# Create Windows CA Certificate Templates for CUCM

### Contents

Introduction Prerequisites Requirements Components Used Background information Configure Callmanager / Tomcat / TVS Template IPsec Template CAPF Template Generate a Certificate Signing Request Verify Troubleshoot

### Introduction

This document describes a step-by-step procedure in order to create certificate templates on Windows Server-based Certification Authorities (CA), that are compliant with X.503 extension requirements for every type of Cisco Unified Communications Manager (CUCM) certificate.

### Prerequisites

#### Requirements

Cisco recommends that you have knowledge of these topics:

- CUCM version 11.5(1) or later
- Basic knowledge of Windows Server administration is also recommended

#### **Components Used**

The information in this document is based on these software and hardware versions:

- The information in this document is based on CUCM Version 11.5(1) or later.
- Microsoft Windows Server 2012 R2 with CA services installed.

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**

There are five types of certificates that can be signed by an external CA:

Certificate	Use Presented at secure device registration, can sign Certificate	Impacted Services
Callmanager	Trust List (CTL)/Internal Trust List (ITL) files, used for secure interactions with other servers such as secure Session Initiation Protocol (SIP) Trunks.	<ul> <li>Cisco Call Manager</li> <li>Cisco CTI Manager</li> <li>Cisco TFTP</li> </ul>
tomcat	Presented for Secure Hypertext Transfer Protocol (HTTPS) interactions.	<ul> <li>Cisco Tomcat</li> <li>Single Sign-On (SSO)</li> <li>Extension Mobility</li> <li>Corporate Directory</li> </ul>
ipsec	Used for backup file generation, as well as IP Security (IPsec) interaction with Media Gateway Control Protocol (MGCP) or H323 gateways.	Cisco DRF Master     Cisco DRF Local
CAPF	Used to generate Locally Significant Certificates (LSC) for phones.	<ul> <li>Cisco Certificate Authority Proxy Function</li> </ul>
TVS	Used to create a connection to the Trust Verification Service (TVS), when the phones are not able to authenticate an unknown certificate.	·Cisco Trust Verification Service

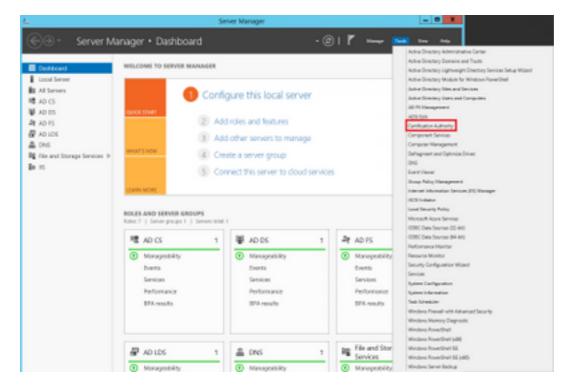
Each of these certificates has some X.509 extension requirements that need to be set, otherwise, you can encounter misbehaviours on any of the aforementioned services:

Certificate	X.509 Key Usage	X.509 Extended Key Usage
Callmanager	<ul> <li>Digital Signature</li> <li>Key Encipherment</li> <li>Data Encipherment</li> </ul>	Web Server Authentication     Web Client Authentication
tomcat	<ul> <li>Digital Signature</li> <li>Key Encipherment</li> <li>Data Encipherment</li> </ul>	Web Server Authentication     Web Client Authentication
ipsec	<ul> <li>Digital Signature</li> <li>Key Encipherment</li> <li>Data Encipherment</li> </ul>	Web Server Authentication     Web Client Authentication     IPsec End System
CAPF	<ul> <li>Digital Signature</li> <li>Certificate Sign</li> <li>Key Encipherment</li> </ul>	<ul> <li>Web Server Authentication</li> <li>Web Client Authentication</li> </ul>
TVS	<ul> <li>Digital Signature</li> <li>Key Encipherment</li> <li>Data Encipherment</li> </ul>	Web Server Authentication     Web Client Authentication

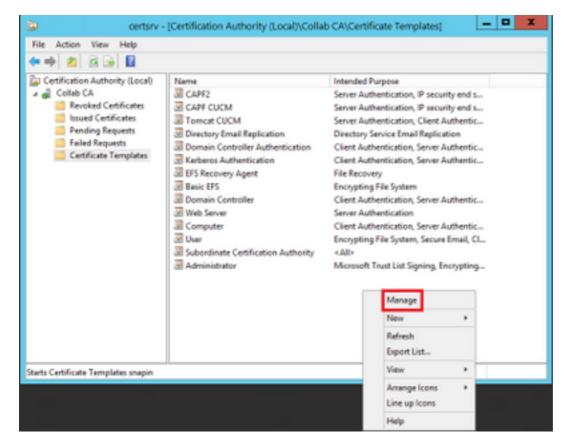
For more information, reference the Security Guide for Cisco Unified Communications Manager

### Configure

Step 1. On the Windows Server, navigate to **Server Manager > Tools > Certification Authority**, as shown in the image.



Step 2. Select your CA, then navigate to **Certificate Templates**, right-click on the list and select **Manage**, as shown in the image.



Callmanager / Tomcat / TVS Template

The next images display only the creation of the CallManager template; but the same steps can be followed for creating the certificate templates for the Tomcat and the TVS services. The only difference is to ensure the respective service name is used for each new template during step 2.

Step 1. Find the **Web Server** template, right-click on it and select **Duplicate Template**, as shown in the image.

3		0	ertificate Te	mplates (	Console	
File Action View Help						
🗰 🗰 🖾 🗟 🔝 📷						
ertificate Templates (win/12.collab.m	Template Display Name	Schema Version	Versi	Intended	Purposes	
	Workstation Authentication	2	101.0	Client Au	thertication	
	Web Server	1	4.1	_		_
	User Signature Only	1	4.1		<b>Duplicate Template</b>	
	3 User	1	3.1		All Tasks	
	Trust List Signing	1	3.1		Properties	
	Tomcat CUCM	2	100.3	Serve		
	Subordinate Certification Authority	1	5.1		Help	
	Smartcard User	1	11.1	-		_
	Smartcard Logon	1	6.1			
	Router (Offline request)	1	4.1			
	Root Certification Authority	1	5.1			
	RAS and IAS Server	2	101.0	Client Au	athentication, Server Authen	tication (

Step 2. Under **General**, you can change the certificate template's name, display name, validity, etc.

Properties of New Template								
Subject Name	Ser	ver	Issuance	Requirements				
Superseded Templa	tes	Ede	ensions	Security				
Compatibility General	Request	Handling	Cryptography	Key Attestation				
Template display name:								
CallManager CUCM								
Template name: CallManager CUCM Validity period: 5 years V	CallManager CUCM Validity period: Renewal period:							
Publish certificate in Do not automatic Directory			cate certificate	exists in Active				
OK	(	Cancel	Apply	Help				

Step 3. Navigate to **Extensions > Key Usage > Edit**, as shown in the image.

	Pro	perties	of New	Template		X			
	Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements								
		Templates Extensions Security							
To modify an extension, select it, and then click Edit. Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Issuance Policies Key Usage									
Description of	of Key Usag	pe:			Edt				
Signature re Digital signa Allow key es Critical exter	ture (change or		ry encryptic	m		< >			
[	ОК		Cancel	Apply	В	elp			

Step 4. Select these options and select **OK**, as shown in the image.

- Digital signature
- Allow key exchange only with key encryption (key encipherment)
- Allow encryption of user data

	Properties of New Template	x
Compatibility Gene Subject Name	eral Request Handling Cryptography Key Attestation Server Issuance Requirements	n
	Edit Key Usage Extension	¢
extension. Signature Digital signatu Signature is p Certificate sig	roof of origin (nonrepudiation)	
<ul> <li>Allow key ex</li> </ul>	change without key encryption (key agreement) change only with key encryption (key encipherment) encryption of user data	
Make this exter	nsion critical OK Cancel	]
	OK Cancel Apply Help	

Step 5. Navigate to Extensions > Application Policies > Edit > Add, as shown in the image.

	Pro	perties of	New	Template	X
Compatibility	General	Request Ha	anding	Cryptography	Key Attestation
Subject N	lame	Server		Issuance R	equirements
Supersec	ded Templa	tes	Exte	nsions	Security
To modify an	extension	, select it, and	d then c	lick Edit.	
1		his template:			
	ion Policies				
2000	onstraints	. Information			
2000	e Policies	e Information			
Key Usa					
					Edit
Description of		on Policies:			
Server Auth	entication				^
					~
	OK	Car	ncel	Apply	Help

Edit Applicatio	on Policies E	tension 🗶				
An application policy def used.	înes how a certi	ficate can be				
Application policies:						
Server Authentication	Server Authentication					
Add	Edit	Remove				
Make this extension	critical					
	OK	Cancel				

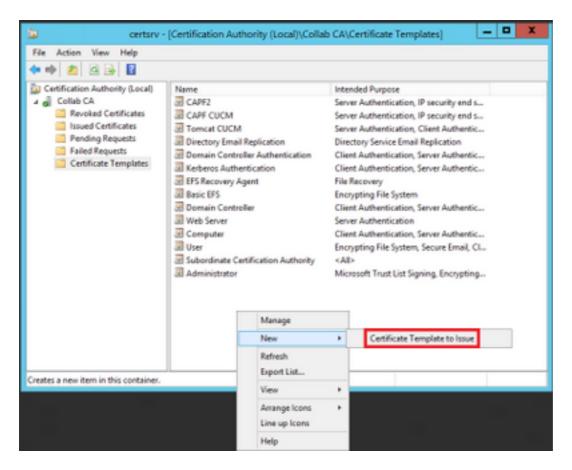
Step 6. Search for **Client Authentication**, select it and select **OK** on both this window and the previous one, as shown in the image.

Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements S Fully Application Policy
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Application policies:
New OK Cancel
OK Cancel Apply Help

Step 7. Back on the template, select Apply and then OK.

Pr	operties of New	/ Template	X				
Compatibility General Subject Name	Request Handling Server		Key Attestation Requirements				
Superseded Templ		tensions	Security				
To modify an extension, select it, and then click Edit. Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Issuance Policies Key Usage							
Description of Applicat	ian Dallaian		Edit				
Client Authentication Server Authentication			×				
ОК	Cancel	Apply	Help				

Step 8. Close the **Certificate Template Console** window, and back on the very first window, navigate to **New > Certificate Template to Issue**, as shown in the image.



Step 9. Select the new CallManager CUCM template and select OK, as shown in the image.

	Enable	Certificate Templates	X
Noi Info All	ect one Certificate Template to enable on this 0 te: If a certificate template that was recently cre smation about this template has been replicater of the certificate templates in the organization m r more information, see <u>Certificate Templa</u>	ated does not appear on this list, you may need to wait until d to all domain controllers. nay not be available to your CA.	
N	ame	Intended Purpose	~
3	Authenticated Session	Client Authentication	
3	CA Exchange	Private Key Archival	
8	CallManager CUCM	Server Authentication, Client Authentication	=
3	CEP Encryption	Certificate Request Agent	
3	Code Signing	Code Signing	
3	Cross Certification Authority	<ab< td=""><td></td></ab<>	
- 3	Enrolment Agent	Certificate Request Agent	
3	Enrollment Agent (Computer)	Certificate Request Agent	
3	Exchange Enrolment Agent (Offline request)	Certificate Request Agent	
3	Exchange Signature Only	Secure Email	
3	Exchange User	Secure Final	$\sim$
		OK Cano	el

Step 10. Repeat all previous steps to create certificate templates for the Tomcat and TVS services as needed.

#### **IPsec Template**

Step 1. Find the **Web Server** template, right-click on it and select **Duplicate Template**, as shown in the image.

		c	ertificate Te	mplates	Console	
File Action View Help						
4 4 🔟 🖸 🖬 🔟 🔟						
ertificate Templates (win12.collab.m	Template Display Name	Schema Version	Versi	Intended	I Purposes	
	Workstation Authentication	2	101.0	Client A	uthentication	
	I Web Server	1	4.1			_
	User Signature Only	1	4.1		Ouplicate Template	
	3 User	1	3.1		All Tasks	
	Trust List Signing	1	3.1		Properties	
	Tomcat CUCM	2	100.3	Serve		-
	Subordinate Certification Authority	1	5.1		Help	
	Smartcard User	1	11.1			
	Smartcard Logon	1	6.1			
	Router (Offline request)	1	4.1			
	Root Certification Authority	1	5.1			
	RAS and IAS Server	2	101.0	Client A	uthentication, Server Authe	nticatie

Step 2. Under **General**, you can change the certificate template's name, display name, validity, etc..

Properties of New Template								
Subject Name	Subject Name Server Issuance Requirements							
Superseded Templa	tes	Ed	Extensions Security					
Compatibility General	Request	Handling	Cryptography	Key Attestation				
Template display name:								
IPSEC CUCM								
Template name: IPSEC CUCM Validity period: 2 years v \$ \$ weeks v								
Publish certificate in Do not automatic Directory			icate certificate	exists in Active				
OK	(	Cancel	Apply	Help				

Step 3. Navigate to **Extensions > Key Usage > Edit**, as shown in the image.

	Pro	perties	of New	Template		X				
Compatibility Subject N			Request Handling Server		Cryptography Key Attestati Issuance Requirements					
	ied Templa		_	ensions	Securi					
To modify an extension, select it, and then click Edit. Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Issuance Policies Key Usage										
Description of	of Key Usag	pe:			Edt					
Signature re Digital signa Allow key es Critical exter	ture (change or		ry encryptic	m		< >				
[	ОК		Cancel	Apply	В	elp				

Step 4. Select these options and select **OK**, as shown in the image.

- Digital signature
- Allow key exchange only with key encryption (key encipherment)
- Allow encryption of user data

	Properties of New Template	x								
Compatibility Gene Subject Name	eral Request Handling Cryptography Key Attestation Server Issuance Requirements	n								
	Edit Key Usage Extension									
extension. Signature Digital signatu Signature is p Certificate sig	Signature  Digital signature  Signature is proof of origin (nonrepudiation)  Certificate signing									
Allow key ex	change without key encryption (key agreement) change only with key encryption (key encipherment) encryption of user data									
Make this exter	nsion critical OK Cancel	]								
	OK Cancel Apply Help									

Step 5. Navigate to Extensions > Application Policies > Edit > Add, as shown in the image.

	Pro	perties	of New	Template			
Compatibility	General	Request	Handling	Cryptography	y H	key Attestation	
Subject N	lame	Sen	Server Issuance Requirement		uirements		
Supersec	ded Templa	tes	Exte	ensions		Security	
To modify an extension, select it, and then click Edit. Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Issuance Policies Key Usage							
Description of Server Auth		on Policies				Edt	
[	ОК		ancel	Apply		Help	

Edit Applicatio	on Policies E	tension 🗶						
An application policy defines how a certificate can be used.								
Application policies:								
Server Authentication								
Add	Edit	Remove						
Make this extension	critical							
	ОК	Cancel						

Step 6. Search for Client Authentication, select it and then OK, as shown in the image.

Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements S Fully Application Policy
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Application policies: Any Purpose Attestation Identity Key Certificate Certificate Request Agent Client Authentication Code Signing CTL Usage Digital Rights
Directory Service Email Replication Disallowed List Document Encryption Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator
OK Cancel
OK Cancel Apply Help

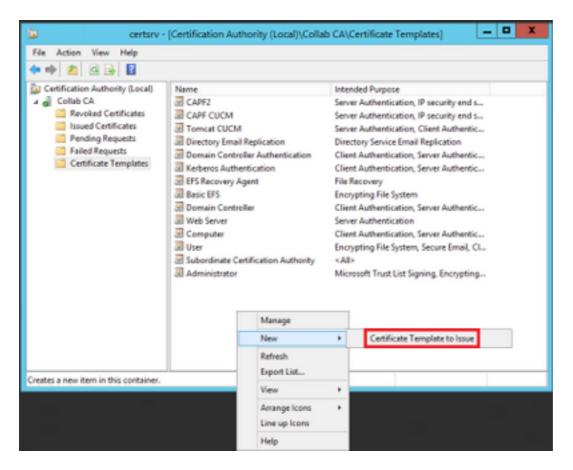
Step 7. Select **Add** again, search for **IP security end system**, select it and then select **OK** on this and on the previous window as well.

Properties of New Template
Subject Name Server Issuance Requirements Compatibility General Request Handling Contography Key Attestation Contography Key Attestation Critic Application Policies Extension
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Application policies: Early Launch Antimalware Driver Embedded Windows System Component Verification Encrypting File System Endorsement Key Certificate File Recovery HAL Extension IP security end system IP security IKE intermediate IP security Lunnel termination
IP security user KDC Authentication Kemel Mode Code Signing Key Pack Licenses
OK Cancel
OK Cancel Apply Help

Step 8. Back on the template, select **Apply** and then **OK**, as shown in the image.

Pro	perties	of New	Template	×			
Subject Name		ver		Requirements			
Compatibility General	Request	Request Handling Cryptog		Key Attestation			
Superseded Templa	Security						
To modify an extension, select it, and then click Edt. Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Issuance Policies Key Usage							
Description of Application Client Authentication IP security end system Server Authentication	on Policier	8:		Edt			
ок		Cancel	Apply	Help			

Step 9. Close the **Certificate Templates Console** window, and back on the very first window, navigate to **New > Certificate Template to Issue**, as shown in the image.



Step 10. Select the new **IPSEC CUCM** template and select on **OK**, as shown in the image.

		Enable Certificate Templates	x
Not info All o	e: If a certificate template that mation about this template hat of the certificate templates in the second sec	o enable on this Certification Authority. t was recently created does not appear on this list, you may need to wait until as been replicated to all domain controllers. he organization may not be available to your CA. rtificate Template Concepts.	
N	ame	Intended Purpose	~
3	Exchange Signature Only	Secure Email	
3	Exchange User	Secure Email	
3	IPSec	IP security IKE intermediate	
8	IPSEC CUCM	Server Authentication, IP security end system, Client Authentication	
3	Key Recovery Agent	Key Recovery Agent	
	OCSP Response Signing	OCSP Signing	=
- 3	RAS and IAS Server	Client Authentication, Server Authentication	
3	Router (Offline request)	Client Authentication	
3	Smartcard Logon	Client Authentication, Smart Card Logon	
3	Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
1.3	Trust List Sinning	Microsoft Trust List Signing	~
		OK Cano	el

#### **CAPF** Template

Step 1. Find the **Root CA** template and right-click on it. Then select **Duplicate Template**, as shown in the image.

3	Certificate Templates Console								
File Action View Help									
🕈 🔶 📅 🖾 🗃 🔝 📷									
Certificate Templates (win/12.col	Template Display Name	Schema Version	Vesi	intend	led Purposes				
	Router (Offline request)	1	4.1						
	Root Certification Authority		54		Duplicate Template				
	RAS and IAS Server	2	101.0	Ch	Explorate Template		stion		
	CCSP Response Signing	3	101.0	00	All Tasks				
	3 LOAPS	2	100.6	10	Properties		Server Authentication, Client A		
	Key Recovery Agent	2	105.0	Ke					
	Keberos Authentication	2	110.0	Ch.	Help		ition, Smart Card Logen, KDC J		
	2 IPSEC CUCM	2	100.4	Server	Authentication, IP securit	ty end:	system, Client Authentication		
	B (PSec (Office request)	1	7.1						
	2 Plac		6.1						

Step 2. Under **General**, you can change the certificate template's name, display name, validity, etc.

Properties of New Template								
Superseded Templa	d Templates Extensions Security							
Compatibility	General Issuance Requirements							
Template display name CAPF CUCM	Template display name: CAPF CUCM							
Template name: CAPF CUCM								
Validity period: 5 years v								
Publish certificate in Do not automatic Directory		-	licate certificat	e exists in Active				
OK	(	Cancel	Apply	Help				

Step 3. Navigate to Extensions > Key Usage > Edit, as shown in the image.

Pro	operties	of New	Template		X				
Compatibility	Gene	ral	Issuance	Requirements					
Superseded Templ	ates	Ed	ensions	Security					
To modify an extension, select it, and then click Edit.									
Extensions included in	this templa	te:							
Application Policie	5				ור				
Basic Constraints									
Certificate Templat	e Informati	ion							
Issuance Policies									
Key Usage									
					-				
				Edt					
Description of Key Usa	ge:								
Signature requirement	s:			[	~				
Digital signature Certificate signing									
CRL signing									
Critical extension.					_				
					~				
ОК		Cancel	Anch	Hala					
OK		Cancel	Apply	Help					

Step 4. Select these options and select OK, as shown in the image.

- Digital signature
- Certificate signing
- CRL signing

	Properties of New Template	x
Compatibility Gene Subject Name	eral Request Handling Cryptography Key Attestation Server Issuance Requirements	n
	Edit Key Usage Extension	¢
extension. Signature Digital signatu Signature is p Certificate sig	roof of origin (nonrepudiation)	
Allow key ex	change without key encryption (key agreement) change only with key encryption (key encipherment) encryption of user data	
Make this exter	nsion critical OK Cancel	]
	OK Cancel Apply Help	

Step 5. Navigate to Extensions > Application Policies > Edit > Add, as shown in the image.

	Pro	perties of	New	Template	X
Compatibility	General	Request Ha	anding	Cryptography	Key Attestation
Subject N	lame	Server		Issuance R	equirements
Supersec	ded Templa	tes	Exte	nsions	Security
To modify an	extension	, select it, and	d then c	lick Edit.	
1		his template:			
	ion Policies				
2000	onstraints	. Information			
2000	e Policies	e Information			
Key Usa					
					Edit
Description of		on Policies:			
Server Auth	entication				^
					~
	OK	Car	ncel	Apply	Help

Edit Applicatio	on Policies Extension	x
An application policy def used.	fines how a certificate can be	
Application policies:		
Server Authentication		
Add	Edit Remove	
Make this extension	critical	
	OK Cancel	

Step 6. Search for Client Authentication, select it and then select OK, as shown in the image.

Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements S Fully Application Policies Fotossiles X Add Application Policy
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Application policies:          Any Purpose       ^         Attestation Identity Key Certificate       ^         Certificate Request Agent       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator
OK Cancel
OK Cancel Apply Help

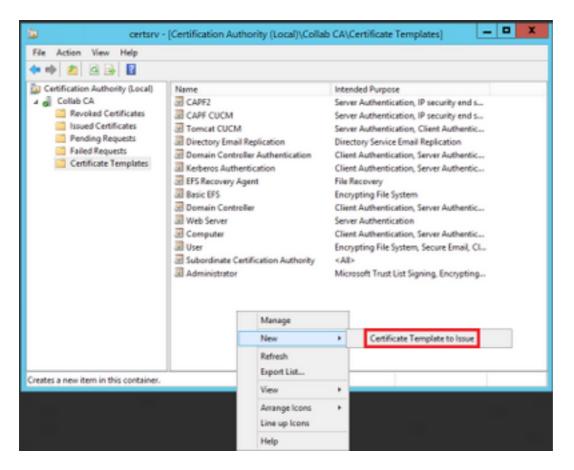
Step 7. Select **Add** again, search for **IP security end system**, select it and then select OK on this and on the previous window as well, as shown in the image.

Properties of New Template
Subject Name Server Issuance Requirements Compatibility General Request Handling Contography Key Attestation Contography Key Attestation Critic Application Policies Extension
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Application policies: Early Launch Antimalware Driver Embedded Windows System Component Verification Encrypting File System Endorsement Key Certificate File Recovery HAL Extension IP security end system IP security IKE intermediate IP security Lunnel termination
IP security user KDC Authentication Kemel Mode Code Signing Key Pack Licenses
OK Cancel
OK Cancel Apply Help

Step 8. Back on the template, select **Apply** and then **OK**, as shown in the image.

Properties of New Template						
Subject Name		ver		Requirements		
Compatibility General	Request	Handing	Cryptography	Key Attestation		
Superseded Templates Extensions Security						
To modify an extension, Extensions included in t Application Policies Basic Constraints Certificate Template Issuance Policies Key Usage	his templa	ite:	lick Edit.			
Description of Application Client Authentication IP security end system Server Authentication	on Policier	8:		Edt		
ок		Cancel	Apply	Help		

Step 9. Close the **Certificate Templates Console** window, and back on the very first window, navigate to **New > Certificate Template to Issue**, as shown in the image.



Step 10. Select the new CAPF CUCM template and select OK, as shown in the image.

		Enable Certificate Templates	x
1	Note: If a certificate template that in information about this template has	enable on this Certification Authority. was recently created does not appear on this list, you may need to wait until been replicated to all domain controllers. e organization may not be available to your CA. ificate Template Concepts.	
	Name	Intended Purpose	~
	Authenticated Session	Client Authentication	
	CA Exchange	Private Key Archival	
	CAPF CUCM	Server Authentication, IP security end system, Client Authentication	=
	Code Signing	Code Signing	
	Cross Certification Authority	<al></al>	
	Enrolment Agent	Certificate Request Agent	
	Enrollment Agent (Computer)	Certificate Request Agent	
	Exchange Signature Only	Secure Email	
	Exchange User	Secure Email	
	IPSec	IP security IKE intermediate	
1	R IPSEC CUCM	Server Authentication JP security end system. Client Authentication	~
		OK Cano	el

#### **Generate a Certificate Signing Request**

Use this example in order to generate a CallManager certificate with the use of the newly created templates. The same procedure can be used for any certificate type, you just need to select the certificate and template types accordingly:

Step 1. On CUCM, navigate to **OS Administration > Security > Certificate Management > Generate CSR**. Step 2. Select these options and select **Generate**, as shown in the image.

- Certificate Purpose: CallManager
- Distribution: < This can either be just for one server or Multi-SAN>

Generate 🔄 Close			
tatus			
🚹 Warning: Generating a	a new CSR for a specific certificate type	vill overwrite the ex	isting CSR for that type
enerate Certificate Sig	sing Request		
ertificate Purpose**	CallManager	*	
stribution*	Hulti-server(SAN)	•	
mmon Name*	115PUB-ms.maucabal.Jab		
bject Alternate Name:	s (SANs)		
its-populated Domains	115PUB.maucabal.lab 115SUB.maucabal.lab		
rent Domain	maucabal.lab		
ther Domains		~	Choose File No file chosen Hease import .TXT file only. For more information please refer to the notes in the Help Section
		v	Bh Add
ay Type**	RSA	v	bba 🕷
ry Type** ry Length*	RSA 2040	•	B Add

#### Step 3. A confirmation message is generated, as shown in the image.

Generate Certificate Signing Request	
Serente T Close	
r Stelus	
Success: Certificate Signing Request Generated	
CSR export operation successful on the nodes (115PU8.maucabal.lab, 115SU8.maucabal.lab).	

Step 4. On the certificate list, look for the entry with type **CSR Only** and select it, as shown in the image.

🔒 Generale Belli	ignes 🐴 Lipited Centificate/Cer	tifcate chain	Cure Care	rate CSR 👔 Download CSR			
Status	und						
Certificate List	(1 - 50 of 56)						Revel per Page 30 +
Find Certificate Lis	t where Certificate	ing with +		Find Over Filter			
Certificate *	Common Name	Type	Key Toos	Distribution	Issued By	Expiration	Description
authe	807962_admits	Self- signed	RSA	115PU8.maxcabal.lab	AUTHZ_admin	01/27/2008	Self-signed certificate penerated by system
Calimanager	113PUB-ms.maucabal.lab	CSR Only	RSA	Multi-server(\$4N)			
Carmanager	1130/E.Marcelause	signed	RDA	1159UE/mascatur.lab	115PUB.mascabal.lab	05/30/2023	Self-signed certificate generated by system
CallHanager- BCDSA	113938-EC-managed-ada	Salf- signed	ec.	115P08.mascabal.lab	115PUB- EC.maucabal.lab	03/04/3033	Salf-signed certificate generated by system
Califianager-trust	115908-00-ликовалав	Salf-	ec.	115PU8.maucabal.lab	115PUB- EC.maucebal.lab	03/04/3023	Trust Certificate

Step 5. On the pop-up window, select **Download CSR**, and save the file on your computer.

CSR Details for 115PUB	-ms.maucabal.lab, CallManager	
🗙 Delete 🔋 Downloa	d CSR	
_ Status		
i Status: Ready		
Certificate Settings-		
File Name	CallManager.csr	
Certificate Purpose	CallManager	
Certificate Type	certs	
Certificate Group	product-cm	
Description(friendly name	e)	
SubjectPKInfo: RSA (1.2 Key value: 3082010a0282010100c1 cabc144fd5f1538efe514f f902277c2ee55d7e5a4d6 9fbd3d5aae5f4f02237eci 79d661582952880d98b3 9be410e8d3b4e1f18a89f	8a6119e66450eef211e6ac9a2349f3466616bd77017095303de7d d8207d3ddea43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34 880f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2 abca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b l290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164 567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c 01	•
Delete Download CS	R	

Step 6. On your browser, navigate to this URL, and enter your domain controller administrator credentials: https://<yourWindowsServerIP>/certsrv/.

Step 7. Navigate to **Request a certificate > advanced certificate request**, as shown in the image.

Microsoft Active Directory Conflicate Services - Collab CA Bottom
Velcome
Ise 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 o people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform ther 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.
or more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.
Request a certificate View the status of a pending certificate request Download a CA certificate, certificate shain, or CRL
Microsoft Active Directory Certificale Services - Collab CA Hom
tequest a Certificate
elect the certificate type: User Certificate
x, submit an advanced certificate request.

Step 8. Open the CSR file and copy all its contents:



Step 9. Paste the CSR on the **Base-64-encoded certificate request** field. Under **Certificate Template**, select the correct template and select **Submit**, as shown in the image.

Base-64-encoded ski70s certificate request 27vev	request to the CA, p (such as a Web service) (such as a Web service) (such as a Web service)	aste a base-64-e ver) in the Savec	d Req
an external source ( saved Request Base-64-encoded 00.700 certificate request 07444	(such as a Web serv y211/2p048/Pp1+ya24 h5m123*14822pp47730 webpfly	ver) in the Saved	d Req
Base-64-encoded Shifts	ທີ່ເລືອດເຊິ່ງເລືອງໃຈກີເຊິ່ງຊົ່ງເຈົ້າກາວໄດ້ ແຜ່ເລື່ອງຊົ່ງງ		
Base-64-encoded ski70s certificate request 27vev	ທີ່ເລືອດເຊິ່ງເລືອງໃຈກີເຊິ່ງຊົ່ງເຈົ້າກາວໄດ້ ແຜ່ເລື່ອງຊົ່ງງ		· ^
PKCS #10 or PKCS #7).	oyiniyani -mio centificare ne		, , ,
Certificate Template:			_
Additional Attributes:	lanager CUCH	v	
Attributes			_
		Submit >	_

Step 10. Finally, select **Base 64 encoded** and **Download certificate chain**, the generated file can now be uploaded the CUCM.



### Verify

The verification procedure is actually part of the configuration process.

#### Troubleshoot

There is currently no specific troubleshooting information available for this configuration.