

Importieren des Zertifikats für Switches der Serien Sx350 und Sx550X

Ziel

Dieses Dokument enthält die Schritte zum erfolgreichen Importieren eines Zertifikats für Switches der Serien Sx350 und Sx550X mithilfe der grafischen Benutzeroberfläche (GUI) und der Befehlszeilenschnittstelle (CLI).

Inhaltsverzeichnis

- [Einführung](#)
- [Anwendbare Geräte und Softwareversion](#)
- [Voraussetzungen](#)
- [Import über GUI](#)
- [Mögliche Fehler Der Header fehlt.Fehler beim Laden des öffentlichen Schlüsselfehlers](#)
- [Importieren über CLI](#)
- [Schlussfolgerung](#)

Einführung

Eines der Probleme beim Importieren eines Zertifikats auf Switches der Serien Sx350 und Sx550X besteht darin, dass der Benutzer dem **Schlüsselheader** gegenübersteht, **der fehlt** und/oder **keine Fehler beim Laden von Fehlern des öffentlichen Schlüssels aufweist**. In diesem Dokument wird erläutert, wie Sie diese Fehler überwinden, um ein Zertifikat erfolgreich zu importieren. Ein Zertifikat ist ein elektronisches Dokument, das eine Person, einen Server, ein Unternehmen oder eine andere Körperschaft identifiziert und dieser Körperschaft einen öffentlichen Schlüssel zuordnet. Zertifikate werden in einem Netzwerk verwendet, um einen sicheren Zugriff bereitzustellen. Zertifikate können selbstsigniert oder digital von einer externen Zertifizierungsstelle (Certificate Authority, CA) signiert werden. Ein selbstsigniertes Zertifikat wird, wie der Name bereits andeutet, vom eigenen Ersteller signiert. Zertifizierungsstellen verwalten Zertifikatsanforderungen und geben Zertifikate an die teilnehmenden Einheiten wie Hosts, Netzwerkgeräte oder Benutzer aus. Ein digitales Zertifikat mit CA-Signatur gilt als Industriestandard und sicherer.

Anwendbare Geräte und Softwareversion

- 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

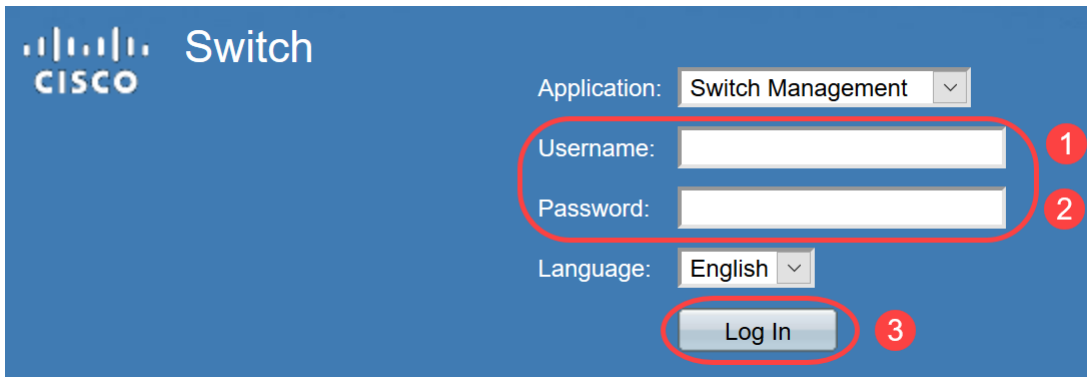
Voraussetzungen

Sie müssen über ein selbstsigniertes Zertifikat oder ein Zertifikat der Zertifizierungsstelle (Certificate Authority, CA) verfügen. Schritte zum Erhalt eines selbstsignierten Zertifikats sind in diesem Artikel enthalten. Weitere Informationen zu Zertifizierungsstellenzertifikaten finden Sie [hier](#)

Import über GUI

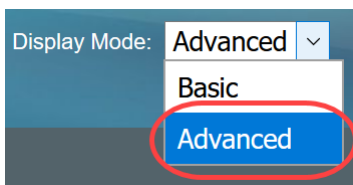
Schritt 1

Melden Sie sich bei der GUI des Switches an, indem Sie Ihren *Benutzernamen* und Ihr *Kennwort* eingeben. Klicken Sie auf **Anmelden**.



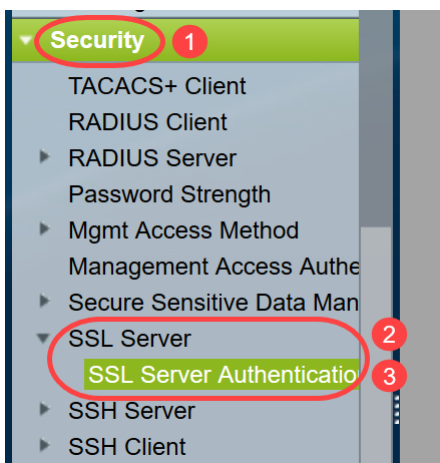
Schritt 2

Wählen Sie im *Anzeigemodus* oben rechts in der GUI die Option **Erweitert** mit der Dropdown-Option aus.



Schritt 3

Navigieren Sie zu **Security > SSL Server > SSL Server Authentication**.



Schritt 4

Wählen Sie eines der Zertifikate aus, das *automatisch generiert wird*. Wählen Sie die *Zertifikats-ID* 1 oder 2 aus, und klicken Sie auf die Schaltfläche **Bearbeiten**.

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

Schritt 5

Um ein selbstsigniertes Zertifikat zu generieren, aktivieren Sie im neuen Popup-Fenster den *RSA-Schlüssel* "Regenerate RSA Key" (Neuer RSA-Schlüssel), und geben Sie die folgenden Parameter ein:

Schlüssellänge

Allgemeiner Name

Organisationseinheit

Name der Organisation

Standort

Staat

Land

Dauer

Klicken Sie auf **Generieren**.

▲ 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

Sie können auch ein Zertifikat von einer Zertifizierungsstelle eines Drittanbieters erstellen.

Schritt 6

Nun können Sie das *benutzerdefinierte* Zertifikat unter der *SSL-Serverschlüsseltabelle* sehen. Wählen Sie das neu erstellte Zertifikat aus, und klicken Sie auf **Details**.

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**

Schritt 7

Im Popup-Fenster werden die Details *Zertifikat, Öffentlicher Schlüssel und privater Schlüssel (verschlüsselt)* angezeigt. Sie können diese in einer separaten Notizblock-Datei kopieren. Klicken Sie auf **Sensible Daten als Nur-Text anzeigen**.

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
A1UEBhMCVVmxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lzY28xOzA1UEBhMAIjE0MDE
DTE5MDYxODAxNTc1NloXDTEwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVmxEzAR
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIb3NIMQ4wDAYDVQQDDAVD

Public Key:
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhICMmAx1peglVb/A+gInieTgB/Z2EL3eT2xJT0MyqFl
mBPNuL4awjvt9E7IEXhBt1HL0Nr/cuVTLmA0IDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel2n4d
mK4GFQvOxzS0A5PcsKUMefaeF/afcbVRcpyy+y88P/DQ/Spq4xsBwjZUDafqt2aSkrl8yHSSD1BWB09X5fjv1
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
Km1b7W0jcoh7CYBkGIAxe5p24pgXf5QWPH2830A0qY0dAiinwZkwPat9BUkVV913eY1tHzHFN/1kvOpvKggus
oO85U5FqFMFUpFD94YDqQ+Xpp+LDuiVPjgFh6DCXq2wBnFBzws7doSHMBU77LHOFnWybmzzmT63DNFN
goUlp0nwskdPoigiHLjrtESSJ5x/tlzkfJx2rGreHz2AMwa1urtJv/+ysGu+R4T0++1RkiUJISCYZW7kmtwFdlchMBv1
YJWPQZ0l9znTXOXgZQbR1MGI5NqrTb1V11Ositb63dqRQKJ4XUdTldQpRgrhTrXUwXHgegCpBtqLg1D6Hp


Close Display Sensitive Data as Plaintext

Schritt 8

Ein Popup-Fenster wird geöffnet, um die Anzeige des privaten Schlüssels als Klartext zu bestätigen. Klicken Sie auf **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

Schritt 9

Nun können Sie den *privaten Schlüssel* in Klartextform sehen. Kopieren Sie diese unverschlüsselte Ausgabe auf eine Notizblock-Datei. Klicken Sie auf **Schließen**.

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

Certificate ID: 2

Certificate: -----BEGIN CERTIFICATE-----
MIIDRzCCAI8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIMQ4wDAYDQDQDAVDAxNjBzEOMAwGA1UECgwFQ2l2Y28xCzAJBgNVBAsMAiVTMB4X
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIMQ4wDAYDQDQDAVDAV

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCGKCAQEAAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT0MyqF1
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-----
MIIEogIBAAKCAQEAAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe0Jp
e0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT0
MyqF1mBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxAC
el2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpyv+y88P/DQ/Spq4xsBwjrzUDafqt2aSkIr8L8yHSSD1BWB0
9X5fjv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PkZmOczkr426JO4DDhFcXdzMI8PzQ6EIKExUH0YpV

Close Display Sensitive Data as Encrypted

Schritt 10

Wählen Sie das neu erstellte *Benutzerdefinierte* Zertifikat aus, und klicken Sie auf **Zertifikat importieren**.

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

2

Schritt 11

Aktivieren Sie im neuen Popup-Fenster die Option *RSA-Schlüsselpaar importieren*, und fügen Sie den privaten Schlüssel (in Schritt 9 kopiert) im Klartextformat ein. Klicken Sie auf **Übernehmen**.

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
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUExETAPBgNVBACMCFNhb1Bkb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAiVTMB4X
DTE5MDYxODA1NTc1Ni0XDTIwMDYxNzA1NTc1Ni0wYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUExETAPBgNVBACMCFNhb1Bkb3NIIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe
0Jp8CFuMH/Az9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEXhB1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypyv+y88P/DQ/Spg4xsBwjRZUDafqt2aSkir8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Private Key: Encrypted 2

Plaintext 3

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV
5jpe0Jp8CFuMH/Az9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2
xiJT0MyqFImBPNuL4awjvt9E7IEXhB1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3
G6wxAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypyv+y88P/DQ/Spg4xsBwjRZUDafqt2aSkir8L8yH
SSD1BWB09X5fjv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PKZmOczkr426JO4DdhFcXdxZMI8PzQ6
```

Apply

Close

Display Sensitive Data as Plaintext

In diesem Beispiel ist das Schlüsselwort *RSA* im *BEGIN* und *END* des *öffentlichen Schlüssels* enthalten.

Schritt 12

Die Erfolgsbenachrichtigung wird auf dem Bildschirm angezeigt. Sie können dieses Fenster schließen und die Konfiguration auf dem Switch speichern.

▲ 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
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhbIBKb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2lyY28xMjY28xMjY28xMjY28x
DTE5MDYxODAxNTc1Ni0xODAxNTc1Ni0xODAxNTc1Ni0xODAxNTc1Ni0xODAxNTc1
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhbIBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

⚙ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCGKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+gInieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xACel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbVrcpyv+y88P/DQ/Spg4xsBwjZUDafqt2aSkIr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

⚙ Private Key: Encrypted Plaintext

Apply Close Display Sensitive Data as Plaintext

Mögliche Fehler

Die beschriebenen Fehler betreffen den öffentlichen Schlüssel. In der Regel werden zwei Arten von Public-Key-Formaten verwendet:

1. RSA Public Key File (PKCS#1): Dies gilt speziell für RSA-Schlüssel.

Am Anfang und Ende steht die Tags:

—BEGINNEN RSA PUBLIC KEY—

BASE64 KODIERTE DATEN

—END RSA PUBLIC KEY—

2. Public Key File (PKCS#8): Dies ist ein generischeres Schlüsselformat, das den Typ des öffentlichen Schlüssels identifiziert und die relevanten Daten enthält.

Am Anfang und Ende steht die Tags:

—ÖFFENTLICHER SCHLÜSSEL BEGINNEN—

BASE64 KODIERTE DATEN

—ÖFFENTLICHER SCHLÜSSEL ENDEN—

Der Header fehlt.

Szenario 1: Sie haben das Zertifikat von einer Zertifizierungsstelle eines Drittanbieters erstellt. Sie haben den öffentlichen Schlüssel kopiert und eingefügt und auf **Übernehmen** geklickt.

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

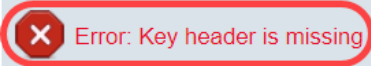
Public Key: -----BEGIN PUBLIC KEY-----
MIIBBgKCAQEAAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0J
p8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peabLvb/A+gInieTaB/Z2EL3eT2xjJT0My
qFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel
2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafat2aSkIrl8L8yHSSD1BWB0
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+QIDAQAB

Apply Close Display Sensitive Data as Plaintext

Sie haben die Meldung Fehler erhalten: Der Header "Key" fehlt. Schließen Sie das Fenster. Es können einige Änderungen vorgenommen werden, um dieses Problem zu eliminieren.



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-----
MIIBKgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcypy+y88P/DQ/Spg4xsBwjrzUDafqt2aSkIr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Private Key: Encrypted
 Plaintext

Apply Close Display Sensitive Data as Plaintext

Beheben Sie diesen Fehler:

Fügen Sie das Schlüsselwort *RSA* am Anfang des öffentlichen Schlüssels hinzu: **BEGINNEN DES RSA-ÖFFENTLICHEN SCHLÜSSELS**

Fügen Sie das Schlüsselwort *RSA* am Ende des öffentlichen Schlüssels hinzu: **END RSA PUBLIC KEY**

Entfernen Sie die ersten 32 Zeichen aus dem Schlüsselcode. Der hervorgehobene Teil unten ist ein Beispiel für die ersten 32 Zeichen.

```
-----BEGIN RSA PUBLIC KEY-----
MIIBKgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
07Pj29mgdVFHX/p3ArKS3QiuDST2l/+A0CGVNj5ZPG8qKw58HWRIMcwy0vblqDJI/ejOaYiGA10GX8eiT8lxfM
bUJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbguVfshpwP2WdWWRReDU9gb8WLFrdnNQhGWR/N794HgAu0
HxypT7qDOVrYv4FAGIR1pbiDdAYHe8/sVXUCCuAFiI92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBePI1yaW
iSOgaG0zqjir7YQIDAQAB
```

Wenn Sie die Einstellungen übernehmen, erhalten Sie in den meisten Fällen keinen Fehler in der *Key-Kopfzeile*.

Fehler beim Laden des öffentlichen Schlüsselfehlers

Szenario 2: Sie haben auf einem Switch ein Zertifikat generiert und es auf einen anderen Switch importiert. Sie haben den öffentlichen Schlüssel kopiert und eingefügt, nachdem Sie die ersten 32 Zeichen entfernt haben, und auf **Übernehmen** geklickt.

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
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMrCzAxBGNVBAYTAkIOMRAw
DgYDVQQIDAdlYXJ5J5YW5hMRAwDgYDVQQHDAhHdXJnYW9uMRAwDgYDVQQDDAcwLjAu

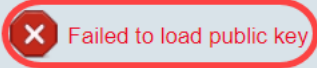
Import RSA Key-Pair: Enable

Public Key: **1** -----BEGIN RSA PUBLIC KEY-----
/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLFRV8LtBFIq3QiIBHDTLJ07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVN
J5ZPG8qKw58HWRIMcyv0vblqDJl/ejOaYiGA10GX8eiT8lxifMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVf
shpwP2WdWWReDU9qb8WLFrdnNQhGWR/N794HqAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil
92aDPeK1ZCMAcDJaMaQ4trqX/Km6vgBnvBePl1yaWiSOqaG0zgjjr7YQIDAQAB
-----END RSA PUBLIC KEY-----

Private Key: Encrypted
 Plaintext **2** -----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAqAgvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLFRV8LtBFIq3QiIBH
DTLJ07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJl/ejOaYiGA10GX8eiT8
lxifMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVfshpwP2WdWWReDU9qb8WLFrdnNQhGWR/N794H
qAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqX/Km6vgBnvBePl
1yaWiSOqaG0zgjjr7YQIDAQABAoIBAQCtUfJvpS1Qvzi21FbNZmhBYkmMoxTpYKHguvowxbZqIS07KdPF5v

Apply Close Display Sensitive Data as Plaintext

Sie haben den Fehler *Beim Laden des öffentlichen Schlüssels* auf dem Bildschirm angezeigt.



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
BgNVBAMMBzAuMC4wLjAxZDpAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLEDAVDAxNjzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMrCzAxBgNVBAYTAkIOMRAw
DgYDVQQIDAdiYXJ5J5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCAgKCAQEAqAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfrV8LtbFIq3QilBHDtL
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

Um diesen Fehler zu beheben, löschen Sie in diesem Fall NICHT die ersten 32 Zeichen des öffentlichen Schlüssels.

⚠ 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
 BgNVBAMMBzAuMC4wLjAxDjAMBGNVBAoMBUNpc2NvMQ4wDAYDVQQQLDAVDAxNjBzAe
 Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMxCzAJBgNVBAYTAkOMRAw
 DgYDVQQIDAdiYXJ5J5YW5hMRAwDgYDVQQHDAhhdXJnYW9uMRAwDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

Public Key: -----BEGIN RSA PUBLIC KEY-----
 MIIBCgKCAQEApaAqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLFRV8LtbFIq3QilBHDtLJ
 07Pj29mgdVFHX/p3ArKS3QiuDST2/+A0CGVNj5ZPG8qKw58HWRIMcyv0vblqDJl/ejOaYiGA10GX8eiT8lxfM
 bJomiiFd/MWof8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWRReDU9qb8WLFrdnNqHGWR/N794HgAu0
 HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBePl1yaW
 iSogaG0zqjir7YQIDAQAB

Private Key: Encrypted Plaintext
 roiJNnzjgteU9ggzGvA6re1+f9z4tqwGn+9/reRq3J16w8vriA3wucP9lmyRIUCqYEAUjA3K3f+pRgBO/vDm0Wn
 lFkSmiG6azhiA4YrRQpVi8uEU7neT7edoNTXjXeB/zpt0hQBHicv1xsc5qv2KvvpTx8k0u5uBgV9hP1qGsEuePc
 G+yndTFdYImZLc0pDEtGwBKV362YnyX4rCZT67RVXBRI3geAmN30DqpygcYLMCgYEAiqhyEg9cWrkQS03
 e904lVAClgjVG05nkeE6Q1BFt8sTDDoGoSKGzLYhRxlkLOXRP990Z2Guqt3xKlVliqhFmZH0YaStLkEY8hZr/
 uTejGQLoCYNoZAQzC1Ac+rjQneCbQ4GIDua0amyetkAjEUoa7cx2skaoziQSiC3dw2F5tw=
 -----END RSA PRIVATE KEY-----

Apply Close Display Sensitive Data as Plaintext

Importieren über CLI

Schritt 1

Geben Sie den folgenden Befehl ein, um ein Zertifikat über die CLI zu importieren.

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

Zertifikat 2 wird in diesem Beispiel importiert.

```
switch(config)#Crypto Certificate 2-Import
```

Schritt 2

Fügt die Eingabe ein; Fügen Sie nach der Eingabe einen Punkt (.) auf einer separaten Zeile hinzu.

```
--BEGINNEN DES PRIVATEN RSA--SCHLÜSSELS--
MIIEVgIBADANBgkqhkiG9w0BAQEFAASCbGwggSkAgEoIBAQC/rZQ6f0rj8neA
...24 Zeilen gekürzt...
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+521D/GokmU
--PRIVATER ENDE--RSA--SCHLÜSSEL--
--BEGINNEN RSA PUBLIC KEY--
MIIBCgKCAQEA62UOn9K4/J3gCAk7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkft0l
...3 Zeilen gekürzt...
64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB
```

```
-END RSA PUBLIC KEY-  
-BEGINNUNGSBESCHEINIGUNG-  
MIIFvTCCBKWgAwIBAgIRA0OBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAw  
-28 Zeilen gekürzt...  
8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVff0cUzqXwOJcsTrMV  
JDpTnbKXG56w0Trecu6UQ9UBoDQnlsN5ZBht1VyjAP  
-ENDBESCHEINIGUNG-  
.  
Zertifikat erfolgreich importiert  
Ausgestellt von: C=xx, ST=Gxxxxx, L=xx, O=xx CA Limited, CN=xx RSA Organization Validation  
Secure Server CA  
Gültig von: 14. Juni 2017, 00:00 Uhr GMT  
Gültig für: 11. September 2020, 23:59:59 Uhr GMT  
Betrifft: C=DE/postCode=xxx, ST=xx, L=xx/street=xxx 2, O=xxx, OU=IT, CN=*.kowi.eu  
SHA-Fingerabdruck: xxxxxx
```

Schlussfolgerung

Nun haben Sie gelernt, wie Sie mithilfe der Benutzeroberfläche und der CLI erfolgreich ein Zertifikat für die Switches der Serien Sx350 und Sx550X importieren.