

Editar configurações de autenticação de servidor SSL (Secure Sockets Layer) em switches empilháveis Sx500 Series

Objetivo

O Secure Sockets Layer (SSL) é um protocolo usado principalmente para gerenciamento de segurança na Internet. Ele usa uma camada de programa localizada entre as camadas HTTP e TCP. Para autenticação, o SSL usa certificados que são assinados digitalmente e vinculados à chave pública para identificar o proprietário da chave privada. Essa autenticação ajuda durante a conexão. Através do uso de SSL, os certificados são trocados em blocos durante o processo de autenticação, que estão no formato descrito na norma ITU-T X.509. Em seguida, pela autoridade de certificação que é uma autoridade externa, são emitidos certificados X.509 que são assinados digitalmente.

Este artigo explica como editar as configurações de autenticação do servidor SSL e como gerar uma solicitação de certificado nos Switches empilháveis Sx500 Series.

Dispositivos aplicáveis

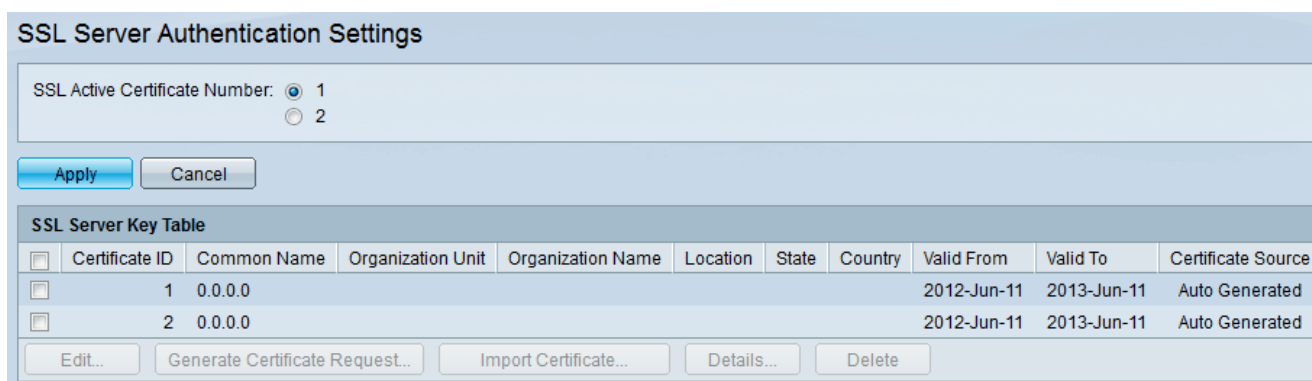
Switches Empilháveis Sx500 Series

Versão de software

•1.3.0.62

Configurações de autenticação do servidor SSL

Etapa 1. Faça login no Switch Configuration Utility e escolha **Security > SSL Server > SSL Server Authentication Settings**. A página *Configurações de Autenticação de Servidor SSL* é aberta:



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

Note: Siga [Edit SSL Key Information](#) para gerar o certificado automaticamente, [Generate Certificate Request](#) para gerar novamente a solicitação de certificado pelo switch e [Import Certificate](#) para importar o certificado desejado e a chave.

[Editar informações de chave SSL](#)

SSL Server Authentication Settings

SSL Active Certificate Number: 1
 2

<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

Etapa 2. Marque a caixa de seleção do certificado ativo que deseja editar na Tabela de chaves do servidor SSL.

SSL Server Authentication Settings

SSL Active Certificate Number: 1
 2

<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

Etapa 3. Clique em **Editar** para fazer as alterações no certificado existente. A janela *Editar certificado* é exibida:

Note: Neste exemplo, certificado 1 é verificado.

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)

Etapa 4. No campo ID do certificado, escolha 1 ou 2 como ID do certificado. Há apenas 2 opções disponíveis no campo ID do certificado nesta configuração.

Etapa 5. Marque a caixa de seleção no campo Regenerar chave RSA para regenerar a chave RSA.

Etapa 6. No campo Tamanho da chave, clique em um dos botões de opção.

Usar padrão — O comprimento da chave padrão é usado.

Definido pelo usuário — Neste campo, o comprimento da chave pode ter o valor de 512 a 2048. O valor padrão é 1024. Neste exemplo, 2000 é inserido.

Passo 7. No campo Common Name (Nome comum), insira a URL do dispositivo totalmente qualificada ou um endereço IP público específico. Se deixado em branco, o padrão é o endereço IP mais baixo do dispositivo (quando o certificado é gerado). Neste exemplo, o endereço padrão do switch SG500X é usado como nome comum.

Etapa 8. No campo Unidade da organização, insira o nome da unidade da organização ou do departamento.

Etapa 9. No campo Nome da organização, insira o nome da organização.

Etapa 10. No campo Local, insira o nome do local ou da cidade.

Etapa 11. No campo Estado, insira o nome do estado ou província.

Etapa 12. No campo País, insira o nome do país. Como isso aceita apenas um valor alfanumérico, use o formato global de 2 letras. Por exemplo, para os Estados Unidos, entre nos EUA.

Etapa 13. No campo Duração, insira o número de dias em que uma certificação é válida.

Etapa 14. Clique em **Gerar** para salvar as configurações.

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

Gerar uma solicitação de certificado

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

Etapa 1. Na página *Configurações de autenticação do servidor SSL*, verifique a ID do certificado e clique em **Gerar solicitação de certificado**.

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

Etapa 2. Clique em **Gerar solicitação de certificado** na página *Editar configurações de autenticação do servidor 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
/TiivIdifTW2GRmW/sw7e8+GCA0RU
/oRjDpRu1mi3R6z1PU4cK3UMWVzH1hQ5BG+IR+Ju8jOrMseRqjKRROZQz+aHHBPV/kwdfly51q
Cuk2R55lsbu2l6Fi7FQ5CY7jw4vj+pO2ZL0uz9q8qsDFxi
-----
```

Agora, no campo Solicitação de certificado, você pode ver as informações de certificado criptografado.

Etapa 3. Clique em **Gerar solicitação de certificado** para salvar as configurações.

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

Agora, na página *Configurações de autenticação do servidor SSL*, você pode ver o certificado editado com todas as informações inseridas acima.

Válido de — Especifica a data a partir da qual o certificado é válido.

Válido até — Especifica a data até a qual o certificado é válido.

Fonte do certificado — Especifica se o certificado foi gerado pelo sistema (Gerado automaticamente) ou pelo usuário (Definido pelo usuário).

Importar certificado

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

Etapa 1. Clique na caixa de seleção desejada e clique em **Importar certificado** para importar um certificado.

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
A1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAcJckxvY2F0aW9uXzEx
FjAUBgNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW1lXzExEzAR
BgNVBAsUCk9yZ19Vbml0XzEwHhcNMTEwNjExMTg0NTQ5WkdNMTMwNjExMTg0NTQ5
WjB2MzQswCQYDVQQGEwJDMTEQMA4GA1UECBQHU3RhdGVfMTETMBEGA1UEBxQKTG9j
YXRpb25fMTEwMzQ1UEAxMNMTEyLjE2OC4xLjI1NDQ5MTEwMzQ1UEBBAQ==
-----
```

Import RSA Key-Pair: Enable

★ Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBAwKB+wDFB1ToNF0tnPghLIT2/zqP9OKVUu6p5GhEBbcOKfjAVrNy6DS4cSIQldqM6JG+G7klm9LupeFIOAc
If9FTfp5IetemQ9FEj0RZZxfyD5qfdPsmjbaSAGzIXW4ZkWezYtfi33r5e5W3X328lkf2IutUyz3VUCdUKrBmLIPpTM0
zXjHLrk1bIEFVSN50fPhVSp0fX+UTTpGvw3n1VJ1Ct80bje+r/M/YO+Gx7DnZTrhEpcocptsZ81z6ub4wY4xAtPnD
/4DWFQkdDwfQetFut32hGu2SakWzAVLVLhgQHnSNmCuFnVUX0OYW0wBwvt3Rkji85RtkarjFAgMBAAE=
-----
```

★ Private Key: Encrypted Plaintext

```
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
SOxOUPh1Gq1Fc39s+49gkYuCnOuDQHGeTf6yM5yulSj5Et4163XgSBARH2CVOcZOLngik+fG9UtvbxlOJq11SI
I+NjjsMv0HiZyV/DacVsXM2N3kPHELFBNhKowZuA9RL0pIRPNa73pW2BzQ6vWNjudUBMEL6b6pc3I4CNVCrwt
HSNvOo9IA7ZZEHG/TEzNFdE+GShszuzbpTwtD6a4iQVB01BQGh8rMp0u/pL3e9pSayV3+60YYgXNPho
/XWaEH1udzHqQAG1lrW+A
/s8iq2Hsg9+6g6uFJgew2Yh2z7Ls64EMte104wJkbLJrwXJWhJirwCyC2PtSnU4dityfC71H7V4V8P0rKavdq1OH
Tu0HXiV9MeEgv3/cp6ptdVyzjm3vbOQbQ62Yywd5S4rRxgeAdumWsdR0HfheogIwqKNqOfvx03XKk779H8
-----
```

Apply Close Display Sensitive Data As Plaintext

ID do certificado — Escolha o certificado ativo

Certificado — Copie ou cole o certificado em um configurado.

Import RSS KEY-Pair — Escolha para habilitar o par de chaves RSA.

Public Key (Encrypted) — Copie ou cole a chave pública numa forma encriptada.

Chave privada (Texto simples) — Copie ou cole a chave privada em formato de texto simples.

Exibir Dados Sensíveis como Criptografados — Escolha esta opção para que as chaves privadas sejam gravadas de forma criptografada no arquivo de configuração.

Etapa 2. Clique em Apply.

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

Etapa 3. (Opcional) Clique na ID de certificado desejada e clique em **Detalhes** para ver os detalhes do SSL.

Certificate ID: 1

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDYTCCAIACEFGqVx5pfPjlr9M+uUyA5UwDQYJKoZIhvcNAQEEBQAwdjELMAkG
A1UEBhMCQzExEDAOBgNVBAGUB1N0YXRlXzExEzARBgNVBAcJClxvY2F0aW9uXzEx
FjAUBgNVBAMTDTE5Mi4xNjguMS4yNTQxExARBgNVBAoUCk9yZ190YW11XzExEzAR
BgNVBAsUCk9yZ19Vbml0XzEwHhcNMTEwNjExMTg0NTQ5WhcNMTEwNjExMTg0NTQ5
WjB2MQswCQYDVQQGEwJDMTEQMA4GA1UECBHU3RhdGVfMTETMBEGA1UEBxQKTG9j
YXRpb25fMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEw
-----END CERTIFICATE-----
```

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
MIIBAwKB+wDFB1ToNF0tnPghLIT2/ZqP9OKVUu6p5GhEBbcOKfjAVrNy6DS4cSIQIdqM6JG+G7klm9LupEFlOAc
If9FTfp5IetemQ9FEj0RZZxfD5qfdPsmjbaSAGzIXW4ZkWezYtFi33r5e5W3X328lkf2IutUyz3VUCdUKrBmLIPpTM0
zXjhLink1bfEFVSNs0fPhVSp0fX+UTTpGww3n1VJ1Ct80bje+r/M/YO+Gx7DnZTrhEpcptsZ81z6ubb4wY4xAtPnD
/4DWFQkdDwfQetFut32hGu2SakWzAVLVLhgQHnSNmCuFnVUX0OYW0wBwvt3Rkji85RtkarjFAgMBAAE=
-----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+49gkYuCnOuDQHGeTf6yM5yuISj5Et4163XgSBRH2CVOcZOLngik+fG9UtvbxiOJq1SI
I+NjjsMv0HiZyV/DacVsXM2N3kPHELfBNhkowZuA9RL0pIRPNa73pW2BzQ6vWNjudUBMEL8b6pc3I4CNVCrwt
HSNvOo9IA7ZZEHG/TEzNFdE+GShszuzbpTWTd6a4iQVB01BQGH8rfMp0u/pL3e9pSayV3+60YYgXNPho
/XWaeEH1udzHqQAG1lrW+A
/s8iq2Hsg9+6g6uFJgew2Yh2z7Ls64EMte104wJkbLJrwXJWhJinwCyC2PtSnU4dityfC71H7V4V8POrKavdq1OH
Tu0HXiV9MeEgv3/cp8ptdVyzjm3vbOQbQ62Ywd5S4rRxgeAdumWs/drOHfeogIWqKNqOfvxx03XKk779H8
-----END RSA ENCRYPTED PRIVATE KEY-----
```

Close Display Sensitive Data As Plaintext

Etapa 4. (Opcional) Clique na ID de certificado desejada e clique em **Excluir** para excluir os detalhes do servidor SSL da tabela do servidor SSL.