CUCM サードパーティ CA 署名済み LSC の作成 およびインポートの設定例

内容

概要 前提条件 要件 使用するコンポーネント 設定 CA ルート証明書のアップロード エンドポイントに対する証明書発行者としてのオフライン CA の設定 電話機の証明書署名要求(CSR)の生成 FTP(または TFTP)サーバを介した CUCM からの生成済み CSR の取得 電話機の証明書の取得 .cer から .der 形式への変換 .tgz 形式への証明書(.der)の圧縮 <u>SFTP サーバへの .tgz ファイルの転送</u> CUCM サーバへの .tgz ファイルのインポート Microsoft Windows 2003 認証局による CSR の署名 CA からのルート証明書の取得 確認 トラブルシュート

概要

認証局プロキシ機能(CAPF)のローカルで有効な証明書(LSC)は、ローカルで署名が付けら れます。ただし、電話機でサードパーティ認証局(CA)の署名付き LSC を使用しなければなら ない場合もあります。このドキュメントでは、その場合の手順について説明します。

前提条件

要件

このドキュメントの読者は Cisco Unified Communications Manager(CUCM)に関する知識を持っていることを推奨します。

使用するコンポーネント

このドキュメントの情報は、CUCM バージョン 10.5(2) に基づいています。ただし、ここで説明 する機能はバージョン 10.0 以降で有効です。

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、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

設定

この手順を構成するステップは次のとおりです。それぞれのステップについて、個別のセクショ ンで詳しく説明します。

- 1. <u>CA ルート証明書のアップロード</u>
- 2. エンドポイントに対する証明書発行者としてのオフライン CA の設定
- 3. <u>電話機の証明書署名要求(CSR)の生成</u>
- 4. <u>FTP(または TFTP)サーバを介した Cisco Unified Communications Manager(CUCM)か</u> <u>らの生成済み CSR の取得</u>
- 5. CA からの電話機の証明書の取得
- 6. <u>.cer から .der 形式への変換</u>
- 7. <u>.tgz 形式への証明書(.der)の圧縮</u>
- 8. <u>セキュア シェル FTP(SFTP)サーバへの .tgz ファイルの転送</u>
- 9. <u>CUCM サーバへの .tgz ファイルのインポート</u>
- 10. Microsoft Windows 2003 認証局による CSR の署名
- 11. <u>CA からのルート証明書の取得</u>

CA ルート証明書のアップロード

- 1. Cisco Unified Operating System (OS) 管理 Web GUI にログインします。
- 2. [Security Certificate Management] に移動します。
- 3. [Upload Certificate/Certificate chain] をクリックします。
- 4. [Certificate Purpose] で [CallManager-trust] を選択します。
- 5. CA のルート証明書を参照し、[Upload] をクリックします。

Cisco Uni For Cisco Uni	fied Operating System Administration
Show - Settings - Security	y ▾ Software Upgrades ▾ Services ▾ Help ▾
Upload Certificate/Certific	te chain - Mozilla Firefox
https://10.106.122.173/cm	platform/certificateUpload.do
Upload Certificate/Certi	ficate chain
Dipload 🖳 Close	
Status Warning: Uploading a	a cluster-wide certificate will distribute it to all servers in this cluster
Certificate Purpose*	CallManager-trust
Description(friendly name)
Upload File	Browse AMEER-CA.cer
Upload Close	

エンドポイントに対する証明書発行者としてのオフライン CA の設定

- 1. CUCM 管理 Web GUI にログインします。
- 2. [System] > [Service Parameters] に移動します。
- 3. CUCM サーバを選択し、[Service] として [Cisco Certificate Authority Proxy Function] を選択 します。
- 4. [Certificate Issuer to Endpoint] で [Offline CA] を選択します。

Internation Cisco Unified CM Administration	
For Cisco Unified Communications Solutions	
System 🗸 Call Routing 👻 Media Resources 👻 Advanced Features 👻 D	Device 👻 Application 👻 User Mana <u>c</u>
Service Parameter Configuration	
Save Set to Default	
⊂ Status	
i Status: Ready	
Select Server and Service	
Server* 10.106.122.173CUCM Voice/Video (Active)	-
Service* Cisco Certificate Authority Proxy Function (Active)	-
All parameters apply only to the current server except parameters the	hat are in the cluster-wide group(s
Cisco Certificate Authority Proxy Function (Active) Paramete	ers on server 10.106.122.173
Parameter Name	Parameter Value
Certificate Issuer to Endpoint *	Offline CA
Duration Of Certificate Validity	5
Key Size *	1024
Maximum Allowable Time For Key Generation	30
Maximum Allowable Attempts for Key Generation *	3

電話機の証明書署名要求(CSR)の生成

- 1. CUCM 管理 Web GUI にログインします。
- 2. [Device Phones] に移動します。
- 3. LSC に外部 CA による署名が必要な電話機を選択します。
- 4. [Device security profile] で、デバイス セキュリティ プロファイルを保護されたものに変更し ます(保護されたデバイス セキュリティ プロファイルがない場合は、[Phone Security Profile Configuration] で新規に追加してください)。
- 5. 電話機の設定ページにある [CAPF] セクションで、[Certification Operation] として [Install/Upgrade] を選択します。このステップを、LSC に外部 CA による署名が必要な電話 機のすべてに対して行います。[Certificate Operation Status] には [Operation Pending] と表 示されているはずです。

Protocol Specific Inform	nation			
Packet Capture Mode*	None			
Packet Capture Duration	0			
BLF Presence Group*	Standard Presence group			
Device Security Profile*	Cisco 7962 - Standard SCCP - Secure Profile			
SUBSCRIBE Calling Search	Space < None >			
Unattended Port				
Require DTMF Reception	1			
RFC2833 Disabled				
Certification Authority P	Proxy Function (CAPF) Information			
Certification Authority P Certificate Operation*	Proxy Function (CAPF) Information			
RFC2833 Disabled Certification Authority P Certificate Operation* Authentication Mode*	Proxy Function (CAPF) Information Install/Upgrade			
RFC2833 Disabled Certification Authority P Certificate Operation* Authentication Mode* Authentication String	Proxy Function (CAPF) Information Install/Upgrade			
RFC2833 Disabled Certification Authority P Certificate Operation* Authentication Mode* Authentication String Generate String	Proxy Function (CAPF) Information Install/Upgrade			
RFC2833 Disabled Certification Authority P Certificate Operation* Authentication Mode* Authentication String Generate String Key Size (Bits)*	Proxy Function (CAPF) Information Install/Upgrade			

Note: Security Profile Contains Addition CAPF Settings.

以下に、電話機のセキュリティ プロファイル(7962 モデル)を示します。

	Phone Security Profi	le Configuration			
	Save 🗶 Delete	Copy 🎦 Reset 🧷 Apply Config 🕂 Add New			
	Status				
	i Status: Ready				
	-Phone Security Prof	ile Information			
	Product Type: Device Protocol:	Cisco 7962 SCCP			
	Name*	Cisco 7962 - Standard SCCP - Secure Profile			
	Description	Cisco 7962 - Standard SCCP - Secure Profile			
	Device Security Mode	Authenticated 🗸			
1	TFTP Encrypted Co	nfig			
	Phone Security Prof	ile CAPF Information			
	Authentication Mode*	By Existing Certificate (precedence to LSC)			
	Key Size (Bits)*	1024 🗸			
	Note: These fields are	related to the CAPF Information settings on the Phone Configuration			

CSR が生成されるかどうかを確認するために、セキュア シェル(SSH)セッションで utils capf csr count コマンドを入力します。(次のスクリーン ショットには、3 台の電話機に対して CSR が生成されたことが示されています)。

admin:					
admin utils	Ci	apf	csr	count	
Count CSR/Ce	r	tif	icate	e file	s.
Valid CSR	:	3			
Invalid CSR	:	0			
Certificates	3:	0			

注:電話機の [CAPF] セクションにある [Certificate Operation Status] は、[Operation Pending] 状態のままになります。

FTP(または TFTP)サーバを介した CUCM からの生成済み CSR の取得

- 1. CUCM サーバに SSH でログインします。
- 2. utils capf csr dump コマンドを実行します。このスクリーン ショットには、FTP に転送中の ダンプが示されています。



3. ダンプ ファイルを開き、WinRAR を使用して CSR をローカル マシンに抽出します。



電話機の証明書の取得

1. 電話機の CSR を CA に送信します。

2. CA によって署名付き証明書が提供されます。

注:CA. として Microsoft Windows 2003 サーバを使用できます。Microsft Windows 2003 CA で CSR に署名を付けるための手順は、このドキュメントの後半で説明します。

.cer から .der 形式への変換

受信した証明書が.cer 形式になっている場合は、ファイル名を.der に変更します。

🔄 SEPD0574CF6BD0F.cer	1/22/2015 3:03 AM	Security Certificate	2 KB
🔄 SEPB83861583BB9.cer	1/22/2015 3:03 AM	Security Certificate	2 KB
SEP1C17D341FD21.cer	1/22/2015 3:00 AM	Security Certificate	2 KB

SEPD0574CF6BD0F.der	1/22/2015 3:03 AM	Security Certificate	2 KB
🔄 SEPB83861583BB9.der	1/22/2015 3:03 AM	Security Certificate	2 KB
🔄 SEP1C17D341FD21.der	1/22/2015 3:00 AM	Security Certificate	2 KB

.tgz 形式への証明書(.der)の圧縮

証明書を圧縮形式にするには、CUCM サーバのルート(Linux)を使用できます。この手順は、 通常の Linux システムでも実行できます。

1. SFTP サーバを使用して、すべての署名付き証明書を Linux システムに転送します。



2. 次のコマンドを入力して、すべての .der 証明書を .tgz ファイルに圧縮します。

tar -zcvf



SFTP サーバへの.tgz ファイルの転送

次のスクリーン ショットに示すステップを実行して、.tgz ファイルを SFTP サーバに転送します。



CUCM サーバへの .tgz ファイルのインポート

1. CUCM サーバに SSH でログインします。

2. utils capf cert import コマンドを実行します。



証明書が正常にインポートされると、CSR カウントの値がゼロになります。



Microsoft Windows 2003 認証局による CSR の署名

この手順は、Microsoft Windows 2003 を CA として使用する場合に実行します。

1. [Certification Authority] を開きます。

	1	Windows Catalog					
	4	Windows Update					
	i	<u>P</u> rograms	•		Administrative Tools		Certification Authority
lition		Documents	+		*	Ŧ	*
ise Ed	₽	Settings	•				
Interpr	\mathcal{Q}	Search	۲				
003	3	Help and Support					
erver		<u>R</u> un					
lows S	\square	Log Off administrator					
Wind	0	Sh <u>u</u> t Down					
			-40	<u>ата</u>			

2. CA を右クリックし、[All Tasks] > [Submit new request...] に移動します。

Eile Action Yiew Help ← → € Image: Certification Authority (Local) Name Certification Authority (Local) Name Revoked Certificates Revok All Tasks Start Service
 ← →
Certification Authority (Local) Name AMEER-CA Revoked Certificates Revoked All Tasks Start Service
AMEER-CA All Tasks Start Service
Issued Stop Service
Pendin View
Failed Refresh
Export List Back up CA
Restore CA
Properties
Help Rene <u>w</u> CA Certificate

o

3. CSR を選択して [Open] をクリックします。すべての CSR に対して、この操作を行います



開いた CSR がすべて、[Pending Requests] フォルダ内に表示されます。

4. それぞれを右クリックし、[All Tasks] > [Issue] に移動します。保留中のすべてのリクエスト に対して、この操作を行います。

📴 Certification Authority					
<u>File Action View H</u> elp					
← → 🗈 🖬 🔂 🗟 😭 🖬					
Certification Authority (Local)	Request ID	Binary Request	Request Status Code	Request Dispos	sition Messag
AMEER-CA	36 37 38	All Tas <u>k</u> s ► Refresh	View Attributes/Extensions Export Binary Data	Under Si Under Si Under Si	ubmission ubmission ubmission
Pending Requests			Issue Deny		

5. 証明書をダウンロードするために、[Issued Certificate] を選択します。

6. 証明書を右をクリックし、[Open] をクリックします。

📴 Certification Authority				
<u>File Action View H</u> elp				
Certification Authority (Local)	Request ID	Requester Name	Binary Certificate	Serial Numl 🔺
🖻 🕜 AMEER-CA	30	DATA-SRV225\A	BEGIN CERTI	11cd7e36C
Revoked Certificates	31	DATA-SRV225\A	BEGIN CERTI	11cf86c70
Issued Certificates	32	DATA-SRV225\A	BEGIN CERTI	11d088d60
Pending Requests	33	DATA-SRV225\A	BEGIN CERTI	11af75cb0
Failed Requests	🔛 34	DATA-SRV225\A	BEGIN CERTI	11af83490
	35	DATA-SRV225\A	BEGIN CERTI	11af8e450
	🔤 36 👘	Q	BEGIN CERTI	122267260
	🕮 37	Open 4	BEGIN CERTI	122272900
	🔛 38	All Tasks 🔸 A	BEGIN CERTI	12227c920
	•	Refresh		▼ ▶
Open this item		Help		

7. 証明書の詳細が表示されます。証明書をダウンロードするには、[Details] タブを選択し、 [Copy to File...] を選択します。

Certificate ? 🗙
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s): •All application policies
Issued to: SEP1C17D341FD21
Issued by: AMEER-CA
Valid from 1/22/2015 to 1/22/2016
Issuer Statement
ОК

8. [Certificate Export Wizard] で、[DER encoded binary X.509 (.CER)] を選択します。

iow: <ali></ali>	-	
Reld Version Senal number Issuer Valid from Valid to Subject Public key	Value × V3 12 22 67 26 00 00 00 00 00 24 sha1RSA AMEER-CA Thursdey, January 22, 2015 2 Friday, January 22, 2015 2 Friday, January 22, 2016 2:51 SEP1C17D341FD21, ourm, cls RSA (2048 Bks) ×	Select the format you want to use: © DER encoded binary X.509 (.CER): © Bage-64 encoded X.509 (.CER) © Oyptographic Message Syntax Standard - PKCS #7 Certificates (.P78) © Diricude all certificates in the certification path if possible © Dersonal Information Exchange - PKCS #12 (.PFX) © Diricude all certificates in the certification path if possible © Diricude all certificates in the certification path if possible © Diricude all certificates in the certification path if possible © Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above) © Delete the private (sey if the export is successful
		< Back Next > Cance

9. ファイルに適切な名前を付けます。この例では、<MAC>.cer 形式を使用します。

ate Export Wizard	
to Export	
Specify the name of the file you want to export	
File name:	
	- 1
LIAICAIRameshCUCMILABPhoneCSRICERISEPICI/D341ED21.cerL	Browse
	ate Export Wizard to Export Specify the name of the file you want to export File name: T0\C0\PamesbCUCM\L08PhoneCSP\CEP\SEP1C17D341ED21_cer

10. 以上の手順を使用して、[Issued Certificate] セクションに表示されている他の電話機の証明 書を取得します。

CA からのルート証明書の取得

1. [Certification Authority] を開きます。

2. 次のスクリーン ショットに示すステップを実行して、ルート CA をダウンロードします。

Test.pcop Ele Action Authority Test.pcop Ele Action Yest Ele Action Yest AMEER-CA Properties Image: State of the	7 × Auditing Security Addule Extensions Storage	Certificate General Details Certification Show: <	Path
Certificate Information This certificate is intended for the following purpose(s): •Al issuance policies •Al application policies	3 <u>View Certificate</u>	Field Version Signature algorithm Issuer Vaid from Vaid to Subject Public key	Value ▲ V3 12 96 ad 39 4c 29 97 a0 45 c5 shaIRSA AMEER-CA Tuesday, May 07, 2013 8:55: Monday, May 07, 2018 9:02:4 AMEER-CA RSA (2048 Bhs)
Issued to: AMEER-CA Issued by: AMEER-CA	uplographic Provider		
Valid from 5/7/2013 to 5/7/2018	Cancel		5 Edit Properties
Isouer glatement			ок

確認

ここでは、設定が正常に機能しているかどうかを確認します。

- 1. 電話機の設定ページに移動します。
- 2. [CAPF] セクションで、[Certificate Operation Status] に [Upgrade Success] と表示されてい ることを確認します。

Certificate Operation	No Pending Operation	•
uthentication Mode*	By Existing Certificate (precedence to LSC)	्र
uthentication String		
Generate String		
	1024	
ey Size (Bits)*	1024	
Key Size (Bits)* Operation Completes By	2015 1 24 12 (YYYY:MM:DD:HH)	-

注:詳細については、<u>サードパーティ CA 署名付き LSC の生成を参照してください。</u>

トラブルシュート

現在、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。