# **Setup Unified Communication Cluster**

## Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
<u>Configure</u>
<u>Verify</u>
CallManager Multi-Server SAN Certificate
Troubleshoot
Known Caveats

## 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**.

Generate Certificate Si	igning Request			
Generate 🖳 Close				
- Status				
Warning: Generatin	ig a new CSR for a	specific certificate ty	ype will overwrite the exis	ting CSR for that type
Generate Certificate	Signing Request-			
Certificate Purpose*	tomcat			
Distribution*	cs-ccm-pub.	.com	-	
Common Name*	cs-ccm-pub.	.com	-	
Subject Alternate Nar	nes (SANs)	N)	-	
Parent Domain	com			
Key Length*	2048			
Hash Algorithm*	SHA256		•	
Generate				
indicates require	ed item.			

Step 2.

Choose Multi-Server SAN in Distribution.

Generate Certificate S	igning Request
💽 Generate 🖳 Close	
Status Warning: Generation	ng 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.v .com v
Common Name*	cs-ccm-pub
Subject Alternate Na	mes (SANs)
Parent Domain	com
Key Length*	2048
Hash Algorithm*	SHA256
Generate Close	
- indicates requir	ea 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 Sign	ing Request	
Generate 🖳 Close		
Status		
Warning: Generating a	new CSR for a specific certificate type will overwrite th	e existing CSR for that type
Generate Certificate Sign	ning Request	
Certificate Purpose*	tomcat 🔹	
Distribution*	Multi-server(SAN)	
Common Name*	cs-ccm-pub	
Subject Alternate Name	s (SANs)	
Auto-populated Domains	cs-ccm-pubcom cs-ccm-subcom cs-imp. k.com	
Parent Domain		7
Other Domains	com a	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	tem.	

### 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
r Status
Juccess: Certificate Signing Request Generated
CSR export operation successful on the nodes [cs-ccm-sub.v .com, cs-ccm-pub.v .com, cs-imp.v .com].

In Certificate Management, the SAN Request is generated:

Certificate L	ist (1 - 15 of 15)				
Find Certificate	List where Certificate V begins with	n 🗸 tomcat		Find Clear Filter	
Certificate 🔺	Common Name	Туре	Кеу Туре	Distribution	Issued By
tomcat	115pub-ms.	CSR Only	RSA	Multi-server(SAN)	
tomcat	115pub-ms.	CA-signed	RSA	Multi-server(SAN)	

Step 4.

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

CISCO Cisco Unified Operating System Administration For Cisco Unified Communications Solutions
Show - Settings - Security - Software Upgrades - Services - Help -
Certificate List
Generate Self-signed Poload Certificate/Certificate chain Generate CSR Lownload CSR
Download Certificate Signing Request
Download CSR Close
- Status
Certificate names not listed below do not have a corresponding CSR
Download Certificate Signing Request
Certificate Purpose* tomcat v
Download CSR Close
i *- indicates required item.

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.



#### Submit the CSR request as shown here.

Microsoft Active Directory Certificate Services vasank-DC1-GA	Home
Submit a Certificate Request or Renewal Request	
To submit a saved request to the CA, paste a base-84-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: Example - REGIN CERTIFICATE REGISTOR: contrare request REDISALCAR OXAGAN = DOCUMENTARY CONTRACT CONTRACT = DOCUMENTARY CONTRACTANTS = DOCUMENTARY = DOCU	
Additional Attributors:	
Attitutes C	
Sutmit >	

#### Microsoft Active Directory Certificate Services -- vasank-DC1-CA

#### **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.

cisco	Cisco For Cisco	Unified Co	d Operating	System	Administ	ration
Show - S	Settings 👻	Security 👻	Software Upgrades	<ul> <li>Services</li> </ul>	Help 👻	
Certificate	a List					
Gener	ate Self-signe	nd 🐴 Up	ioad Certificate/Certifi	cate chain	Generate CSR	Download CSR

Upload Certificate/Certificate	chain
Dipload 🖳 Close	
Status Warning: Uploading a cluster	er-wide certificate will distribute it to all servers
Certificate Purpose* tomcat-tru Description(friendly	ist v
Upload File Choose File	ertchain.p7b
Upload Close	

### 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:

Upload Certificate/Certificate	chain	
Upload Close		
Status Certificate upload operation ccm-sub. Restart Cisco Tomcat Service	successful for the nodes cs-ccm-pub. com,cs- c.com.	7
U imp	CLI "utils service restart Cisco Tomcat".	
Upload Certificate/Certificate	e chain	
Certificate Purpose*	tomcat 💌	
Description(friendly name)	Self-signed certificate	
Upload File	Browse_ No file selected.	
Upload Close		_
indicates required item.		
•		

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

ipsec-trust	a-con-pub.	Self-signed	cs-com-pub	cs-con-pub	04/18/2019	Trust Certificate
TURecovery	TLRECOVERY cs-com-pub.vasank.com	Self-signed	ITURECOVERY_cs-com-pub.numil.com	ITLRECOVERY_cs-com-pub.immil.com	04/18/2019	Self-signed certificate generated by system
tornat	cs-com-pub	CA-signed	Nubi-server(SAN)	-DCI-CA	12/19/2015	Certificate Signed by mani: OC1-CA
torncat-brust	a-con-pub	CA-signed	Nubi-server(SAN)	suult-DCI-CA	12/19/2015	Trust Certificate
torncat-trust	os-com-outo: com	Self-scred	gs-com-pub	gs-con-pub. International Action	04/21/2019	Trust Certificate
tomcat-trust	VeriSign Class 3 Secure Server CA - G3	CA-signed	VeriSign_Class_3_Secure_Server_CA - G3	VeriSign_Class_3_Public_Primary_Certification_AuthorityG5	02/08/2020	Trust Certificate
tomcat-bust	dc1-com-pub.vauariu.com	Self-signed	dc1-com-pub.ymmil.com	dc1-com-pub.remil.com	04/17/2019	Trust Certificate
tomcat-trust	dc1-con-sub.view.i.com	Self-signed	dc1-ccm-sub	dc1-com-sub.veue l.com	04/18/2019	Trust Certificate
tomcat-brust		Self-signed	-DC1-CA	DCI-CA	04/29/2064	Root CA
TVS	cs-com-publivesank.com	Self-signed	cs-com-public	cs-com-pub.	04/18/2019	Self-signed certificate generated by system

### 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**.

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[STARTING] Cisco Tomcat[STARTING] Cisco Tomcat[STARTED] admin:

## Verify

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

Issued To         Common Name (CN)       cs-ccm-pub.         Organisation (O)       Cisco         Organisational Unit (OU)       TAC         Serial Number       1D:54:C2:6E         Issued By       Dommon Name (CN)         Organisation (O)       -DC1-         Organisational Unit (OU) <not o<="" part="" td="">         /alidity       ssued On         ssued On       12/19/2014         ixpires On       12/19/2015         Ingerprints       HA1 Fingerprint</not>	E:00:00:00:00:20 I-CA I-CA Of Certificate >
Organisation (O)     Cisco       Organisational Unit (OU)     TAC       Gerial Number     1D:54:C2:6E       Ssued By       Common Name (CN)     -DC1-       Organisation (O)     -DC1-       Organisational Unit (OU) <not o<="" part="" td="">       /alidity     ssued On     12/19/2014       ixpires On     12/19/2015       Ingerprints     HA1 Engerprint</not>	E:00:00:00:00:20 I-CA I-CA Of Certificate >
Organisational Unit (OU)       TAC         Derial Number       1D:54:C2:6E         Serial Number       1D:54:C2:6E         Common Name (CN)       DC1:         Organisation (O)       -DC1:         Organisational Unit (OU) <not o<="" part="" td="">         Organisational Unit (OU)       <not o<="" part="" td="">         Alidity       ssued On       12/19/2014         Expires On       12/19/2015         Eingerprints       DC:E3:94:DE</not></not>	E:00:00:00:00:20 I-CA I-CA Of Certificate >
ierial Number       1D:54:C2:68         issued By       DC         Common Name (CN)       DC1-         Organisation (O)       DC1-         Organisational Unit (OU)       Not Part O         /alidity       ssued On       12/19/2014         ixpires On       12/19/2015         ingerprints       C:E3:94:DC	E:00:00:00:00:20 I-CA I-CA Of Certificate >
Assued By       Common Name (CN)       Organisation (O)       Organisational Unit (OU)       Organisational Unit (OU)       Alidity       ssued On       12/19/2014       Expires On       12/19/2015       Fingerprints       CHA1 Fingerprint	I-CA I-CA Of Certificate >
Common Name (CN)     DC1-       Organisation (O)     DC1-       Organisational Unit (OU) <not o<="" part="" td="">       /alidity     12/19/2014       Ssued On     12/19/2015       Fingerprints     C:E3:94:DC</not>	I-CA I-CA Of Certificate >
Organisation (O)     Image: DC1-       Organisational Unit (OU) <not o<="" part="" td="">       /alidity     ssued On     12/19/2014       ixpires On     12/19/2015       Fingerprints     DC:E3:94:DC</not>	I-CA Of Certificate >
Organisational Unit (OU) <not o<="" part="" td="">         /alidity       ssued On       12/19/2014         sxpires On       12/19/2015         Fingerprints       C:E3:94:D0</not>	Of Certificate>
/alidity           ssued On         12/19/2014           Expires On         12/19/2015           Fingerprints         C:E3:94:D0	
ssued On         12/19/2014           Expires On         12/19/2015           Fingerprints         C:E3:94:D0	
Expires On 12/19/2015 Fingerprints CHA1 Fingerprint DC:F3:9A:D(	i de la companya de l
Fingerprints HA1 Fingerprint DC+F3+9A+D(	
HA1 Fingerprint DC:E3:9A:D	
Concertain Concertainte	6:F4:81:6F:A7:38:4F:DB:1B:AA:BF:CC:05:F5:A7:A3:1A
4D5 Fingerprint 97:EA:6C:A	D:91:12:88:DD:0E:30:C9:46:54:89:3E:59

### 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: <u>Token</u> or <u>Tokenless</u>.

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
- <u>Certificate renew process</u>

### **Known Caveats**

- Cisco bug ID <u>CSCur97909</u> Uploading multiserver cert does not delete self-signed certs in DB
- Cisco bug ID <u>CSCus47235</u> CUCM 10.5.2 CN not duplicated into SAN for CSR
- Cisco bug ID <u>CSCup28852</u> 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 <u>CSCuv75957</u>



to add this feature.)