Erstellen von Windows CA-Zertifikatvorlagen für CUCM

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren CallManager/Tomcat/TVS-Vorlage IPsec-Vorlage CAPF-Vorlage Generieren einer Zertifikatsignierungsanforderung Überprüfung Fehlerbehebung

Einleitung

Dieses Dokument beschreibt eine schrittweise Vorgehensweise zum Erstellen von Zertifikatvorlagen auf Windows Server-basierten Zertifizierungsstellen, die die X.509-Erweiterungsanforderungen für jeden Typ eines Cisco Unified Communications Manager (CUCM)-Zertifikats erfüllen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CUCM-Version 11.5(1) oder höher
- Grundkenntnisse der Windows Server-Administration werden ebenfalls empfohlen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Die Informationen in diesem Dokument basieren auf CUCM-Version 11.5(1) oder höher.
- Microsoft Windows Server 2012 R2 mit installierten Zertifizierungsstellendiensten.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Es gibt fünf Zertifikatstypen, die von einer externen Zertifizierungsstelle signiert werden können:

Zertifikat	Nutzung	Betroffene Services
CallManager	Wird bei der Registrierung sicherer Geräte angezeigt und kann CTL- (Certificate Trust List)/ITL-Dateien (Internal Trust List) signieren, die für sichere Interaktionen mit anderen Servern, z. B. sicheren SIP-Trunks (Session Initiation Protocol), verwendet werden.	 Cisco Call Manager Cisco CTI Manager Cisco TFTP
tomcat	Präsentiert für HTTPS-Interaktionen (Secure Hypertext Transfer Protocol).	 Cisco Tomcat Single Sign-On (SSO) Anschlussmobilität Firmenverzeichnis
IPsec	Verwendet für die Erstellung von Sicherungsdateien sowie für die IP Security (IPsec)-Interaktion mit MGCP- (Media Gateway Control Protocol) oder H323-Gateways.	Cisco DRF Master · Cisco DRF Lokal
CAPF	Wird zum Generieren von LSC- Zertifikaten (Locally Significant Certificates) für Telefone verwendet.	 Cisco Certificate Authority Proxy-Funktion
TVS	Verbindung mit dem Trust Verification Service (TVS) herzustellen, wenn die Telefone ein unbekanntes Zertifikat nicht authentifizieren können.	 Cisco Trust Verification Service

Für jedes dieser Zertifikate müssen einige X.509-Erweiterungsanforderungen festgelegt werden. Andernfalls können Sie bei den oben genannten Services auf Fehlverhalten stoßen:

Zertifikat	X.509- Schlüsselverwendun g		X.509 Extended Key- Verwendung
CallManager	 Digitale Signatur Schlüsselverschlüss elung 	•	Webserver-Authentifizierung Webclient-Authentifizierung
	Datenverschlüsselun g · Digitale Signatur ·		
tomcat	Schlüsselverschlüss elung • Datenverschlüsselun	•	Webserver-Authentifizierung Webclient-Authentifizierung

	-		
	 Digitale Signatur 		
IPsec	Schlüsselverschlüss elung Datenverschlüsselun	•	Webserver-Authentifizierung Webclient-Authentifizierung IPsec-Endsystem
CAPF	g · Digitale Signatur · Zertifikatzeichen · Schlüsselverschlüss elung · Digitale Signatur ·	•	Webserver-Authentifizierung Webclient-Authentifizierung
TVS	Schlüsselverschlüss elung • Datenverschlüsselun g	•	Webserver-Authentifizierung Webclient-Authentifizierung

Weitere Informationen finden Sie im <u>Sicherheitsleitfaden für Cisco Unified Communications</u> <u>Manager.</u>

Konfigurieren

g

Schritt 1: Navigieren Sie auf dem Windows Server zu **Server Manager > Tools > Certification Authority**, wie im Bild dargestellt.



Schritt 2: Wählen Sie Ihre Zertifizierungsstelle aus, navigieren Sie zu Zertifikatvorlagen, klicken

Sie mit der rechten Maustaste auf die Liste, und wählen Sie Verwalten, wie im Bild dargestellt.

🦕 certsrv -	(Certification Authority (Local)\Colla	b CA\Certificate Templates] 📃 🗖 🗙
File Action View Help		
Certification Authority (Local) Collab CA Coll	Name CAPF2 CAPF CUCM Tomcat CUCM Directory Email Replication Kerberos Authentication EFS Recovery Agent Basic EFS Domain Controller Web Server Computer User Subordinate Certification Authority Administrator	Intended Purpose Server Authentication, IP security end s Server Authentication, IP security end s Server Authentication, IP security end s Server Authentication, Client Authentic Directory Service Email Replication Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication, Server Authentic Server Authentication, Server Authentic Encrypting File System, Secure Email, CL «All» Microsoft Trust List Signing, Encrypting
Starts Certificate Templates snapin		Arrange Icons
		Help

CallManager/Tomcat/TVS-Vorlage

Die nächsten Bilder zeigen nur die Erstellung der CallManager-Vorlage. Die gleichen Schritte können jedoch auch ausgeführt werden, um die Zertifikatvorlagen für die Tomcat- und TVS-Dienste zu erstellen. Der einzige Unterschied besteht darin, dass in Schritt 2 für jede neue Vorlage der entsprechende Servicename verwendet wird.

Schritt 1: Suchen Sie die **Webserver**-Vorlage, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Vorlage duplizieren** aus, wie im Bild dargestellt.

3	Certificate Templates 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				
	Web Server	1	4.1	_	and the second second	_			
	Juser Signature Only	1	4.1		Duplicate Template				
	3 User	1	3.1		All Tasks				
	Trust List Signing	1	3.1		Properties				
	Tomcat CUCM	2	100.3	Serve	risperses	- in			
	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 Av	uthentication, Server Auther	ntication			

Schritt 2: Unter **Allgemein** können Sie den Namen der Zertifikatvorlage, den Anzeigenamen, die Gültigkeit usw. ändern.

Properties of New Template						
Subject Name Server 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:	Template name: CallManager CUCM Validty period: Renewal period:					
Publish certificate in Do not automatic Directory	Active Di	rectory oil if a dupl	icate certificate	, exists in Active		
OK	(Cancel	Apply	Help		

Schritt 3: Navigieren Sie zu **Erweiterungen > Schlüsselverwendung > Bearbeiten**, wie im Bild dargestellt.

	Pro	perties	of New	Template	X	
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation	
Subject	Name	Se	ver	Issuance	Requirements	
Superse	Superseded Templates Edensions 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 Signature n Digital sign Allow key e	of Key Usag equirements ature exchange or	ge: : ily with ke	ry encryptic	m	Edt	
Critical exte	OK		Cancel	Apply		

Schritt 4: Wählen Sie diese Optionen aus, und wählen Sie OK, wie im Bild dargestellt.

- Digitale Signatur
- Schlüsselaustausch nur mit Schlüsselverschlüsselung zulassen (Schlüsselverschlüsselung)
- Verschlüsselung von Benutzerdaten zulassen

	Pro	perties of New	/ Template		x		
Compatibility Subject	General Name	Request Handling Server	Cryptography Issuance	Key Attesta Requirements	tion		
	E	dit Key Usage E	xtension	-	x		
Specify the extension.	required sig	nature and security	options for a ke	y usage			
Signature Diotal	signature						
Signati	ure is proof	of origin (nonrepudi	ation)				
Certific	ate signing						
CRL si	gning						
Encryption O Allow	key exchar	ge without key end	ryption (key agr	eement)			
 Alow 	key exchan	ge only with key en	cryption (key en	cipherment)			
⊻	Allow encry	ption of user data					
Make thi	Make this extension critical OK Cancel						
	ОК	Cancel	Apply	Help	,		

Schritt 5: Navigieren Sie zu **Erweiterungen > Anwendungsrichtlinien > Bearbeiten > Hinzufügen**, wie im Bild dargestellt.

	Pro	perties	of New	Template)
Compatibility	General	Request	Handling	Cryptography	Key Attestation
Subject Na	ame	Ser	ver	Issuance F	Requirements
Supersede	ed Templa	tes	Exte	nsions	Security
To modify an	extension,	select it,	and then c	lick Edit.	
Extensions in	cluded in t	his templa	te:		
Application	n Policies				
Basic Cor	nstraints				
Centricate	Policies	e informati	on		
Key Usad	e				
					Edit
Description of	Application	on Policies	9:		
Server Authe	ntication				^
					~
	OK	(Cancel	Apply	Help

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

Schritt 6: Suchen Sie nach **Client Authentication (Client-Authentifizierung**), wählen Sie sie aus, und wählen Sie **OK** für dieses und das vorherige Fenster aus, wie im Bild gezeigt.

Properties of New Template							
Compatibility General Request Handing Cryptography Key Attestation Subject Name Server Issuance Requirements C Edit A policities Deliving Education X 4 Add 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: Any Purpose ^ Attestation Identity Key Certificate ^ Certificate Request Agent III Citent Authentication IIII Code Signing CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Encryption Document Signing Domain Name System (DNS) Server Trust							
OK Cancel							
OK Cancel Apply Help							

Schritt 7. Wählen Sie auf der Vorlage die Option Übernehmen und dann OK aus.

Pro	perties	of New	Template		x		
Compatibility General	Request	Handling	Cryptograph	y Key Attest	stion		
Subject Name	Ser	ver	Issuance	Requirements	_		
Superseded Templa	tes	Ed Ed	ensions	Security	_		
To modify an extension, select it, and then click Edit. Extensions included in this template:							
Application Policies							
Basic Constraints							
Certificate Template	e Informat	ion					
Issuance Policies							
Key Usage							
				Edit			
Description of Application	n Policie	s:					
Client Authentication Server Authentication					~		
ОК		Cancel	Apply	Helç)		

Schritt 8: Schließen Sie das Fenster **Zertifikatvorlagenkonsole**, und navigieren Sie im ersten Fenster zu **Neu > Zertifikatvorlage zur Ausgabe**, wie im Bild dargestellt.



Schritt 9. Wählen Sie die neue **CallManager-CUCM-**Vorlage aus, und wählen Sie **OK** aus, wie im Bild gezeigt.

	Enable	Certificate Templates	X
Sel No info All Fo	ect one Certificate Template to enable on this 0 te: If a certificate template that was recently cre smation about this template has been replicate of the certificate templates in the organization m r more information, see <u>Certificate Templa</u>	Certification Authority. sated does not appear on this list, you may need to wait until d to all domain controllers. nay not be available to your CA. <u>site Concepts.</u>	
N	lame	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	Enrolment 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	~
		OK Cance	k

Schritt 10. Wiederholen Sie alle vorherigen Schritte, um nach Bedarf Zertifikatvorlagen für die Tomcat- und TVS-Dienste zu erstellen.

IPsec-Vorlage

Schritt 1: Suchen Sie die Webserver-Vorlage, klicken Sie mit der rechten Maustaste darauf, und wählen Sie Vorlage duplizieren aus, wie im Bild dargestellt.

2		c	Certificate 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 A	uthentication	
	Web Server		4.1	_	and the second second	-
	🗟 User Signature Only	1	4.1		Duplicate Template	
	3 User	1	3.1		All Tasks	
	Trust List Signing	1	3.1		Properties	
	Tomcat CUCM	2	100.3	Serve	risperses	- in
	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 Auther	tication

Schritt 2: Unter **Allgemein** können Sie den Namen der Zertifikatvorlage, den Anzeigenamen, die Gültigkeit usw. ändern.

Properties of New Template										
Subject Name Server Issuance Requirements										
Superseded Templa	tes	Ede	Extensions Security							
Compatibility General	Request	Handling	Cryptography	Key Attestation						
Template display name	Template display name:									
IPSEC CUCM										
Template name: IPSEC CUCM Validity period: 2 years v	Template name: IPSEC CUCM Validity period: 2 years % </td									
Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory										
OK		Cancel	Apply	Help						

Schritt 3: Navigieren Sie zu **Erweiterungen > Schlüsselverwendung > Bearbeiten**, wie im Bild dargestellt.

Properties of New Template								
Compatibility	General	Request	Handling	Cryptograph	y Key Attestation			
Subject	Name	Se	ver	Issuance	Requirements			
Superse	Superseded Templates Edensions 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 Signature n Digital sign Allow key e	Edt Description of Key Usage: Signature requirements: Digital signature Allow key exchange only with key encryption							
OK Cancel Apply Help								

Schritt 4: Wählen Sie diese Optionen aus, und wählen Sie OK, wie im Bild dargestellt.

- Digitale Signatur
- Schlüsselaustausch nur mit Schlüsselverschlüsselung zulassen (Schlüsselverschlüsselung)
- Verschlüsselung von Benutzerdaten zulassen

	Properties of New Template							
Compatibility Subject	General Name	Request Handling Server	Cryptography Issuance	Key Attesta Requirements	tion			
	E	dit Key Usage E	xtension	-	x			
Specify the extension.	required sig	nature and security	options for a ke	y usage				
Signature Diotal	signature							
Signati	ure is proof	of origin (nonrepudi	ation)					
Certific	ate signing							
CRL si	gning							
Encryption O Allow	key exchar	ge without key end	ryption (key agr	eement)				
 Alow 	key exchan	ge only with key en	cryption (key en	cipherment)				
⊻	Allow encry	ption of user data						
Make thi	Make this extension critical OK Cancel							
	ОК	Cancel	Apply	Help	,			

Schritt 5: Navigieren Sie zu **Erweiterungen > Anwendungsrichtlinien > Bearbeiten > Hinzufügen**, wie im Bild dargestellt.

	Pro	perties	of New	Template		×	
Compatibility	General	Request	Handling	Cryptography	Key Att	estation	
Subject N	lame	Ser	ver	Issuance	Requireme	ints	
Supersec	ded Templa	tes	Ede	ensions	Secu	rity	
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							
Edt Description of Application Policies:							
[ОК		Cancel	Apply		Help	

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

Schritt 6: Suchen Sie nach **Client Authentication (Client-Authentifizierung**), wählen Sie sie aus, und klicken Sie dann auf **OK**, wie im Bild gezeigt.

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.
Any Purpose Attestation Identity Key Certificate Certificate Request Agent Citeral 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
New OK Cancel
OK Cancel Apply Help

Schritt 7. Wählen Sie erneut **Hinzufügen** aus, suchen Sie nach dem **IP-Sicherheits-Endsystem**, wählen Sie es aus, und wählen Sie dann in diesem und im vorherigen Fenster die Option **OK** aus.

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

Schritt 8: Wählen Sie auf der Vorlage Apply (Übernehmen) und dann OK, wie im Bild dargestellt.

Properties of New Template							
Subject Name	Ser	Server Issue		Requirements			
Compatibility General	Request	Handing	Cryptography	Key Attestation			
Superseded Templa	plates 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 Apolicati	on Policie			Edt			
Client Authentication IP security end system Server Authentication				< >			
ОК		Cancel	Apply	Help			

Schritt 9. Schließen Sie das Fenster **Zertifikatvorlagen-Konsole**, und navigieren Sie im ersten Fenster zu **Neu > Zertifikatvorlage zur Ausgabe**, wie im Bild dargestellt.



Schritt 10. Wählen Sie die neue **IPSEC-CUCM**-Vorlage aus, und wählen Sie auf **OK** aus, wie im Bild gezeigt.

	Enable Certificate Templates	x
Select one Certificate Template Note: If a certificate template th information about this template in All of the certificate templates in For more information, see <u>C</u>	to enable on this Certification Authority. at 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. ertificate Template Concepts.	
Name	Intended Purpose	
Exchange Signature Only Exchange User IPSec	Secure Email Secure Email IP security IKE intermediate	
IPSEC CUCM	Server Authentication, IP security end system, Client Authentication	
Key Recovery Agent OCSP Response Signing RAS and IAS Server Router (Offline request)	Key Recovery Agent OCSP Signing Client Authentication, Server Authentication Client Authentication	-
Smartcard Logon	Client Authentication, Smart Card Logon	
Smartcard User	Secure Email, Client Authentication, Smart Card Logon Microsoft Trust List Signing	v
	OK Can	cel

CAPF-Vorlage

Schritt 1: Suchen Sie die Vorlage für die **Stammzertifizierungsstelle**, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie anschließend **Vorlage duplizieren**, wie im Bild dargestellt.

3			ertificate Te	mplate	s Console		
File Action View Help							
** 🗊 🗊 🖬 📰							
2 Certificate Templates (win12.col	Template Display Name	Schema Version	Veni-	Intend	Red Purposes		2
	Router (Offline request)	1	4.1				
	Root Certification Authority	1	5.1		Destants Transition		
	RAS and IAS Server	2	101.0	Ch	Dupicate rempiate		dien
	CCSP Response Signing	3	101.0	00	All Tasks		
	E LOAPS	2	100.6	10	Properties		Server Authentication, Client A
	Key Recovery Agent	2	105-0	Ee.			
	Enteros Authentication	2	110.0	Ch	Help		ition, Smart Card Logon, KDC A
	B PSEC CUCM	2	100.4	Seve	Authentication, IP security	rend	system, Client Authentication
	IPSec (Offline request)	1	7.1				
	E Plet	1	8.1				

Schritt 2: Unter **Allgemein** können Sie den Namen der Zertifikatvorlage, den Anzeigenamen, die Gültigkeit usw. ändern.

Properties of New Template							
Superseded Templa	Superseded Templates Extensions Securit						
Compatibility	Gene	n	Issuance	Requirements			
Template display name:							
CAPF CUCM							
Template name: CAPF DUCM							
Validity period: 5 years v]	Renew 6	al period: weeks	~			
Publish certificate in Do not automatic Directory	Active Dir ally reenro	rectory oll if a dup	licate certificat	e exists in Active			
ОК		Cancel	Apply	Help			

Schritt 3: Navigieren Sie zu **Erweiterungen > Schlüsselverwendung > Bearbeiten**, wie im Bild dargestellt.

Properties	of New	Template		X
Compatibility Gene	ral	Issuance	Requirements	
Superseded Templates	Ed	ensions	Security	
To modify an extension, select it,	and then	click Edit.		
Extensions included in this templa	te:			
Application Policies				
Basic Constraints				
Certificate Template Informati	on			
Issuance Policies				
Key Usage				
			Edit	
Description of Key Usage:				
Signature requirements: Digital signature Certificate signing CRL signing			-	^
Critical extension.				_
				_
ОК	Cancel	Apply	Help	

Schritt 4: Wählen Sie diese Optionen aus, und wählen Sie OK, wie im Bild dargestellt.

- Digitale Signatur
- Zertifikatssignatur
- CRL-Signierung

	Pro	perties of New	/ Template		x
Compatibility Subject	General Name	Request Handling Server	Cryptography Issuance	Key Attesta Requirements	tion
	E	dit Key Usage E	xtension	-	x
Specify the extension.	required sig	nature and security	options for a ke	y usage	
Signature Diotal	signature				
Signati	ure is proof	of origin (nonrepudi	ation)		
Certific	ate signing				
CRL si	gning				
Encryption O Allow	key exchar	ge without key end	ryption (key agr	eement)	
 Alow 	key exchan	ge only with key en	cryption (key en	cipherment)	
⊻	Allow encry	ption of user data			
Make thi	s extension	ortical	ок	Cancel	
	ОК	Cancel	Apply	Help	,

Schritt 5: Navigieren Sie zu **Erweiterungen > Anwendungsrichtlinien > Bearbeiten > Hinzufügen**, wie im Bild dargestellt.

	Pro	perties	of New	Template)
Compatibility	General	Request	Handling	Cryptography	Key Attestation
Subject Na	ame	Ser	ver	Issuance F	Requirements
Supersede	ed Templa	tes	Exte	nsions	Security
To modify an	extension,	select it,	and then c	lick Edit.	
Extensions in	cluded in t	his templa	te:		
Application	n Policies				
Basic Cor	nstraints				
Centricate	Policies	e informati	on		
Key Usad	e				
					Edit
Description of	Application	on Policies	9:		
Server Authe	ntication				^
					~
	OK	(Cancel	Apply	Help

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

Schritt 6: Suchen Sie nach **Client Authentication (Client-Authentifizierung**), wählen Sie sie aus, und wählen Sie dann **OK** aus, wie im Bild gezeigt.

Properties of New Template
Compatibility General Request Handling Cryptography Key Attestation Subject Name Server Issuance Requirements S Fully Acceleration Publicity 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:
OK Cancel
OK Cancel Apply Help

Schritt 7. Wählen Sie erneut **Hinzufügen** aus, suchen Sie nach dem **IP-Sicherheits-Endsystem**, wählen Sie es aus, und wählen Sie dann OK für dieses und das vorherige Fenster aus, wie im Bild gezeigt.

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

Schritt 8: Wählen Sie auf der Vorlage Apply (Übernehmen) und dann OK, wie im Bild dargestellt.

Pro	operties	of New	Template	X			
Subject Name	bject Name Server Issuance Requiremen		Requirements				
Compatibility General	Request	Handing	Cryptography	Key Attestation			
Superseded Templa	stes	Ede	insions	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 Apolicati	on Policie			Edt			
Client Authentication IP security end system Server Authentication				< >			
ОК		Cancel	Apply	Help			

Schritt 9. Schließen Sie das Fenster **Zertifikatvorlagen-Konsole**, und navigieren Sie im ersten Fenster zu **Neu > Zertifikatvorlage zur Ausgabe**, wie im Bild dargestellt.



Schritt 10. Wählen Sie die neue **CAPF CUCM-**Vorlage aus, und wählen Sie **OK**, wie im Bild dargestellt.

8	Enable Certificate Templates	x
Select one Certificate Template to Note: if a certificate template that information about this template ha All of the certificate templates in th For more information, see <u>Cer</u>	e enable on this Certification Authority. was recently created does not appear on this list, you may need to wait until s been replicated to all domain controllers. he organization may not be available to your CA. tificate Template Concepts.	
Name	Intended Purpose	~
Authenticated Session CA Exchange	Client Authentication Private Key Archival	
CAPF CUCM	Server Authentication, IP security end system, Client Authentication	=
Code Signing Cross Certification Authority	Code Signing <al></al>	
Enrolment Agent	Certificate Request Agent Certificate Request Agent Secure Email	
Exchange User	Secure Email IP security IKE intermediate	
IPSEC CLICM	Server Authentication IP security end system Client Authentication	~
	OK Cano	;el

Generieren einer Zertifikatsignierungsanforderung

Verwenden Sie dieses Beispiel, um unter Verwendung der neu erstellten Vorlagen ein CallManager-Zertifikat zu generieren. Das gleiche Verfahren kann für jeden Zertifikatstyp verwendet werden. Sie müssen nur das Zertifikat und die Vorlagentypen entsprechend auswählen:

Schritt 1: Navigieren Sie auf CUCM zu OS Administration > Security > Certificate Management >

Generate CSR (Betriebssystemverwaltung > Sicherheit > Zertifikatsverwaltung > CSR erstellen).

Schritt 2: Wählen Sie diese Optionen aus, und wählen Sie Generate (Erstellen) aus, wie im Bild dargestellt.

- Zertifikatzweck: CallManager
- Distribution: < Dies kann entweder nur für einen Server oder mehrere SANs sein>

Generate 🔄 Close			
tatus			
Warning: Generating a	new CSR for a specific certificate type	will overwrite the ex	isting CSR for that type
anarata Castificata Sias	Ine Result		
entiticate formane II	anny kequesa		
eroncace Purpose	Califianaper	;	
surgeoun	(Psub-server(SAN)	•	
ammon Name	115PUB-ms.maucabal.lab		
abject Alternate Names	(SANS)		
into-populated Domains	115PU8.maucabal.lab 115SU8.maucabal.lab		
arent Domain	maucabal.lab		
ther Domains			Choses File No file choses
		_	Charles I and The Charles
			Please import .TXT file only. For more information please refer to the notes in the
			Help Section
		*	
			🛈 Add
ev Type**	RSA		
ey Length*	2048		
lash Algorithm*	SH4256		

Schritt 3: Es wird eine Bestätigungsmeldung generiert, wie im Bild dargestellt.

Generate Certificate Signing Request	
Generate 💽 Close	
r Status-	
Success: Certificate Signing Request Generated	
CSR export operation successful on the nodes [115PUB.maucabal.lab, 115SUB.maucabal.lab].	

Schritt 4: Suchen Sie in der Zertifikatliste nach dem Eintrag mit dem Typ **CSR Only**, und wählen Sie ihn aus, wie im Bild dargestellt.

Certificate List							
💽 Generalis Self-s	iper 🐴 speer centure ce	sticate chain	il, cere	rate CSR 🔋 Doumland CSR			
Status 16 records for	und						
Certificate List	(1 - 50 of 56)						Rows per Pape 50 *
Find Certificate List	where Certificate • beg	ins with . +		Find Clear	Filter 💠 🚥		
Certificate *	Common Name	Type	Key Type	Distribution	based by	Expiration	Description
av012	auticz, admin	Self-	RSA	115PU8.maucabal.lab	AUTH2_admin	01/27/2038	Self-signed certificate generated by system
CallHanager	115PUB-ms.maucabel.lab	CSR. Only	RSA	Multi-server(SAN)	-	-	
canvarager	TIMOR PROCEEDING	signed	K54	111000 macration ab	115PUB.maucabal.lab	05/30/2023	Self-signed certificate penerated by system
Califianaper- ECDSA	115PUB-EC.maucabal.lab	Self- signed	ec.	115PU8.maucabal.lab	115PUB- EC.maucabal.lab	63/04/2023	Self-signed certificate generated by system
Califfanaper-brust	113908-8C-mascabal.lab	Self- signed	ec.	115P08.maucabal.lab	115P08- EC.mascabal.lab	03/04/2023	Trust Certificate

Schritt 5: Wählen Sie im Popup-Fenster die Option **CSR herunterladen**, und speichern Sie die Datei auf Ihrem Computer.

CSR Details for 115PUB-ms.maucabal.lab, CallManager				
X Delete 🗿 Download CSR				
_ Status				
(i) Status: Ready				
Certificate Settings-				
File Name	CallManager.csr			
Certificate Purpose	CallManager			
Certificate Type	certs			
Certificate Group	product-cm			
Description(friendly name)				
Certificate File Data PKCS10 Request: [Version: 0 Subject: CN=115PUB-ms.maucabal.lab, OU=cisco, O=cisco, L=cisco, ST=cisco, C=MIX SubjectPKInfo: RSA (1.2.840.113549.1.1.1) Key value: 3082010a0282010100c18a6119e66450eef211e6ac9a2349f3466616bd77017095303de7d cabc144fd5f1538efe514fd8207d3ddea43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34 f902277c2ee55d7e5a4d680f8e96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2 9fbd3d5aae5f4f02237ecabca74cf6e2d9b463805eae9ea17b98f83e6232ccc0a7dcd33c76b 79d661582952880d98b3290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c 9be410e8d3b4e1f18a89bcd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b3339a962164 Sa9467d4963f226b6ab0567b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c 6b25a37e84cd0203010001 Attributes: [Requested Extensions [
Delete Download CS	58			

Schritt 6: Navigieren Sie in Ihrem Browser zu dieser URL, und geben Sie die Administratoranmeldeinformationen für den Domänencontroller ein: https://

Schritt 7. Navigieren Sie zu **Request a certificate > advanced certificate request** (Zertifikat anfordern > Erweiterte Zertifikatanforderung), wie im Bild dargestellt.



Schritt 8: Öffnen Sie die CSR-Datei, und kopieren Sie den gesamten Inhalt:



Schritt 9. Fügen Sie den CSR in das **Base-64-kodierte Zertifikatsanforderungsfeld** ein. Wählen Sie unter **Zertifikatvorlage** die richtige Vorlage aus, und wählen Sie **Senden** aus, wie im Bild dargestellt.

Microsoft Active	Directory Certificate Services - Collab CA	Home
Submit a Cert	ificate Request or Renewal Request	
To submit a sa an external so	ved request to the CA, paste a base-64-encode urce (such as a Web server) in the Saved Requ	d CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by est box.
Saved Request		
Base-64-encoded certificate request (CMC or PNCS #10 or PNCS #17)	IThky213/Tp0tBorgHvysBH6gHT_DMeg * B070Bhet19674K20ga4T50ah803bor7u92y89d Qrunnadge0 Jubgs Spatter Jubgs Spatter 4 b	
Certificate Temp	late:	
	CalManager CUCM v	
Additional Attribu	utes:	
Allribules		
	Submt >	

Schritt 10. Wählen Sie **Base 64-codiert** und **Download certificate chain**, die generierte Datei kann jetzt in den CUCM hochgeladen werden.



Überprüfung

Das Prüfverfahren ist Teil des Konfigurationsprozesses.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.