

Edite las configuraciones de la autenticación de servidor de Secure Sockets Layer (SSL) en los switches para pila de las Sx500 Series

Objetivo

Secure Sockets Layer (SSL) es un protocolo usado principalmente para la Administración de seguridad en Internet. Utiliza una capa del programa que esté situada entre el HTTP y las capas TCP. Para la autenticación, el SSL utiliza los Certificados que se firman digitalmente y se limitan a la clave pública para identificar al propietario de la clave privada. Esta autenticación ayuda durante la época de la conexión. Con el uso del SSL, los Certificados se intercambian en los bloques durante el proceso de autenticación que están en el formato descrito en ITU-T X.509 estándar. Entonces por las autoridades de certificación que es una autoridad externa, se publican los Certificados X.509 se firman digitalmente que.

Este artículo explica cómo editar las configuraciones de la autenticación de servidor SSL y cómo generar un pedido de certificado en los switches para pila de las Sx500 Series.

Dispositivos aplicables

- Switches para pila de las Sx500 Series

Versión del software

- 1.3.0.62

Configuraciones de la autenticación de servidor SSL

Paso 1. Inicie sesión a la utilidad de configuración del switch y elija las **configuraciones de la Seguridad > del servidor SSL > de la autenticación de servidor SSL**. *La página Configuración de la autenticación de servidor SSL se abre:*

Note: Siga la [información fundamental del editar SSL](#) para generar el certificado automáticamente, [genere el pedido de certificado](#) de regenerar el pedido de certificado por

el Switch y [Import Certificate \(Importar certificado\)](#) de importar su certificado deseado y la clave.

[Edite la información fundamental SSL](#)

Paso 2. Marque la casilla de verificación del certificado activo que usted desea editar en la tabla de la clave del servidor SSL.

Paso 3. El tecleo **edita** para realizar los cambios al certificado existente. La ventana del *certificado del editar* aparece:

Note: En este ejemplo, se marca el certificado 1.

Certificate ID: 1 2

Regenerate RSA Key:

Key Length: Use Default User Defined (Range: 512 - 2048, Default: 1024)

Common Name: (13/64 Characters Used, Default: 0.1.134.160)

Organization Unit: (10/64 Characters Used)

Organization Name: (10/64 Characters Used)

Location: (10/64 Characters Used)

State: (7/64 Characters Used)

Country: ASCII Alphanumeric

Duration: (Range: 30 - 3650 Days)

Paso 4. En el campo del certificado ID, elija 1 o 2 como el ID del certificado. Hay solamente 2 opciones disponibles en el campo del certificado ID en esta configuración.

Paso 5. Marque la casilla de verificación en el campo clave regenerado RSA para regenerar la clave RSA.

Paso 6. En el campo de la longitud de clave, haga clic cualquiera uno de los botones de radio.

- Valor por defecto del uso — Se utiliza la longitud de clave predeterminada.
- Definido por el usuario — En este campo, la longitud de clave puede tener el valor a partir del 512 a 2048. El valor predeterminado es 1024. En este ejemplo, se ingresa 2000.

Paso 7. En el campo del Common Name, ingrese el dispositivo calificado completamente URL o al IP Address público determinado. Si está ido espacio en blanco, omita la dirección IP más baja del dispositivo (cuando se genera el certificado). En este ejemplo, utilizan a la dirección predeterminada del Switch SG500X como Common Name.

Paso 8. En el campo de la unidad de la organización, ingrese el nombre de la organización-unidad o del departamento.

Paso 9. En el campo de nombre de la organización, ingrese el nombre de la organización.

Paso 10. En el campo de la ubicación, ingrese el nombre de la ubicación o de la ciudad.

Paso 11. En el campo de estado, ingrese el nombre del estado o de la provincia.

Paso 12. En el campo del país, ingrese el nombre del país. Como esto valida solamente el valor alfanumérico, utilice el formato global de 2 cartas. Por ejemplo, porque los Estados Unidos ingrese los E.E.U.U.

Paso 13. En el campo de la duración, ingrese el número de días que una certificación es válida.

Paso 14. El tecleo **genera** para salvar las configuraciones.

Genere un pedido de certificado

Paso 1. En la *página Configuración de la autenticación de servidor SSL*, marque el certificado ID y el tecleo **generan el pedido de certificado**.

Paso 2. El tecleo **genera el pedido de certificado** en la *página Configuración de la autenticación de servidor SSL del editar*.

Ahora en el campo del pedido de certificado, usted puede ver la información cifrada del certificado.

Paso 3. El tecleo **genera el pedido de certificado** de salvar las configuraciones.

Ahora en las *configuraciones* página de la *autenticación de servidor SSL*, usted puede ver el certificado editado con toda la información arriba ingresada.

- Válido de — Especifica la fecha de la cual el certificado es válido.
- Válido a — Especifica la fecha hasta la cual el certificado es válido.
- Fuente del certificado — Especifica si el certificado fue generado por el sistema (auto generado) o el usuario (definido por el usuario).

[Import Certificate \(Importar certificado\)](#)

Paso 1. Haga clic deseó la casilla de verificación y hacen clic **Import Certificate (Importar certificado)** para importar un certificado.

- Certificado ID — Elija el certificado activo
- Certificado — La copia o pega el certificado al configurado.
- Par clave de la importación RSS — Elija habilitar el par clave RSA.
- Clave pública (cifrada) — La copia o pega la clave pública en una forma encriptada.
- Clave privada (texto simple) — La copia o pega la clave privada en la forma de sólo texto.
- Datos vulnerables de la visualización como cifrado — Elija esta opción que usted necesita las claves privadas ser escrito en la forma encriptada al archivo de configuración.

Paso 2. El tecleo **se aplica**.

El teclado (opcional) del paso 3. el certificado deseado ID y los **detalles del** teclado para ver los detalles del SSL detalla.

El teclado (opcional) del paso 4. el certificado deseado ID y el teclado **borran** para borrar a los detalles del servidor SSL de la tabla del servidor SSL.