CUCM用のWindows CA証明書テンプレートの作 成

内容

 はじめに

 前提条件

 要件

 使用するコンボーネント

 背景説明

 設定

 Callmanager/Tomcat/TVSテンプレート

 IPsecテンプレート

 CAPFテンプレート

 正明書署名要求の生成

 確認

 トラブルシュート

はじめに

このドキュメントでは、Windows Serverベースの証明機関(CA)で証明書テンプレートを作成する 手順を説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CUCM バージョン 11.5(1)
- ・ Windows Serverの管理に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM バージョン 11.5(1)
- ・ CAサービスがインストールされたMicrosoft Windows Server 2012 R2。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

これらの証明書テンプレートは、すべてのタイプのCisco Unified Communications Manager(CUCM)証明書のX.509拡張要件に準拠しています。

外部CAによって署名できる証明書には、次の5種類があります。

証明書	利用	影響を受けるサービス
CallManager	セキュアなデバイス登録で提示さ れ、証明書信頼リスト(CTL)/内部信 頼リスト(ITL)ファイルに署名でき ます。このファイルは、セキュア なセッション開始プロトコル (SIP)トランクなど、他のサーバと のセキュアなインタラクションに 使用されます。	 Cisco Call Manager Cisco CTI Manager Cisco TFTP
Tomcat	Secure Hypertext Transfer Protocol(HTTPS)の相互対話に対し て提示されます。	·Cisco Tomcat ・シングルサインオン(SSO) ・エクステンションモビリティ ·Corporate Directory
IPSec	バックアップファイルの生成、お よびIP Security(IPsec)とMedia Gateway Control Protocol(MGCP)またはH323ゲート ウェイとのインタラクションに使 用されます。	・Cisco DRFプライマリ ·Cisco DRF Local
CAPF	電話機のローカルで有効な証明書 (LSC)を生成するために使用されま す。	•Cisco Certificate Authority Proxy Function
TVS	電話機が不明な証明書を認証でき ない場合に、Trust Verification Service(TVS)への接続を作成する ために使用されます。	·Cisco Trust Verification Service

◆ 注:14以降のバージョンではTomcat証明書が代わりに使用されるため、ipsec証明書はCisco DRFプライマリおよびCisco DRFローカルとは関連していません。この変更を12.5以前のバ ージョンに追加する予定はありません。

これらの証明書にはそれぞれX.509拡張要件があり、これを設定する必要があります。これを設 定しないと、前述のサービスのいずれかで誤動作が発生する可能性があります。

証明書	X.509キーの使用法	X.509拡張キーの使用
CallManager	·デジタル署名 (Digital Signature) ・主要な暗号化 ・データの暗号化	・Webサーバ認証 ・Webクライアント認証
Tomcat	·デジタル署名 (Digital Signature) ・主要な暗号化 ・データの暗号化	・Webサーバ認証 ・Webクライアント認証
IPSec	·デジタル署名 (Digital Signature) ・主要な暗号化 ・データの暗号化	・Webサーバ認証 ・Webクライアント認証 ・IPsecエンドシステム
CAPF	·デジタル署名 (Digital Signature) ·証明書署名 ・主要な暗号化	・Webサーバ認証 ・Webクライアント認証
TVS	·デジタル署名 (Digital Signature) ・主要な暗号化 ・データの暗号化	・Webサーバ認証 ・Webクライアント認証

詳細については、『<u>Security Guide for Cisco Unified Communications Manager</u>』を参照してくだ さい。

設定

ステップ1:図に示すように、Windows ServerでServer Manager > Tools > Certification Authorityの順に移動します。

<u>6</u>		Server Manager		
⊕⊛- Server Ma	nager • Dashboard	٠@) 🗖 🛶 🧧	al ten tely
	WELCOME TO SERVER MANAGER	figure this local server dd roles and features dd other servers to manage heate a server group connect this server to doud service to t Managrability Dents Services Performance	A AD IS A AD IS Manaprability Events Services Performance	Active Directory Relationstrative Center Active Directory Domains and Pounts Active Directory United and Pounts Active Directory United and Pount Services Active Directory United and Services Active Directory United and Computers Active Directory Computers Active Directory United Active Directory Active Directory United Active Directory Active Directory United Active Native Research Information Ward Computer Services Active Directory United Active Native Computer Ward Services Active Directory United Active System Computers System Computers System Computers
	# AD 105 1	DA multi	BPA results	Tant Scheduler Windows Remort Weinhoused Security Windows Remort (Pagnostic Windows RemortStall Windows RemortStall (201) Windows RemortStall (201) Windows RemortStall (2010)
	Manageability	Manageability	🕐 Manageobility	Window Serve Ballup

ステップ2:次の図に示すように、CAを選択し、Certificate Templatesに移動して、リストを右 クリックし、Manageを選択します。



Callmanager/Tomcat/TVSテンプレート

次の図は、CallManagerテンプレートの作成のみを示しています。同じ手順で、Tomcatおよび TVSサービスの証明書テンプレートを作成できます。唯一の違いは、手順2で新しいテンプレート ごとに各サービス名が使用されるようにすることです。

ステップ 1: Web Serverテンプレートを見つけ、右クリックして、図に示すようにDuplicate Templateを選択します。

3		c	Certificate 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	thentication	
	3 Web Server	1	4.1	-	_	_
	User Signature Only	1	4,1		Duplicate Template	
	🗟 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	thentication, Server Authen	dication.

ステップ2: Generalの下で、証明書テンプレートの名前、表示名、有効性、およびその他の変数 を変更できます。

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

ステップ 3:図に示すように、Extensions > Key Usage > Editの順に移動します。

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			

ステップ4:次の図に示すように、これらのオプションを選択してOKを選択します。

- デジタル署名(Digital Signature)
- キーの暗号化(キーの暗号化)でのみキー交換を許可する
- ユーザーデータの暗号化を許可する

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

ステップ 5:図に示すように、Extensions > Application Policies > Edit > Addの順に移動します。

Compatibility	General	Request	Handling	Cryptography	Key Attestation	
Subject N	Subject Name 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	

手順 6 : Client Authenticationを検索して選択し、次の図に示すように、このウィンドウと前のウィンドウの両方でOKを選択します。

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

手順 7:テンプレートに戻り、Applyを選択してからOKを選択します。

X

ステップ 8 : Certificate Template Consoleウィンドウを閉じ、最初のウィンドウに戻り、図に示 すようにNew > Certificate Template to Issueの順に移動します。



ステップ 9 : 図に示すように、新しいCallManager CUCMテンプレートを選択し、OKを選択します。

	sated does not appear on this list, you may need to wait u	rti
ormation about this template has been replicate of the certificate templates in the organization r	d to all domain controllers. nay not be available to your CA.	
r more information, see <u>Certificate Templ</u>	ate Concepts.	
Vame	Intended Purpose	/
Authenticated Session	Client Authentication	
CA Exchange	Private Key Archival	
Cal Manager CUCM	Server Authentication, Client Authentication	
CEP Encryption	Certificate Request Agent	
Code Signing	Code Signing	
Cross Certification Authority	< Al>	
Enrolment Agent	Certificate Request Agent	
Enrollment Agent (Computer)	Certificate Request Agent	
Exchange Enrolment Agent (Offline request)	Certificate Request Agent	
Exchange Signature Only	Secure Email	

ステップ 10:必要に応じて、前述のすべての手順を繰り返して、TomcatおよびTVSサービスの 証明書テンプレートを作成します。

IPsecテンプレート

ステップ1:Web Serverテンプレートを見つけ、右クリックして、図に示すようにDuplicate Templateを選択します。

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	
	Jiel 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	1 repenses	20
	Subordinate Certification Authority	1	5.1		Help	
	Smartcard User	1	11.1			
	Smattcard 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

ステップ2:Generalの下で、証明書テンプレートの名前、表示名、有効性、およびその他の変数 を変更できます。

Subject Name	Sen	Server Issuance		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

ステップ 3:図に示すように、Extensions > Key Usage > Editの順に移動します。

Pro	perties of N	lew Tem	plate		x
Compatibility General	Request Hand	sling Cryp	tography	Key Attestat	tion
Superseded Templa	tes	Edension	5	Security	-
Superseded Templates Extensions Security To modify an extension, select it, and then click Edit. Extensions included in this template: Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Superseded Template Information Issuance Policies Key Usage 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	

ステップ4:次の図に示すように、これらのオプションを選択してOKを選択します。

- デジタル署名(Digital Signature)
- キーの暗号化(キーの暗号化)でのみキー交換を許可する
- ユーザーデータの暗号化を許可する

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

ステップ 5:図に示すように、Extensions > Application Policies > Edit > Addの順に移動します。

Compatibility	General	Request	Handling	Cryptography	y Key Attestation	
Subject N	Subject Name 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	click Edit.		
Description of Server Auth	of Application	on Policie:	3.		Edt	
					~	
	OK		Cancel	Apply	Help	

x

手順 6 : Client Authenticationを検索して選択し、図に示すようにOKをクリックします。

Properties of New Template	X
Compatibility General Request Handling Cryptography Key Attest Subject Name Server Issuance Requirement C Fulls A subject To the state of the server X Add Application Policy X	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
Application policies:	
Attestation Identity Key Certificate	Ê
Certificate Request Agent	=
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	þ

手順 7:再度Addを選択し、IP security end systemを検索して選択し、これと前のウィンドウの 両方でOKを選択します。

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

ステップ8: テンプレートに戻り、図に示すように、Applyを選択してからOKを選択します。

	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

ステップ 9: Certificate Templates Consoleウィンドウを閉じ、最初のウィンドウに戻り、図に示 すようにNew > Certificate Template to Issueの順に移動します。



ステップ10:図に示すように、新しいIPSEC CUCMテンプレートを選択し、OKを選択します。

8	Enable Certificate Templates						
Select Note: Inform All of t For m	t one Certificate Template to If a certificate template that ation about this template has the certificate templates in the nore 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 is been replicated to all domain controllers. he organization may not be available to your CA. rtificate Template Concepts.					
Nam	ne .	Intended Purpose	~				
. R 🖸 🖸	Exchange Signature Only	Secure Email					
🛛 🗷 ह	Exchange User	Secure Email					
. <u>R</u> 1	PSec	IP security IKE intermediate					
	PSEC CUCM	Server Authentication, IP security end system, Client Authentication					
- R -	Key Recovery Agent	Key Recovery Agent					
- 🗷 🔾	CSP Response Signing	OCSP Signing					
. 🗵 F	RAS and IAS Server	Client Authentication, Server Authentication					
2 F	Router (Offline request)	Client Authentication					
- B 9	Smartcard Logon	Client Authentication, Smart Card Logon					
- E S	Smartcard User	Secure Email, Client Authentication, Smart Card Logon					
ि 🗐 १	Trust List Signing	Mcmsoft Trust List Signing	\sim				
		OK Cano	d				

CAPFテンプレート

ステップ1:ルートCAテンプレートを見つけて右クリックします。次に、図に示すように、 Duplicate Templateを選択します。

8		Cert	ificate Templat	tes Console	
File Action View Help					
💠 🕈 🐷 🖾 🐷 🖾					
Certificate Templates (win12.col)	Template Display Nanile	Schema Version	Versi., Inter	nded Purposes	A
	Router (Offline request)	1	4.3		
	Rent Certification Authority		5.1	Residents Result in	
	RMS and IAS Server	1	101.0 Ch	Dignoste tempote	elien.
	CCIP Response Signing	3	101.0 00	All Tasks +	
	E LOAPS	2	100.6 KD	Properties	Server Authentication, Client A
	Key Recovery Agent	2	105.0 Key		
	Enteros Authentication	2	110.0 CH	Help	Hion, Smart Card Logon, KDC A
	PRECOUCH	2	100.4 Serve	er Authentication, IP security and s	ystem, Client Authentication
	IPSec (Office request)	1	2.1		
	I Plet	1	8.1		

ステップ2:Generalの下で、証明書テンプレートの名前、表示名、有効性、およびその他の変数 を変更できます。

Superseded Templa	tes	Extensions	Security
Compatibility	General	Issuanc	e Requirements
Template display name:			
CAPF CUCM			
Template name:			
CAPF CUCM			
Valida, parted	Dec	- heired	
S S		e lucelo	
J years V		o weeks	*
Publish certificate in	Active Directory	1	
Do not automatic	ally reenroll if a	duplicate certifica	te exists in Active
Directory			
OK	Cance	Apply	Help

ステップ3:図に示すように、Extensions > Key Usage > Editの順に移動します。

Compatibility	General	Issuance	Requirements
Superseded Temp	lates	Extensions	Security
To modify an extension	n, select it, and	then click Edit.	
Extensions included in Application Policie	this template:		
Basic Constraints	to beformation		
Centricate Templa	se information		
Key Usage			
			Edit
Department of Key Use			
Circuit up up immediate	age:		
Digital signature	15.		^
Certificate signing			
Critical extension.			
			~

ステップ4:次の図に示すように、これらのオプションを選択してOKを選択します。

- ・ デジタル署名(Digital Signature)
- ・ 証明書の署名
- CRL署名

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

ステップ 5:図に示すように、Extensions > Application Policies > Edit > Addの順に移動します。

Compatibility	General	Request	Handling	Cryptography	Key Attestation
Subject N	Vame	Ser	ver	Issuance	Requirements
Superseded Templates		Ed	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 Application	on Policies	B;		Edt
Server Auth	entication				
[ОК		Cancel	Apply	Help

手順 6:Client Authenticationを検索して選択し、図に示すようにOKを選択します。

Properties of New Template	X
Compatibility General Request Handling Cryptography Key Attest Subject Name Server Issuance Requirement C Fulls A subject To the Duli size Future To the subject To the	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.	ured
Application policies:	_
Any Purpose Attestation Identity Key Catilicate	<u>^</u>
Certificate Request Agent	=
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	þ

手順 7:再度Addを選択し、IP security end systemを検索して選択し、次に図に示すようにこの ウィンドウと前のウィンドウでOKを選択します。

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

ステップ8: テンプレートに戻り、図に示すように、Applyを選択してからOKを選択します。

	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

ステップ 9: Certificate Templates Consoleウィンドウを閉じ、最初のウィンドウに戻り、図に示 すようにNew > Certificate Template to Issueの順に移動します。



ステップ 10:図に示すように、新しいCAPF CUCMテンプレートを選択し、OKを選択します。

	Enable Certificate Templates	x
Select one Certificate Template to Note: If a certificate template that information about this template has All of the certificate templates in th For 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. ifficate Template Concepts.	
Name	Intended Purpose	~
Authenticated Session CA Exchange	Client Authentication Private Key Archival	_
Code Signing Cross Certification Authority	Code Signing	
Enrolment Agent	Certificate Request Agent Certificate Request Agent	
Exchange Signature Only Exchange User	Secure Email Secure Email	
IPSec IPSEC CLICM	IP security IKE intermediate Server Authentication IP security end system. Client Authentication	~
	OK Cano	ł

証明書署名要求の生成

新しく作成したテンプレートを使用してCallManager証明書を生成するには、次の例を使用しま す。同じ手順を任意の証明書タイプに使用できます。証明書とテンプレートのタイプを選択する だけです。

ステップ1: CUCMで、OS Administration > Security > Certificate Management > Generate CSRの順に移動します。

ステップ2:次の図に示すように、これらのオプションを選択し、Generateを選択します。

- ・ 証明書の目的: CallManager
- ・ディストリビューション:<1台のサーバまたはマルチSAN用のいずれか>

enerate Certificate Sig	ning Request		
Generate 📑 Close			
Status-			
Warning: Generating	a new CSR for a specific certificate type	will overwrite the exi	sting CSR for that type
Generate Certificate Sig	ning Request		
Certificate Purpose**	CallManaper		
Distribution*	Multi-server(SAN)		
Common Name*	115PUB-ms.maucabal.lab		1
Subject Alternate Name	s (SANs)		
Auto-populated Domains	1159U8.maucabal.lab 1155U8.maucabal.lab		
Parent Domain	maucabal.lab		
Other 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.		
	(and a		
Key Length*	2048		

Generate Close

ステップ3:次の図に示すように、確認メッセージが生成されます。

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

ステップ4:証明書リストで、CSR Onlyタイプのエントリを探し、図に示すように選択します。

Certificate List							
Constant Self-s	igned 🐴 Uplant CertificatorCert	num man (i, cere	rate CSR 🔋 Counteed CSR			
Status -							
(1) 16 records for	und						
Certificate List	(1 · 50 of 56)						Rows per Page 10
Find Certificate Us	t where Certificate • begi	na with 💌		Find Over	ritter 💠 🚥		
Cartificate*	Common Name	1.0e	Key Teps	Datribution	baued fly	Depiration	Description
autho	AUTH2_admin	Self-	RSA	115PU8.maucabal.lab	AUTH2_admin	01/27/2038	Self-signed certificate penerated by system
Califfonaper	115PUB-ma.maucabal.lab	CSR Only	854	Hulti-server(SAN)	-		
causarapp.	TURNER STORE AND	signed	No.4	111PORTACIONAL 40	115PUB.maucabal.lab	05/30/2023	Self-signed certificate penerated by system
Califfunaper- ECDSA	115RUB-EC.mascabal.lab	Self- signed	00	115PUB.maucabal.lab	115PUB- EC.maycabal.lab	63/94/2023	Self-signed certificate penerated by system
CallManager-trust	1139x8.8Cmassabal.lab	Self- signed	60	115PG8.maucabal.lab	115PVB- EC:maucabal.lab	03/94/2023	Trust Certificate

ステップ 5 : ポップアップウィンドウでDownload CSRを選択し、コンピュータにファイルを保存します。

CSR Details for 115PUB-ms.maucabal.lab, CallManager				
Celete 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. SubjectPKInfo: RSA (1.2.3 Key value: 3082010a0282010100c18 cabc144fd5f1538efe514fd f902277c2ee55d7e5a4d64 9fbd3d5aae5f4f02237ecal 79d661582952880d98b33 9be410e8d3b4e1f18a89b Sa9467d4963f226b6ab05 6b2Sa37e84cd020301000 Attributes: [Requested Extensions [maucabal.lab, OU=cisco, O=cisco, L=cisco, ST=cisco, C=MX 840.113549.1.1.1) 8a6119e66450eef211e6ac9a2349f34666616bd77017095303de7d 88207d3ddea43b35ce4f0512cf748a2032bfd72fd7431b41a7cc34 80f8c96b6f46ed533b21c6146619f775b65da8b7a5a2de7dd8dd2 bca74cf6e2d9b463805eae9ee17b98f83e6232ccc0a7dcd33c76b 290d44117a2d8cbfac2b164ace9a23611fa8683ba82d9a3d30a0c cd3858463ae5e039fd2fd31a8fdd6e45cf48734f97b339a962164 67b7f92735368edee64713f627d76b0c0e1e1b45b23698f15b8c			
Delete Download CSR				

手順 6 : ブラウザでURLに移動し、ドメインコントローラ管理者のクレデンシャル (https://<yourWindowsServerIP>/certsrv/)を入力します。

手順7:図に示すように、Request a certificate > advanced certificate requestの順に移動します。

Microsoft Active Detectory 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.



ステップ8: CSRファイルを開き、すべての内容をコピーします。

3	CallManager - Notepad		X
File Edit Format View Help			
BEGIN CERTIFICATE REQ aXNjb:2EOMAwGA1UEChWFY21:Y2E G9w08AQEFAADCAQ8AMIIBCgKCAQ 10MbQafMNPkCJ3wu5V1+Wk1oD4y 2t51mFYKVKID2i:KQ1EEXotjL+s 8ia2qa/Nrt/knNTa0Ju2HE/Yn12s HAwEGCCsGAQUFBuMCMAsGA1Ud0 xtYXVjYNJhbC5sYNIw0QYJKo2IN 4P9JuckGcS+ivInw8T69h08Yx81 1Yhky213/Zp0t9oVg6vynR96opN Ds8gs9gxNXXcf8DcdWu+eG8qWR9	IESTHIIDNDCCAhuCAQAubjELMAkGALUEBHMCTVgxDjAMBgMVBAgTBMNpc2HvMQ4uDA kxDjAMBgMVBAsTBMNpc2NvMR8uHQYDVQQDExYxMTVQVUItbXMubWF1Y2FiYWuubGFIHIIBI XEAuYphGe2kU07yEeasmiN2802mFr13AXCVMD3n3Kv8RP1fFTjv5RT9ggfT3epDs1zk8FEs AktvRu1T0yHGFGY293W2Xai3paLefdjdKfvT1ar19PAiN+yrynTPbi2bRjgF6unuF7mPg+Y IKxZKzpojYR+oaDuoL2oSMKD3vkE0jTtOHxiom804WEY65eA5/5/TGo/dbkXP5HNP17H5qu HDh4bRb12mPFbjGs1o36EzQIDAQABoIGAMH4GCSqGS1b3DQE30jFxMG8uHQYDVR81887wF AQEAuIEs0888gNVHREE0jA4ghMxHTVQVUIubWF1Y2FiYMuubGFighMxHTVTVUIubWF1Y2Fi tvcNAQELBQADggE8AIgutjgKH/LLvLogS1/tba62o/ViXcI2QmuH+SIywiiUH1b55fRuyu 18hDc5LhdkTfmEd7XHAMEEhZ45cuFbaYnugMAMYQ8c1p5UMhck3yzQQbL5pjcv3LCPiqbz AL2H+gGb70hImtIjGe74X2Qqu4YT50uHH03EcH7v92yBPdKQa1fP+oAGMx1nocta2NojmRQ ins2hMUMJNb1o7a1Qbyxdf7r7dbSqW8Gyo8qkM=END_CERTIFICATE_REQUEST	YDVQQHEwYj JANBgkqhki 9011Ayv9cv JLMwKfc0zx TWRa1GFU1j AYIKwY8BQU YMwubGFigg ApijQXsk2d jn6pOUJf2o UuxuwAgqUy	4
< #			э.

ステップ 9: Base-64-encoded certificate requestフィールドにCSRを貼り付けます。図に示すよ うに、Certificate Templateで正しいテンプレートを選択し、Submitを選択します。

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.

Laved Request:					
Base-64-encoded certificate request (CMC or PNCS #10 or PNCS #7);	SthAy213/2gotBorg4+ya856gpt120+g Gb70hlat196474822ggsKT50uh803bof7u92g8 STannakgfSy JubgeSgatOkofBoodMu+e00gMRanalbot505blo BgMS9geSgat EDO CENTIFICATE REQUEST				
	4				
Certificate Temp	lation:				
	CalManager CUCH	w.			

Additional Attributes:

Allebules

					100
	節	100	1	2	100

ステップ 10:最後に、Base 64 encodedとDownload certificate chainを選択します。 これで、生成されたファイルをCUCMにアップロードできます。

Home

Microsoft Active Directory Certificate Services - Colab CA

Certificate Issued

The certificate you requested was issued to you.



確認

検証手順は、実際には設定プロセスの一部です。

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。