# Criar e usar certificado de terceiros no UCSM

## Contents Introdução Pré-requisitos **Requisitos** Componentes Utilizados Etapas para configurar Configurar Ponto de Confiança Passo 1 Passo 2 Etapa 3 Criar chaveiro e CSR Passo 1 Passo 2 Etapa 3 Passo 4 Aplicar o toque de tecla Passo 1 Informações Relacionadas

## Introdução

Este documento descreve o procedimento para criar e usar certificados de terceiros no Unified Computing System (UCS) para comunicação segura.

## Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- · Acesso à autoridade de certificação
- UCSM 3.1

### **Componentes Utilizados**

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Etapas para configurar

## Configurar Ponto de Confiança

Passo 1

- Baixe a cadeia de certificados da autoridade de certificação para criar um Ponto de Confiança. Consulte <u>http://localhost/certsrv/Default.asp</u> no Servidor Cert.
- Verifique se a codificação está definida como Base 64.

Microsoft Active Directory Certificate Services - Enterprise CA-1	Recording	00:06:21	Ш	
Download a CA Certificate, Certificate Chain, or CRL				
To trust certificates issued from this certification authority, install this CA certificate.				
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.				
CA certificate:  Current [Enterprise CA-1(1)]				
Encoding method: ODER @Base 64				(0, ↑)
Install CA certificate Download CA certificate Download latest base CRL Download latest delta CRL				- <sup>2</sup> .

Baixar cadeia de certificados da autoridade de certificação

### Passo 2

• A cadeia de certificados baixada está no formato PB7.



- · Converta o arquivo .pb7 para o formato PEM com a ferramenta OpenSSL.
- Por exemplo, no Linux, você pode executar esse comando no terminal para executar a conversão- openssl pkcs7 -print\_certs -in <cert\_name>.p7b -out <cert\_name>.pem.

#### Etapa 3

- Crie um ponto de confiança no UCSM.
- Navegue até Admin > Gerenciamento de chaves > Trustpoint.
- Ao criar o ponto de confiança, cole o conteúdo completo do arquivo .PEM criado na etapa 2 desta seção no espaço de detalhes do certificado.



## Criar chaveiro e CSR

### Passo 1

- Navegue até UCSM > Admin > Key Management > Keyring.
- · Escolha o Módulo necessário para o certificado de terceiros.

Key Ring			
Name :		3rd-party	
Modulus	8 :	○ Mod2048 ○ Mod2560 ○ Mod3072 ○ Mod3584 ④ Mod4096	

Passo 2

- Clique em criar solicitação de certificado e preencha os detalhes solicitados.
- · Copie o conteúdo do campo de solicitação.

TUGADCGAUAWX7ELMAKHATUERDMGSU4XETAP
RAGMCEthcm5hdGErMRIw
OOHDAICYW5n/WyycmLyEzARBaN//BAaMCk/
E N

### Etapa 3

Para gerar o certificado, cole a solicitação copiada da etapa 2 no espaço mostrado abaixo:

Microsoft Active Directory Certificate Services - Enterprise CA-1

#### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 the Saved Request box.

Saved Request:					
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	<		~ ~		
Certificate Templ	ate: User - ING				
Additional Attribu	tes:				
Attributes:	<	>			
		Submi	t>		

#### Passo 4

 Depois de enviado, um novo certificado é gerado. Abra o arquivo e copie todo o conteúdo do certificado recém-gerado no campo do certificado no keyring criado na etapa 1 desta seção.

Trusted Point :	Trust-test	<b>T</b>	
Certificate :	BEGIN CERTIF MIIGLJCCBRagAwIB 9w0BAQsFADBIMR CZImiZPyLGQBGRY ZAEZFgJJTJEYMBY AxMPRW50ZXJwcr	FICATE AgiKS4anFAABAAa9 gwFgYK /laW50cmFuZXQxEjA GA1UE mlzZSBDQS0xMB4X[	DANBgkqhkiG QBgoJkiaJk/Is FE4MDUwOD

• Escolha o ponto de confiança no menu suspenso criado na etapa 3 de Criar chaveiro e CSR.

## Aplicar o toque de tecla

### Passo 1

Escolha o chaveiro criado nos serviços de comunicação como mostrado abaixo:

cisco	UCS Manager	
æ	All	All / Communication Management / Communication Services
8	<ul> <li>Locally Authenticated Users</li> <li>Remotely Authenticated Users</li> </ul>	Communication Services Events FSM Redirect HTTP to HTTPS : • Enabled O Disabled
格	<ul> <li>▶ Roles</li> <li>▼ Key Management</li> </ul>	Telnet
重	KeyRing default	Admin State : Enabled  Disabled
Q	KeyRing Test_Keyring KeyRing ucsm_5108	Admin State :  Enabled Disabled
=	TP inter TP root	Port : 443 Operational Port : 443
	TP Trust-test  Communication Management	Key Ring : KeyRing Test_Keyring ▼
20	Call Home	Cipher Suite Mode : High Strength I Medium Strength Cow Strength Coustom
	Communication Services	Cipher Suite : ALL:IDH:IEDH:IADH:IEXPORT40:IEXPORT56:ILOW:IR
	DNS Management Management Interfaces	Allowed SSL Protocols : Only TLSv1.2

Após a alteração no chaveiro, a conexão HTTPS com o UCSM aparece como segura em seu navegador da Web.



Observação: isso exige que a área de trabalho local também use o certificado da mesma autoridade CA que o UCSM.



## Informações Relacionadas

<u>Suporte Técnico e Documentação - Cisco Systems</u>

### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.