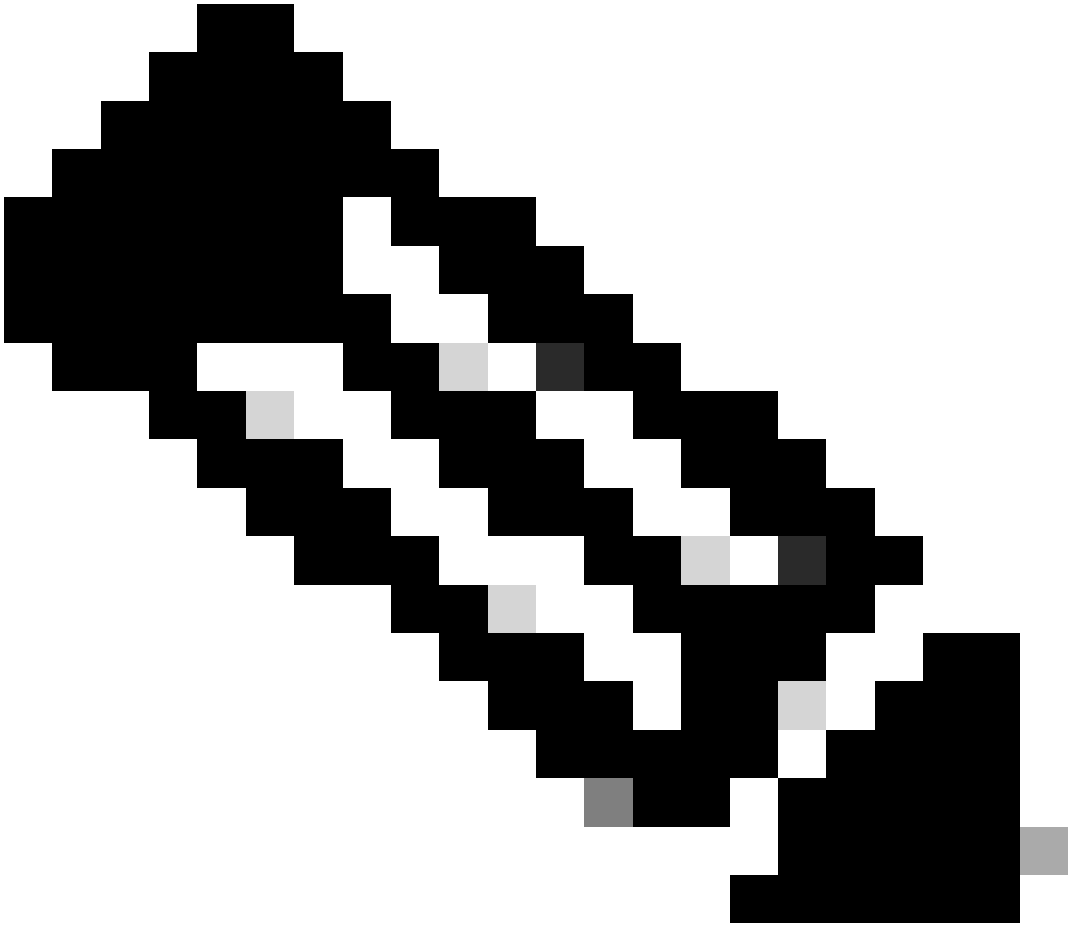
Note: Since Jabber utilizes the CUCM Tomcat and IM/P Tomcat and CUP-XMPP server certificates to validate the connections for Tomcat and CUP-XMPP services, these CUCM and IM/P certificates are in most cases CA-signed. Suppose the Jabber device does not have the root and any intermediate certificate that is part of the Tomcat certificate installed in its certificate trust store. In that case, the Jabber client displays a security warning popup for the untrusted certificate. If not already installed in the certificate trust store of the Jabber device, the root, and any intermediate certificate must be pushed to the Jabber device through group policy, MDM, email, and so on, which depends on the Jabber client.

Note: If the Tomcat certificate is self-signed, the Jabber client displays a security warning popup for the untrusted certificate, if the Tomcat certificate is not installed in the certificate trust store of the Jabber device. If not already installed in the certificate trust store of the Jabber device, the self-signed CUP-XMPP certificate must be pushed to the Jabber device through group policy, MDM, email, and so on, which depends on the Jabber client.

Step 1. Open a GUI for each server in your cluster. Start with the IM/P publisher, then open a GUI for each IM/P subscriber server in turn and navigate to Cisco Unified OS Administration > Security > Certificate Management.

Step 2. Begin with the publisher GUI, and choose Find to show all the certificates.
• From the Type column for the tomcat.pem certificate, determine whether it is self-signed or CA-signed.

• If the tomcat.pem certificate is a third-party signed (type CA-signed) distribution multi-SAN, review this link on how to generate a multi-SAN Tomcat CSR and submit to CA for a CA-signed Tomcat certificate, Unified Communication Cluster Setup with CA-Signed Multi-Server Subject Alternate Name Configuration Example



Note: The multi-SAN Tomcat CSR is generated on the CUCM publisher and is distributed to all CUCM and IM/P nodes in the cluster.

• If the tomcat.pem certificate is a third-party signed (type CA-signed) distribution single node (distribution name equals the Common Name for the certificate), review this link to generate a single-node CUP-XMPP CSR, and submit it to CA for CA-signed CUP-XMPP certificate, Jabber Complete How-To Guide for Certificate Validation

• If the tomcat.pem certificate is self-signed, continue to Step 3

Step 3. Choose Find in order to show all the certificates:
• Choose the tomcat.pem certificate.
• Once open, choose Regenerate and wait until you see the success pop-up before the pop-up is closed.

Step 4. Continue with each subsequent subscriber, refer to the procedure in Step 2, and complete all subscribers in your cluster.

Step 5. After all nodes have regenerated the Tomcat certificate, Restart the Tomcat service on all the nodes. Begin with the publisher, followed by the subscribers.
• In order to Restart Tomcat service, you must open a CLI session for each node and run the command until

the service restarts Cisco Tomcat, as shown in the image:

Delete Expired Trust Certificates

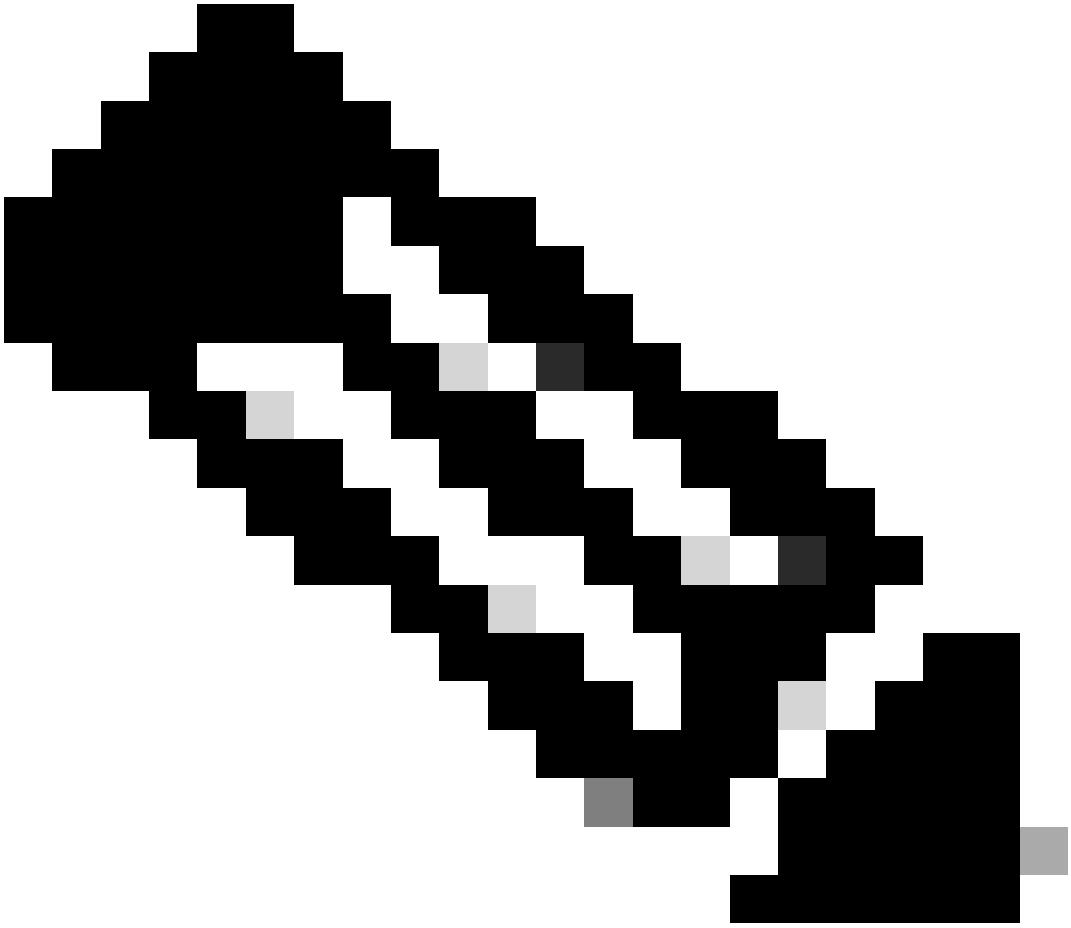
Note: Trust certificates (that end in -trust) can be deleted when appropriate. Trust certificates that can be deleted are those that are no longer required, have expired, or are obsolete. Do not delete the five identity certificates: the cup.pem , cup-xmpp.pem , cup-xmpp-s2s.pem , ipsec.pem , and tomcat.pem certificates. The service restarts, as shown, are designed to clear any in-memory information of these legacy certificates within those services.

Note: If the Presence Redundancy Group Configuration has Enable High Availability checked, Uncheck this before a service is Stopped/Started or Restarted. Presence Redundancy Group Configuration can be accessed at CUCM Pub Administration > System > Presence Redundancy Group. A restart of some of the services, as shown, causes a temporary outage of IM/P and must be done outside production hours.

Step 1. Navigate to Cisco Unified Serviceability > Tools > Control Center - Network Services:

• From the drop-down menu, choose your IM/P publisher, choose Stop from Cisco Certificate Expiry Monitor, followed by Stop in Cisco Intercluster Sync Agent.

• Repeat Stop for these services for each IM/P node in your cluster.



Note: If the Tomcat-trust certificate must be deleted, navigate to Cisco Unified Serviceability > Tools > Control Center - Network Services of the CUCM publisher.

• From the drop-down, choose the CUCM publisher.
• Choose Stop from Cisco Certificate Expiry Monitor, followed by Stop in Cisco Certificate Change Notification.
• Repeat for every CUCM node in your cluster.

Step 2. Navigate to Cisco Unified OS Administration > Security > Certificate Management > Find.

• Find the expired trust certificates (for versions 10.x and later, you can filter by Expiration. From versions earlier than 10.0 you must 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.
• Choose the trust certificate to be deleted (based on the version, you either get a pop-up or you are navigated to the certificate on the same page).

• Choose Delete (you get a pop-up that begins with "you are about to permanently delete this certificate...").
• Click OK.

Step 3. Repeat the process for every trust certificate to be deleted.

Step 4. Upon completion, services must be restarted that are directly related to the certificates deleted.

• CUP-trust: Cisco SIP Proxy, Cisco Presence Engine, and if configured for SIP Federation, Cisco XCP SIP Federation Connection Manager (see CUP Certificate section)
• CUP-XMPP-trust: Cisco XCP Router (see CUP-XMPP certificate section)
• CUP-XMPP-S2S-trust: Cisco XCP Router and Cisco XCP XMPP Federation Connection Manager
• IPSec-trust: DRF Source/DRF Local (see IPSec certificate section)
• Tomcat-trust: Restart Tomcat Service via the command line (see Tomcat certificate section)

Step 5. Restart services stopped in Step 1.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.