

# Einstellungen für die SSL-Serverauthentifizierung (Secure Sockets Layer) auf stapelbaren Switches der Serie Sx500 bearbeiten

## Ziel

Secure Sockets Layer (SSL) ist ein Protokoll, das hauptsächlich für das Sicherheitsmanagement im Internet verwendet wird. Dabei wird eine Programmschicht verwendet, die sich zwischen der HTTP- und der TCP-Schicht befindet. Für die Authentifizierung verwendet SSL Zertifikate, die digital signiert und an den öffentlichen Schlüssel gebunden sind, um den Besitzer des privaten Schlüssels zu identifizieren. Diese Authentifizierung hilft während der Verbindungszeit. Durch die Verwendung von SSL werden die Zertifikate während des Authentifizierungsprozesses in Blöcken ausgetauscht, die das im ITU-T-Standard X.509 beschriebene Format haben. Anschließend werden von der Zertifizierungsstelle, die eine externe Behörde ist, X.509-Zertifikate ausgestellt, die digital signiert sind.

In diesem Artikel wird erläutert, wie Sie die Einstellungen für die SSL-Serverauthentifizierung bearbeiten und eine Zertifikatsanforderung für die Stackable Switches der Serie Sx500 generieren.

## Anwendbare Geräte

·Stackable Switches der Serie Sx500

## Softwareversion

·1.3.0.62

## Authentifizierungseinstellungen für SSL-Server

Schritt 1: Melden Sie sich beim Switch-Konfigurationsprogramm an, und wählen Sie **Security > SSL Server > SSL Server Authentication Settings**. Die Seite *SSL Server Authentication Settings* (Authentifizierungseinstellungen für SSL-Server) wird geöffnet:

Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
1	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated
2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

**Hinweis:** Folgen Sie den [Informationen zum SSL-Schlüssel bearbeiten](#), um das Zertifikat automatisch zu generieren, [Zertifikatsanforderung](#) zur Neugenerierung der Zertifikatsanforderung durch den Switch [zu generieren](#) und [Zertifikat importieren](#), um das gewünschte Zertifikat und den Schlüssel zu importieren.

## SSL-Schlüsselinformationen bearbeiten

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 checked="" type="checkbox"/>	1	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Edit... Generate Certificate Request... Import Certificate... Details... Delete

Schritt 2: Aktivieren Sie das Kontrollkästchen des aktiven Zertifikats, das in der Tabelle für den SSL-Serverschlüssel bearbeitet werden soll.

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 checked="" type="checkbox"/>	1	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Edit... Generate Certificate Request... Import Certificate... Details... Delete

Schritt 3: Klicken Sie auf **Bearbeiten**, um die Änderungen am vorhandenen Zertifikat vorzunehmen. Das Fenster *Zertifikat bearbeiten* wird angezeigt:

**Hinweis:** In diesem Beispiel wird Zertifikat 1 überprüft.

Certificate ID:  1  
 2

Regenerate RSA Key:

Key Length:  Use Default  
 User Defined  (Range: 512 - 2048, Default: 1024)

Common Name:  (13/64 Characters Used, Default: 0.1.134.160)

Organization Unit:  (10/64 Characters Used)

Organization Name:  (10/64 Characters Used)

Location:  (10/64 Characters Used)

State:  (7/64 Characters Used)

Country:  ASCII Alphanumeric

Duration:  (Range: 30 - 3650 Days)

Generate Close

Schritt 4: Wählen Sie im Feld Certificate ID (Zertifikats-ID) entweder 1 oder 2 als ID des Zertifikats aus. In diesem Feld für die Zertifikats-ID sind nur zwei Optionen verfügbar.

Schritt 5: Aktivieren Sie das Kontrollkästchen im Feld RSA-Schlüssel regenerieren, um den RSA-Schlüssel neu zu generieren.

Schritt 6: Klicken Sie im Feld Schlüssellänge auf eine der beiden Optionsfelder.

·Standard verwenden: Die Standardschlüssellänge wird verwendet.

·Benutzerdefiniert - In diesem Feld kann die Schlüssellänge den Wert 512 bis 2048 haben. Der Standardwert ist 1024. In diesem Beispiel wird 2000 eingegeben.

Schritt 7: Geben Sie im Feld "Common Name" die vollständige URL des Geräts oder eine bestimmte öffentliche IP-Adresse ein. Wenn keine IP-Adresse angegeben ist, wird standardmäßig die niedrigste IP-Adresse des Geräts verwendet (wenn das Zertifikat generiert wird). In diesem Beispiel wird die Standardadresse des SG500X-Switches als allgemeiner Name verwendet.

Schritt 8: Geben Sie im Feld Organisationseinheit den Namen der Organisationseinheit oder -abteilung ein.

Schritt 9: Geben Sie im Feld Organization Name (Organisationsname) den Namen der Organisation ein.

Schritt 10: Geben Sie im Feld Location (Ort) den Namen des Standorts oder der Stadt ein.

Schritt 11: Geben Sie im Feld State (Bundesland) den Namen des Staates oder der Provinz ein.

Schritt 12: Geben Sie im Feld Land den Namen des Landes ein. Da dieser nur alphanumerische Werte akzeptiert, verwenden Sie das globale 2-Buchstaben-Format. In die USA beispielsweise.

Schritt 13: Geben Sie im Feld Dauer die Anzahl der Tage ein, für die eine Zertifizierung gültig ist.

Schritt 14: Klicken Sie auf **Generieren**, um die Einstellungen zu speichern.

Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source
1	192.168.1.254	Org_Unit_1	Org_Name_1	Location_1	State_1	C1	2012-Jun-11	2013-Jun-11	User Defined
2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

## [Erstellen einer Zertifikatsanforderung](#)

## 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 checked="" type="checkbox"/>	1	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Edit...

Generate Certificate Request...

Import Certificate...

Details...

Delete

Schritt 1: Überprüfen Sie auf der Seite *SSL-Serverauthentifizierungseinstellungen* die Zertifikat-ID, und klicken Sie auf **Zertifikatsanforderung generieren**.

Enter the data below and generate certificate.

Certificate ID:  1  
 2

✱ Common Name:  (0/64 Characters Used, Default: 0.1.134.160)

Organization Unit:  (0/64 Characters Used)

Organization Name:  (0/64 Characters Used)

Location:  (0/64 Characters Used)

State:  (0/64 Characters Used)

Country:  ASCII Alphanumeric

Certificate Request:

Generate Certificate Request

Close

Schritt 2: Klicken Sie auf **Zertifikatsanforderung generieren** in der Seite *Einstellungen für SSL-Serverauthentifizierung bearbeiten*.

Enter the data below and generate certificate.

Certificate ID:  1  
 2

Common Name:  (0/64 Characters Used, Default: 0.1.134.160)

Organization Unit:  (0/64 Characters Used)

Organization Name:  (0/64 Characters Used)

Location:  (0/64 Characters Used)

State:  (0/64 Characters Used)

Country:  ASCII Alphanumeric

Certificate Request: 

```
-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAzwCAQAwdjELMAkGA1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAc
UCkxY2F0aW9uXzExFjAUBgNVBAMTDE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW11
XzExEzARBgNVBAUUCk9yZ19Vbml0XzEwggEbmA0GCSqGSIb3DQEBAQUAA4IBCAAwggEDAoH
7AL5ep54S5M7LHRLhNmpXmtuxWw070EhfL2cNTfH1RgfCfEs2zy8xUialNCKSoS/HapX3ry2gJZ
CtjFHmwEUjUrYVHxqF9misXODEacranB1iSx4AMKMLy6ed+8tBN5xanhiUqplrXN1w81pEXHRf
/TiivdifTW2GRmW/sw7e8+GCA0RU
/oRjDpRu1mi3R6z1PU4cK3UMWVzH1hQ5BG+IR+Ju8jOrMseRqjKRROZQz+aHHBPVkwdfly51q
Cuk2R55lsbu2l6Fi7FQ5CY7jw4vj+pO2ZL0uz9q8qsDFxi
-----
```

Im Feld Zertifikatsanforderung werden die verschlüsselten Zertifikatsinformationen angezeigt.

Schritt 3: Klicken Sie auf **Zertifikatsanforderung generieren**, um die Einstellungen zu speichern.

SSL Server Authentication Settings

SSL Active Certificate Number:  1  
 2

Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source	
<input checked="" type="checkbox"/>	1	192.168.1.254	Org_Unit_1	Org_Name_1	Location_1	State_1	C1	2012-Jun-11	2013-Jun-11	User Defined
<input type="checkbox"/>	2	0.0.0.0						2012-Jun-11	2013-Jun-11	Auto Generated

Auf der Seite *SSL Server Authentication Settings* (Authentifizierungseinstellungen für SSL-Server) können Sie das bearbeitete Zertifikat mit allen oben eingegebenen Informationen anzeigen.

- Gültig von - Gibt das Datum an, ab dem das Zertifikat gültig ist.
- Gültig bis: Gibt das Datum an, bis zu dem das Zertifikat gültig ist.
- Zertifikatsquelle - Gibt an, ob das Zertifikat vom System (automatisch generiert) oder vom Benutzer (Benutzerdefiniert) generiert wurde.

## Zertifikat importieren



SSL Server Authentication Settings

SSL Active Certificate Number:  1  2

Certificate ID	Common Name	Organization Unit	Organization Name	Location	State	Country	Valid From	Valid To	Certificate Source	
<input checked="" type="checkbox"/>	1	192.168.1.254	Org_Unit_1	Org_Name_1	Location_1	State_1	C1	2012-Jun-11	2013-Jun-11	User Defined
<input type="checkbox"/>	2	0.0.0.0					2012-Jun-11	2013-Jun-11	Auto Generated	

Schritt 1: Aktivieren Sie das Kontrollkästchen gewünscht, und klicken Sie auf **Zertifikat importieren**, um ein Zertifikat zu importieren.

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-----
MIIDYTCCAIAcEFGqVx5pfJlrm9M+uUyA5UwDQYJKoZIhvdNAQEEBQAwdjELMAkG
A1UEBhMCQzExEDAOBgNVBAgUB1N0YXRlXzExEzARBgNVBAcJClxvY2F0aW9uXzEx
FjAUBgNVBAMTDE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW1lXzExEzAR
BgNVBAsUCk9yZ19Vbml0XzEwHhcNMTIwMTg0NTQ5WWhcNMTIwMTg0NTQ5
WjB2MQswCQYDVQQGEwJDMTEQMA4GA1UECBHU3RhdGVfMTEyMBEGA1UEBxQKTG9j
YXRpb25fMTEwMWBQA1UEAxMNMTkyLjE2OC4xLjI1NDNETMBEGA1UEChQKT3JnX05h
-----END CERTIFICATE-----
```

Import RSA Key-Pair:  Enable

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBAwKB+wDFB1ToNF0tnPghLIT2/ZqP9OKVUu6p5GhEBbcOKfjAVrNy8DS4cSIQldqM8JG+G7klm9LupeFIOAc
lF9FTfp5IetemQ9FEj0RZZxyD5qfdPsmjbaSAGzIXW4ZkWezYtfi33r5e5W3X328lkf12lutUyz3VUCdUKrBmLIPpTM0
zXjhLirk1bfEFVSNs0fPhVSp0fX+UTTpGvw3n1VJ1Ct80bje+r/M/YO+Gx7DnZTrhEpcpptsZ81z8ubb4wY4xAtPnD
/4DWFQkdDwfQetFut32hGu2SakWzAVLVLhgQHhSNmCuFnVUX0OYw0wBvwt3Rkji85RtkarjFagMBAAE=
-----END RSA PUBLIC KEY-----
```

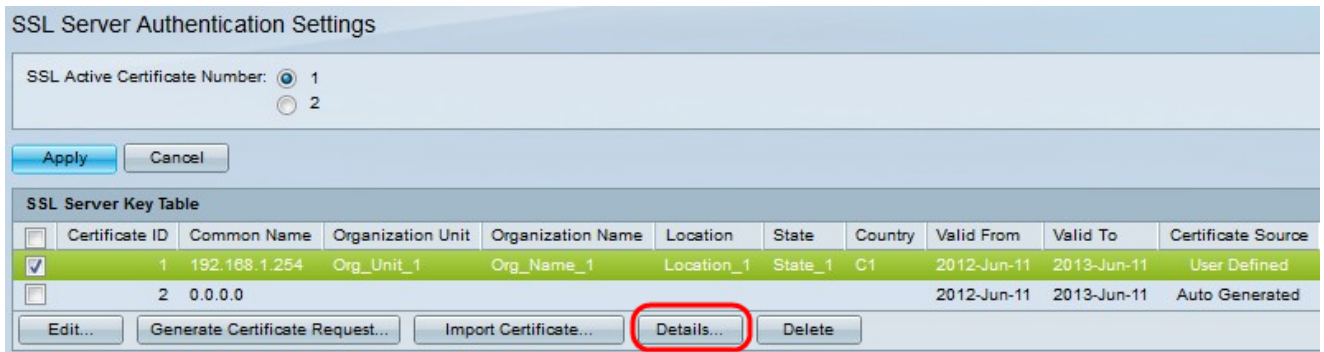
Private Key:  Encrypted  Plaintext

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
SOxOUPh1Gq1Fc39s+49gkYuCnOuDQHGeTf6yM5yuSj5Et4163XgSBRH2CVOcZOLngik+fG9UtvbxIOJq11Sl
l+NjjsMv0HiZyV/DacVsXM2N3kPHELfBNhkowZuA9RL0pIRPNa73pW2BzQ8vWNjudUBMEL8b8pc3i4CNVCrwt
HSNvOo9IA7ZZEHG/TEzNFdE+GShszuzbpTwtD6a4iQVB01BQGh8rMp0u/pL3e9pSayV3+80YYgXNPho
/XWaeEH1udzHqQAG1rW+A
/s8iq2Hsg9+6g8uFJgew2Yh2z7Ls64EMte104wJkbLJwXJWhJinwCyC2PtSnU4dityfC71H7V4V8P0rKavdq1OH
Tu0HXiV9MeEgv3/cp6ptdVyzjm3ybOQbQ82Ywd5S4rRxgeAdumWs/drOHfeoglwqKnqOfvxt03XKk779H8
-----END RSA ENCRYPTED PRIVATE KEY-----
```

- Zertifikat-ID - Wählen Sie das aktive Zertifikat aus.
- Zertifikat - Kopieren oder fügen Sie das Zertifikat in eine konfigurierte Datei ein.
- RSA KEY-Pair importieren — Wählen Sie, um das RSA-Schlüsselpaar zu aktivieren.
- Öffentlicher Schlüssel (verschlüsselt) - Kopieren oder Einfügen des öffentlichen Schlüssels in verschlüsselter Form.
- Privater Schlüssel (Klartext) - Kopieren oder fügen Sie den privaten Schlüssel in Textform ein.

·Sensitive Daten als verschlüsselt anzeigen - Wählen Sie diese Option aus, damit die privaten Schlüssel verschlüsselt in die Konfigurationsdatei geschrieben werden können.

Schritt 2: Klicken Sie auf **Übernehmen**.



Schritt 3: (Optional) Klicken Sie auf die gewünschte Zertifikat-ID und anschließend auf **Details**, um Details zu den SSL-Details anzuzeigen.



Schritt 4: (Optional) Klicken Sie auf die gewünschte Zertifikat-ID, und klicken Sie auf **Löschen**, um die SSL-Serverdetails aus der Tabelle des SSL-Servers zu löschen.