

Comment importer un certificat sur les commutateurs des gammes Sx350 et Sx550X

Objectif

Cet objectif de ce document est de fournir les étapes permettant d'importer un certificat sur les commutateurs des gammes Sx350 et Sx550X à l'aide de l'interface graphique utilisateur (GUI) et de l'interface de ligne de commande (CLI).

Table des matières

- [Introduction](#)
- [Périphériques et version logicielle applicables](#)
- [Conditions préalables](#)
- [Importer à l'aide de l'interface utilisateur graphique](#)
- [Erreurs possibles Erreur d'en-tête de clé manquanteÉchec du chargement de l'erreur de clé publique](#)
- [Importer à l'aide de CLI](#)
- [Conclusion](#)

Introduction

L'un des problèmes rencontrés lors de l'importation d'un certificat sur les commutateurs Sx350 et Sx550X est que l'**en-tête de clé** de l'utilisateur **est manquant** et/ou **n'a pas pu charger** les erreurs de **clé publique**. Ce document explique comment dépasser ces erreurs pour importer un certificat avec succès. Un certificat est un document électronique qui identifie une personne, un serveur, une société ou une autre entité et associe cette entité à une clé publique. Les certificats sont utilisés dans un réseau pour fournir un accès sécurisé. Les certificats peuvent être autosignés ou signés numériquement par une autorité de certification externe. Un certificat auto-signé, comme son nom l'indique, est signé par son propre créateur. Les autorités de certification gèrent les demandes de certificat et délivrent des certificats aux entités participantes telles que les hôtes, les périphériques réseau ou les utilisateurs. Un certificat numérique signé par une autorité de certification est considéré comme une norme de l'industrie et plus sécurisé.

Périphériques et version logicielle applicables

- 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

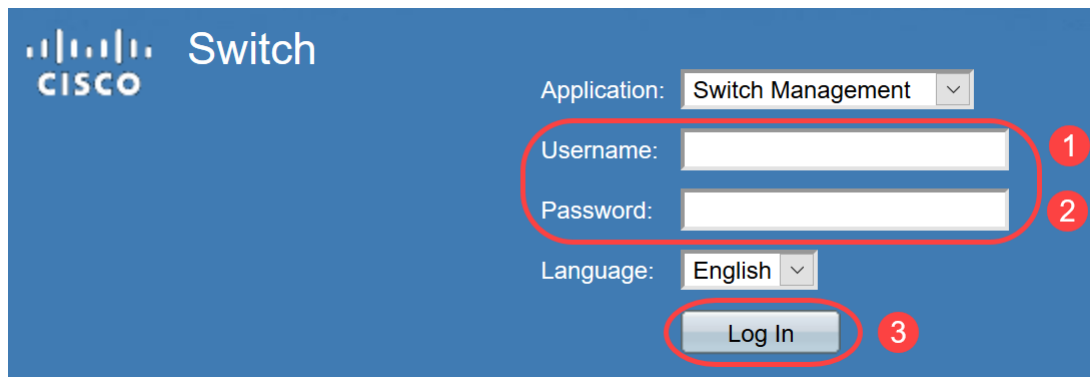
Conditions préalables

Vous devez avoir un certificat auto-signé ou d'autorité de certification (CA). Les étapes pour obtenir un certificat auto-signé sont incluses dans cet article. Pour en savoir plus sur les certificats CA, cliquez [ici](#).

Importer à l'aide de l'interface utilisateur graphique

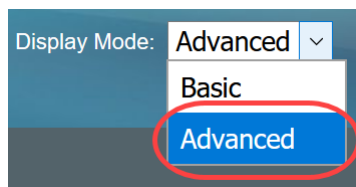
Étape 1

Connectez-vous à l'interface utilisateur graphique du commutateur en entrant votre *nom d'utilisateur* et votre *mot de passe*. Cliquez sur **Connexion**.



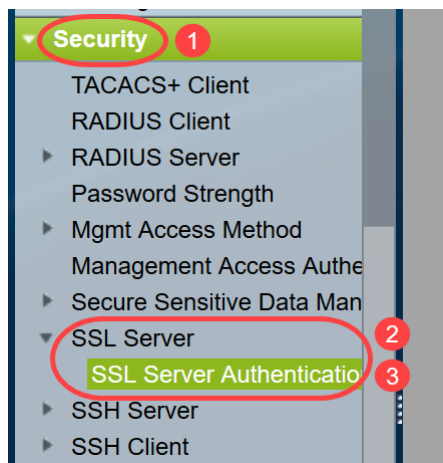
Étape 2

Dans le *mode Affichage* en haut à droite de l'interface utilisateur graphique, sélectionnez **Avancé** à l'aide de l'option de liste déroulante.



Étape 3

Accédez à **Security > SSL Server > SSL Server Authentication**.



Étape 4

Sélectionnez l'un des certificats *générés automatiquement*. Sélectionnez l'*ID de certificat* 1 ou 2 et

cliquez sur le bouton **Modifier**.

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

Étape 5

Pour générer un certificat auto-signé, dans la nouvelle fenêtre contextuelle, activez *Régénérer la clé RSA* et saisissez les paramètres suivants :

Longueur de la clé

Nom commun

Unité d'organisation

Nom de l'organisation

Emplacement

Province

Pays

Durée

Cliquez sur **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
 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

Vous pouvez également créer un certificat à partir d'une autorité de certification tierce.

Étape 6

Vous pouvez maintenant voir le certificat *défini par l'utilisateur* sous la *table des clés du serveur SSL*. Sélectionnez le nouveau certificat et cliquez sur **Détails**.

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... 2 Delete

Étape 7

Dans la fenêtre contextuelle, vous pouvez voir les détails *Certificate*, *Public Key* et *Private Key (Encrypted)*. Vous pouvez les copier sur un autre bloc-notes. Cliquez sur **Afficher les données sensibles en texte clair**.

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

Certificate ID: 2

Certificate: -----BEGIN CERTIFICATE-----
MIIDRzCCAI8CEE90bzMCJXp/nT+78tBROt8wDQYJKoZIhvcNAQELBQAwYjELMAkG
A1UEBhMCVVMxEzARBgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIMQ4wDAYD
VQ4wDAYDQDQDAVDAxNjBzEOMAwGA1UECgwFQ2l2Y28xZzAxBG9wBGA1UEBhMCVVMxEzAR
DTE5MDYxODA1NTc1NloXDTIwMDYxNzA1NTc1NlowYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCkNBTEIGT1JOSUEXETAPBgNVBACMCFNhb3NIMQ4wDAYDQDQDAVDA

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBBgKCAQEAAuxUF71CPBJ6asoghDOEZbiFnXhflPSFDlu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0Jp
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

Étape 10

Sélectionnez le nouveau certificat *défini par l'utilisateur* et cliquez sur **Importer le certificat**.

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

Étape 11

Dans la nouvelle fenêtre contextuelle, activez l'option *Importer la paire de clés RSA* et collez la clé privée (copiée à l'étape 9) en texte clair. Cliquez sur 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
A1UEBhMCVVMxEzARBgNVBAGMCKNBTEIGT1JOSUExETAPBgNVBACMCFNhb1Bkb3NI
MQ4wDAYDVQQDDAVDaXNjbzEOMAwGA1UECgwFQ2l2Y28xCzAJBgNVBAsMAiVtMB4X
DTE5MDYxODA1NTc1Ni0XDTIwMDYxNzA1NTc1Ni0wYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAGMCKNBTEIGT1JOSUExETAPBgNVBACMCFNhb1Bkb3NIIMQ4wDAYDVQQDDAVD
```

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/Spg4xsBwjRZUDafqt2aSkir8L8yHSSD
1BWB09X5fv10QNAMQ+QIDAQAB
```

Private Key: Encrypted 3

Plaintext

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV
5jpe0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhiCMmAx1pegbLvb/A+glnieTgB/Z2EL3eT2
xjT0MyqFImBPNuL4awjvt9E7IEXBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3
G6wxAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcypyv+y88P/DQ/Spg4xsBwjRZUDafqt2aSkir8L8yH
SSD1BWB09X5fv10QNAMQ+QIDAQABAoIBAAIZH0Lq1V/I45VC/5PKZmOczkr426JO4DdhFcXdzMI8PzQ6
```

Apply Close Display Sensitive Data as Plaintext

Dans cet exemple, le mot clé RSA est inclus dans les DEBUTS et FIN de la clé publique.

Étape 12

La notification de réussite s'affiche à l'écran. Vous pouvez fermer cette fenêtre et enregistrer la configuration sur le commutateur.

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

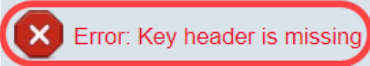
Public Key: -----BEGIN PUBLIC KEY-----
MIIBBgKCAQEAAuxUF71CPBJ6asoghDOEZbifnXhfiPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5jpe0J
p8CFuMH/Azi9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peqLvb/A+glnieTaB/Z2EL3eT2xjJT0My
qFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wxACel
2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafqt2aSkIrl8L8yHSSD1BWB0
9X5fiv10QNAMQ+QIDAQAB

Private Key: Encrypted

Plaintext -----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAAuxUF71CPBJ6asoghDOEZbifnXhfiPSFDIu0SGDtwQHJ7doPp6XVMh7ZCC1TuVWdV5j
pe0Jp8CFuMH/Azi9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peqLvb/A+glnieTaB/Z2EL3eT2xjJT
0MyqFlmBPNuL4awivtt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6wx
ACel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcBvRcpvy+v88P/DQ/Spq4xsBwirZUDafqt2aSkIrl8L8yHSSD1B
WB09X5fiv10QNAMQ+QIDAQAB

Apply Close Display Sensitive Data as Plaintext

Vous avez reçu le message, *Erreur : En-tête de clé manquant*. Fermez la fenêtre. Quelques modifications peuvent être apportées pour faire disparaître ce problème.



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
MQ4wDAYDVQQDDAVDAwXNjbzEOMAwGA1UECgwFQ2IzY28xCzAJBgNVBAsMAIVTMB4X
DTE5MDYxODA1NTc1Nl0XDTIwMDYxNzA1NTc1Nl0wYjELMAkGA1UEBhMCVVMxEzAR
BgNVBAgMCKNBTEIGT1JOSUEXETAPBgNVBACMFNhbIBk3NIMQ4wDAYDVQQDDAVDA
```

Import RSA Key-Pair: Enable

★ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peglVb/A+glnieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcpyv+y88P/DQ/Spg4xsBwjrzUDafqt2aSkIrl8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

★ Private Key: Encrypted
 Plaintext

Pour corriger cette erreur :

Ajoutez le mot clé *RSA* au début de la clé publique : *COMMENCER LA CLÉ PUBLIQUE RSA*

Ajoutez le mot clé *RSA* à la fin de la clé publique : *TERMINER LA CLÉ PUBLIQUE RSA*

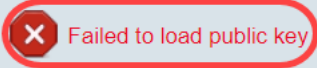
Supprimez les 32 premiers caractères du code clé. La partie mise en surbrillance ci-dessous est un exemple des 32 premiers caractères.

```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuxUF71CPBJ6asoghDOEZbifnXhflPSFDIu0SGDtwQHJ7doPp6XVMh7ZZC1TuVWdV5jpe
0Jp8CFuMH/Azj9JDR1fsVqBAFU2v0L+jhPS5VDN63iUHjeAhlCMmAx1peglVb/A+glnieTgB/Z2EL3eT2xjJT
0MyqFImBPNuL4awjvt9E7IEXhBt1HL0Nr/cuWTLmAOIDmImKN2CRHuz2cxjp0+uA2bY85bNefQoJbE3G6w
xAcel2n4dmK4GFQvOxzS0A5PcsKUMefaeF/afcbvRcpyv+y88P/DQ/Spg4xsBwjrzUDafqt2aSkIrl8yHSSD
1BWB09X5fjv10QNAMQ+QIDAQAB
```

Lorsque vous appliquez les paramètres, vous n'obtiendrez pas l'*en-tête de clé* dans la plupart des cas.

Échec du chargement de l'erreur de clé publique

Scénario 2 : Vous avez généré un certificat sur un commutateur et l'avez importé sur un autre



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
DgYDVQQIDAdiYXJ5J5YW5hMRAwDgYDVQQHDAdHdXJnYW9uMRAwDgYDVQQDDAcwLjAu

Import RSA Key-Pair: Enable

Public Key: -----BEGIN RSA PUBLIC KEY-----
MIIBCAgKCAQEAqAgqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLrV8LtbFIq3QilBHDtL
J07Pj29mgdVFHX/p3ArKS3QjuDST2I/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJI/ejOaYIGA10GX8eIT8lx
lfMblJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWReDU9gb8WLFrdnNQHGWWR/N794H
gAu0HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCCuAFil92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBe
PI1yaWiSOqaG0zgjir7YQIDAQAB

Private Key: Encrypted

Plaintext

Apply Close Display Sensitive Data as Plaintext

Pour corriger cette erreur, NE supprimez PAS les 32 premiers caractères de la clé publique dans ce cas.

▲ 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-----
MIIDSTCCAIECEHV4jm/bIKGoJFHmCvnyTWUwDQYJKoZIhvcNAQELBQAwYzELMAkG
A1UEBhMCSU4xEDA0BgNVBAGMB0hhcnlhbmExEDA0BgNVBAMBA0d1cmdhb24xEDAO
BgNVBAMMBzAuMC4wLjAxDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVDaXNjbzAe
Fw0xOTA2MTkwMjQyMzRaFw0yMDA2MTgwMjQyMzRaMGMAcCzAJBgNVBAYTAkOMRAw
DgYDVQQIDAdiYXJ5J5YW5hMRAwDgYDVQQHDAhhdXJnYW9uMRAwDgYDVQQDDAcwLjAu
```

Import RSA Key-Pair: Enable

Public Key:


```
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEApaAqvAcD58ScvYwW5vzx/oy4ryP3fqiO8QHfzQsMSCCHrq5repNDfLFRV8LtbFlq3QilBHDtLJ
07Pj29mgdVFHX/p3ArKS3QiuDST2/+A0CGVNJ5ZPG8qKw58HWRIMcyv0vblqDJl/ejOaYiGA10GX8eiT8lxfM
blJomiiFd/MWOf8C2/3nmbhKk/LsKI+koTucCbquVfshpwP2WdWWRReDU9qb8WLFrdnNqhgWR/N794HgAu0
HyxpT7qDOVrYv4FAGIR1pblDdAYHe8/sVXUCuAFil92aDPeK1ZCMAcDJaMaQ4trqx/Km6vgBnvBePl1yaW
iSogaG0zqjir7YQIDAQAB
```

Private Key: Encrypted Plaintext


```
roiJNnzjgteU9ggzGvA6re1+f9z4tqwGn+9/reRq3J16w8vriA3wucP9lmyRIUCqYEAUjA3K3f+pRgBO/vDm0Wn
lFkSmiG6azhiA4YrRQpVi8uEU7neT7edoNTXjXEB/zpt0hQBHicv1xsc5qv2KvvpTx8k0u5uBgv9hP1qGsEuePc
G+ynDTFdYImZLc0pDEtGwBKV362YnyX4rCZT67RVXBRI3geAmN30DqpygcYLMCgYEAiqhyEg9cWrkQS03
e904lVAClgjVG05nfeE6Q1BFt8sTDDOGoSKGzLYhRxlkLOXRP990Z2Guqt3xKlViqhFmZH0YaStLkEY8hzr/
uTejGQLoCYNoZAQzC1Ac+rjQneCbQ4GIDua0amyetkAjEUoa7cx2skaoziQSIC3dw2F5tw=
-----END RSA PRIVATE KEY-----
```

Importer à l'aide de CLI

Étape 1

Pour importer un certificat à l'aide de l'interface de ligne de commande, entrez la commande suivante.

```
switch(config)#crypto certificate [numéro de certificat] import
```

Le certificat 2 est importé dans cet exemple.

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

Étape 2

Collez l'entrée ; ajoutez un point (.) sur une ligne distincte après l'entrée.

```
--COMMENCER LA CLÉ PRIVÉE RSA--
MIIEVgIBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQC/rZQ6f0rj8neA
...24 lignes tronquées...
h27Zh+aWX7dxakaoF5QokBTqWDHcMAvNluwGiZ/O3BQYgSiI+SYrZXAbUiSvfIR4
NC1WqkWzML6jW+52lD/GokmU
--FIN DE LA CLÉ PRIVÉE RSA--
--COMMENCER LA CLÉ PUBLIQUE RSA--
MIIBCgKCAQEA62Uon9K4/J3gCAK7i9nYL5zYm4kQVQhCcAo7uGblEprxdWkf0l
...3 lignes tronquées...
```

64jc5fzIfNnE2QpgBX/9M40E41BX5Z0B/QIDAQAB

–FIN DE LA CLÉ PUBLIQUE RSA–

–CERTIFICAT DE DÉBUT–

MIIFvTCCBKwgIBAgIRA0OBWg4bkStdWPvCNYjHpbYwDQYJKoZIhvcNAQELBQAww

–28 lignes tronquées...

8S+39m9wPAOZipI0JA1/0IeG7ChLWOXKncMeZWVTIUZaEwVff0cUzqXwJOcsTrMV

JDPTnbKXG56w0Trecu6UQ9HsUBoDQnlsN5ZBht1VyjAP

–CERTIFICAT DE FIN–

.

Le certificat a été importé

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

Valide à partir de : 14 juin 00:00:00 2017 GMT

Valide : 11 septembre 23:59:59 2020 GMT

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

Empreinte digitale SHA : xxxxxxx

Conclusion

Vous avez maintenant appris les étapes permettant d'importer un certificat sur les commutateurs des gammes Sx350 et Sx550X à l'aide de l'interface utilisateur graphique et de l'interface de ligne de commande.