

Editar los parámetros de autenticación del servidor de capa de sockets seguros (SSL) en los switches apilables de la serie Sx500

Objetivo

Secure Sockets Layer (SSL) es un protocolo utilizado principalmente para la gestión de la seguridad en Internet. Utiliza una capa de programa que se encuentra entre las capas HTTP y TCP. Para la autenticación, SSL utiliza certificados firmados digitalmente y enlazados a la clave pública para identificar el propietario de la clave privada. Esta autenticación ayuda durante el tiempo de conexión. Mediante el uso de SSL, los certificados se intercambian en bloques durante el proceso de autenticación, que tienen el formato descrito en la norma ITU-T X.509. A continuación, la autoridad certificadora que es una autoridad externa emite certificados X.509 que se firman digitalmente.

En este artículo se explica cómo editar la configuración de autenticación del servidor SSL y cómo generar una solicitud de certificado en los switches apilables de la serie Sx500.

Dispositivos aplicables

Switches apilables · Sx500 Series

Versión del software

•1.3.0.62

Configuración de autenticación del servidor SSL

Paso 1. Inicie sesión en Switch Configuration Utility y elija **Security > SSL Server > SSL Server Authentication Settings**. Se abre la página *SSL Server Authentication Settings*:

<input type="checkbox"/>	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
<input type="checkbox"/>	1	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Nota: Siga el comando [Edit SSL Key Information](#) para generar el certificado automáticamente, [Generate Certificate Request](#) para volver a generar la solicitud de certificado por el switch y [Import Certificate](#) para importar el certificado deseado y la clave.

[Editar información de clave SSL](#)

SSL Server Authentication Settings

SSL Active Certificate Number: 1
 2

SSL Server Key Table

<input type="checkbox"/>	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
<input checked="" type="checkbox"/>	1	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Paso 2. Active la casilla de verificación del certificado activo que desea editar en la tabla de claves de servidor SSL.

SSL Server Authentication Settings

SSL Active Certificate Number: 1
 2

SSL Server Key Table

<input type="checkbox"/>	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
<input checked="" type="checkbox"/>	1	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Paso 3. Haga clic en **Editar** para realizar los cambios en el certificado existente. Aparece la ventana *Editar certificado*:

Nota: 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 ID de certificado, elija 1 o 2 como ID del certificado. Sólo hay 2 opciones disponibles en el campo ID de certificado en esta configuración.

Paso 5. Active la casilla de verificación en el campo Regenerar clave RSA para regenerar la clave RSA.

Paso 6. En el campo Key Length (Longitud de la clave), haga clic en uno de los botones de opción.

·Usar valor predeterminado: se utiliza la longitud de clave predeterminada.

·definido por el usuario: en este campo, la longitud de la clave puede tener el valor de 512 a 2048. El valor predeterminado es 1024. En este ejemplo, se ingresa 2000.

Paso 7. En el campo Nombre común, introduzca la URL del dispositivo completa o una dirección IP pública determinada. Si se deja en blanco, el valor predeterminado es la dirección IP más baja del dispositivo (cuando se genera el certificado). En este ejemplo, la dirección predeterminada del switch SG500X se utiliza como nombre común.

Paso 8. En el campo Unidad de organización, introduzca el nombre de la unidad de organización o departamento.

Paso 9. En el campo Organization Name (Nombre de la organización), introduzca el nombre de la organización.

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

Paso 11. En el campo Estado, introduzca el nombre del estado o provincia.

Paso 12. En el campo País, introduzca el nombre del país. Dado que sólo acepta un valor alfanumérico, utilice el formato global de dos letras. Por ejemplo, para Estados Unidos, introduzca Estados Unidos.

Paso 13. En el campo Duración, introduzca el número de días que una certificación es válida.

Paso 14. Haga clic en **Generar** para guardar la configuración.

SSL Server Authentication Settings

SSL Active Certificate Number: 1 2

Apply Cancel

SSL Server Key Table

<input type="checkbox"/>	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
<input checked="" type="checkbox"/>	1	192.168.1.254	Org_Unit_1	Org_Name_1	Location_1	State_1	C1	2012-Jun-11	2013-Jun-11	User Defined
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Edit... Generate Certificate Request... Import Certificate... Details... Delete

[Generar una solicitud de certificado](#)

SSL Server Authentication Settings

SSL Active Certificate Number: 1 2

Apply Cancel

SSL Server Key Table

<input type="checkbox"/>	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
<input checked="" type="checkbox"/>	1	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Edit... Generate Certificate Request... Import Certificate... Details... Delete

Paso 1. En la página *SSL Server Authentication Settings*, verifique el ID del certificado y haga clic en **Generate Certificate Request**.

Enter the data below and generate certificate.

Certificate ID: 1
 2

✱ Common Name: (0/64 Characters Used, Default: 0.1.134.160)

Organization Unit: (0/64 Characters Used)

Organization Name: (0/64 Characters Used)

Location: (0/64 Characters Used)

State: (0/64 Characters Used)

Country: ASCII Alphanumeric

Certificate Request:

Generate Certificate Request

Paso 2. Haga clic en **Generar solicitud de certificado** en la página *Editar configuración de autenticación del servidor SSL*.

Enter the data below and generate certificate.

Certificate ID: 1
 2

✱ Common Name: (0/64 Characters Used, Default: 0.1.134.160)

Organization Unit: (0/64 Characters Used)

Organization Name: (0/64 Characters Used)

Location: (0/64 Characters Used)

State: (0/64 Characters Used)

Country: ASCII Alphanumeric

Certificate Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAzwCAQAwdjELMAkGA1UEBhMCQzExEDAOBgNVBAgUB1N0YXRlXzExEzARBgNVBAc
UCkxY2F0aW9uXzExFjAUBGNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW11
XzExEzARBgNVBAsUCk9yZ19Vbml0XzEwggEbMA0GCsqGSIb3DQEBAQUAA4IBCAAwggEDAoH
7AL5ep54S5M7LHRLhNmpXmtuxWw070Ehfl2cNTfH1RgfCFes2zy8xUialNCKSoS/HapX3ry2gJZ
CtjFHmwEUjpUrYvHxqF9misXODEacranB1iSx4AMKMLy6ed+8tBN5xanhiUqplrXN1w81pEXHRf
/TtiivdifTW2GRmW/sw7e8+GCA0RU
/oRjDpRu1mi3R6z1PU4cK3UMWVzH1hQ5BG+IR+Ju8jOrMseRqjKRROZQz+aHHBPVkwdfly51q
Cuk2R55lsbu2l6Fi7FQ5CY7jw4vj+pO2ZL0uz9q8qsDFxi
-----
```

Ahora, en el campo Solicitud de certificado, puede ver la información de certificado cifrada.

Paso 3. Haga clic en **Generar solicitud de certificado** para guardar la configuración.

SSL Server Authentication Settings

SSL Active Certificate Number: 1
 2

Apply Cancel

SSL Server Key Table

<input type="checkbox"/>	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
<input checked="" type="checkbox"/>	1	192.168.1.254	Org_Unit_1	Org_Name_1	Location_1	State_1	C1	2012-Jun-11	2013-Jun-11	User Defined
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Edit... Generate Certificate Request... Import Certificate... Details... Delete

Ahora en la página *SSL Server Authentication Settings*, puede ver el certificado editado con toda la información introducida anteriormente.

·Válido desde: especifica la fecha a partir de la cual el certificado es válido.

·Válido para: especifica la fecha hasta la que el certificado es válido.

Origen de certificado :: especifica si el certificado fue generado por el sistema (Generado automáticamente) o el usuario (Definido por el usuario).

Importar certificado

SSL Server Authentication Settings

SSL Active Certificate Number: 1
 2

Apply Cancel

SSL Server Key Table

<input type="checkbox"/>	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
<input checked="" type="checkbox"/>	1	192.168.1.254	Org_Unit_1	Org_Name_1	Location_1	State_1	C1	2012-Jun-11	2013-Jun-11	User Defined
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Edit... Generate Certificate Request... **Import Certificate...** Details... Delete

Paso 1. Haga clic en la casilla de verificación deseada y haga clic en **Importar certificado** para importar un certificado.

When a Certificate and/or a Key is entered, it should contain the "BEGIN" and "END" markers.

Certificate ID: 1 2

Certificate Source: User Defined

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDYTCCAIACEFGqVx5pfJlrr9M+uUyA5UwDQYJKoZIhvcNAQEEBQAwdjELMAkG
A1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAcJCKxvY2F0aW9uXzEx
FjAUBgNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW1lXzExEzAR
BgNVBAsUCk9yZ19Vbml0XzEwHhcNMTEwNjExMTg0NTQ5WWhcNMTEwNjExMTg0NTQ5
WjB2MzQwCQYDVGQGEWJDMTEQMA4GA1UECBQU3RhdGVfMTETMBEGA1UEBxQKTG9j
YXRpb25fMTEwMzQwCQYDVGQGEWJDMTEQMA4GA1UECBBG9yZ190YW1lXzExEzAR
-----END CERTIFICATE-----
```

Import RSA Key-Pair: Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBAwKB+wDFB1ToNF0tnPghLIT2/ZqP9OKVUu6p5GhEBbcOKfjAvrNy6DS4cSIQldqM6JG+G7klm9LupeFIOAc
If9FTfpf5IetemQ9FEj0RZZxfyD5qfdPsmjbaSAGzIXW4ZkWezYtfi33r5e5W3X328lkf2IutUyz3VUCdUKrBmLIPpTMO
zXjhlLink1bIEFVSN50fPhVSp0fX+UTTpGww3n1VJ1Ct80bje+tr/MYO+Gx7DnZTrhEpcocptsZ81z6ubb4wY4xAtPnD
/4DWFQkdDwfQetFut32hGu2SakWzAVLVLhgQHnSNmCuFnVUX0OYW0wBwvt3RKJi85RtkarjFAGMBAAE=
-----END RSA PUBLIC KEY-----
```

Private Key: Encrypted Plaintext

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
SOxOUPh1Gq1Fc39s+49gkYuCnOuDQHGeTf6yM5yulSj5Et4163XgSBARH2CVOcZOLngik+fG9UtvbxIQJq1SI
I+NjjsMv0HiZyV/DacVsXM2N3kPHELfBNhkwZuA9RL0pIRPNa73pW2BzQ6vWNjudUBMEL6b6pc3I4CNVCrwt
HSNvOo9IA7ZZEHG/TEzNFdE+GShszuzbpTwtD6a4iQVB01BQGh8rMp0u/pL3e9pSayV3+60YYgXNPho
/XWaEH1udzHqQAG1lrW+A
/s8iq2Hsg9+6g6uFJgew2Yh2z7Ls64EMte104wJkbLJrwXJWhJirwCyC2PtSnU4dityfC71H7V4V8P0rKavdq1OH
Tu0HXiV9MeEgv3/cp6ptdVyzjzm3vbOQbQ62Ywd5S4rRxgeAdumWs/drOHfeogIwqKNqOfvdk03Xk779H8
-----END RSA ENCRYPTED PRIVATE KEY-----
```

Apply Close Display Sensitive Data As Plaintext

ID del certificado : elija el certificado activo

Certificado : copie o pegue el certificado en un archivo configurado.

·Importar par de claves RSS: elija habilitar el par de claves RSA.

Clave pública · (cifrada): copie o pegue la clave pública en un formulario cifrado.

Clave privada · (texto sin formato): copie o pegue la clave privada en texto sin formato.

·Mostrar datos confidenciales como cifrados: elija esta opción para que las claves privadas se escriban de forma cifrada en el archivo de configuración.

Paso 2. Haga clic en Apply (Aplicar).

SSL Server Authentication Settings

SSL Active Certificate Number: 1 2

Apply Cancel

Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source	
<input checked="" type="checkbox"/>	1	192.168.1.254	Org_Unit_1	Org_Name_1	Location_1	State_1	C1	2012-Jun-11	2013-Jun-11	User Defined
<input type="checkbox"/>	2	0.0.0.0					2012-Jun-11	2013-Jun-11	Auto Generated	

Edit... Generate Certificate Request... Import Certificate... Details... Delete

Paso 3. (Opcional) Haga clic en la ID de certificado deseada y haga clic en **Detalles** para ver los detalles de SSL.

The screenshot shows a window with the following fields and content:

- Certificate ID:** 1
- Certificate:**-----BEGIN CERTIFICATE-----
MIIDYTCCAIAACEFgqVx5pfPjlr9M+uUyA5UwDQYJKoZIhvdNAQEEBQAwdjELMAkG
A1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAcJUCxvY2F0aW9uXzEx
FjAUBgNVBAMTDE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW1lXzExEzAR
BgNVBAsUCk9yZ19Vbml0XzEwHhcNMTEwNjExMTg0NTQ5WkdMTMwNjExMTg0NTQ5
WjB2MQswCQYDVQGEwJDMTEQMA4GA1UECBHU3RhdGVfMTETMBEGA1UEBxQKTG9j
YXRpb25fMTEWMBQGA1UEAxMNMTkyLjE2OC4xLjI1NDETMDEGA1UEChQKT3JnX05h
- Public Key:**-----BEGIN RSA PUBLIC KEY-----
MIIBAwKB+wDFB1ToNF0tnPghLIT2/ZqP9OKVUu6p5GhEBbcOKfjAvrNy6DS4cSIQIdqM8JG+G7kIm9LupeFIOAc
lf9FTfpf5IetemQ9FEj0RZZxfyD5qfdPsmjbaSAGzIXW4ZkWezYtfi33r5e5W3X328lkfI2IutUyz3VUCdUKrBmLIPpTM0
zXjhLirk1bfEFVSNS0fPhVSp0fX+UTTpGww3n1VJ1Ct80bje+r/M/YO+Gx7DnZTrhEpcapsZ81z6ubb4wY4xAtPnD
/4DWFQkdDwfQetFut32hGu2SakWzAVLVLhgQHnSNmCuFnVUX0OYW0wBvwt3RKJi85RtkarjFagMBAAE=
-----END RSA PUBLIC KEY-----
- Fingerprint(Hex):** B2:BA:C6:EB:E5:FE:DE:83:46:58:EC:87:77:7F:B5:8F:EE:A5:90:55
- Private Key (Encrypted):**-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
SOxOUPh1Gq1Fc39s+49gkYuCnOuDuDQHGeTf6yM5yulSj5Et4163XgSBRARH2CVOoZOLngik+fG9UtvbxiOJq11SI
I+NjffsMv0HiZyV/DacVsXM2N3kPHELFBNhkwZuA9RL0pIRPNa73pW2BzQ6vWNjudUBMEL6b6pc3I4CNVCrwt
HSNvOo9IA7ZZEHG/TEzNFdE+GShszuzbpTWtD6a4iQVB01BQGh8rMp0u/pL3e9pSayV3+60YYgXNPho
/XWaeEH1udzHqQAG1IrW+A
/s8iq2Hsg9+8g8uFJgew2Yh2z7Ls64EMte104wJkbLjrwXJWhJirwCyC2PtSnU4dityfC71H7V4V8POrKavdq1OH
Tu0HXiV9MeEgv3/cp8ptdVyzjm3vbOQbQ62Yvwd5S4rRxgeAdumWs/drOHfeogIwqKNqOfvdk03XKk779H8

At the bottom of the window, there are two buttons: **Close** and **Display Sensitive Data As Plaintext**.

Paso 4. (Opcional) Haga clic en el ID de certificado deseado y haga clic en **Eliminar** para eliminar los detalles del servidor SSL de la tabla de servidor SSL.