

Edit Secure Sockets Layer (SSL) Server Authentication Settings on Sx500 Series Stackable Switches

Objective

The Secure Sockets Layer (SSL) is a protocol used mainly for security management on the Internet. It uses a program layer which is located between the HTTP and the TCP layers. For authentication, SSL uses certificates which are digitally signed and bounded to the public key to identify the private key owner. This authentication helps during the time of connection. Through the use of SSL, the certificates are exchanged in blocks during the authentication process which are in the format described in ITU-T standard X.509. Then by the certification authority which is an external authority, X.509 certificates are issued which are digitally signed.

This article explains how to edit SSL server authentication settings and how to generate a certificate request on the Sx500 Series Stackable Switches.

Applicable Devices

- Sx500 Series Stackable Switches

Software Version

- 1.3.0.62

SSL Server Authentication Settings

Step 1. Log in to the Switch Configuration Utility and choose **Security > SSL Server > SSL Server Authentication Settings**. The *SSL Server Authentication Settings* page opens:

Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
1	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated
2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Note: Follow the [Edit SSL Key Information](#) to generate the certificate automatically, [Generate Certificate Request](#) to re-generate the certificate request by the switch and [Import Certificate](#) to import your desired certificate and the key.

[Edit SSL Key Information](#)

SSL Server Authentication Settings

SSL Active Certificate Number: ☒ 1
☐ 2

<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

Step 2. Check the check box of the active certificate you wish to edit in the SSL Server Key Table.

SSL Server Authentication Settings

SSL Active Certificate Number: ☒ 1
☐ 2

<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

Step 3. Click **Edit** to make the changes to the existing certificate. The *Edit Certificate* window appears:

Note: In this example, certificate 1 is checked.

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)

Step 4. In the Certificate ID field, choose either 1 or 2 as the ID of the certificate. There are only 2 options available in the Certificate ID field in this configuration.

Step 5. Check the check box in the Regenerate RSA Key field to regenerate the RSA key.

Step 6. In the Key Length field, click either one of the radio buttons.

- Use Default — The default key length is used.

- User Defined — In this field, the key length can have the value from 512 to 2048. The default value is 1024. In this example, 2000 is entered.

Step 7. In the Common Name field, enter the fully-qualified device URL or particular public IP address. If left blank, it defaults to the lowest IP address of the device (when the certificate is generated). In this example, the default address of the SG500X switch is used as common name.

Step 8. In the Organization Unit field, enter the name of the organization-unit or department.

Step 9. In the Organization Name field, enter the name of the organization.

Step 10. In the Location field, enter the name of the location or city.

Step 11. In the State field, enter the name of the state or province.

Step 12. In the Country field, enter the name of the country. As this accepts only alphanumeric value, use the global 2 letter format. For example, for the United States enter US.

Step 13. In the Duration field, enter the number of days a certification is valid.

Step 14. Click **Generate** to save the settings.

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

Generate a Certificate Request

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	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

Step 1. In the *SSL Server Authentication Settings* page, check the certificate ID and click **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

Step 2. Click **Generate Certificate Request** in the *Edit SSL Server Authentication Settings* page.

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-----
MIICrTCCAzwCAQAwZjELMAkGA1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAc
UCkxY2F0aW9uXzExFjAUBGNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW1l
XzExEzARBgNVBAUUCk9yZ19Vbml0XzEwggEbmA0GCSqGSIb3DQEBAQUAA4IBCAAwggEDAoH
7AL5ep54S5M7LHRLhNmpXmtuxWw070Ehfl2cNTfH1RgfCfEs2zy8xUialNCKSoS/HapX3ry2gJZ
CtjFHMwEUjpUrYvHxqF9misXODEacranB1iSx4AMKmLy6ed+8tBN5xanhiUqplrXN1w81pEXHRf
/TtiVdiTW2GRmW/sw7e8+GCA0RU
/oRjDpRu1mi3R6z1PU4cK3UMWVzH1hQ5BG+IR+Ju8jOrMseRqjKRROZQz+aHHBPV/kwdfly51q
Cuk2R55Isbu2l6FI7FQ5CY7jw4vj+pO2ZL0uz9q8qsDFxi
-----
```

Now in the Certificate Request field, you can see the encrypted certificate information.

Step 3. Click **Generate Certificate Request** to save the settings.

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

Now in the *SSL Server Authentication Settings* page, you can see the edited certificate with all the above entered information.

- Valid From — Specifies the date from which the certificate is valid.
- Valid To — Specifies the date up to which the certificate is valid.
- Certificate Source — Specifies whether the certificate was generated by the system (Auto Generated) or the user (User Defined).

Import Certificate

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

Step 1. Click desired check box and click **Import Certificate** to import a certificate.

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-----
MIIDYTCCAIACEGqVx5pfJlr9M+uUyA5UwDQYJKoZIhvdNAQEEDQAwjdJELMAkG
A1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAcJClxvY2F0aW9uXzEx
FjAUBgNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YXV1IXzExEzAR
BgNVBAsUCk9yZ19Vbml0XzExEwHdNMTIwNjExMTg0NTQ5WkdNMTMwNjExMTg0NTQ5
WjB2MQswCQYDVQQGEwJDMTEQMA4GA1UECBHU3RhdGVfMTETMBEGA1UEBxQKTG9j
YXRpb25fMTETMBEGA1UEAxMNMTkyLjE2OC4xLjI1NDETMBEGA1UEChQKT3JnX05h
-----END CERTIFICATE-----
```

Import RSA Key-Pair: ☐ Enable

★ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBAwKB+wDFB1ToNF0tnPghLIT2ZqP9OKVUu6p5GhEBbcOKfjAVrNy6DS4cSIQldqM8JG+G7klm9LupeFIOAc
If9FTfp5IetemQ9FEj0RZZxfyD5qfdPsmjbaSAGzIXW4ZkWezYtfi33r5e5W3X328lkf2IutUyz3VUCdUkRmLIPpTMQ
zXjhLrk1bfEFVSNS0fPhVSp0fX+UTTPGvw3n1VJ1Ct80bje+rr/M/YO+Gx7DnZTrhEpcqptsZ81z6ubb4wY4xAtPnD
/4DWFQkdDwfQetFut32hGu2SakWzAVLVLhgQHnSNmCuFnVUX0OYW0wBwt3RKJi85RtkarjFAgMBAAE=
-----END RSA PUBLIC KEY-----
```

★ Private Key: ☒ Encrypted ☐ Plaintext

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
SOxOUPh1Gq1Fc39s+49gkYuCnOuDQHGeTf6yM5yulSj5Et4163XgSBARH2CVOcZOLngik+fG9UtvbxlOJq1SI
I+NjfsMv0HiZyV/DacVsXM2N3kPHELFBNhkwZuA9RL0pIRPNa73pW2BzQ6vWNjudUBMEL6b6pc3I4CNVCrwt
HSNvOo9IA7ZZEHG/T EzNFdE+GShszuzbpTWtD6a4iQVB01BQGh8rMp0u/pL3e9pSayV3+60YYgXNPho
/XWaeEH1udzHqQAG1IrW+A
/s8iq2Hsg9+6g6uFJgew2Yh2z7Ls64EMte104wJkbLJrwXJWhJinwCyC2PtSnU4dityfC71H7V4V8P0rKavdq1OH
Tu0HXIV9MeEgv3/cp6ptdVyzjzm3vbOQbQ62Ywmd5S4rRxgeAdumWs/drOHfeogIWqKNqOfvdk03XKq779H8
-----END RSA ENCRYPTED PRIVATE KEY-----
```

Apply Close Display Sensitive Data As Plaintext

- Certificate ID — Choose the active certificate
- Certificate — Copy or paste the certificate to a configured.
- Import RSS KEY-Pair — Choose to enable the RSA key pair.
- Public Key (Encrypted) — Copy or paste the public key in an encrypted form.
- Private Key (Plaintext) — Copy or paste the private key in plain text form.
- Display Sensitive Data as Encrypted — Choose this option you need the private keys to be written in encrypted form to the configuration file.

Step 2. Click **Apply**.

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

Step 3. (Optional) Click the desired certificate ID and click **Details** to view details of the SSL details.

Certificate ID:	1
Certificate:	<pre>-----BEGIN CERTIFICATE----- MIIDYTCCAIACEFGqVx5pfJlrr9M+uUyA5UwDQYJKoZIhvcNAQEEBQAwdjELMAkG A1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAcUJG9wY2F0aW9uXzEx FjAUBGNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW1lXzExEzAR BgNVBAsUCk9yZ19Vbml0XzEwHhcNMTEwNjExMTg0NTQ5WkdNMTMwNjExMTg0NTQ5 WjB2MQswCQYDVQGEwJDMTEQMA4GA1UECBQU3RhdGVfMTETMBEGA1UEBxQKTG9j YXRpb25fMTETMBQGA1UEAxMNMTkyLjE2OC4xLjI1NDETMBEGA1UEChQKT3JnX05h -----</pre>
Public Key:	<pre>-----BEGIN RSA PUBLIC KEY----- MIIBAwKB+wDFB1ToNF0tnPghLIT2/ZqP9OKVUu6p5GhEBbcOKfjAvrNy6DS4cSIQIdqM6JG+G7kIm9LupeFIOAc If9FTfpf5IetemQ9FEj0RZZxfyD5qfdPsmjbaSAGzIXW4ZkWezYtfi33r5e5W3X328lkfI2IutUyz3VUCdUKrBmLIPpTM0 zXjhLink1bEFVSNs0fPhVSp0fX+UTTpgWw3n1VJ1Ct80bje+r/M/YO+Gx7DnZTrhEpcptsZ81z8ubb4wY4xAtPnD /4DWFQkdDwfQetFut32hGu2SakWzAVLVLhgQHnSNmCuFnVUX0OYW0wBvwt3RKJi85RtkarjFAgMBAAE= -----END RSA PUBLIC KEY-----</pre>
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):	<pre>-----BEGIN RSA ENCRYPTED PRIVATE KEY----- SOxOUPh1Gq1Fc39s+49gkYuCnOuDQHGeTf6yM5yulSj5Et4163XgSBAH2CVOocZOLngik+fG9UtvbxdIOJq11SI I+NjffsMv0HiZyV/DacVsXM2N3kPHELFBNhkwZuA9RL0pIRPNs73pW2BzQ6vWNjudUBMEL6b6pc3I4CNVCnwt HSNvOo9IA7ZZEHG/TEzNFdE+GShszuzbpTWtD8a4iQVB01BQGh8rMp0u/pL3e9pSayV3+60YYgXNPho /XWaeH1udzHqQAG1lrW+A /s8iq2Hsg9+6g6uFJgew2Yh2z7Ls64EMte104wJkbLjrwXJWhJinwCyC2PtSnU4dityfC71H7V4V8PQrKavdq1OH Tu0HXiV9MeEgv3/cp8ptdVyzjm3vbOQbQ62Yvwd5S4rRxgeAdumWs/drOHfeogIwqKNqOfvxd03XKk779H8 -----</pre>
<div>Close Display Sensitive Data As Plaintext</div>	

Step 4. (Optional) Click the desired certificate ID and click **Delete** to delete the SSL server details from the SSL server table.