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**.

(←) → G	۵ 🛛 🔒	https://hq-c	ucm.la	o.local/cmplatform/certificateFin	dList.do								
Initiality Cisco Unified Operating System Administration Gisco Unified Communications Solutions For Cisco Unified Communications Solutions admin Search Documentation About Logor 													
Show - Setting	Show + Settings + Security + Software Upgrades + Services + Help +												
Certificate List													
🙀 Generate Self-signed 👜 Upload Certificate/Certificate chain 🔋 Generate CSR													
- Status													
i 34 records found													
Certificate Lis	Cartificata List (1 - 24 of 34)												
Find Certificate L	list where Certificate 👻 be	gins with 🔻	•	Find	lear Filter 🕀 📼								
Certificate 🔺	Common Name	Туре	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	hg-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	<u>ad-lab</u>	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	e Signing Request		
Generate 🖳 C	lose		
-			
Status			
Warning: Gener	ating a new CSR for a specific certific	cate type will overwrite the exis	sting CSR for that type
Generate Certificate	e Signing Request		
Certificate Purpose*	tomcat	▼	
Distribution*	Multi-server(SAN)	•	
Common Name*	hq-cucm-ms.lab.local		
Subject Alternate N	lames (SANs)		
Auto-populated	hq-cucm.lab.local		
Domains	hq-sub.lab.local		
	imp-sub1.lab.local		
		-	
Parent Domain	lab.local		
Other Domains			Parcourir Aucun fichier sélectionné.
			Please import .TXT file only.
			fiedbe import from the only.
			+ Add
Key Type**	RSA		
Key Length*	2048	•	
Hash Algorithm*	SHA256	▼	
Generate Close			
C C C C C C C C C C C C C C C C C C C		111	•

Generate Certificat	e Signing Request		
🔃 Generate	Close		
Status			
i Success: Certifi	cate Signing Request Generated		
CSR export op	eration successful on the nodes [ha-cucm.la	b.local, hg-sub.lab.lo	ocal, imp-sub1.lab.local].
•			
Generate Certificat	e Signing Request		
Certificate Purpose*	tomcat	•	
Distribution*	Multi-server(SAN)	•	
Common Name*	hq-cucm-ms.lab.local		
Subject Alternate	Names (SANs)		
Auto-populated	hq-cucm.lab.local	*	
Domano	hq-sub.lab.local		
		÷	
Parent Domain	lab.local		
Other Domains			Parcourir Aucun fichier sélectionné.
			Please import .TXT file only.
		-	
			+ Add
Key Type**	RSA		
Key Length*	2048	•	
Hash Algorithm*	SHA256	•	

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

(←) → C'	û 🛛 🖗	https://ho	q-cucm.la	ab.local/cmplatform/certificateFir	ndList.do		···· 🖂 🚽 🕅 🗉 🛎					
cisco For	sco Unified Operatin Cisco Unified Communications Sol	g Syste	em Ad	Iministration			Navigation Gisco Unified OS Administration • G admin Search Documentation About Logou					
Show - Setting	s 🔹 Security 👻 Software Upgrades	 Service 	es 🕶 He	ip 🕶								
Certificate List												
Generate Se	If-signed Dipload Certificate/Cert	tificate chain	💽 Ge	enerate CSR 🔋 Download CSR								
Status	Status i 35 records found											
Certificate Lis	t (1 - 35 of 35)						Rows per Page 50 💌					
Find Certificate L	ist where Certificate	ns with 🔻		Find Clear	r 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	hg-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	X
🛛 🕼 https://hq-cucm.lab.local/cmplatform/certificateDownloadNewCsr.do	 ≞
Download Certificate Signing Request	
Download CSR The Close	
Status Certificate names not listed below do not have a corresponding CSR Download Certificate Signing Request Certificate Purpose* tomcat	
Download CSR Close (i) *- 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.



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

← → ♂ +	ŵ	🛛 🔏 ad-lab.lab.local/certsrv/d	ertrqxt.asp		⊡ ☆	$\overline{\mathbf{A}}$	lii\ 🖸	⊛ ≟		
Microsoft Active	Directory Certificate Serv	vices ad-lab						Home		
Submit a Certificate Request or Renewal Request										
To submit a sa box.	aved request to the C	A, paste a base-64-encoded	CMC or PKCS #10 certificate request or PK	CS #7 renewal request generated by an	external source (such as a Web serve	er) in the Sa	aved Requ	Jest		
Saved Request:										
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	6McPQVF065FwAcZmd] 0CXtDDE+JuioIvYMAH UpZnj7Vwj6Bietw4U ndDHPP3Ts57zslQEN END CERTIFIC 4 III	LpVSkBN3U0+bgSRqofracOP KHNjIWalvHSQXEYFE/INS Ls06aD9acLUtTUTRC011g (9d4ij1DBpTqk4sp0s= VTE REQUEST								
Certificate Templ	late:									
	Web Server	•								
Additional Attrib	utes:									
Attributes:		Â								
		Submit >								

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

← → C' û	0 🔏 ad-lab.lac.l/certsrv/certfnsh.asp	⊌ ☆	⊻ ∥\ 🗊 🛎 🖆
Microsoft Active Directory Certificate	Services ad-lab		Home
Certificate Issued			
The certificate you requested w	vas issued to you.		
○ DER encoded or <u>Download certificate</u> <u>Download certificate</u>	Base 64 encoded 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**.

\leftarrow \rightarrow C \textcircled{a}	🖸 🔏 10.1.5.19/certsrv/			⊠ ☆	$\overline{\mathbf{A}}$	III\ C		≡			
Microsoft Active Directory Certificate	Services ad-lab							<u>Home</u>			
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	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 fro	om this certification authority, install this CA certificate.										
To download a CA certificate	, certificate chain, or CRL, select the certificate and encodi	ing method.									
CA certificate:	HQ-DC-CA]										
Encoding method:											
Base 64											
Install CA certificate Download CA certificate Download CA certificate cha Download latest base CRL Download latest delta CRL	in										

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



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.

← → ♂	۵	🛛 🔒 http	os://hq-	-cucm.lab.local/cmplatfo	orm/ce	ertificateFind	dList.do						••	• 🛛	☆		$\overline{\mathbf{A}}$	111\	=	۲	=
cisco _{Fo}	isco Unified O	perating	Syst	ystem Administration								lavigati admin	on <mark>Cis</mark>	ico Unified OS Gearch Docum	Administr entation	ation	bout	• [Go gou		
Show - Setting	is ▼ Security ▼ Softw	are Upgrades 👻	- 😐 י	Upload Certificate/Certificat	e chain	n - Mozilla Fire	efox					1 X									
Certificate List			0	🕽 🖍 https://hq-cucm.	lab.lo	cal/cmplatfo	orm/certific	ateUpload.d	lo		••	• =	0								
Generate Se	elf-signed 🐴 Upload (Certificate/Certific	cat Up	oload Certificate/Certil	ficate	chain															
- Status			E.	👌 Upload 🛛 🖳 Close																	_
i 35 records	s found		s	Status																	
Certificate Lis	st (1 - 35 of 35)			i) Warning: Uploading a	a cluste	er-wide certif	ficate will dis	tribute it to a	all servers i	in this clu	ister						Rows	per I	Page 5	io 🔻	
Find Certificate I	List where Certificate	▼ begins	w ru	Jpload Certificate/Certi	ficate	chain ——							٦ 🛛								
Certificate 📩	Common Nam	e	ту	Certificate Purpose*	to	omcat-trust				•					D	escription					
authz	AUTHZ_hq-cucm.lab.	local S	Self	Description(friendly name) Ipload File		Parcourir R	PootCA car							genera	ted by	system					
CallManager	hg-cucm.lab.local	S					COUCA.CEI							genera	ted by	system					
CallManager- ECDSA	hq-cucm-EC.lab.local	S	Sell	Upload Close										genera	ted by	system					
CallManager- trust	CAPF-261b6be2	S	Sell (*- indicates required 	item.																
CallManager- trust	<u>Cisco_Manufacturing</u>	CA SHA2 C si	CA- ligr											ed to s cate all ien ass	ign th ows th ociate	e MIC installe ne end point t d with a secu	d on Cisc o commu re profile.	o end unicate	point. e secur	ely wit	ch
CallManager- trust	<u>HQ-CA</u>	S	Self ligr 4				111						•								
CallManager- trust	ad-lab	S	self	100.00	-	_		_		,		-									
CallManager-	ACT2_SUDI_CA	C	CA-	RSA ACT2_SUDI_C	A		Cisco_Root	t_CA_2048	05/14	/2029	This certif	icate wa	as us	ed to s	ign th	e MIC installe	d on Cisc	o end	point.		

The CA certificate is now uploaded.

← →	<u>۵</u>	🛡 🔒 https://	/hq-cucm. lab.local /cmplat	form/certificate	eFindList.do					🗵	9 ☆	7	: III\		۲	=
cisco Fo	Sisco Unified Op or Cisco Unified Communic	erating Stations Solution	ystem Administration								ition <mark>Ci</mark>	sco Unified OS Adminis Search Documentatio	stration	About	▼ u	Go
Show - Setting	gs - Security - Softwar	e Upgrades 👻	Upload Certificate/Certific	ate chain - Mozill	la Firefox				x							
Certificate Lis	t		🛛 🕼 https://hq-cucr	n. lab.local /cmp	olatform/certificatel	Jpload.do		•••	- @							
Generate S	Self-signed 🌇 Upload Cer	rtificate/Certificat	Upload Certificate/Cert	ificate chain					^							
Status			Dpload 🖳 Close													-
35 record	Is found		⊤ Status													
Certificate Li	ist (1 - 35 of 35)		Success: Certificate Uploaded Restart Cisco Tomcat Service using the CLI "utils service restart Cisco Tomcat" on all cluster						Rows per Page 50 V							
Find Certificate	List where Certificate	 begins with 	If SAML SSO is ena	oled, please disa	able and re-enable it.	Also re-provisio	on the SP me	etadata on		_						
Certificate 🕇	Common Name	Ty	the IDP.						=		C	Description				
authz	AUTHZ_hq-cucm.lab.loc	al Self sigr	Upload Certificate/Cer	tificate chain –					- 11	gener	rated by	y system				
CallManager	hq-cucm.lab.local	Self	Certificate Purpose*	tomcat-tru	ust		-			gener	rated by	y system				
CallManager- ECDSA	hq-cucm-EC.lab.local	Self	Description(friendly nam Upload File	Parcourir	Aucun fichier sélec	ctionné.				gener	rated by	y system				
CallManager- trust	CAPF-261b6be2	Self		<u></u>												
CallManager- trust	Cisco_Manufacturing_C	A <u>SHA2</u> CA- sigr	Upload Close							ed to icate a nen as	sign th allows t ssociate	he MIC installed on Ci he end point to com d with a secure prof	sco en nunica ile.	dpoint. te secu	rely with	
CallManager- trust	HQ-CA	Self	1 *- indicates require	d item.					-							
CallManager- trust	<u>ad-lab</u>	Sell	ed	_			.,,			J						
CallManager-	ACT2_SUDI_CA	CA-	RSA ACT2_SUDI_	CA	Cisco_Root_CA	_2048 05	5/14/2029	This certificat	e was u	ised to	sign th	e MIC installed on Ci	sco en	dpoint.		

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

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

← → ⊂	۵	0 🔒	https://hq-cucm. lab.local /cmpl	atform/certificateFi	indList.do			⊍	☆	$\overline{\mathbf{A}}$	\ ⊡	<u>ا</u>
cisco _{Fo}	isco Unified Op r Cisco Unified Communic	peratir	ng System Administ	ration				Navigati admin	on Cisco Unified OS	Administration	ation About	✓ Go t Logou [*]
Show - Setting	is ▼ Security ▼ Softwar	are Upgrade	😉 Upload Certificate/Certificate c	hain - Mozilla Firefox			- 🗆 🗙					
Certificate List	:		🛛 🖗 https://hq-cucm.la	.local/cmplatform/	/certificateUpload.do		●					
Generate Se	elf-signed 🐴 Upload Ce	ertificate/Ce	Upload Certificate/Certific	ate chain								
- Status		_	Dipload 🕎 Close									
i 35 records	found	_	Status									
Certificate Lis	st (1 - 35 of 35)		Warning: Uploading a cl	uster-wide certificate	e will distribute it to all ser	vers in this cluster				Rows	per Page	50 🔻
Find Certificate I	List where Certificate	▼ beç	Upload Certificate/Certific	ate chain								
Certificate 📤	Common Name		Certificate Purpose*	tomcat		•			Description			
authz	AUTHZ_hg-cucm.lab.log	ocal	Description(friendly name)	Self-signed certifica	ate			lificate genera	ted by system			
CallManager	hq-cucm.lab.local		Upload File	Parcourir CUCM	M-Cert.cer			ificate genera	ted by system			
CallManager- ECDSA	hq-cucm-EC.lab.local		Upload Close					ificate genera	ted by system			
CallManager- trust	CAPF-261b6be2		(i) *- indicates required ite	em.								
CallManager- trust	Cisco_Manufacturing_C	CA_SHA2	U					was used to s certificate all MIC when ass	ign the MIC install ows the end point ociated with a secu	d on Cisc to commu ure profile.	o endpoint inicate sec	urely with
CallManager- trust	HQ-CA							te				
CallManager- trust	ad-lab	l	signed				Þ	te				
CallManager-	ACT2_SUDI_CA		CA- RSA ACT2_SUD	I_CA	Cisco_Root_CA_2048	05/14/2029	This certificate	was used to s	ign the MIC install	d on Cisc	o endpoint	

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

\leftarrow \rightarrow C \textcircled{a} $\boxed{0}$ \textcircled{b} http://www.eta	s://hq-cucm. lab.local /cmplatform/certificateFindList.do	⊠ ☆ ⊻ Ⅲ\ ⊡ ◎ =
Cisco Unified Operating For Cisco Unified Communications Solution	System Administration	Navigation Cisco Unified OS Administration Gamma G
Show - Settings - Security - Software Upgrades -	🛛 🔥 https://hq-cucm.lab.local/cmplatform/certificateUpload.do 🛛 😶	
Certificate List	Upload Certificate/Certificate chain	
Generate Sen-signed	Upload 🖳 Close	
36 records found	Status	
Certificate List (1 - 36 of 36)	Restart Cisco Tomcat Service for the nodes hq-cucm.lab.local,hq-sub.lab.local,imp-sub1.lab.local	Rows per Page 50 🔻
Find Certificate List where Certificate	If SAML SSO is enabled, please disable and re-enable it. Also re-provision the SP metadata on	
Certificate Common Name		Description
authz <u>AUTHZ_hq-cucm.lab.local</u> S	Upload Certificate/Certificate chain	te generated by system
CallManager <u>hq-cucm.lab.local</u> S	Certificate Purpose tomcat	te generated by system
CallManager- <u>hq-cucm-EC.lab.local</u> S ECDSA S	Upload File Parcourir Aucun fichier sélectionné.	te generated by system
CallManager- CAPF-261b6be2 Strust	Upload Close	
CallManager- <u>Cisco Manufacturing CA SHA2</u> C trust s	(i) *- indicates required item.	used to sign the MIC installed on Cisco endpoint. tificate allows the end point to communicate securely with when associated with a secure profile.
CallManager- HQ-CA S trust s		
CallManager- <u>ad-lab</u> S trust s	elf- RSA ad-lab 05/06/2025 Signed Certificate Igned	

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



<pre>_ login as: admin _ admin@10.1.5.13's password: Command line Interface is starting up, please wait</pre>
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[STARTING] Cisco Tomcat[STARTED] admin:



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

\leftrightarrow > C $$	Ū	https://hq-cucm.lab.local		⊠ ☆	± III\ ⊡ ⊜						
		Informations pour le site hq-cucm.lab.local									
	CISCO Installed App	Connexion sécurisée									
		Connexion vérifiée par un émetteur de certificat non reconnu par Mozilla.	>								
	Cisco Unifier Cisco Unifier	25 Permissions Vous n'avez pas accordé de permission particulière à ce	site.								
		Effacer les cookies et les données de sites									
	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 furth	ner assistance please contact us by sending email to exp	oort@cis	co.com.							

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

← → ♂ ✿	Ū	🔒 htt	:ps://hq-sub. lab.local		⊍ ☆	$\underline{+}$	111	=	۲	- 0
			Informations pour le site hq-sub.lab.local							
	CISCO	۵	Connexion sécurisée							
			Connexion vérifiée par un émetteur de certificat non reconnu par Mozilla.	>						
	Cisco Unifie Cisco Unifie	25 Vo	Permissions ous n'avez pas accordé de permission particulière à ce	site.						
			Effacer les cookies et les données de sites							
	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 fur	rther as	sistance please contact us by sending email to exp	ort@ci	;co.com.					

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

← → ♂ ଢ		https://imp-sub1.lab.local		··· ⊠ ☆	: 1	11\	۲	- 0
		Informations pour le site imp-sub1.lab.local						
		 Connexion sécurisée Connexion vérifiée par un émetteur de certificat non reconnu par Mozilla. 	>					
	Cisco Unifier	Permissions Vous n'avez pas accordé de permission particulière à ce sit	e.					
	Cryptographic This product conte of Cisco cryptogra users are respons you are unable to A summary of U.S If you require furth	Effacer les cookies et les données de sites reatures ains cryptographic features and is subject to United States aphic products does not imply third-party authority to import sible for compliance with U.S. and local country laws. By us comply with U.S. and local laws, return this product immed S. laws governing Cisco cryptographic products may be fou her assistance please contact us by sending email to export	and lo , expo ing th liately nd at: t@cis	cal country laws governing import, export, transfer and use. Delivery rt, distribute or use encryption. Importers, exporters, distributors and is product you agree to comply with applicable laws and regulations. If http://tools.cisco.com/legal/export/pepd/Search.do co.com.				