

Cómo importar el certificado en los switches Sx350 y Sx550X Series

Objetivo

Este objetivo de este documento es proporcionar los pasos para importar con éxito un certificado en los switches de las series Sx350 y Sx550X utilizando la interfaz gráfica de usuario (GUI) y la interfaz de línea de comandos (CLI).

Table Of Contents

- [Introducción](#)
- [Dispositivos y versión de software aplicables](#)
- [Prerequisites](#)
- [Importar mediante la GUI](#)
- [Errores posibles Falta el encabezado de la claveError al cargar el error de clave pública](#)
- [Importar mediante CLI](#)
- [Conclusión](#)

Introducción

Uno de los problemas encontrados al importar un certificado en los switches Sx350 y Sx550X es que el usuario se enfrenta a ***un encabezado de clave que falta*** y/o ***no pudo cargar*** errores de ***clave pública***. Este documento explicará cómo superar estos errores para importar un certificado correctamente. Un certificado es un documento electrónico que identifica a una persona, un servidor, una empresa u otra entidad y asocia esa entidad a una clave pública. Los certificados se utilizan en una red para proporcionar acceso seguro. Los certificados pueden ser firmados automáticamente o firmados digitalmente por una autoridad certificadora externa (CA). Un certificado autofirmado, como su nombre indica, está firmado por su propio creador. Las CA administran solicitudes de certificados y emiten certificados a entidades participantes como hosts, dispositivos de red o usuarios. Un certificado digital firmado por CA se considera estándar del sector y más seguro.

Dispositivos y versión de software aplicables

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

Prerequisites

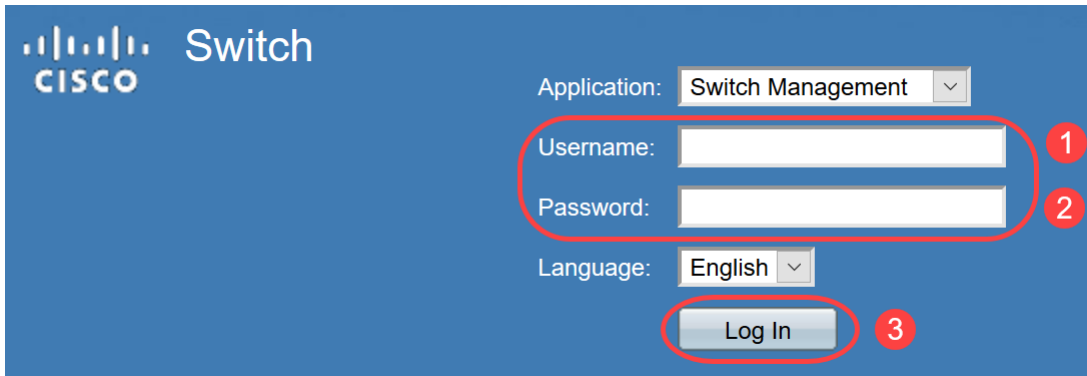
Debe tener un certificado de autoridad certificadora (CA) o autofirmado. En este artículo se

incluyen los pasos para obtener un certificado autofirmado. Para obtener más información sobre los certificados de CA, haga clic [aquí](#).

Importar mediante la GUI

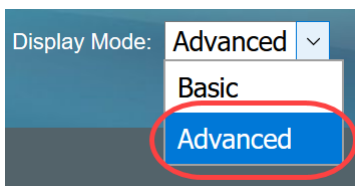
Paso 1

Inicie sesión en la GUI del switch ingresando su *nombre de usuario* y *contraseña*. Haga clic en **Iniciar sesión**.



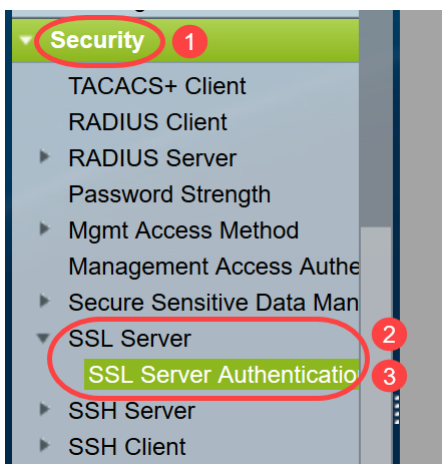
Paso 2

En el *Modo de visualización* en la parte superior derecha de la GUI, elija **Avanzado** usando la opción desplegable.



Paso 3

Vaya a **Security > SSL Server > SSL Server Authentication**.



Paso 4

Seleccione uno de los certificados que se *Generó automáticamente*. Seleccione el *ID de certificado* 1 ó 2 y haga clic en el **botón 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

Paso 5

Para generar un certificado autofirmado, en la nueva ventana emergente active *Regenerar clave RSA* e ingrese los siguientes parámetros:

Longitud de la clave

Nombre común

Unidad de organización

Nombre de la organización

Ubicación

Estado

País

Duration

Haga clic en **Generar**.

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 2
 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) 3

Generate Close

También puede crear un certificado de una CA de terceros.

Paso 6

Ahora podrá ver el certificado *definido por el usuario* bajo la *Tabla de claves de servidor SSL*. Seleccione el certificado recién creado y haga clic en **Detalles**.

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... Detalles... 2 Delete

Paso 7

En la ventana emergente podrá ver los detalles *Certificate*, *Public Key* y *Private Key (Encrypted)*. Puede copiarlos en un archivo de bloc de notas independiente. Haga clic en **Mostrar datos confidenciales como texto sin formato**.

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
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xZzA1UEBhMAIUVMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhbikB3NIMQ4wDAYDVQQDDAVD

Public Key:
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMMaX1pegbLvb/A+gInieTgB/Z2EL3eT2xJT0MyqFl
mBPNuL4awjvt9E7IEXhBt1HL0Nr/cuVTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel2n4d
mK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpyy+y88P/DQ/Spq4xsBwjRZUDafqt2aSkIR8LyHSSD1BWB09X5fjv1
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+VW5KbjvH3UsR
Km1b7W0jcoh7CYBkGIAxe5p24pgXf5QWPH2830A0qY0dAiinwIZkwPat9BUkVV913eY1thzHFN/1kvOpvKggus
oO85U5FqFMFUpFD94YDqQ+Xpp+LDuiVPjgFh6DCXq2wBnFBzws7doSHMBU77LHOFNWybmzzmT63DNFN
goUlp0nwskdPoigilHJrtESSJ5x/tizkfJx2rGreHz2AMwa1urtJv/+ysGu+R4T0++1RkiUJISCYZW7kmtwFdlchMBv1
YJWPQZ0l9znTXOXgZQbtR1MGI5NqrTb1V11Ositb63dqRQKJ4XUdTldQpRPgrhTrXUwXHgegCpBtqLg1D6Hp

Close Display Sensitive Data as Plaintext

Paso 8

Se abrirá una ventana emergente para confirmar la visualización de la clave privada como texto sin formato, haga clic en **Aceptar**.

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

Paso 9

Ahora podrá ver la *clave privada* en formato de texto sin formato. Copie ese resultado de texto sin formato en un archivo de bloc de notas. Haga clic en Close (Cerrar).

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

Certificate ID: 2

Certificate: -----BEGIN CERTIFICATE-----
MIIDRzCCAI8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2l2Y28xZzAxBGgNVBAsMAI
VITMB4XDTE5MDYxODAxNTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBh
MCVVMxEzARBgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NI
MQ4wDAYDVQQDDAVD

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCGKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT0MyqF
lMbpNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel2n4d
mK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpyv+y88P/DQ/Spq4xsBwjrzUDafqt2aSkI8L8yHSSD1BWB09X5fjv1
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/Z2EL3eT2xjJT0
MyqFlMbpNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxAC
el2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpyv+y88P/DQ/Spq4xsBwjrzUDafqt2aSkI8L8yHSSD1BWB0
9X5fjv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PkZmOczkr426JO4DDhFcXdzMI8PzQ6EIKExUH0YpV

Close | Display Sensitive Data as Encrypted

Paso 10

Seleccione el certificado *definido por el usuario* recién creado y haga clic en **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

Paso 11

En la nueva ventana emergente, active la opción *Importar par de claves RSA* y pegue la clave privada (copiada en el paso 9) en formato de texto sin formato. Haga clic en **Apply** (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: 1

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

Import RSA Key-Pair: Enable

Public Key: 2

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xJT
0MyqFImBPNuL4awjvt9E7IEXBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypyv+y88P/DQ/Spg4xsBwjRZUDafqt2aSkIrl8LyHSSD
1BWB09X5fv10QNAMQ+QIDAQAB
```

Private Key: Encrypted

Plaintext 3

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV
5jpe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2
xjT0MyqFImBPNuL4awjvt9E7IEXBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3
G6wxAcEl2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypyv+y88P/DQ/Spg4xsBwjRZUDafqt2aSkIrl8LyH
SSD1BWB09X5fv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PKZmOczkr426JO4DdhFcXdzMI8PzQ6
```

Apply

Close

Display Sensitive Data as Plaintext

En este ejemplo, la palabra clave, *RSA*, se incluye en el *COMIENZO* y el *FIN* de la *Clave Pública*.

Paso 12

Verá la notificación de éxito en la pantalla. Puede cerrar esta ventana y guardar la configuración en el 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
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lyY28xMzY2Z28xMzY2Z28x
DTE5MDYxODAxNTc1Ni0xODIwMDYxNzA1NTc1Ni0wYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

★ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgkCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xACel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpv+y88P/DQ/Spg4xsBwjZUDafqt2aSkIr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

★ Private Key: Encrypted Plaintext

Apply Close Display Sensitive Data as Plaintext

Errores posibles

Los errores analizados pertenecen a la clave pública. Normalmente se utilizan dos tipos de formatos de clave pública:

1. Archivo de clave pública RSA (PKCS#1): Esto es específico para las claves RSA.

Comienza y termina con las etiquetas:

—COMENZAR CLAVE PÚBLICA RSA—

DATOS CODIFICADOS BASE64

—FINALIZAR CLAVE PÚBLICA RSA—

2. Archivo de clave pública (PKCS#8): Este es un formato de clave más genérico que identifica el tipo de clave pública y contiene los datos relevantes.

Comienza y termina con las etiquetas:

—INICIE CLAVE PÚBLICA—

DATOS CODIFICADOS BASE64

—FINALIZAR CLAVE PÚBLICA—

Falta el encabezado de la clave

Escenario 1: Ha generado el certificado de una CA de terceros. Ha copiado y pegado la clave pública y ha hecho clic en **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
A1UEBHMCVVMxEzARBgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhbIBk3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xCzAJBgNVBAsMAIVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBHMCVVMxEzAR
BgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhbIBk3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

Public Key:

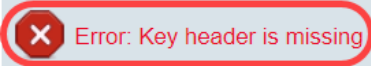
```
-----BEGIN PUBLIC KEY-----
MIIBBgKCAQEAAuxUF/1CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0J
p8CFuMH/Azj9JDR1fsVgBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peqLvb/A+glnieTqB/Z2EL3eT2xjJT0My
qFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel
2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafqt2aSkIrl8L8yHSSD1BWB0
9X5fiv10QNAMQ+QIDAQAB
```

Private Key: Encrypted

Plaintext

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAAuxUF/1CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5j
pe0Jp8CFuMH/Azj9JDR1fsVgBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peqLvb/A+glnieTqB/Z2EL3eT2xjJT
0MyqFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wx
ACel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafqt2aSkIrl8L8yHSSD1B
WB09X5fiv10QNAMQ+QIDAQABAOIBAAIzH0Lq1V/I45VC/5PkZmOczkr426JO4DdhFcXdzMI8PzQ6EIKExUH
```

Ha recibido el mensaje, *Error: Falta el encabezado de la clave.* Cerrar ventana Se pueden hacer algunas modificaciones para hacer desaparecer este problema.



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
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhbIBKb3NI
MQ4wDAYDVQQDDAVDAXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAIVTMB4X
DTE5MDYxODA1NTc1NloXDTEwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhbIBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBKgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhICMmAxp1pegbLvb/A+glnieTgB/Z2EL3eT2xJT
0MyqFImBPNuL4awjvt9E7IEHbT1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcypyv+y88P/DQ/Spg4xsBwjrzUDafqt2aSkir8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Para corregir este error:

Agregue la palabra clave, *RSA*, al principio de la clave pública: **COMIENZE LA CLAVE PÚBLICA RSA**

Agregue la palabra clave, *RSA*, al final de la Clave Pública: **CLAVE PÚBLICA RSA FINAL**

Quite los primeros 32 caracteres del código de clave. La parte resaltada que se muestra a continuación es un ejemplo de los primeros 32 caracteres.

```
-----BEGIN RSA PUBLIC KEY-----
MIIBKgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhICMmAxp1pegbLvb/A+glnieTgB/Z2EL3eT2xJT
0MyqFImBPNuL4awjvt9E7IEHbT1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcypyv+y88P/DQ/Spg4xsBwjrzUDafqt2aSkir8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Cuando aplique la configuración, no obtendrá el error *Key header is missing* en la mayoría de los casos.

Error al cargar el error de clave pública

Escenario 2: Ha generado un certificado en un switch y lo ha importado en otro switch. La clave pública se copió y pegó después de quitar los primeros 32 caracteres y se hizo clic en **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/blKGoJFhmCvnyTWUwDQYJKoZIhvcNAQELBQAwwYzELMAKG
A1UEBhMCSU4xEDAObgNVBAgMB0hhcnlhbmExEDAObgNVBAcMB0d1cmdbb24xEDA
BgNVBAMMBzAuMC4wLjAxDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGmxCzAJBgNVBAYTAkIOMRAw
DgYDVQQIDAdiYXJ5J5YW5hMRawDgYDVQQHDAhdXJnYW9uMRawDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

✱ Public Key: 1 -----BEGIN RSA PUBLIC KEY-----
/oy4ryP3fqjO8QHfzQsMSCCHrq5repNDflfRV8LlBFIq3QilBHDtLJ07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVN
J5ZPG8qKw58HWRIMcyv0vblqDjJ/ejOaYiGA10GX8eiT8lxfMblJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbquVf
shpwP2WdWWWReDU9qb8WLFrdnNQhGWR/N794HgAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil
92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBePl1yaWiSOqaG0zgjir7YQIDAQAB
-----END RSA PUBLIC KEY-----

✱ Private Key: Encrypted
 Plaintext 2 -----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEApAgvAcD58ScvYwW5vzx/oy4ryP3fqjO8QHfzQsMSCCHrq5repNDflfRV8LlBFIq3QilBH
DtLJ07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDjJ/ejOaYiGA10GX8eiT8
lxfMblJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWWReDU9qb8WLFrdnNQhGWR/N794H
gAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBePl
1yaWiSOqaG0zgjir7YQIDAQABAoIBAQTUfJvpS1Qvzi21FbNZmhBYkmMoxTpYKHguvowxbZqIS07KdPF5v

Apply Close Display Sensitive Data as Plaintext

Se ha producido el error *Failed to load public key* en la pantalla.

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
A1UEBhMCSU4xEDAObGNVBAgMB0hhcnIhbmExEDAObGNVBAcMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxZDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLEDAVdXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMrCzAJBGNVBAYTAkIOMRAw
DgYDVQQIDAdiYXJ5J5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCAgKCAQEAqAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLrV8LtbFIq3QilBHDtL
J07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJI/ejOaYIGA10GX8eif8lx
lfMblJomiiF/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWReDU9gb8WLFrdnNQHGWWR/N794H
gAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBe
P11yaWiSOqaG0zgjir7YQIDAQAB

Private Key: Encrypted
 Plaintext

Apply Close Display Sensitive Data as Plaintext

Para corregir este error, NO elimine los primeros 32 caracteres de la clave pública en este caso.

▲ 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-----
 MIIDSTCAjECEHV4jm/bIKGoJFHmCvnyTWUwDQYJKoZIhvcNAQELBQAwYzELMAkG
 A1UEBhMCSU4xEDA0BgNVBAGMB0hhcnlhbmExEDA0BgNVBACjMB0d1cmdhb24xEDAO
 BgNVBAMMBzAuMCAwLjAxZDQAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQQLDAVDAxNjBzAe
 Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMxMzAxBG9vBAYTAkiOMRAw
 DgYDVQQIDAdiYXJ5J5YW5hMRAwDgYDVQQHDAhhdXJnYW9uMRAwDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

Public Key: -----BEGIN RSA PUBLIC KEY-----
 MIIBCgKCAQEApaAqavAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLFRV8LtbFIq3QilBHDtLJ
 07Pj29mgdVFHX/p3ArKS3QiuDST2/+A0CGVNj5ZPG8qKw58HWRIMcyv0vblqDJl/ejOaYiGA10GX8eiT8lxfM
 bJomiiFd/MWof8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWRReDU9qb8WLFrdnNqHGWR/N794HgAu0
 HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBePl1yaW
 iSOgaG0zqjir7YQIDAQAB

Private Key: Encrypted Plaintext
 roiJNnzjgteU9ggzGvA6re1+f9z4tqwGn+9/reRq3J16w8vriA3wucP9lmvRIUCqYEAUjA3K3f+pRgBO/vDm0Wn
 lFkSmiG6azhiA4YrRQpVi8uEU7neT7edoNTXjXeb/zpt0hQBHicv1xsc5qv2KvvpTx8k0u5uBgv9hP1qGsEuePc
 G+yndTFdYImZLc0pDEtGwBKV362YnyX4rCZT67RVXBRI3geAmN30DqpygcYLMCgYEAiqhyEg9cWrkQS03
 e904lVAClgjVG05nkfE6Q1BFt8sTDDoGoSKGzLYhRxlIkLOXRP990Z2Guqt3xKlViqhFmZH0YaSTLkEY8hZr/
 uTejGQLoCYNoZAQzC1Ac+rjQneCbQ4GIDua0amyetkAjEUoa7cx2skaoziQSIC3dw2F5tw=
 -----END RSA PRIVATE KEY-----

Apply Close Display Sensitive Data as Plaintext

Importar mediante CLI

Paso 1

Para importar el certificado mediante CLI, introduzca el siguiente comando.

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

El certificado 2 se importa en este ejemplo.

```
switch(config)#importación de certificado 2 de criptografía
```

Paso 2

Pegar la entrada; agregue un punto (.) en una línea independiente después de la entrada.

```
—COMENZAR CLAVE PRIVADA RSA—
MIIEVgIBADANBgkqhkiG9w0BAQEFAASCBCGwggSkAgEAAoIBAQC/rZQ6f0rj8neA
...truncado 24 líneas...
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+521D/GokmU
—FINALIZAR CLAVE PRIVADA RSA—
—COMENZAR CLAVE PÚBLICA RSA—
MIIBCgKCAQEA62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkft0l
...3 líneas truncadas...
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB
```

–FINALIZAR CLAVE PÚBLICA RSA–

–CERTIFICADO DE INICIO–

MIIFvTCCBKWgAwIBAgIRAOOBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw

–truncado 28 líneas...

8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVff0cUzqXwOJcsTrMV

JDpTnbKXG56w0Tæ6UQ9HsUBoDQnlsN5ZBht1VyjAP

–CERTIFICADO FINAL–

.

Certificado importado correctamente

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

Válido desde: 14 jun 00:00:00 2017 GMT

Válido para: 11 sep 23:59:59 2020 GMT

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

Huella digital SHA: xxxxxxx

Conclusión

Ya ha aprendido los pasos para importar correctamente un certificado en los switches de las series Sx350 y Sx550X mediante la GUI y la CLI.