CSM - Cómo instalar certificados SSL de terceros para el acceso a la GUI

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Creación de CSR desde la interfaz de usuario](#)
[Carga de certificado de identidad en el servidor CSM](#)

Introducción

Cisco Security Manager (CSM) proporciona una opción para utilizar certificados de seguridad emitidos por autoridades certificadoras (CA) de terceros. Estos certificados se pueden utilizar cuando la política organizativa impide el uso de certificados autofirmados CSM o requiere que los sistemas utilicen un certificado obtenido de una CA determinada.

TLS/SSL utiliza estos certificados para la comunicación entre el servidor CSM y el navegador cliente. Este documento describe los pasos para generar una solicitud de firma de certificado (CSR) en CSM y cómo instalar la identidad y los certificados de CA raíz en el mismo.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la arquitectura de certificados SSL.
- Conocimiento básico de Cisco Security Manager.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Security Manager versión 4.11 y posteriores.

Creación de CSR desde la interfaz de usuario

Esta sección describe cómo generar una CSR.

Paso 1. Ejecute la página de inicio de Cisco Security Manager y seleccione **Server Administration > Server > Security > Single-Server Management > Certificate Setup .**

Paso 2. Introduzca los valores necesarios para los campos descritos en esta tabla:

Campo	Notas de uso
Nombre del país	Código de país de dos caracteres.
Estado o provincia	Código provincial o de estado de dos caracteres o nombre completo del estado o provin
Localidad	El código de ciudad o ciudad de dos caracteres o el nombre completo de la ciudad o ciu
Nombre de la organización	Nombre completo de su organización o abreviatura.
Nombre de la unidad de organización	Complete el nombre de su departamento o una abreviatura.
Nombre del servidor	Nombre DNS, dirección IP o nombre de host del ordenador. Introduzca el nombre del servidor con un nombre de dominio correcto y resoluble. Es muestra en el certificado (ya sea autofirmado o emitido por un tercero). No se debe host local o 127.0.0.1.
Dirección de correo electrónico	Dirección de correo electrónico a la que se debe enviar el correo.

Paso 3. Haga clic en **Aplicar** para crear la CSR.

El proceso genera los siguientes archivos:

- server.key: clave privada del servidor.

- server.crt: certificado autofirmado del servidor.
- server.pk8: clave privada del servidor en formato PKCS#8.
- server.csr: archivo de solicitud de firma de certificado (CSR).

Nota: Esta es la ruta de acceso para los archivos generados.
~CSCOpx\MDC\Apache\conf\ssl\chain.cer
~CSCOpx\MDC\Apache\conf\ssl\server.crt
~CSCOpx\MDC\Apache\conf\ssl\server.csr
~CSCOpx\MDC\Apache\conf\ssl\server.pk8
~CSCOpx\MDC\Apache\conf\ssl\server.key

Nota: Si el certificado es un certificado autofirmado, no podrá modificar esta información.

Carga de certificado de identidad en el servidor CSM

Esta sección describe cómo cargar el certificado de identidad proporcionado por la CA en el servidor CSM

Paso 1 Busque el script de utilidad SSL disponible en esta ubicación

```
NMSROOT\MDC\Apache
```

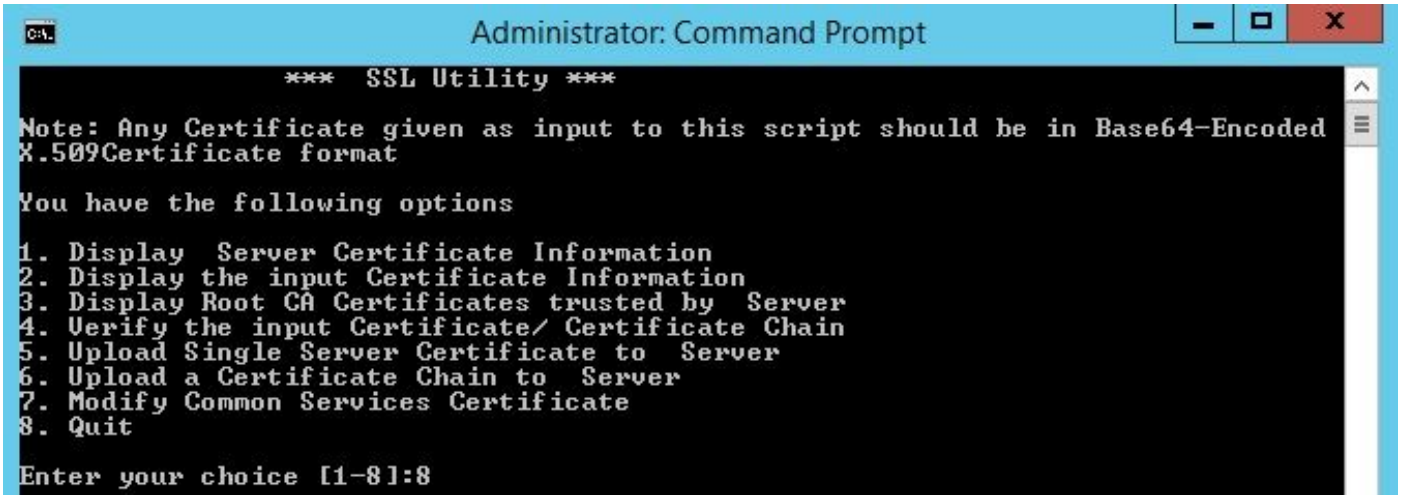
Nota: NMSROOT se debe reemplazar por el directorio donde se instala CSM.

Esta utilidad tiene estas opciones.

Número	Opción	Lo que hace...
1	Mostrar información del certificado del servidor	• Muestra los detalles del certificado del servidor CSM. Para los certificados emitidos por terceros, esta opción muestra los detalles del certificado del servidor, los certificados intermedios, si los hubiera, y el certificado de CA raíz.
2	Mostrar la información del certificado de entrada	• Verifica si el certificado es válido. Esta opción acepta un certificado como entrada y: • Verifica si el certificado está en formato de certificado X.509 codificado. • Muestra el asunto del certificado y los detalles del certificado em • Verifica si el certificado es válido en el servidor.
3	Mostrar certificados de CA raíz en los que confía el servidor	Genera una lista de todos los certificados de CA raíz.
4	Verificar el certificado de entrada o la cadena de certificado	Verifica si el certificado de servidor emitido por las CA de terceros pu cargarse. Al elegir esta opción, la utilidad: • Verifica si el certificado está en el formato de certificado X.509codificado Base64. • Verifica si el certificado es válido en el servidor • Verifica si la clave privada del servidor y el certificado del servido

		entrada coinciden. • Verifica si el certificado del servidor se puede rastrear hasta el certificado de CA raíz requerido mediante el cual se firmó. • Construye la cadena de certificados, si también se dan las caden intermedias, y verifica si la cadena termina con el certificado de C raíz adecuado. Después de completar la verificación correctamente, se le solicitará c cargue los certificados en el servidor CSM. La utilidad muestra un error: • Si los certificados de entrada no están en el formato requerido • Si la fecha del certificado no es válida o si el certificado ya ha caducado. • Si no se pudo verificar o rastrear el certificado del servidor a un certificado de CA raíz. • Si alguno de los certificados intermedios no se entregó como ent • Si falta la clave privada del servidor o si el certificado del servido se está cargando no se pudo verificar con la clave privada del servidor. Debe ponerse en contacto con la CA que emitió los certificados para corregir estos problemas antes de cargar los certificados en CSM. Debe verificar los certificados mediante la opción 4 antes de seleccio esta opción.
5	Cargar certificado de servidor único en el servidor	Seleccione esta opción, sólo si no hay certificados intermedios y sólo un certificado de servidor firmado por un certificado de CA raíz desta Si CSM no confía en la CA raíz, no seleccione esta opción. En estos casos, debe obtener un certificado de CA raíz utilizado para firmar el certificado de la CA y cargar ambos certificados mediante la opción 6. Cuando seleccione esta opción y proporcione la ubicación del certific la utilidad: • Verifica si el certificado está en el formato de certificado X.509 codificado Base64. • Muestra el asunto del certificado y los detalles del certificado em • Verifica si el certificado es válido en el servidor. • Verifica si la clave privada del servidor y el certificado del servido entrada coinciden. • Verifica si el certificado del servidor se puede rastrear al certifica CA raíz requerido que se utilizó para la firma. Después de completar la verificación correctamente, la utilidad carga certificado en CiscoWorks Server. La utilidad muestra un error: • Si los certificados de entrada no están en el formato requerido • Si la fecha del certificado no es válida o si el certificado ya ha caducado. • Si no se pudo verificar o rastrear el certificado del servidor a un certificado de CA raíz. • Si falta la clave privada del servidor o si el certificado del servido se está cargando no se pudo verificar con la clave privada del servidor.

		Debe ponerse en contacto con la CA que emitió los certificados para corregir estos problemas antes de volver a cargar los certificados en Debe verificar los certificados mediante la opción 4 antes de seleccio esta opción.
6	Cargar una cadena de certificados en el servidor	Seleccione esta opción si está cargando una cadena de certificados. también está cargando el certificado de CA raíz, debe incluirlo como de los certificados de la cadena. Cuando seleccione esta opción y proporcione la ubicación de los certificados, la utilidad: • Verifica si el certificado está en el formato de certificado X.509 codificado Base64. • Muestra el asunto del certificado y los detalles del certificado emi • Verifica si el certificado es válido en el servidor • Verifica si la clave privada del servidor y el certificado del servido coinciden. • Verifica si el certificado del servidor se puede rastrear al certifica CA raíz que se utilizó para la firma. • Construye la cadena de certificados, si se dan cadenas intermed verifica si la cadena termina con el certificado de CA raíz adecua Después de que la verificación se complete correctamente, el certific del servidor se carga en CiscoWorks Server. Todos los certificados intermedios y el certificado de CA raíz se carga copian en CSM TrustStore. La utilidad muestra un error: • Si los certificados de entrada no están en el formato requerido. • Si la fecha del certificado no es válida o si el certificado ya ha caducado. • Si no se pudo verificar o rastrear el certificado del servidor a un certificado de CA raíz. • Si alguno de los certificados intermedios no se entregó como ent • Si falta la clave privada del servidor o si el certificado del servido se está cargando no se pudo verificar con la clave privada del servidor. Debe ponerse en contacto con la CA que emitió los certificados para corregir estos problemas antes de volver a cargar los certificados en CiscoWorks.
7	Modificar certificado de servicios comunes	Esta opción le permite modificar la entrada Host Name en Common Services Certificate. Puede introducir un nombre de host alternativo si desea cambiar la entrada de nombre de host existente.



Paso 2 Utilice **la opción 1** para obtener una copia del certificado actual y guardarlo para referencia futura.

Paso 3 Detenga el administrador de demonio CSM utilizando este comando en el símbolo del sistema de Windows antes de iniciar el proceso de carga del certificado.

```
net stop crmdmgtd
```

> **Nota**: Los servicios CSM se desactivan mediante este comando. Asegúrese de que no haya implementaciones activas durante este procedimiento.

Paso 4 Abra SSL Utility una vez más. Esta utilidad se puede abrir utilizando el símbolo del sistema. Para ello, vaya a la ruta mencionada anteriormente y utilice este comando.

```
perl SSLUtil.pl
```

Paso 5 Seleccione **la opción 4**. **Verifique la cadena de certificado/certificado introducida.**

Paso 6 Introduzca la ubicación de los certificados (certificado de servidor y certificado intermedio).

> **Nota**: La secuencia de comandos verifica si el certificado del servidor es válido. Una vez finalizada la verificación, la utilidad muestra las opciones. Si el script informa de errores durante la validación y verificación, la utilidad SSL muestra instrucciones para corregirlos. Siga las instrucciones para corregir esos problemas y, a continuación, intente la misma opción una vez más.

Paso 7 Seleccione cualquiera de las dos opciones siguientes.

Seleccione la **opción 5** si sólo hay un certificado para cargar, es decir, si el certificado del servidor está firmado por un certificado de CA raíz.

O

Seleccione la **opción 6** si hay una cadena de certificados para cargar, es decir, si hay un

certificado de servidor y un certificado intermedio.

> **Nota**: CiscoWorks no permite continuar con la carga si no se ha detenido CSM Daemon Manager. La utilidad muestra un mensaje de advertencia si se detectan discrepancias de nombre de host en el certificado del servidor que se está cargando, pero la carga puede continuar.

Paso 8 Introduzca estos detalles obligatorios.

- Ubicación del certificado
- Ubicación de los certificados intermedios, si los hubiere.

SSL Utility carga los certificados si todos los detalles son correctos y los certificados cumplen los requisitos de CSM para los certificados de seguridad.

Paso 9 Reinicie el gestor de demonio CSM para que el nuevo cambio surta efecto y habilite los servicios CSM.

```
net start crmdmgtd
```

> **Nota**: Espere un total de 10 minutos para que se reinicien todos los servicios CSM.

Paso 10 Confirme que el CSM esté utilizando el certificado de identidad instalado.

> **Nota**: No olvide instalar los certificados raíz e intermedio de CA en el PC o servidor desde donde se establece la conexión SSL en el CSM.