# UCCE \ PCCE -程序获得并上载Windows服务器 自已-签字的或在2008个服务器的Certificate Authority (CA)认证

## Contents

 Introduction

 Prerequisites

 Requirements

 Components Used

 Configure

 步骤1.生成从互联网信息服务(IIS)管理器的CSR

 步骤2.加载CA签名的证书到互联网信息服务(IIS)管理器

 步骤3.捆绑签字的CA证书到默认网站

 Verify

 Troubleshoot

 相关的思科支持社区讨论

### Introduction

本文描述如何配置在统一的联系中心企业(UCCE) Windows的自已签署的或Certificate Authority (CA)认证2008个R2服务器。

## Prerequisites

### Requirements

Cisco建议您有签字的和自签证书进程知识。

### **Components Used**

本文档中的信息基于以下软件版本:

- Windows 2008个R2
- UCCE 10.5(1)

## Configure

设置HTTPS通信的认证关于Windows服务器是三步的过程

- •生成认证署名请求(CSR)从互联网信息服务(IIS)管理器
- •加载CA签名的证书到互联网信息服务(IIS)管理器
- 捆绑签字的CA证书到默认网站

### 步骤1.生成从互联网信息服务(IIS)管理器的CSR

1. 登录到Windows,点击**Start > Run >所有Programs > Administrative工具> Internet信息服务** (IIS)如此镜像所显示,**管理器**。如果存在,请勿选择IIS版本6。

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) 6.0 (	Computer
Internet Information Services (IIS) Man	Network
Local Security Policy	Control Panel
Security Configuration Wizard	Devices and Printers
Services	Administrative Tools
Storage Explorer           Image Storage Explorer           Image Storage Explorer	Help and Support
🖲 Task Scheduler 📃 🚽	Run
✓ Back	Windows Security
Search programs and files	Log off

2. 如此镜像所显示,在连接窗口面中到左边,请选择服务器名。

hternet Information Services (IIS	i) Manager				
GO ICMWORK >					
File View Help					
Connections		ome			
:	Filter:	🝷 🔐 Go 👒 🥁 Show All 🛛 Gr	oup by: Area		-
<u> </u>	ASP.NET				
	🔖 🔌	404		<b>\$</b>	ab
	.NET .NET Authorizati Compilation	.NET Error .NET Pages Globalization	.NET Trust Levels	Application Settings	Connection Strings
	SMTP E-mail				

3. 在中间窗玻璃中,请选择IIS >Server证书。如此镜像所显示,双击服务器证明生成认证窗口。

Connections 🔍 - 🔚   🖄   🔗		MWORK H	ome					
Start Page	Filter:		🕶 👬 Go 🕞 😼	Show All G	roup by: Area		-	
Application Pools ⊡ Sites	IIS							•
		Ą	0		404			
	Authentication	Compression	Default Document	Directory Browsing	Error Pages	Handler Mappings	HTTP Redirect	
			3		<b>3</b>			
	HTTP Respo	ISAPI and CGI Restrictions	ISAPI Filters	Logging	MIME Types	Modules	Output Caching	
	Sequest Filtering	Server Certificates	Worker Processes					•

4. 如此镜像所显示,在右窗格上,请点击**动作>创建证书请求**。

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

5. 如此镜像所显示,要完成证书请求,请进入在普通的名字、组织、组织单位、城市/现场、州/省 和国家/区域。

Request Certificate	? ×
Distinguished	Name Properties
Specify the required information as official names and they car	on for the certificate. State/province and City/locality must be specified not contain abbreviations.
Common name:	
Organization:	
Organizational unit:	
City/locality	
State/province:	
Country/region:	US 🔻
	Previous Next Finish Cancel

6.在修改旁边点击密码如此镜像所显示,并且安全比特长度,推荐使用至少2048更好的安全。

Request Certificate	? ×
Cryptographic Service Provider Properties	
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.	
Cryptographic service provider:	
Bit length:	

7. 如此镜像所显示,保存在将被保存作为.TXT格式的所需位置的证书请求。

8. 提供管理内部CA或外部CA服务请求的小组将签字的此文件,如此镜像所显示。

### 步骤2.加载CA签名的证书到互联网信息服务(IIS)管理器

1.登录到Windows,点击**Start > Run >所有Programs > Administrative工具> Internet信息服务** (IIS)如此镜像所显示,**管理器**。如果存在,请勿选择IIS版本6。

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) 6.0 [	Computer
Internet Information Services (IIS) Man Construction	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. 如此镜像所显示,在连接窗口面中到左边,请选择服务器名。



3. 在中间窗玻璃中,请选择IIS >Server证书。如此镜像所显示,双击服务器证明生成认证窗口。

Connections	🧤 ICI	MWORK H	ome					
Start Page     ICMWORK (ORA\administrator)     Application Pools	Filter:		• 👬 Go 🔹 👳	Show All   G	roup by: Area		▼ 33 ▼	•
tes €	115							
		Compression	Default	Directory	Frror Pages	andler (	HTTP Redirect	
			Document	Browsing		Mappings		
			3		<b>jn</b>	4		
	HTTP Respo	ISAPI and CGI Restrictions	ISAPI Filters	Logging	MIME Types	Modules	Output Caching	
	Cequest Filtering	Server Certificates	Worker Processes					•

4. 如此镜像所显示,在右窗格上,请点击动作>完全证书请求。

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

5. 在此步骤之前,请保证签名的证书以.CER格式和被加载了到当地服务器。点击…按钮访问 .CER文件。如此镜像所显示,在友好名称里面,请使用服务器的FQDN。

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. 点击OK键加载认证。如此镜像所显示,当完成时,请确认认证当前出现于服务器证明窗口。

Server Certificate	S		
Use this feature to request and mana	age certificates that	the Web server can use with Web sites conf	igured for SSL.
Name 🔶	Issued To	Issued By	Expi
Cisco ICM Diagnostic Framework	icmwork	icmwork.	6/30
Cisco ICM SSL Certificate	ICMWORK	ICMWORK	6/25
		InCommon RSA Server CA	6/2/2018 6:59

### 步骤3.捆绑签字的CA证书到默认网站

1. 如此镜像所显示,在连接窗口飞机下的IIS管理器,左手,点击**<server\_name> >站点>默认网站** 。



2. 如此镜像所显示,在动作在右边的窗玻璃下,请点击捆绑。

Act	tions
è.	Explore Edit Permissions
	Edit Site
- (	Bindings
Ē	Basic Settings
	View Applications
	View Virtual Directories

#### 3. 在站点捆绑窗口,请点击https突出显示更多选项。如此镜像所显示,点击Edit继续。

site Bindings ? 🗙									
	Type http net.tcp net.pipe net.m msmq	Host Name	Port 80	IP Address *	Binding 808:* * localho: localho:	Add Edit Remove Browse			
	https		443						
						Close			

4. 在SSL验证参数下,请点击下箭头选择以前被加载的签名的证书。查看签名的证书验证证书路径 并且重视匹配当地服务器。如此镜像所显示,当完成请按OK,然后接近退出在站点捆绑窗口外面。

Edit Site Binding		? ×		
Type: https	IP address: All Unassigned	Port:		
Host name:	Host name:			
SSL certificate:				
Not selected	•	View		
Cisco ICM SSL Certin Cisco ICM Diagnostic	icace : Framework service certificate	Cancel		

5. 重新启动IIS Admin服务在服务MMC下卡扣式通过单击在**Start > Run > services.msc。**如此镜像 所显示。

Help									
Name 🔶	Description	Status	Startup Type	Log On As					
🔍 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	Charles 1	natic	Local System					
SA IKE and AuthIP IPs	The IKEEX	a fort	hatic	Local System					

6. 如果成功,客户端Web浏览器不应该提示警告任何的验证错误,当进入在网站的时FQDN URL。

Note:如果IIS Admin服务失踪请重新启动Web发布服务。

## Verify

当前没有可用于此配置的验证过程。

## Troubleshoot

目前没有针对此配置的故障排除信息。