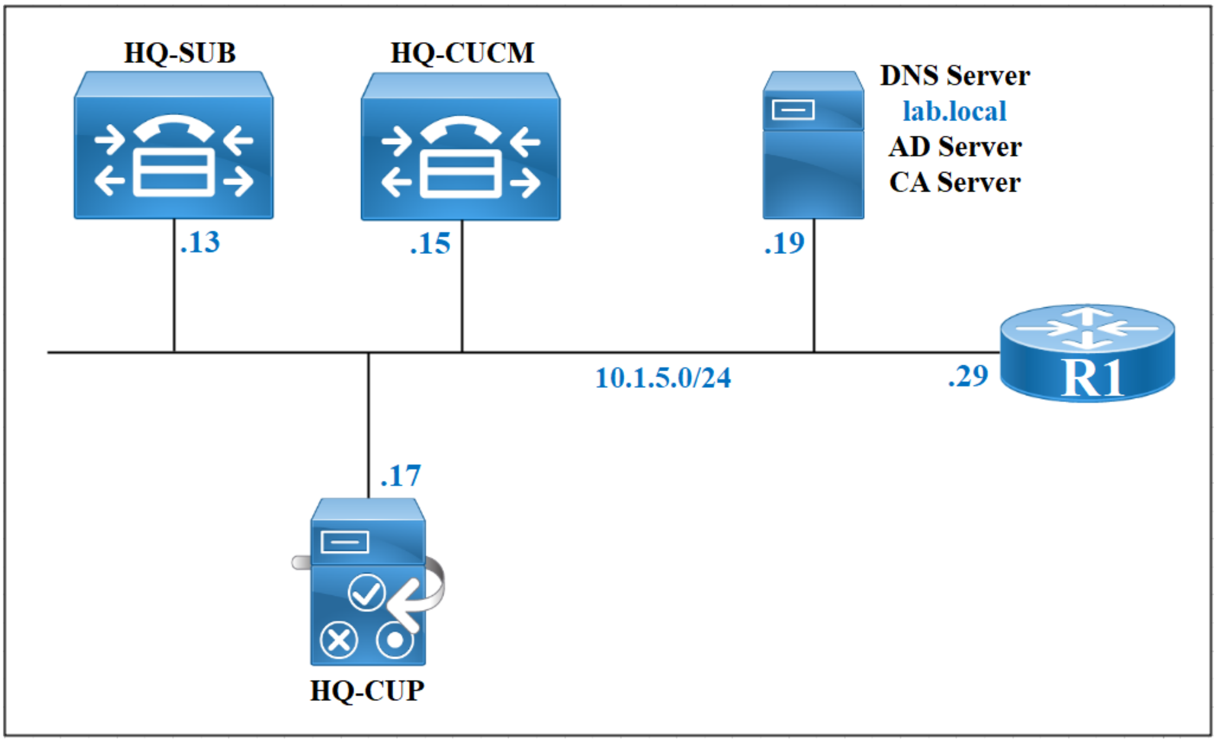
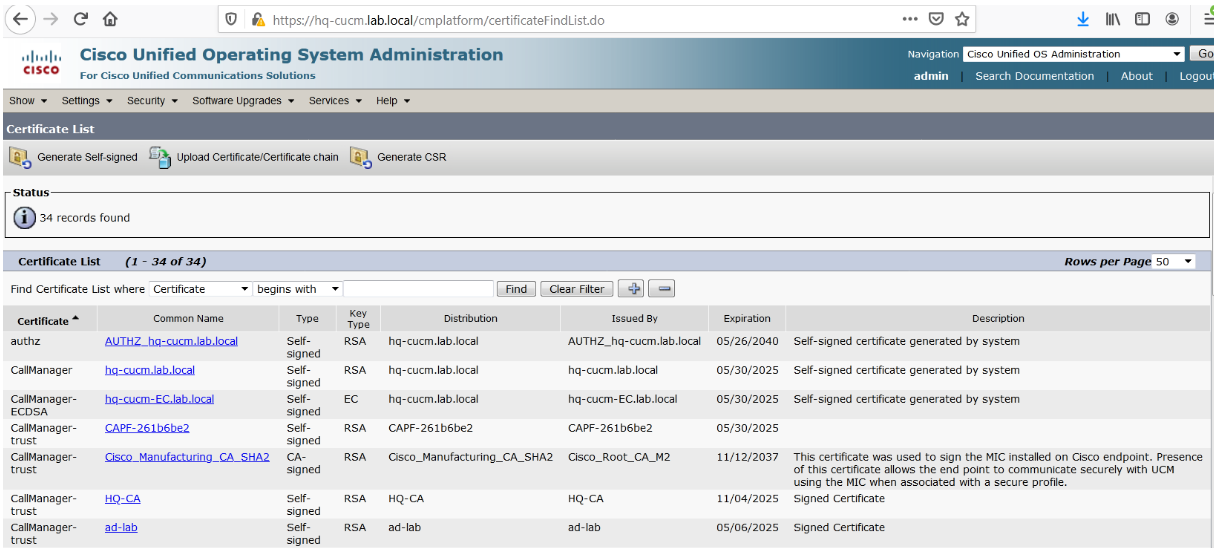
How To Configure Multi-server (SAN) Tomcat certificate on Cisco Unified CM Cluster

Redouane MEDDANE



Create a CSR for the Tomcat Service

From the Cisco Unified OS Administration module. Navigate to **Security > Certificate Management**. Click **Generate CSR**.


https://hq-cucm.lab.local/cmplatform/certificateFindList.do
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration Go
admin | Search Documentation | About | Logout
Show Settings Security Software Upgrades Services Help
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Find Clear Filter

Certificate List

Status

34 records found

Certificate List (1 - 34 of 34) Rows per Page 50

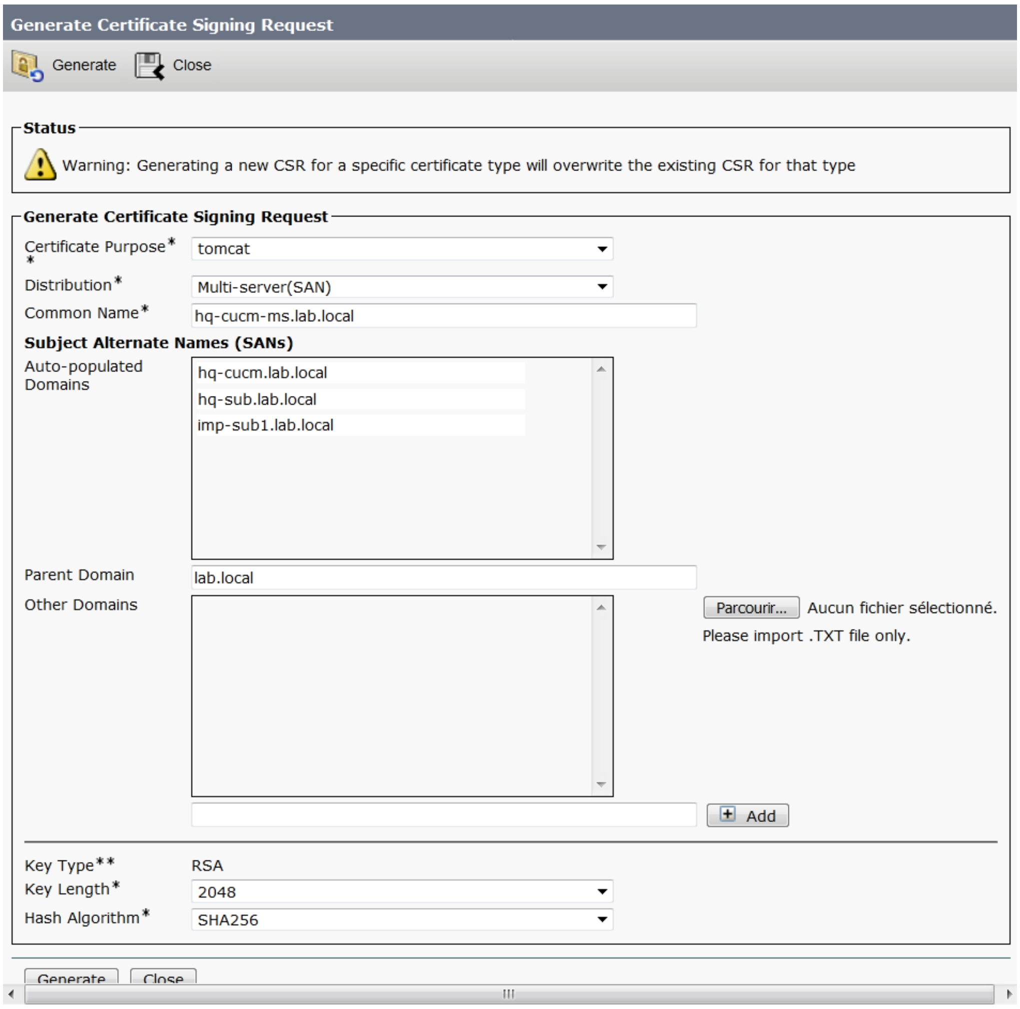
Find Certificate List where Certificate begins with

Certificate ▲	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
authz	AUTHZ_hq-cucm.lab.local	Self-signed	RSA	hq-cucm.lab.local	AUTHZ_hq-cucm.lab.local	05/26/2040	Self-signed certificate generated by system
CallManager	hq-cucm.lab.local	Self-signed	RSA	hq-cucm.lab.local	hq-cucm.lab.local	05/30/2025	Self-signed certificate generated by system
CallManager-ECDSA	hq-cucm-EC.lab.local	Self-signed	EC	hq-cucm.lab.local	hq-cucm-EC.lab.local	05/30/2025	Self-signed certificate generated by system
CallManager-trust	CAPF-261b6be2	Self-signed	RSA	CAPF-261b6be2	CAPF-261b6be2	05/30/2025	
CallManager-trust	Cisco_Manufacturing_CA_SHA2	CA-signed	RSA	Cisco_Manufacturing_CA_SHA2	Cisco_Root_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CallManager-trust	HQ-CA	Self-signed	RSA	HQ-CA	HQ-CA	11/04/2025	Signed Certificate
CallManager-trust	ad-lab	Self-signed	RSA	ad-lab	ad-lab	05/06/2025	Signed Certificate

Select **Tomcat** from the **Certificate Purpose**. In the **Distribution** field, select **Multi-Server (SAN).**

This option allow you to create a single tomcat certificate for each node on the cluster instead of a separate certificate with its own Common Name, the Publisher **HQ-CUCM** will populate automatically the Subject Alternative Names with the FQDN of each nodes, in this case the subscriber **hq-sub.lab.local** and **imp-sub1.lab.local**.

Click **Generate**.



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* Multi-server(SAN)

Common Name* hq-cucm-ms.lab.local

Subject Alternate Names (SANs)

Auto-populated Domains
hq-cucm.lab.local
hq-sub.lab.local
imp-sub1.lab.local

Parent Domain lab.local

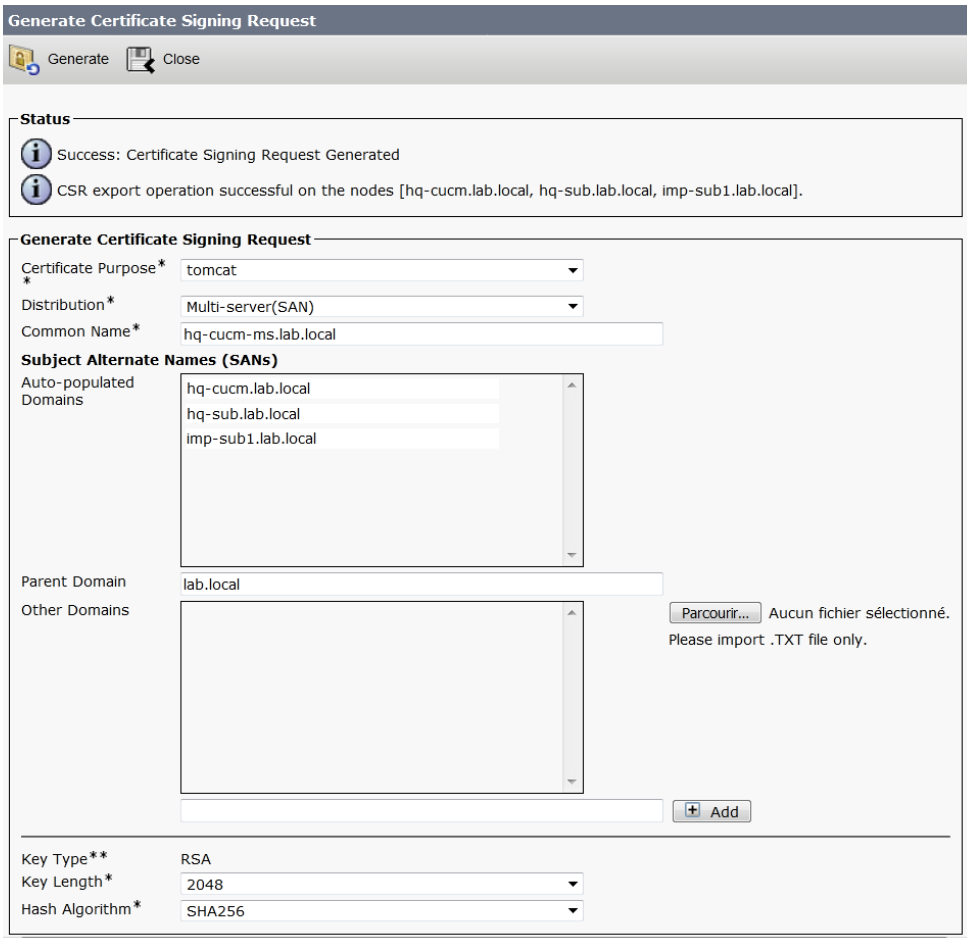
Other Domains

Aucun fichier sélectionné.
Please import .TXT file only.

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256



Status

Success: Certificate Signing Request Generated

CSR export operation successful on the nodes [hq-cucm.lab.local, hq-sub.lab.local, imp-sub1.lab.local].

Generate Certificate Signing Request

Certificate Purpose**	tomcat
Distribution*	Multi-server(SAN)
Common Name*	hq-cucm-ms.lab.local

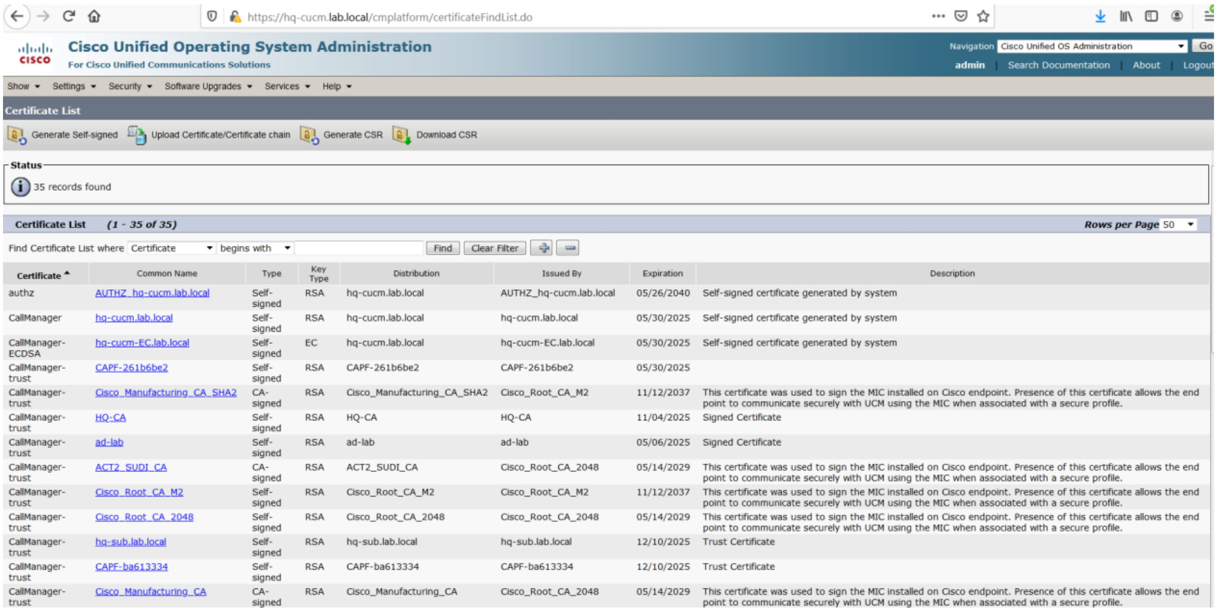
Subject Alternate Names (SANs)

Auto-populated Domains	hq-cucm.lab.local hq-sub.lab.local imp-sub1.lab.local
Parent Domain	lab.local
Other Domains	

Please import .TXT file only.

Key Type**	RSA
Key Length*	2048
Hash Algorithm*	SHA256

Click **Download CSR**. Then, Select **Tomcat** and click **Download CSR**.



https://hq-cucm.lab.local/cmplatform/certificateFindList.do
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified OS Administration
Go
admin
Search Documentation
About
Logout
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Download CSR

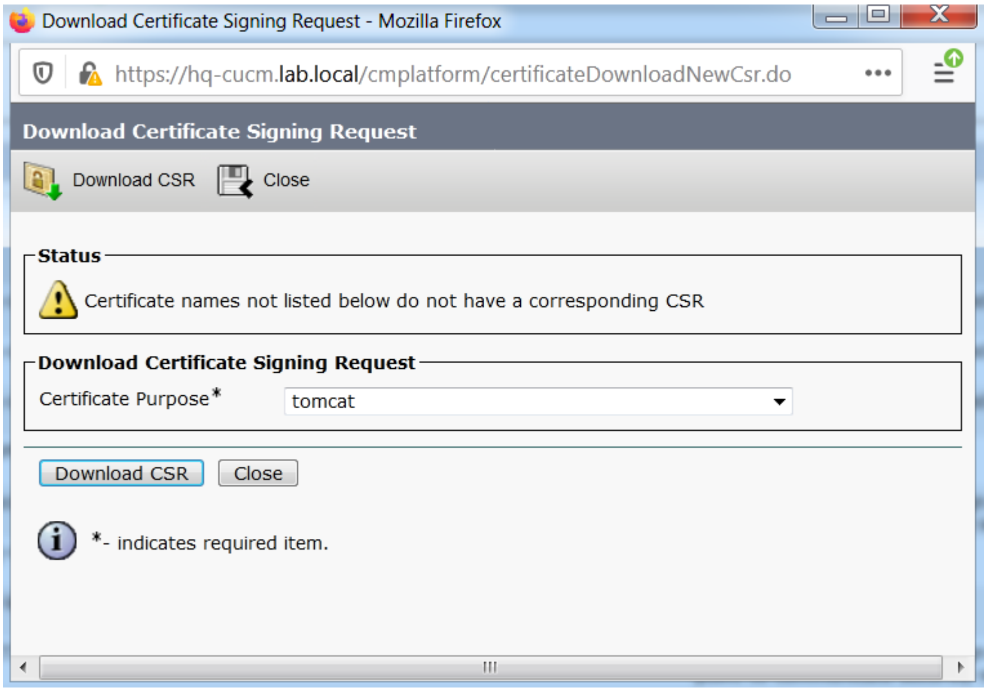
Status

35 records found

Certificate List *(1 - 35 of 35)*

Rows per Page 50
Find Certificate List where
Certificate
begins with
Find
Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
authz	AUTHZ_hq-cucm.lab.local	Self-signed	RSA	hq-cucm.lab.local	AUTHZ_hq-cucm.lab.local	05/26/2040	Self-signed certificate generated by system
CallManager	hq-cucm.lab.local	Self-signed	RSA	hq-cucm.lab.local	hq-cucm.lab.local	05/30/2025	Self-signed certificate generated by system
CallManager-ECDSA	hq-cucm-EC.lab.local	Self-signed	EC	hq-cucm.lab.local	hq-cucm-EC.lab.local	05/30/2025	Self-signed certificate generated by system
CallManager-trust	CAPF-261b6be2	Self-signed	RSA	CAPF-261b6be2	CAPF-261b6be2	05/30/2025	
CallManager-trust	Cisco_Manufacturing_CA_SHA2	CA-signed	RSA	Cisco_Manufacturing_CA_SHA2	Cisco_Root_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CallManager-trust	HQ-CA	Self-signed	RSA	HQ-CA	HQ-CA	11/04/2025	Signed Certificate
CallManager-trust	ad-lab	Self-signed	RSA	ad-lab	ad-lab	05/06/2025	Signed Certificate
CallManager-trust	ACT2_SUDI_CA	CA-signed	RSA	ACT2_SUDI_CA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CallManager-trust	Cisco_Root_CA_M2	Self-signed	RSA	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CallManager-trust	Cisco_Root_CA_2048	Self-signed	RSA	Cisco_Root_CA_2048	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CallManager-trust	hq-sub.lab.local	Self-signed	RSA	hq-sub.lab.local	hq-sub.lab.local	12/10/2025	Trust Certificate
CallManager-trust	CAPF-ba613334	Self-signed	RSA	CAPF-ba613334	CAPF-ba613334	12/10/2025	Trust Certificate
CallManager-trust	Cisco_Manufacturing_CA	CA-signed	RSA	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.



Download Certificate Signing Request - Mozilla Firefox

https://hq-cucm.lab.local/cmplatform/certificateDownloadNewCsr.do

Download Certificate Signing Request

Status

Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

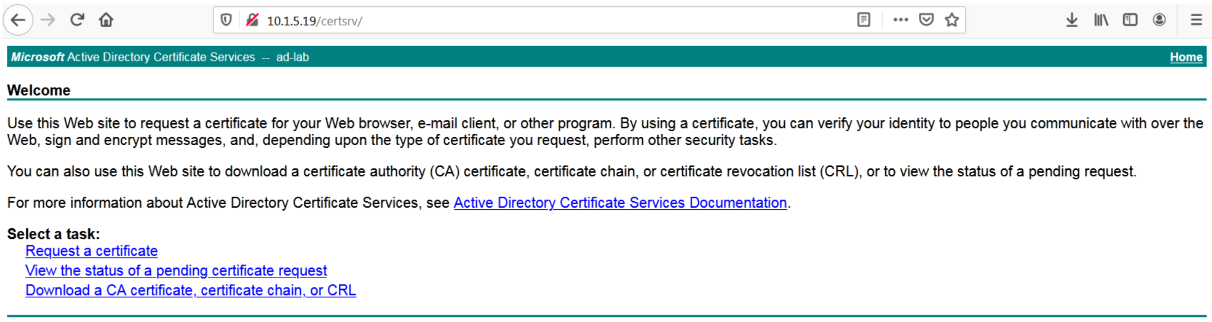
Certificate Purpose* tomcat

*- indicates required item.

Create a Certificate from CSR

From your PC, access the CA Server **10.1.5.19** using the url **https://10.1.5.19/certsrv**.

Click **Request a certificate**, then click **advanced certificate request**, you should see the Submit a **Certificate Request or Renewal Request** page.



10.1.5.19/certsrv/

Microsoft Active Directory Certificate Services -- ad-lab

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.

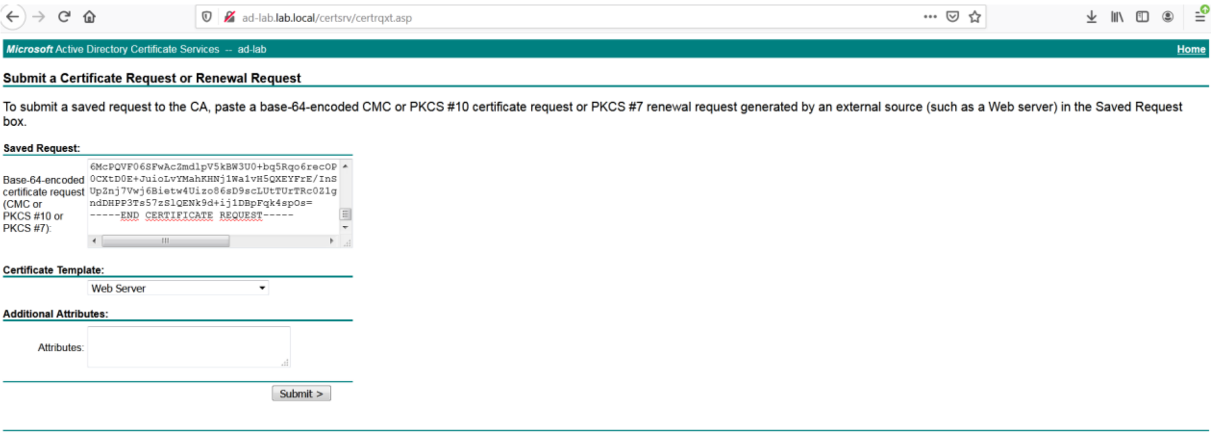
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

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

Past the CSR content into the **Base-64-encoded certificate request** field. Click **Submit.**



ad-lab.lab.local/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services -- ad-lab

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):

```
6McPQVF06SFwAcZmdlpV5kBW3U0+bq5Rqo6recOP
0CXtD0E+JuioLvYMahKHNj1Wa1vH5QXEYFrE/InS
UpZnj7Vwj6Bietw4Uizo86sD9scLUtTUrTRc0Z1g
ndDHPP3Ts57zSlQENk9d+ij1DBpFqk4spOs=
-----END CERTIFICATE REQUEST-----
```

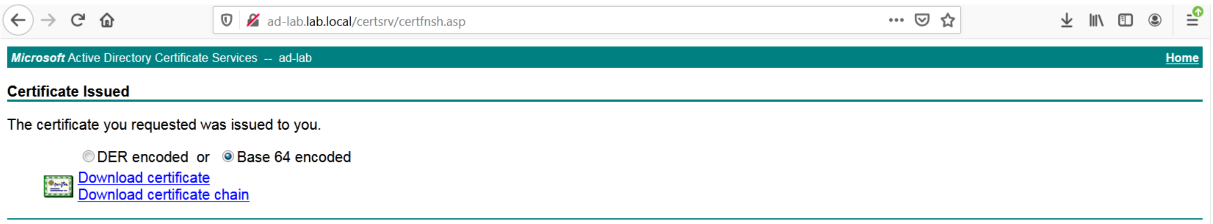
Certificate Template:

Web Server

Additional Attributes:

Attributes:

Select **Base 64 encoded** and click **Download certificate**. Name it **CUCM-Cert**.



Microsoft Active Directory Certificate Services -- ad-lab **Home**

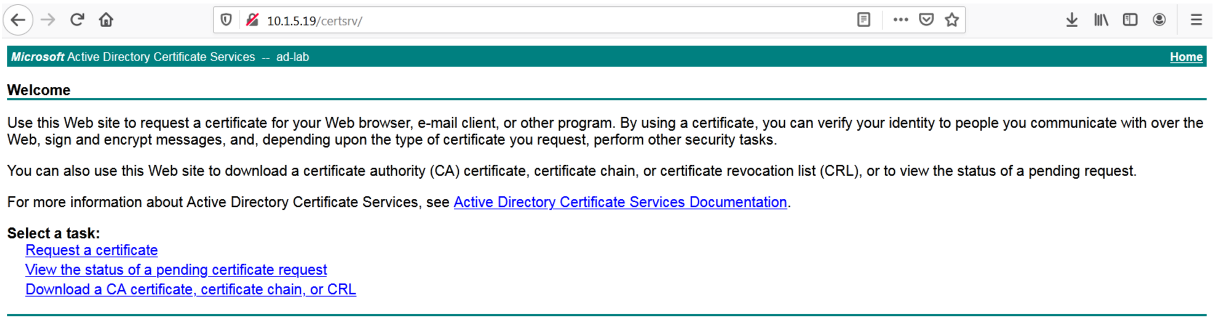
Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

Before uploading the CUCM certificate, you need to download the CA certificate, in the first page, click on **Download a CA certificate, certificate chain, or CRL**.
Ensure **Base 64** is selected and click on **Download CA certificate**. Name it **RootCA**.



Microsoft Active Directory Certificate Services -- ad-lab **Home**

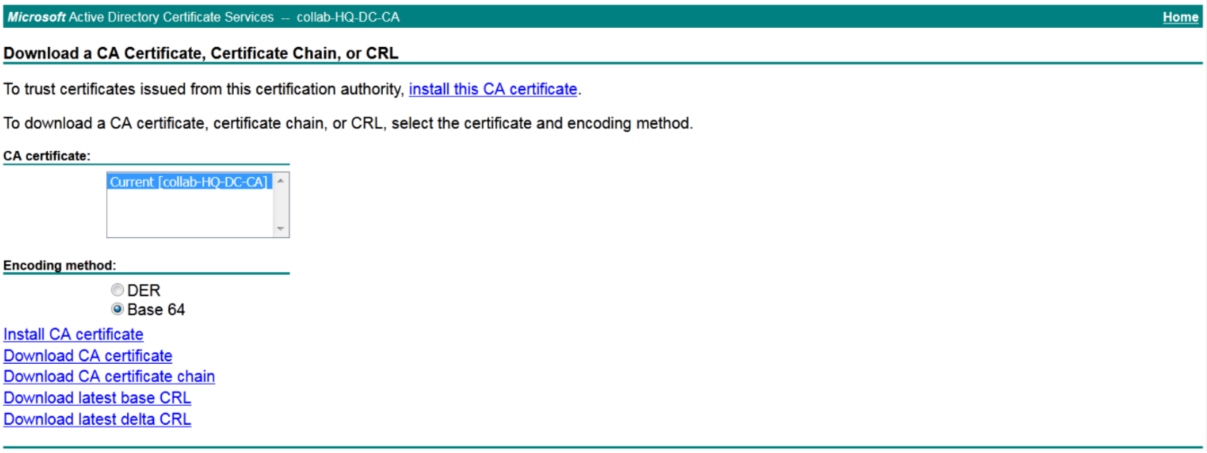
Welcome

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



Microsoft Active Directory Certificate Services -- collab-HQ-DC-CA **Home**

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

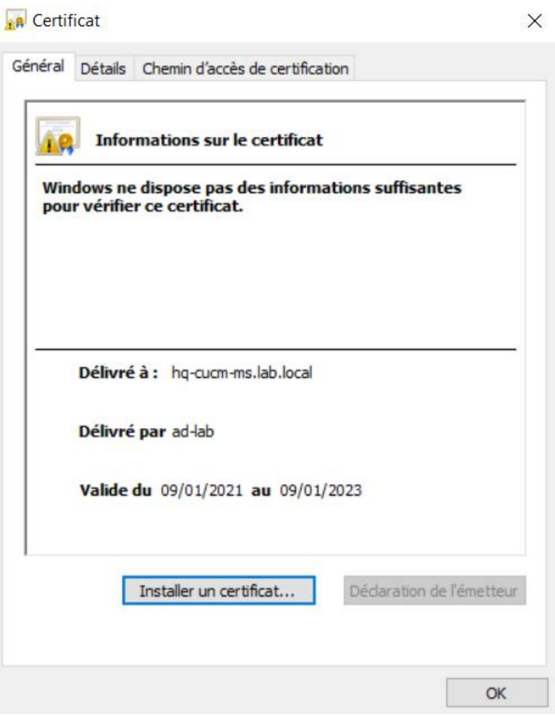
Current [collab-HQ-DC-CA]

Encoding method:

○ DER
● Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Below the **HQ-CUCM** certificate with the appropriate SANs.



Certificat

Général | Détails | Chemin d'accès de certification

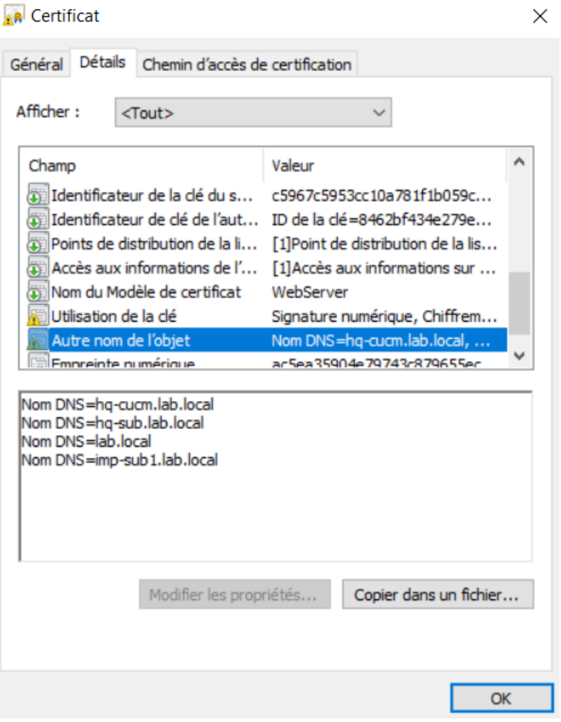
Informations sur le certificat

Windows ne dispose pas des informations suffisantes pour vérifier ce certificat.

Délivré à : hq-cucm-ms.lab.local

Délivré par ad-lab

Valide du 09/01/2021 **au** 09/01/2023



Certificat

Général | Détails | Chemin d'accès de certification

Afficher : <Tout>

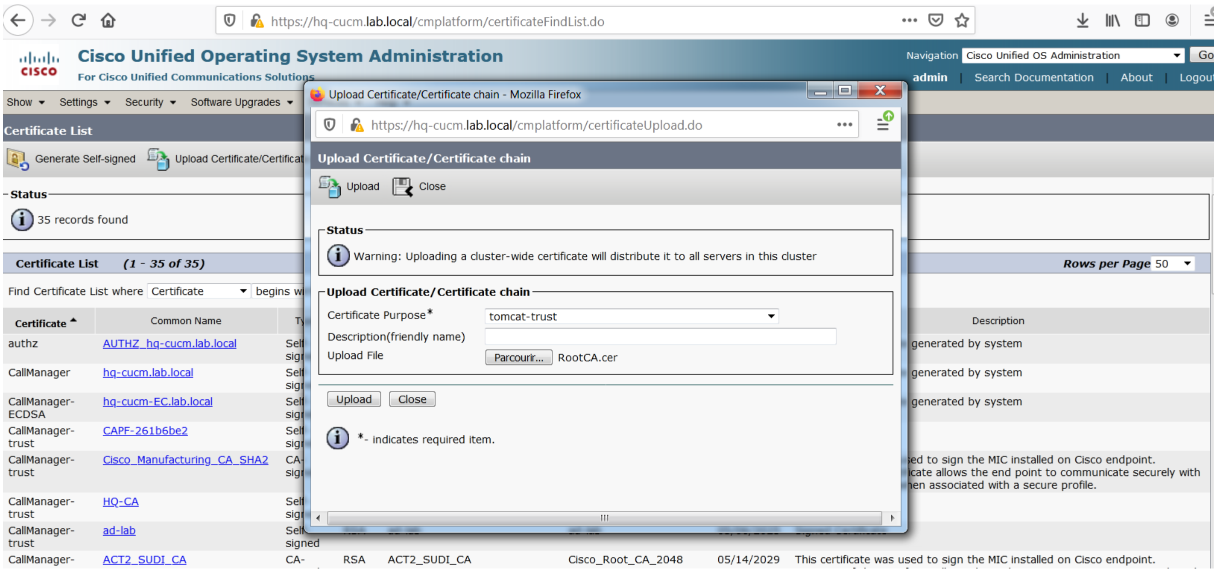
Champ	Valeur
Identificateur de la clé du s...	c5967c5953cc10a781f1b059c...
Identificateur de clé de l'aut...	ID de la clé=8462bf434e279e...
Points de distribution de la li...	[1]Point de distribution de la lis...
Accès aux informations de l'...	[1]Accès aux informations sur ...
Nom du Modèle de certificat	WebServer
Utilisation de la clé	Signature numérique, Chiffrem...
Autre nom de l'objet	Nom DNS=hq-cucm.lab.local, ...
Empreinte numérique	ac5ea35904e79743c879655ec

Nom DNS=hq-cucm.lab.local
Nom DNS=hq-sub.lab.local
Nom DNS=lab.local
Nom DNS=imp-sub1.lab.local

Uploading the Certificates to Cisco Unified Communication Manager.

From the **Certificate Management** page, click Upload Certificate/Certificate Chain.

First you need to upload the CA certificate. Select **Tomcat-trust** from the **Certificate Purpose** and click **Choose file**. Select the CA certificate downloaded previously.



https://hq-cucm.lab.local/cmplatform/certificateFindList.do

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration

Go
admin | Search Documentation | About | Logout
Show
Settings
Security
Software Upgrades

Certificate List

Generate Self-signed
Upload Certificate/Certificat

Status

35 records found

Certificate List (1 - 35 of 35)

Rows per Page 50

Find Certificate List where Certificate begins wi

Certificate	Common Name	Ty					Description
authz	AUTHZ_hq-cucm.lab.local	Self-sig					generated by system
CallManager	hq-cucm.lab.local	Self-sig					generated by system
CallManager-ECDSA	hq-cucm-EC.lab.local	Self-sig					generated by system
CallManager-trust	CAPF-261b6be2	Self-sig					
CallManager-trust	Cisco_Manufacturing_CA_SHA2	CA-sig					ed to sign the MIC installed on Cisco endpoint. icate allows the end point to communicate securely with hen associated with a secure profile.
CallManager-trust	HQ-CA	Self-sig					
CallManager-trust	ad-lab	Self-signed					
CallManager-	ACT2_SUDI_CA	CA-	RSA	ACT2_SUDI_CA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint.

Upload Certificate/Certificate chain - Mozilla Firefox

https://hq-cucm.lab.local/cmplatform/certificateUpload.do

Upload Certificate/Certificate chain

Status

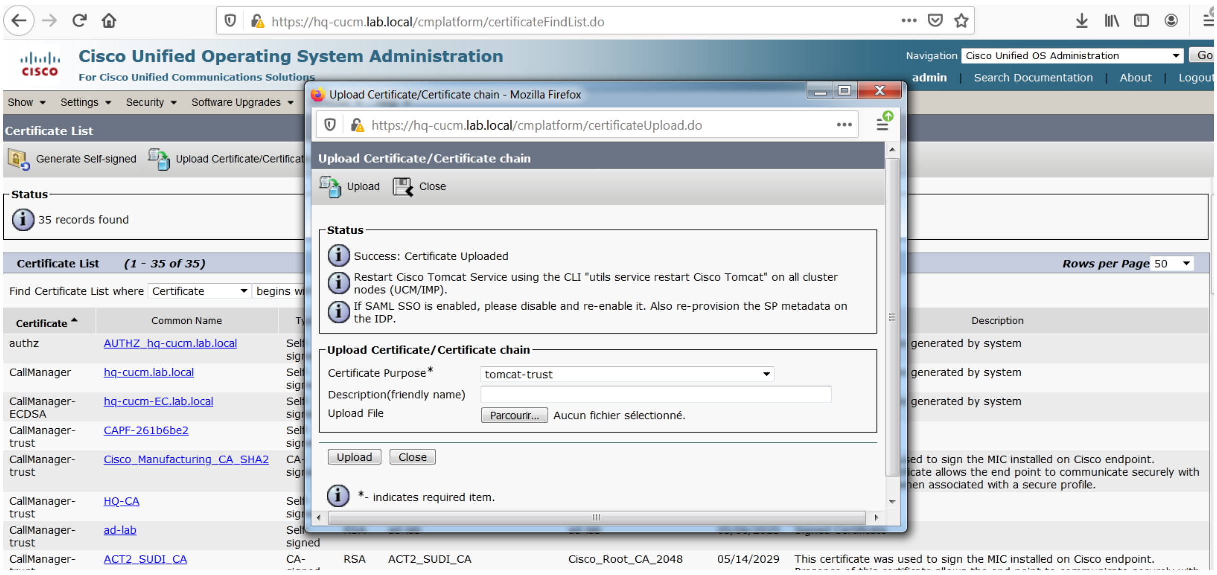
Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*	tomcat-trust
Description(friendly name)	
Upload File	Parcourir... RootCA.cer

*- indicates required item.

The CA certificate is now uploaded.



Upload Certificate/Certificate chain

Status

Success: Certificate Uploaded

Restart Cisco Tomcat Service using the CLI "utils service restart Cisco Tomcat" on all cluster nodes (UCM/IMP).

If SAML SSO is enabled, please disable and re-enable it. Also re-provision the SP metadata on the IDP.

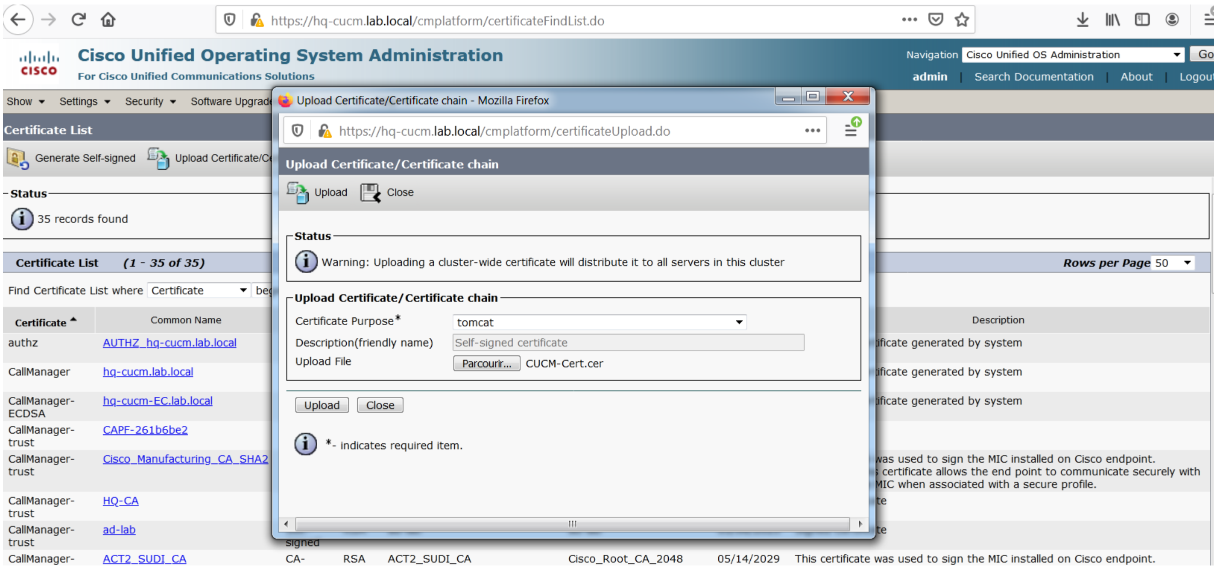
Upload Certificate/Certificate chain

Certificate Purpose*	tomcat-trust
Description(friendly name)	
Upload File	Parcourir... Aucun fichier sélectionné.

*- indicates required item.

Now upload the **HQ-CUCM** certificate. Select **Tomcat** from the **Certificate Purpose** and click **Choose File**.

Select the **HQ-CUCM** certificate created previously.



Upload Certificate/Certificate chain

Status

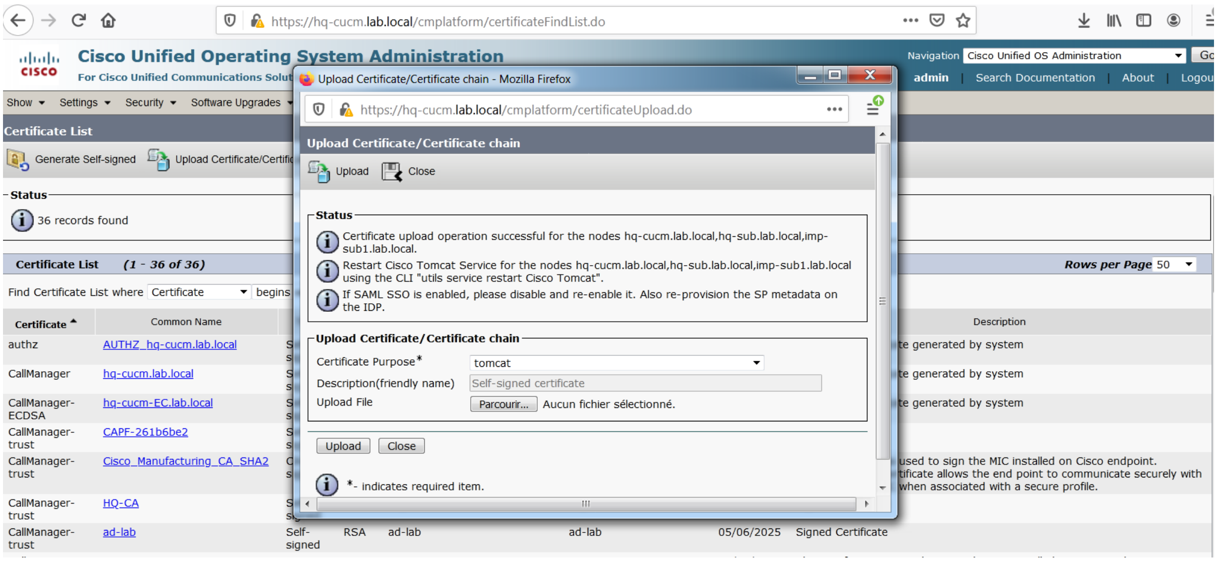
Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*	tomcat
Description(friendly name)	Self-signed certificate
Upload File	Parcourir... CUCM-Cert.cer

*- indicates required item.

The **HQ-CUCM** certificate is now uploaded.



https://hq-cucm.lab.local/cmplatform/certificateFindList.do

Cisco Unified Operating System Administration

For Cisco Unified Communications Solut

Navigation: Cisco Unified OS Administration | admin | Search Documentation | About | Logou

Certificate List

Status

36 records found

Certificate List (1 - 36 of 36) Rows per Page 50

Upload Certificate/Certificate chain - Mozilla Firefox

https://hq-cucm.lab.local/cmplatform/certificateUpload.do

Upload Certificate/Certificate chain

Status

Certificate upload operation successful for the nodes hq-cucm.lab.local,hq-sub.lab.local,imp-sub1.lab.local.

Restart Cisco Tomcat Service for the nodes hq-cucm.lab.local,hq-sub.lab.local,imp-sub1.lab.local using the CLI "utils service restart Cisco Tomcat".

If SAML SSO is enabled, please disable and re-enable it. Also re-provision the SP metadata on the IDP.

Upload Certificate/Certificate chain

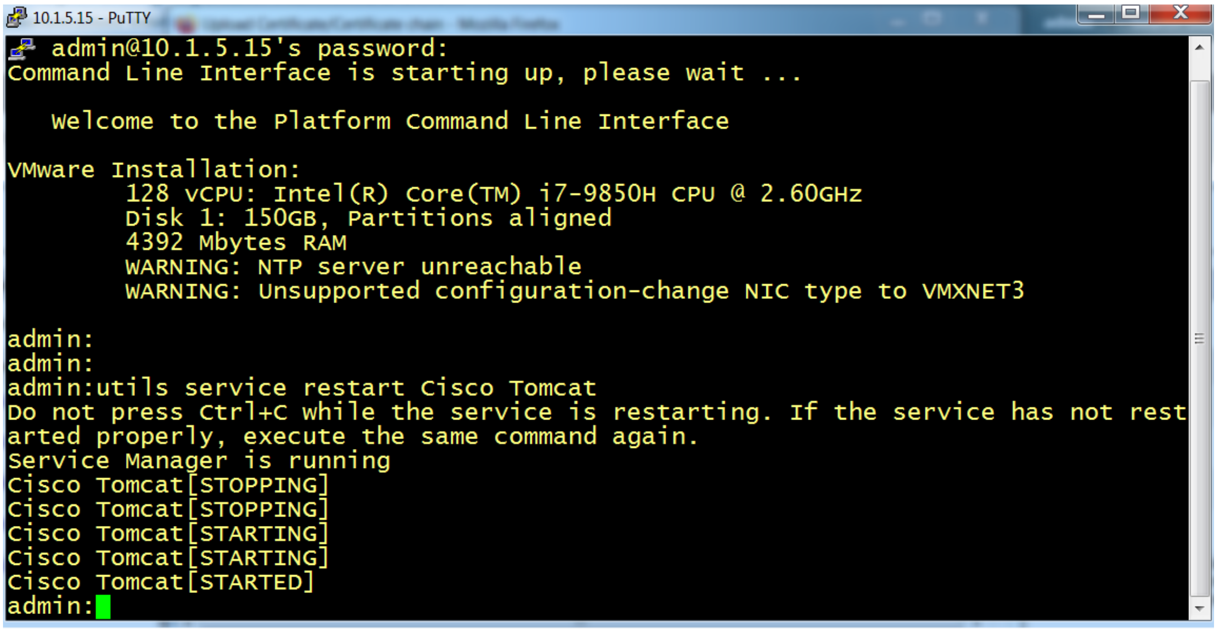
Certificate Purpose*: tomcat

Description(friendly name): Self-signed certificate

Upload File: Parcourir... Aucun fichier sélectionné.

*- indicates required item.

SSH to **HQ-CUCM**, **HQ-SUB** and **imp-sub1** and restart the tomcat service.



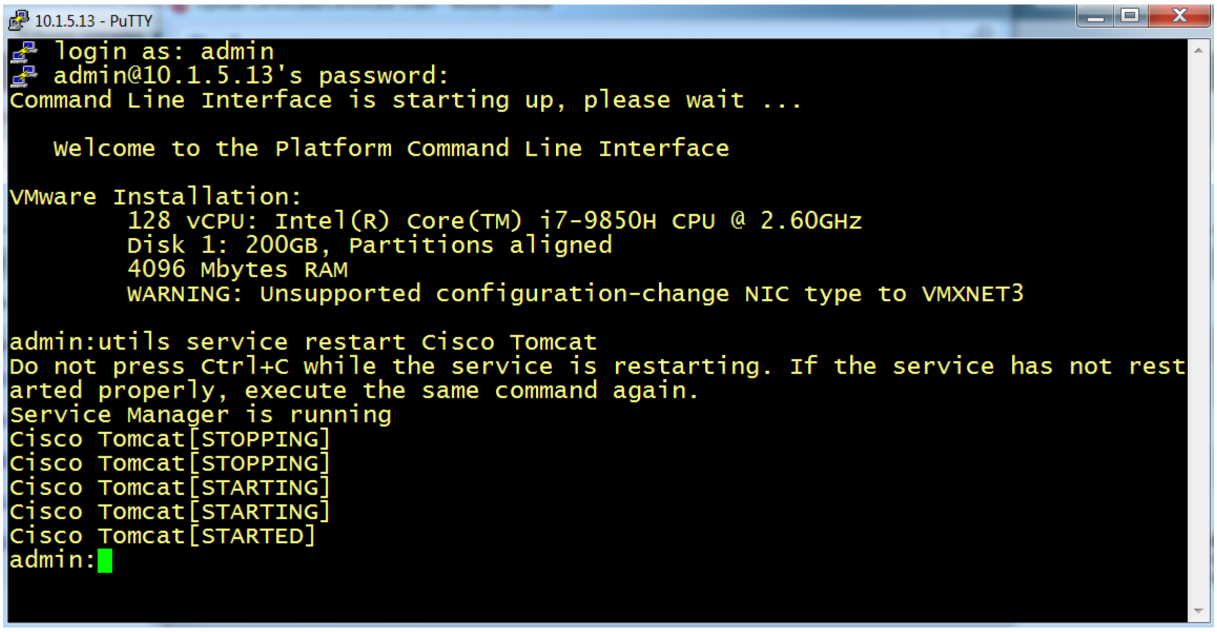
10.1.5.15 - PuTTY

```
admin@10.1.5.15's password:
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        128 vCPU: Intel(R) Core(TM) i7-9850H CPU @ 2.60GHz
        Disk 1: 150GB, Partitions aligned
        4392 Mbytes RAM
        WARNING: NTP server unreachable
        WARNING: Unsupported configuration-change NIC type to VMXNET3

admin:
admin:
admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
arted properly, execute the same command again.
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

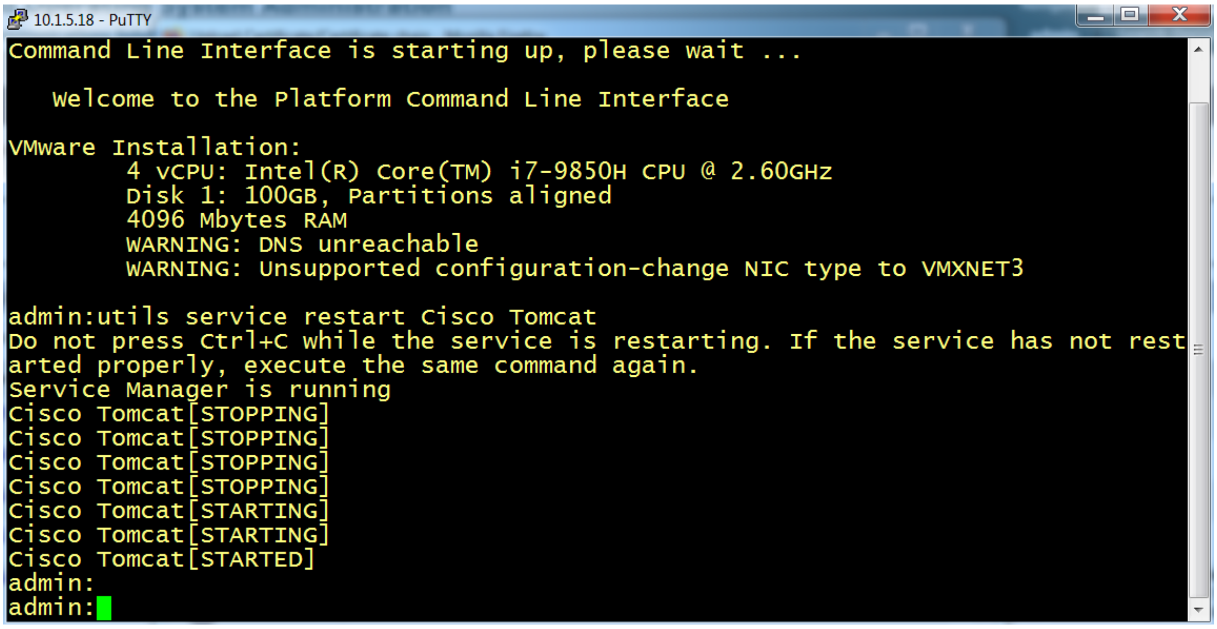


```
login as: admin
admin@10.1.5.13's password:
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        128 vCPU: Intel(R) Core(TM) i7-9850H CPU @ 2.60GHz
        Disk 1: 200GB, Partitions aligned
        4096 Mbytes RAM
        WARNING: Unsupported configuration-change NIC type to VMXNET3

admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
arted properly, execute the same command again.
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```



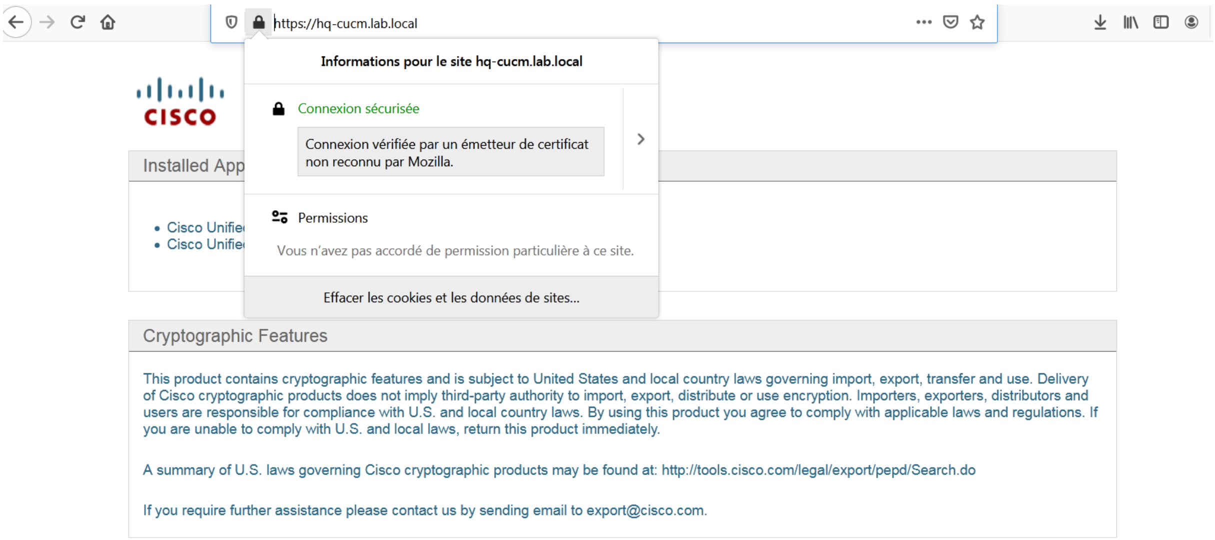
```
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        4 vCPU: Intel(R) Core(TM) i7-9850H CPU @ 2.60GHz
        Disk 1: 100GB, Partitions aligned
        4096 Mbytes RAM
        WARNING: DNS unreachable
        WARNING: Unsupported configuration-change NIC type to VMXNET3

admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
arted properly, execute the same command again.
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
admin:
```

Access the **hq-cucm** GUI using a web browser, now the HTTPS access is secured with a valid certificate, no warning certificate error.



https://hq-cucm.lab.local

Informations pour le site hq-cucm.lab.local

Connexion sécurisée

Connexion vérifiée par un émetteur de certificat non reconnu par Mozilla.

Permissions

Vous n'avez pas accordé de permission particulière à ce site.

Effacer les cookies et les données de sites…

Installed App

- Cisco Unifie
- Cisco Unifie

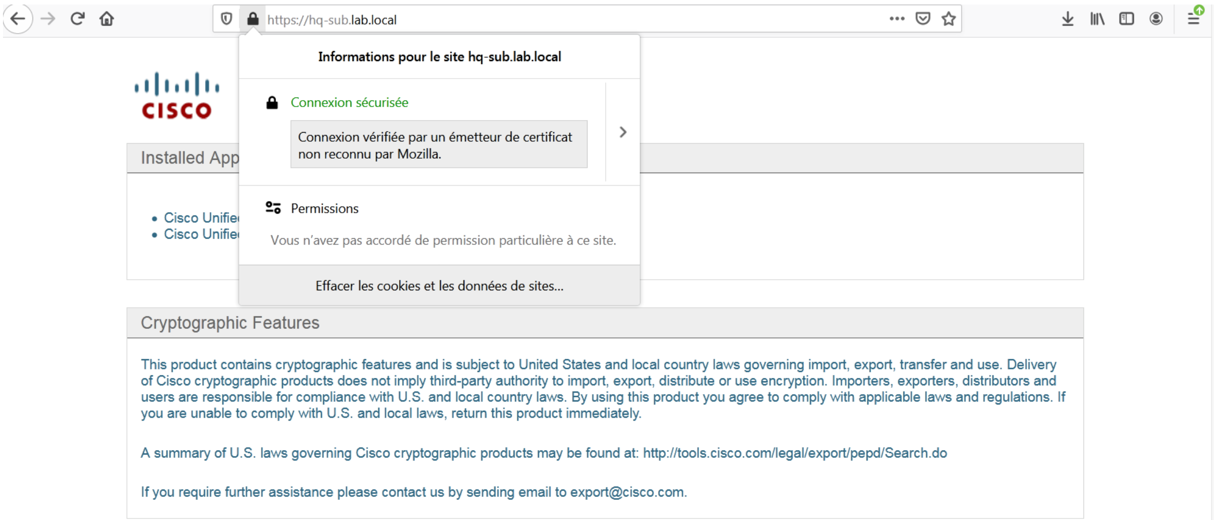
Cryptographic Features

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://tools.cisco.com/legal/export/pepd/Search.do

If you require further assistance please contact us by sending email to export@cisco.com.

Access the **hq-sub** GUI using a web browser, now the HTTPS access is secured with a valid certificate, no warning certificate error.



https://hq-sub.lab.local

Informations pour le site hq-sub.lab.local

Connexion sécurisée

Connexion vérifiée par un émetteur de certificat non reconnu par Mozilla.

Permissions

Vous n'avez pas accordé de permission particulière à ce site.

Effacer les cookies et les données de sites…

Installed App

- Cisco Unifie
- Cisco Unifie

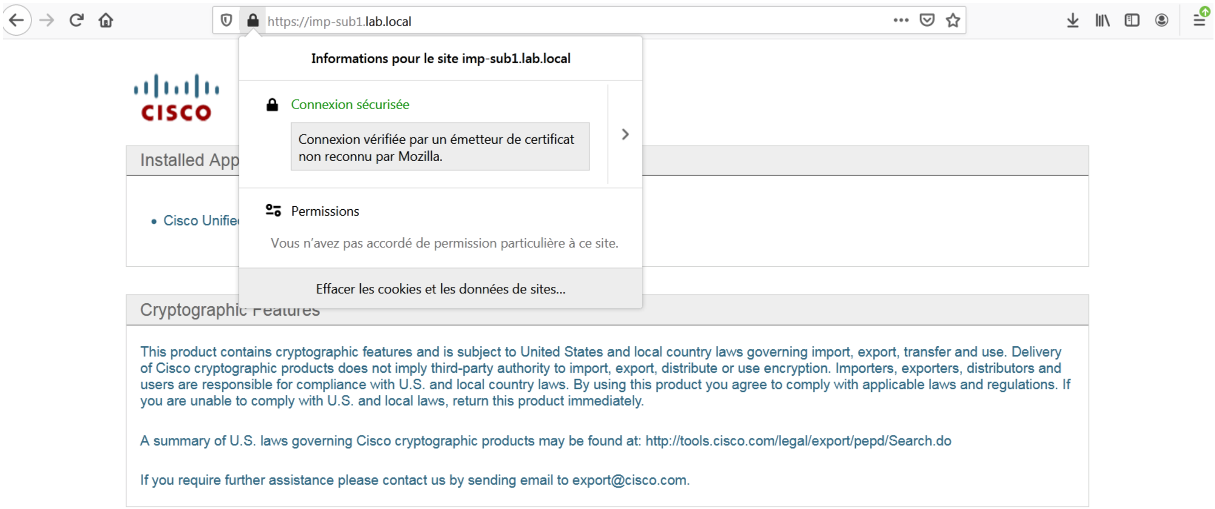
Cryptographic Features

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://tools.cisco.com/legal/export/pepd/Search.do

If you require further assistance please contact us by sending email to export@cisco.com.

Access the **imp-sub1** GUI using a web browser, now the HTTPS access is secured with a valid certificate, no warning certificate error.



https://imp-sub1.lab.local

Informations pour le site imp-sub1.lab.local

Connexion sécurisée

Connexion vérifiée par un émetteur de certificat non reconnu par Mozilla.

Permissions

Vous n'avez pas accordé de permission particulière à ce site.

Effacer les cookies et les données de sites…

Installed App

- Cisco Unifie

Cryptographic Features

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://tools.cisco.com/legal/export/pepd/Search.do

If you require further assistance please contact us by sending email to export@cisco.com.