# Creación y uso de certificados de terceros en UCSM

Contenido
ntroducción
Prerequisites
Requirements
Componentes Utilizados
Pasos que se deben configurar
Configurar punto de confianza
Paso 1
Paso 2
Paso 3
Crear llavero y CSR
Paso 1
Paso 2
Paso 3
Paso 4
Aplicación del llavero
Paso 1
nformación Relacionada

# Introducción

Este documento describe el procedimiento para crear y utilizar certificados de terceros en Unified Computing System (UCS) para una comunicación segura.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso a la autoridad de la CA
- UCSM 3.1

### **Componentes Utilizados**

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Pasos que se deben configurar

### Configurar punto de confianza

Paso 1

- Descargue la cadena de certificados de la autoridad de la CA para crear un punto de confianza. Consulte <u>http://localhost/certsrv/Default.asp</u> dentro del servidor de certificados.
- Asegúrese de que la codificación está establecida en Base 64.

Microsoft Active Directory Certificate Services - Enterprise CA-1 00.05/21	
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:	۲
⊙DER ⊛Base 64	Ģ
Install CA certificate Download CA certificate Download Latest base	. <sup>4</sup> .

Descargar cadena de certificados de la autoridad de CA

### Paso 2

· La cadena de certificados descargada está en formato PB7.

Do you want to open or save certnew.p7b (4.83 KB) from

- Convierta el archivo .pb7 al formato PEM con la herramienta OpenSSL.
- Por ejemplo, en Linux, puede ejecutar este comando en terminal para realizar la conversiónopenssl pkcs7 -print\_certs -in <cert\_name>.p7b -out <cert\_name>.pem.

Paso 3

- Cree un punto de confianza en UCSM.
- Vaya a Admin > Key Management > Trustpoint.
- Cuando cree el punto de confianza, pegue todo el contenido del archivo .PEM creado en el paso 2 de esta sección en el espacio de detalles del certificado.



### Crear llavero y CSR

### Paso 1

- Vaya a UCSM > Admin > Key Management > Keyring.
- · Elija el módulo necesario para el certificado de terceros.

# Key Ring

Name :	3rd-party	
Modulus :	O Mod2048 O Mod2560 O Mod3072 O Mod3584	Mod4096

### Paso 2

- Haga clic en crear solicitud de certificado y rellene los detalles solicitados.
- Copie el contenido del campo de solicitud.

MIIC7z0	OA HAD A DAWNELLA AND A 11 FORMOUT IN FTAD
	CAOCCAQAWAZELMAKGA TUEBIMUSU4XETAP
BgNVB/	gMCEthcm5hdGFrMRIw
EAYDVO	QHDAICYW5nYWxvcmUxEzARBgNVBAoMCkV

### Paso 3

Para generar el certificado, pegue la solicitud copiada del paso 2 en el espacio que se muestra a continuación:

### 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.

ISE-64-encoded rtificate request MC or (CS #10 or (CS #7)-			< >	
	<		>	
artificato Tomplat				
	ser - ING	V		
ditional Attribute				
	э.			
A.H. 1.		$\bigcirc$		
Attributes:				

### Paso 4

 Una vez enviado, se genera un nuevo certificado. Abra el archivo y copie todo el contenido del certificado recién generado en el campo de certificado en el llavero creado en el paso 1 de esta sección.

Trusted Point :	Trust-test	<b>T</b>	
Certificate :	BEGIN CER MIGLJCCBRagAv W0BAQsFADBIN 22ImiZPyLGQBG AEZFgJJTJEYM8 AXMPRW50ZXJw	TIFICATE vIBAgIKS4anFAABAA MRgwFgYK RYIaW50cmFuZXQx BYGA1UE vcmIzZSBDQS0xMB4	DANBgkqhkiG QBgoJkiaJk/Is TE4MDUwOD

• Elija el punto de confianza en el menú desplegable creado en el paso 3 de Crear anillo de claves y CSR.

### Aplicación del llavero

### Paso 1

Elija el llavero creado en los servicios de comunicación como se muestra a continuación:

ili.ili. cisco	UCS Manager	
æ	All	All / Communication Management / Communication Services
8	Locally Authenticated Users     Remotely Authenticated Users	Communication Services Events FSM
뢂	<ul> <li>▶ Roles</li> <li>▼ Key Management</li> </ul>	Redirect HTTP to HTTPS :  Enabled Obisabled Telnet
≣	KeyRing default	Admin State : C Enabled  Disabled
Q	KeyRing Test_Keyring KeyRing ucsm_5108	Admin State :   Enabled  Disabled
≡	TP inter TP root	Port : 443
	TP Trust-test Communication Management	Key Ring : KeyRing Test_Keyring ▼
20	Call Home	Cipher Suite Mode : High Strength  Medium Strength  Low Strength  Custom
	Communication Services	Cipher Suite : ALL:IDH:IEDH:IADH:IEXPORT40:IEXPORT56:ILOW:IR
	DNS Management Management Interfaces	Allowed SSL Protocols : (e) default (Allow all except SSLv2 and SSLv3) () Only TLSv1.2 CIM XML

Después del cambio en el llavero, la conexión HTTPS con UCSM se muestra como segura en su navegador web.



Nota: Esto requiere que el escritorio local también utilice el certificado de la misma autoridad de CA que UCSM.



### Información Relacionada

Soporte Técnico y Documentación - Cisco Systems

### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).