如何在Sx350和Sx550X系列交換器上匯入憑證

目標

本文的目的是提供使用圖形使用者介面(GUI)和命令列介面(CLI)在Sx350和Sx550X系列交換機上成功匯入證書的步驟。

目錄

簡介

在Sx350和Sx550X交換機上匯入證書時遇到的一個問題是，使用者面臨金鑰標頭丟失和/或無法載入公鑰錯*誤*。本文說明如何克服這些錯誤以成功匯入證書。證書是一種電子文檔，用於標識個人、伺服器、公司或其他實體，並將該實體與公鑰相關聯。證書用於網路中，以提供安全訪問。證書可以由外部證書頒發機構(CA)自簽名或數位簽章。如名稱所示，自簽名證書由自己的建立者簽名。CA管理證書請求並向參與實體（如主機、網路裝置或使用者）頒發證書。CA簽名的數位證書被視為行業標準和更安全。

適用裝置和軟體版本

- SG350版本2.5.0.83
- SG350X版本2.5.0.83
- SG350XG版本2.5.0.83
- SF350版本2.5.0.83
- SG550X版本2.5.0.83
- SF550X版本2.5.0.83
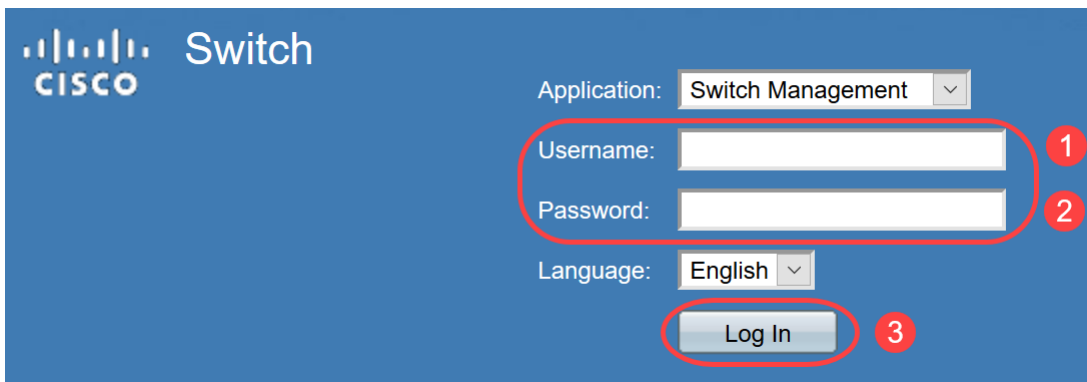- SG550XG版本2.5.0.83
- SX550X版本2.5.0.83

必要條件

您必須具有自簽名或證書頒發機構(CA)證書。本文包含獲取自簽名證書的步驟。要瞭解有關CA證書的詳細資訊，請按一下[此處](#)。
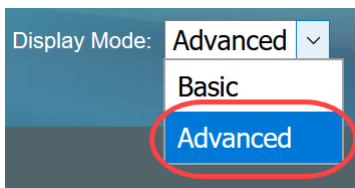
使用GUI匯入

步驟1
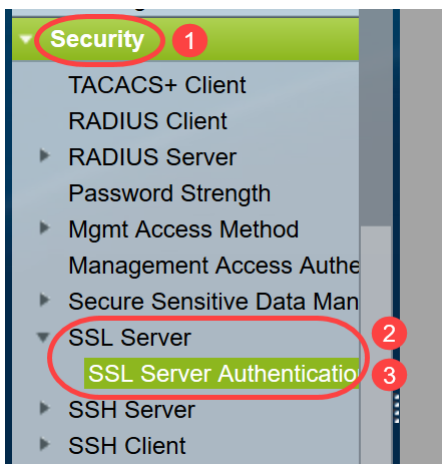
輸入*Username*和*Password*以登入交換器的GUI。按一下「**Log In**」。

步驟2

在GUI右上角的 *Display Mode* 中，使用下拉選項選擇 **Advanced**。
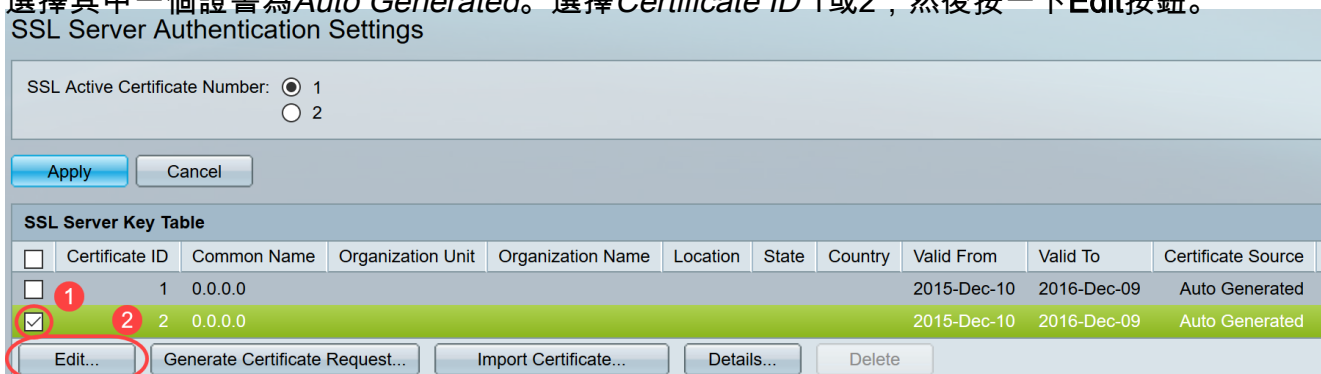

步驟3

導覽至 Security > SSL Server > SSL Server Authentication。

步驟4

選擇其中一個證書為 *Auto Generated*。選擇 *Certificate ID* 1或2，然後按一下 **Edit** 按鈕。

步驟5

要生成自簽名證書，請在新的彈出視窗中啟用*Regenerate RSA Key*並輸入以下引數：

金鑰長度

公用名

組織單位

組織名稱

位置

狀態

國家/地區

持續時間

按一下「**Generate**」。

您也可以從第三方CA建立憑證。

步驟6

現在您可以在*SSL Server Key Table*下看到*User Defined*證書。選擇新建立的證書,然後按一下
Details。

第7步

在彈出視窗中,您可以看到*Certificate*、*Public Key and Private Key(Encrypted)*詳細資訊。您可以
在單獨的記事本檔案中複製它們。按一下**Display Sensitive Data as Plaintext**。

步驟8

將會開啟一個彈出視窗,確認私鑰顯示為明文,然後按一下**OK**。

步驟9

現在，您將能夠以明文形式檢視*私鑰*。將明文輸出複製到記事本檔案。按一下「**Close**」。

步驟10

選擇新建立的*User Defined*證書，然後按一下Import Certificate。

步驟11

在新彈出視窗中，啟用*Import RSA Key-Pair*選項，然後以明文格式貼上私鑰（在步驟9中複製）。
按一下「**Apply**」。

在本示例中，公鑰的*BEGIN*和*END*處包含關鍵字*RSA*。

步驟12

螢幕上將顯示成功通知。您可以關閉此視窗並將組態儲存到交換器上。

✓ Success. To permanently save the configuration, go to the File Operations page or click the Save icon.

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-----
MIIDRzCCAi8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNBTEIGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAIVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NIowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCkNBTEIGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NIMQ4wDAYDVQQDDAVD

Import RSA Key-Pair: ☐ Enable

⚙ Public Key:
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xACel2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSkIr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB

⚙ Private Key: ● Encrypted

○ Plaintext

[Apply] [Close] [Display Sensitive Data as Plaintext]

可能的錯誤

所討論的錯誤與公鑰有關。通常使用兩種型別的公鑰格式：

1. RSA公鑰檔案(PKCS#1):這是針對RSA金鑰的。
它以標籤開始和結束：
-----開始RSA公鑰-----
BASE64編碼資料
-----結束RSA公鑰-----

2.公鑰檔案(PKCS#8):這是一種更為通用的金鑰格式，用於標識公鑰的型別並包含相關資料。
它以標籤開始和結束：
-----BEGIN PUBLIC KEY-----
BASE64編碼資料
-----END PUBLIC KEY-----

缺少金鑰標頭錯誤

案例 1:您從第三方CA生成了證書。複製並貼上公鑰並按一下Apply。

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-----
MIIDRzCCAi8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNBTEIGT1JOSUExETAPBgNVBAcMCFNhbiBKb3Nl
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAlVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCkNBTEIGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NlMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair:　☑ Enable

⚙ Public Key:
```
-----BEGIN PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe0J
p8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT0My
qFlmBPNuL4awjvtt9E7lEXhBt1HL0Nr/cuWTLmAOlDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel
2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafgt2aSklr8L8yHSSD1BWB0
9X5fjv10QNAMQ+QIDAQAB
```

⚙ Private Key:　○ Encrypted
```
```

　　　　　　　　　● Plaintext
```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5j
pe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT
0MyqFlmBPNuL4awjvtt9E7lEXhBt1HL0Nr/cuWTLmAOlDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wx
ACel2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafgt2aSklr8L8yHSSD1B
WB09X5fjv10QNAMQ+QIDAQABAolBAAlZH0Lg1V/I45VC/5PkZmOczkr426JO4DDhFcXdzMl8PzQ6ElKExUH
```

[**Apply**]　[Close]　[Display Sensitive Data as Plaintext]

您收到消息*Error:缺少金鑰標頭*。關閉視窗。可以做一些修改以使此問題消失。

❌ Error: Key header is missing

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-----
MIIDRzCCAi8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNBTEIGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAIVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCkNBTEIGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair:	☐ Enable

⚙ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhICMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xACel2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSkIr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

⚙ Private Key:	◉ Encrypted
	◯ Plaintext

[Apply] [Close] [Display Sensitive Data as Plaintext]

修復此錯誤：

　　將關鍵字*RSA*新增到公鑰的開頭：*開始RSA公鑰*

　　將關鍵字*RSA*新增到公鑰的末尾：*結束RSA公鑰*

　　從金鑰代碼中刪除前32個字元。下面顯示的突出顯示部分是前32個字元的示例。

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEApAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFlq3QilBHDtLJ
07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRlMcyv0vblqDJI/ejOaYiGA10GX8eiT8IxIfM
blJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVfshpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794HgAu0
HyxpT7qDOVrYv4FAGIR1pbIDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trxqX/Km6vgBnvBePI1yaW
iSOqaG0zqjjr7YQIDAQAB
```

在應用設定時，在大多數情況下*不會獲取Key header is missing* error。

無法載入公鑰錯誤

案例 2:您在一台交換機上生成了證書，並將其匯入到另一台交換機上。刪除前32個字元並按一下**Apply**後，複製並貼上了公鑰。

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-----
MIIDSTCCAjECEHV4jm/blKGoJFHmCvnyTWUwDQYJKoZIhvcNAQELBQAwYzELMAkG
A1UEBhMCSU4xEDAOBgNVBAgMB0hhcnlhbmExEDAOBgNVBAcMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMxCzAJBgNVBAYTAklOMRAw
DgYDVQQIDAdlYXJ5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu
```

Import RSA Key-Pair: ☑ Enable

⚙ Public Key:

(1)
```
-----BEGIN RSA PUBLIC KEY-----
/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFlq3QilBHDtLJ07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVN
J5ZPG8qKw58HWRlMcyv0vblqDJl/ejOaYiGA10GX8eiT8lxlfMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbguVf
shpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794HgAu0HyxpT7gDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFiI
92aDPeK1ZCMAcDJaMaQ4trxgX/Km6vgBnvBePl1yaWiSOqaG0zgjjr7YQIDAQAB
-----END RSA PUBLIC KEY-----
```

⚙ Private Key: ○ Encrypted
```

```

               ● Plaintext
```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEApAggvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFlq3QilBH
DtLJ07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVNJ5ZPG8qKw58HWRlMcyv0vblqDJl/ejOaYiGA10GX8eiT8
lxlfMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbguVfshpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794H
gAu0HyxpT7gDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFiI92aDPeK1ZCMAcDJaMaQ4trxgX/Km6vgBnvBePl
1yaWiSOqaG0zgjjr7YQIDAQABAoIBAQCTUfJvpS1Qvzi21FbNZmhBYkmMoxTpYKHguvoxwbZqlS07KdPF5v
```

(2)

[Apply]   [Close]   [Display Sensitive Data as Plaintext]

螢幕上出現*Failed to load public key*錯誤。

❌ Failed to load public key

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-----
MIIDSTCCAjECEHV4jm/blKGoJFHmCvnyTWUwDQYJKoZIhvcNAQELBQAwYzELMAkG
A1UEBhMCSU4xEDAOBgNVBAgMB0hhcnlhbmExEDAOBgNVBAcMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMxCzAJBgNVBAYTAklOMRAw
DgYDVQQIDAdIYXJ5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu
```

Import RSA Key-Pair: ☐ Enable

⚙ Public Key:
```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEApAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFIq3QiIBHDtL
J07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRlMcyv0vblqDJI/ejOaYiGA10GX8eiT8Ix
IfMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVfshpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794H
gAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFiI92aDPeK1ZCMAcDJaMaQ4trxqX/Km6vgBnvBe
PI1yaWiSOqaG0zgjjr7YQIDAQAB
```

⚙ Private Key: ○ Encrypted
```
```
○ Plaintext
```
```

[Apply] [Close] [Display Sensitive Data as Plaintext]

要解決此錯誤，請不要在此情況下刪除公鑰的前32個字元。

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-----
MIIDSTCCAjECEHV4jm/blKGoJFHmCvnyTWUwDQYJKoZIhvcNAQELBQAwYzELMAkG
A1UEBhMCSU4xEDAOBgNVBAgMB0hhcnlhbmExEDAOBgNVBAcMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMxCzAJBgNVBAYTAklOMRAw
DgYDVQQIDAdIYXJ5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu
```
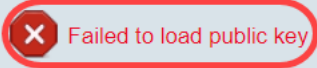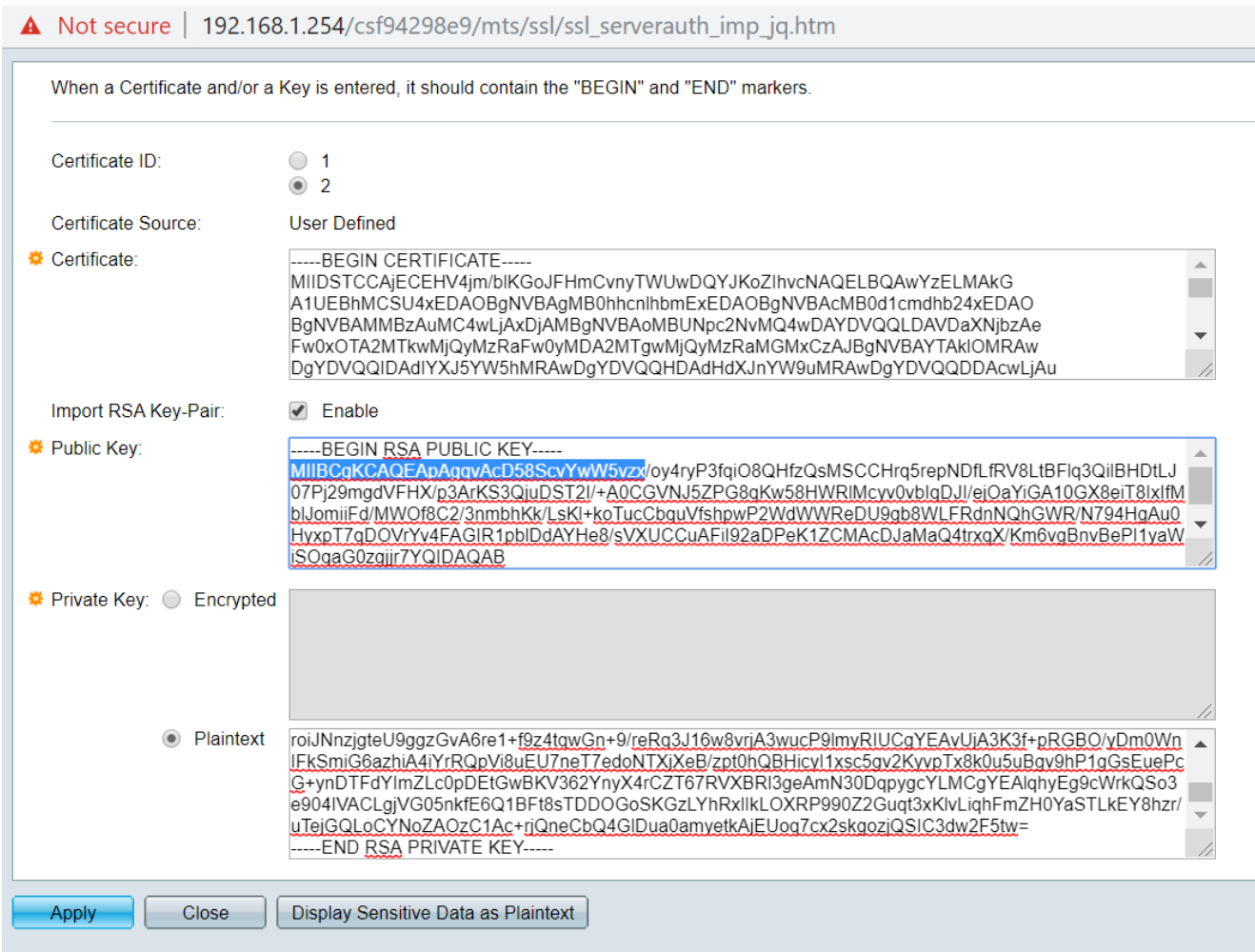
Import RSA Key-Pair: ☑ Enable

⚙ **Public Key:**
```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEApAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFlq3QilBHDtLJ
07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRlMcyv0vblgDJl/ejOaYiGA10GX8eiT8IxIfM
blJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbguVfshpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794HgAu0
HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFiI92aDPeK1ZCMAcDJaMaQ4trxqX/Km6vgBnvBePl1yaW
iSOqaG0zgjjr7YQIDAQAB
```

⚙ **Private Key:** ○ **Encrypted**
```

```

● **Plaintext**
```
roiJNnzjgteU9ggzGvA6re1+f9z4tqwGn+9/reRq3J16w8vrjA3wucP9lmyRIUCgYEAvUjA3K3f+pRGBO/yDm0Wn
lFkSmiG6azhiA4iYrRQpVi8uEU7neT7edoNTXjXeB/zpt0hQBHicyI1xsc5gv2KyvpTx8k0u5uBgv9hP1gGsEuePc
G+ynDTFdYlmZLc0pDEtGwBKV362YnyX4rCZT67RVXBRI3geAmN30DqpygcYLMCgYEAlqhyEg9cWrkQSo3
e904IVACLgjVG05nkfE6Q1BFt8sTDDOGoSKGzLYhRxIlkLOXRP990Z2Guqt3xKlvLiqhFmZH0YaSTLkEY8hzr/
uTejGQLoCYNoZAOzC1Ac+rjQneCbQ4GlDua0amyetkAjEUoq7cx2skgozjQSIC3dw2F5tw=
-----END RSA PRIVATE KEY-----
```

[**Apply**] [Close] [Display Sensitive Data as Plaintext]

使用CLI匯入

步驟1

要使用CLI匯入證書,請輸入以下命令。

```
switch(config)#crypto certificate [certificate number] import
```

在此範例中匯入憑證2。

```
switch(config)#crypto certificate 2 import
```

步驟2

貼上輸入;在輸入後單獨的行上新增句點(.)。

```
-----RSA-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAAASCBKGWGskAgEAAoIBAQC/rZQ6f0rj8neA
...24…….
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+52lD/GokmU
-----END RSA PRIVATE KEY-----
-----RSA-----
MIIBCgKCAQEAv62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkfT0l
...3…….
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB
```

```
-----RSA-----
-----BEGIN CERTIFICATE-----
MIIFvTCCBKWgAwIBAgIRAOOBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw
— 28……
8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVFf0cUzqXwOJcsTrMV
JDPtnbKXG56w0Trecu6UQ9HsUBoDQnlsN5ZBHtlVyjAP
-----END CERTIFICATE-----
.

C=xxST=GxxxxxL=xxO=xx CA LimitedCN=xx RSACA
61400:00:00 2017 GMT
91123:59:59 2020 GMT
C=DE/postalCode=xxxST=xxL=xx/street=xxx 2O=xxxOU=ITCN=*.kowi.eu
SHAxxxxxx
```

結論

現在，您已學習使用GUI和CLI在Sx350和Sx550X系列交換機上成功匯入證書的步驟。