UCCE\PCCE - Verfahren zum Abrufen und Hochladen des Zertifikats der selbstsignierten Windows-Server- oder Zertifizierungsstelle (Certificate Authority, CA) für 2008-Server

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Schritt 1: Erstellen von CSR über den IIS-Manager (Internetinformationsdienste) Schritt 2: Laden Sie das CA Signed Certificate in den IIS-Manager (Internetinformationsdienste) hoch. Schritt 3: Binden des signierten CA-Zertifikats an die Standardwebsite Überprüfen Fehlerbehebung Ähnliche Diskussionen in der Cisco Support Community

## Einführung

In diesem Dokument wird beschrieben, wie das Zertifizierungszertifikat der Zertifizierungsstelle (Certificate Authority, CA) auf Unified Contact Center Enterprise (UCCE)-Windows 2008 R2-Servern konfiguriert wird.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie mit dem Prozess für signierte und selbstsignierte Zertifikate vertraut sind.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Windows 2008 R2
- UCCE 10.5(1)

## Konfigurieren

Das Einrichten eines Zertifikats für die HTTPS-Kommunikation auf dem Windows-Server ist ein

dreistufiger Prozess.

- Erstellen einer CSR-Anfrage (Certificate Signing Request) vom IIS-Manager (Internetinformationsdienste)
- Laden Sie das CA Signed Certificate in den IIS-Manager (Internetinformationsdienste) hoch.
- Binden des signierten CA-Zertifikats an die Standardwebsite

### Schritt 1: Erstellen von CSR über den IIS-Manager (Internetinformationsdienste)

1. Melden Sie sich bei Windows an, und klicken Sie auf **Start > Ausführen > Alle Programme > Verwaltung > Internetinformationsdienste (IIS)-Manager**, wie in diesem Bild gezeigt. Wählen Sie IIS-Version 6 nicht aus, sofern vorhanden.

Active Directory Domains and Trusts           Active Directory Module for Windows Po           Active Directory Sites and Services           Active Directory Users and Computers	
ADSI Edit Component Services	administrator
Computer Management Data Sources (ODBC)	Documents
Event Viewer Internet Information Services (IIS) 6.01	Computer
internet Information Services (IIS) Man ISCSI Initiator	Network
Local Security Policy Performance Monitor	Control Panel
🚡 Security Configuration Wizard 🗕 🗕	Devices and Printers
🤹 Services 🙀 🙀 Share and Storage Management	Administrative Tools
Storage Explorer System Configuration	Help and Support
🖲 Task Scheduler 📃 💌	Run
▲ Back	Windows Security
Search programs and files	Log off

2. Wählen Sie im Fensterbereich Verbindungen links den Servernamen aus, wie in diesem Bild gezeigt.



3. Wählen Sie im mittleren Fensterbereich **IIS > Serverzertifikate aus**. Doppelklicken Sie auf Serverzertifikate, um das Zertifikatsfenster zu erstellen, wie in diesem Bild gezeigt.

Connections	Si 👘	MWORK H	ome					
Start Page ICMWORK (ORA\administrator)	Filter:		▪ 👬 Go - ⊽	Show All   G	iroup by: Area			-
		A			<u> </u>			
	Authentication	Compression	Default Document	Directory Browsing	Error Pages	Handler Mappings	HTTP Redirect	
		<b>6</b>	۵			4		
	HTTP Respo	ISAPI and CGI Restrictions	ISAPI Filters	Logging	MIME Types	Modules	Output Caching	
	Carlos Request Filtering	Server Certificates	Worker Processes					

4. Klicken Sie im rechten Teilfenster auf **Aktionen > Zertifikatsanforderung erstellen**, wie in diesem Bild gezeigt.

Act	tions
	Import
	Create Certificate Request
	Complete Certificate Request
	Create Domain Certificate
	Create Self-Signed Certificate
?	Help
	Online Help

5. Geben Sie zum Ausfüllen des Zertifikatsantrags den Gemeinsamen Namen, die Organisation, die Organisationseinheit, Stadt/Ort, Bundesland/Region und das Land/die Region ein, wie in diesem Bild gezeigt.

Request Certificate		? X
Distinguishe	d Name Properties	
Specify the required informa as official names and they ca	tion for the certificate. State/province and City/locality must be specified annot contain abbreviations.	
Common name:		
Organization:		
Organizational unit:		
City/locality		
State/province:		
Country/region:	US	
	Previous Next Finish Cano	el

6. Klicken Sie auf Next (Weiter), um die Länge des kryptografischen und Sicherheitsbits zu ändern. Es wird empfohlen, mindestens 2048 zu verwenden, um die Sicherheit zu verbessern, wie in diesem Bild gezeigt.

<b>P</b>	Cryptographic Service Provider Properties
Select a c determine However,	ryptographic service provider and a bit length. The bit length of the encryption key is the certificate's encryption strength. The greater the bit length, the stronger the security. a greater bit length may decrease performance.
Cryptogra	aphic service provider:
Microsoft	RSA SChannel Cryptographic Provider
Bit length 2048	

7. Speichern Sie die Zertifikatsanforderung an dem gewünschten Speicherort, der wie in diesem Bild gezeigt als TXT-Format gespeichert wird.

8. Geben Sie diese Datei an, die von dem Team signiert wird, das die interne CA oder die externe CA-Serviceanfrage verwaltet, wie in diesem Bild gezeigt.

# Schritt 2: Laden Sie das CA Signed Certificate in den IIS-Manager (Internetinformationsdienste) hoch.

1. Melden Sie sich bei Windows an, und klicken Sie auf **Start > Ausführen > Alle Programme > Verwaltung > Internetinformationsdienste (IIS)-Manager,** wie in diesem Bild gezeigt. Wählen Sie IIS-Version 6 nicht aus, sofern vorhanden.

Active Directory Domains and Trusts          Active Directory Module for Windows Po         Active Directory Sites and Services         Active Directory Users and Computers	
ADSI Edit	administrator
Computer Management     Data Sources (ODBC)	Documents
Event Viewer Internet Information Services (IIS) 6.0 [	Computer
Internet Information Services (IIS) Man ISCSI Initiator	Network
Local Security Policy	Control Panel
Security Configuration Wizard	Devices and Printers
Services	Administrative Tools
Storage Explorer	Help and Support
Task Scheduler	Run
<ul> <li>■ Back</li> </ul>	Windows Security
Search programs and files	Log off

2. Wählen Sie im Fensterbereich Verbindungen links den Servernamen aus, wie in diesem Bild gezeigt.



3. Wählen Sie im mittleren Fensterbereich IIS > Serverzertifikate aus. Doppelklicken Sie auf

Serverzertifikate, um das Zertifikatsfenster zu erstellen, wie in diesem Bild gezeigt.



4. Klicken Sie im rechten Teilfenster auf **Aktionen > Zertifikatsanforderung abschließen**, wie in diesem Bild gezeigt.

Ac	tions
	Import
	Create Certificate Request
	Complete Certificate Request
	Create Domain Certificate
	Create Self-Signed Certificate
?	Help
	Online Help

5. Stellen Sie vor diesem Schritt sicher, dass das signierte Zertifikat im CER-Format vorliegt und auf den lokalen Server hochgeladen wurde. Klicken Sie auf die Schaltfläche ..., um die CER-Datei zu durchsuchen. Verwenden Sie im Namen Friendly den FQDN des Servers, wie in diesem Bild gezeigt.

Complete C	ertificate Request	? ×
<b>F</b>	Specify Certificate Authority Response	
Complete authority's	a previously created certificate request by retrieving the file that contains the certificate s response.	
File name	containing the certification authority's response:	
Friendly n	ame:	

6. Klicken Sie auf OK, um das Zertifikat hochzuladen. Bestätigen Sie nach Abschluss dieses Vorgangs, dass das Zertifikat jetzt im Fenster Serverzertifikate angezeigt wird, wie in diesem Bild gezeigt.

#### Server Certificates Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL. Name -Issued To Issued By Expir Cisco ICM Diagnostic Framework ... icmwork icmwork 6/30 **ICMWORK** Cisco ICM SSL Certificate **ICMWORK** 6/25 InCommon RSA Server CA 6/2/2018 6:59

### Schritt 3: Binden des signierten CA-Zertifikats an die Standardwebsite

1. Klicken Sie im IIS-Manager auf der linken Seite unter dem Fenster Verbindungen auf <server\_name> > Sites > Default Web Site, wie in diesem Bild gezeigt.



2. Klicken Sie im Fenster Aktionen auf der rechten Seite auf Bindungen, wie in diesem Bild gezeigt.



3. Klicken Sie im Fenster für Sitebindungen auf https, um weitere Optionen zu markieren. Klicken Sie auf Bearbeiten, um fortzufahren, wie in diesem Bild gezeigt.

5ite Bin	dings				? ×
Type http net.to net.p net.m	Host Name	Port 80	IP Address *	Binding 808:* * localhos localhos	Add Edit Remove Browse
https ◀		443			Close

4. Klicken Sie unter dem SSL-Zertifikatparameter auf den Abwärtspfeil, um das zuvor hochgeladene signierte Zertifikat auszuwählen. Zeigen Sie das signierte Zertifikat an, um den Zertifizierungspfad zu überprüfen, und die Werte stimmen mit dem lokalen Server überein. Wenn Sie fertig sind, drücken Sie OK, und schließen Sie das Fenster Site Bindings, wie in diesem Bild gezeigt.

Edit Site Binding	? ×
Type: IP address: https 💌 All Unassigned	Port:
Host name:	
SSL certificate:	
Not selected	View
Cisco ICM SSL Certificate Cisco ICM Diagnostic Framework service cer	tificate Cancel

5. Starten Sie den IIS-Admin-Dienst unter dem MMC-Snap-In Dienste neu, indem Sie auf **Start > Ausführen > services.msc** klicken, wie in diesem Bild gezeigt.

Help							
Name 🔶	Description	Status	Startup Type	Log On As			
Q Diagnostic Service	The Diagno		Manual	Local Service			
🔍 Diagnostic System	The Diagno		Manual	Local System			
🧛 Disk Defragmenter	Provides Di		Manual	Local System			
🔍 Distributed Link Tra	Maintains li	Started	Automatic	Local System			
Q Distributed Transac	Coordinate	Started	Automatic (D	Network S			
Q DNS Client	The DNS Cl	Started	Automatic	Network S			
Encrypting File Syst	Provides th		Manual	Local System			
Extensible Authenti	The Extens		Manual	Local System			
Runction Discovery	The FDPH		Manual	Local Service			
Runction Discovery	Publishes t		Manual	Local Service			
Group Policy Client	The servic	Started	Automatic	Local System			
Health Key and Cer	Provides X		Manual	Local System			
O-Human Interface D	Enables de		Manual	Local System			
IIS Admin Service	Enables thi	Chard	natic	Local System			
SA IKE and AuthIP IPs	The IKEEX		batic	Local System			

6. Bei erfolgreicher Eingabe der FQDN-URL für die Website sollte der Client-Webbrowser keine Warnung wegen eines Zertifikatsfehlers auslösen.

**Hinweis**: Wenn der IIS-Admin-Dienst fehlt, starten Sie den World Wide Web Publishing-Dienst neu.

## Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## 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.