Automatische Zertifikatregistrierung und verlängerung über CAPF Online CA konfigurieren

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Serverzeit und -datum überprüfen Computername des Aktualisierungsservers Konfigurieren AD-Dienste, Benutzer und Zertifikatvorlage Konfiguration für IIS-Authentifizierung und SSL-Bindung Konfiguration des CUCM Überprüfung Überprüfen von IIS-Zertifikaten CUCM-Konfiguration überprüfen Verwandte Links

Einleitung

Dieses Dokument beschreibt die automatische Zertifikatregistrierung und -verlängerung über die Online-Funktion der Certificate Authority Proxy Function (CAPF) für Cisco Unified Communications Manager (CUCM).

Beitrag von Michael Mendoza, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

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

- Cisco Unified Communications Manager
- X.509-Zertifikate
- Windows-Server
- Windows Active Directory (AD)
- Windows-Internetinformationsdienste (IIS)
- NT (New Technology) LAN Manager (NTLM)-Authentifizierung

Verwendete Komponenten

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

• CUCM-Version 12.5.1.10000-22

- Windows Server 2012 R2
- IP-Telefon CP-8865/Firmware: SIP 12-1-1SR1-4 und 12-5-1SR2.

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 kennen.

Hintergrundinformationen

In diesem Dokument wird die Konfiguration der Funktion und der zugehörigen Ressourcen für weitere Recherchen beschrieben.

Serverzeit und -datum überprüfen

Stellen Sie sicher, dass auf dem Windows-Server das richtige Datum, die richtige Uhrzeit und die richtige Zeitzone konfiguriert sind, da sich dies auf die Gültigkeitsdauer des Zertifikats der Stammzertifizierungsstelle (Certificate Authority) des Servers sowie der von ihm ausgestellten Zertifikate auswirkt.

Computername des Aktualisierungsservers

Standardmäßig hat der Computername des Servers einen zufälligen Namen wie WIN-730K65R6BSK. Bevor Sie die AD-Domänendienste aktivieren, müssen Sie zunächst sicherstellen, dass der Computername des Servers auf den Namen des Servers und den Namen des Herausgebers der Stammzertifizierungsstelle aktualisiert wird. Andernfalls sind nach der Installation der AD-Dienste viele zusätzliche Schritte erforderlich, um diesen Namen zu ändern.

- Navigieren Sie zu Lokaler Server, wählen Sie den Computernamen aus, um die Systemeigenschaften zu öffnen.
- Wählen Sie die Schaltfläche Ändern, und geben Sie den neuen Computernamen ein:



• Starten Sie den Server neu, damit die Änderungen angewendet werden.

Konfigurieren

AD-Dienste, Benutzer und Zertifikatvorlage

Aktivieren und Konfigurieren der Active Directory-Dienste

• Wählen Sie im Server Manager die Option **Rollen und Features hinzufügen aus**, wählen Sie die **rollenbasierte oder die funktionsbasierte Installation aus**, und wählen Sie den Server aus dem Pool (es darf nur einen Server im Pool geben) und dann die Active Directory-Domänendienste aus:



- Fahren Sie mit der Auswahl der Schaltfläche "Weiter" fort, und klicken Sie dann auf Installieren.
- Wählen Sie nach Abschluss der Installation die Schaltfläche Schließen aus.
- Unter Server Manager > AD DS wird eine Warnregisterkarte mit dem Titel Configuration required for Active Directory Domain Services; Select more link and then available action to start the setup wizard angezeigt:



 Folgen Sie den Anweisungen im Domänen-Setup-Assistenten, fügen Sie eine neue Gesamtstruktur mit dem gewünschten Stammdomänennamen hinzu (in dieser Übung michamen.com), und deaktivieren Sie das DNS-Feld, sofern verfügbar. Definieren Sie das DSRM-Kennwort (verwenden Sie für diese Übung *C1sc0123!*):



<u>L</u>	Active Directory Domain Services C	Configuration Wizard		- 0 X
Domain Controlle	er Options		LAB-DO	TARGET SERVER
Deployment Configuration	Select functional level of the new forest	and root domain		
Additional Options	Forest functional level:	Windows Server 2012 R2	٠	
Paths	Domain functional level:	Windows Server 2012 R2	•	
Review Options Prerequisites Check Installation Results	Specify domain controller capabilities Domain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Type the Directory Services Restore Mod Password: Confirm password:	e (DSRM) password		

- Es muss ein NetBIOS-Domänenname angegeben (in dieser Übung mit MICHAMEN1 verwendet) werden.
- Folgen Sie dem Assistenten bis zum Abschluss. Der Server wird dann neu gestartet, um die Installation abzuschließen.
- Wenn Sie sich das nächste Mal anmelden, müssen Sie den neuen Domänennamen angeben. Beispiel: MICHAMEN1\Administrator.

€ Server	Manager + AD DS	· © I
Dashboard	All servers 1 total	
🗎 AD DS	Server Name IPv4 Address Manageability	Last Update
File and Storage Services	LA8-DC-RTP 14.48.31.153 Online - Performance counters	not started 2/26/2019 4/20:10 PM

Aktivieren und Konfigurieren der Zertifikatdienste

- Wählen Sie im Server Manager die Option Rollen und Features hinzufügen aus.
- Wählen Sie Active Directory-Zertifikatdienste aus, und befolgen Sie die Anweisungen, um die erforderlichen Funktionen hinzuzufügen (alle verfügbaren Funktionen wurden aus den Rollendiensten ausgewählt, die für diese Übung aktiviert wurden).
- Für Role Services Check Certification Authority Web Enrollment



<u>L</u>	Add Roles and Features Wizard	_ _ X
Select role service Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Web Server Role (IS) Role Services Confirmation Results	Select the role services to install for Web Server (IIS) Role services	DISTINATION SIRVIR (JAI-OC-RTP.michamen.com Description Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to posside an environment for developers to create Web-based applications.
	C III)	
	< Previous Next	> Install Cancel

 Unter Server Manager >AD DS muss eine Warnregisterkarte mit dem Titel Configuration required for Active Directory Certificate Services (Für Active Directory-Zertifikatdienste erforderliche Konfiguration) angezeigt werden. Wählen Sie den Link more (Mehr) und anschließend die verfügbare Aktion aus:

€ • Server M	Aanager + AD CS	;		• @ /_A *****	Tools View Holy	
Cool Server Local Server A Server A Server A Docs A D DS R File and Storage Services	SERVERS Al servers 1 km/d Configuration region Filter Server have 0-6 800 MACC 2010 644511	ed for Active Denotory Catolicate Se P (8) • (8) The Manageneticity 12 Online - References spectras	Last Typine	Windows Actuation	tass • Men. *	ĺ
lo 15		All Servers Task	k Details and No	All Servers Task Deta	in .	
	EVENTS All events (2 total	Fiber Status Task Name Rod deployment	P (8 +	 enage enage enage enage	Action whey Co., Configure A	Kons Kolona Densburg Carti-

- Navigieren Sie im AD-CS-Assistenten nach der Installation durch die folgenden Schritte:
- Wählen Sie die Zertifizierungsstelle und die Web Enrollment-Rollen der Zertifizierungsstelle aus.
- Enterprise CA mit Optionen auswählen:
- Stamm-CA
- Neuen privaten Schlüssel erstellen
- Privaten Schlüssel verwenden SHA1 mit Standardeinstellungen
- Legen Sie einen gemeinsamen Namen für die Zertifizierungsstelle fest (muss mit dem Hostnamen des Servers übereinstimmen):

L	AD CS Configuration	_ 0 X
CA Name	ı	DESTINATION SERVER A8-DC-RTP:michamen.com
Credentials Role Services	Specify the name of the CA	
Setup Type CA Type	Type a common name to identify this certification authority (CA). This n certificates issued by the CA. Distinguished name suffix values are autor be modified.	ame is added to all natically generated but can
Private Key	Common name for this CA:	
CA Name	LA8-DC-RTP	
Validity Period	Distinguished name suffice	
Certificate Database	DC=michamen,DC=com	
Confirmation	Preview of distinguished name:	
	CN=LA8-DC-RTP,DC=michamen,DC=com	
Results		

- Gültigkeit für 5 Jahre (oder mehr, falls gewünscht) festlegen
- Wählen Sie die Schaltfläche Weiter im restlichen Assistenten aus.

Erstellung von Zertifikatvorlagen für Cisco RA

- MMC öffnen. Wählen Sie das Windows Start-Logo aus, und geben Sie mmc unter Ausführen ein.
- Öffnen Sie ein MMC-Fenster, und fügen Sie die folgenden Snap-Ins hinzu (an verschiedenen Stellen der Konfiguration verwendet). Wählen Sie anschließend **OK**:



- Wählen Sie **Datei** > **Speichern** und speichern Sie diese Konsolensitzung auf dem Desktop, um schnell wieder darauf zuzugreifen.
- Wählen Sie in den Snap-Ins Zertifikatvorlagen aus.
- Erstellen oder Klonen einer Vorlage (vorzugsweise der Vorlage "*Root Certification Authority*", falls verfügbar) und Benennen Sie sie CiscoRA



- Ändern Sie die Vorlage. Klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Eigenschaften** aus
- Wählen Sie die Registerkarte **Allgemein**, und legen Sie die Gültigkeitsdauer auf 20 Jahre (oder einen anderen Wert, falls gewünscht) fest. Stellen Sie auf dieser Registerkarte sicher, dass die Werte für "Anzeigename" und "Name" der Vorlage übereinstimmen.

Cis	coRA Propert	ties	? X
Subject Name	lss	uance Require	ments
Superseded Templates	Extensions	Security	Server
General Compatibility Rev	quest Handling C	hyptography	Key Attestation
Template display name:			
CiscoRA			
Template name: CiscoRA Validity period:	Renewal p	eriod: tys V	
Publish cetificate in Acti Do not automatically Directory	ve Directory reenroll if a duplicat	e certificate ex	dets in Active
ОК	Cancel	Apply	Help

• Wählen Sie die Registerkarte **Erweiterungen aus**, markieren Sie **Anwendungsrichtlinien**, und wählen Sie dann **Bearbeiten aus**.



- Entfernen Sie alle Richtlinien, die im angezeigten Fenster angezeigt werden
- Wählen Sie die Registerkarte Subject Name (Betreffname) und anschließend das Optionsfeld Supply in Request (Versorgung anfordern).
- Wählen Sie die Registerkarte **Sicherheit**, und gewähren Sie alle Berechtigungen für alle angezeigten Gruppen/Benutzernamen.

CiscoRA Properties ? X
General Compatibility Request Handling Cryptography Key Attestation Subject Name Issuance Requirements Superseded Templates Extensions Security Server
Group or user names:
Authenticated Users Administrator Common Admins (MICHAMEN1\Domain Admins) Enterprise Admins (MICHAMEN1\Enterprise Admins)
Add Remove Permissions for Authenticated Users Allow Deny
Full Control
Read 🗹 🗌
Write 🗹 🗌
Enrol V
For special permissions or advanced settings, click Advanced
OK Cancel Apply Help

Bereitstellung der Zertifikatvorlage für die Ausgabe

- Wählen Sie in den MMC-Snap-Ins **Zertifizierungsstelle aus**, und erweitern Sie die Ordnerstruktur, um den Ordner **Zertifikatvorlagen** zu suchen.
- Klicken Sie mit der rechten Maustaste in den leeren Bereich im Rahmen, der Name und beabsichtigte Verwendung enthält.
- Neue und auszugebende Zertifikatvorlage auswählen
- Wählen Sie die neu erstellte und bearbeitete Cisco RA-Vorlage aus.



Active Directory CiscoRA-Kontoerstellung

- Navigieren Sie zu MMC-Snap-Ins, und wählen Sie Active Directory-Benutzer und -Computer aus.
- Wählen Sie den Ordner **Benutzer** in der Struktur im linken Bereich aus.
- Klicken Sie mit der rechten Maustaste in das Leerzeichen im Rahmen, das Name, Typ und Beschreibung enthält.
- Neu und Benutzer auswählen
- Erstellen Sie ein CiscoRA-Konto mit Benutzername/Kennwort (für diese Übung wurde *Cisco/Cisco123* verwendet), und aktivieren Sie das Kontrollkästchen **Kennwort läuft nie ab,** wenn angezeigt wird.

++ 2 📷 4 0 🗙 🗆 2 🖬 🖬	5 X X X Y 2 X	
Console Root	Name	Type
p 🚜 Active Directory Domains and Trusts LAB-DC	Administrator	User
# 🧧 Active Directory Users and Computers (LAB-D	& Allowed RODC Password	Security Gr
5 Sevel Queries	& calo-maintenance	User
a 🛐 michamen.com	SR. Cert Publishers	Security Ge
p 🛄 Builtin	R. CountA	User
p 🛄 Computers	R Clonable Domain Centr-	Security Go
Domain Controllers	R Denied RODC Passaged -	Security Co.
E ForeignGecurityPrincipals	SR Desidences	Serverity Con
p Annaged Service Accounts	12 Could a fait day	Second Co.
Die Contraction in the Contraction	& Domain Admins	Security Ge

IIS Konfiguration für Authentifizierung und SSL-Bindung

Aktivieren NTLM Authentifizierung

- Navigieren Sie zu MMC-Snap-Ins, und wählen Sie unter dem Snap-In Internetinformationsdienste (IIS)-Manager den Servernamen aus.
- Die Funktionsliste wird im nächsten Frame angezeigt. Doppelklicken Sie auf das Symbol **für die** Authentifizierungsfunktion.



• Windows-Authentifizierung markieren und im Bereich "Aktionen" (rechter Bereich) die Option Aktivieren auswählen

● ● ▲ AB-DC-RTP →				
Connections Q	Authentication Group by: No Grouping -			Actions Enable Help
Application Pools P- Sites	Name Anonymous Authentication ASP.NET Impersonation Windows Authentication	Status Enabled Disabled Disabled	Response Type HTTP 401 Challenge	

• Aktionsbereich zeigt die Option **"Erweiterte Einstellungen**" an; wählen Sie sie aus, und deaktivieren Sie die Option **"Kernel-Modus-Authentifizierung aktivieren".**



• Wählen Sie Provider aus, und ordnen Sie NTML und Negotiate an.

Connections	Authentication			Alerts
0, • 🔚 ☎ 🖗,	Authentication			Click here to learn how
Start Page	Group by: No Grouping .			Protection.
Application Pools	Name *	Status	Response Type	Artises
p 🙀 Stes	Anonymous Authentication ASP.NET Impersonation	Enabled Disabled		Disable
	Windows Authentication	Enabled	HTTP 401 Challenge	Advanced Settings
	Enabled Providers: NTLM Negotiate Negotiate:Kerberos		Move Up	
			Remove	
	Select a provider from the list o to add it to the enabled provide Available Providers:	f available provide ns.	rs and click Add	

Identitätszertifikat für den Webserver generieren

Wenn dies nicht bereits der Fall ist, müssen Sie ein Zertifikat und ein Identitätszertifikat für Ihren Webdienst generieren, das von der Zertifizierungsstelle signiert wird, da CiscoRA keine Verbindung mit dem Zertifikat herstellen kann, wenn das Zertifikat des Webservers "Selbst signiert" ist:

• Wählen Sie Ihren Webserver aus dem **IIS-Snap-In aus**, und doppelklicken Sie auf das Funktionssymbol **Serverzertifikate**:



 Standardmäßig wird dort ein Zertifikat angezeigt, nämlich das selbstsignierte Stammzertifikat der Zertifizierungsstelle. Wählen Sie im Menü Aktionen die Option Domänenzertifikat erstellen. Geben Sie die Werte im Konfigurationsassistenten ein, um das neue Zertifikat zu erstellen. Stellen Sie sicher, dass es sich bei dem Common Name um einen auflösbaren FQDN (Fully Qualified Domain Name) handelt, und wählen Sie dann Weiter aus:



• Wählen Sie das Zertifikat Ihrer Stammzertifizierungsstelle als Aussteller aus, und wählen Sie **Beenden aus**:

Online Certification Authority Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember. Specify Online Certification Authority: LAB-DC-RTP\LAB-DC-RTP.michamen.com Example: CertificateAuthorityName\ServerName Friendly name: Web Cert issued by LAB-DC-RTP[Create Certif	icate		? X
Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember. Specify Online Certification Authority: LAB-DC-RTP\LAB-DC-RTP.michamen.com Example: CertificateAuthorityName\ServerName Friendly name: Web Cert issued by LAB-DC-RTP	Online Certification Autho	rity			
LAB-DC-RTP\LAB-DC-RTP.michamen.com Select Example: CertificateAuthorityName\ServerName Friendly name: Web Cert issued by LAB-DC-RTP	Specify the certification authority within yo and should be easy to remember. Specify Online Certification Authority:	ur domain that will si	ign the certificate. A	friendly name is	required
Example: CertificateAuthorityName\ServerName Friendly name: Web Cert issued by LAB-DC-RTP	LAB-DC-RTP\LAB-DC-RTP.michamen.com				Select
Friendly name: Web Cert issued by LAB-DC-RTP	Example: CertificateAuthorityName\Server	lame			
Web Cert issued by LAB-DC-RTP	Friendly name:				
	Web Cert issued by LAB-DC-RTP				
		Previous	Net	Finish	Cancel
Previous Next Finish Cancel				-	

• Es werden sowohl das Zertifizierungsstellenzertifikat als auch das Identitätszertifikat Ihres Webservers aufgeführt:

• 🖬 🖄 😣	•	Server Certificates			
Start Page LAB-DC-RTP (MICHAMENT).A	Use this	feature to request and mana	ge certificates that the Web serv	er can use with websites c	onfigured for SSL
Application Pools	Filter	• 7 G	🛛 - 🥁 Show All Group by: - M	No Grouping •	
a 😹 Stei	Name	•	Issued To	issued By	Expiration Date
a 😔 Default Web Site			LAB-DC-RTP	LAB-DC-RTP	2/26/2024 4:34:42
p - 20 CertEnvoll	Web C	et issued by L&B-DC-RTP	LAR-DC-IS michamen.com	LAB-DC-RTP	2/25/2021 6:56:01

Webserver SSL-Bindung

• Wählen Sie in der Strukturansicht eine Site aus (Sie können die Standardwebsite verwenden oder sie für bestimmte Sites detaillierter gestalten), und wählen Sie **Bindungen** aus dem Aktionsbereich aus. Dadurch wird der Bindungs-Editor geöffnet, mit dem Sie Bindungen für die Website erstellen, bearbeiten und löschen können. Wählen Sie **Hinzufügen** aus, um die neue SSL-Bindung zur Site hinzuzufügen.

Sites + Def	ault Web Site	•					10 100 (5
🥥 D	efault Web	Site Hom	е				Actions
Filter		• ¥ 60 - 5	Show All	Group by:		1	Edit Permissions
		a		-		^	Edit Site Bendings
ASP	Authentic	Compression	Default	Directory Browsing	Error Pages		View Applications
	Sites > Def	Sites > Default Web Site Default Web Filter S Ass Authentic.	Sites > Default Web Site > Default Web Site Hom Fite: • @ Go • C S AsP Authentic Compression	Sites -> Default Web Site +> Default Web Site Home Fite: • • • • Go - • • • Show All S As9 Authentic Compression Default De	Sites > Default Web Site + > Default Web Site Horne Fite: Site Site AsP Authentic_ Compression Compared Compared Default Defau	Sites > Default Web Site + > Default Web Site Horne Fite:	Sites > Default Web Site + > Default Web Site Horne Fite: Fite: Asp Authentic_ Compression Default Directory Ener Pages Directory Ener Pages

• Die Standardeinstellungen für eine neue Bindung werden auf HTTP an Port 80 festgelegt. Wählen Sie in der Dropdown-Liste **Type** (**Typ**) die Option **https aus**. Wählen Sie das selbstsignierte Zertifikat, das Sie im vorherigen Abschnitt erstellt haben, aus der Dropdown-Liste **SSL-Zertifikat**, und wählen Sie dann **OK aus**.

			Site	Bindings	? X
Type http	Host Name	Port 80	IP Address	Binding Informa	Add Edit
			Add Site Bi	nding	? X emove
Ho	ps v st name: Require Server Nar	All Unass	igned on	v 443	
SSL	. certificate:				
We	eb Cert issued by L	AB-DC-RTP		✓ Select	View
	b Cert issued by U B-DC-RTP	AB-DC-RTP		OK	Caprel

• Jetzt haben Sie eine neue SSL-Bindung auf Ihrer Website und alles, was bleibt, ist zu überprüfen, dass es funktioniert, indem Sie **Durchsuchen *:443 (https)** Option aus dem Menü und stellen Sie sicher, dass die Standard-IIS-Webseite HTTPS verwendet:

			Site	Bindings	?
Type	Host Name	Port 80	IP Address	Binding Informa	Add
ittps		443	•		Edit
					Bemove
					Browse
					Church

Act	tions
0	Explore
1000	Edit Permissions
	Edit Site
	Bindings
Ē	Basic Settings
	View Applications
	View Virtual Directories
Ma	nage Website 🔗
2	Restart
▶	Start
	Stop
	Browse Website
•	Browse *:80 (http)
•	Browse *:443 (https)
	Advanced Settings
	Configure

• Denken Sie daran, den IIS-Dienst nach Konfigurationsänderungen neu zu starten. Verwenden Sie die Option **Neustart** im Aktionsbereich.

Konfiguration des CUCM

 Navigieren Sie zu Ihrer AD CS-Webseite (<u>https://YOUR_SERVER_FQDN/certsrv/</u>), und laden Sie das CA-Zertifikat herunter.



• Navigieren Sie von der Seite "OS Administration" zu Security > Certificate Management, und wählen Sie die Schaltfläche Upload Certificate/Certificate chain aus, um das CA-Zertifikat hochzuladen, dessen Zweck auf CAPF-trust festgelegt ist.

Upload Certificate/Certificate/	ate chain
Upload 🖳 Close	
Status Warning: Uploading a clu	uster-wide certificate will distribute it to a
Certificate Purpose* Description(friendly name) Upload File	CAPF-trust Browse LAB-DC-RTP_CA.cer

... An dieser Stelle ist es auch empfehlenswert, dasselbe CA-Zertifikat wie *CallManager-trust* hochzuladen, da es erforderlich ist, wenn die sichere Signalisierungsverschlüsselung für die Endpunkte aktiviert ist (oder aktiviert wird). Dies ist wahrscheinlich, wenn sich der Cluster im gemischten Modus befindet.

- Navigieren Sie zu **System > Service Parameters (System > Dienstparameter).** Wählen Sie den Unified CM Publisher-Server im Serverfeld und die **Cisco Certificate Authority Proxy-Funktion** im Dienstfeld aus.
- Legen Sie den Wert des Zertifikatausstellers auf Endpunkt auf Online-Zertifizierungsstelle fest, und geben Sie die Werte für die Felder "Online-Zertifizierungsparameter" ein. Stellen Sie sicher, dass Sie den FQDN des Webservers, den Namen der zuvor erstellten Zertifikatvorlage (Cisco RA), den CA-Typ als Microsoft CA und die Anmeldeinformationen des zuvor erstellten CiscoRA-Benutzerkontos verwenden.

Service Para	meter Configuration	
🔚 Save 🧬	Set to Default	
Select Serve	r and Service	
Server*	cucm125pubCUCM Voice/Video (Active)	
Service*	Cisco Certificate Authority Proxy Function (Active) 🗸	
All parameters	s apply only to the current server except parameters that are in the clu	ster-wide group(s).
Cisco Certifie	cate Authority Proxy Function (Active) Parameters on server o	ucm125pubCUCM Voice/Video (Activ
Parameter Na	me	Parameter Value
Certificate Iss	uer to Endpoint_*	Online CA
Duration Of Co	ertificate Validity (in days) *	1825
Key Size *		1024
Maximum Allo	wable Time For Key Generation *	30
Maximum Allo	wable Attempts for Key Generation *	3
-Online CA P	arameters	
Online CA H	arametars	
Online CA R		lab-dc-lis.michamen.com
Online CA Po	<u>.</u>	443
Online CA Te	emplate	CiscoRA
Online CA Ty	rpe_*	Microsoft CA
Online CA Us	sername	•••••
Online CA Pa	assword	•••••

 Ein Popup-Fenster informiert Sie, dass der CAPF-Dienst neu gestartet werden muss. Aktivieren Sie jedoch zuerst den Cisco Certificate Enrollment Service über Cisco Unified Serviceability > Tools > Service Activation, wählen Sie den Publisher im Serverfeld aus, aktivieren Sie das Kontrollkästchen Cisco Certificate Enrollment Service, und klicken Sie dann auf die Schaltfläche Save:



Überprüfung

Überprüfen von IIS-Zertifikaten

• Navigieren Sie von einem Webbrowser auf einem PC mit Verbindung zum Server (vorzugsweise im selben Netzwerk wie der CUCM Publisher) zu URL:

https://YOUR_SERVER_FQDN/certsrv/

• Das Zertifikat wird als nicht vertrauenswürdig angezeigt. Fügen Sie die Ausnahme hinzu, und überprüfen Sie das Zertifikat. Stellen Sie sicher, dass er dem erwarteten FQDN entspricht:



• Nachdem Sie die Ausnahme akzeptiert haben, müssen Sie sich authentifizieren. An dieser Stelle müssen Sie die für das Cisco RA-Konto konfigurierten Anmeldeinformationen früher verwenden:

Authentication	n Required >
?	https://lab-dc-iis.michamen.com is requesting your username and password.
User Name:	ciscora
Password:	••••••
	OK Cancel
	OK Cancel

• Nach der Authentifizierung müssen Sie in der Lage sein, die Willkommensseite von AD CS (Active Directory Certificate Services) anzuzeigen:



CUCM-Konfiguration überprüfen

Führen Sie die üblichen Schritte aus, um ein LSC-Zertifikat auf einem der Telefone zu installieren.

Schritt 1: Öffnen Sie die Seite CallManager Administration, Device (Gerät) und dann Phone (Telefon).

Schritt 2: Wählen Sie die Schaltfläche Suchen, um die Telefone anzuzeigen.

Schritt 3: Wählen Sie das Telefon aus, auf dem Sie das LSC installieren möchten.

Schritt 4: Blättern Sie nach unten zu CAPF-Informationen (Certification Authority Proxy Function)

Schritt 5: Wählen Sie im Zertifikatvorgang die Option Installieren/Aktualisieren aus.

Schritt 6: Wählen Sie den Authentifizierungsmodus aus. (Mit Null String ist für Testzwecke kein Problem.)

Schritt 7. Navigieren Sie zum oberen Seitenrand, und wählen Sie Save (Speichern) und dann Apply Config (Konfiguration für Telefon übernehmen) aus.

Schritt 8: Verwenden Sie nach dem Neustart und der Registrierung des Telefons den LSC-Statusfilter, um die erfolgreiche Installation des LSC zu bestätigen.

- Öffnen Sie auf dem AD-Server die MMC, und erweitern Sie das Snap-In Zertifizierungsstelle, um den Ordner Ausgestellte Zertifikate auszuwählen.
- Der Eintrag für das Telefon wird angezeigt. In der Zusammenfassungsansicht werden einige Details angezeigt:
 - Anforderungs-ID: Eindeutige Sequenznummer
 - Name des Antragstellers: Der Benutzername des konfigurierten CiscoRA-Kontos muss angezeigt werden.
 - · Zertifikatvorlage: Der Name der erstellten CiscoRA-Vorlage muss angezeigt werden.
 - Ausgestellter allgemeiner Name: Das Modell des Telefons, an das der Gerätename angehängt wird, muss angezeigt werden.
 - · Gültigkeitsdatum des Zertifikats und Ablaufdatum des Zertifikats



Verwandte Links

- Fehlerbehebung CAPF Online CA
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>

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.