Setup Unified Communication Cluster

Contents

Introduction

This document describes how to set up a Unified Communication Cluster with the use Certificate Authority (CA)-Signed Multi-Server SAN certificates.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Unified Communications Manager (CUCM)
- CUCM IM and Presence Version 10.5

Before you attempt this configuration, ensure these services are up and functional:

- Cisco Platform Administrative Web Service
- Cisco Tomcat Service

In order to verify these services on a web interface, navigate to **Cisco Unified Serviceability Page Services > Network Service > Select a server**. In order to verify them on the CLI, enter the **utils service list** command.

If SSO is enabled in the CUCM cluster, it is required to be disabled and enabled again.

Components Used

This document is not restricted to specific software and hardware versions.

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

In CUCM Version 10.5 and later, this trust-store Certificate Signing Request (CSR) can include Subject Alternate Name (SAN) and alternate domains.

1. Tomcat - CUCM and IM&P
2. Cisco CallManager - Only CUCM
3. Cisco Unified Presence-Extensible Messaging and Presence Protocol (CUP-XMPP) - Only IM&P
4. CUP-XMPP Server-to-Server (S2S) - Only IM&P

It is simpler to obtain a CA-signed certificate in this version. Only one CSR is required to be signed by CA rather than the requirement to obtain a CSR from each server node and then obtain a CA-signed certificate for each CSR and manage them individually.

Configure

Step 1.

Log into Publisher's Operating System (OS) Administration and navigate to **Security > Certificate Management > Generate CSR**.

Step 2.
Choose **Multi-Server SAN** in Distribution.

Generate Certificate Signing Request

🔒 Generate   💾 Close

Status

⚠ Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat ▾
Distribution*	cs-ccm-pub.\█████.com ▾
Common Name*	cs-ccm-pub.\█████.com
	Multi-server(SAN)

Subject Alternate Names (SANs)

Parent Domain	█████ com
Key Length*	2048 ▾
Hash Algorithm*	SHA256 ▾

Generate   Close

ⓘ *- indicates required item.

It auto-populates the SAN domains and the parent domain.

Verify all the nodes of your cluster are listed for Tomcat: all CUCM and IM&P nodes bs for CallManager: only CUCM nodes are been listed.

Generate Certificate Signing Request

🔐 Generate 💾 Close

Status

⚠ Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat
Distribution*	Multi-server(SAN)
Common Name*	cs-ccm-pub.▓▓▓▓.com-ms

Subject Alternate Names (SANs)

Auto-populated Domains

```
cs-ccm-pub.▓▓▓.com
cs-ccm-sub.▓▓▓.com
cs-imp.▓▓▓▓k.com
```

Parent Domain ▓▓▓▓ com

Other Domains

Browse_ No file selected.
Please import .TXT file only.
For more information please refer to the notes in the Help Section

➕ Add

Key Length*	2048
Hash Algorithm*	SHA256

Generate   Close

ⓘ *- indicates required item.

Step 3.

Click generate and once the CSR is generated, verify all the nodes listed in the CSR are also displayed in the Successful CSR exported list.

Generate Certificate Signing Request

🔐 Generate 💾 Close

Status

ⓘ Success: Certificate Signing Request Generated

ⓘ CSR export operation successful on the nodes [cs-ccm-sub.▓▓▓.com, cs-ccm-pub.▓▓▓.com, cs-imp.▓▓▓▓.com].

In Certificate Management, the SAN Request is generated:

Step 4.

Click **Download CSR** then choose the certificate purpose and Click **Download CSR**.

It is possible to use the local CA or an External CA like VeriSign in order to get the CSR (File downloaded in the previous step) signed.

This example shows configuration steps for a Microsoft Windows Server-based CA. If you use a different CA or an external CA go to Step 5.

Log into https://<windowsserveripaddress>/certsrv/
Choose **Request a Certificate > Advanced Certificate Request.**
Copy the content of the CSR file to the Base-64-encoded certificate request field and click **Submit**.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
   Request a certificate
   View the status of a pending certificate request
   Download a CA certificate, certificate chain, or CRL

Submit the CSR request as shown here.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):
```
-----BEGIN CERTIFICATE REQUEST-----
```

Additional Attributes:

Attributes:

[Submit >]

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 32.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with **this** web browser within 10 days to retrieve your certificate

Step 5.

✎ **Note**: Before you upload a Tomcat certificate, verify SSO is disabled. In case it is enabled, SSO must be disabled and re-enabled once all the Tomcat certificate regeneration process is finished.

With the certificate signed, upload the CA certificates as tomcat-trust. First the Root certificate and then the intermediate certificate if it exists.

Step 6.

Now upload the CUCM signed certificate as Tomcat and verify all the nodes of your cluster are listed in the "Certificate upload operation successful" as shown in the image:

Multi-Server SAN is listed in Certificate Management as shown in the image:
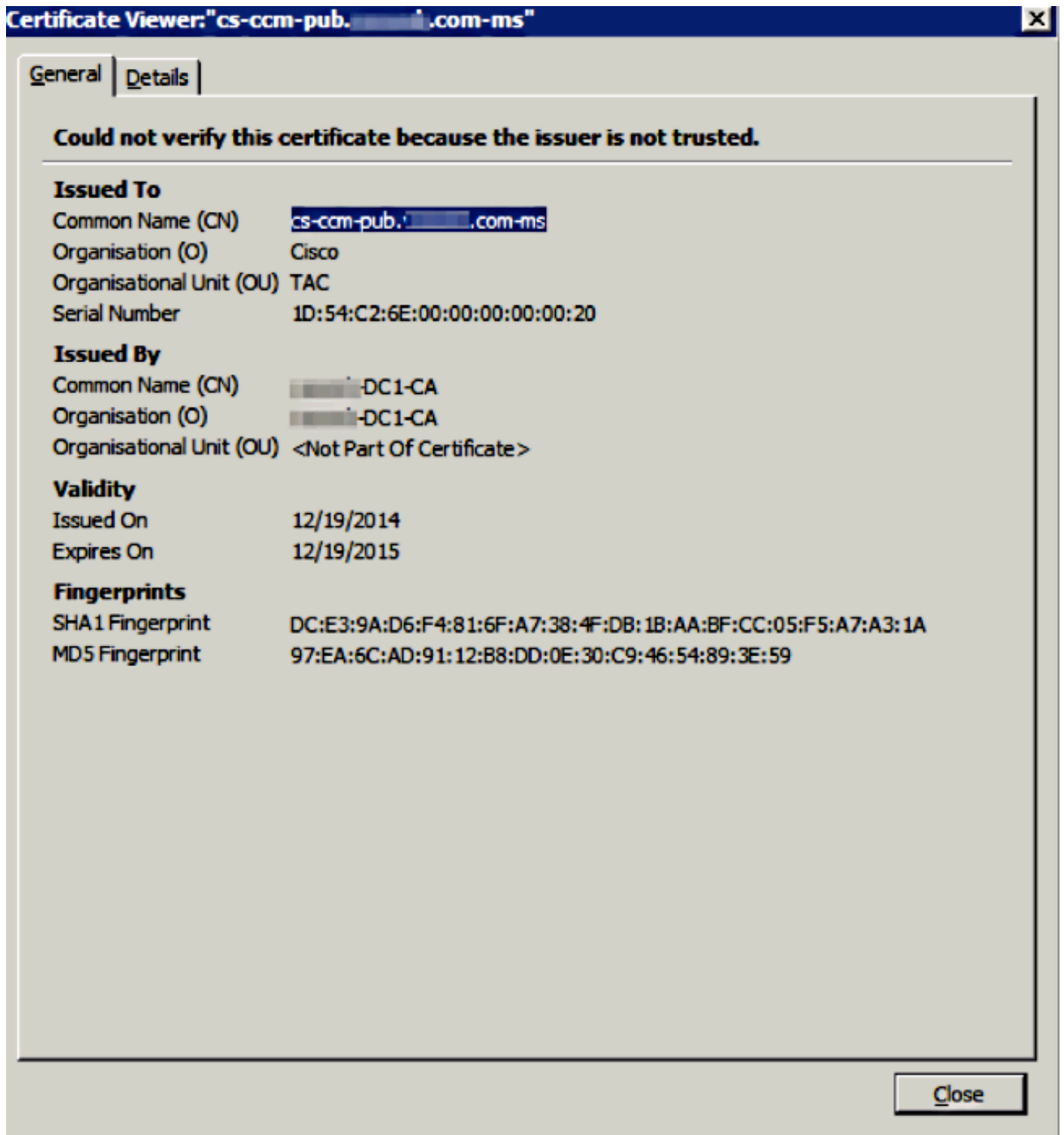

Step 7.

Restart the Tomcat service on all nodes in the SAN list (first Publisher and then subscribers) via CLI with the command: **utils service restart Cisco Tomcat**.

Verify

Log into http://<fqdnofccm>:8443/ccmadmin in order to ensure that the new certificate is used.

CallManager Multi-Server SAN Certificate

A similar procedure can be followed for the CallManager certificate. In this case, the auto-populated domains are only CallManager nodes. If the Cisco CallManager service is not running, you can choose to keep it in the SAN list or remove it.

⚠️ **Warning**: This process impacts phone registration and call processing. Make sure to shedule a maintenance window for any work with CUCM/TVS/ITL/CAPF certificates.

Before the CA-signed SAN certificate for CUCM, ensure that:

- The IP Phone is able to trust the Trust Verification Service (TVS). This can be verified with access to any HTTPS service from the phone. For example, if Corporate Directory access works, then it means that the phone trusts TVS service.
- Verify if the cluster is in Non-Secure Mode or Mixed Mode.

To determine if it is Mixed-Mode cluster, choose **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure; 1 == Mixed Mode)**.

⚠️ **Warning**: If you are in a Mixed Mode Cluster before services restart, the CTL must be updated: Token or Tokenless.

After you install the certificate issued by CA, the next list of services must be restarted in the nodes that are enabled:

- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager
- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service

Troubleshoot

These logs can help the Cisco Technical Assistance Center identify any issues related to Multi-Server SAN CSR generation and upload of CA-Signed Certificate.
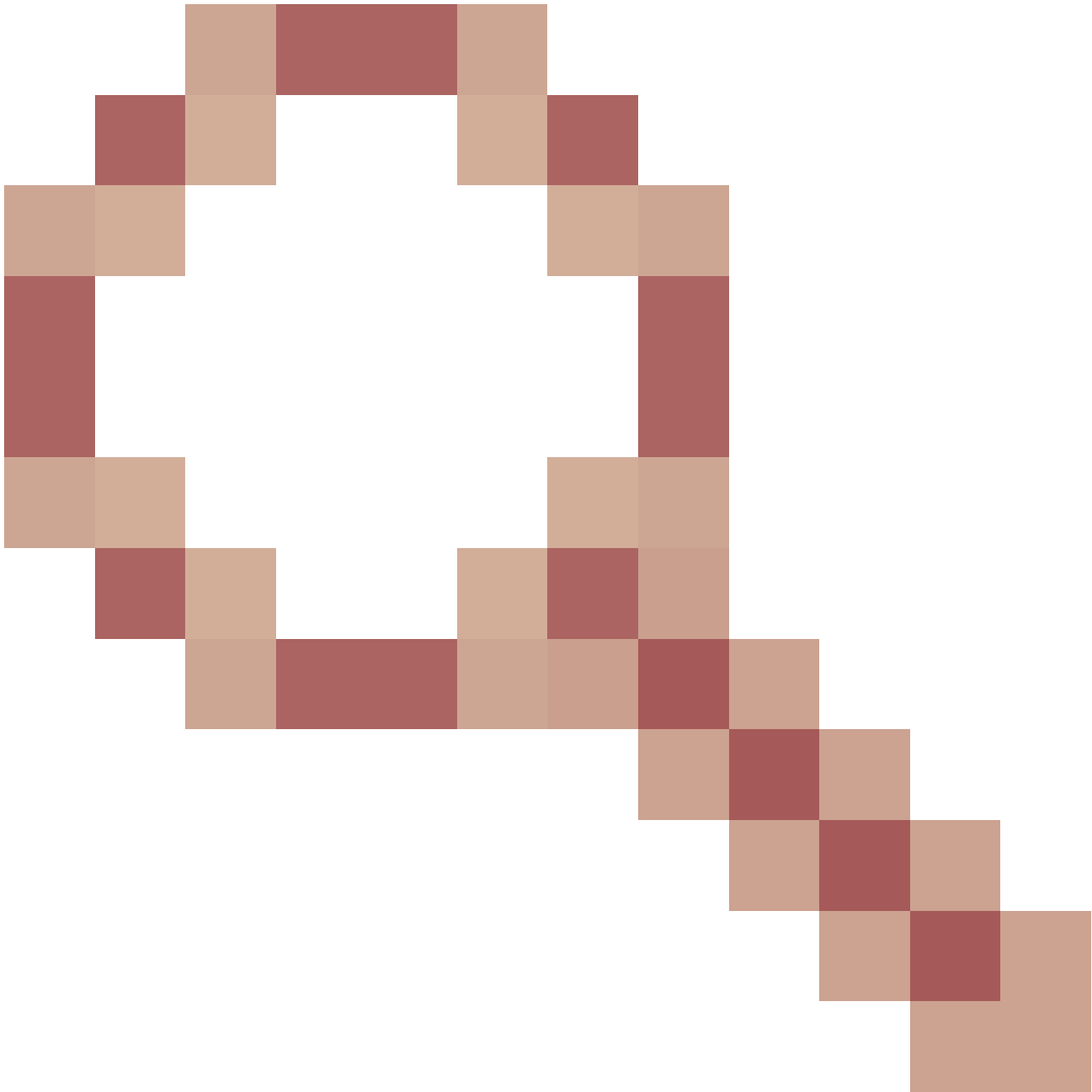
- Cisco Unified OS Platform API
- Cisco Tomcat
- IPT Platform CertMgr Logs
- Certificate renew process

Known Caveats

• Cisco bug ID CSCur97909 - Uploading multiserver cert does not delete self-signed certs in DB
• Cisco bug ID CSCus47235 - CUCM 10.5.2 CN not duplicated into SAN for CSR
• Cisco bug ID CSCup28852 - phone reset every 7min due to cert update when you use multi-server cert

If there is an existing Multi-Server Certificate, the regeneration is recommended in these scenarios:

- Hostname or Domain change. When a hostname or domain change is performed the certificates are regenerated automatically as Self-Signed. To change it to a CA-Signed the previous steps must be followed.
- If a new node was added to the cluster, a new CSR must be generated to include the new node.
- When a subscriber is restored and no backup was used, the node can have new Self-Signed certificates. A new CSR for the complete cluster can be required to include the subscriber. (There is an enhancement requestCisco bug ID CSCuv75957

to add this feature.)