CS - Cómo instalar los Certificados de tercera persona SSL para el acceso a GUI

Contenido

Introducción

El Cisco Security Manager (CS) proporciona una opción para utilizar los Certificados de la Seguridad publicados por las autoridades de certificación de tercera persona (CA). Estos Certificados pueden ser utilizados cuando la política organizativa previene de usar los certificados autofirmados CS o requiere los sistemas utilizar un certificado obtenido de CA determinado.

TLS/SSL utiliza estos Certificados para la comunicación entre el servidor CS y el buscador del cliente. Este documento describe los pasos para generar un pedido de firma de certificado (CSR) en el CS y cómo instalar la identidad y raíz CA los Certificados en lo mismo.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- El conocimiento del SSL certifica la arquitectura.
- Conocimiento básico del Cisco Security Manager.

Componentes Utilizados

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

- Versión 4.11 y posterior del Cisco Security Manager.

Creación CSR de la interfaz de usuario

Esta sección describe cómo generar un CSR.

Paso 1. Ejecute el Home Page del Cisco Security Manager y seleccione la **Administración de la administración de servidores > de la Seguridad > del servidor único del server> > la configuración**

del certificado.

Paso 2. Ingrese los valores requeridos para los campos descritos en esta tabla:

Campo	Notas de uso
Nombre del país	Código del país de dos caracteres.
Estado o provincia	Código del estado o de la provincia de dos caracteres o el nombre completo del estado la provincia.
Lugar	Código de ciudad o del pueblo de dos caracteres o el nombre completo de la ciudad pueblo.
Nombre de la organización	Nombre completo de su organización o de una abreviatura.
Nombre de la unidad de la organización	Nombre completo de su departamento o de una abreviatura.
Nombre del servidor	Nombre DNS, dirección IP o nombre de host del ordenador. Ingrese Nombre del servidor con un Domain Name apropiado y resolvable. Esto se vis en su certificado (si uno mismo-está firmado o otro vendedor publicado). El host l 127.0.0.1 no debe ser dado.
Dirección de correo electrónico	Dirección de correo electrónico a la cual el correo tiene que ser enviado.

Paso 3. El tecleo **se aplica** para crear el CSR.

El proceso genera los archivos siguientes:

- server.key — La clave privada del servidor.
- server.crt — El certificado autofirmado del servidor.
- server.pk8 — La clave privada del servidor en el formato PKCS#8.
- server.csr — Archivo del pedido de firma de certificado (CSR).

Note: Ésta es la trayectoria 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

Note: Si el certificado es un certificado autofirmado, después usted no puede modificar esta información.

Carga del certificado de identidad en el servidor CS

Esta sección describe cómo cargar el certificado de identidad proporcionado por CA al servidor CS

Paso 1 Encuentre el script utilitario SSL disponible en esta ubicación

```
NMSROOT\MDC\Apache
```

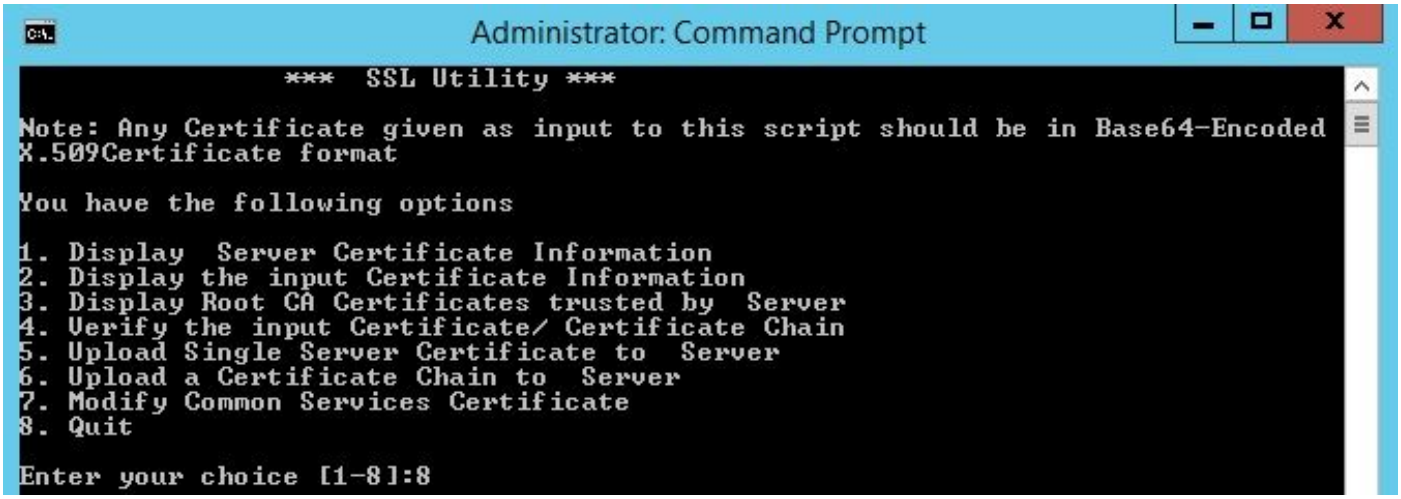
Note: El NMSROOT se debe substituir por el directorio donde el CS está instalado.

Esta utilidad tiene estas opciones.

Número	Opción	Qué lo hace…
1	Información del certificado de servidor de la visualización	• Visualiza los detalles del certificado del servidor CS. Para el otro vendedor publicado los Certificados, esta opción visualiza detalles del certificado de servidor, los Certificados intermedios, eventualmente, y certificado raíz CA.
2	Visualice la información del certificado de la entrada	• Verifica si el certificado es válido. Esta opción valida un certificado como entrada y: • Verifica si el certificado esté en el formato del certificado codificad X.509. • Visualiza el tema del certificado y a los detalles del certificado de publicación. • Verifica si el certificado sea válido en el servidor.
3	Certificados de la visualización raíz CA confiados en por el servidor	Genera una lista de todos raíz CA los Certificados.
4	Verifique el certificado o la Cadena de certificados de la entrada	Verifica si el certificado de servidor publicado por el otro vendedor CA pueda ser cargado. Cuando usted elige esta opción, la utilidad:

		• Verifica si el certificado está en el formato codificado base64 X.509Certificate. • Verifica si el certificado es válido en el servidor • Verifica si el certificado de servidor de la clave privada y de la ent del servidor hace juego. • Verifica si el certificado de servidor se puede localizar al requerid certificado raíz CA usando cuál fue firmado. • Construye la Cadena de certificados, si los encadenamientos intermedios también se dan, y la verifica si el encadenamiento ter con el apropiado certificado raíz CA. Después de que la verificación se complete con éxito, a le indican que cargue los Certificados al servidor CS. La utilidad visualiza un error: • Si los Certificados de la entrada no son formato adentro requerido • Si la fecha del certificado es inválida o si ha expirado el certificado • Si el certificado de servidor no se podría verificar o localizar a certificado raíz CA. • Si es un de los Certificados intermedios no fueron dados como entrada. • Si la clave privada del servidor falta o si el certificado de servidor está siendo cargado no se podría verificar con la clave privada de servidor. Usted debe entrar en contacto CA que publicó los Certificados para co estos problemas antes de que usted cargue los Certificados al CS. Usted debe verificar los Certificados usando la opción 4 antes de que seleccione esta opción. Seleccione esta opción, sólo si no hay Certificados del intermedio y ha solamente el certificado de servidor firmado por un prominente certific raíz CA. Si raíz CA no es uno confiado en por el CS, no seleccione esta opción En estos casos, usted debe obtener certificado raíz CA usado para fir certificado de CA y cargar ambos los Certificados usando la opción 6.
5	Certificado de servidor único de la carga al servidor	Cuando usted selecciona esta opción, y proporciona la ubicación del certificado, la utilidad: • Verifica si el certificado esté en el formato del certificado codificad base64 X.509. • Visualiza el tema del certificado y a los detalles del certificado de publicación. • Verifica si el certificado sea válido en el servidor. • Verifica si el certificado de servidor de la clave privada y de la ent del servidor haga juego. • Verifica si el certificado de servidor se pueda localizar al requerid certificado raíz CA que fue utilizado para firmar. Después de que la verificación se complete con éxito, la utilidad carga certificado a Servidor CiscoWorks. La utilidad visualiza un error: • Si los Certificados de la entrada no son formato adentro requerido • Si la fecha del certificado es inválida o si ha expirado el certificado • Si el certificado de servidor no se podría verificar o localizar a

		certificado raíz CA. • Si la clave privada del servidor falta o si el certificado de servidor está siendo cargado no se podría verificar con la clave privada de servidor. Usted debe entrar en contacto CA que publicó los Certificados para co estos problemas antes de que usted cargue los Certificados en el CS vez. Usted debe verificar los Certificados usando la opción 4 antes de que seleccione esta opción.
6	Cargue una Cadena de certificados al servidor	Seleccione esta opción, si usted está cargando una Cadena de certificados. Si usted es también el cargar certificado raíz CA también usted debe incluirlo como uno de los Certificados en el encadenamien Cuando usted selecciona esta opción y proporciona la ubicación de lo Certificados, la utilidad: • Verifica si el certificado esté en el formato del certificado codificad base64 X.509. • Visualiza el tema del certificado y a los detalles del certificado de publicación. • Verifica si el certificado sea válido en el servidor • Verifica si la clave privada del servidor y el certificado de servidor hagan juego. • Verifica si el certificado de servidor se pueda localizar al certificad CA que fue utilizado para firmar. • Construye la Cadena de certificados, si se dan los encadenamien intermedios y la verifica si el encadenamiento termina con el apro certificado raíz CA. Después de que la verificación se complete con éxito, el certificado de servidor está cargado a Servidor CiscoWorks. Todos los Certificados del intermedio y certificado raíz CA están carga copiados al CS TrustStore. La utilidad visualiza un error: • Si los Certificados de la entrada no son formato adentro requerido • Si la fecha del certificado es inválida o si ha expirado el certificad • Si el certificado de servidor no se podría verificar o localizar a certificado raíz CA. • Si es un de los Certificados intermedios no fueron dados como entrada. • Si la clave privada del servidor falta o si el certificado de servidor está siendo cargado no se podría verificar con la clave privada de servidor. Usted debe entrar en contacto CA que publicó los Certificados para co estos problemas antes de que usted cargue los Certificados en los CiscoWorks otra vez.
7	Modifique el certificado común de los servicios	Esta opción permite que usted modifique la entrada de nombre del ho el certificado común de los servicios. Usted puede ingresar un nombre de host alterno si usted desea camb entrada de nombre del host existente.



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

Paso 3 Pare al administrador de Daemon CS que usa este comando en el comando prompt de Windows antes de comenzar el proceso de la carga del certificado.

```
net stop crmdmgtd
```

> **Note**: Los servicios CS van abajo de usar este comando. Aseegurese allí no son ningún active de las implementaciones durante este procedimiento.

Paso 4 Abra la utilidad SSL una vez más. Esta utilidad se puede abrir usando el comando prompt navegando a la trayectoria previamente mencionada y usando este comando.

```
perl SSLUtil.pl
```

Paso 5 La opción selecta **4. verifica la Cadena de certificados del certificado de la entrada.**

Paso 6 Ingrese la ubicación de los Certificados (certificado de servidor y certificado del intermedio).

> **Note**: El script verifica si el certificado de servidor es válido. Después de que la verificación sea completa, la utilidad visualiza las opciones. Si los errores de los informes del script durante la validación y la verificación, los mandos de visualizaciones utilitarios SSL de corregir estos errores. Siga las instrucciones de corregir esos problemas y después de intentar el mismo opción uno más tiempo.

Paso 7 Seleccione las después dos opciones unas de los.

Seleccione la **opción 5** si hay solamente un certificado a cargar, eso es si el certificado de servidor es firmado por a certificado raíz CA.

O

Seleccione la **opción 6** si hay una Cadena de certificados a cargar, eso es si hay un certificado de

servidor y un certificado del intermedio.

> **Note**: Los CiscoWorks no permiten proceder con la carga si no han parado al administrador de Daemon CS. La utilidad visualiza un mensaje de advertencia si hay discordancías del nombre de host detectadas en el certificado de servidor que es cargado, pero la carga puede ser continuada.

Paso 8 Ingrese estos detalles requeridos.

- Ubicación del certificado
- Ubicación de los Certificados intermedios, si los hay.

La utilidad SSL carga los Certificados si todos los detalles están correctos y los Certificados cumplen los requisitos CS para los Certificados de la Seguridad.

Paso 9 Recomience al administrador de Daemon CS para que el nuevo cambio tome el efecto y habilite los servicios CS.

```
net start crmdmgtd
```

> **Note**: Aguarde para un guardapolvo de 10 minutos para que todos los servicios CS sean recomenzados.

Paso 10 Confirme el CS está utilizando el certificado de identidad instalado.

> **Note**: No olvide instalar los Certificados de CA de la raíz y del intermedio en el PC o el servidor de donde la conexión SSL stablished al CS.