Unified Communication Cluster Setup with CA−Signed Multi−Server Subject Alternate Name Configuration Example

TAC **Document ID: 118731**

Contributed by Vasanth Kumar K, Cisco TAC Engineer.

Mar 09, 2015

Contents

Introduction

This document describes how to set up a Unified Communication Cluster with the use of a Certificate Authority (CA)−Signed Multi−Server Subject Alternate Name (SAN).

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.

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, make sure that you understand the potential impact of any command.

Background Information

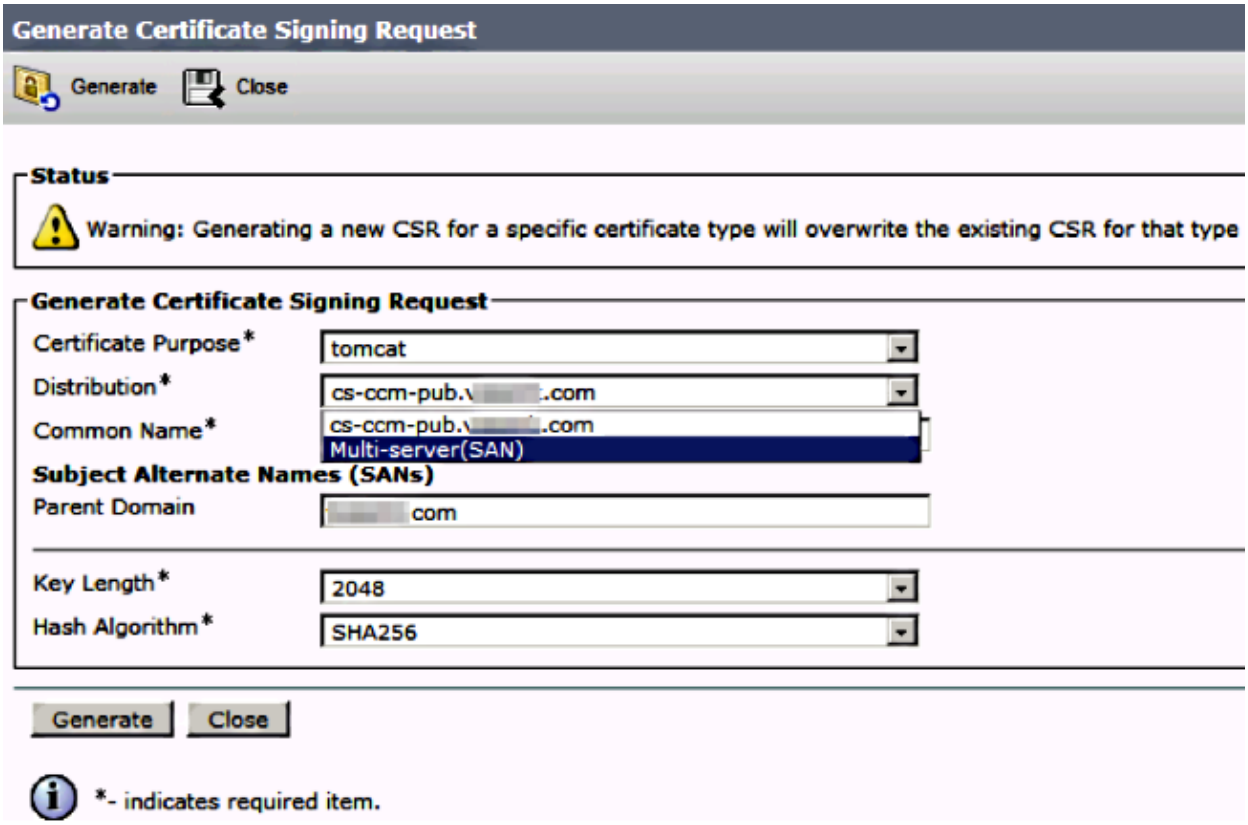
In CUCM Version 10.5 and later, this trust−store Certificate Signing Request (CSR) request can include SAN and alternate domains.

1. Tomcat
2. Cisco CallManager (CCM)
3. Cisco Unified Presence−Extensible Messaging and Presence Protocol (CUP−XMPP)
4. CUP−XMPP Server−to−Server (S2S)

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

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



Generate Certificate Signing Request

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.[redacted].com

Common Name*

cs-ccm-pub.[redacted].com
Multi-server(SAN)

Subject Alternate Names (SANs)

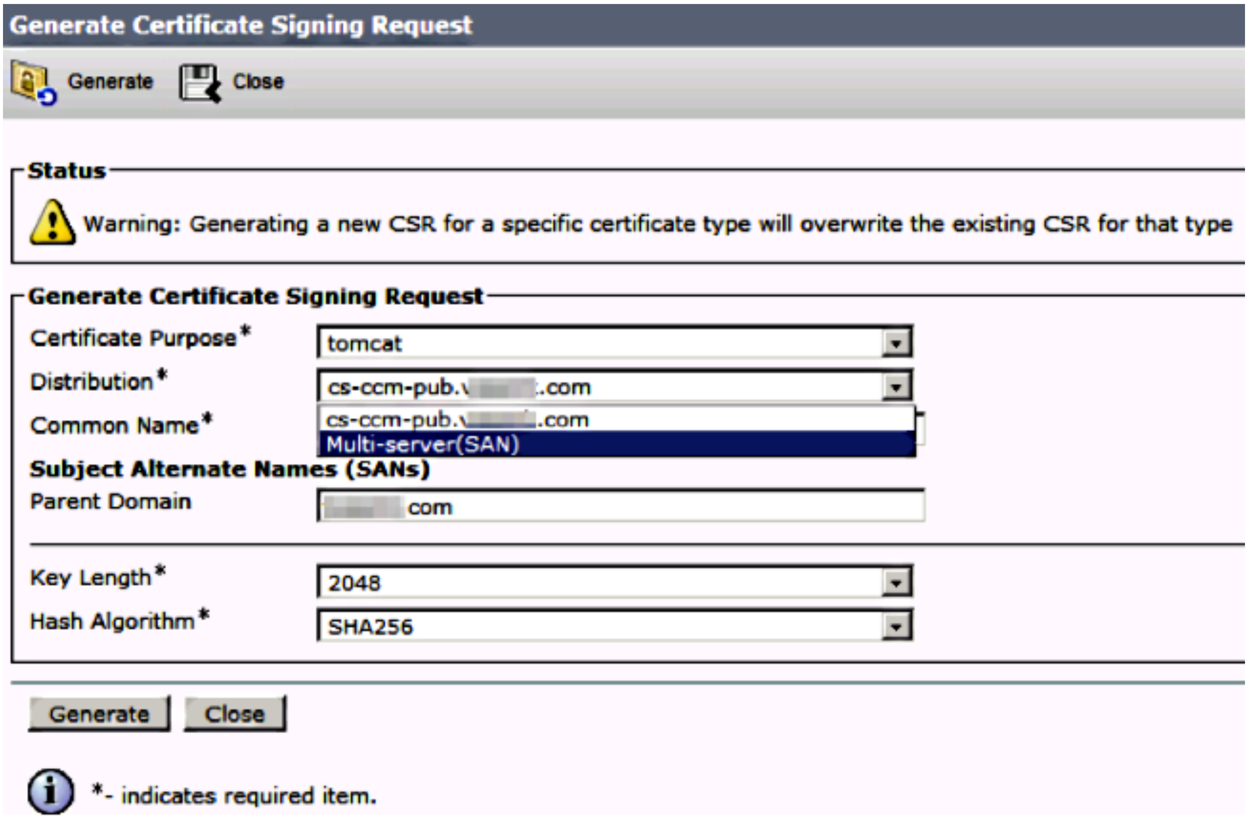
Parent Domain [redacted] com

Key Length* 2048

Hash Algorithm* SHA256

*- indicates required item.

2. Select ***Multi−Server SAN*** in Distribution.



Status

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

Generate Certificate Signing Request

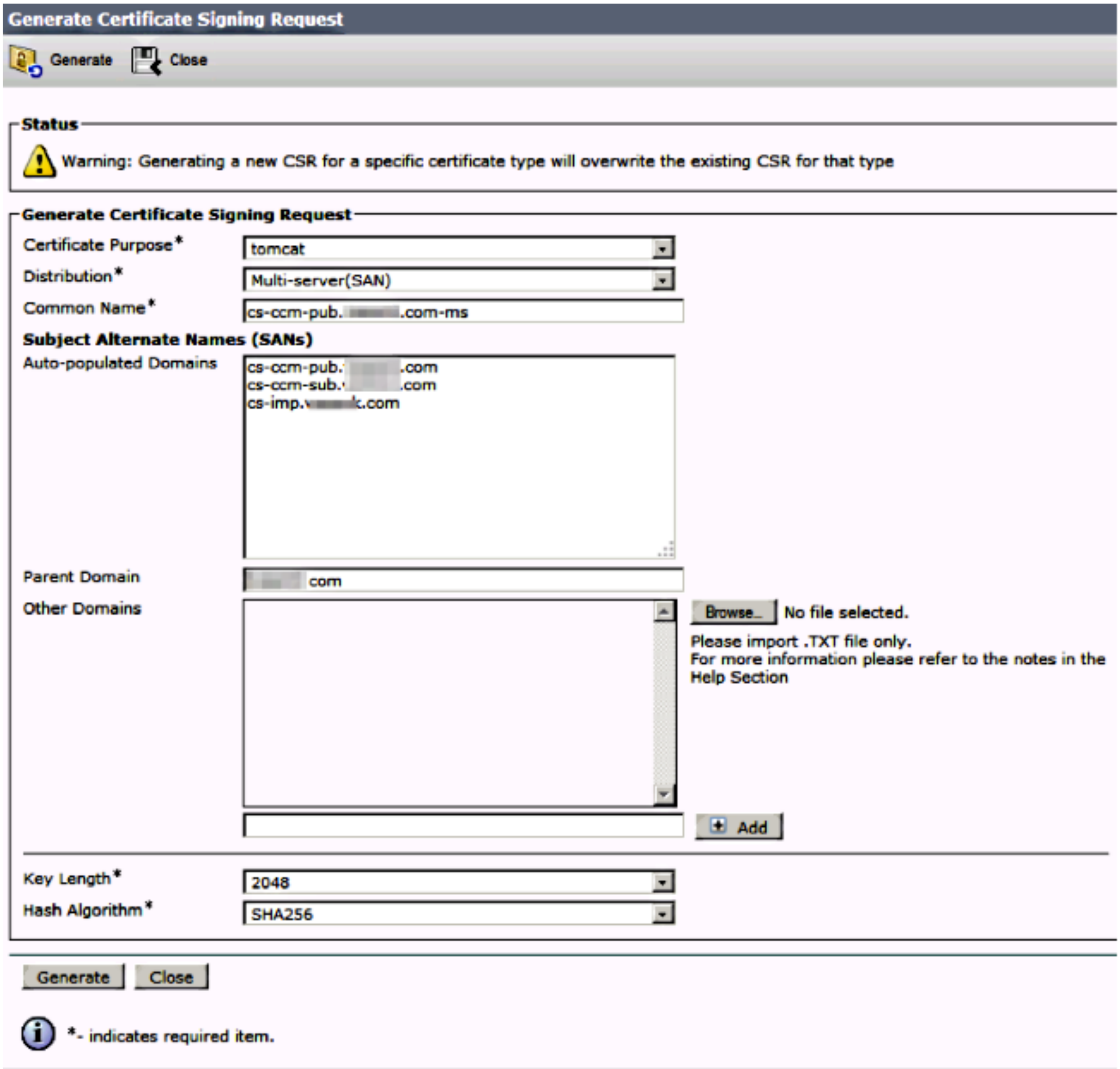
Certificate Purpose*	tomcat
Distribution*	cs-ccm-pub.[redacted].com
Common Name*	cs-ccm-pub.[redacted].com Multi-server(SAN)

Subject Alternate Names (SANs)

Parent Domain	[redacted] com
Key Length*	2048
Hash Algorithm*	SHA256

*- indicates required item.

It autopopulates the SAN domains and the parent domain.



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.[redacted].com-ms

Subject Alternate Names (SANs)

Auto-populated Domains	cs-ccm-pub.[redacted].com cs-ccm-sub.[redacted].com cs-imp.[redacted].com
Parent Domain	[redacted] com
Other Domains	

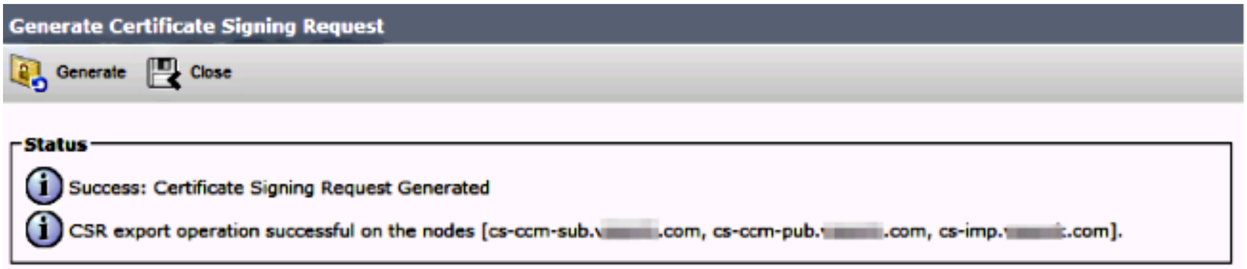
No file selected.

Please import .TXT file only.
For more information please refer to the notes in the Help Section

Key Length*	2048
Hash Algorithm*	SHA256

*- indicates required item.

Once it is generated, this displays:

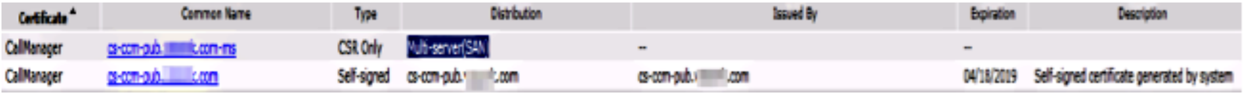


Status

Success: Certificate Signing Request Generated

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

In Certificate Management, the SAN Request is generated:

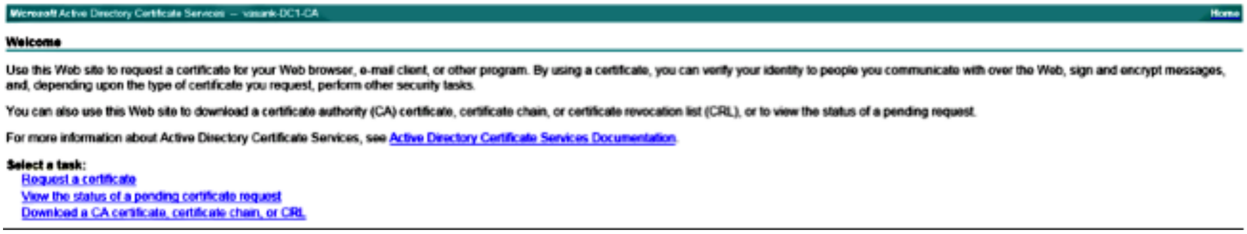


Certificate ▲	Common Name	Type	Distribution	Issued By	Expiration	Description
CallManager	cs-ccm-pub.[redacted].com-ms	CSR Only	Multi-server(SAN)	--	--	
CallManager	cs-ccm-pub.[redacted].com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system

3. You can use the local CA or an External CA like VeriSign in order to get it signed. This example shows configuration steps for a Microsoft Windows Server−based CA.

   Log into https://<windowsserveripaddress>/certsrv/

   Select ***Request a Certificate > Advanced Certificate Request***.



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

Welcome

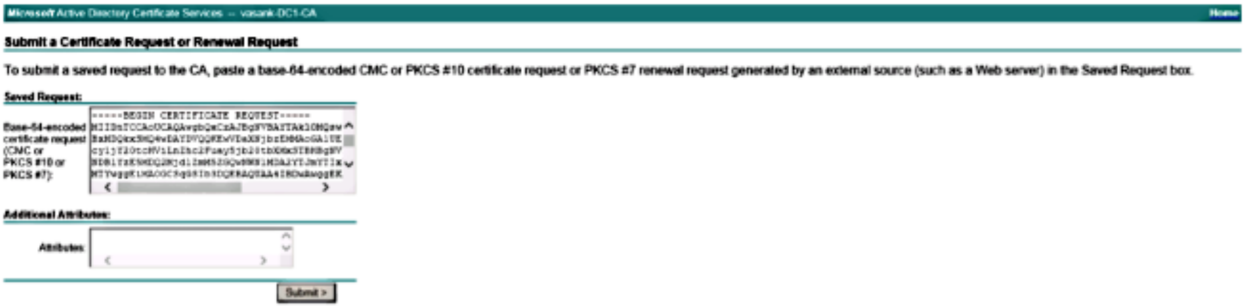
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security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

4. Submit the CSR request as shown here.



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

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.

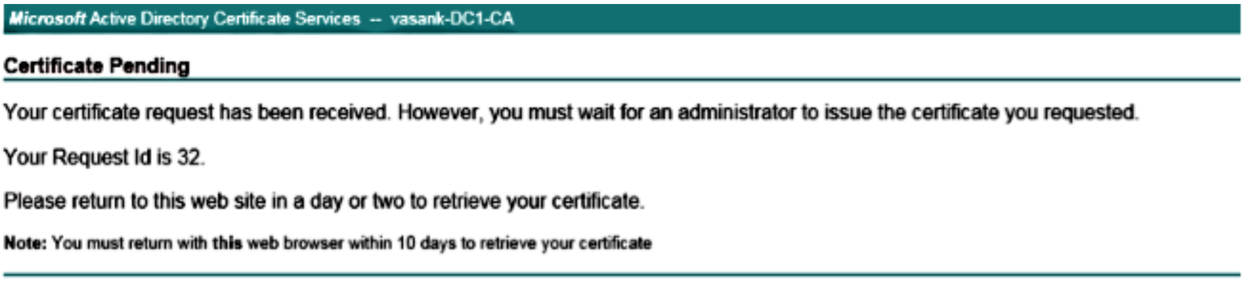
Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDnTCCAoUCAQAwgbQxCzAJBgNVBAYTAklOMQsw
[illegible]
[illegible]
[illegible]
[illegible]
```

Additional Attributes:

Attributes:



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

Certificate Pending

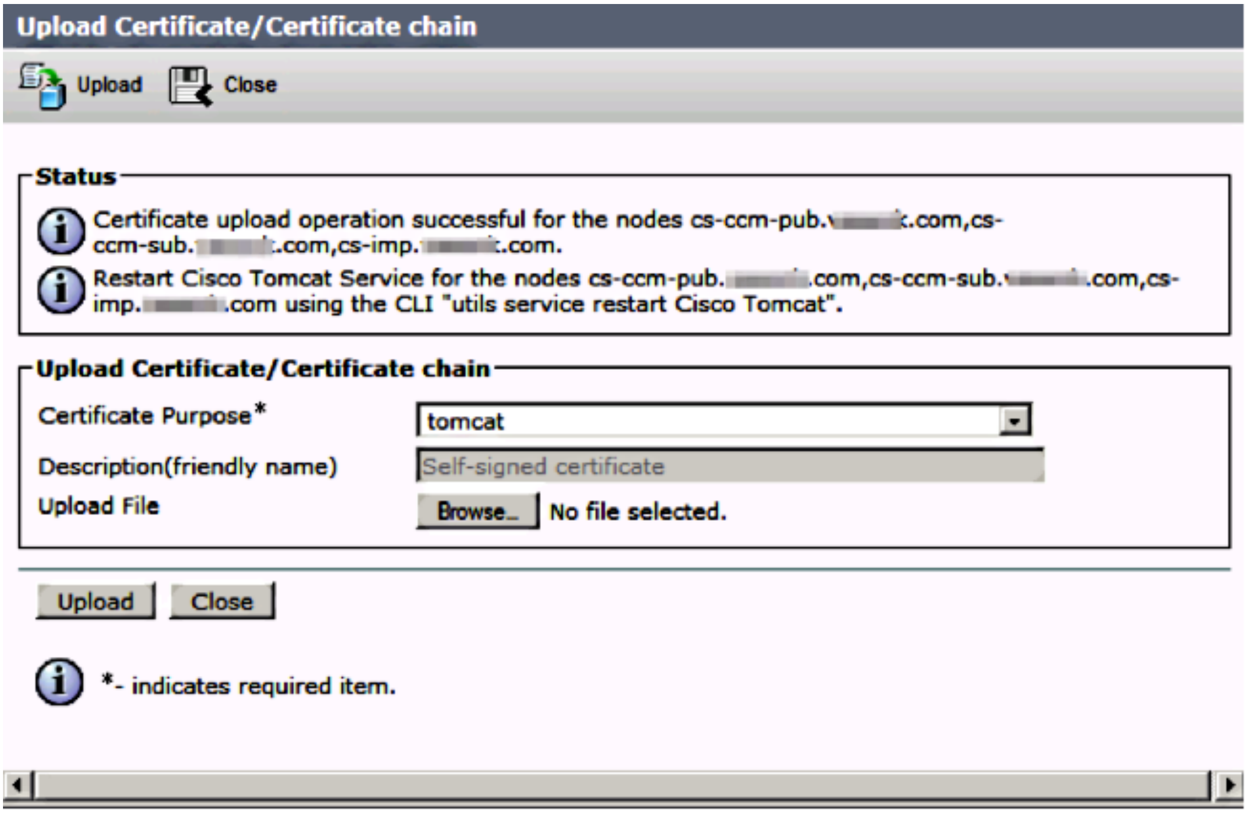
Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

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

5. Once you obtain the certificate, you must upload the CA certificate as tomcat−trust and then upload the CA−signed certificate as tomcat.



Status

Certificate upload operation successful for the nodes cs-ccm-pub.[redacted].com,cs-ccm-sub.[redacted].com,cs-imp.[redacted].com.

Restart Cisco Tomcat Service for the nodes cs-ccm-pub.[redacted].com,cs-ccm-sub.[redacted].com,cs-imp.[redacted].com using the CLI "utils service restart Cisco Tomcat".

Upload Certificate/Certificate chain

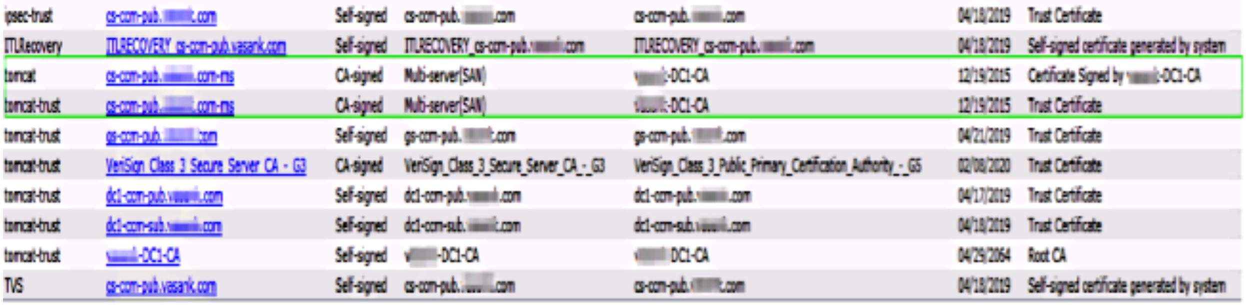
Certificate Purpose* tomcat

Description(friendly name) Self-signed certificate

Upload File No file selected.

*- indicates required item.

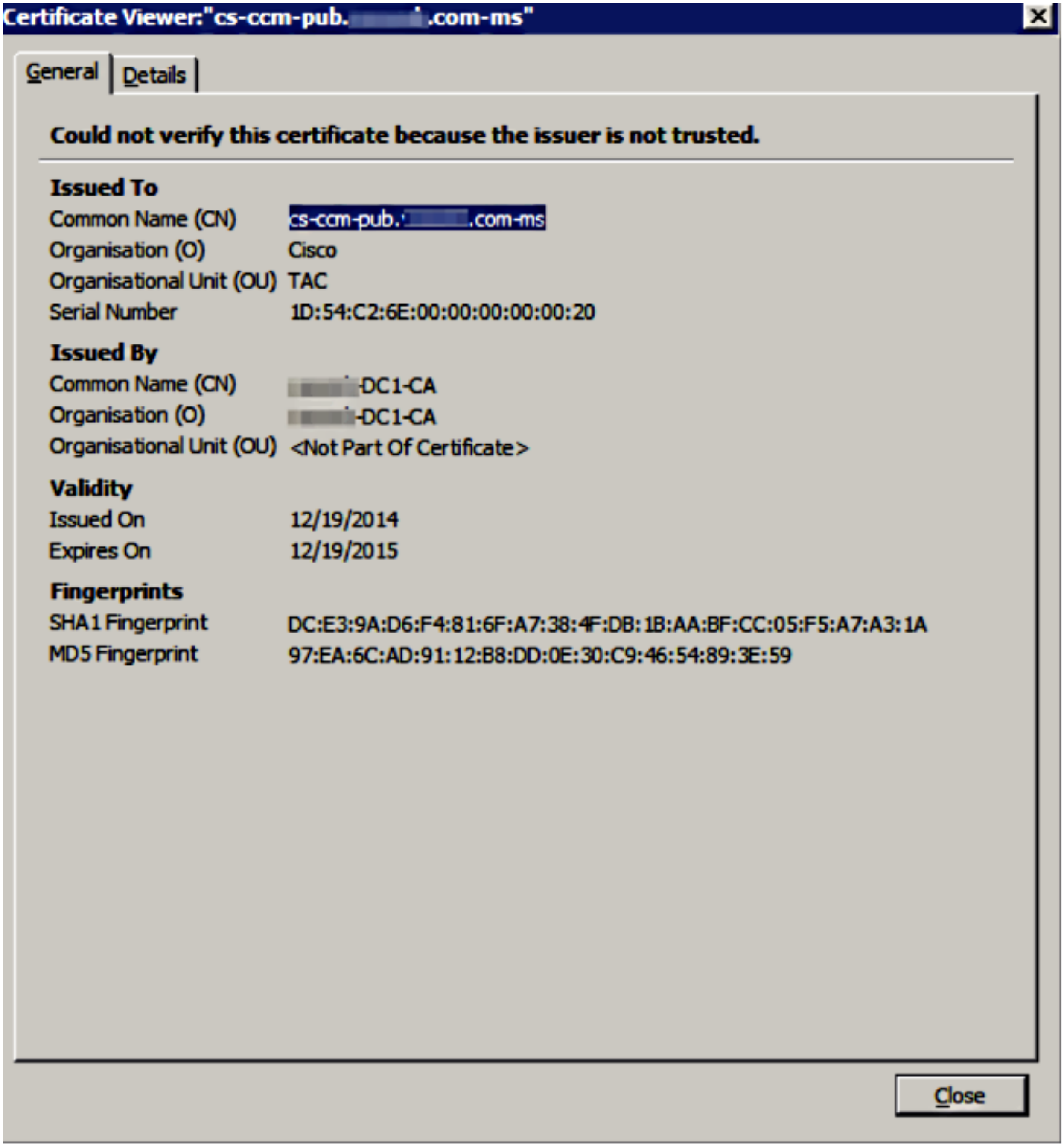
6. Ensure the service is restarted on all nodes in the SAN list, which includes the node where it is uploaded. You see Multi−Server SAN listed in Certificate Management.



ipsec-trust	cs-ccm-pub.[redacted].com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY_cs-ccm-pub.vasank.com	Self-signed	ITLRECOVERY_cs-ccm-pub.[redacted].com	ITLRECOVERY_cs-ccm-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-ccm-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Certificate Signed by [redacted]-DC1-CA
tomcat-trust	cs-ccm-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	gs-ccm-pub.[redacted].com	Self-signed	gs-ccm-pub.[redacted].com	gs-ccm-pub.[redacted].com	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_Authority_-_G5	02/08/2020	Trust Certificate
tomcat-trust	dc1-ccm-pub.[redacted].com	Self-signed	dc1-ccm-pub.[redacted].com	dc1-ccm-pub.[redacted].com	04/17/2019	Trust Certificate
tomcat-trust	dc1-ccm-sub.[redacted].com	Self-signed	dc1-ccm-sub.[redacted].com	dc1-ccm-sub.[redacted].com	04/18/2019	Trust Certificate
tomcat-trust	[redacted]-DC1-CA	Self-signed	[redacted]-DC1-CA	[redacted]-DC1-CA	04/29/2064	Root CA
TVS	cs-ccm-pub.vasank.com	Self-signed	cs-ccm-pub.[redacted].com	cs-ccm-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system

Verify

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



Certificate Viewer:"cs-ccm-pub.[redacted].com-ms"

Could not verify this certificate because the issuer is not trusted.

Issued To
Common Name (CN) cs-ccm-pub.[redacted].com-ms
Organisation (O) Cisco
Organisational Unit (OU) TAC
Serial Number 1D:54:C2:6E:00:00:00:00:00:20

Issued By
Common Name (CN) [redacted]-DC1-CA
Organisation (O) [redacted]-DC1-CA
Organisational Unit (OU) <Not Part Of Certificate>

Validity
Issued On 12/19/2014
Expires On 12/19/2015

Fingerprints
SHA1 Fingerprint DC:E3:9A:D6:F4:81:6F:A7:38:4F:DB:1B:AA:BF:CC:05:F5:A7:A3:1A
MD5 Fingerprint 97:EA:6C:AD:91:12:B8: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 autopopulated domains are all of the CallManager nodes. If it does not run, you can choose to keep it from the SAN list or remove it from there.

After you install the certificate issued by CA, you must restart the CallManager service on all nodes.

Before you get 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 if you access any HTTPS service from the phone. For example, if Corporate Directory access works, then it means that the phone trusts TVS service.
- If it is a secure cluster, ensure that the Certificate Trust List (CTL) client is rerun so that a new CTL file is created and the cluster is rebooted.

Troubleshoot

These logs should help the Cisco Technical Assistance Center identify any issues related to Multi−Server SAN CSR generation and upload of CA−Signed Certficate.

- Cisco Unified OS Platform API
- Cisco Tomcat
- IPT Platform CertMgr Logs

In an existing Multi−Server Certifcate CUCM, if the hostname of the server changes, it is recommended to generate a multi−server SAN CSR request as explained previously in order to get the certificate signed by CA.

Updated: Mar 09, 2015 Document ID: 118731