# Crear plantillas de certificados de CA de Windows para CUCM

### Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Callmanager / Tomcat / Plantilla de TVS
Plantilla IPsec
Plantilla CAPF
Generar una solicitud de firma de certificado
Verificación
Troubleshoot

#### Introducción

Este documento describe un procedimiento paso a paso para crear plantillas de certificados en entidades de certificación (CA) basadas en Windows Server.

### Prerequisites

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM, versión 11.5(1).
- También se recomiendan conocimientos básicos de la administración de Windows Server

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- La información de este documento se basa en CUCM versión 11.5(1).
- Microsoft Windows Server 2012 R2 con servicios de CA instalados.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

#### Antecedentes

Estas plantillas de certificado cumplen los requisitos de la extensión X.509 para cada tipo de certificado de Cisco Unified Communications Manager (CUCM).

Hay cinco tipos de certificados que puede firmar una CA externa:

Certificado	Uso	Servicios afectados
CallManager	Presentado en el registro de dispositivos seguros, puede firmar archivos de lista de confianza de certificados (CTL)/lista de confianza interna (ITL), que se utilizan para interactuar de forma segura con otros servidores, como enlaces troncales de protocolo de inicio de sesión (SIP) seguros.	· Cisco Call Manager · Cisco CTI Manager ·Cisco TFTP
tomcat	Presentado para interacciones de protocolo seguro de transferencia de hipertexto (HTTPS).	<ul> <li>Tomcat de Cisco</li> <li>Inicio de sesión único (SSO)</li> <li>Movilidad de extensiones</li> <li>Corporate Directory</li> </ul>
ipsec	Se utiliza para la generación de archivos de copia de seguridad, así como para la interacción de la seguridad IP (IPsec) con el protocolo de control de gateway de medios (MGCP) o las puertas de enlace H323.	· Cisco DRF Master · Cisco DRF Local
CAPF	Se utiliza para generar certificados de importancia local (LSC) para teléfonos.	<ul> <li>Función de proxy de Cisco</li> <li>Certificate Authority</li> </ul>
TVS	Se utiliza para crear una conexión con el Servicio de verificación de	· Servicio Cisco Trust Verification

Nota: el certificado IPSec no está relacionado con Cisco DRF Master y Cisco DRF Local, ya que en las versiones más recientes se utiliza el certificado Tomcat 14. No existe ningún plan para agregar este cambio a la versión 12.5 o anteriores.

Cada uno de estos certificados tiene algunos requisitos de extensión X.509 que deben establecerse; de lo contrario, puede encontrar comportamientos incorrectos en cualquiera de los servicios mencionados:

Certificado	Uso de claves X.509	Uso de clave ampliada X.509
CallManager	<ul> <li>Firma digital</li> <li>Cifrado de claves</li> <li>Cifrado de datos</li> </ul>	<ul> <li>Autenticación de servidor web</li> <li>Autenticación de cliente web</li> </ul>
tomcat	<ul> <li>Firma digital</li> <li>Cifrado de claves</li> <li>Cifrado de datos</li> </ul>	<ul> <li>Autenticación de servidor web</li> <li>Autenticación de cliente web</li> </ul>
ipsec	<ul> <li>Firma digital</li> <li>Cifrado de claves</li> <li>Cifrado de datos</li> </ul>	<ul> <li>Autenticación de servidor web</li> <li>Autenticación de cliente web</li> <li>Sistema final IPsec</li> </ul>
CAPF	<ul> <li>Firma digital</li> <li>Signo de certificado</li> <li>Cifrado de claves</li> </ul>	<ul> <li>Autenticación de servidor web</li> <li>Autenticación de cliente web</li> </ul>
TVS	<ul> <li>Firma digital</li> <li>Cifrado de claves</li> <li>Cifrado de datos</li> </ul>	<ul> <li>Autenticación de servidor web</li> <li>Autenticación de cliente web</li> </ul>

Para obtener más información, consulte la <u>Guía de seguridad de Cisco Unified Communications</u> <u>Manager</u>

### Configurar

Paso 1. En Windows Server, navegue hasta Administrador del servidor > Herramientas > Entidad emisora de certificados, como se muestra en la imagen.

<u>L</u>	Se	rver Manager		
⊛⊕ - Server Ma	nager • Dashboard	٠e	) i 🖍 🛶 🛌	Nice Subp
	WELCOME TO SERVER MARAGER	gure this local server i roles and features d other servers to manage ate a server group meet this server to cloud service Manapability Dents Services	AD IS Wanapability Dens Servors	Active Discretary Interintentine Exerce Active Discretary Spreads and Fourth Active Discretary Optimizing Discretary Services Server Wand Active Discretary Optimized Discretary Active Discretary Optimized Discretary Computer Management Active Discretary Computer Management Optimized Discretary Optimized Optimized Discretary Optimized Optimized Optimized Optimized Active Discretary Active Discretary Ac
	Performance BPA-results PAD LDS 1	Performance BPA results	Performance BPA results	System Information Text Scheduler Windows Ferenzi with Astronaut Security Windows Ferenzi Stati Windows Ferenzi Stati

Paso 2. Seleccione su CA, navegue hasta Plantillas de certificado, haga clic con el botón derecho en la lista y seleccione Administrar, como se muestra en la imagen.



#### Callmanager / Tomcat / Plantilla de TVS

Las imágenes siguientes muestran solo la creación de la plantilla de CallManager; pero se pueden seguir los mismos pasos para crear las plantillas de certificado para Tomcat y los servicios de TVS. La única diferencia consiste en garantizar que se utiliza el nombre de servicio correspondiente para cada nueva plantilla en el paso 2.

Paso 1. Busque la plantilla Web Server, haga clic con el botón derecho en ella y seleccione Duplicate Template, como se muestra en la imagen.

3		c	ertificate Te	mplates	Console
File Action View Help					
🕈 🔶 📷 🐨 🐨 🐨					
Certificate Templates (win12.collab.m	Template Display Name	Schema Version	Versi	Intended	(Purposes
	Workstation Authentication	2	101.0	Client Av	uthentication
	Jii Web Server		4.1		
	User Signature Only	1	4.1		Duplicate Template
	2 User	1	3.1		All Tasks +
	Trust List Signing	1	3.1		Burnetter
	Tomcat CUCM	2	100.3	Serve	m
	Subordinate Certification Authority	1	5.1		Help
	Smartcard User	1	11.1		
	E 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 Ar	uthentication, Server Authentication

Paso 2. En General, puede cambiar el nombre de la plantilla de certificado, el nombre para mostrar, la validez y algunas otras variables.

Subject Name	Sen	/er	Issuance R	equirements
Superseded Temp	lates	Ede	nsions	Security
Compatibility General	Request	Handling	Cryptography	Key Attestation
Template display nam CallManager CUCM	e:			
Template name:				
CalManager CUCM				
Validity period:		Renewa	period:	
5 years	~	6	weeks 🗸	
Publish certificate	in Active Dir	ectory		
Do not automa	tically reenro	l if a dupli	cate certificate (	ssists in Active
Directory				
OK		Jancel	Abbia	мер

X

Paso 3. Navegue hasta Extensiones > Uso de claves > Editar, como se muestra en la imagen.

Pro	perties of N	lew Tem	plate		X
Compatibility General	Request Hand	sling Cryp	tography	Key Attestat	tion
Superseded Templa	tes	Edension	5	Security	-
To modify an extension. Extensions included in the Constraints Basic Constraints Certificate Template Issuance Policies	select it, and this template:	hen click E	dit.		
Description of Key Usag Signature requirements Digital signature Allow key exchange on	je: : iv with key enc	rvotion		Edit	
Critical extension.	.,,,				
OK	Cance	el	Apply	Help	

Paso 4. Seleccione estas opciones y seleccione OK, como se muestra en la imagen.

- Firma digital
- Permitir el intercambio de claves sólo con el cifrado de claves (cifrado de claves)
- Permitir cifrado de datos de usuario

Pro	perties of New	Template	X
Compatibility General Subject Name	Request Handing Server	Cryptography Issuance Re	Key Attestation squirements
Specify the required signature  Signature  Digital signature  Signature is proof	nature and security of origin (nonrepuda	options for a key (	usage
Certificate signing CRL signing Encryption Allow key exchant Allow key exchant	nge without key enc ige only with key en	ryption (key agree cryption (key enci	ment) phement)
Allow encry	ption of user data		
<u>ОК</u>	Cancel	Apply	Cancel

Paso 5. Navegue hasta Extensiones > Políticas de aplicación > Editar > Agregar, como se muestra en la imagen.

Compatibility	General	Request	Handling	Cryptography	Key Attestation
Subject N	Vame	Ser	ver	Issuance	Requirements
Supersec	ded Templa	ites	Ed	ensions	Security
To modify an Extensions in Applicat Basic Co Certificat Issuance Key Usa	n extension included in t ion Policies onstraints te Template e Policies age	, select it, his templa e Informati	and then o te:	click Edit.	
Description	of Application	on Policies	B;		Edt
Server Auth	entication				
[	ОК		Cancel	Apply	Help

Paso 6. Busque Client Authentication, selecciónela y seleccione OK tanto en esta ventana como en la anterior, como se muestra en la imagen.

Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements C Edit Application Policy X
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:
Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator
OK Cancel
OK Cancel Apply Help

Paso 7. Vuelva a la plantilla, seleccione Aplicar y, a continuación, Aceptar.

X

Paso 8. Cierre la ventana Consola de Plantilla de Certificado y, nuevamente en la primera ventana, navegue hasta Nuevo > Plantilla de Certificado para Emitir, como se muestra en la imagen.



Paso 9. Seleccione la nueva plantilla de CallManager CUCM y seleccione OK, como se muestra en la imagen.

elect one Certificate Template to enable on this ote: If a certificate template that was recently on ormation about this template has been replicate of the certificate templates in the organization re or more information, see Certificate Templates or more information.	Certification Authority. sated does not appear on this list, you may need to wait unti d to all domain controllers. may not be available to your CA. ate Concepts.	i.
Name	Intended Purpose	1
Authenticated Session	Client Authentication	
CA Exchange	Private Key Archival	
CalManager CUCM	Server Authentication, Client Authentication	
CEP Encryption	Certificate Request Agent	
Code Signing	Code Signing	
Cross Certification Authority	<al></al>	
Enrolment Agent	Certificate Request Agent	
Enrollment Agent (Computer)	Certificate Request Agent	
Exchange Enrolment Agent (Offine request)	Certificate Request Agent	
	Secure Email	
Exchange Signature Only		- 1 k

Paso 10. Repita todos los pasos anteriores para crear plantillas de certificado para los servicios Tomcat y TVS según sea necesario.

#### Plantilla IPsec

Paso 1. Busque la plantilla Web Server, haga clic con el botón derecho en ella y seleccione Duplicate Template, como se muestra en la imagen.

3		c	ertificate Te	mplates	Console	
File Action View Help						
🕈 🕈 🛅 🔂 🔂 🛅						
Certificate Templates (win12.collab.m	Template Display Name	Schema Version	Vesi	Intended	Purposes	
	Workstation Authentication	2	101.0	Client Av	uthentication	
	Web Server		4.1			_
	User Signature Only	1	4.1		Duplicate Template	
	🐷 User	1	3.1		All Tasks	
	I Trust List Signing	1	3.1		Properties	
	Tomcat CUCM	2	100.3	Serve	r repenses	20
	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 Ar	uthentication, Server Authe	ntication

Paso 2. En General, puede cambiar el nombre de la plantilla de certificado, el nombre para mostrar, la validez y algunas otras variables.

Subject Name	Sen	ver	Issuance F	Requirements
Superseded Templa	tes	Ede	ensions Securi	
Compatibility General	Request	Handling	Cryptography	Key Attestation
Template display name	1			
IPSEC CUCM				
Template name: IPSEC CUCM Validity period: 2 years v	]	Renewa	l period: weeks ∽	]
Publish certificate in Do not automatic Directory	Active Dir ally reenro	rectory oil if a dupli	cate certificate	exists in Active

X

Paso 3. Navegue hasta Extensiones > Uso de claves > Editar, como se muestra en la imagen.

Pro	perties of N	lew Tem	plate		X
Compatibility General	Request Hand	sling Cryp	tography	Key Attestat	tion
Superseded Templa	tes	Edension	5	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 Key Usag Signature requirements Digital signature Allow key exchange on	je: : iv with key enc	rvotion		Edit	
Critical extension.	.,,,				
OK	Cance	el	Apply	Help	

Paso 4. Seleccione estas opciones y seleccione OK, como se muestra en la imagen.

- Firma digital
- Permitir el intercambio de claves sólo con el cifrado de claves (cifrado de claves)
- Permitir cifrado de datos de usuario

Pro	perties of New	Template	X
Compatibility General Subject Name	Request Handing Server	Cryptography Issuance Re	Key Attestation squirements
Specify the required signature  Signature  Digital signature  Signature is proof	nature and security of origin (nonrepuda	options for a key (	usage
Certificate signing CRL signing Encryption Allow key exchant Allow key exchant	nge without key enc ige only with key en	ryption (key agree cryption (key enci	ment) phement)
Allow encry	ption of user data		
<u>ОК</u>	Cancel	Apply	Cancel

Paso 5. Navegue hasta Extensiones > Políticas de aplicación > Editar > Agregar, como se muestra en la imagen.

Compatibility	General	Request	Handling	Cryptography	y Key Attestation
Subject N	lame	Ser	ver	Issuance	Requirements
Supersec	ded Templa	tes	Ext	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	of Application	on Policie:	3.		Edt
					~
	OK		Cancel	Apply	Help

x

Paso 6. Busque Client Authentication, selecciónela y luego OK, como se muestra en la imagen.

Properties of New Template	X
Compatibility General Request Handling Cryptography Key Attes Subject Name Server Issuance Requirement C Edit Application Deligities Extension X Add Application Policy	tation s
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.	uired
Any Purpose	
Attestation Identity Key Certificate Certificate Request Agent	Ê
Client Authentication	
CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Encryption Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator	<
New	
OK Cancel	
OK Cancel Apply He	lp .

Paso 7. Seleccione Add nuevamente, busque IP security end system, selecciónelo y luego seleccione OK en esta ventana y en la anterior.

Subject Name	Server	Issuance Re	quirements
Compatibility General	Request Handling	Csyntography	Key Attestation
d Edit A	Add Applicatio	n Policy	×
An application policy (cr defines how a certificate for valid signatures of cr	alled enhanced key e can be used. Sele artificates issued by	usage in Windows act the application p this template.	2000) colicy required
Application policies:			
Early Launch Antimalw Embedded Windows S Encrypting File System Endorsement Key Cetti	are Driver ystem Component	Verification	^
File Recovery HAL Extension			=
IP security end system IP security IKE intermed IP security tunnel termin IP security user KDC Authentication Kernel Mode Code Sign Key Pack Licenses	diate nation ning		~
			New
		OK	Cancel
ОК	Cancel	Apply	Help

X

Paso 8. De nuevo en la plantilla, seleccione Apply y luego OK, como se muestra en la imagen.

	vame	Ser	ver	Issuance R	equirements
Compatibility	General	Request	Handing	Cryptography	Key Attestation
Superse	ded Templa	tes	Ed	ensions	Security
To modify an Extensions in Applicat Basic Co Certifica Issuanco Key Usa	n extension ncluded in t ion Policies onstraints te Template e Policies age	, select it, his templa	and then o te:	click Edit.	
Description Client Author IP security ( Server Author	of Application entication end system entication	on Policies	IC		Edit
Description ( Client Author IP security ( Server Author)	of Application end system entication	on Policies			Edit

X

Paso 9. Cierre la ventana de la Consola de Plantillas de Certificado y, nuevamente en la primera ventana, navegue hasta Nuevo > Plantilla de Certificado para Emitir, como se muestra en la imagen.



Paso 10. Seleccione la nueva plantilla IPSEC CUCM y seleccione en Aceptar, como se muestra en la imagen.

Select one Certificate Template t Note: If a certificate template tha information about this template he All of the certificate templates in t For more information, see <u>Ce</u>	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. the organization may not be available to your CA. rtificate Template Concepts.	
Name	Intended Purpose	~
Exchange Signature Only	Secure Email	
Exchange User	Secure Email	
IPSec	IP security IKE intermediate	
IPSEC CUCM	Server Authentication, IP security end system, Client Authentication	
Rey Recovery Agent	Key Recovery Agent	
CCSP Response Signing	OCSP Signing	
RAS and IAS Server	Client Authentication, Server Authentication	
Router (Offine request)	Client Authentication	
Smartcard Logon	Client Authentication, Smart Card Logon	
Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
Trust List Storion	Microsoft Trust List Signing	$\sim$
	OK Can	cel

#### Plantilla CAPF

Paso 1. Busque la plantilla de CA raíz y haga clic con el botón derecho en ella. A continuación, seleccione Duplicate Template, como se muestra en la imagen.

3		0	ertificate Te	mpilate	s Console		
File Action View Help							
** 📰 🗟 🖬 📼							
🗟 Cetificate Templates (win12.cel	Template Display Name	Schema Version	Versi-	Intend	ed Purposes		A
	Router (Offline request)	1	43				
	Root Certification Authority	1	5.1		Realized Transfer		
	RNS and IAS Server	1	101.0	Ch.	Dupicate tempore		dian.
	CCSP Response Signing	3	101.0	<b>64</b>	All Tasks		
	JE LOAPS	2	100.6	10	Properties		Server Authentication, Client A
	Key Recovery Agent	2	105.0	Cargo -			
	Enteres Authentication	2	110.0	Ch.	Help		Hion, Smart Card Logon, KDC A
	PREC CUCM	2	100.4	Server	Authentication, IP security	r end s	ystem, Client Authentication
	PSec (Office request)	1	7.1				
	a Plac	1	4.1				

Paso 2. En General, puede cambiar el nombre de la plantilla de certificado, el nombre para mostrar, la validez y algunas otras variables.

Superseded Templates	Extension	18	Security
Compatibility Ger	neral	Issuance Rei	quirements
Template display pame:			
CAPE CUCM			
Cra i coom			
Template name:			
CAPF CUCM			
-			
Volderserved	Descuration of		
validity period:	Henewal pen	00:	
j years V	o wee	KS Y	
Publish certificate in Active I	Directory		
Do not automatically reen	voll if a duplicate	certificate ex	ists in Active
Directory			
	Grand	Ande	11.1.
UK	Cancel	HODIY	нер

Paso 3. Navegue hasta Extensiones > Uso de claves > Editar, como se muestra en la imagen.

х

X

Compatibility	General	Issuance	Requirements
Superseded Templa	ates	Extensions	Security
To modify an extension Extensions included in Application Policies Basic Constraints Certificate Templat	this template:	hen click Edt.	
Key Usage			Edt
Description of Key Usa Signature requirements Digital signature Certificate signing CRL signing Critical extension.	ge: s:		× ×
OK	Cano	el Apply	Help

Paso 4. Seleccione estas opciones y seleccione OK, como se muestra en la imagen.

- Firma digital
- Firma de certificados
- firma de CRL

Pro	perties of New	Template	X		
Compatibility General Subject Name	Request Handing Server	Cryptography Issuance Re	Key Attestation squirements		
Specify the required signature  Signature  Digital signature  Signature is proof	nature and security of origin (nonrepuda	options for a key (	usage		
Certificate signing CRL signing Encryption Allow key exchange without key encryption (key agreement)  Allow key exchange only with key encryption (key enciphement)					
<ul> <li>Allow encryption of user data</li> <li>Make this extension critical</li> </ul>					
<u>ОК</u>	Cancel	Apply	Cancel		

Paso 5. Navegue hasta Extensiones > Políticas de aplicación > Editar > Agregar, como se muestra en la imagen.

Compatibility	General	Request	Handling	Cryptography	Key Attestation
Subject N	Subject Name Sery		ver	Issuance	Requirements
Superseded Templates		Ed	ensions	Security	
To modify an Extensions in Applicat Basic Co Certificat Issuance Key Usa	n extension included in t ion Policies onstraints te Template e Policies age	, select it, his templa e Informati	and then o te:	click Edit.	
Description	of Application	on Policies	B;		Edt
Server Auth	entication				
[	ОК		Cancel	Apply	Help

Paso 6. Busque Client Authentication, selecciónela y luego seleccione OK, como se muestra en la imagen.

Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements C Edit Application Policy X
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:
Document Signing Domain Name System (DNS) Server Trust Dynamic Code Generator
OK Cancel
OK Cancel Apply Help

Paso 7. Seleccione Add nuevamente, busque IP security end system, selecciónelo y luego seleccione OK en este y en la ventana anterior también, como se muestra en la imagen.

Subject Name	Server	Issuance Re	quirements			
Compatibility General	Request Handling	Csyntography	Key Attestation			
d Edit A	Add Applicatio	n 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:						
Early Launch Antimalw Embedded Windows S Encrypting File System Endorsement Key Cetti	are Driver ystem Component	Verification	^			
File Recovery HAL Extension			=			
IP security end system IP security IKE intermed IP security tunnel termin IP security user KDC Authentication Kernel Mode Code Sign Key Pack Licenses	diate nation ning		~			
			New			
		OK	Cancel			
ОК	Cancel	Apply	Help			

X

Paso 8. De nuevo en la plantilla, seleccione Apply y luego OK, como se muestra en la imagen.

	Subject Name Sen		ver	Issuance R	equirements
Compatibility	General	Request	Handing	Cryptography	Key Attestation
Superse	ded Templa	tes	Ed	ensions	Security
To modify an Extensions in Applicat Basic Co Certifica Issuanco Key Usa	n extension ncluded in t ion Policies onstraints te Template e Policies age	, select it, his templa	and then o te:	click Edit.	
Description Client Author IP security ( Server Author	of Application entication end system entication	on Policies	IC		Edit
Description ( Client Author IP security ( Server Author)	of Application end system entication	on Policies			Edit

X

Paso 9. Cierre la ventana de la Consola de Plantillas de Certificado y, nuevamente en la primera ventana, navegue hasta Nuevo > Plantilla de Certificado para Emitir, como se muestra en la imagen.



Paso 10. Seleccione la nueva plantilla CAPF CUCM y seleccione OK, como se muestra en la imagen.

B	Enable Certificate Templates					
Seli Not All o For	ect one Certificate Template to e: If a certificate template that mation about this template has of the certificate templates in the more information, see <u>Cert</u>	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.				
N	ате	Intended Purpose	~			
2	Authenticated Session CA Exchange	Client Authentication Private Key Archival				
	CAPF CUCM	Server Authentication, IP security end system, Client Authentication	=			
- 3	Code Signing	Code Signing				
3	Cross Certification Authority	(Ab)				
	Enrolment Agent	Certificate Request Agent				
8	Enrolment Agent (Computer)	Certificate Request Agent				
12	Exchange Signature Only	Secure Email				
12	Exchange User	Secure Email				
	IPSec	IP security IKE intermediate				
1.1	IPSEC CUCM	Server A thentication IP security end system Client Authentication	~			
		OK Cano	el			

Generar una solicitud de firma de certificado

Utilice este ejemplo para generar un certificado de CallManager con el uso de las plantillas recién creadas. El mismo procedimiento se puede utilizar para cualquier tipo de certificado, solo tiene que seleccionar el certificado y los tipos de plantilla en consecuencia:

Paso 1. En CUCM, vaya a OS Administration > Security > Certificate Management > Generate CSR.

Paso 2. Seleccione estas opciones y seleccione Generate, como se muestra en la imagen.

- Propósito del certificado: CallManager
- Distribución: <Puede ser solo para un servidor o para varias SAN>

enerate Certificate Sigr	ving Request		
🖏 Generate 📑 Close			
Status			
A Warning: Generating	a new CSR for a specific certificate type	will overwrite the ex	isting CSR for that type
Generate Certificate Sig	ning Request		
Certificate Purpose**	CallManager		
Distribution*	Hulti-server(SAN)	•	
Common Name*	115PUB-ms.maucabal.lab		
Subject Alternate Name	s (SANs)		
Auto-populated Domains	115PU8.maucabal.lab 115SUB.maucabal.lab		
Parent Domain	maucabal.lab		
Uner Domains			Choose File No file chosen Please import .TXT file only. For more information please refer to the notes in the Help Section
		-	🗷 Add
Key Type **	RSA		
Key Length*	2048		

Generate Close

Paso 3. Se genera un mensaje de confirmación, como se muestra en la imagen.



Paso 4. En la lista de certificados, busque la entrada con el tipo CSR Only y selecciónela, como se muestra en la imagen.

Certificate List							
Constant Sette	iper 🔒 oper cestance	nun chan	il, cere	rate CSR 🛐 Doumbed CSR			
Status 16 records for	und						
Certificate List	(1 - 50 of 56)						Rows per Page 30
Find Certificate Us	t where Certificate •   begi	na with 💌		Find Clear F	War 💠 💻		
Certificate *	Common Name	Toje -	Key Teps	Datribution	laund by	Expiration	Oescription
autho	autric admin	Self-	RSA	115PU8.maucabal.lab	AUTH2_admin	01/27/2038	Self-signed certificate penerated by system
Califfanaper	115PUB-ma.maucabal.lab	CSR Only	85.4	Hulti-server(SAN)	-	-	
canvasager	TURNER WARDEN IN	signed	NG.	1110/06/04/04/04/04/04/04/04/04/04/04/04/04/04/	115PUB.maucabal.lab	05/30/2023	Self-signed certificate penerated by system
Califfanager- ECOSA	115PUB-EC.maucabal.lab	Self- signed	0C	115PUB.maucabal.lab	115PUB- EC.maycabal.lab	63/94/2023	Self-signed certificate penerated by system
Califfanaper-trust	113958.0Cmascabal.lab	Self.	00	115PUB.maucabal.lab	115PUB- EC.maucabal.lab	03/94/2023	Trust Certificate
	and the second			1 A A A A A A A A A A A A A A A A A A A			

Paso 5. En la ventana emergente, seleccione Descargar CSR y guarde el archivo en el equipo.

CSR Details for 115PUB-ms.maucabal.lab, CallManager					
🗙 Delete 🔋 Downloa	d CSR				
Status					
<b>U</b>					
Certificate Settings —					
File Name	CallManager.csr				
Certificate Purpose	CallManager				
Certificate Type	certs				
Certificate Group	product-cm				
Description(friendly nam-	e)				
PKCS10 Request: [ Version: 0 Subject: CN=115PUB-m SubjectPKInfo: RSA (1.2 Key value: 3082010a0282010100c1 cabc144fd5f1538efe5140 f902277c2ee55d7e5a4d0 9fbd3d5aae5f4f02237ec 79d661582952880d98b3 9be410e8d3b4e1f18a89 5a9467d4963f226b6ab0 6b25a37e84cd02030100 Attributes: [ Requested Extensions	s.maucabal.lab, OU=clsco, O=clsco, L=clsco, ST=clsco, C=MX .840.113549.1.1.1) I8a6119e66450eef211e6ac9a2349f3466616bd77017095303de7d d8207d3ddea43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34 580f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2 abca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b 0290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164 567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c 001	*			
Delete Download CS	R				

Paso 6. En el explorador, desplácese hasta esta dirección URL e introduzca las credenciales de administrador del controlador de dominio: https://<yourWindowsServerIP>/certsrv/.

Paso 7. Navegue hasta Solicitar un certificado > Solicitud de certificado avanzada, como se muestra en la imagen.

Microsoft Active Directory Certificate Services - Colab CA	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

#### Paso 8. Abra el archivo CSR y copie todo su contenido:

CallManager - Notepad		X	C I
File Edit Format View Help			
BEGIN CERTIFICATE REQUESTRIIDNDCCAhwCAQAwbjELMAKGAIUEBHMCTVgxDjAMBgMVBAgTBMbpc2NvMQ4wQ aXNjb2EOMAwGAIUEChWFY2IrY28xDjAMBgMVBAsTBMpc2NvMRBwHQYDVQQDExYxMTVQVUIt5XNubHF1Y2FiYMwubGFIMIBE G9w8BAQEFAAOCAQBAMIIBCgKCAQEAwYphGe2kU07yEeasmiN3802mFr13AXCVMD3n3Xv88P1fFTjv5RT9ggfT3epDs1zk8FE 10MbQafMVPkC33wu5V1+Mk1oD4yMtvRu1T0yHGFGY293H2Xai3paLefdjdKfvT1ar19PAiN+yrynTPbi2bRjgFGunuF7mPg+ 2t51mFYKVKID2irKQ1EEXotjL+sKx2KxpojYR+oaDuoL2o9MKD3vkE0jTt0Hxiom804WEY65eA5/5/TGo/dbkXP5HNP17M5qJ 8ia2qu/nt/knNTa03u2HE/m12sMDh4bRb12mFFbjGs1o36EzQIDAQABoIGAMH4GCSqGS1b30QE3DjFxMGBwHQYDVR81BBYwH HAwEGCCsGAQUFBwMCMAsGA1UdDwQEAwIEsDB8BgWMREE0jAAgMtwMTVQVUIubWF1Y2FiYMwubGFigMtwMTVTVUIubWF1Y2F xtYXVjYNJhbC5sYNIwDQY3KoZIhvcNAQELBQADggEBAIgwtjgKM/LLvLogSI/tba62o/ViXcI2QwwM+SIywiiUH3b55fRuy 4P93uckGcSrivInwBT69h0BYx8T8hDc5LhdkTfmEd7XMAMEEhZ4ScwFbaVnugMJWYQ8c1p5UMhcK3y2QQDc5pjcv3LCPiqbc 1Yhky213/Zp0t9oVg&vynR96opVL2WigG570hImt1jGe74X2Qqu4YTS0uMM93BcH7u92y8PdKQa1FP+oAGMx1nocta2Nojmm 3s8gs9gxNXXcf8DcdWw+eG8qWRsnsZNMUND1o7a1Qbyxdf7r7dbSqW8Gy08qkM+END_CERTIFICATE_REQUEST	YDVQQHEwVj jANBgkahki 9011Ayv9cv jUNAKfc02; TWRa1GFU1j AYIKwY80Q YMAUbGF1gg Ap1jQXsk2v jn6pDU3f2v UuxunAgqUy	S L V X S D S d o Y	-
C 10		1.5	1

Paso 9. Pegue el CSR en el campo Solicitud de certificado codificado en Base-64. En Plantilla de certificado, seleccione la plantilla correcta y seleccione Enviar, como se muestra en la imagen.

Mienself Active Directory Certificate Services - Collab CA	Listine.
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.

<b>Laved Request</b>			_
Base-64-encoded certificate request (CMC or PNCS #10 or PNCS #7)	Inthky213/2p0tBornpringe GR7052at1y0e74K20pp4Y gDumonkpg5y 2ndgalogddWoof2CodMare BgWD0ycBgA0M =====BD_CERTIFICATE	AS-GopT_200+g TSOubBOJBOB7u92y894 ORQMEstaTIONSND107 REQUEST	*
e reaction and the	4	1	
Additional Attribu	CalManager CUCH	Y	
Altribules			
		Submit >	

Paso 10. Por último, seleccione Base 64 codificada y Descargar cadena de certificados; el archivo generado se puede cargar ahora en CUCM.



#### Verificación

El procedimiento de verificación es en realidad parte del proceso de configuración.

#### Troubleshoot

Actualmente no hay información de troubleshooting específica disponible para esta configuración.

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).