

Cómo instalar un certificado encadenado SSL al módulo CSS SSL

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Instrucciones Paso a Paso](#)

[Información Relacionada](#)

[Introducción](#)

Una Cadena de certificados es una secuencia de Certificados, donde cada certificado en el encadenamiento es firmado por el certificado subsiguiente. El propósito de la Cadena de certificados es establecer un encadenamiento de la confianza de un certificado de peer a un certificado de la autoridad confiable de certificación (CA). CA atestigua para la identidad en el certificado de peer firmándolo. Si CA es uno que usted confía en (indicado por la presencia de una copia del certificado de CA en su directorio del certificado raíz), éste le implica puede confiar en el certificado de peer firmado también.

A menudo, los clientes no validan los Certificados porque CA conocido los no crearon. Del cliente los estados típicamente que la validez del certificado no puede ser verificada. Éste es el caso cuando el certificado es firmado por CA intermedio, que no se sabe al buscador del cliente. En estos casos, es necesario utilizar un certificado SSL o un grupo encadenado del certificado. Este documento discute cómo instalar correctamente un certificado encadenado del Secure Socket Layer (SSL) a un módulo CSS SSL.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Módulo SSL CSS11506 (encriptación fuerte) - CSS 506-SSL-K9
- Módulo SSL CSS11501 (encriptación fuerte) - CSS 501-SSL-K9
- Solamente módulo del switch CSS11506 - CSS 506-SM

- WebNS 7.10 y 7.20

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

[Instrucciones Paso a Paso](#)

Esta sección muestra cómo instalar un certificado encadenado en el módulo CSS SSL con el CSS11500.

Si el certificado encadenado está en los Archivos múltiples, utilice el procedimiento delineado abajo.

1. Convierta todos los Certificados al mismo formato. Si los Certificados son separados y no en el formato de Privacy Enhanced Mail (PEM), usted necesita convertirlos al formato PEM y después concatenarlos.
2. Concatene todos los Certificados en un archivo; asegúrese de que estén concatenados mientras que aparecen en el encadenamiento. El certificado de servidor debe ser primer en el encadenamiento, seguido por los intermedios (los certificados de servidor y Certificados de CA intermedios).
3. Importe el archivo de certificado concatenado en el CSS.
4. Asocie el certificado al servidor del SSL.
5. Aplique CA del servidor del SSL dentro de la lista SSL del proxy.

Si todos estos Certificados se encadenan en un archivo del PKCS-12 (tanto de los Certificados del PKCS-12 sea), usted debe importar el certificado encadenado como PKCS-12, y el socio/lo aplica como normal. El PKCS-12 no es capaz de la concatenación.

Nota: Los formatos distinguidos de la regla de la codificación (DER) no soportan los encadenamientos, así que esto no debe ser un problema.

Para verificar, la clave que necesita ser utilizada es la clave que generó el archivo del pedido de firma de certificado (CSR) para crear el certificado de servidor. Hay solamente una clave para un certificado, sea encadenado o asiduo. Asegúrese verificar el certificado y la clave después de que se importen. Usted puede publicar el comando mostrado abajo.

```
(config)# ssl verify myrsacert1 myrsakey1 Certificate and key match
```

[Información Relacionada](#)

- [Guía de configuración avanzada CSS](#)
- [Asegure/ID de instalación del servidor del sitio del comercio favorable - Acelerador de comercio electrónico de Intel NetStructure 7110](#)
- [Soporte de productos del Application Networking Services](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)