

Como importar certificado nos switches Sx350 e Sx50X Series

Objetivo

Este objetivo deste documento é fornecer as etapas para importar com êxito um certificado nos switches das séries Sx350 e Sx550X usando a Interface Gráfica do Usuário (GUI - Graphical User Interface) e a Interface de Linha de Comando (CLI - Command Line Interface).

Table Of Contents

- [Introduction](#)
- [Dispositivos aplicáveis e versão de software](#)
- [Prerequisites](#)
- [Importar usando GUI](#)
- [Possíveis erros Erro de cabeçalho de chave ausenteFalha ao carregar erro de chave pública](#)
- [Importar usando CLI](#)
- [Conclusão](#)

Introduction

Um dos problemas encontrados ao importar um certificado em switches Sx350 e Sx550X é que o usuário enfrenta *o cabeçalho da chave ausente* e/ou *falha ao carregar* erros *de chave pública*. Este documento explicará como ultrapassar esses erros para importar com êxito um certificado. Um certificado é um documento eletrônico que identifica um indivíduo, um servidor, uma empresa ou outra entidade e associa essa entidade a uma chave pública. Os certificados são usados em uma rede para fornecer acesso seguro. Os certificados podem ser autoassinados ou assinados digitalmente por uma autoridade de certificação externa (AC). Um certificado autoassinado, como o nome indica, é assinado por seu próprio criador. As CAs gerenciam solicitações de certificado e emitem certificados para entidades participantes, como hosts, dispositivos de rede ou usuários. Um certificado digital assinado por CA é considerado padrão do setor e mais seguro.

Dispositivos aplicáveis e versão de software

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

Prerequisites

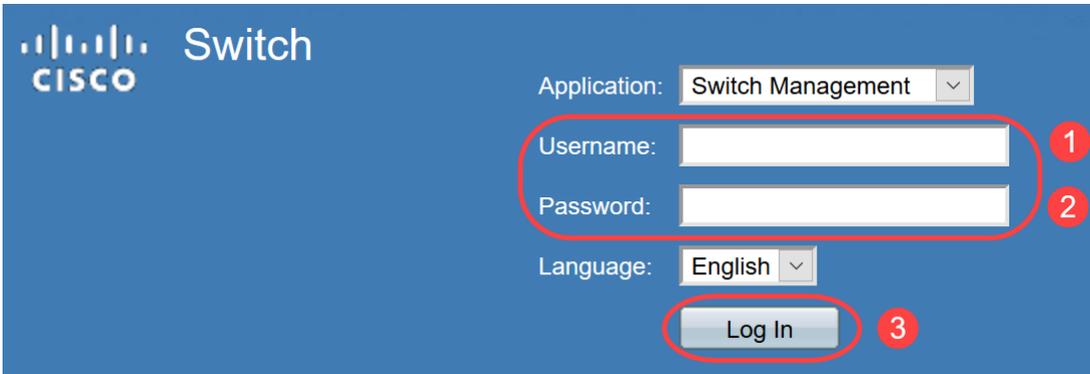
Você deve ter um certificado de Autoridade de Certificação (CA) ou autoassinado. As etapas para obter um certificado autoassinado estão incluídas neste artigo. Para saber mais sobre certificados

CA, clique [aqui](#).

Importar usando GUI

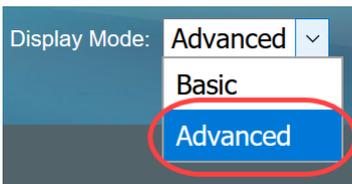
Passo 1

Faça login na GUI do switch digitando seu *nome de usuário* e *senha*. Clique em **Login**.



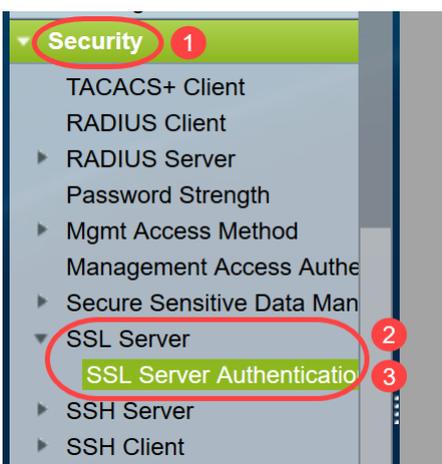
Passo 2

No *Modo de exibição* na parte superior direita da GUI, escolha **Avançado** usando a opção suspensa.



Etapa 3

Navegue até **Security > SSL Server > SSL Server Authentication**.



Passo 4

Selecione um dos certificados que é *gerado automaticamente*. Selecione a *ID de certificado* 1 ou 2 e clique no botão **Editar**.

SSL Server Authentication Settings

SSL Active Certificate Number: 1
 2

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 type="checkbox"/>	1	0.0.0.0						2015-Dec-10	2016-Dec-09	Auto Generated
<input checked="" type="checkbox"/>	2	0.0.0.0						2015-Dec-10	2016-Dec-09	Auto Generated

Etapa 5

Para gerar um certificado autoassinado, na nova janela pop-up, habilite *Recriar chave RSA* e insira os seguintes parâmetros:

Comprimento da chave

Nome comum

Unidade organizacional

Nome da organização

Local

Estado

País

Duration

Clique em **Gerar**.

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

Certificate ID: 1
 2

Regenerate RSA Key: 1

Key Length: 2048 bits
 3072 bits 2

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) 3

Generate Close

Você também pode criar um certificado de uma CA de terceiros.

Etapa 6

Agora você poderá ver o certificado *definido pelo usuário* na *Tabela de chaves do servidor SSL*. Selecione o certificado recém-criado e clique em **Detalhes**.

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 type="checkbox"/>	1	0.0.0.0						2017-Nov-08	2018-Nov-08	Auto Generated
<input checked="" type="checkbox"/> 1	2	Cisco	US	Cisco	San Jose	California	US	2019-Mar-13	2020-Mar-12	User Defined

Edit... Generate Certificate Request... Import Certificate... **Details...** Delete 2

Etapa 7

Na janela pop-up, você poderá ver os detalhes *Certificado*, *Chave pública* e *Chave privada (criptografada)*. Você pode copiá-los em um arquivo do bloco de notas separado. Clique em **Exibir dados confidenciais como texto sem formatação**.

SSL Details - Google Chrome

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

Certificate ID: 2

Certificate: -----BEGIN CERTIFICATE-----
MIIDRzCCAi8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhbikB3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2l2Y28xCzAJBgNVBAsMAiVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhbikB3NIMQ4wDAYDVQQDDAVD

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1peglvb/A+gInieTgB/Z2EL3eT2xJT0MyqFl
mBPNuL4awjvt9E7IEXhBt1HL0Nr/cuVTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel2n4d
mK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpyv+y88P/DQ/Spq4xsBwjRZUDafqt2aSkIrl8yHSSD1BWB09X5fjv1
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-----
oIAbmqdHV/WOCsWTno8EsO1FXk81mva9RGX2rBMhCDJzeZjmj6aa8y4rDJmcrF98ri5CBJ+WV5KbjvH3UsR
Km1b7W0jcoh7CYBkGIAxe5p24pgXf5QWPH2830A0qY0dAiinwIZkwPat9BUkVV913eY1tHzHFN/1kvOpvKggus
oO85U5FqFMFUpFD94YDqQ+Xpp+LDuiVPjgFh6DCXq2wBnFBzws7doSHMBU77LHOFnWybmzzmT63DNFN
goUlp0nwskdPoigihLjrtESSJ5x/tizkfJx2rGreHz2AMwa1urtJv/+ysGu+R4T0++1RkiUJISCYZW7kmtwFdlchMBv1
YJWPQZ0l9znTXOXgZQbtR1MGI5NqrTb1V11Ositb63dqRQKJ4XUdTldQpRPgrhTrXUwXHgegCpBtqLg1D6Hp

Close Display Sensitive Data as Plaintext

Passo 8

Uma janela pop-up será aberta para confirmar a exibição da chave privada como texto não criptografado e clique em **OK**.

Confirm Display Method Change - Google C...

Not secure | 192.168.1.254/csf94298e9/mts/kubrick/co...

 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

OK Cancel

Passo 9

Agora você poderá ver a *chave privada* no formato de texto simples. Copie essa saída de texto simples em um arquivo do bloco de notas. Clique em Close.

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

Certificate ID: 2

Certificate: -----BEGIN CERTIFICATE-----
MIIDRzCCAI8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2l2Y28xCzAJBgNVBAsMAiVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIIMQ4wDAYDVQQDDAVD

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCGKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjT0MyqF1
mBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel2n4d
mK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcpyv+y88P/DQ/Spq4xsBwjrzUDafqt2aSkIr8L8yHSSD1BWB09X5fjv1
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-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0Jp
e0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjT0
MyqF1mBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxAC
el2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcpyv+y88P/DQ/Spq4xsBwjrzUDafqt2aSkIr8L8yHSSD1BWB0
9X5fjv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PkZmOczkr426JO4DDhFcXdzMI8PzQ6EIKExUH0YpV

Close Display Sensitive Data as Encrypted

Passo 10

Selecione o certificado *definido pelo usuário* recém-criado e clique em **Importar certificado**.

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 type="checkbox"/>	1	0.0.0.0						2017-Nov-08	2018-Nov-08	Auto Generated
<input checked="" type="checkbox"/>	2	Cisco	US	Cisco	San Jose	California	US	2019-Mar-13	2020-Mar-12	User Defined

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

Passo 11

Na nova janela pop-up, ative a opção *Importar par de chaves RSA* e cole a chave privada (copiada na etapa 9) no formato de texto simples. Clique em **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: 1

```
-----BEGIN CERTIFICATE-----
MIIDRzCCAi8CEE90bzMCJXp/nT+78tBROT8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUExETAPBgNVBACMCFNhbIBKb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAiVtMB4X
DTE5MDYxODA1NTc1Ni0XDTIwMDYxNzA1NTc1Ni0wYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUExETAPBgNVBACMCFNhbIBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEXhB1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypyv+y88P/DQ/Spg4xsBwjRZUDafqt2aSkir8L8yHSSD
1BWB09X5fv10QNAMQ+QIDAQAB
```

Private Key: Encrypted

2

Plaintext

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV
5jpe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2
xjJT0MyqFImBPNuL4awjvt9E7IEXhB1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3
G6wxAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypyv+y88P/DQ/Spg4xsBwjRZUDafqt2aSkir8L8yH
SSD1BWB09X5fv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PKZmOczkr426JO4DdhFcXdzMI8PzQ6
```

3

Neste exemplo, a palavra-chave, *RSA*, está incluída no *BEGIN* e *END* da *chave pública*.

Etapa 12

Você verá a notificação de sucesso na tela. Você pode fechar esta janela e salvar a configuração no 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
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lyY28xMzY2ZjEjZjEjZjEj
DTE5MDYxODA1NTc1Ni0xODIwMDYxNzA1NTc1Ni0wYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIb3NIb3NIb3NIb3NIb3NI
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Import RSA Key-Pair: Enable

⚙ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBKgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xACel2n4dmK4GFQvOxZS0A5PcsKUMefaeF/afcBvRcpv+y88P/DQ/Spg4xsBwjZUDafqt2aSkIr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

⚙ Private Key: Encrypted Plaintext

Apply Close Display Sensitive Data as Plaintext

Possíveis erros

Os erros discutidos pertencem à chave pública. Normalmente, há dois tipos de formatos de chave pública que são usados:

1. Arquivo de chave pública RSA (PKCS#1): Isso é específico para chaves RSA.

Começa e termina com as marcas:

—INICIAR A CHAVE PÚBLICA RSA—

DADOS CODIFICADOS BASE64

—ENCERRA A CHAVE PÚBLICA RSA—

2. Arquivo de chave pública (PKCS#8): Trata-se de um formato de chave mais genérico que identifica o tipo de chave pública e contém os dados relevantes.

Começa e termina com as marcas:

—INICIAR CHAVE PÚBLICA—

DADOS CODIFICADOS BASE64

—CHAVE PÚBLICA FINAL—

Erro de cabeçalho de chave ausente

Cenário 1: Você gerou o certificado de uma CA de terceiros. Você copiou e colou a chave pública e clicou em **Aplicar**.

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+78tBR0t8wDQYJKoZIhvcNAQELBQAwYjELMAkG  
A1UEBHMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhbIBKb3NI  
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xCzAJBgNVBAsMAIVTMB4X  
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBHMCVVMxEzAR  
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhbIBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

Public Key:

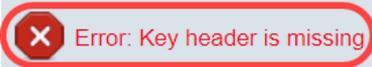
```
-----BEGIN PUBLIC KEY-----  
MIIBBgKCAQEAAuxUF71CPBJ6asoghDOEZbifnXhfiPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0J  
p8CFuMH/Azi9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peqLvb/A+gInieTqB/Z2EL3eT2xiJT0My  
qFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel  
2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafqt2aSkIrl8yHSSD1BWB0  
9X5fiv10QNAMQ+QIDAQAB
```

Private Key: Encrypted

Plaintext

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEogIBAAKCAQEAAuxUF71CPBJ6asoghDOEZbifnXhfiPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5j  
pe0Jp8CFuMH/Azi9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peqLvb/A+gInieTqB/Z2EL3eT2xiJT  
0MyqFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wx  
ACel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafqt2aSkIrl8yHSSD1B  
WB09X5fiv10QNAMQ+QIDAQABAOIBAAIzH0Lq1V/I45VC/5PkZmOczkr426JO4DdhFcXdzMI8PzQ6EIKExUH
```

Você recebeu a mensagem, *Erro: Cabeçalho da chave ausente*. Feche a janela. Algumas modificações podem ser feitas para que esse problema desapareça.



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
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhbIBk3NI
MQ4wDAYDVQQDDAVDAXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAIVTMB4X
DTE5MDYxODA1NTc1NloXDTEwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhbIBk3NIMQ4wDAYDVQQDDAVD

Import RSA Key-Pair: Enable

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDiu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhICMmAxi1peglvB/A+glnieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcpyv+y88P/DQ/Spg4xsBwjrzUDafqt2aSkIrl8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Para corrigir este erro:

Adicione a palavra-chave, RSA, ao início da chave pública: *INICIAR CHAVE PÚBLICA RSA*

Adicione a palavra-chave, RSA, ao fim da chave pública: *CHAVE PÚBLICA FINAL RSA*

Remova os primeiros 32 caracteres do código de chave. A parte destacada abaixo é um exemplo dos primeiros 32 caracteres.

```
-----BEGIN RSA PUBLIC KEY-----  
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDiu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe  
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhICMmAxi1peglvB/A+glnieTgB/Z2EL3eT2xjJT  
0MyqFImBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w  
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcpyv+y88P/DQ/Spg4xsBwjrzUDafqt2aSkIrl8yHSSD  
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Ao aplicar as configurações, você não obterá o erro *Cabeçalho da chave ausente* na maioria dos casos.

Falha ao carregar erro de chave pública

Cenário 2: Você gerou um certificado em um switch e o importou em outro switch. Você copiou e

colou a chave pública após remover os primeiros 32 caracteres e clicar em **Aplicar**.

▲ 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
A1UEBhMCSU4xEDA0BgNVBAGMB0hcnlnhbmExEDA0BgNVBACMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxZjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMrCzAJBgNVBAYTAkIOMRAw
DgYDVQQIDAdiYXJ5J5Yw5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu
```

Import RSA Key-Pair: Enable

★ Public Key: 1

```
-----BEGIN RSA PUBLIC KEY-----
/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfrV8LtBFq3QilBHDTLJ07Pj29mgdVFHX/p3ArKS3QiuDST2I/+A0CGVN
J5ZPG8qKw58HWRIMcyy0vblqDJl/ejOaYiGA10GX8eiT8lxIfMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVf
shpwP2WdWWReDU9qb8WLFERdnNQhGWR/N794HqAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil
92aDPeK1ZCMAcDJaMaQ4trqxX/Km6vgBnvBePl1yaWiSOqaG0zgjir7YQIDAQAB
-----END RSA PUBLIC KEY-----
```

★ Private Key: Encrypted Plaintext 2

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEApAqgvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfrV8LtBFq3QilBH
DtLJ07Pj29mgdVFHX/p3ArKS3QiuDST2I/+A0CGVNJ5ZPG8qKw58HWRIMcyy0vblqDJl/ejOaYiGA10GX8eiT8
lxIfMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVfshpwP2WdWWReDU9qb8WLFERdnNQhGWR/N794H
qAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqxX/Km6vgBnvBePl
1yaWiSOqaG0zgjir7YQIDAQABAoIBAQCTUfJvpS1Qvzi21FbNZmhBYkmMoxTpYKHguvowxbZqIS07KdPF5v
```

Apply

Você recebeu o erro *Falha ao carregar chave pública* na tela.



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
A1UEBhMCSU4xEDAObGNVBAgMB0hhcnIhbmExEDAObGNVBAcMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxZDpAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLEDAVDAxNjBzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMrCzAJBGNVBAYTAkiOMRAw
DgYDVQQIDAdiYXJ5J5YW5hMRAwDgYDVQQHDAAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

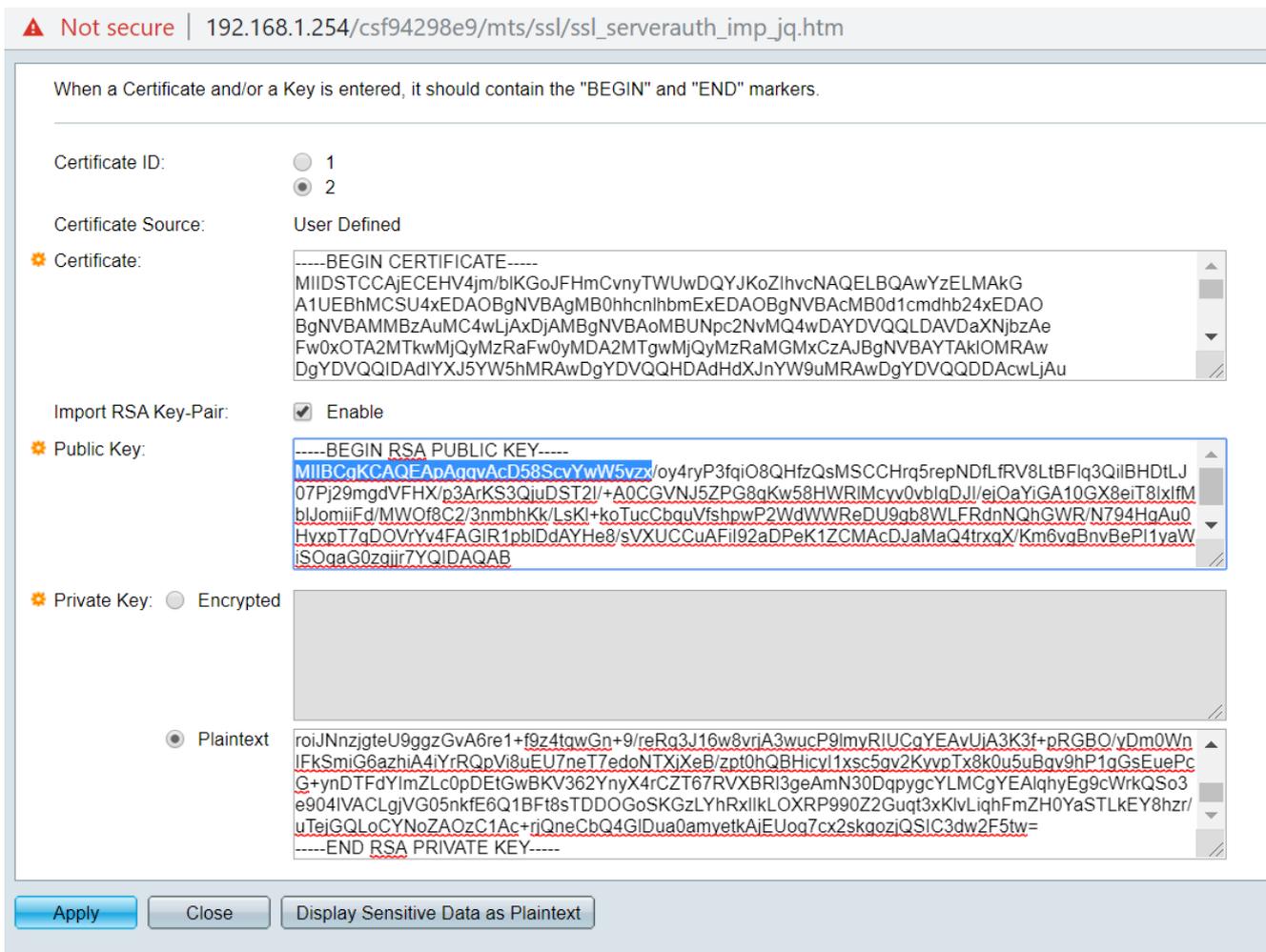
Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCAgKCAQEAqAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLrV8LtbFIq3QilBHDtL
J07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJI/ejOaYIGA10GX8eif8lx
lfMblJomiiF/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWReDU9gb8WLFrdnNQhGWR/N794H
gAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBe
PI1yaWiSOqaG0zgjir7YQIDAQAB

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Para corrigir esse erro, NÃO exclua os primeiros 32 caracteres da chave pública nesse caso.



Importar usando CLI

Passo 1

Para importar certificado usando CLI, digite o seguinte comando.

```
switch(config)#crypto certificate [número do certificado] import
```

O certificado 2 é importado neste exemplo.

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

Passo 2

Colar a entrada; adicione um ponto (.) em uma linha separada após a entrada.

```
--INICIAR A CHAVE PRIVADA RSA--
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC/rZQ6f0rj8neA
...truncada 24 linhas...
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+521D/GokmU
--ENCERRA A CHAVE PRIVADA RSA--
--INICIAR A CHAVE PÚBLICA RSA--
MIIBCgKCAQEA...v62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkft0l
...truncada 3 linhas...
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB
```

–ENCERRA A CHAVE PÚBLICA RSA–

–INICIAR CERTIFICADO–

MIIFvTCCBKWgAwIBAgIRA0OBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw

–truncada 28 linhas...

8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVff0cUzqXwOJcsTrMV

JDptnbKXG56w0Trecu6UQ9HsUBoDQnlsN5ZBht1VyjAP

–CERTIFICADO FINAL–

.

Certificado importado com êxito

Emitido por: C=xx, ST=Gxxxx, L=xx, O=xx CA Limited, CN=xx RSA Organization Validation Secure Server CA

Válido de: Jun 14 00:00:00 2017 GMT

Válido para: 11 de setembro 23:59:59 2020 GMT

Assunto: C=DE/postalCode=xxx, ST=xx, L=xx/street=xxx 2, O=xxx, OU=IT, CN=*.kowi.eu

Impressão digital SHA: xxxxxx

Conclusão

Agora você aprendeu as etapas para importar com êxito um certificado nos switches das séries Sx350 e Sx550X usando a GUI e a CLI.