## UCCE\PCCE - procedure voor het verkrijgen en uploaden van Windows-serverzelf-ondertekend of CA-certificaat (certificaatautoriteit) op 2008servers

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Stap 1. Generate CSR van Internet Information Services (IS) Manager Stap 2. Upload het CA-ondertekende certificaat naar Internet Information Services (IS) Manager Stap 3. Bind het ondertekende CA-certificaat aan de standaardwebsite Verifiëren Problemen oplossen Gerelateerde Cisco Support Community-discussies

## Inleiding

Dit document beschrijft hoe u zelfgetekende of een certificaat van de Autoriteit (CA) kunt configureren op Unified Contact Center Enterprise (UCCE) Windows 2008 R2-servers.

## Voorwaarden

#### Vereisten

Cisco raadt u aan kennis te hebben van het proces van het ondertekende en zelfondertekende certificaat.

#### Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Windows 2008 R2
- UCS E10.5(1)

## Configureren

Het instellen van een certificaat voor HTTPS-communicatie op Windows-server is een proces dat drie stappen omvat

- CSR (certificaataanvraag) genereren via Internet Information Services (IS) Manager
- Upload het CA-ondertekend certificaat naar Internet Information Services (IS) Manager
- Bind het ondertekende CA-certificaat op de Standaardwebsite

#### Stap 1. Generate CSR van Internet Information Services (IS) Manager

1. Meld u aan bij Windows en klik op Start > Start > Alle programma's > Administratieve tools > Internet Information Services (IS) Manager, zoals in deze afbeelding. Selecteer geen IS versie 6 als deze bestaat.

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

2. Selecteer in het venster Connections links de servernaam, zoals in deze afbeelding.



3. Selecteer in het middenvenster de optie **IS > Server Certificates**. Dubbelklik op Servercertificaten om het certificaatvenster te genereren, zoals in deze afbeelding wordt weergegeven.

Connections	Sin Ici	MWORK H	ome					
Start Page	Filter:		• 👬 60 - 😼	Show All 6	iroup by: Area		▼ as ▼	<b>_</b>
'. En es	IIS Authentication	Compression	Default Document	Directory Browsing	404 Error Pages	Handler Mappings	HTTP Redirect	
	HTTP Respo	ISAPI and CGI Restrictions	لی ISAPI Filters	Logging	MIME Types	Modules	Output Caching	
	Sequest Filtering	Server Certificates	Worker Processes					<b>•</b>

4. Klik in het rechtervenster op Acties > certificaataanvraag maken zoals in deze afbeelding.

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

5. Om het certificaatverzoek in te vullen, vermeld de gemeenschappelijke naam, organisatie, organisatie-eenheid, stad/plaats, staat/provincie en land/regio, zoals in deze afbeelding aangegeven.

Request Certificate		? ×
Distinguished	Name Properties	
Specify the required informati as official names and they car	on for the certificate. State/province and City/locality must be specified mot contain abbreviations.	
Common name:		
Organization:		
Organizational unit:		
City/locality		
State/province:		
Country/region:	US 🗸	
	·	
	Previous Next Finish Can	el

6. Klik op Next om de cryptografische en beveiligingsbit length te wijzigen, en wordt aanbevolen om ten minste 2048 te gebruiken voor een betere beveiliging, zoals in deze afbeelding wordt getoond.

<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. Sla de certificaataanvraag op de gewenste locatie op, die als een .TXT-indeling wordt opgeslagen, zoals in deze afbeelding.

8. Geef dit bestand op dat moet worden getekend door het team dat het interne CA- of externe CA-serviceverzoek beheert, zoals in deze afbeelding.

# Stap 2. Upload het CA-ondertekende certificaat naar Internet Information Services (IS) Manager

1. Meld u aan bij Windows en klik op Start > Start > Alle programma's > Administratieve tools > Internet Information Services (IS) Manager, zoals in deze afbeelding wordt getoond. Selecteer geen IS versie 6 als deze bestaat.

Active Directory Domains and Trusts          Active Directory Module for Windows Po         Active Directory Sites and Services         Active Directory Users and Computers	
ADSI Edit	administrator
Somponent Sonnees	Documents
Event Viewer           Internet Information Services (IIS) 6.01         ••••••••••••••••••••••••••••••••••••	Computer
Internet Information Services (IIS) Man Contractor	Network
Local Security Policy	Control Panel
Security Configuration Wizard	Devices and Printers
Services	Administrative Tools
Storage Explorer	Help and Support
🕘 Task Scheduler 📃 💌	Run
▲ Back	Windows Security
Search programs and files	Log off

2. Selecteer in het venster Connections links de servernaam, zoals in deze afbeelding.



3. Selecteer in het middenvenster de optie **IS > Server Certificates**. Dubbelklik op Server Certificaten om het certificaatvenster te genereren, zoals in deze afbeelding wordt weergegeven.



4. Klik in het rechtervenster op **Acties > Complete certificaataanvraag**, zoals in deze afbeelding weergegeven.

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

5. Zorg ervoor dat het ondertekende certificaat in .CER-indeling is en aan de lokale server is geüpload. Klik op de knop ... om door het .CER-bestand te bladeren. In de Vriendelijke naam, gebruik FQDN van de server, zoals getoond in deze afbeelding.

Complete C	ertificate Request	? ×
<b>F</b>	Specify Certificate Authority Response	
Complete authority'	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. Klik op OK om het certificaat te uploaden. Na voltooiing, bevestig het certificaat nu in het venster Server Certificates, zoals in deze afbeelding weergegeven.

Server Certificate	<b>S</b> age certificates that the Web se	rver can use with Web sites con	figured for SSL.
Name 🔺	Issued To	Issued By	Expir
Cisco ICM Diagnostic Framework	icmwork	icmwork	6/30
Cisco ICM SSL Certificate	ICMWORK	ICMWORK	6/25
	A CONTRACTOR OF A CONTRACTOR OF A CONTRACTOR OF A CONTRACTOR OF A CONTRACTOR A CONT	InCommon RSA Server CA	6/2/2018 6:59

#### Stap 3. Bind het ondertekende CA-certificaat aan de standaardwebsite

1. In het vliegtuig van het venster Connections Manager, klik met de linkerhand op de **<server\_name> Plaatsen > Standaardwebsite**, zoals in deze afbeelding wordt getoond.



2. Klik in het deelvenster Handelingen aan de rechterkant op Bindingen, zoals in deze afbeelding.

Ac	Actions				
2	Explore				
	Edit Site				
	Bindings				
	Basic Settings				
	View Applications				
	View Virtual Directories				

3. Klik in het venster Site bindings op https om meer opties te markeren. Klik op Bewerken om verder te gaan, zoals in deze afbeelding.

Si	te Binding	gs				? ×
	Type http net.tcp net.pipe net.m msmq	Host Name	Port 80	IP Address *	Binding 808:* * localhos localhos	Add Edit Remove Browse
	https		443			
						Close

4. Klik onder de SSL certificaatparameter op het pijltje onder in om het eerder geüpload Gesigneerde certificaat te selecteren. Bekijk het ondertekende certificaat om het certificeringspad en de waarden die overeenkomen met de lokale server te controleren. Na voltooiing druk op OK, dan sluit u af om uit het venster Site Bindings, zoals in deze afbeelding weergegeven.

dit Site Bindin	g	? >
Type: https	IP address:	Port:
Host name:		_
SSL certificate:		
Not selected	Contraction of the second	▼ View
Cisco ICM SSL Cisco ICM Diag	Cercinicace nostic Framework service certificat	cancel

5. Start de IIS Admin Service opnieuw onder de CZS MCS-module door op **Start > Run > Services.msc.** te klikken, zoals in deze afbeelding wordt getoond.

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	Chart	patic	Local System
SA IKE and AuthIP IPs	The IKEEX		batic	Local System

6. Indien geslaagd, zou de client web browser geen certificaatfout moeten veroorzaken wanneer zij de FQDN URL voor de website invoert.

Opmerking: Als de IIS Admin Service niet is voltooid, levert u de World Wide Web Publishing Service op.

## Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

### Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.