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

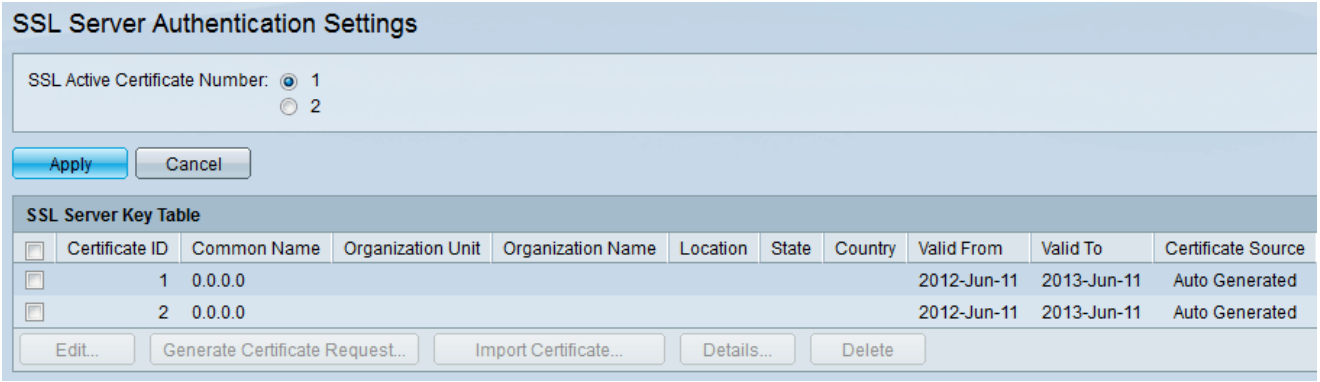
- Sx500 Series Stackable Switches

Software Version

- 1.3.0.62

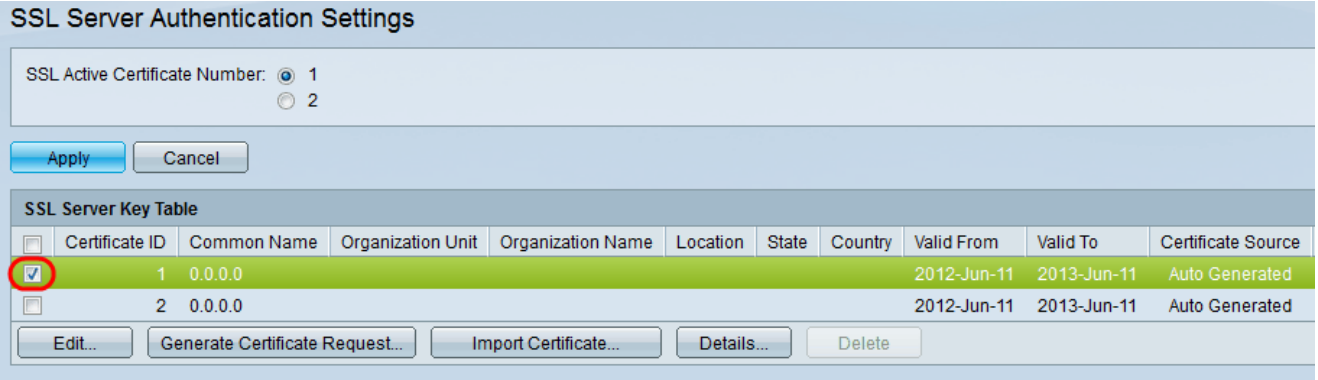
SSL Server Authentication Settings

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:

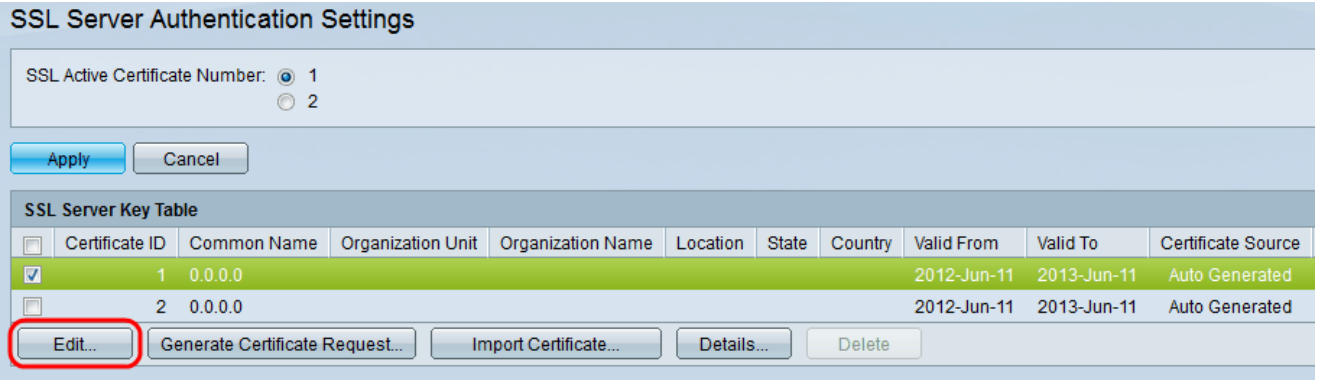


Note: Follow the Edit SSL Key Information to generate the certificate automatically, Generate Certificate Request to re-generate the certificate request by the switch and Import Certificate to import your desired certificate and the key.

Edit SSL Key Information

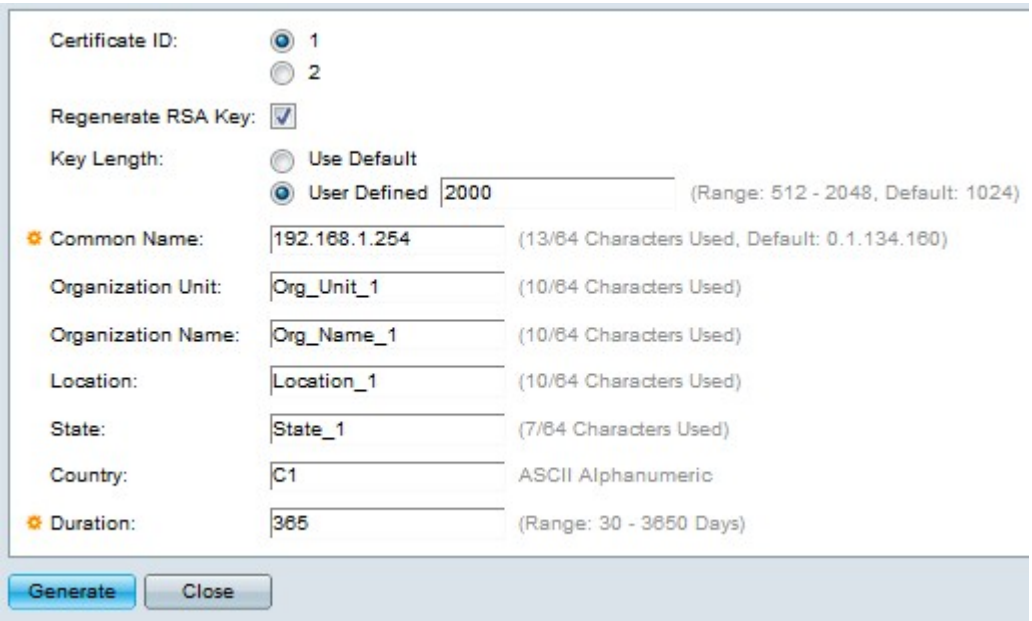


Step 2. Check the check box of the active certificate you wish to edit in the SSL Server Key Table.



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.



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.

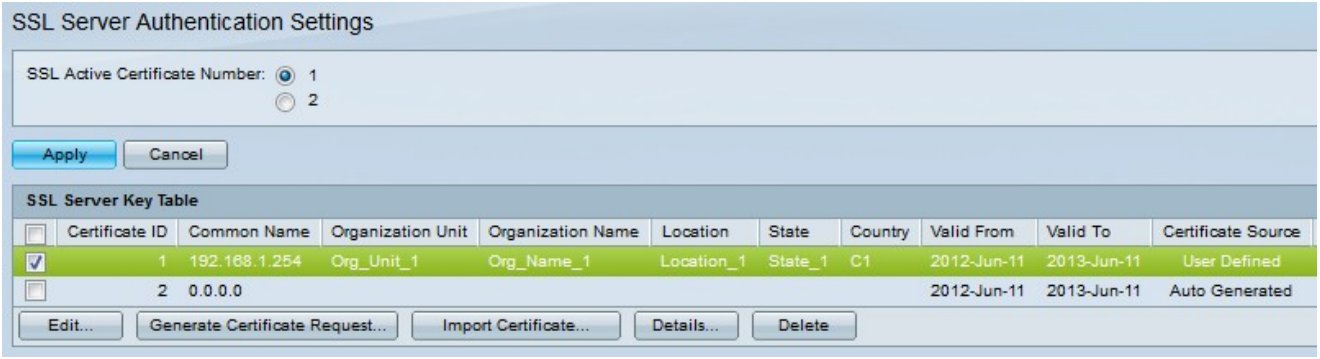
Step 10. In the Location field, enter the name of the location or city.

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

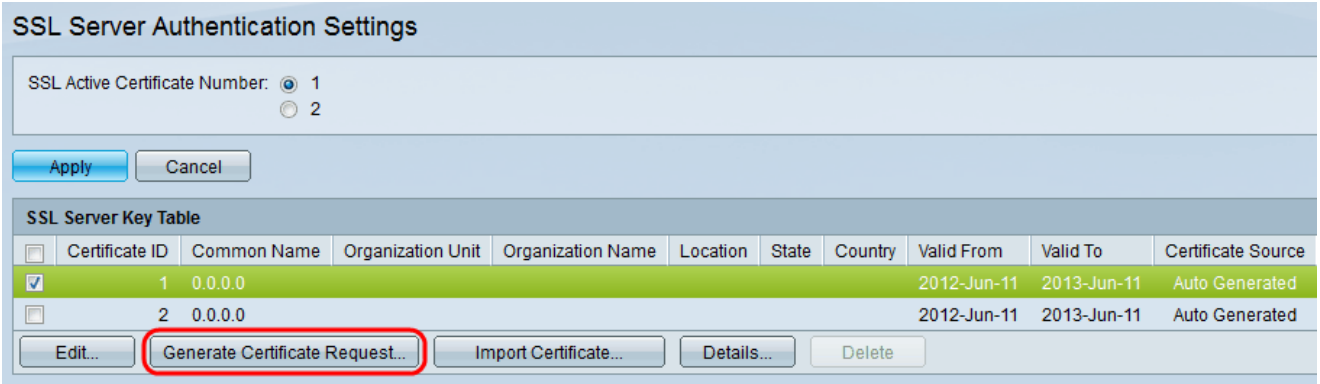
Step 12. In the Country field, enter the name of the country. As this accepts only alphanumeric value, use the global 2 letter format. For example, for the United States enter US.

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

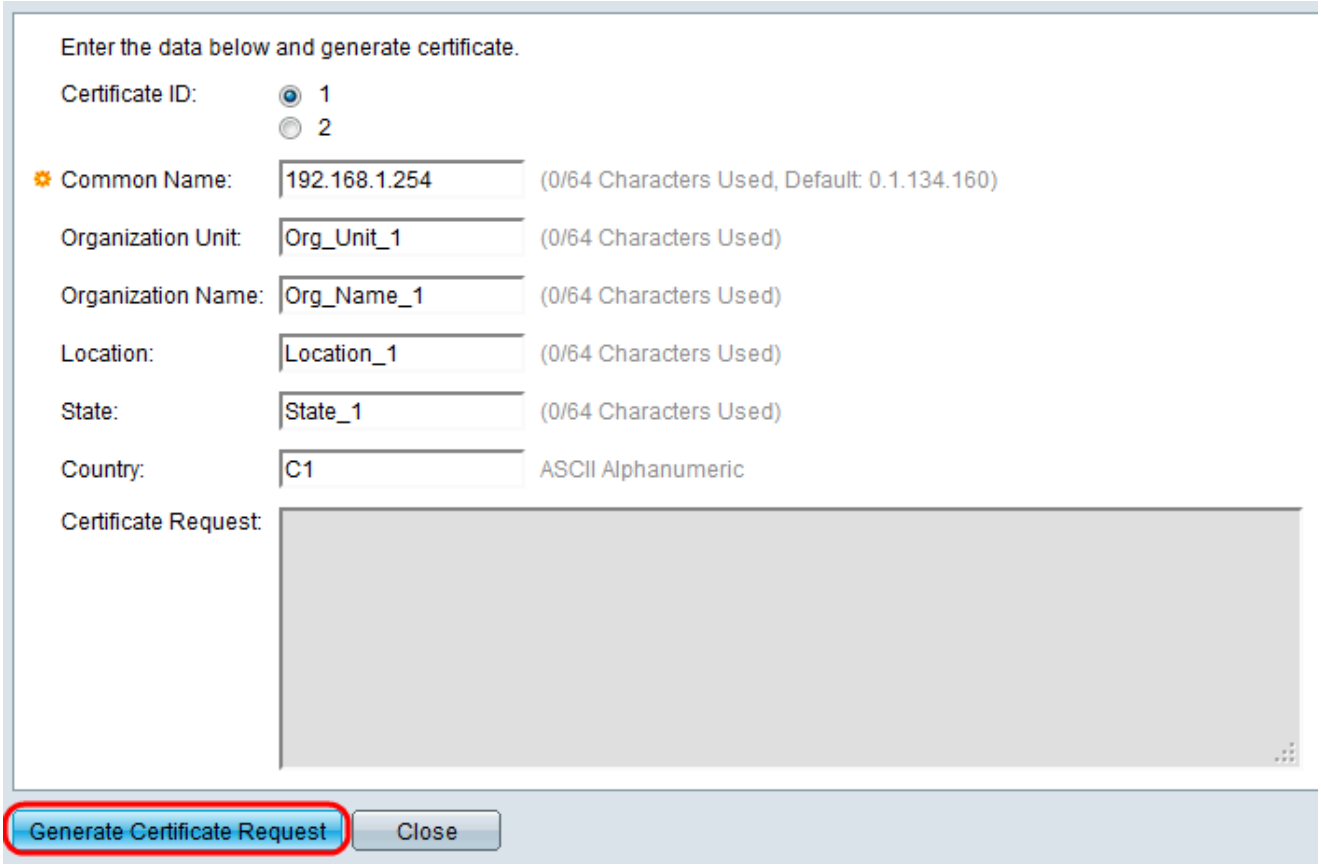
Step 14. Click **Generate** to save the settings.



Generate a Certificate Request



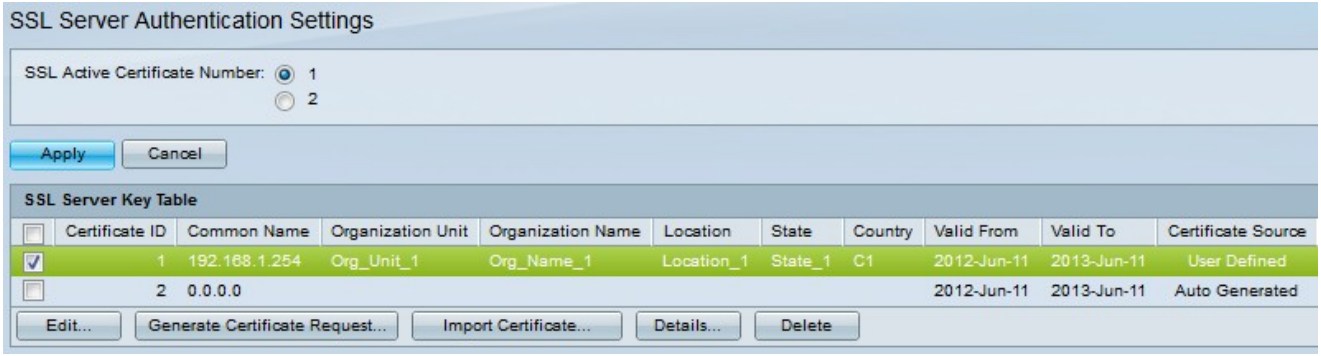
Step 1. In the *SSL Server Authentication Settings* page, check the certificate ID and click **Generate Certificate Request**.



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

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

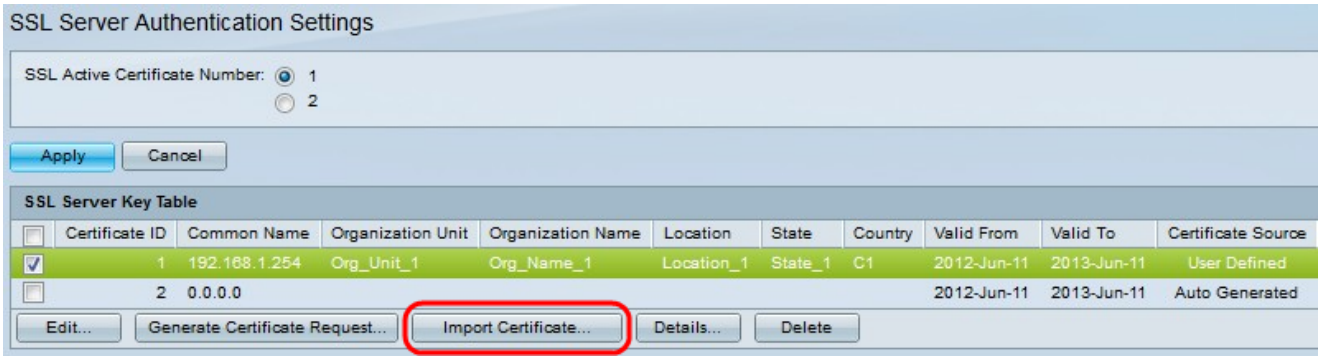
Step 3. Click **Generate Certificate Request** to save the settings.



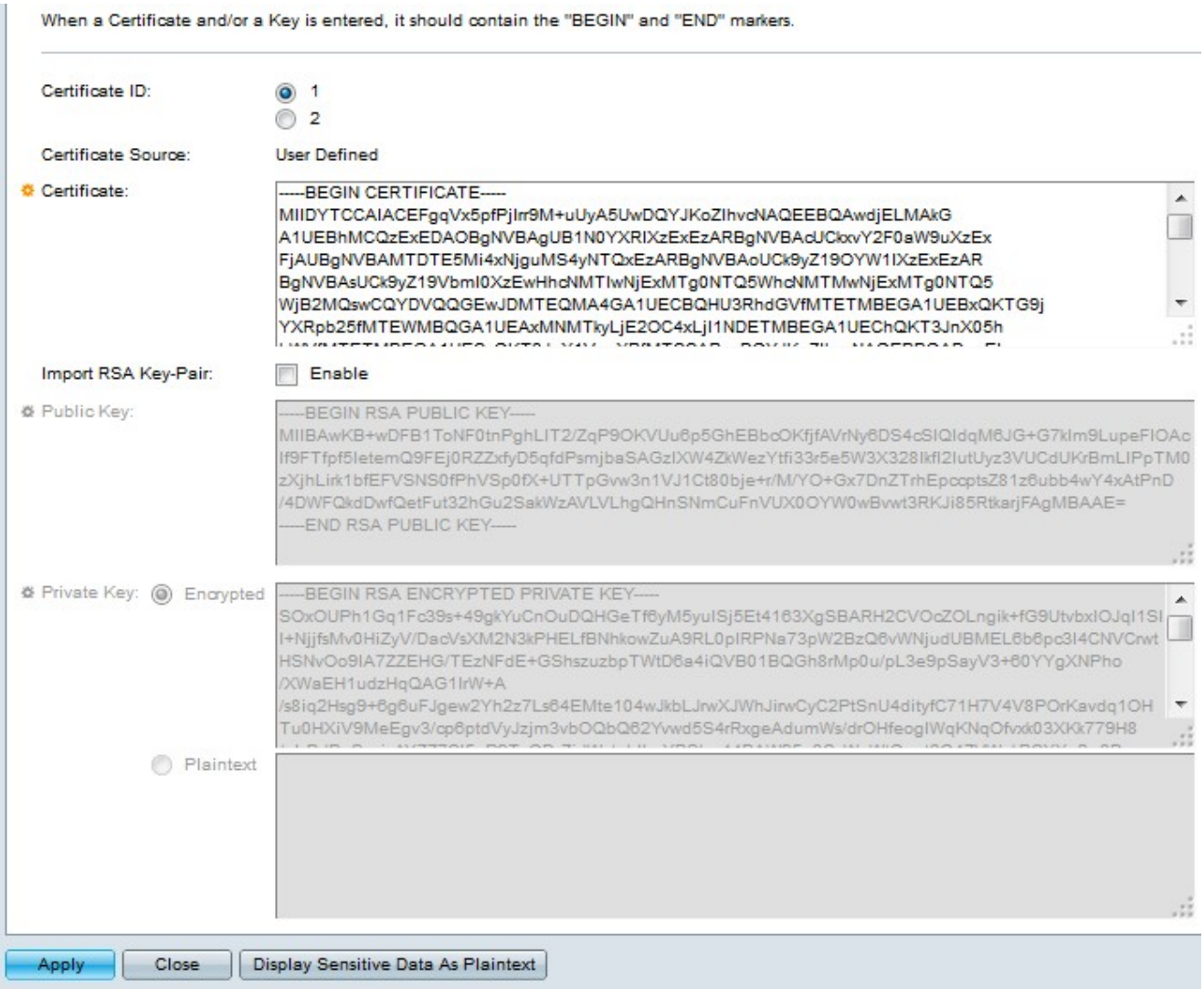
Now in the *SSL Server Authentication Settings* page, you can see the edited certificate with all the above entered information.

- 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

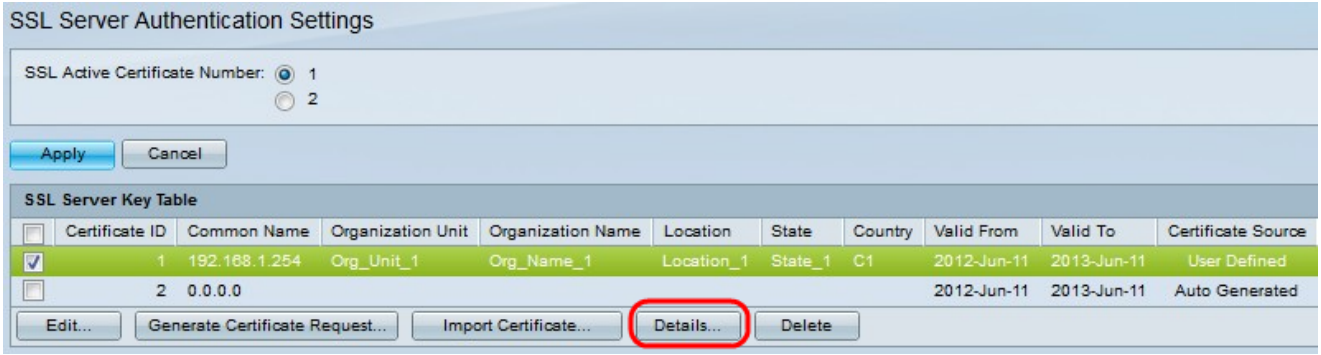


Step 1. Click desired check box and click **Import Certificate** to import a certificate.

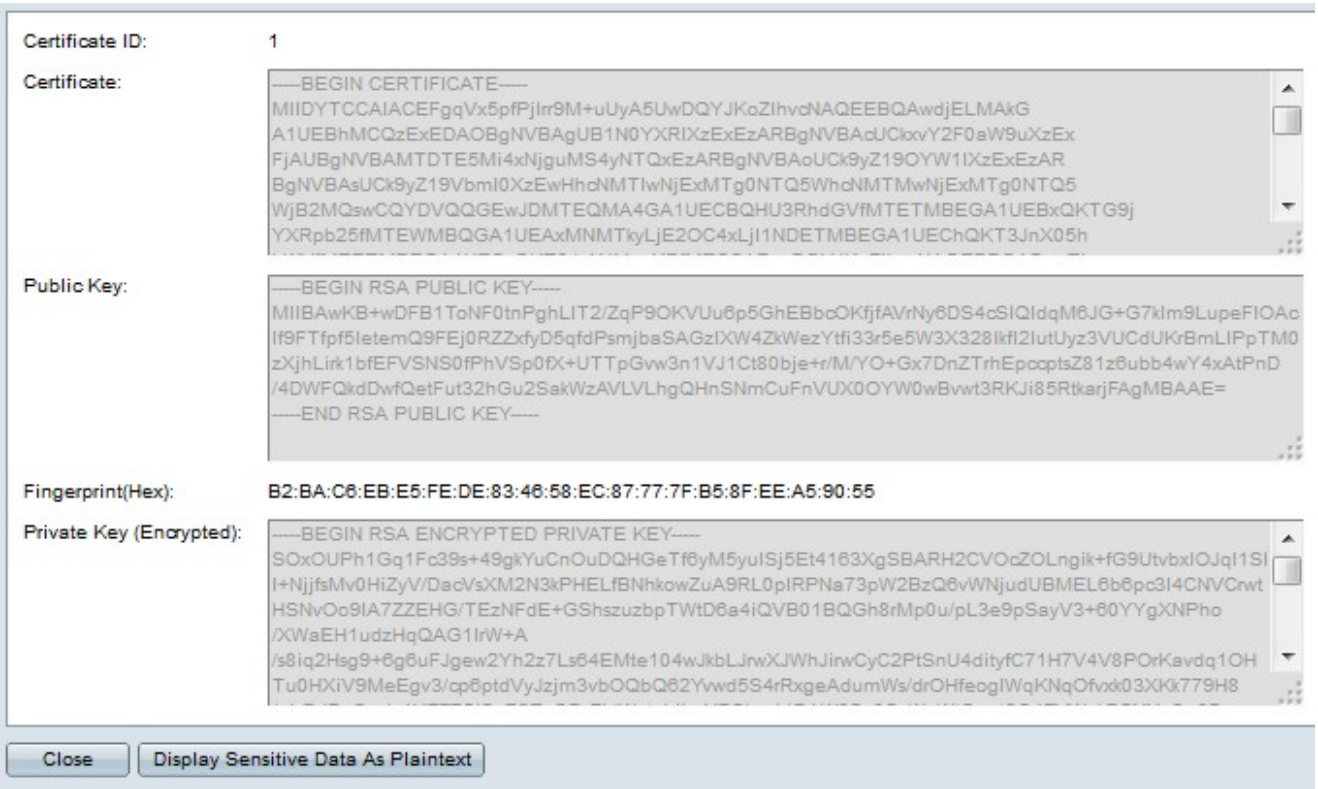


- Certificate ID — Choose the active certificate
- Certificate — Copy or paste the certificate to a configured.
- Import RSS KEY-Pair — Choose to enable the RSA key pair.
- Public Key (Encrypted) — Copy or paste the public key in an encrypted form.
- Private Key (Plaintext) — Copy or paste the private 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**.



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



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