Implement Reuse of Multi-SAN Tomcat Certificate for CallManager

Contents

Introduction

This document describes a step by step process on how to reuse the Multi-SAN Tomcat certificate for CallManager on CUCM.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager (CUCM)
- CUCM Certificates
- Identity Trust List (ITL)

Components Used

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

- CUCM release 15 SU1

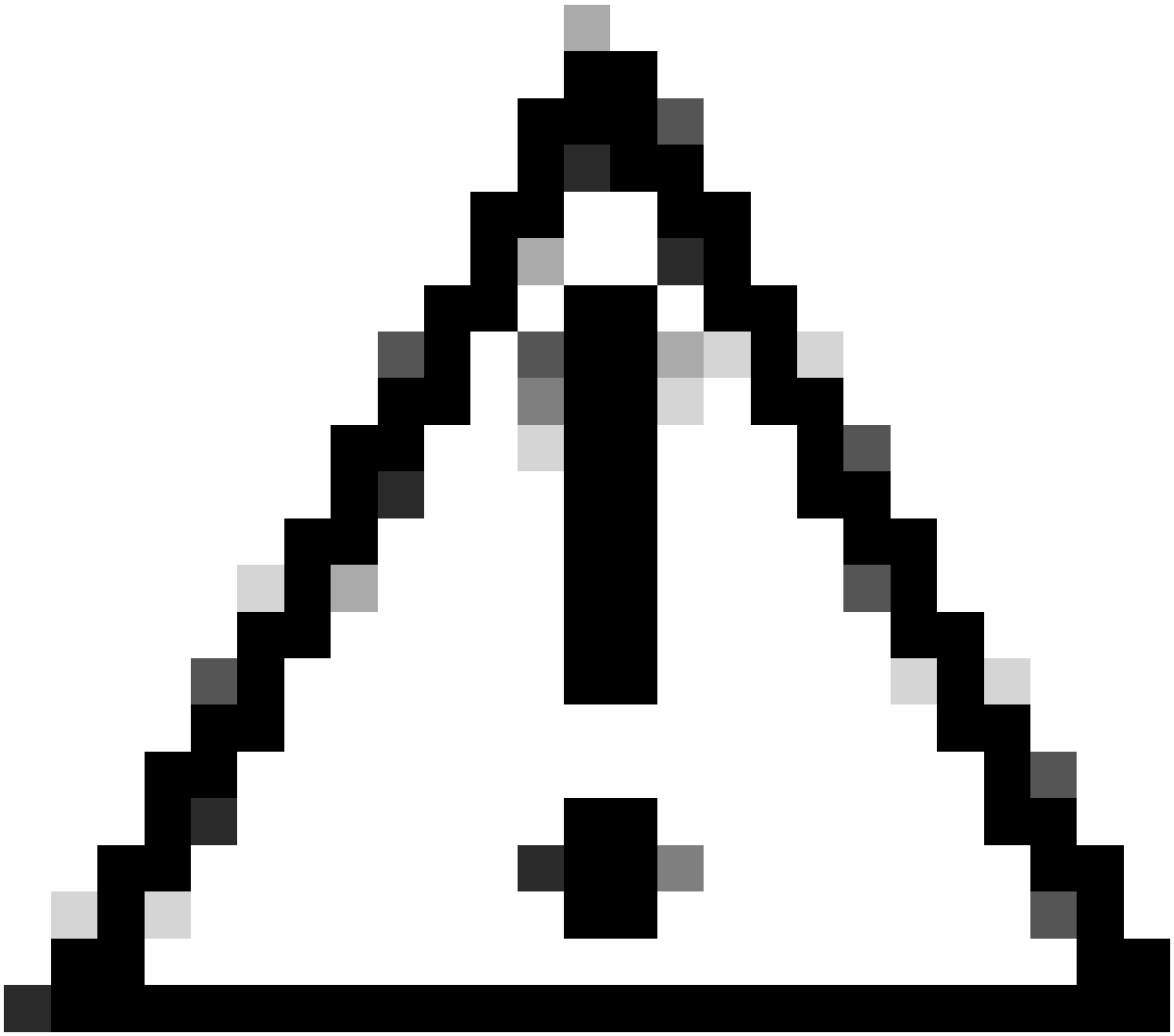
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Earlier versions of CUCM used different certificates for each service for the complete cluster which increased the number of certificates and cost. This includes Cisco Tomcat and Cisco CallManager which are critical services running on CUCM which also have respective Identity certificates.

Starting with CUCM version 14, a new feature was added to reuse the Multi-SAN Tomcat certificate for CallManager service.

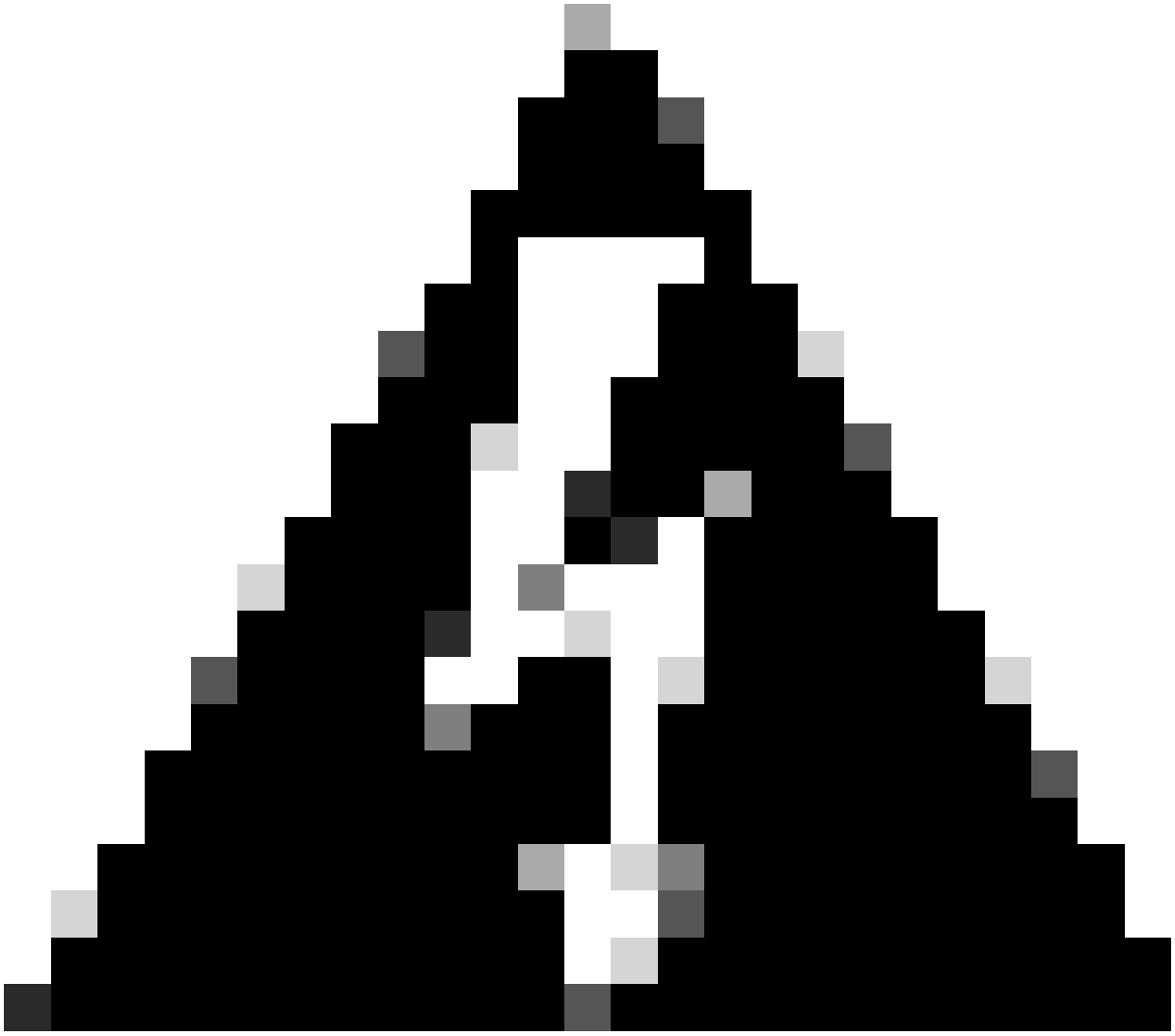
The benefit of using this feature is that you can obtain one certificate from the CA and use it across several applications. This ensures cost optimization and a reduction in management and reduces the size of the ITL file, thereby reducing overhead.



Caution: Before proceeding further with reuse configuration, make sure Tomcat Certificate is Multi-Server SAN certificate. Tomcat Multi-SAN certificate can be Self-Signed or CA-signed.

Configure

Reuse Tomcat Certificate for CallManager



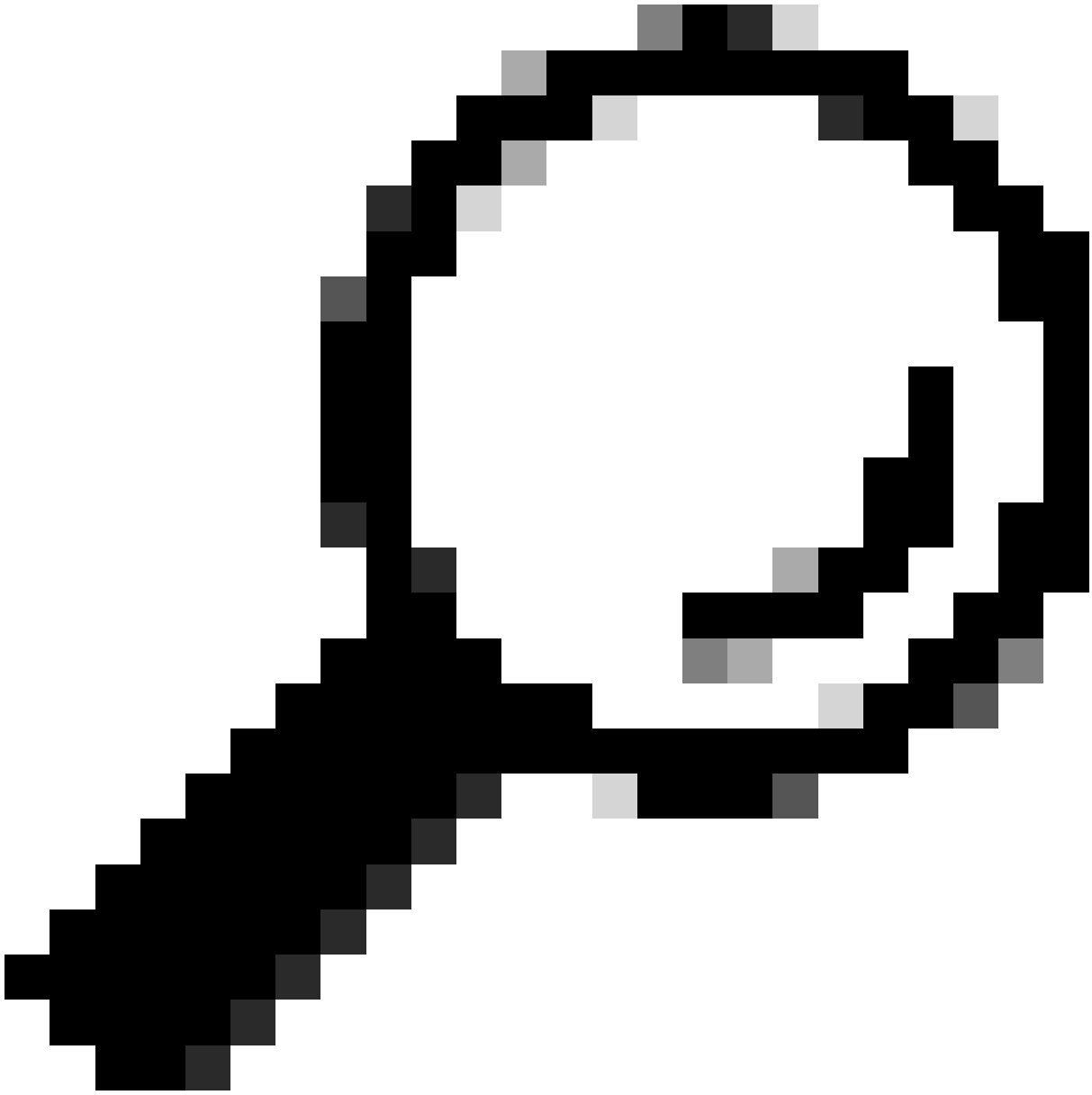
Warning: Ensure you have identified if your Cluster is in Mixed-Mode or Non-Secure mode before you proceed.

Step 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.

Step 2. Navigate to your **CUCM publisher**, and then to **Cisco Unified OS Administration > Security > Certificate Management**.

Step 3. Upload **Multi-SAN Tomcat CA Certificate Chain** to CallManager Trust store.



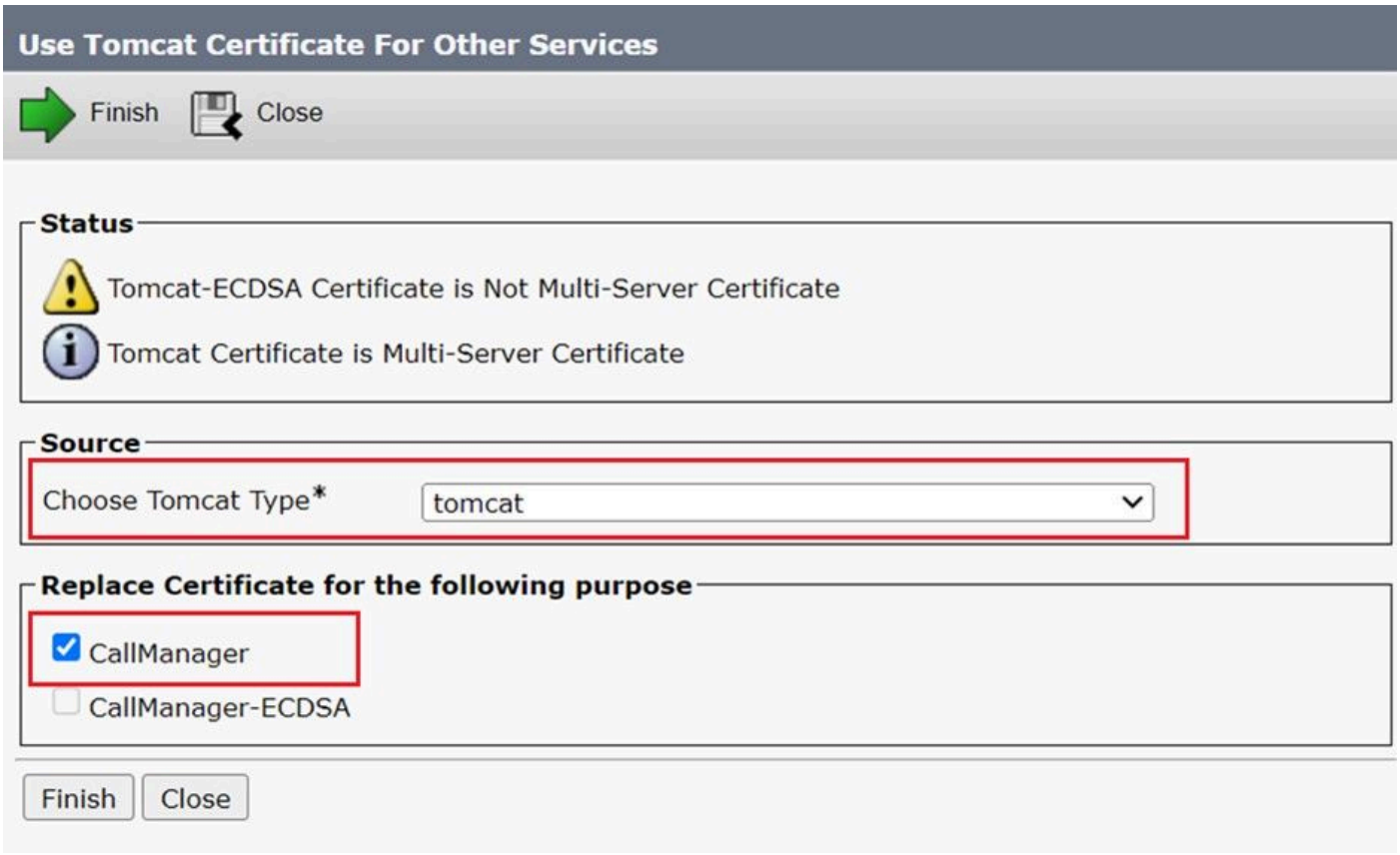
Tip: If you are using Self-Signed Multi-Server SAN certificate for Tomcat, you can skip this step.

Before reusing the certificates, ensure that you manually upload the CA certificate chain (that signed the tomcat identity certificate) to the CallManager trust store.

Restart these services when you upload the tomcat certificate chain to the CallManager trust.

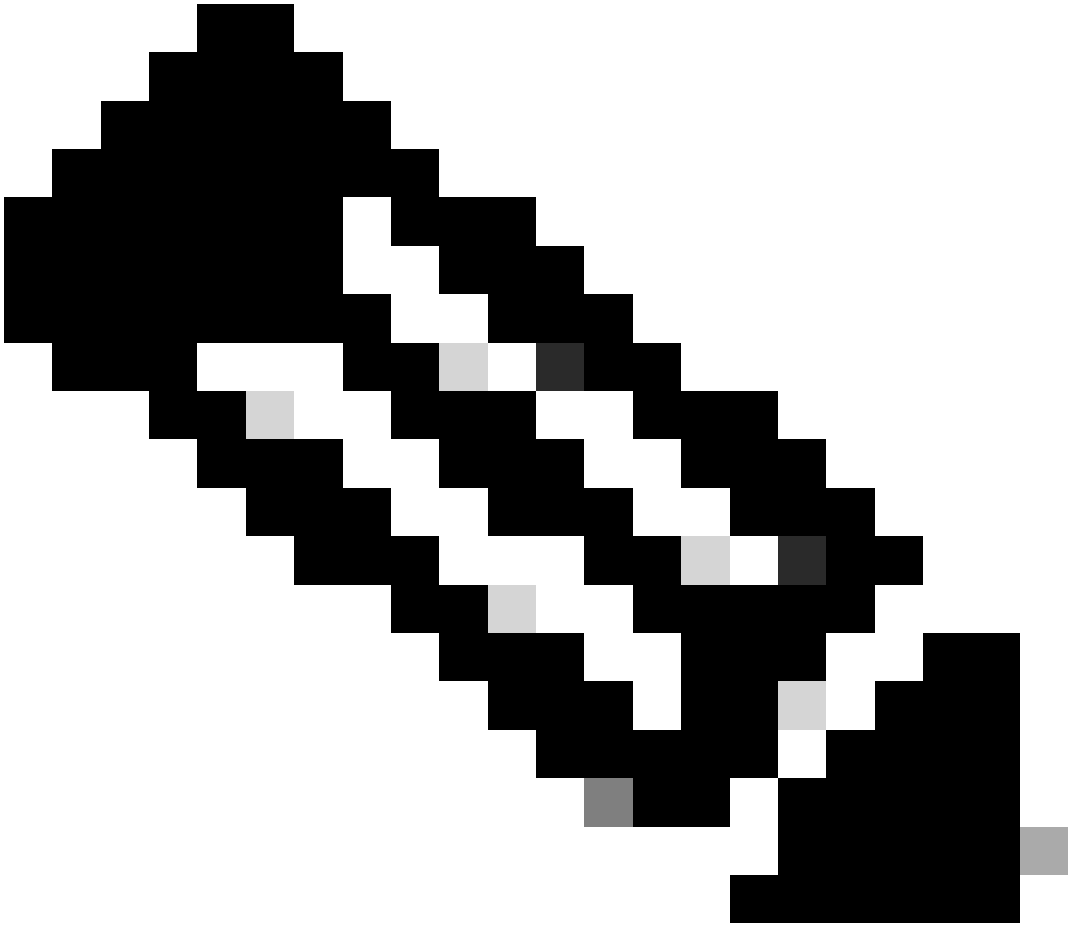
- CallManager: Cisco HAProxy Service
- CallManager-ECDSA: Cisco CallManager Service and Cisco HAProxy Service

Step 4. Click **Reuse Certificate**. The Use Tomcat Certificates For Other Services page appears.



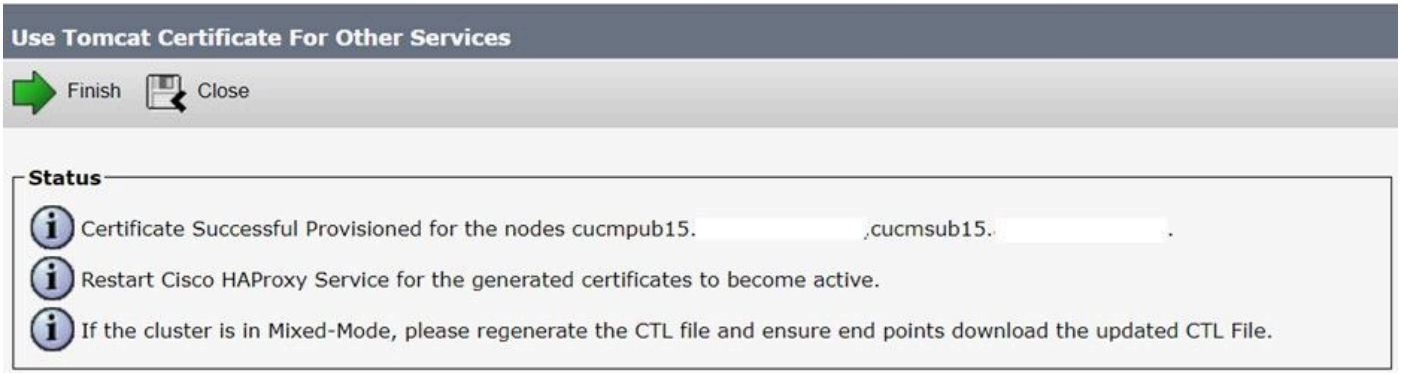
Step 5. From the **Tomcat type** drop-down list, choose either **Tomcat** or **Tomcat-ECDSA**.

Step 6. From the **Replace Certificate for the following purpose** pane, check either the **CallManager** or **CallManager-ECDSA** check box based on the selected certificate in earlier step.



Note: If you choose Tomcat as the certificate type, CallManager is enabled as the replacement. If you choose tomcat-ECDSA as the certificate type, CallManager-ECDSA is enabled as the replacement.

Step 7. Click **Finish** to replace the CallManager certificate with the tomcat multi-server SAN certificate.



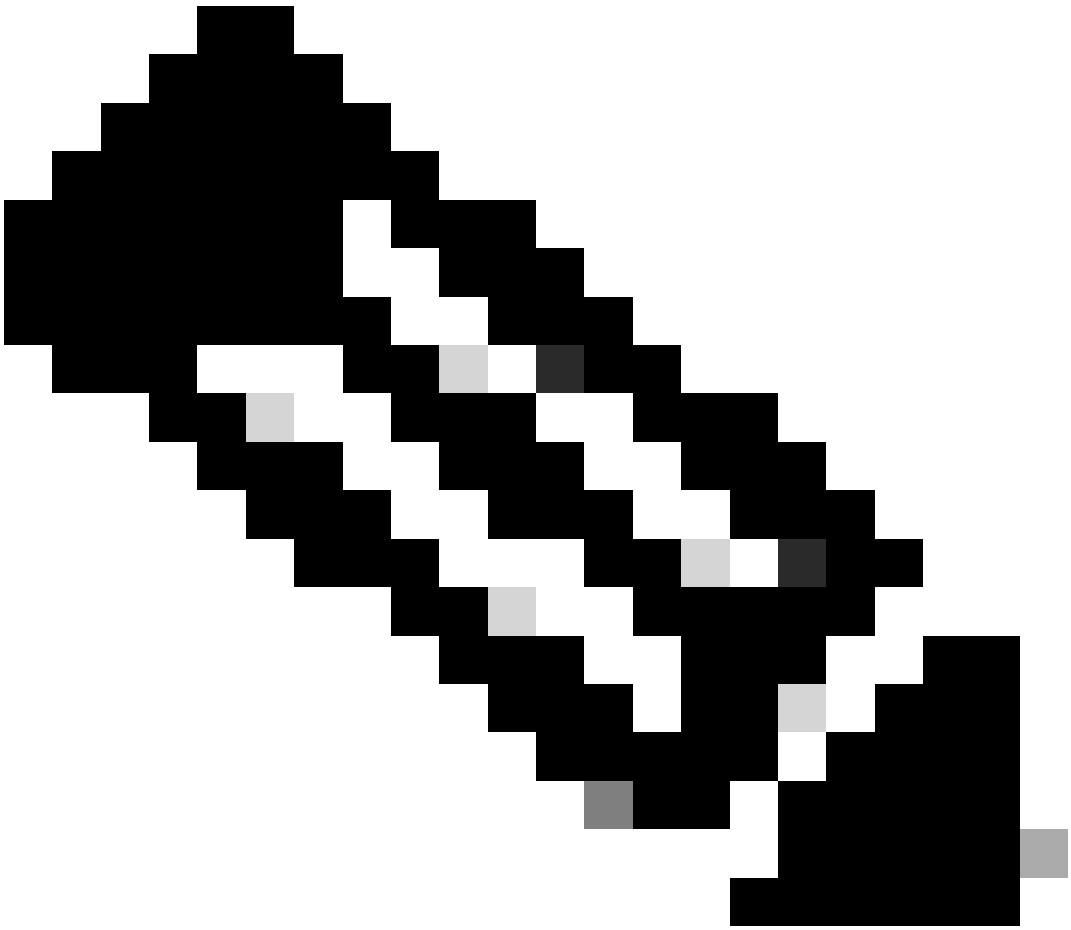
Step 8. Restart the **Cisco HAProxy** service on all the nodes of the cluster by executing **utils service restart Cisco HAProxy** command via CLI.

```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin:
```

Step 9. If the cluster is in Mixed Mode, update the CTL file by running command **utils ctl update CTLFile** via CLI of CUCM Publisher and proceed to reset the phones to get the new CTL File.

Verify



Note: The CallManager certificate is not displayed on GUI when you reuse the certificate.

You can run the command from the CLI to confirm that CallManager reuses the Tomcat certificate.

- **show cert list own**