

編輯Sx500系列堆疊式交換機上的安全套接字層(SSL)伺服器身份驗證設定

目標

安全套接字層(SSL)是一種協定，主要用於網際網路上的安全管理。它使用位於HTTP層和TCP層之間的程式層。對於身份驗證，SSL使用經過數位簽章並繫結到公鑰的證書來標識私鑰所有者。此身份驗證在連線期間很有幫助。使用SSL進行證書的交換，在認證過程中採用ITU-T標準X.509中描述的格式，然後由作為外部權威的認證機構簽發數位簽章的X.509證書。

本文說明如何編輯SSL伺服器身份驗證設定，以及如何在Sx500系列堆疊式交換機上生成證書請求。

適用裝置

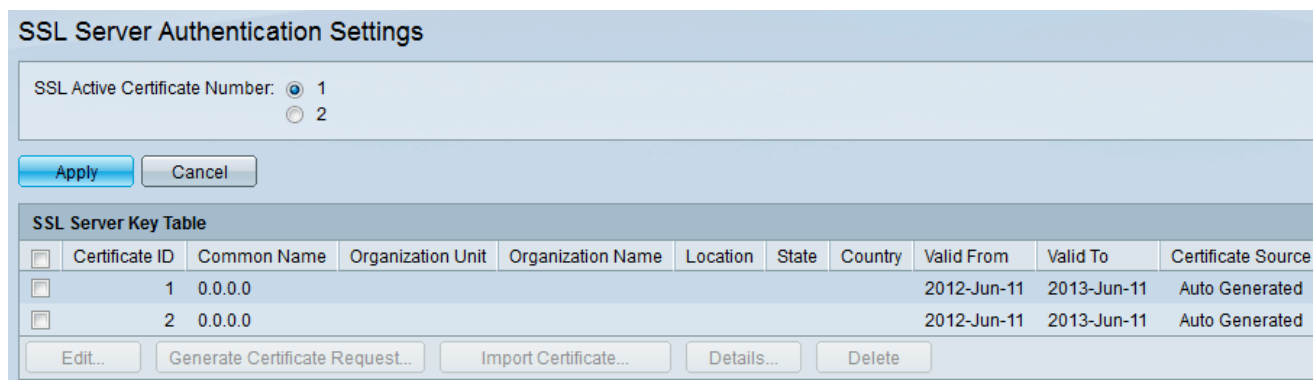
- Sx500系列堆疊式交換器

軟體版本

- 1.3.0.62

SSL伺服器身份驗證設定

步驟1.登入到交換機配置實用程式，然後選擇安全> SSL伺服器> SSL伺服器身份驗證設定。將開啟SSL Server Authentication Settings頁面：



SSL Server Authentication Settings

SSL Active Certificate Number: 1 2

Apply Cancel

<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

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

附註：請按照[編輯SSL金鑰資訊](#)自動生成證書、[生成證書請求](#)以重新生成交換機傳送的證書請求，以及[匯入證書](#)以匯入所需的證書和金鑰。

[編輯SSL金鑰資訊](#)

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

步驟2.在SSL伺服器金鑰表中選中要編輯的活動證書的覈取方塊。

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

步驟3.按一下Edit以變更現有的憑證。此時會顯示Edit Certificate視窗：

附註：在此範例中，憑證1已勾選。

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)

Generate Close

步驟4.在「憑證ID」欄位中，選擇1或2作為憑證的ID。在此配置中，「證書ID」(Certificate ID)欄位中只有2個可用選項。

步驟5.選中Regenerate RSA Key欄位中的覈取方塊以重新生成RSA金鑰。

步驟6.在Key Length欄位中，按一下任一單選按鈕。

·使用預設值 — 使用預設金鑰長度。

·使用者定義 — 在此欄位中，金鑰長度可以具有從512到2048的值。預設值為 1024。在此範

例中輸入2000。

步驟7.在Common Name欄位中，輸入完全限定裝置URL或特定公共IP地址。如果留空，則預設為裝置的最小IP地址（當生成證書時）。在本示例中，SG500X交換機的預設地址用作公用名。

步驟8.在「組織單位」欄位中輸入組織單位或部門的名稱。

步驟9.在「組織名稱」欄位中輸入組織名稱。

步驟10.在「地點」欄位中，輸入地點或城市的名稱。

步驟11.在「州」欄位中輸入州或省的名稱。

步驟12.在「國家/地區」欄位中，輸入國家/地區的名稱。由於它只接受字母數字值，因此使用全域性2字母格式。例如，對於United，請輸入US。

步驟13.在「持續時間」欄位中，輸入證書有效的天數。

步驟14.按一下**Generate**以儲存設定。

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

生成證書請求

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

步驟1. 在「*SSL Server Authentication Settings*」頁中，檢查證書ID，然後按一下**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 Close

步驟2.在編輯SSL伺服器身份驗證設定頁中按一下**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:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICTCCAzwCAQAwdjELMAkGA1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAc
UCkxvY2F0aW9uXzExFjAUBgNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190Y
W11XzExEzARBgNVBAUUCk9yZ19Vbml0XzEwggEbmA0GCSqGSIb3DQEBAQUAA4IBCAAwggEDAoH
7AL5ep54S5M7LHRLhNmpXmtuxWw070EhfL2cNTfH1RgfCfEs2zy8xUialNCKSoS/HapX3ry2gJZ
CtjFHmwEUjpUrYVHxqF9misXODEacranB1iSx4AMKMLy6ed+8tBN5xanhiUqplrXN1w81pEXHRf
/TtiivdifTW2GRmW/sw7e8+GCA0RU
/oRjDpRu1mi3R6z1PU4cK3UMWVzH1hQ5BG+IR+Ju8jOrMseRqjKRROZQz+aHHPVkwdfly51q
Cuk2R55lsbu2i6Fi7FQ5CY7jw4vj+pO2ZL0uz9q8qsDFxi
```

現在，在「Certificate Request」欄位中，您可以看到加密的憑證資訊。

步驟3.按一下**Generate Certificate Request**以儲存設定。

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

現在，在「SSL Server Authentication Settings」頁面中，可以看到包含所有上述輸入資訊的已編輯證書。

- 生效日期 — 指定證書的生效日期。
- 失效截止日期 — 指定證書失效的截止日期。
- 證書源 — 指定證書是由系統（自動生成）還是使用者（使用者定義）生成。

匯入證書

SSL Server Authentication Settings

SSL Active Certificate Number: 1
 2

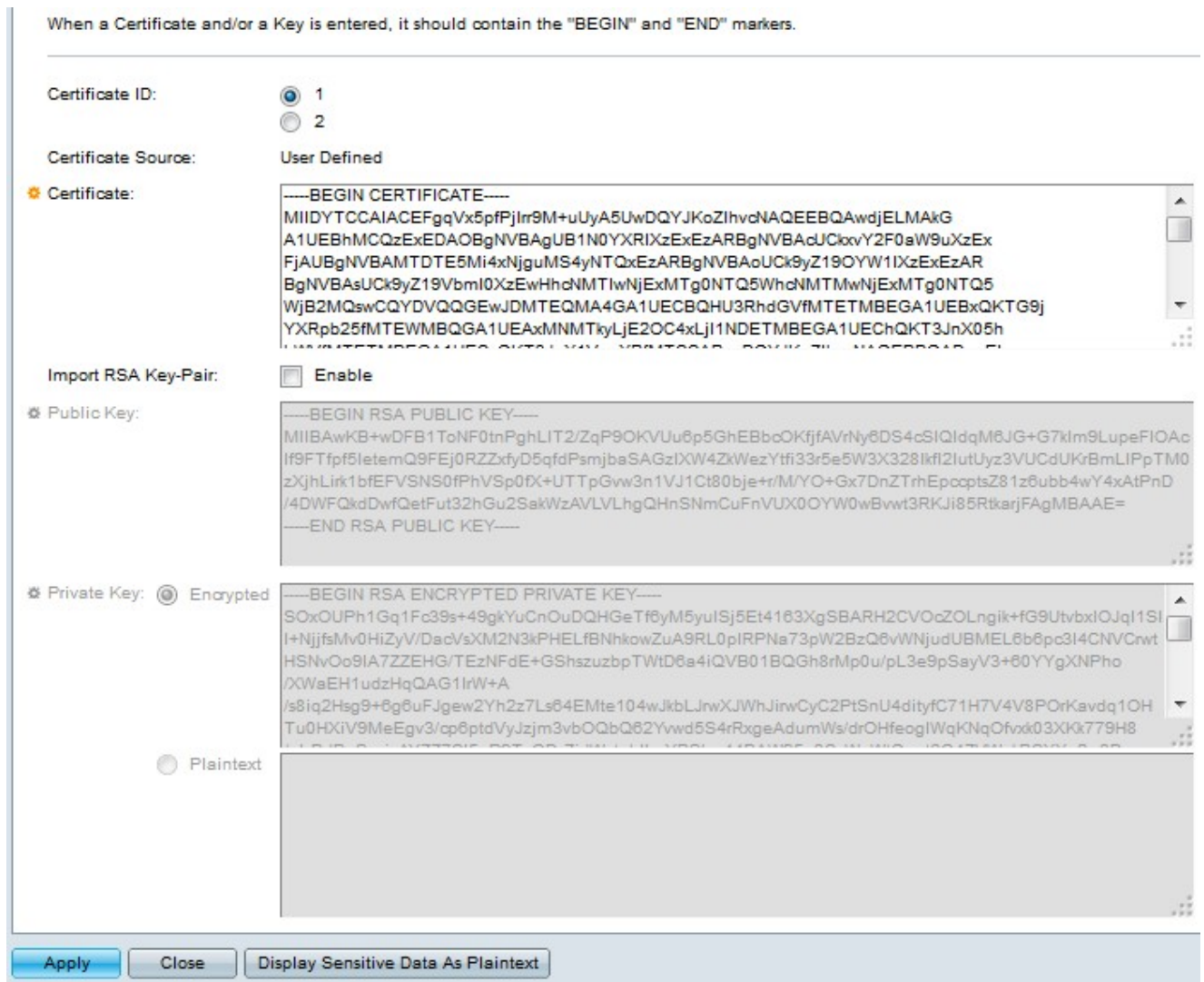
Apply Cancel

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

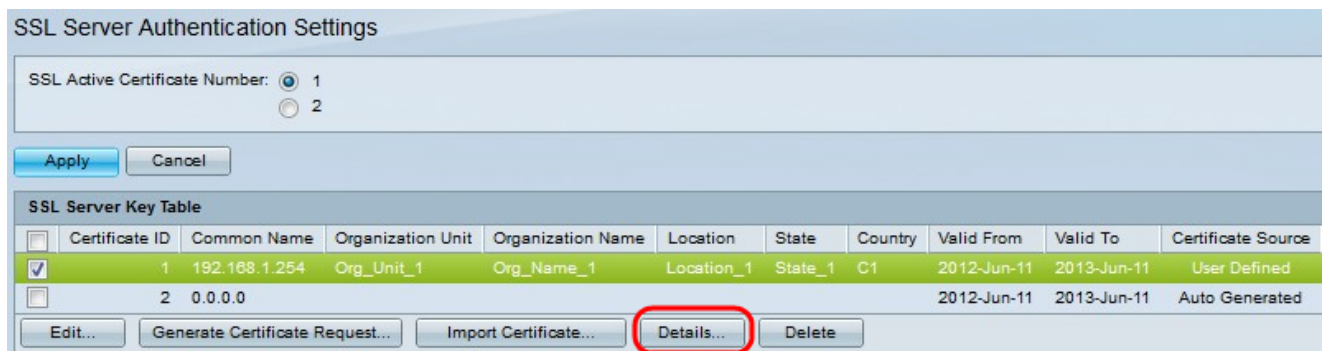
Edit... Generate Certificate Request... **Import Certificate...** Details... Delete

步驟1. 按一下所需的覈取方塊，然後按一下**匯入證書**以匯入證書。



- 證書ID — 選擇活動證書
- 證書 — 將證書複製或貼上到已配置的證書。
- 匯入RSA金鑰對 — 選擇以啟用RSA金鑰對。
- 公鑰 (已加密) — 以加密形式複製或貼上公鑰。
- 私鑰 (明文) — 以純文字檔案形式複製或貼上私鑰。
- 將敏感資料顯示為已加密 — 選擇此選項，您需要將私鑰以加密形式寫入配置檔案。

步驟2. 按一下 **Apply**。



步驟3. (可選) 按一下所需的證書ID，然後按一下 **Details** 檢視SSL詳細資訊的詳細資訊。

Certificate ID: 1

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDYTCCAIAACEFgqVx5pfJlr9M+uUyA5UwDQYJKoZIhvcNAQEEBQAwdjELMAkG
A1UEBhMCQzExEDAOBgNVBAgUB1N0YXRlXzExEzARBgNVBAcUCloY2F0aW9uXzEx
FjAUBgNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW1lXzExEzAR
BgNVBAsUCk9yZ19Vbml0XzEwHhcNMTIwMTg0NTQ5WWhcNMTMwNjExMTg0NTQ5
WjB2MQswCQYDVQQGEwJDMTEQMA4GA1UECBHU3RhdGVfMTETMBEGA1UEBxQKTG9j
YXRpb25fMTEWMBQGA1UEAxMNMTkyLjE2OC4xLj11NDETMBEGA1UEChQKT3JnX05h
-----
```

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBAwKB+wDFB1ToNF0tnPghLIT2/ZqP9OKVUu6p5GhEBbcOKfjAVrNy6DS4cSIQIdqM6JG+G7Im9LupeFIOAc
If9FTfp5IetemQ9FEj0RZZxfyD5qfdPsmjbaSAGzIXW4ZkWezYffi33r5e5W3X328kfl2lutUyz3VUCdUKrBmLIPpTM0
zXjhLirk1bFEFVSNS0fPhVSp0fX+UTTpGwv3n1VJ1Ct80bje+rM/YO+Gx7DnZTrhEpcoptsZ81z6ubb4wY4xAtPnD
/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+49gkYuCnOuDQHGeTf6yM5yulSj5Et4163XgSBRH2CVOcZOLngik+fG9UtvbxlOJq1Sl
I+NjffsMv0HiZyV/DacVsXM2N3kPHELfBNhkwZuA9RL0pIRPNa73pW2BzQ6vWNjudUBMEL6b6pc3I4CNVCrwt
HSNvOo9IA7ZZEHG/TEzNFdE+GShszuzbpTWtD8a4iQVB01BQGh8rMp0u/pL3e9pSayV3+80YYgXNPho
/XWaEH1udzHqQAG1rW+A
/s8iq2Hsg9+6g8uFJgew2Yh2z7Ls64EMte104wJkbLJrwXJWhJirwCyC2PtSnU4dityfC71H7V4V8POrKavdq1OH
Tu0HXiV9MeEgv3/op6ptdVyJzjm3vbOQbQ62Yvwd5S4rXgeAdumWs/drOHfeogIWqKNqOfvxx03XKk779H8
-----
```

Close Display Sensitive Data As Plaintext

步驟4. (可選) 按一下所需的證書ID，然後按一下**Delete**從SSL伺服器表中刪除SSL伺服器詳細資訊。