Creación y uso de certificados de terceros en UCSM

Contenido

Introducción

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

Información 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

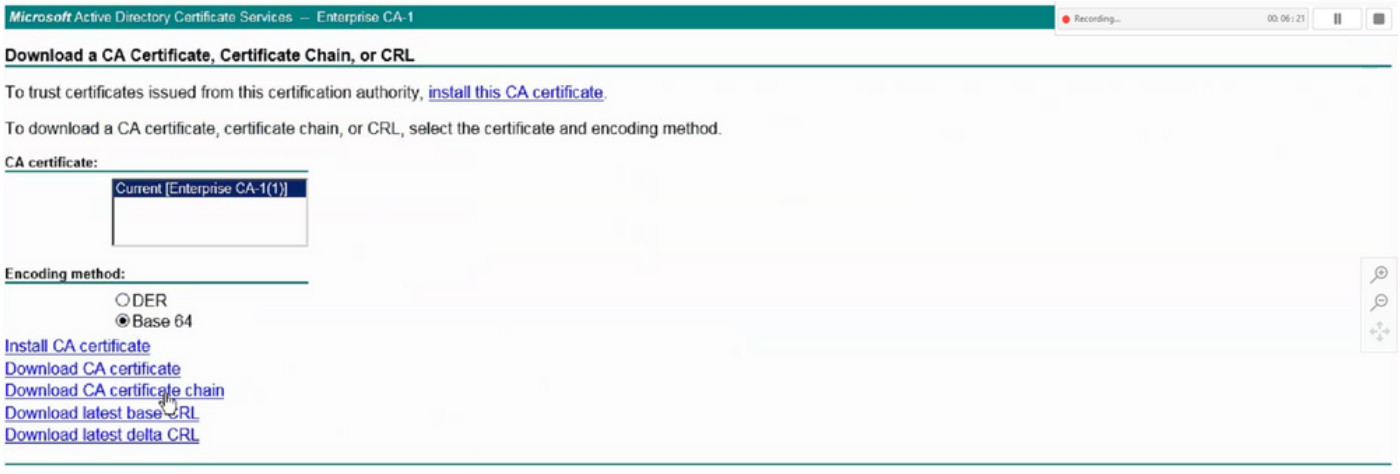
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Pasos que se deben configurar

Configurar punto de confianza

Paso 1

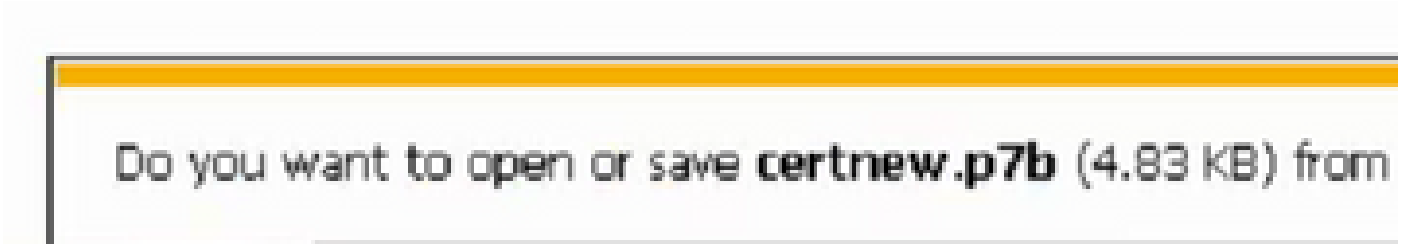
- Descargue la cadena de certificados de la autoridad de la CA para crear un punto de confianza. Consulte http://localhost/certsrv/Default.asp dentro del servidor de certificados.
- Asegúrese de que la codificación está establecida en Base 64.



Descargar cadena de certificados de la autoridad de CA

Paso 2

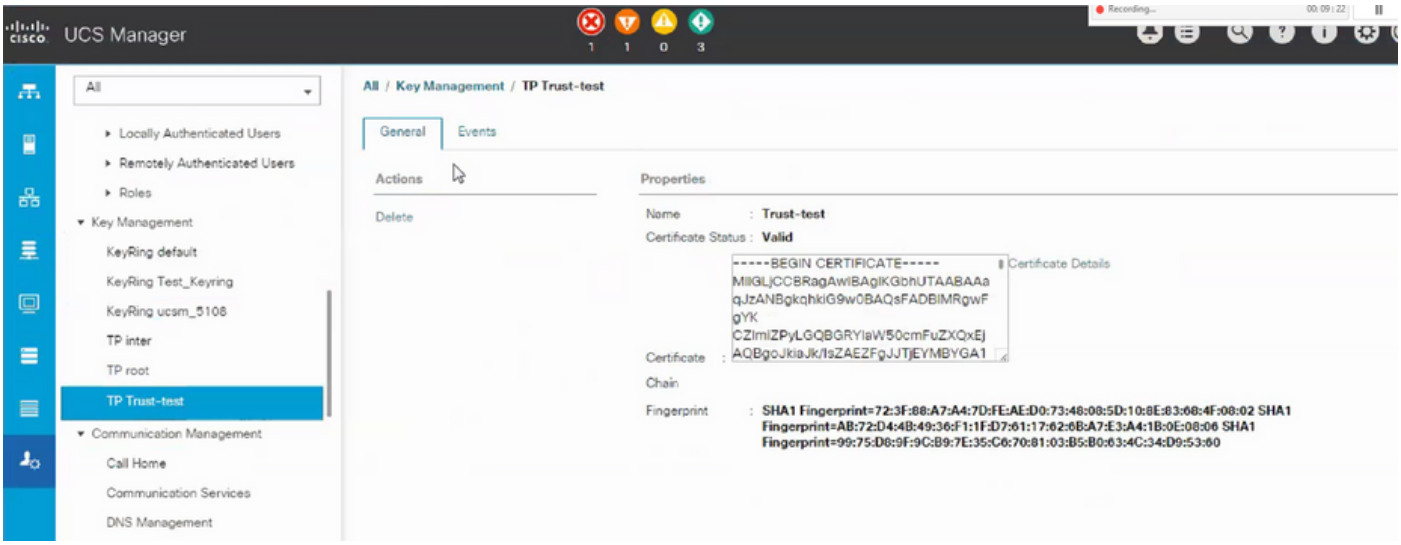
- La cadena de certificados descargada está en formato PB7.



- Convierta el archivo .pb7 al formato PEM con la herramienta OpenSSL.
- Por ejemplo, en Linux, puede ejecutar este comando en terminal para realizar la conversión- openssl pkcs7 -print_certs -in <cert_name>.p7b -out <cert_name>.pem.

Paso 3

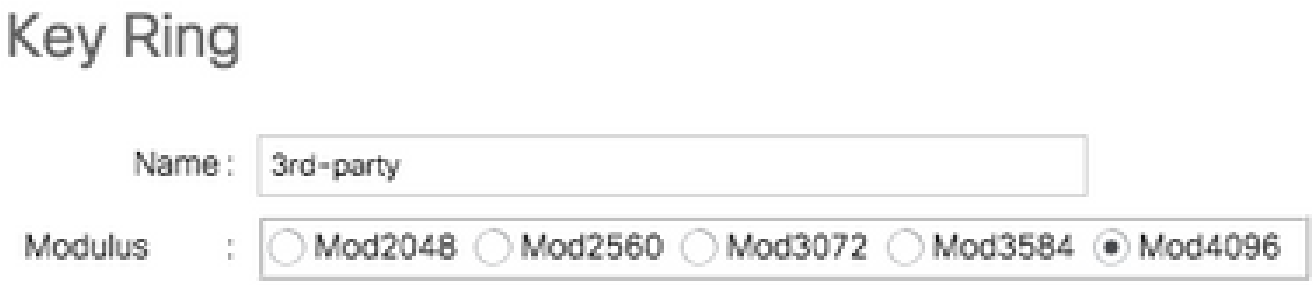
- Cree un punto de confianza en UCSM.
- Vaya a Admin > Key Management > Trustpoint.
- Cuando cree el punto de confianza, pegue todo el contenido del archivo .PEM creado en el paso 2 de esta sección en el espacio de detalles del certificado.



Crear llavero y CSR

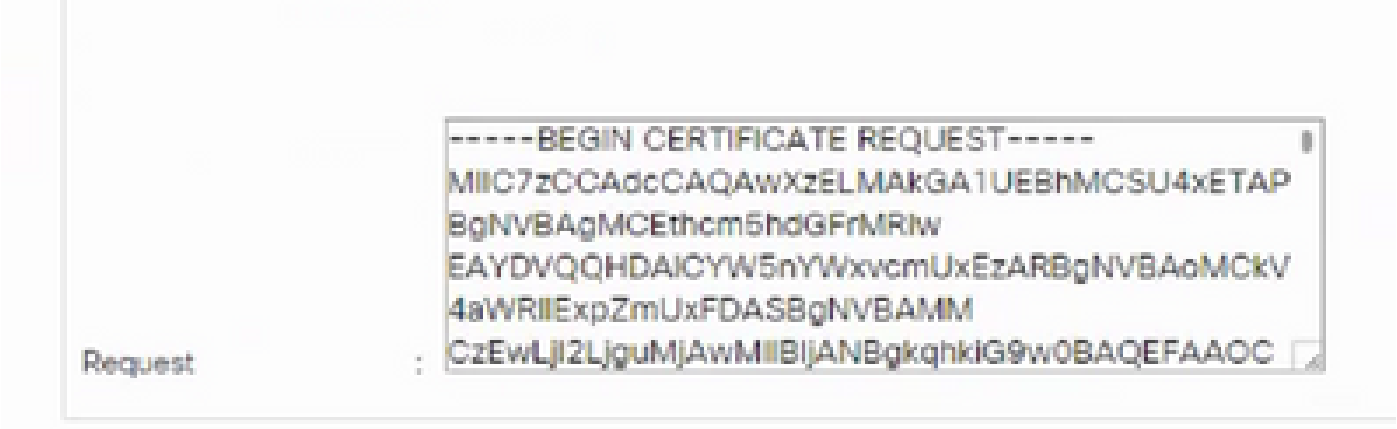
Paso 1

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



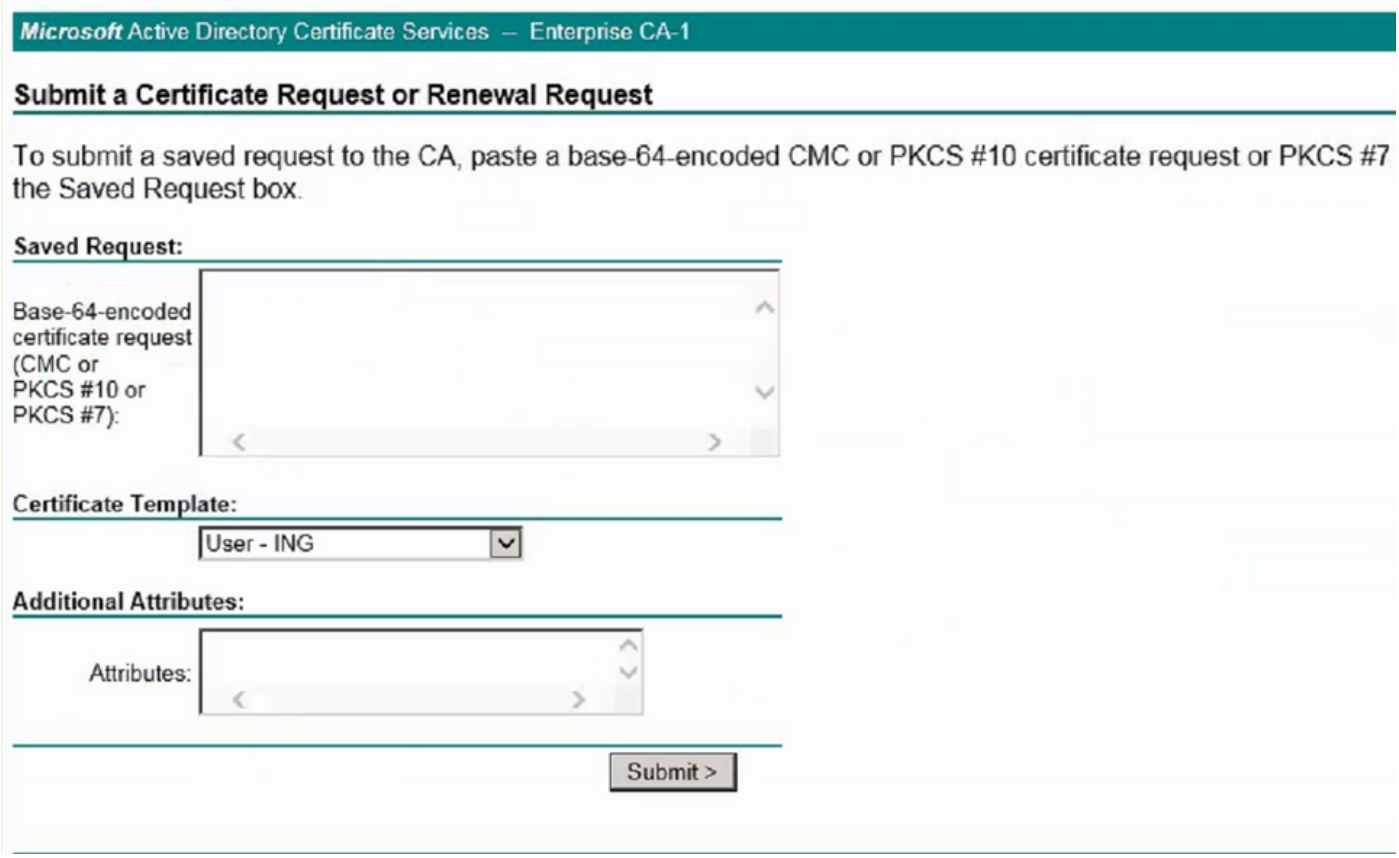
Paso 2

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



Paso 3

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



Paso 4

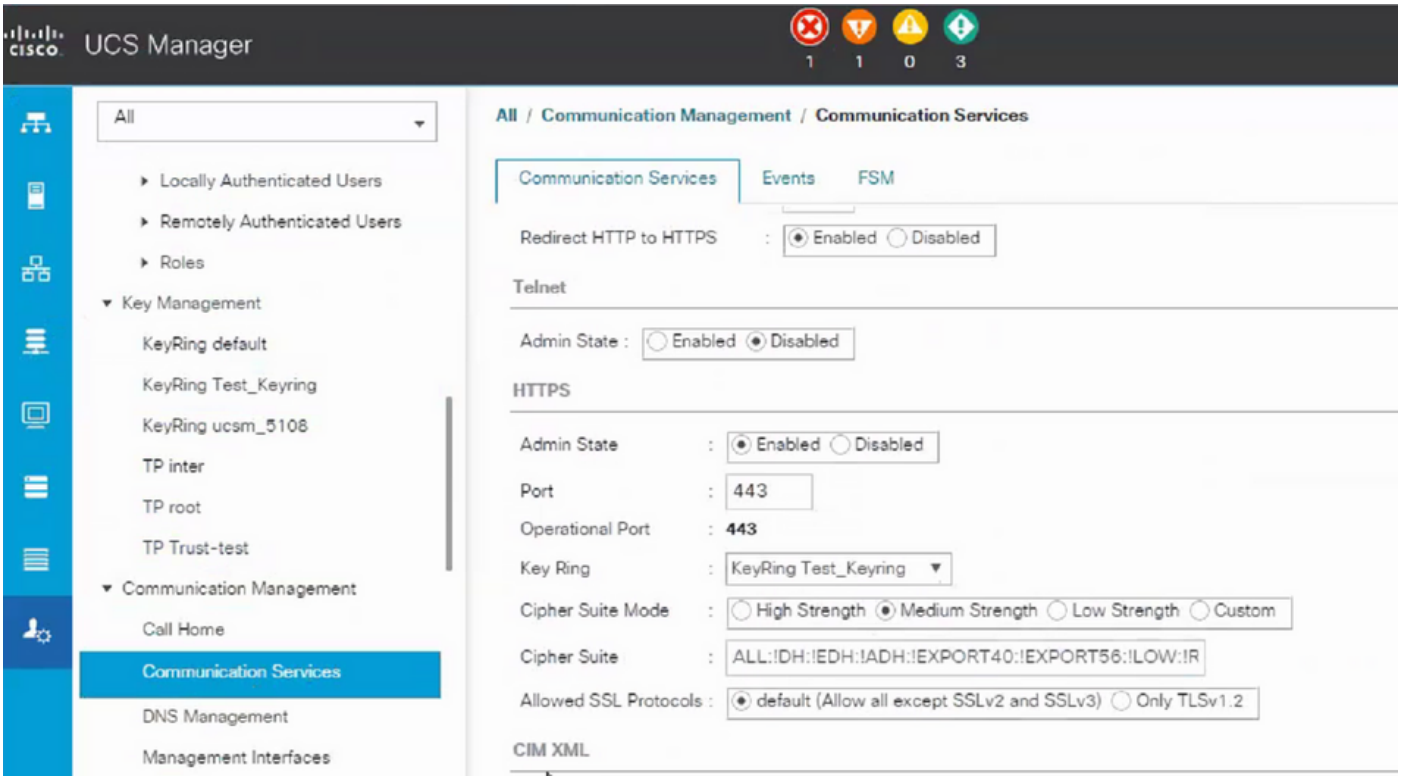
- Una vez enviado, se genera un nuevo certificado. Abra el archivo y copie todo el contenido del certificado recién generado en el campo de certificado en el llavero creado en el paso 1 de esta sección.

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

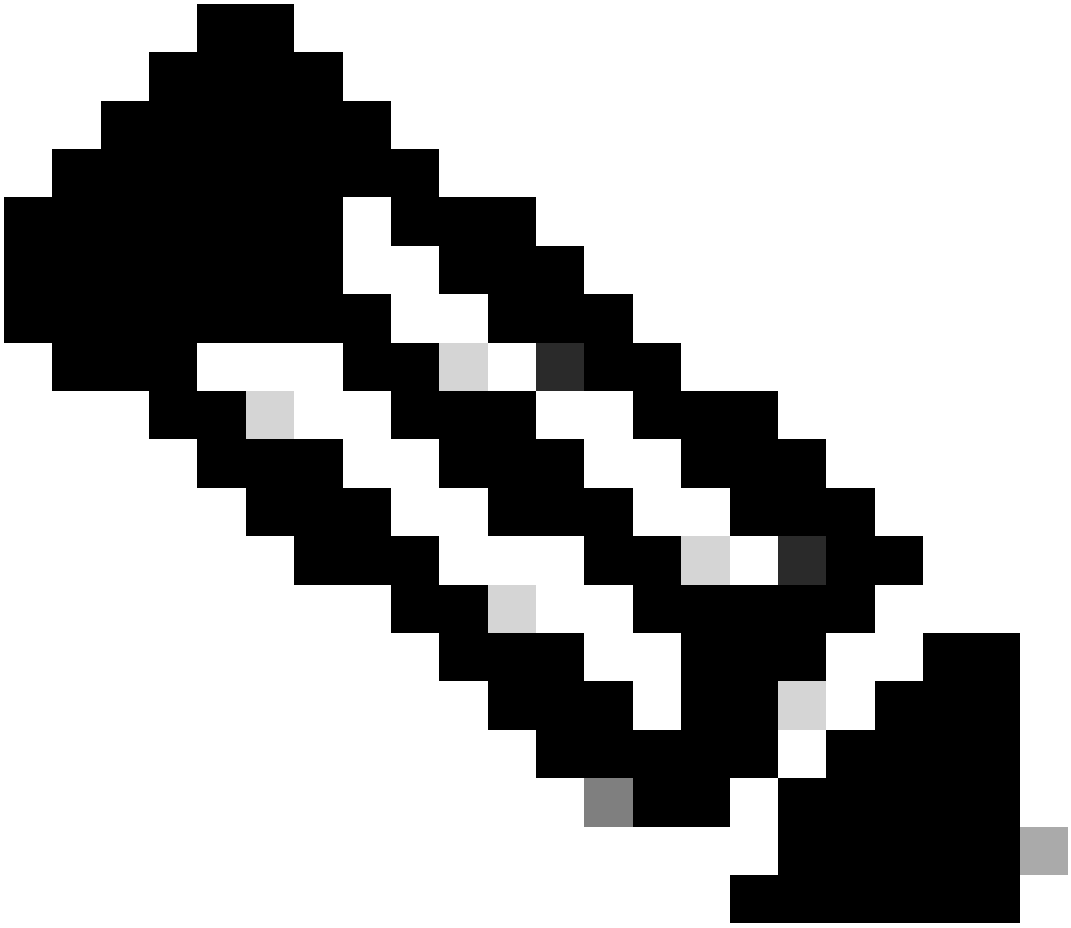
Aplicación del llavero

Paso 1

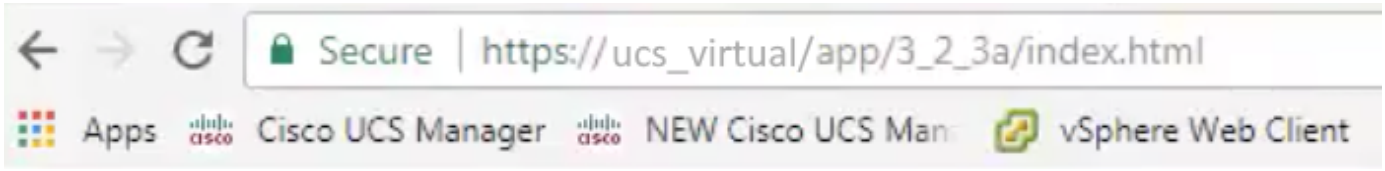
Elija el llavero creado en los servicios de comunicación como se muestra a continuación:



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).