How to Import Certificate on Sx350 and Sx550X Series Switches

Objective

This objective of this document is to provide the steps to successfully import a certificate on Sx350 and Sx550X series switches using the Graphical User Interface (GUI) and the Command Line Interface (CLI).

Table of Contents

Introduction

One of the issues encountered when importing a certificate on Sx350 and Sx550X switches is that the user faces ***key header is missing*** and/or ***failed to load public key*** errors. This document will explain how to get past these errors to successfully import a certificate. A certificate is an electronic document that identifies an individual, a server, a company, or other entity and associates that entity with a public key. Certificates are used in a network to provide secure access. Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). A self-signed certificate, as the name indicates, is signed by its own creator. CAs manage certificate requests and issue certificates to participating entities such as hosts, network devices, or users. A CA-signed digital certificate is considered industry standard and more secure.

Applicable Devices and Software Version

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

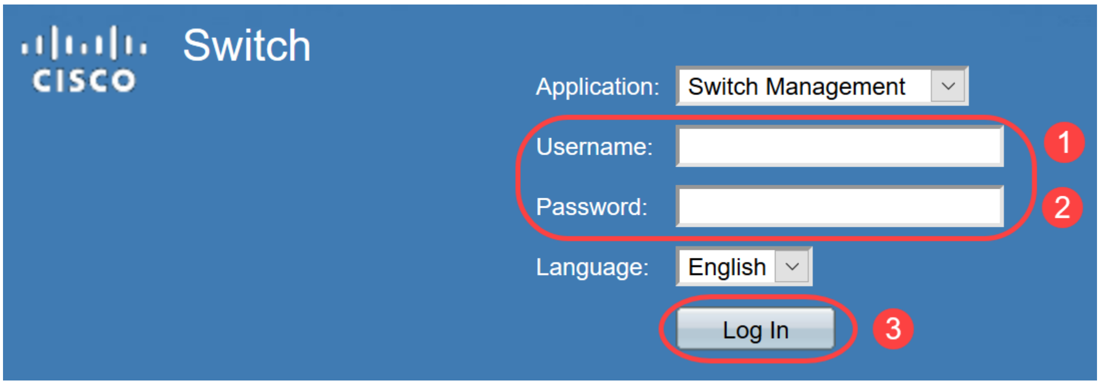
Prerequisites

You must have a self-signed or Certificate Authority (CA) certificate. Steps for obtaining a self-signed certificate are included in this article. To learn more about CA certificates, click here.

Import using GUI

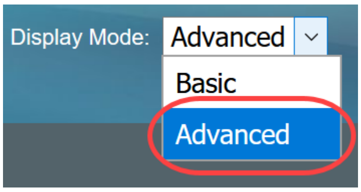
Step 1

Log in to the GUI of the switch by entering your *Username* and *Password*. Click **Log In**.



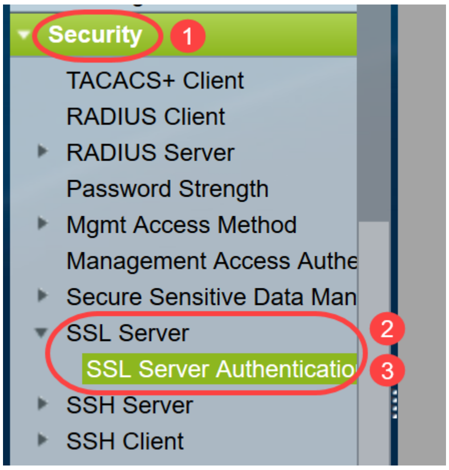
Step 2

From the *Display Mode* on the top right side of the GUI, choose **Advanced** using the drop-down option.



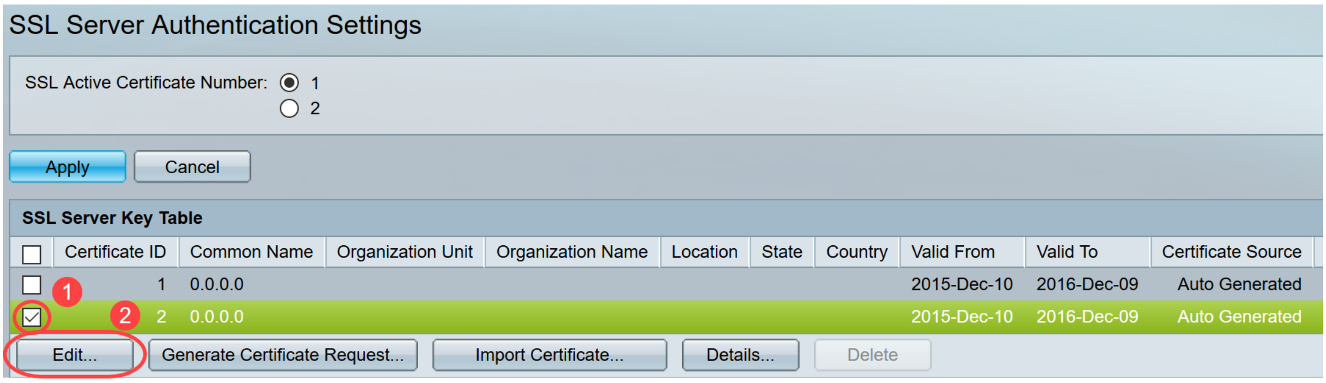
Step 3

Navigate to **Security > SSL Server > SSL Server Authentication**.



Step 4

Select one of the certificates that is *Auto Generated*. Select the *Certificate ID* 1 or 2 and click on the **Edit** button.



SSL Server Authentication Settings

SSL Active Certificate Number: ● 1 ○ 2

SSL Server Key Table

□	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
□	1	0.0.0.0						2015-Dec-10	2016-Dec-09	Auto Generated
☑	2	0.0.0.0						2015-Dec-10	2016-Dec-09	Auto Generated

Step 5

To generate a self-signed certificate, on the new pop-up window enable *Regenerate RSA Key* and enter the following parameters:

Key Length

Common Name

Organization Unit

Organization Name

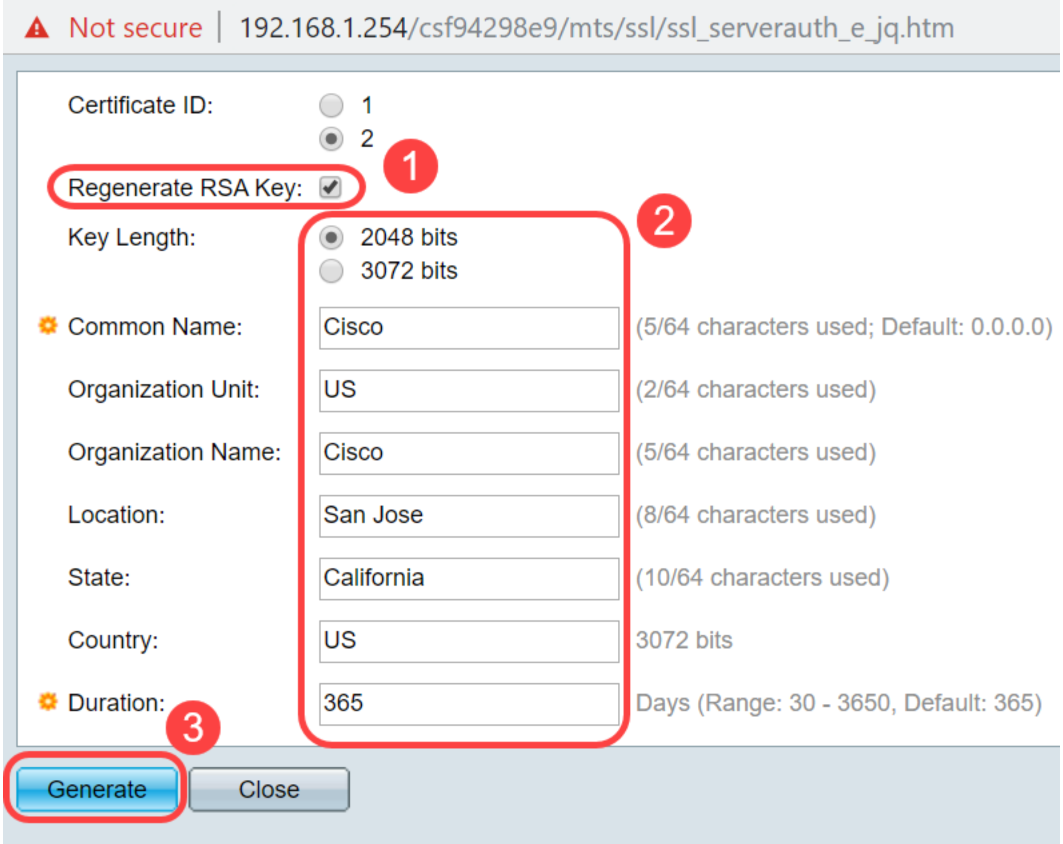
Location

State

Country

Duration

Click **Generate**.



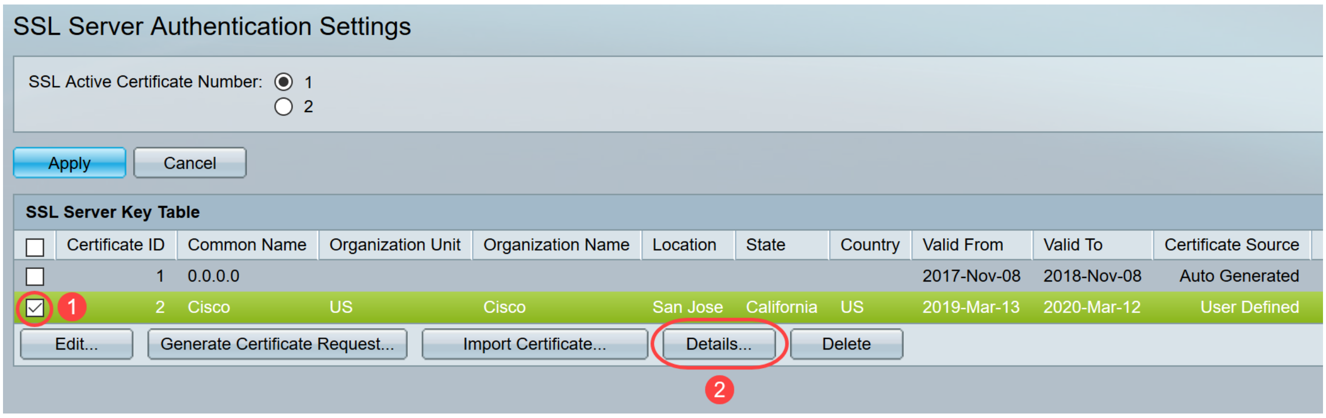
Not secure | 192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_e_jq.htm

Certificate ID:	○ 1 ● 2	
Regenerate RSA Key:	☑	
Key Length:	● 2048 bits ○ 3072 bits	
Common Name:	Cisco	(5/64 characters used; Default: 0.0.0.0)
Organization Unit:	US	(2/64 characters used)
Organization Name:	Cisco	(5/64 characters used)
Location:	San Jose	(8/64 characters used)
State:	California	(10/64 characters used)
Country:	US	3072 bits
Duration:	365	Days (Range: 30 - 3650, Default: 365)

You may also create a certificate from a third-party CA.

Step 6

Now you will be able to see the *User Defined* certificate under the *SSL Server Key Table*. Select the newly created certificate and click on **Details**.



SSL Server Authentication Settings

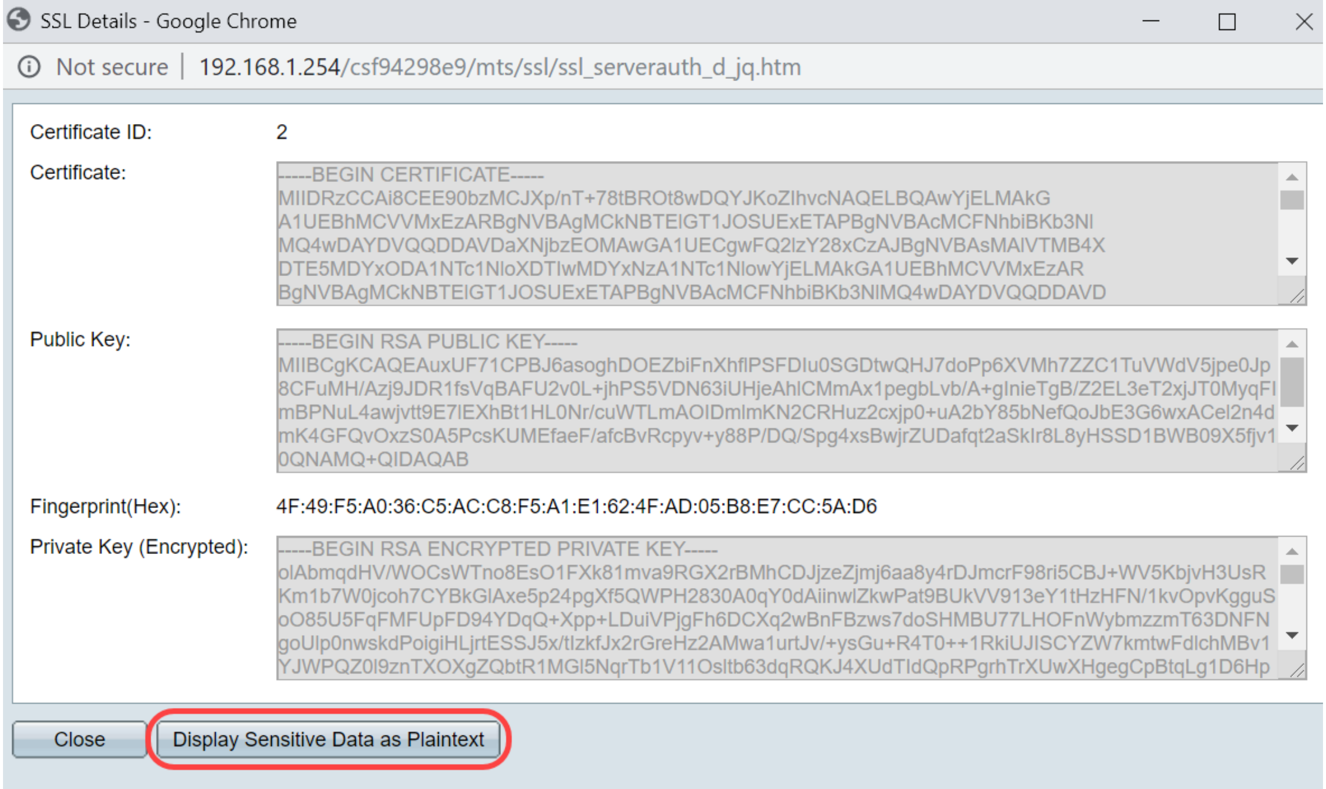
SSL Active Certificate Number: ● 1 ○ 2

SSL Server Key Table

□	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
□	1	0.0.0.0						2017-Nov-08	2018-Nov-08	Auto Generated
☑	2	Cisco	US	Cisco	San Jose	California	US	2019-Mar-13	2020-Mar-12	User Defined

Step 7

On the pop-up window you will be able to see the *Certificate*, *Public Key and Private Key (Encrypted)* details. You may copy those on a separate notepad file. Click **Display Sensitive Data as Plaintext**.


SSL Details - Google Chrome
Not secure | 192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_d_jq.htm
Close
Display Sensitive Data as Plaintext

Certificate ID: 2

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDRzCCAi8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNBTElGT1JOSUExETAPBgNVBAcMCFNhbiBKb3Nl
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xCzAJBgNVBAsMAlVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCkNBTElGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NlMQ4wDAYDVQQDDAVD
```

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT0MyqFI
mBPNuL4awjvtt9E7lEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel2n4d
mK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSkIr8L8yHSSD1BWB09X5fjv1
0QNAMQ+QIDAQAB
```

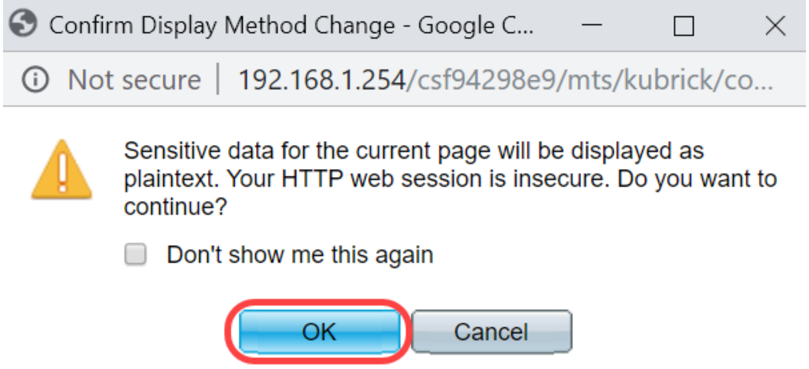
Fingerprint(Hex): 4F:49:F5:A0:36:C5:AC:C8:F5:A1:E1:62:4F:AD:05:B8:E7:CC:5A:D6

Private Key (Encrypted):

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
olAbmqdHV/WOCsWTno8EsO1FXk81mva9RGX2rBMhCDJjzeZjmj6aa8y4rDJmcrF98ri5CBJ+WV5KbjvH3UsR
Km1b7W0jcoh7CYBkGlAxe5p24pgXf5QWPH2830A0qY0dAiinwlZkwPat9BUkVV913eY1tHzHFN/1kvOpvKgguS
oO85U5FqFMFUpFD94YDqQ+Xpp+LDuiVPjgFh6DCXq2wBnFBzws7doSHMBU77LHOFnWybmzzmT63DNFN
goUlp0nwskdPoigiHLjrtESSJ5x/tIzkfJx2rGreHz2AMwa1urtJv/+ysGu+R4T0++1RkiUJISCYZW7kmtwFdlchMBv1
YJWPQZ0l9znTXOXgZQbtR1MGl5NqrTb1V11Osltb63dqRQKJ4XUdTldQpRPgrhTrXUwXHgegCpBtqLg1D6Hp
```

Step 8

A pop-up window will open to confirm the display of Private Key as plaintext, click **OK**.

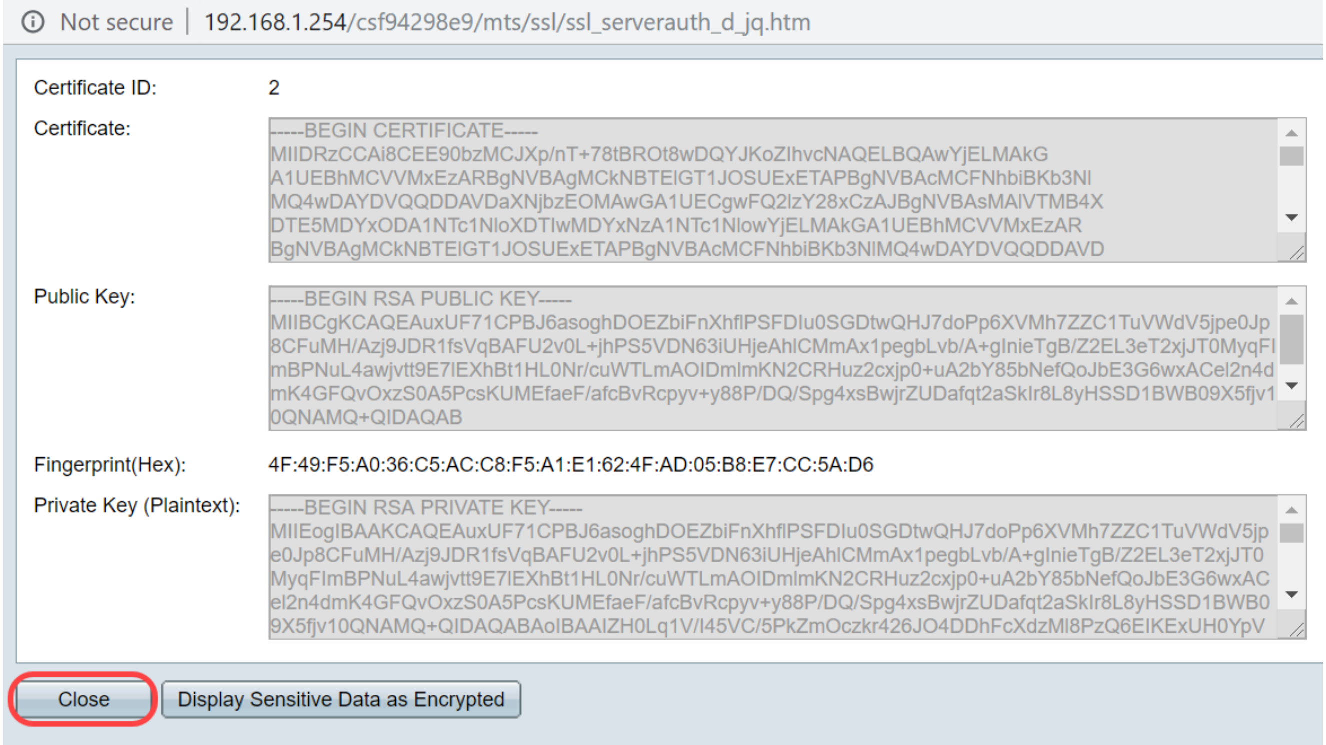

Confirm Display Method Change - Google C...
Not secure | 192.168.1.254/csf94298e9/mts/kubrick/co...
OK
Cancel

Sensitive data for the current page will be displayed as plaintext. Your HTTP web session is insecure. Do you want to continue?

□ Don't show me this again

Step 9

Now you will be able to see the *Private Key* in plaintext form. Copy that plaintext output on a notepad file. Click **Close**.



ⓘ Not secure | 192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_d_jq.htm

Certificate ID: 2

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDRzCCAi8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNBTElGT1JOSUExETAPBgNVBAcMCFNhbiBKb3Nl
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xCzAJBgNVBAsMAlVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCkNBTElGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NlMQ4wDAYDVQQDDAVD
```

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT0MyqFl
mBPNuL4awjvtt9E7lEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel2n4d
mK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSklr8L8yHSSD1BWB09X5fjv1
0QNAMQ+QIDAQAB
```

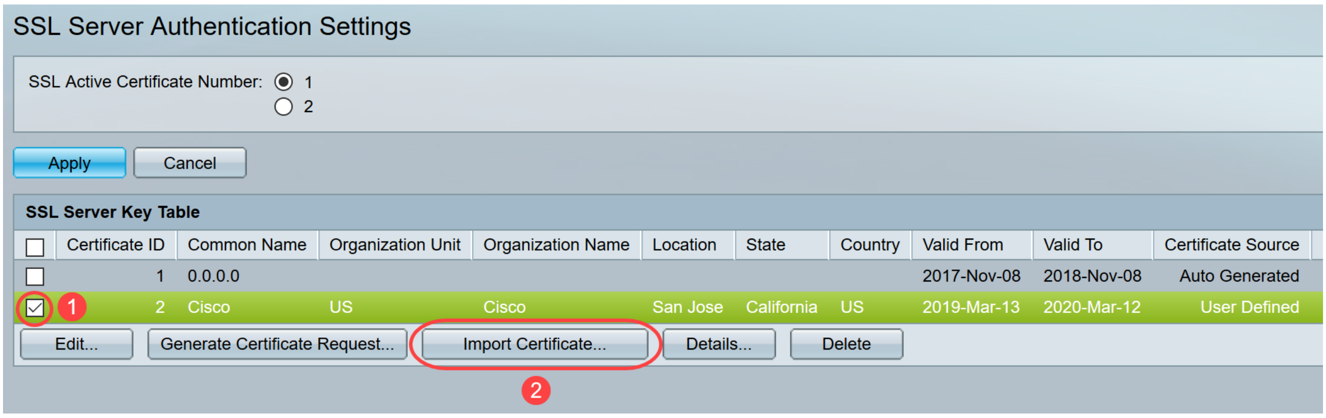
Fingerprint(Hex): 4F:49:F5:A0:36:C5:AC:C8:F5:A1:E1:62:4F:AD:05:B8:E7:CC:5A:D6

Private Key (Plaintext):

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jp
e0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT0
MyqFlmBPNuL4awjvtt9E7lEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxAC
el2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSklr8L8yHSSD1BWB0
9X5fjv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PkZmOczkr426JO4DDhFcXdzMI8PzQ6EIKExUH0YpV
```

Step 10

Select the newly created *User Defined* certificate and click **Import Certificate**.



SSL Server Authentication Settings

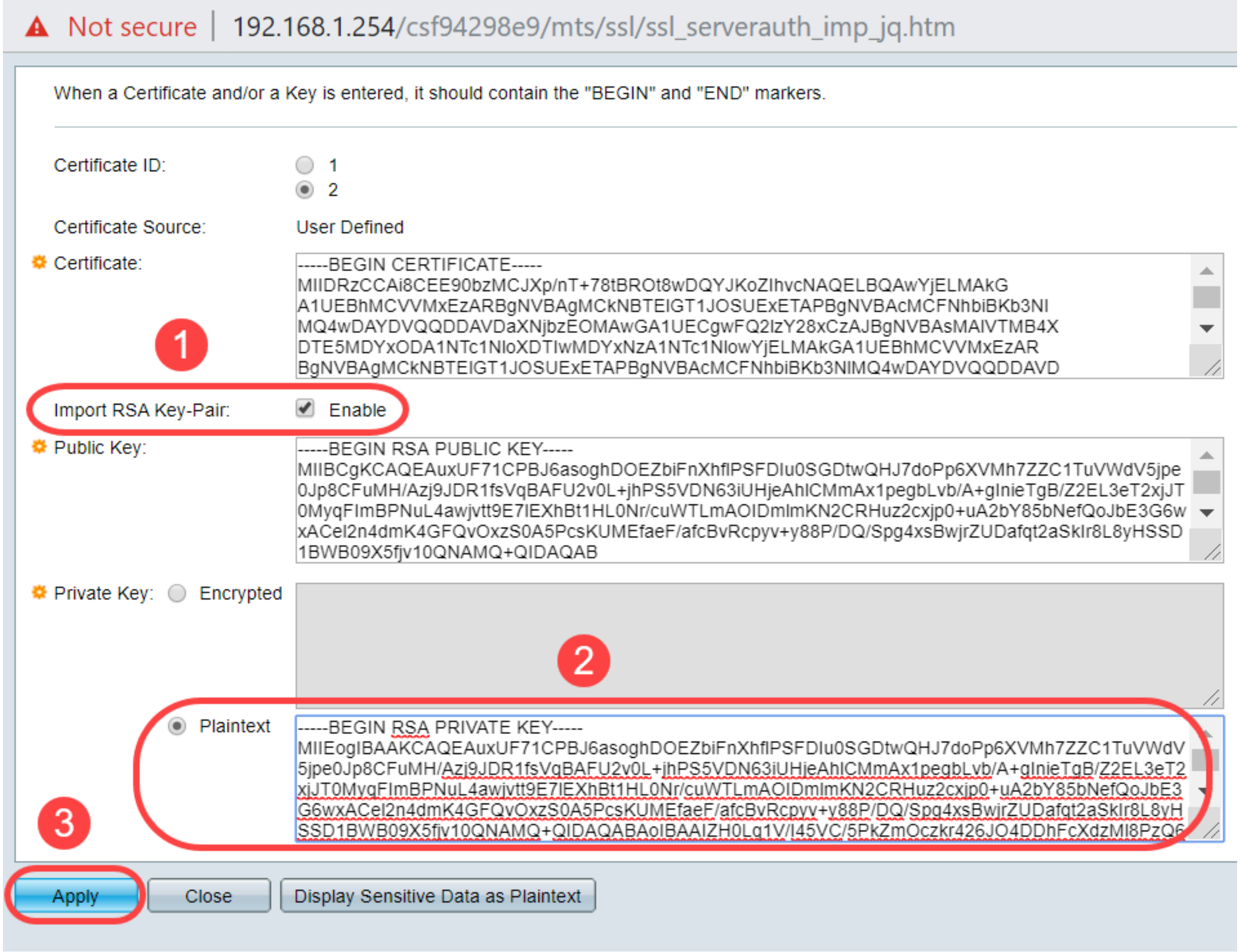
SSL Active Certificate Number: ● 1 ○ 2

SSL Server Key Table

□	Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
□	1	0.0.0.0						2017-Nov-08	2018-Nov-08	Auto Generated
☑	2	Cisco	US	Cisco	San Jose	California	US	2019-Mar-13	2020-Mar-12	User Defined

Step 11

On the new pop-up window, enable *Import RSA Key-Pair* option and paste the private key (copied in step 9) in plaintext format. Click **Apply**.



Not secure
192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_imp_jq.htm
1
2
3
Apply
Close
Display Sensitive Data as Plaintext

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
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xCzAJBgNVBAsMAIVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCkNBTEIGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: ☑ Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xACel2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSklr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Private Key: ○ Encrypted

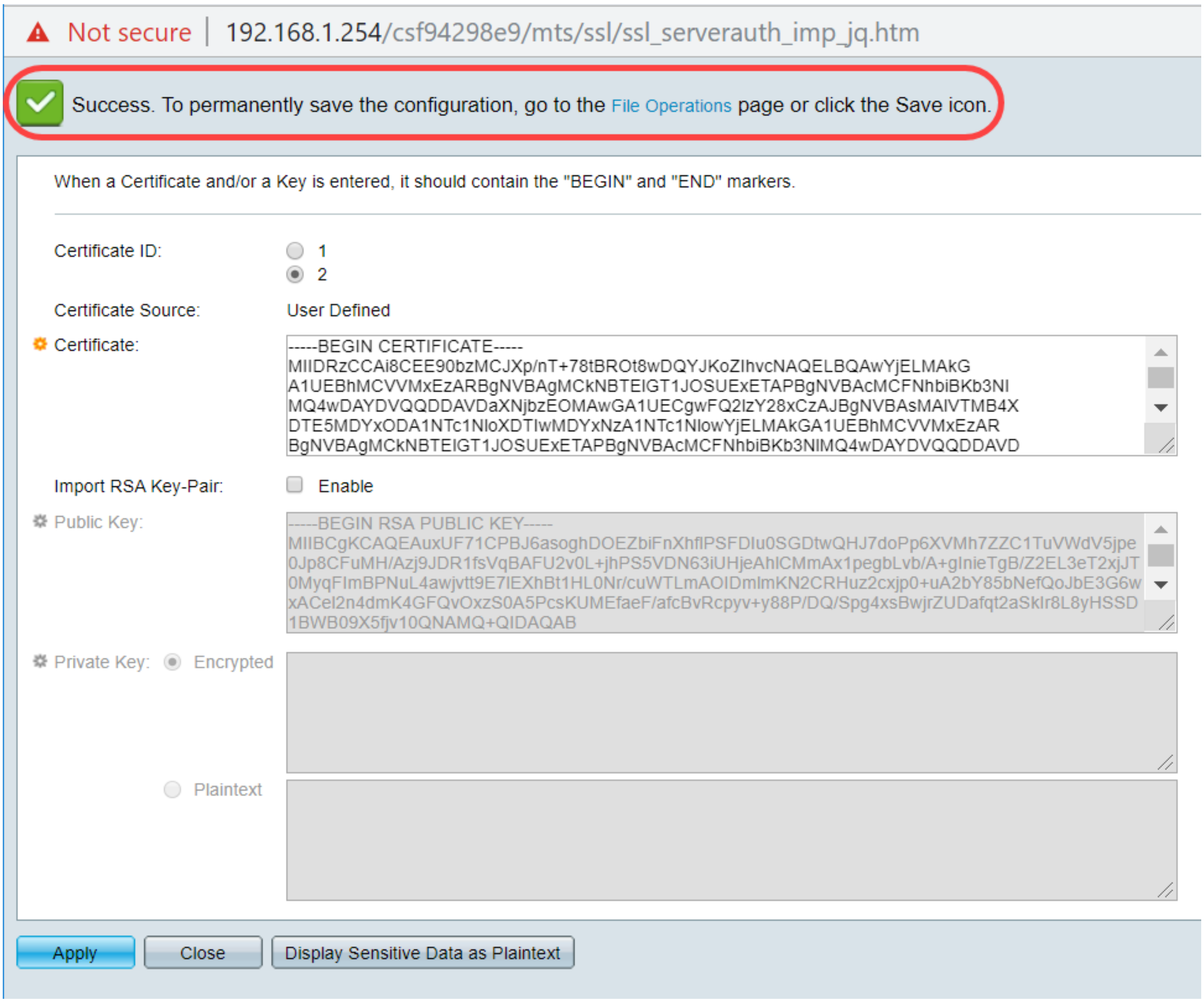
● Plaintext

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV
5jpe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2
xjJT0MyqFImBPNuL4awjvtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3
G6wxACel2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSklr8L8yH
SSD1BWB09X5fjv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PkZmOczkr426JO4DDhFcXdzMI8PzQ6
```

In this example the key word, *RSA*, is included at the *BEGIN* and *END* of the *Public Key*.

Step 12

You will see the success notification on the screen. You may close this window and save the configuration on the switch.


Not secure | 192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_imp_jq.htm

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
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xCzAJBgNVBAsMAIVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCkNBTEIGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: □ Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xACel2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSklr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Private Key: ● Encrypted

○ Plaintext

Possible Errors

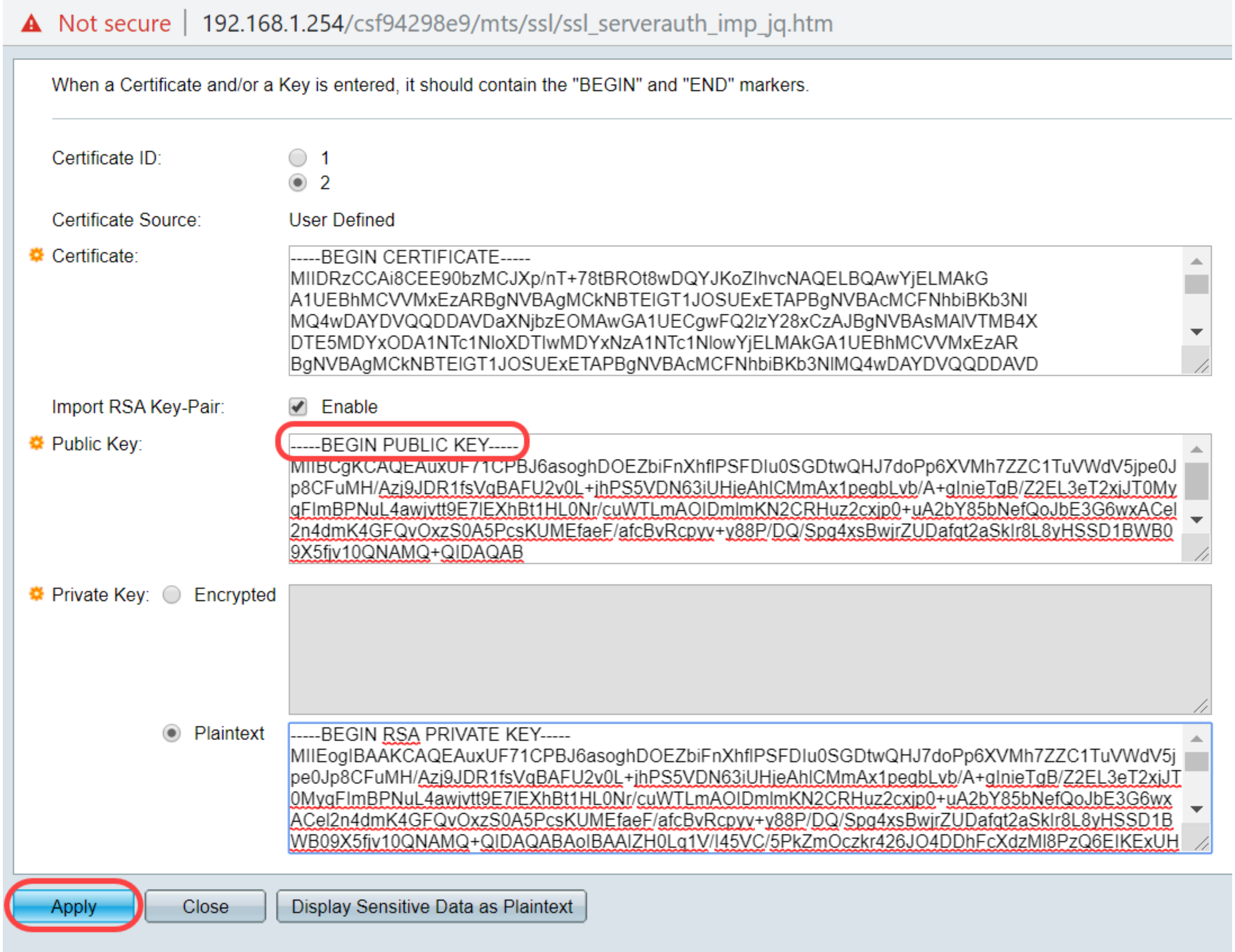
The errors discussed pertain to the public key. Normally there are two types of public key formats that are used:

1. RSA Public Key file (PKCS#1): This is specific for RSA keys.
It starts and ends with the tags:
-----BEGIN RSA PUBLIC KEY-----
BASE64 ENCODED DATA
-----END RSA PUBLIC KEY-----

2. Public Key file (PKCS#8): This is a more generic key format that identifies the type of public key and contains the relevant data.
It starts and ends with the tags:
-----BEGIN PUBLIC KEY-----
BASE64 ENCODED DATA
-----END PUBLIC KEY-----

Key header is missing error

Scenario 1: You generated the certificate from a third-party CA. You copied and pasted the Public Key and clicked **Apply**.



Not secure | 192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_imp_jq.htm

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
A1UEBhMCVVMxEzARBgNVBAgMCkNBTElGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xCzAJBgNVBAsMAlVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCkNBTElGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: ☑ Enable

Public Key:

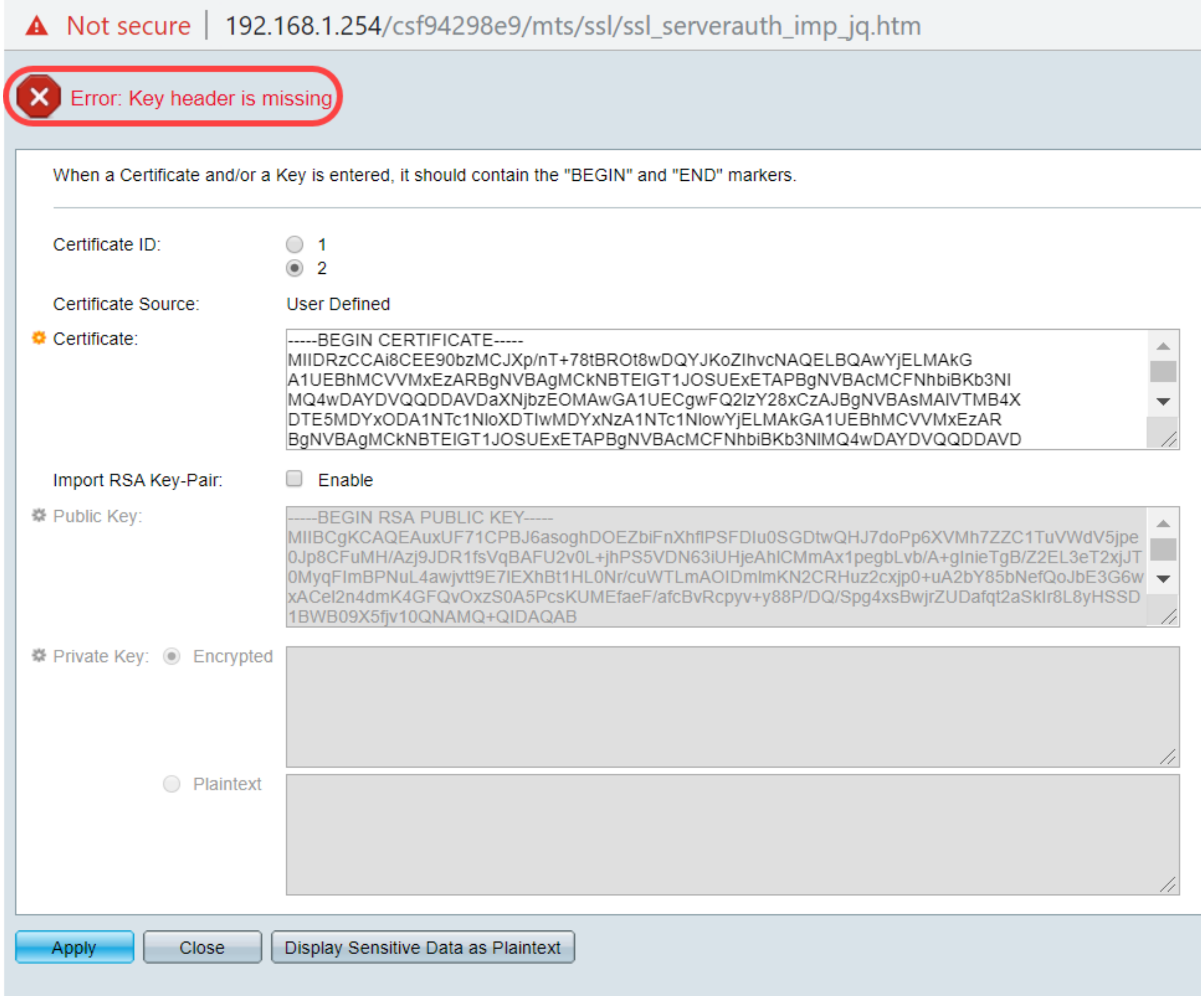
```
-----BEGIN PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe0J
p8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT0My
qFImBPNuL4awjvtt9E7lEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel
2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSkIr8L8yHSSD1BWB0
9X5fjv10QNAMQ+QIDAQAB
```

Private Key: ○ Encrypted

● Plaintext

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5j
pe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvtt9E7lEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wx
ACel2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSkIr8L8yHSSD1B
WB09X5fjv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PkZmOczkr426JO4DDhFcXdzMI8PzQ6EIKExUH
```

You received the message, *Error: Key header is missing*. Close the window. A few modifications can be made to make this problem disappear.



Not secure | 192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_imp_jq.htm

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
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xCzAJBgNVBAsMAIVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCkNBTEIGT1JOSUExETAPBgNVBAcMCFNhbiBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: □ Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xACel2n4dmK4GFQvOxzS0A5PcsKUMEfaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjrZUDafqt2aSkIr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Private Key: ● Encrypted

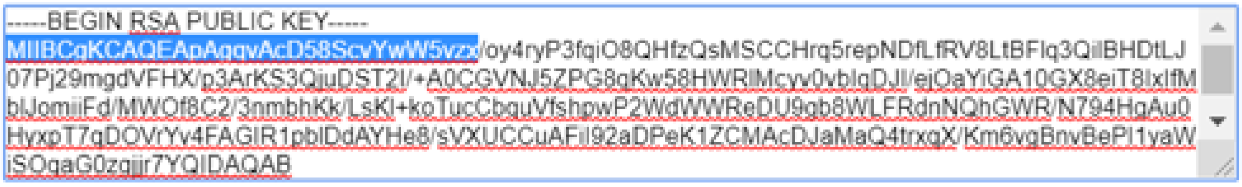
○ Plaintext

To fix this error:

Add the key word, *RSA*, to the beginning of the Public Key: *BEGIN **RSA** PUBLIC KEY*

Add the key word, *RSA*, to the end of the Public Key: *END **RSA** PUBLIC KEY*

Remove the first 32 characters from the key code. The highlighted portion shown below is an example of the first 32 characters.

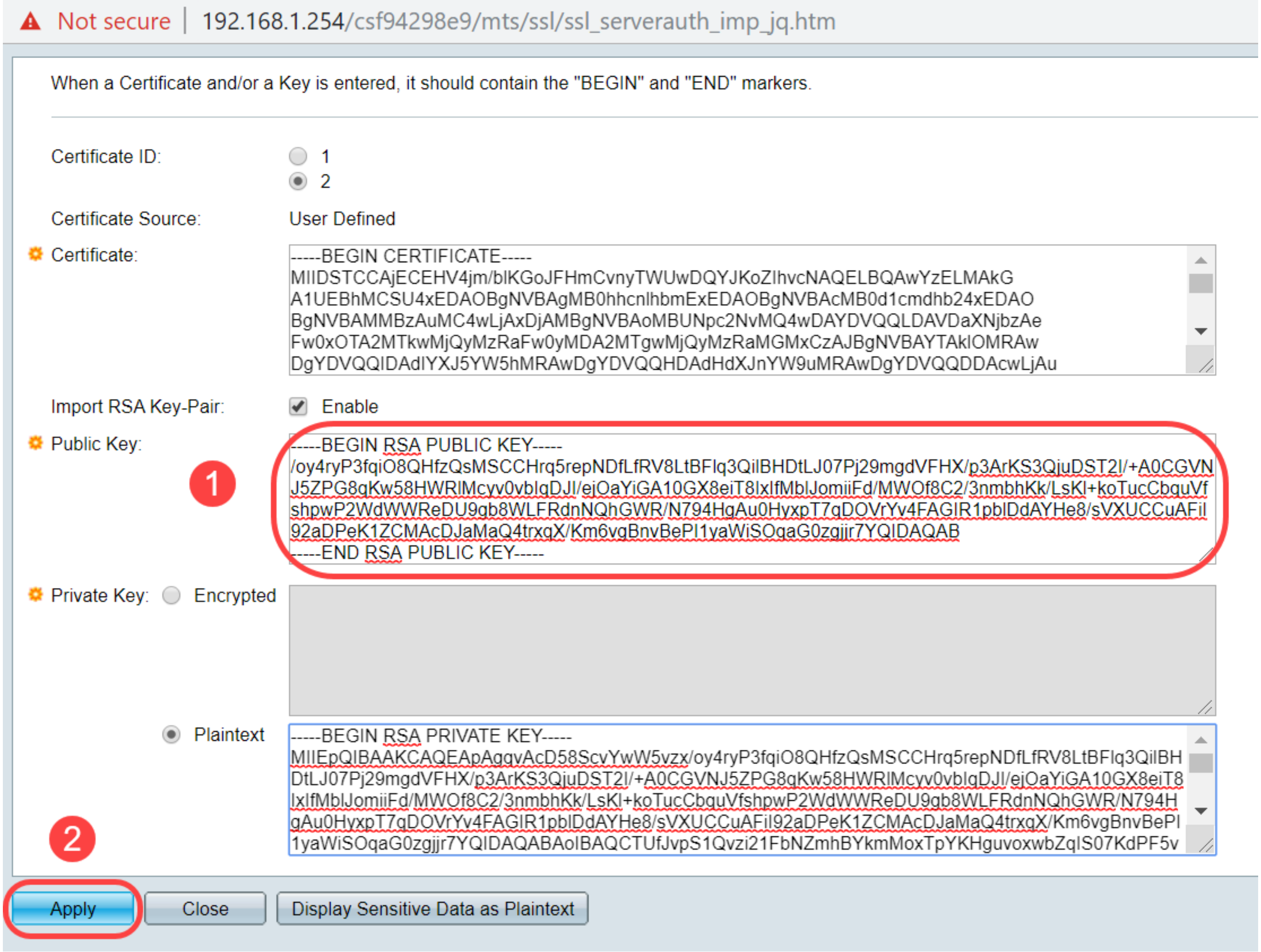


```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEApAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFIq3QiIBHDtLJ
07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJI/ejOaYiGA10GX8eiT8IxIfM
bIJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794HqAu0
HyxpT7qDOVrYv4FAGIR1pbIDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trxqX/Km6vgBnvBePI1yaW
iSOqaG0zqjjr7YQIDAQAB
```

When you apply the settings, you will not get the *Key header is missing* error in most cases.

Failed to load public key error

Scenario 2: You generated a certificate on one switch and imported it onto another switch. You copied and pasted the Public Key after removing the first 32 characters and clicked **Apply**.


Not secure | 192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_imp_jq.htm

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:

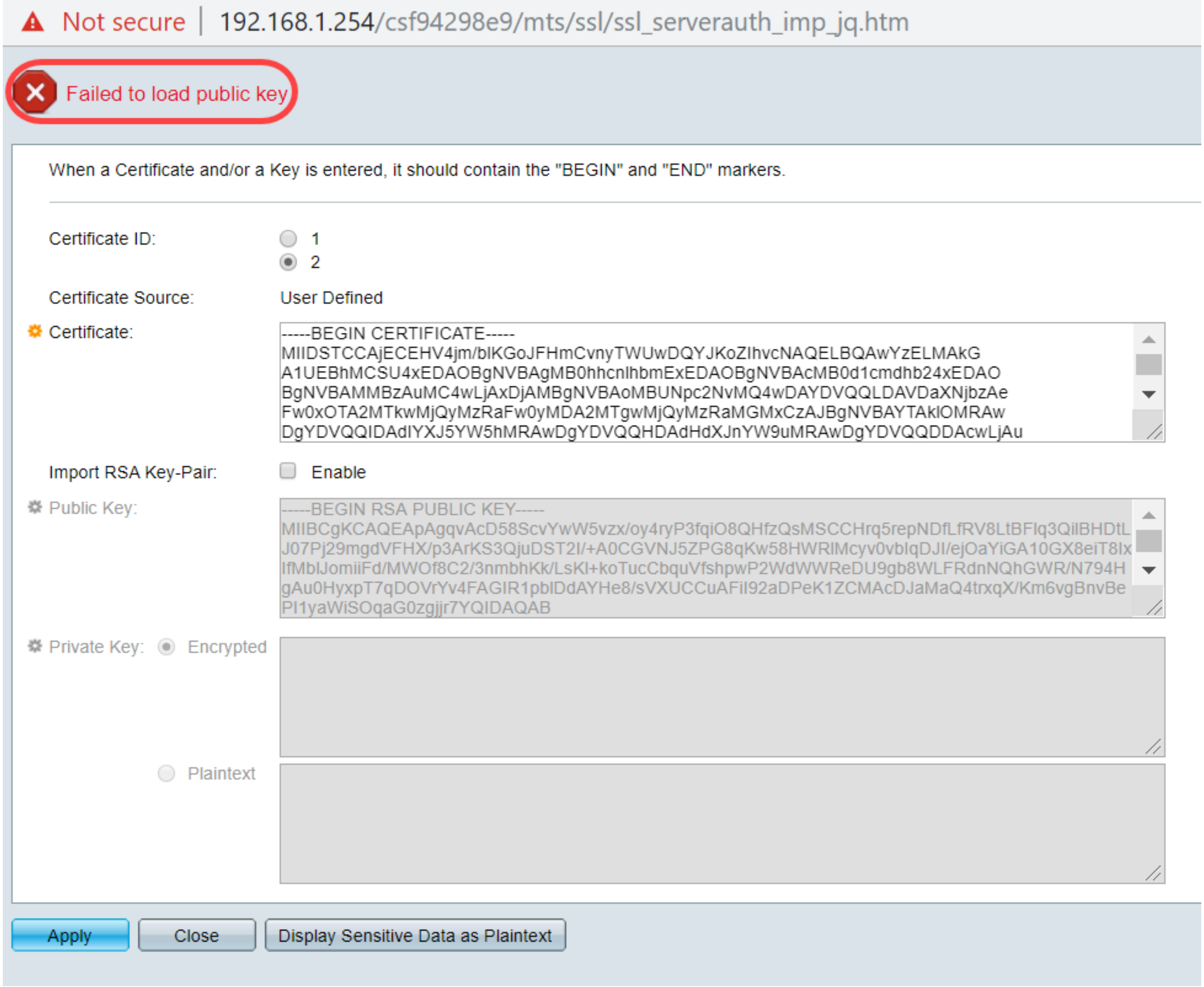
```
-----BEGIN RSA PUBLIC KEY-----
/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFlq3QilBHDtLJ07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVN
J5ZPG8qKw58HWRlMcyv0vblqDJl/ejOaYiGA10GX8eiT8lxlfMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVf
shpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794HgAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil
92aDPeK1ZCMAcDJaMaQ4trxqX/Km6vgBnvBePl1yaWiSOqaG0zgjjr7YQIDAQAB
-----END RSA PUBLIC KEY-----
```

Private Key: ○ Encrypted

● Plaintext

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEApAggvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFlq3QilBH
DtLJ07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRlMcyv0vblqDJl/ejOaYiGA10GX8eiT8
lxlfMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVfshpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794H
gAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trxqX/Km6vgBnvBePl
1yaWiSOqaG0zgjjr7YQIDAQABAoIBAQCTUfJvpS1Qvzi21FbNZmhBYkmMoxTpYKHguvoxwbZqIS07KdPF5v
```

You got the *Failed to load public key* error on the screen.



Not secure | 192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_imp_jq.htm

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/bIKGoJFHmCvnyTWUwDQYJKoZIhvcNAQELBQAwYzELMAkG
A1UEBhMCSU4xEDAOBgNVBAgMB0hhcnlhbmExEDAOBgNVBAcMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMxCzAJBgNVBAYTAklOMRAw
DgYDVQQIDAdIYXJ5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu
```

Import RSA Key-Pair: □ Enable

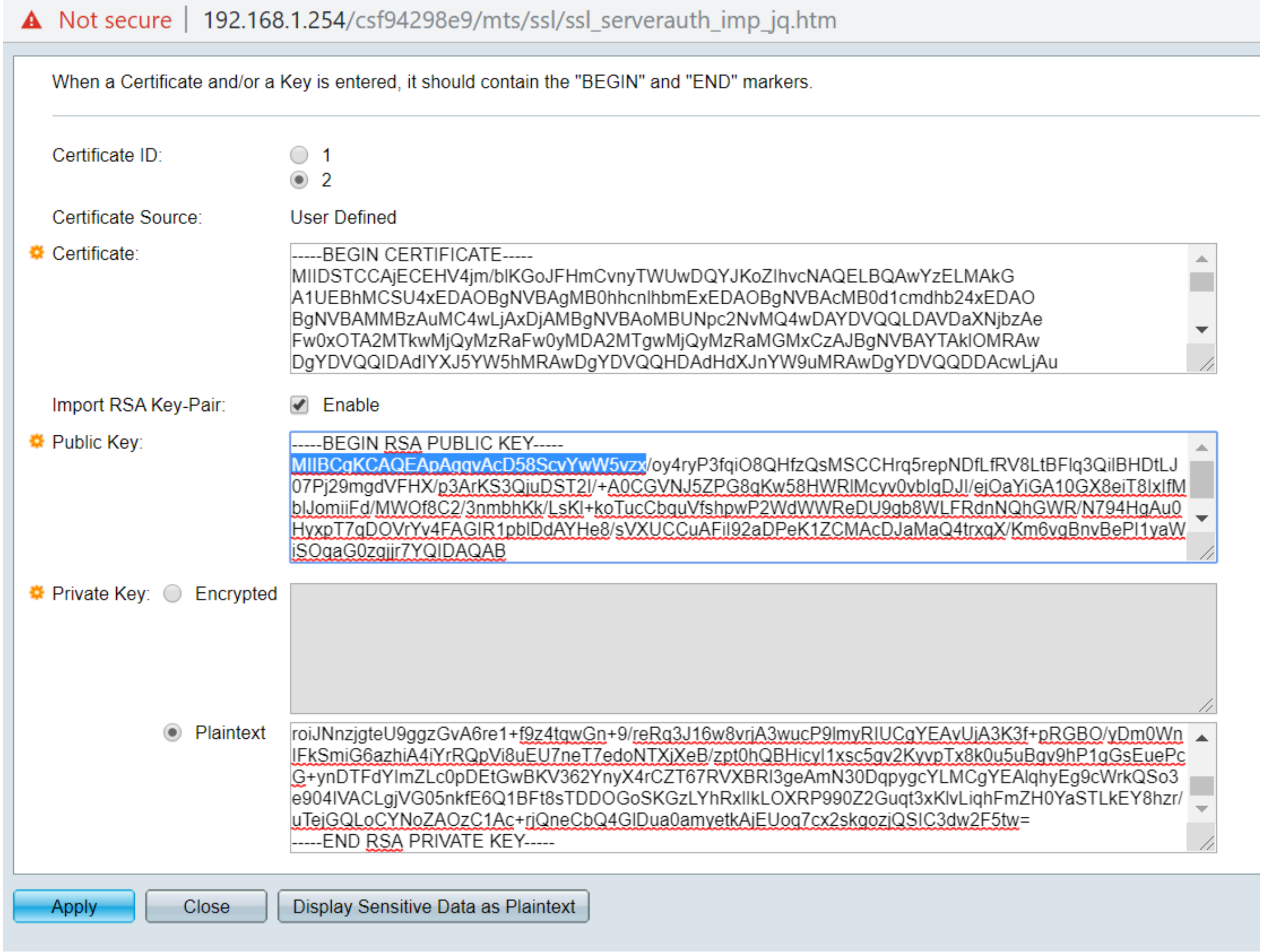
Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEApAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFIq3QilBHDtL
J07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJI/ejOaYiGA10GX8eiT8Ix
IfMblJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794H
gAu0HyxpT7qDOVrYv4FAGIR1pbIDdAYHe8/sVXUCCuAFiI92aDPeK1ZCMAcDJaMaQ4trxqX/Km6vgBnvBe
PI1yaWiSOqaG0zgjjr7YQIDAQAB
```

Private Key: ● Encrypted

○ Plaintext

To fix this error, DO NOT delete the first 32 characters of the public key in this case.



Not secure | 192.168.1.254/csf94298e9/mts/ssl/ssl_serverauth_imp_jq.htm

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/bIKGoJFHmCvnyTWUwDQYJKoZIhvcNAQELBQAwYzELMAkG
A1UEBhMCSU4xEDAOBgNVBAgMB0hhcnlhbmExEDAOBgNVBAcMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMxCzAJBgNVBAYTAklOMRAw
DgYDVQQIDAdIYXJ5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu
```

Import RSA Key-Pair: ☑ Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEApAqqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfRV8LtBFIq3QilBHDtLJ
07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVNJ5ZPG8qKw58HWRlMcyv0vbIqDJl/ejOaYiGA10GX8eiT8IxIfM
bIJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVfshpwP2WdWWReDU9gb8WLFRdnNQhGWR/N794HgAu0
HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trxqX/Km6vgBnvBePl1yaW
iSOqaG0zqjjr7YQIDAQAB
```

Private Key: ○ Encrypted

● Plaintext

```
roiJNnzjgteU9ggzGvA6re1+f9z4tqwGn+9/reRq3J16w8vrjA3wucP9lmyRIUCgYEAvUjA3K3f+pRGBO/yDm0Wn
lFkSmiG6azhiA4iYrRQpVi8uEU7neT7edoNTXjXeB/zpt0hQBHicyl1xsc5gv2KyvpTx8k0u5uBgv9hP1gGsEuePc
G+ynDTFdYlmZLc0pDEtGwBKV362YnyX4rCZT67RVXBRl3geAmN30DqpygcYLMCgYEAlqhyEg9cWrkQSo3
e904lVACLgjVG05nkfE6Q1BFt8sTDDOGoSKGzLYhRxllkLOXRP990Z2Guqt3xKlvLiqhFmZH0YaSTLkEY8hzr/
uTejGQLoCYNoZAOzC1Ac+rjQneCbQ4GlDua0amyetkAjEUoq7cx2skgozjQSIC3dw2F5tw=
-----END RSA PRIVATE KEY-----
```

Import using CLI

Step 1

To import certificate using CLI, enter the following command.

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

Certificate 2 is imported in this example.

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

Step 2

Paste the input; **add a period (.)** on a separate line after the input.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC/rZQ6f0rj8neA
...truncated 24 lines....
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+52lD/GokmU
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAv62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkfT0l
...truncated 3 lines....
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB
```

```
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIIFvTCCBKWgAwIBAgIRAOOBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw
---truncated 28 lines...
8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVFf0cUzqXwOJcsTrMV
JDPtnbKXG56w0Trecu6UQ9HsUBoDQnlsN5ZBHt1VyjAP
-----END CERTIFICATE-----
.
Certificate imported successfully
Issued by : C=xx, ST=Gxxxxx, L=xx, O=xx CA Limited, CN=xx RSA Organization Validation Secure
Server CA
Valid From: Jun 14 00:00:00 2017 GMT
Valid to: Sep 11 23:59:59 2020 GMT
Subject: C=DE/postalCode=xxx, ST=xx, L=xx/street=xxx 2, O=xxx , OU=IT, CN=*.kowi.eu
SHA Fingerprint: xxxxxx
```

Conclusion

You have now learned the steps to successfully import a certificate on the Sx350 and Sx550X series switches using the GUI and CLI.