

Hoe invoert u Document op SX350 en SX550X Series-switches

Doel

Dit doel van dit document is te voorzien in de stappen om met succes een certificaat op de switches van de Sx350- en de Sx550X-serie te importeren met behulp van de Graphical User Interface (GUI) en de Opdrachtlijn Interface (CLI).

Inhoud

- [Inleiding](#)
- [Toepasselijk apparaat en softwareversie](#)
- [Voorwaarden](#)
- [Importeren met GUI](#)
- [Mogelijke fouten Toetskop ontbreekt foutOpenbare belangrijke fout laden mislukt](#)
- [Importeren met CLI](#)
- [Conclusie](#)

Inleiding

Een van de problemen die zijn aangetroffen bij het importeren van een certificaat op de switches Sx350 en Sx550X is dat de gebruiker voor de *kop* staat ***dat de kop ontbreekt en/of er niet in is geslaagd belangrijke fouten van het publiek te laden***. Dit document legt uit hoe u voorbij deze fouten bent gegaan om een certificaat met succes te importeren. Een certificaat is een elektronisch document dat een individu, een server, een bedrijf of een andere entiteit identificeert en die entiteit met een openbare sleutel associeert. Certificaten worden in een netwerk gebruikt om veilige toegang te verschaffen. Certificaten kunnen zelf worden ondertekend of digitaal worden ondertekend door een externe certificaatinstantie (CA). Een zelfondertekend certificaat, zoals de naam aangeeft, wordt door zijn eigen schepper ondertekend. CA's beheren certificaatverzoeken en geven certificaten af aan deelnemende entiteiten zoals hosts, netwerkapparaten of gebruikers. Een door CA ondertekend digitaal certificaat wordt als industriestandaard en veiliger beschouwd.

Toepasselijk apparaat en softwareversie

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

Voorwaarden

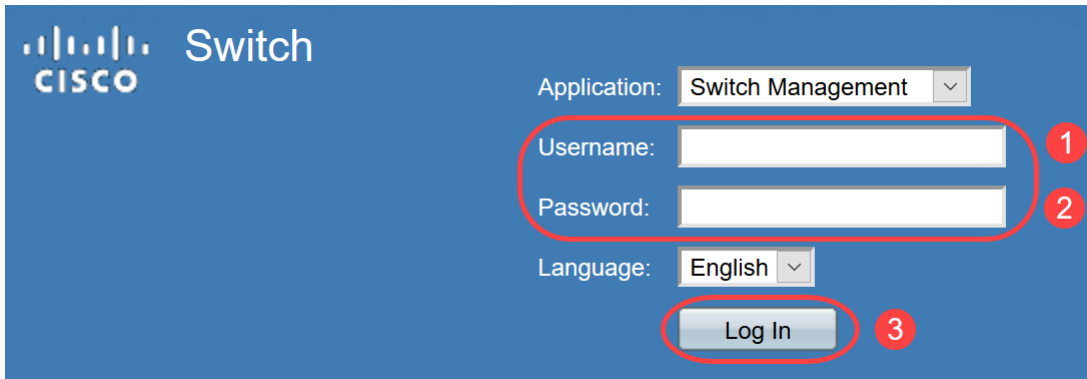
U moet beschikken over een zelfgetekend certificaat of een certificaat van de bevoegde autoriteit

(CA). In dit artikel zijn stappen opgenomen om een zichzelf ondertekend certificaat te verkrijgen. Klik [hier](#) voor meer informatie over CA-certificaten.

Importeren met GUI

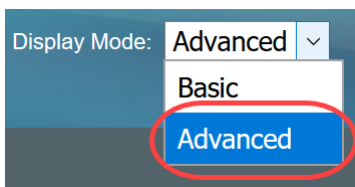
Stap 1

Meld u aan bij de GUI van de schakelaar door uw *gebruikersnaam* en *wachtwoord* in te voeren. Klik op **Inloggen**.



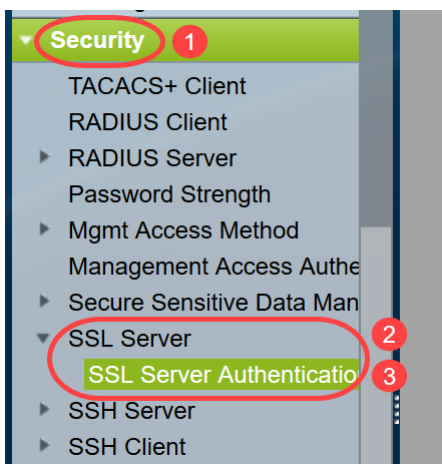
Stap 2

Kies in de *weergavemodus* rechtsboven in de GUI, **Geavanceerd** met behulp van de vervolgkeuzelijst.



Stap 3

Navigeer naar **Security > SSL Server > SSL Server verificatie**.



Stap 4

Selecteer een van de certificaten die *automatisch worden gegenereerd*. Selecteer de optie *Certificaat-ID 1* of *2* en klik op de knop **Bewerken**.

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

Stap 5

Om een zichzelf ondertekend certificaat te genereren, stelt u in het nieuwe pop-upvenster de *RSA-toets* in en voert u de volgende parameters in:

Sleutellengte

Algemene naam

Organisatie-eenheid

Naam van organisatie

Locatie

Staat

Land

Duur

Klik op **Generate**.

▲ 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

U kunt ook een certificaat maken van een CA van derden.

Stap 6

U kunt het *door de gebruiker gedefinieerde* certificaat nu zien in het *hoofdvenster* van de *SSL-server*. Selecteer het nieuwe certificaat en klik op **Details**.

SSL Server Authentication Settings

SSL Active Certificate Number: 1
 2

Apply Cancel

	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**

Stap 7

In het pop-upvenster kunt u de gegevens *over het certificaat, de openbare sleutel en de particuliere sleutel (Encrypted)* zien. U kunt deze kopiëren in een afzonderlijk notebookbestand. Klik op **Gevoelige gegevens weergeven als illustratie**.

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
BgNVBAGMCkNBTEIGT1JOSUExETAPBgNVBACMCFNhb3NI MQ4wDAYDVQQDDAVD

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCGKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0Jp
8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xjJT0MyqF1
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/Z2EL3eT2xjJT0
MyqF1mBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmlmKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxAC
el2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcpyv+y88P/DQ/Spq4xsBwjrzUDafqt2aSkI8L8yHSSD1BWB0
9X5fjv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PkZmOczkr426JO4DDhFcXdzMI8PzQ6EIKExUH0YpV

Close Display Sensitive Data as Encrypted

Stap 10

Selecteer het nieuwe *gebruikersgedefinieerde* certificaat en klik op **Importeren**.

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

Stap 11

In het nieuwe pop-upvenster, schakelt u de optie *RSA Key-Pair importeren in* en plakt u de privé-toets (gekopieerd in stap 9) in bestandsindeling. Klik op **Toepassen**.

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
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUExETAPBgNVBACMFNhbIBKb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAiVtMB4X
DTE5MDYxODA1NTc1Ni0XDTIwMDYxNzA1NTc1Ni0wYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUExETAPBgNVBACMFNhbIBKb3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

Public Key: 2

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xJT
0MyqFImBPNuL4awjvt9E7IEXhB1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjRZUDafqt2aSkIrl8LyHSSD
1BWB09X5fv10QNAMQ+QIDAQAB
```

Private Key: Encrypted

Plaintext 3

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV
5jpe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2
xjT0MyqFImBPNuL4awjvt9E7IEXhB1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3
G6wxAcEl2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpyv+y88P/DQ/Spg4xsBwjRZUDafqt2aSkIrl8LyH
SSD1BWB09X5fv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PKZmOczkr426JO4DdhFcXdzMI8PzQ6
```

Apply Close Display Sensitive Data as Plaintext

In dit voorbeeld is het sleutelwoord, *RSA*, opgenomen bij het *BEGIN* en *EINDE* van de *Public Key*.

Stap 12

Het succesbericht wordt op het scherm weergegeven. U kunt dit venster sluiten en de configuratie op de schakelaar opslaan.

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:

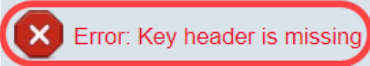
```
-----BEGIN PUBLIC KEY-----
MIIBBgKCAQEAAuxUF/1CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0J
p8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peabLvb/A+glnieTaB/Z2EL3eT2xjJT0My
qFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel
2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafqt2aSkIrl8L8yHSSD1BWB0
9X5fiv10QNAMQ+QIDAQAB
```

Private Key: Encrypted

Plaintext

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5j
pe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peabLvb/A+glnieTaB/Z2EL3eT2xjJT
0MyqFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wx
ACel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafqt2aSkIrl8L8yHSSD1B
WB09X5fiv10QNAMQ+QIDAQABAOiBAAIzH0Lq1V/I45VC/5PkZmOczkr426JO4DdhFcXdzMI8PzQ6EIKExUH
```

U hebt het bericht ontvangen, fout: Key header ontbreekt. Sluit het venster. Er kunnen enkele wijzigingen worden aangebracht om dit probleem te doen verdwijnen.



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
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhb3NiBk3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2IzY28xYzZyY28xYzZyY28xYzZy
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhb3NiBk3NIMQ4wDAYDVQQDDAVD
```

Import RSA Key-Pair: Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBKgKCAQEAAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2xJT
0MyqFImBPNuL4awjvt9E7IEhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcypy+y88P/DQ/Spg4xsBwjzUDafqt2aSkIr8L8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Private Key: Encrypted
 Plaintext

Apply Close Display Sensitive Data as Plaintext

U lost deze fout als volgt op:

Voeg het sleutelwoord, *RSA*, aan het begin van de Openbare sleutel toe: **BEGIN RSA PUBLIEKE SLEUTEL**

Voeg het sleutelwoord, *RSA*, aan het eind van de Openbare sleutel toe: **PUBLIEKE SLEUTEL VAN EINDRSA**

Verwijder de eerste 32 tekens uit de sleutelcode. Het gemarkeerde gedeelte dat hieronder wordt weergegeven is een voorbeeld van de eerste 32 tekens.

```
-----BEGIN RSA PUBLIC KEY-----
MIIBKgKCAQEAAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
07Pj29mgdVFHX/p3ArKS3QiuDST2l/+A0CGVNj5ZPG8qKw58HWRIMcYv0vblqDJI/ejOaYiGA10GX8eiT8lxfM
blJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbguVfshpwP2WdWWRReDU9gb8WLFrdnNQhGWR/N794HgAu0
HyxpT7qDOVrYv4FAGIR1pbiDdAYHe8/sVXUCCuAFiI92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBePI1yaW
iSOgaG0zqjir7YQIDAQAB
```

Wanneer u de instellingen toepast, krijgt u niet dat de *Key header* in de meeste gevallen *een* fout mist.

Openbare belangrijke fout laden mislukt

Scenario 2: U genereerde een certificaat op één schakelaar en importeerde het op een andere schakelaar. U kopieerde en plaste de openbare sleutel na het verwijderen van de eerste 32 tekens en klikte op **Toepassen**.

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/bIKGoJFHmCvnyTWUwDQYJKoZlIhvcNAQELBQAwwYzELMAkG
A1UEBhMCSU4xEDAObgNVBAGMB0hcnlhbmExEDAObgNVBACMB0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxDjAMBGNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGxMxGZAJBgNVBAYTAklOMRAw
DgYDVQQIDAdlYXJ5J5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu

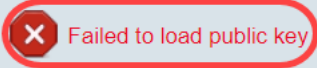
Import RSA Key-Pair: Enable

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-----
MIIEpQIBAAKCAQEApaAgvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNdfLfrV8LtbFlq3QiIbH
DTLJ07Pj29mgdVFHX/p3ArKS3QjuDST2l/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJl/ejOaYiGA10GX8eiT8
lxifMblJomiiFd/MWOf8C2/3nmbhKk/LsKl+koTucCbquVfshpwP2WdWWReDU9qb8WLFrdnNqHGWR/N794H
qAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqX/Km6vgBnvBePl
1yaWiSOqaG0zgjir7YQIDAQABAoIBAQCtUfJvpS1Qvzi21FbNZmhBYkmMoxTpYKHguvowxbZqIS07KdPF5v

Apply Close Display Sensitive Data as Plaintext

U hebt de *openbare* fout op het scherm *geladen*.



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
BgNVBAMMBzAuMC4wLjAxZDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMrCzAJBgNVBAYTAklOMRAw
DgYDVQQIDAdlYXJ5J5Yw5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCAgKCAQEAqAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLfrV8LtbFIq3QilBHDtL
J07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJI/ejOaYIGA10GX8eIT8lx
lfMblJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWReDU9gb8WLFrdnNQHGWRR/N794H
gAu0HyxpT7qDOvrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBe
P11yaWiSOqaG0zgjir7YQIDAQAB

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Om deze fout te repareren, verwijdert u de eerste 32 tekens van de openbare sleutel NIET.


```
-EINDRSA PUBLIEKSLEUTEL-  
-BEGIN CERTIFICAAT-  
MIIFvTCCBKWgIBAgIRAO0BWg4bkStdWPvcNYHBYWYWoZIhvcNAQELBQAw  
-ingekort 28 lijnen...  
8S+39m9WPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVff0cUzqXwOJTrMV  
JDptnbKXG56w0Trecu6UQ9HSUBoDQnlsN5ZBht1VyjAP  
-EINDCERTIFICAAT-
```

.
Met succes geïmporteerd certificaat

Afgegeven door : C=xx, ST=Gxxxxx, L=xx, O=xx CA Limited, CN=xx RSA Organisatieserver CA

Geldig van: 14 jun. 00:00:00 GMT 2017

Geldig aan: 11 sep. 23:59:59 GMT 2020

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

Vingerafdruk van SHA: xxxxxx

Conclusie

U hebt nu de stappen geleerd om met succes een certificaat op de switches van de SX350 en Sx550X-serie te importeren met behulp van de GUI en de CLI.