

Come importare un certificato sugli switch serie Sx350 e Sx550X

Obiettivo

Questo documento descrive i passaggi per importare un certificato sugli switch serie Sx350 e Sx550X usando l'interfaccia grafica dell'utente (GUI) e l'interfaccia della riga di comando (CLI).

Sommario

- [Introduzione](#)
- [Dispositivi e versione software interessati](#)
- [Prerequisiti](#)
- [Importazione tramite GUI](#)
- [Errori possibili Intestazione chiave mancanteImpossibile caricare errore di chiave pubblica](#)
- [Importazione tramite CLI](#)
- [Conclusioni](#)

Introduzione

Uno dei problemi riscontrati durante l'importazione di un certificato sugli switch Sx350 e Sx550X è che l'*intestazione della chiave* dell'utente è *mancante* e/o *non è stata in grado di caricare* gli errori della *chiave pubblica*. In questo documento verrà illustrato come superare questi errori per importare correttamente un certificato. Un certificato è un documento elettronico che identifica un individuo, un server, una società o un'altra entità e associa tale entità a una chiave pubblica. I certificati vengono utilizzati in una rete per fornire un accesso sicuro. I certificati possono essere autofirmati o firmati digitalmente da un'Autorità di certificazione (CA) esterna. Un certificato autofirmato, come indica il nome, è firmato dal proprio creatore. Le CA gestiscono le richieste di certificati e rilasciano i certificati alle entità partecipanti, ad esempio host, dispositivi di rete o utenti. Un certificato digitale firmato da CA è considerato uno standard del settore e più sicuro.

Dispositivi e versione software interessati

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

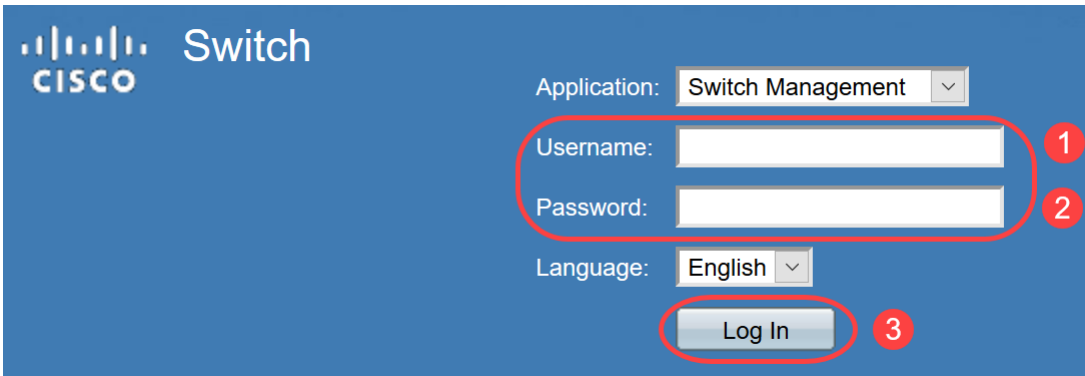
Prerequisiti

È necessario disporre di un certificato autofirmato o di un certificato dell'Autorità di certificazione (CA). In questo articolo sono illustrate le procedure per ottenere un certificato autofirmato. Per ulteriori informazioni sui certificati CA, fare clic [qui](#).

Importazione tramite GUI

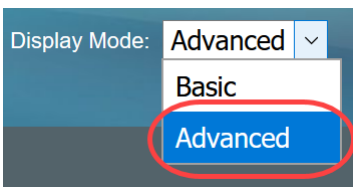
Passaggio 1

Accedere alla GUI dello switch immettendo il *nome utente* e la *password*. Fare clic su **Log In**.



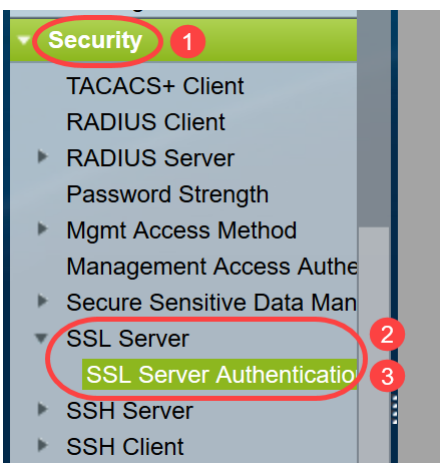
Passaggio 2

Dalla *modalità di visualizzazione* in alto a destra nell'interfaccia utente, scegliere **Advanced** (Avanzate) dall'elenco a discesa.



Passaggio 3

Selezionare **Protezione > Server SSL > Autenticazione server SSL**.



Passaggio 4

Selezionare uno dei certificati *generati automaticamente*. Selezionare l'*ID certificato* 1 o 2 e fare clic sul pulsante **Modifica**.

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

Passaggio 5

Per generare un certificato autofirmato, nella nuova finestra popup abilitare *Regenerate RSA Key* e immettere i seguenti parametri:

Lunghezza chiave

Nome comune

Unità organizzativa

Nome organizzazione

Posizione

State

Paese

Durata

Fare clic su **Genera**.

▲ 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

È inoltre possibile creare un certificato da una CA di terze parti.

Passaggio 6

A questo punto sarà possibile visualizzare il certificato *definito dall'utente* nella *tabella delle chiavi del server SSL*. Selezionare il certificato appena creato e fare clic su **Dettagli**.

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...** 2 Delete

Passaggio 7

Nella finestra popup sarà possibile visualizzare i dettagli *Certificato*, *Chiave pubblica* e *Chiave privata (crittografata)*. È possibile copiarli in un file del Blocco note separato. Fare clic su **Visualizza dati sensibili come testo normale**.

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

Certificate ID: 2

Certificate: -----BEGIN CERTIFICATE-----
MIIDRzCCAI8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIMQ4wDAYD
VQ4wDAYDQDQDAVDAxNjBzEOMAwGA1UECgwFQ2l2Y28xZzAxBG9NVBAsMAIVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIMQ4wDAYDQDQDAVDA

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCGKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjT0MyqF1
mBPNuL4awjvt9E7IEXhBt1HL0Nr/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/Z2EL3eT2xjT0
MyqF1mBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxAC
el2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpyv+y88P/DQ/Spq4xsBwjrzUDafqt2aSkI8L8yHSSD1BWB0
9X5fjv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PkZmOczkr426JO4DDhFcXdzMI8PzQ6EIKExUH0YpV

Close Display Sensitive Data as Encrypted

Passaggio 10

Selezionare il nuovo certificato *definito dall'utente* creato e fare clic su **Importa certificato**.

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

Passaggio 11

Nella nuova finestra popup, abilitare l'opzione *Import RSA Key-Pair* e incollare la chiave privata (copiata al passaggio 9) in formato testo normale. Fare clic su **Apply** (Applica).

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
0MyqFImBPNuL4awjvt9E7IEXhB1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypyv+y88P/DQ/Spg4xsBwirZUDafqt2aSkir8L8yHSSD
1BWB09X5fv10QNAMQ+QIDAQAB
```

Private Key: Encrypted

Plaintext 3

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV
5jpe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2
xiJT0MyqFImBPNuL4awjvt9E7IEXhB1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3
G6wxAcEl2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypyv+y88P/DQ/Spg4xsBwirZUDafqt2aSkir8L8yH
SSD1BWB09X5fv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PKZmOczkr426JO4DdhFcXdzMI8PzQ6
```

Apply Close Display Sensitive Data as Plaintext

Nell'esempio, la parola chiave *RSA* viene inclusa in *BEGIN* e *END* della *chiave pubblica*.

Passaggio 12

Sullo schermo verrà visualizzata la notifica di esito positivo. È possibile chiudere questa finestra e salvare la configurazione sullo 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
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lyY28xMzY2Z28xMzY2Z28x
DTE5MDYxODAxNTc1Ni0xODIwMDYxNzA1NTc1Ni0wYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhb3NIb3NIb3NIb3NIb3NIb3NI
BQNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhb3NIb3NIb3NIb3NIb3NIb3NI
-----
```

Import RSA Key-Pair: Enable

⚙ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcEl2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypv+y88P/DQ/Spg4xsBwjZUDafqt2aSkIr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
-----
```

⚙ Private Key: Encrypted Plaintext

Apply Close Display Sensitive Data as Plaintext

Errori possibili

Gli errori discussi riguardano la chiave pubblica. In genere vengono utilizzati due tipi di formati di chiave pubblica:

1. File di chiave pubblica RSA (PKCS#1): È specifico per le chiavi RSA.

Inizia e termina con i tag:

—INIZIO CHIAVE PUBBLICA RSA—

DATI CODIFICATI BASE64

—END RSA PUBLIC KEY—

2. File di chiave pubblica (PKCS#8): Si tratta di un formato di chiave più generico che identifica il tipo di chiave pubblica e contiene i dati rilevanti.

Inizia e termina con i tag:

—INIZIA CHIAVE PUBBLICA—

DATI CODIFICATI BASE64

—END PUBLIC KEY—

Intestazione chiave mancante

Scenario 1: Il certificato è stato generato da una CA di terze parti. La chiave pubblica è stata copiata e incollata e si è fatto clic su **Applica**.

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  
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xCzAJBgNVBAsMAITMB4X  
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBHMCVVMxEzAR  
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhbIBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

Public Key:

```
-----BEGIN PUBLIC KEY-----  
MIIBBgKCAQEAAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0J  
p8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peabLvb/A+gInieTaB/Z2EL3eT2xjJT0My  
qFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel  
2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafat2aSkIrl8L8yHSSD1BWB0  
9X5fiv10QNAMQ+QIDAQAB
```

Private Key: Encrypted

Plaintext

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEogIBAAKCAQEAAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5j  
pe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peabLvb/A+gInieTaB/Z2EL3eT2xjJT  
0MyqFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wx  
ACel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafat2aSkIrl8L8yHSSD1B  
WB09X5fiv10QNAMQ+QIDAQABAOIBAAIZH0Lq1V/I45VC/5PkZmOczkr426JO4DdhFcXdzMI8PzQ6EIKExUH
```

È stato visualizzato il messaggio *Errore: Intestazione chiave mancante*. Chiudete la finestra. È possibile apportare alcune modifiche per eliminare questo problema.

✖ 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  
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhbIBk3NI  
MQ4wDAYDVQQDDAVDAXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAIVTMB4X  
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR  
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhbIBk3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

✦ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----  
MIIBKgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe  
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhICMmAxp1pegLvb/A+glnieTgB/Z2EL3eT2xJT  
0MyqFImBPNuL4awjvt9E7IEhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w  
xAceI2n4dmK4GFQvOxS0A5PcsKUMefaeF/afcBvRcypy+y88P/DQ/Spg4xsBwjZUDafqt2aSkIr8L8yHSSD  
1BWB09X5fjv10QNAMQ+QIDAQAB
```

✦ Private Key: Encrypted
 Plaintext

Apply Close Display Sensitive Data as Plaintext

Per correggere l'errore:

Aggiungere la parola chiave RSA all'inizio della chiave pubblica: **INIZIO CHIAVE PUBBLICA RSA**

Aggiungere la parola chiave RSA alla fine della chiave pubblica: **FINE CHIAVE PUBBLICA RSA**

Rimuovere i primi 32 caratteri dal codice del tasto. La parte evidenziata mostrata di seguito è un esempio dei primi 32 caratteri.

```
-----BEGIN RSA PUBLIC KEY-----  
MIIBKgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe  
07Pj29mgdVFHX/p3ArKS3QiuDST2l/+A0CGVNj5ZPG8qKw58HWRIMcyy0vblqDJ/iejOaYiGA10GX8eiT8lxfM  
bUJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbguVfshpwP2WdWWReDU9gb8WLFrdnNQhGWR/N794HgAu0  
HyxpT7qDOVrYv4FAGIR1pbiDdAYHe8/sVXUCCuAFiI92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBePI1yaW  
iSOgaG0zqjir7YQIDAQAB
```

Quando si applicano le impostazioni, nella maggior parte dei casi l'intestazione *Chiave mancante* non viene visualizzata.

Impossibile caricare errore di chiave pubblica

Scenario 2: Il certificato è stato generato su uno switch e importato su un altro switch. La chiave pubblica è stata copiata e incollata dopo aver rimosso i primi 32 caratteri e aver fatto clic su **Applica**.

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/bIKGoJFHmCvnyTWUwDQYJKoZIhvcNAQELBQAwwYzELMAkG
A1UEBhMCSU4xEDAObgNVBAGMB0hcnlhbmExEDAObgNVBACMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxDjAMBGNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVdaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMrCzAJBgNVBAYTAklOMRAw
DgYDVQQIDAdlYXJ5J5YW5hMRAwDgYDVQQHDAhHdXJnYW9uMRAwDgYDVQQDDAcwLjAu

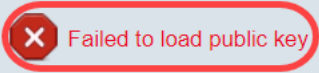
Import RSA Key-Pair: Enable

Public Key: 1 -----BEGIN RSA PUBLIC KEY-----
/oy4ryP3fqiO8QHfzQsMSCCHrq5repNdfLfrV8LtbFlq3QiIbHDTLJ07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVN
J5ZPG8qKw58HWRIMcyv0vblqDJl/ejOaYiGA10GX8eiT8lxifMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVf
shpwP2WdWWReDU9qb8WLFrdnNqHGWR/N794HqAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil
92aDPeK1ZCMAcDJaMaQ4trqX/Km6vgBnvBePl1yaWiSOqaG0zgjir7YQIDAQAB
-----END RSA PUBLIC KEY-----

Private Key: Encrypted
 Plaintext 2 -----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEApAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNdfLfrV8LtbFlq3QiIbH
DTLJ07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJl/ejOaYiGA10GX8eiT8
lxifMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVfshpwP2WdWWReDU9qb8WLFrdnNqHGWR/N794H
qAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqX/Km6vgBnvBePl
1yaWiSOqaG0zgjir7YQIDAQABAoIBAQCtUfJvpS1Qvzi21FbNZmhBYkmMoxTpYKHguvowxbZqIS07KdPF5v

Apply Close Display Sensitive Data as Plaintext

È stato visualizzato il messaggio di errore *Impossibile caricare la chiave pubblica*.



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/bIKGoJFHmCvnyTWUwDQYJKoZIhvcNAQELBQAwwYzELMAkG
A1UEBhMCSU4xEDAObGNVBAgMB0hhcnIhbmExEDAObGNVBAcMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxZDpAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLEDAVDAxNjBzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMrCzAJBGNVBAYTAkIOMRAw
DgYDVQQIDAdiYXJ5J5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

Public Key:
-----BEGIN RSA PUBLIC KEY-----
MIIBCAgKCAQEAqAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfrV8LtbFIq3QilBHDtL
J07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJI/ejOaYIGA10GX8eIT8lx
lfrMblJomiiF/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWReDU9gb8WLFrdnNqHGWR/N794H
gAu0HyxpT7qDOvrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBe
PI1yaWiSOqaG0zgjjr7YQIDAQAB

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Per correggere l'errore, NON eliminare i primi 32 caratteri della chiave pubblica in questo 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
 BgNVBAMMBzAuMC4wLjAxZDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQQLDAVDAxNjBzAe
 Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMAcCzAJBgNVBAYTAkOMRAw
 DgYDVQQIDAdiYXJ5J5YW5hMRAwDgYDVQQHDAHdXJnYV9uMRAwDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

Public Key: -----BEGIN RSA PUBLIC KEY-----
 MIIBCgKCAQEApaAqavAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLFRV8LtbFIq3QilBHDtLJ
 07Pj29mgdVFHX/p3ArKS3QiuDST2/+A0CGVNj5ZPG8qKw58HWRIMcyv0vblqDJl/ejOaYiGA10GX8eiT8lxlfM
 bJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWRReDU9qb8WLFrdnNqHGWR/N794HgAu0
 HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCuAFil92aDPeK1ZCMAcDJaMaQ4trqxX/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

Importazione tramite CLI

Passaggio 1

Per importare il certificato tramite CLI, immettere il comando seguente.

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

In questo esempio viene importato il certificato 2.

```
switch(config)#importazione certificato crittografico 2
```

Passaggio 2

Incollare l'input; aggiungere un punto (.) su una riga separata dopo l'input.

```

--INIZIO CHIAVE PRIVATA RSA--
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQC/rZQ6f0rj8neA
...24 linee troncate...
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+521D/GokmU
--END RSA PRIVATE KEY--
--INIZIO CHIAVE PUBBLICA RSA--
MIBCgKCAQEA62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkft01
...troncate di 3 righe...
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB

```

–END RSA PUBLIC KEY–

–BEGIN CERTIFICATE–

MIIFvTCCBKWgAwIBAgIRA0OBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw

- 28 linee troncate...

8S+39m9wPAOZipIOJA1/0IeG7ChLWOXKncMeZWVTIUZaEwVff0cUzqXwOJcsTrMV

JDptnbKXG56w0Trecu6UQ9HsUBoDQnlsN5ZBht1VyjAP

–END CERTIFICATE–

.

Importazione del certificato completata

Rilasciato da: C=xx, ST=Gxxxxxx, L=xx, O=xx CA Limited, CN=xx RSA Convalida organizzazione CA
Secure Server

Valido da: 14 giu 00:00:00 2017 GMT

Valido fino al: 11 set 23:59:59 2020 GMT

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

Impronta digitale SHA: xxxxxxx

Conclusioni

A questo punto, è possibile importare un certificato sugli switch serie Sx350 e Sx550X dalla GUI e dalla CLI.