# Crea modelli di certificato CA di Windows per CUCM

Sommario
Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Configurazione
Modello Callmanager / Tomcat / TVS
Modello IPSec
Modello CAPE
Genera una richiesta di firma del certificato
Verifica
Risoluzione dei problemi

### Introduzione

In questo documento viene descritta una procedura dettagliata per creare modelli di certificato in Autorità di certificazione (CA) basate su Windows Server.

### Prerequisiti

#### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CUCM versione 11.5(1).
- È inoltre consigliabile avere una conoscenza di base dell'amministrazione di Windows Server

#### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Le informazioni fornite in questo documento si basano sulla versione 11.5(1) di CUCM.
- Microsoft Windows Server 2012 R2 con i servizi CA installati.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Premesse

Questi modelli di certificato sono conformi ai requisiti di estensione X.509 per ogni tipo di certificato Cisco Unified Communications Manager (CUCM).

Esistono cinque tipi di certificati che possono essere firmati da una CA esterna:

Certificato	Utilizzo	Servizi interessati
CallManager	Presentato durante la registrazione sicura del dispositivo, può firmare i file CTL (Certificate Trust List)/ITL (Internal Trust List), utilizzati per interazioni protette con altri server, ad esempio i trunk SIP (Secure Session Initiation Protocol).	· Cisco Call Manager · Cisco CTI Manager ·Cisco TFTP
tomcat	Presentato per le interazioni HTTPS (Secure Hypertext Transfer Protocol).	·Cisco Tomcat · Single Sign-On (SSO) · Mobilità di estensione · Directory aziendale
ipsec	Utilizzato per la generazione di file di backup, nonché per l'interazione di IPsec (IP Security) con i gateway Media Gateway Control Protocol (MGCP) o H323.	<ul> <li>Cisco DRF Master</li> <li>Cisco DRF locale</li> </ul>
CAPF	Utilizzato per generare certificati LSC (Locally Significant Certificates) per telefoni.	<ul> <li>Funzione proxy Cisco</li> <li>Certificate Authority</li> </ul>
TVS	Utilizzato per creare una connessione al servizio di verifica attendibilità (TVS), quando i telefoni non sono in grado di autenticare un certificato sconosciuto.	<ul> <li>Servizio di verifica attendibilità</li> <li>Cisco</li> </ul>

Nota: il certificato IPSec non è correlato al master DRF Cisco e a Cisco DRF Local poiché nelle versioni più recenti viene utilizzato il certificato Tomcat. Non è prevista l'aggiunta di questa modifica alla versione 12.5 o precedenti.

Ognuno di questi certificati ha alcuni requisiti di estensione X.509 che devono essere impostati, altrimenti si possono verificare comportamenti errati su uno qualsiasi dei suddetti servizi:

Certificato	Utilizzo chiavi X.509	Utilizzo chiavi esteso X.509
CallManager	Firma digitale · Crittografia · Crittografia dei dati	<ul> <li>Autenticazione server Web</li> <li>Autenticazione client Web</li> </ul>
tomcat	Firma digitale · Crittografia · Crittografia dei dati	<ul> <li>Autenticazione server Web</li> <li>Autenticazione client Web</li> </ul>
ipsec	Firma digitale · Crittografia · Crittografia dei dati	<ul> <li>Autenticazione server Web</li> <li>Autenticazione client Web</li> <li>Sistema terminale IPsec</li> </ul>
CAPF	Firma digitale · Firma certificato · Crittografia	<ul> <li>Autenticazione server Web</li> <li>Autenticazione client Web</li> </ul>
TVS	Firma digitale · Crittografia · Crittografia dei dati	<ul> <li>Autenticazione server Web</li> <li>Autenticazione client Web</li> </ul>

Per ulteriori informazioni, fare riferimento alla <u>Guida alla sicurezza per Cisco Unified</u> <u>Communications Manager</u>

### Configurazione

Passaggio 1. In Windows Server, selezionare Server Manager > Strumenti > Autorità di certificazione, come mostrato nell'immagine.

<u>L</u>		Server Manager		- 0 -
€⊕ - Server Ma	nager • Dashboard	·@	)  🗗 🏎 🖪	
Control Server  Local Server  A AD CS  AD CS  AD DS  AD DS  AD LOS  AD NS  File and Storage Services  I  I  I  I  I  I  I  I  I  I  I  I  I	WELCOME TO SERVER MANAGER	figure this local server dd roles and features dd other servers to manage reate a server group onnect this server to doud service	8	Active Directory Relaximistrative Denter Active Directory Domains and Trutis Active Directory Uniteenpite Directory Services Service United Active Directory Module for Windows Prove/Shall Active Directory Services Active Directory Unite and Services Active Directory Unite and Computers ACV 15 Management ACV Edit Computer Management Directory Territors Computer Management Uniterest Vehiculation Services (0) Managem BCI Interest ACV Interest
	AD CS     Manageability     Events     Services     Performance     BPA results	AD DS 1 Manapeability Dents Services Parlormance BPA results	AD PS Manageability Events Services Performance BPA results	CORE Sata Sources (20-bit) CORE Sata Sources (20-bit) CORE Sata Sources (20-bit) Parlymanus Mantar Sources Sources Sources System Configuration Waard Sources System Configuration System Scheduler Windows Through with Advanced Sourcely Windows Through Stagraphic Windows Through Stagraphic
	AD LDS 1	CINS 1	File and Stor Senices	Windows Param Snell (48) Windows Param Snell (48) Windows Param Snell (52 (46)) Windows Sanar Backup

Passaggio 2. Selezionare la CA, passare a Modelli di certificato, fare clic con il pulsante destro del mouse sull'elenco e selezionare Gestisci, come mostrato nell'immagine.



#### Modello Callmanager / Tomcat / TVS

Nelle immagini successive viene visualizzata solo la creazione del modello CallManager, ma è possibile seguire gli stessi passaggi per creare i modelli di certificato per i servizi Tomcat e TVS. L'unica differenza consiste nel garantire che il nome del servizio corrispondente venga utilizzato per ogni nuovo modello al passaggio 2.

Passaggio 1. Individuare il modello Web Server, fare clic con il pulsante destro del mouse su di esso e selezionare Duplica modello, come mostrato nell'immagine.

2		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 Ar	uthentication	
	Web Server		4.1		The second second second	
	User Signature Only	1	4.1		Duplicate Template	
	🗟 User	1	3.1		All Tasks	
	Trust List Signing	1	3.1		Properties	
	Tomat CUCM	2	100.3	Serve	r repenses	
	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 Autho	noiteation

Passaggio 2. In Generale è possibile modificare il nome, il nome visualizzato, la validità e altre variabili del modello di certificato.

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 V		
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

Passaggio 3. Passare a Estensioni > Uso chiave > Modifica, come mostrato nell'immagine.

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	

Passaggio 4. Selezionate queste opzioni e fate clic su OK, come mostrato nell'immagine.

- Firma digitale
- Consenti scambio chiave solo con crittografia (cifratura chiave)
- Consenti crittografia dei dati utente

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

Passaggio 5. Passare a Estensioni > Criteri di applicazione > Modifica > Aggiungi, come mostrato nell'immagine.

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

Passaggio 6. Cercare Autenticazione client, selezionarlo e scegliere OK sia in questa finestra che in quella precedente, come mostrato nell'immagine.

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

Passaggio 7. Tornare al modello, selezionare Applica, quindi OK.

X

Passaggio 8. Chiudere la finestra Console modello certificato e tornare alla prima finestra, selezionare Nuovo > Modello di certificato da emettere, come mostrato nell'immagine.



Passaggio 9. Selezionare il nuovo modello CallManager CUCM e scegliere OK, come mostrato nell'immagine.

Select one Certificate Template to ena lote: If a certificate template that was information about this template has bee VI of the certificate templates in the org For more information, see Certificate	e on this Certification Auth cently created does not a replicated to all domain o nization may not be avail a Template Concepts.	nority. sppear on this list, you may need to wait until ontrollers. able to your CA.	
Name	Intended Purp	ose	~
Authenticated Session	Client Authenti	cation	
CA Exchange	Private Key An	chival	
Call Manager CUCM	Server Authen	tication, Client Authentication	=
CEP Encryption	Certificate Reg	uest Agent	
Code Signing	Code Signing		-
Cross Certification Authority	<ab< td=""><td></td><td></td></ab<>		
Enrolment Agent	Certificate Reg	uest Agent	
Enrollment Agent (Computer)	Certificate Req	uest Agent	
R Exchange Enrolment Agent (Offin	request) Certificate Req	uest Agent	
R Exchange Signature Only	Secure Email		
R Exchange Liser	Secure Final		V
		OK Cano	el

Passaggio 10. Ripetere tutti i passaggi precedenti per creare modelli di certificato per i servizi Tomcat e TVS in base alle esigenze.

#### Modello IPSec

Passaggio 1. Individuare il modello Web Server, fare clic con il pulsante destro del mouse su di esso e selezionare Duplica modello, come mostrato nell'immagine.

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

Passaggio 2. In Generale è possibile modificare il nome, il nome visualizzato, la validità e altre variabili del modello di certificato.

Subject Name	Sen	ver	Issuance F	Requirements
Superseded Templa	tes	Ede	nsions	Security
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

Passaggio 3. Passare a Estensioni > Uso chiave > Modifica, come mostrato nell'immagine.

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	

Passaggio 4. Selezionate queste opzioni e fate clic su OK, come mostrato nell'immagine.

- Firma digitale
- Consenti scambio chiave solo con crittografia (cifratura chiave)
- Consenti crittografia dei dati utente

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

Passaggio 5. Passare a Estensioni > Criteri di applicazione > Modifica > Aggiungi, come mostrato nell'immagine.

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 Extensions in Applicat Basic Co Certificat Issuance Key Usa	n extension included in t ion Policies onstraints te Template e Policies ige	, select it, his templa e Informati	and then o te:	click Edit.	
Description of Server Auth	of Application	on Policie:	3.		Edt
					~
	OK		Cancel	Apply	Help

x

Passaggio 6. Cercare Autenticazione client, selezionarla e quindi OK, come mostrato nell'immagine.

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

Passaggio 7. Selezionare di nuovo Add, cercare IP security end system, selezionarlo, quindi selezionare OK anche in questo caso e nella finestra precedente.

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

Passaggio 8. Tornare al modello, selezionare Apply (Applica), quindi OK, come mostrato nell'immagine.

	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

Passaggio 9. Chiudere la finestra della console Modelli di certificato e tornare alla prima finestra, passare a Nuovo > Modello di certificato da emettere, come mostrato nell'immagine.



Passaggio 10. Selezionare il nuovo modello IPSEC CUCM e scegliere OK, come mostrato nell'immagine.

elect one Certificate Template to ote: If a certificate template that ormation about this template has of the certificate templates in to or 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. he organization may not be available to your CA. <u>rtificate Template Concepts.</u>	
Name	Intended Purpose	1
Exchange Signature Only	Secure Email	
Exchange User	Secure Email	
😨 IPSec	IP security IKE intermediate	
PSEC CUCM	Server Authentication, IP security end system, Client Authentication	
Key Recovery Agent	Key Recovery Agent	
OCSP Response Signing	OCSP Signing	
RAS and IAS Server	Client Authentication, Server Authentication	
Router (Offline request)	Client Authentication	
Smartcard Logon	Client Authentication, Smart Card Logon	
Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
		1.1

#### Modello CAPF

Passaggio 1. Individuare il modello Root CA (CA radice) e fare clic con il pulsante destro del mouse su di esso. Quindi selezionate Duplica modello (Duplicate Template), come mostrato nell'immagine.

2		c	ertificate Ten	rplate	s Console		
File Action View Help							
🔶 🕂 🔂 🔂 🔂 🔂 🔂							
🗵 Certificate Templates (win12.cal	Template Display Nanke	Schema Version	Veni-	intend	ed Purposes		
	Router (Offline request)	1	4.3				
	Rent Certification Authority	1	5.1		Restants Townships		
	RNS and IAS Server	1	101.0	Ch.	Dupicate tempote		tion
	CCSP Response Signing	1	101.0	Q\$	All Tasks	10	
	E LOAPS	2	100.6	10	Properties		Server Authentication, Client A
	E Kay Recovery Agent	2	105.0	Car.			
	Enteros Authentication	2	110.0	0	Help		Hion, Smart Card Logon, KDC A
	PSEC QUOM	2	100.4	Sever	Authentication, IP security	end a	ystem, Clent Authentication
	IPSec (Offline request)	1	2.1				
	2 Plac	1	8.1				

Passaggio 2. In Generale è possibile modificare il nome, il nome visualizzato, la validità e altre variabili del modello di certificato.

Superseded Template	e l	Extensions	Security
Compatibility	General	Issuance	Requirements
Templete dealers areas			
Constant Con			
CAPFCOCM			
Template name:			
CAPF CUCM			
	_		
Validity period:	Rene	swal period:	_
5 years ❤		6 weeks	~
Publish certificate in A	ctive Directory		
Do not automatica	ly reenroll if a d	uplicate certificat	te exists in Active
Directory			
		_	
OK	Cancel	Apply	Help

Passaggio 3. Passare a Estensioni > Uso chiave > Modifica, come mostrato nell'immagine.

x

Compatibility	General	Issuance	Requirements
Superseded Temp	lates	Extensions	Security
To modify an extension	n, select it, and t	hen click Edt.	
Extensions included in Application Policie Basic Constraints Certificate Templa Issuance Policies	this template: s te Information		
			Edit
Description of Key Usa	sge:		
Digital signature Certificate signing CRL signing Critical extension.			~

Passaggio 4. Selezionate queste opzioni e fate clic su OK, come mostrato nell'immagine.

- Firma digitale
- Firma certificato
- Firma 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 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

Passaggio 5. Passare a Estensioni > Criteri di applicazione > Modifica > Aggiungi, come mostrato nell'immagine.

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

Passaggio 6. Cercare Autenticazione client, selezionarla e quindi scegliere OK, come mostrato nell'immagine.

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

Passaggio 7. Selezionare di nuovo Add, cercare IP security end system, selezionarlo, quindi selezionare OK anche su questo e sulla finestra precedente, come mostrato nell'immagine.

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

Passaggio 8. Tornare al modello, selezionare Apply (Applica), quindi OK, come mostrato nell'immagine.

	ject Name Server Issuance Requirement		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 ientication	on Policies	IC		Edit
Description ( Client Author IP security ( Server Author)	of Application end system entication	on Policies			Edit

X

Passaggio 9. Chiudere la finestra della console Modelli di certificato e tornare alla prima finestra, passare a Nuovo > Modello di certificato da emettere, come mostrato nell'immagine.



Passaggio 10. Selezionate il nuovo modello CAPF CUCM e OK, come mostrato nell'immagine.

B		Enable Certificate Templates	x
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></ab>	
3	Enrolment Agent	Certificate Request Agent	
	Enrolment Agent (Computer)	Certificate Request Agent	
3	Exchange Signature Only	Secure Email	
	Exchange User	Secure Email	
	IPSec	IP security IKE intermediate	
1.1	IPSEC CLICM	Server A thentication IP security end system Client Authentication	~
		OK Cano	el

Genera una richiesta di firma del certificato

Utilizzare questo esempio per generare un certificato CallManager con l'utilizzo dei nuovi modelli creati. La stessa procedura può essere utilizzata per qualsiasi tipo di certificato. È sufficiente selezionare il certificato e i tipi di modello di conseguenza:

Passaggio 1. In CUCM, selezionare Amministrazione sistema operativo > Protezione > Gestione certificati > Genera CSR.

Passaggio 2. Selezionate queste opzioni e selezionate Genera (Generate), come mostrato nell'immagine.

- Scopo certificato: CallManager
- Distribuzione: <può trattarsi di un solo server o di più SAN>

Generate Close			
itatus-			
🚹 Warning: Generating :	a new CSR for a specific certificate type	will overwrite the ex	isting CSR for that type
Generate Certificate Sig	ning Request		
ertificate Purpose **	CallManager		
istribution*	Multi-server(SAN)	•	
ommon Name*	115PUB-ms.maucabal.lab		
bject Alternate Name	s (SANs)		
uto-populated Domains	1159U8.maucabal.lab 1155U8.maucabal.lab		
arent Domain	maucabal.lab		
arent Domain Kher Domains	maucabal.lab	AA	Choose File No file chosen Please import .TXT file only. For more information please refer to the notes in the Help Section
tarent Domain Other Domains	maucabal.lab	A	Choose File No file chosen Rease import .TxT file only. For more information please refer to the notes in the Help Section
arent Domain ther Domains	maucabal.lab	*	Choose File No file chosen Please import .TXT file only. For more information please refer to the notes in the Help Section
ev Type ** ev Length	RSA 2048	*	Choose File No file chosen Rease import .TxT file only. For more information please refer to the notes in the Help Section

Passaggio 3. Viene generato un messaggio di conferma, come mostrato nell'immagine.



Passaggio 4. Nell'elenco dei certificati cercare la voce con il tipo Solo CSR e selezionarla, come mostrato nell'immagine.

Certificate List							
Constant Set o	iner 🔒 chen cestance	nun chan (	il, con	rate CSR 👔 Dounteed CSR			
Status 16 records for	und						
Certificate List	(1 - 50 of 56)						Rows per Pape 50
Find Certificate List	t where Certificate •   begi	na with 💌		Fied Cear	ritter 💠 🚥		
Certificate *	Common Name	7.pe	Key Type	Datribution	baued fiv	Expiration	Osciption
autho	autric admin	Self-	RSA	115PUB.maucabal.lab	AUTH2_admin	01/27/2038	Self-signed certificate penerated by system
Califfunaper	115PUB-ma.maucabal.lab	CSR Only	85.8	Hulti-server(SAN)	-	-	
canadaba	TURNET RECEIPTING	signed	No.4	1110/08/84003038-140	115PUB.maucabal.lab	05/30/2023	Self-signed certificate penerated by system
Califfunaper- ECDSA	115PUB-EC.maucabal.lab	Self- signed	00	115PUB.maucabal.lab	115PUB- EC.mascabal.lab	63/94/2023	Self-signed certificate generated by system
Califianaper-trust	115938-BC-mascabal.lab	Self- signed	90	115P08.maucabal.lab	115PVB- EC:maucabal.lab	03/94/2023	Trust Cartificate
	and the second			and the second			

Passaggio 5. Nella finestra pop-up, selezionare Download CSR, quindi salvare il file sul computer.

CSR Details for 115PUB-	SR Details for 115PUB-ms.maucabal.lab, CallManager			
X Delete 🔋 Download	CSR			
Status Status: Ready				
Certificate Settings				
File Name Certificate Purpose Certificate Type Certificate Group Description(friendly name)	CallManager.csr CallManager certs product-cm			
Certificate File Data PKCS10 Request: [ Version: 0 Subject: CN=115PUB-ms. SubjectPKInfo: RSA (1.2.8 Key value: 3082010a0282010100c18 cabc144fd5f1538efe514fd f902277c2ee55d7e5a4d68 9fbd3d5aae5f4f02237ecab 79d661582952880d98b32 9be410e8d3b4e1f18a89bc 5a9467d4963f226b6ab05c 6b25a37e84cd020301000 Attributes: [ Requested Extensions [	maucabal.lab, OU=clsco, O=clsco, L=clsco, ST=clsco, C=MX 440.113549.1.1.1) a6119e66450eef211e6ac9a2349f3466616bd77017095303de7d 8207d3ddea43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34 10f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2 ca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b 90d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c cd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164 57b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c			
Delete Download CSR	1			

Passaggio 6. Nel browser passare a questo URL e immettere le credenziali dell'amministratore del controller di dominio: https://<yourWindowsServerIP>/certsrv/.

Passaggio 7. Passare a Richiedi un certificato > Richiesta avanzata di certificati, come mostrato nell'immagine.

Microsoft Active Directory Certificate Services - Collab 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

#### Passaggio 8. Aprire il file CSR e copiarne il contenuto:

CallManager - Notepad	_ 0	X	<b>C</b>
File Edit Format View Help			
BEGIN CERTIFICATE REQUESTHIDNOCCAhuCAQAubjELMAkGABUEBHNCTVgxDjAMBgHVBAgTBMhpc2Hv4Q4u aXNjb2EOMAuGABUECHNFY2l1Y28xDjAMBgNVBAsTBMhpc2NvMR8uHQYDVQQDExYxMTVQVUIB5NubWF1Y2FiYMaubGFIMID G9u8BAQEFAADCAQBAMIJBCgKCAQEAuYphGeZkU07yEeasmiNJ882mFr13AXCVMD3n3Kv8RP1fFTjv5RT9ggfT3epDs1zk8F 10MbQafNNPkCJ3uu5V1+Wk1oD4yWtvRu1T0yHGFGY293N2Xai3paLefdjdKfvT1ar19PAIN+yrynTPbi2bRjgFGunuF7mPg 2t51mFYKVKIDZizKQIEEXotjL+sKxZKzpojYR+oaDuoLZo9NKD3vkE0jTtOHxiom804WEY65eA5/5/TGo/dbkXP5HNP17H5 8ia2quAnt/knNTa03u2HE/Yn12sMDh4bRb12mPFbjGs1o36EzQIDAQABoIGAMH4GCSqGSIb30QEJDjFxHGBuHQYDVR81BBY HAuEGCCsGAQUFBuHCMAsGA1UdDuQEAuIEsDB8BgNVHREE0jA4ghMxHTVQVUIubWF1Y2FiYMaubGFighMxHTVTVUIubWF1Y2 xtYXVjYNJhbC5sYNLuOQY3KoZIhvcNAQELBQADggEBAIgutjgKN/LLvLogSI/tba62o/ViXcI2QmuH+SIyuiIUHb55fRu 4P93uckGcSrivInwBT69hOBYx8T8hDc5LhdkTfmEd7XHMEEbZ45cuFbaYnugMUMYQ8c1p5UMhck3yzQpQeL5pjcv3LCPio 1Yhky213/2p0t9oVg&vynR96opVL2N+gG570hImtIjGe74X2Qqu4YT50uHM93EcH7u92y8PdKQa1fP+oAGPXInocta2Nojn ps8gs9gxNXXcf8DcdWu+eG8qWRsnsZhMUNDlo7a1Qbyxdf7r7dbSqW8Gyo8qkM+END_CERTIFICATE_REQUEST	MYDVQQHEW/ SIJANBgkohk: SOBIJAyv9c: YJLNwKfc0z PIWkalGfU1 #AYIKwYBBQ SAYIKwYBBQ SAYIKwYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBBQ SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIK SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIK SAYIK SAYIK SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIK SAYIKWYBC SAYIKWYBC SAYIKWYBC SAYIK SA	5 v x 5 U ad o y	
C #		-	×.

Passaggio 9. Incollare il CSR nel campo Richiesta certificato con codifica Base 64. In Modello di certificato selezionare il modello corretto e scegliere Invia, come illustrato nell'immagine.

<b>Material Address Develops Cardinate Services — Collab Ca</b>
server states have been been and the server states and the server and the server states and th

#### 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.

Hom

Saved Request			_
Base-64-encoded certificate request (CMC or	115Ay213/2p0t6rmp+vyx864oprt20*p db70h2m120+7482ppsKT250uh802bcH7u92y884 gDunoskpgTy JebgeSp8006cf20cdMa++00q88ass2100555b1c7		^
PNCS #10 or	Principal Contractions of		
PRES #T):	a state of the second s	a second s	
			100
Certificate Template:			
	CalManager CUCH	-	
Additional Attributes:			
Attributes			

Submit >

Passaggio 10. Infine, selezionare Base 64 encoded (Codificato in base 64) e Download certificate chain (Scarica catena di certificati), il file generato può ora essere caricato in CUCM.



#### Verifica

La procedura di verifica fa effettivamente parte del processo di configurazione.

#### Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi per questa configurazione.

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).