

Modifica delle impostazioni di autenticazione server Secure Sockets Layer (SSL) sugli switch impilabili serie Sx500

Obiettivo

SSL (Secure Sockets Layer) è un protocollo utilizzato principalmente per la gestione della sicurezza su Internet. Utilizza un livello di programma situato tra i livelli HTTP e TCP. Per l'autenticazione, SSL utilizza certificati con firma digitale e associati alla chiave pubblica per identificare il proprietario della chiave privata. Questa autenticazione consente di controllare l'operatività durante la connessione. Tramite SSL, i certificati vengono scambiati in blocchi durante il processo di autenticazione nel formato descritto nello standard ITU-T X.509. Successivamente, vengono rilasciati certificati X.509 firmati digitalmente dall'autorità di certificazione che è un'autorità esterna.

In questo documento viene spiegato come modificare le impostazioni di autenticazione del server SSL e come generare una richiesta di certificato sugli switch impilabili serie Sx500.

Dispositivi interessati

•Switch Stack Serie Sx500

Versione del software

•1.3.0.62

Impostazioni autenticazione server SSL

Passaggio 1. Accedere all'utility di configurazione dello switch e scegliere **Sicurezza > Server SSL > Impostazioni di autenticazione server SSL**. Viene visualizzata la pagina *Impostazioni autenticazione server SSL*:

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						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

Nota: Seguire le istruzioni [Modifica informazioni chiave SSL](#) per generare il certificato automaticamente, [Genera richiesta certificato](#) per generare nuovamente la richiesta di certificato da parte dello switch e [Importa certificato](#) per importare il certificato desiderato e la chiave.

Modifica informazioni chiave SSL

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

Passaggio 2. Selezionare la casella di controllo del certificato attivo che si desidera modificare nella tabella delle chiavi del server SSL.

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

Passaggio 3. Fare clic su **Modifica** per apportare le modifiche al certificato esistente. Viene visualizzata la finestra *Modifica certificato*:

Nota: In questo esempio, il certificato 1 è selezionato.

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

Passaggio 4. Nel campo ID certificato scegliere 1 o 2 come ID del certificato. In questa configurazione sono disponibili solo due opzioni nel campo ID certificato.

Passaggio 5. Selezionare la casella di controllo nel campo Rigenera chiave RSA per rigenerare la chiave RSA.

Passaggio 6. Nel campo Lunghezza chiave, fare clic su uno dei pulsanti di opzione.

·Usa default - Viene utilizzata la lunghezza di default della chiave.

·Definita dall'utente: in questo campo, la lunghezza della chiave può essere compresa tra 512 e 2048. Il valore predefinito è 1024. Nell'esempio, viene immesso 2000.

Passaggio 7. Nel campo Nome comune, immettere l'URL completo del dispositivo o l'indirizzo IP pubblico specifico. Se lasciato vuoto, per impostazione predefinita viene utilizzato l'indirizzo IP più basso del dispositivo (quando viene generato il certificato). Nell'esempio, l'indirizzo predefinito dello switch SG500X viene usato come nome comune.

Passo 8: nel campo Unità organizzazione inserire il nome dell'organizzazione-unità o del reparto.

Passaggio 9. Nel campo Nome organizzazione, inserire il nome dell'organizzazione.

Passaggio 10. Nel campo Ubicazione, inserire il nome dell'ubicazione o della città.

Passaggio 11. Nel campo Stato, immettere il nome dello stato o della provincia.

Passaggio 12. Nel campo Paese, inserire il nome del paese. Poiché questa opzione accetta solo valori alfanumerici, utilizzare il formato globale a 2 lettere. Ad esempio, per gli Stati Uniti immettere US.

Passaggio 13. Nel campo Durata immettere il numero di giorni di validità di una certificazione.

Passaggio 14. Fare clic su **Genera** per salvare le impostazioni.

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

[Genera una richiesta di certificato](#)

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

Passaggio 1. Nella pagina *Impostazioni autenticazione server SSL*, controllare l>ID certificato e fare clic su **Genera richiesta certificato**.

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

Passaggio 2. Fare clic su **Genera richiesta certificato** nella pagina *Modifica impostazioni di autenticazione server SSL*.

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
UCkxY2F0aW9uXzExFjAUBgNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW11
XzExEzARBgNVBAsUCk9yZ19Vbml0XzEwggEbMA0GCsqGSIb3DQEBAQUAA4IBCAAwggEDAoH
7AL5ep54S5M7LHRLhNmpXmtuxWw070Ehfl2cNTfH1RgfCFes2zy8xUialNCKSoS/HapX3ry2gJZ
CtjFHmwEUjpUrYvHxqF9misXODEacranB1iSx4AMKMLy6ed+8tBN5xanhiUqplrxN1w81pEXHRf
/TiivdifTW2GRmW/sw7e8+GCA0RU
/oRjDpRu1mi3R6z1PU4cK3UMWVzH1hQ5BG+IR+Ju8jOrMseRqjKRROZQz+aHHBPVkwdfly51q
Cuk2R55lsbu2l6Fi7FQ5CY7jw4vj+pO2ZL0uz9q8qsDFxi
-----
```

Nel campo Richiesta certificato è ora possibile visualizzare le informazioni sul certificato crittografato.

Passaggio 3. Fare clic su **Genera richiesta certificato** per salvare le impostazioni.

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	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

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

A questo punto, nella pagina *Impostazioni autenticazione server SSL* è possibile visualizzare il certificato modificato con tutte le informazioni immesse in precedenza.

- Valido - Specifica la data a partire dalla quale il certificato è valido.
- Valido fino a - Specifica la data fino alla quale il certificato è valido.
- Origine certificato — specifica se il certificato è stato generato dal sistema (generato automaticamente) o dall'utente (definito dall'utente).

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 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

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

Passaggio 1. Selezionare la casella di controllo desiderata e fare clic su **Importa certificato** per importare un certificato.

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-----
MIIDYTCCAIAACEFgqVx5pfJlr9M+uUyA5UwDQYJKoZIhvcNAQEEBQAwdjELMAkG
A1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAcJClxvY2F0aW9uXzEx
FjAUBgNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW1lXzExEzAR
BgNVBAsUCk9yZ19Vbml0XzEwHhcNMTEwNjExMTg0NTQ5WWhcNMTEwNjExMTg0NTQ5
WjB2MzQwCQYDVQQGEWJDMTEQMA4GA1UECBQHU3RhdGVfMTETMBEGA1UEBxQKTG9j
YXRpb25fMTEwMzQwCQYDVQQA1UEAxMNMTkyLjE2OC4xLjI1NDQ5WWhcNMTEwNjEx
-----
```

Import RSA Key-Pair: Enable

★ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBAwKB+wDFB1ToNF0tnPghLIT2ZqP9OKVUu6p5GhEBbcOKfjAVrNy6DS4cSIQldqM6JG+G7klm9LupeFIOAc
lf9FTfp5IetemQ9FEj0RZZxfyD5qfdPsmjbaSAGzIXW4ZkWezYtfi33r5e5W3X328lkl2lutUyz3VUCdUKrBmLIPpTM0
zXjhLirk1bIEFVSN50fPhVSp0fX+UTTpGww3n1VJ1Ct80bje+tr/M/YO+Gx7DnZTrhEpcocptsZ81z6ubb4wY4xAtPnD
/4DWFQkdDwfQetFut32hGu2SakWzAVLVLhgQHnSNmCuFnVUX0OYW0wBwvt3RKJi85RtkarjFagMBAAE=
-----END RSA PUBLIC KEY-----
```

★ Private Key: Encrypted Plaintext

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
SOxOUPh1Gq1Fc39s+49gkYuCnOuDQHGeTf6yM5yUjSj5Et4163XgSBRH2CVOcZOLngik+fG9UtvbxlOJq11SI
l+NjjsMv0HiZyV/DacVsXM2N3kPHELfBNhkovZuA9RL0pIRPNa73pW2BzQ6vWNjudUBMEL6b6pc3I4CNVCrwt
HSNvOo9IA7ZZEHG/TEzNFdE+GShszuzbpTwtD6a4iQVB01BQGh8rMp0u/pL3e9pSayV3+60YYgXNPho
/XWaEH1udzHqQAG1lrW+A
/s8iq2Hsg9+6g6uFJgew2Yh2z7Ls64EMte104wJkbLJrwXJWhJirwCyC2PtSnU4dityfC71H7V4V8P0rKavdq1OH
Tu0HXiV9MeEgv3/cp6ptdVyJzjm3vbOQbQ62Ywwd5S4rRxgeAdumWsdR0HfeogIwqKNqOfvdk03XkK779H8
-----
```

Apply Close Display Sensitive Data As Plaintext

- ID certificato — Scegliere il certificato attivo
- Certificato — Copia o incolla il certificato in un file configurato.
- Importa coppia di chiavi RSS: scegliere se abilitare la coppia di chiavi RSA.
- Chiave pubblica (crittografata) — Copia o incolla la chiave pubblica in forma crittografata.
- Chiave privata (testo normale) — Copia o incolla la chiave privata in formato testo normale.
- Visualizza dati sensibili come crittografati: scegliere questa opzione se si desidera che le chiavi private vengano scritte in forma crittografata nel file di configurazione.

Passaggio 2. Fare clic su **Applica**.

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 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

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

Passaggio 3. (Facoltativo) Fare clic sull'ID certificato desiderato e fare clic su **Dettagli** per visualizzare i dettagli SSL.

Certificate ID: 1

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDYTCCAIACEFGqVx5pfPjlr9M+uUyA5UwDQYJKoZIhvcNAQEEBQAwdjELMAkG
A1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAcJClxvY2F0aW9uXzEx
FjAUBgNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW11XzExEzAR
BgNVBAsUCk9yZ19Vbml0XzEwHhcNMTEwNjExMTg0NTQ5WhcNMTEwNjExMTg0NTQ5
WjB2MQswCQYDVQQGEwJDMTEQMA4GA1UECBHU3RhdGVmTETMBEQA1UEBxQKTG9j
YXRpb25fMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEw
-----END CERTIFICATE-----
```

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBAwKB+wDFB1ToNF0tnPghLIT2/ZqP9OKVUu6p5GhEBbcOKfjAVrNy6DS4cSIQIdqM6JG+G7klm9LupEFlOAc
If9FTfp5IetemQ9FEj0RZZxfyD5qfdPsmjbaSAGzIXW4ZkWezYtfi33r5e5W3X328lkf2IutUyz3VUCdUKrBmLIPpTM0
zXjhLink1bfEFVSNs0fPhVSp0fX+UTTpGww3n1VJ1Ct80bje+r/M/YO+Gx7DnZTrhEpcptsZ81z6ubb4wY4xAtPnD
/4DWFQkdDwfFut32hGu2SakWzAVLVLhgQHnSNmCuFnVUX0OYW0wBwvt3Rkji85RtkarjFAgMBAAE=
-----END RSA PUBLIC KEY-----
```

Fingerprint(Hex): B2:BA:C6:EB:E5:FE:DE:83:46:58:EC:87:77:7F:B5:8F:EE:A5:90:55

Private Key (Encrypted):

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
SOxOUPh1Gq1Fc39s+49gkYuCnOuDQHGeTf6yM5yuISj5Et4163XgSBARH2CVOccZOLngik+fG9UtvbxiOJq1SI
I+NjjsMv0HiZyV/DacVsXM2N3kPHELfBNhkwZuA9RL0pIRPNa73pW2BzQ6vWNjudUBMEL8b6pc3I4CNVCrwt
HSNvOo9IA7ZZEHG/TEzNFdE+GShszuzbpTWTd6a4iQVB01BQGH8rM0u/pL3e9pSayV3+60YYgXNPho
/XWaeEH1udzHqQAG1lrW+A
/s8iq2Hsg9+6g6uFJgew2Yh2z7Ls64EMte104wJkbLJrwXJWhJinwCyC2PtSnU4dityfC71H7V4V8P0rKavdq1OH
Tu0HXiV9MeEgv3/cp8ptdVyzjm3vbOQbQ62Ywd5S4rRxgeAdumWs/drOHeogIWqKNqOfvxx03XKk779H8
-----END RSA ENCRYPTED PRIVATE KEY-----
```

Close Display Sensitive Data As Plaintext

Passaggio 4. (Facoltativo) Fare clic sull'ID certificato desiderato e fare clic su **Elimina** per eliminare i dettagli del server SSL dalla tabella del server SSL.