Configuration Guide

For Accessing the Switch Securely

T1500/T1500G/T1600G/T1700G/T1700X
T2500/T2500G/T2600G/T2700G/T3700G

1910012326 REV1.0.0

January 2018

CONTENTS

1 Overview

In the enterprise network, the administrator has the demand to access and manage the switch. However, accessing the switch in traditional methods, such as via telnet or http, can cause security problems. The communication data faces the danger of various attacks, such as eavesdropping and tampering. To solve this problem, the administrator can access the switch via SSH or HTTPS. These protocols provide a secure mechanism which ensures data confidentiality and data integrity, and provides data origin authentication.

There are two methods to access the switch securely, that is via SSH and via HTTPS.

- SSH

  The SSH (Secure Shell) is a method for secure login from a terminal to a managed device. It protects communication security and integrity with strong authentication and encryption. It is a secure alternative to the non-protected login protocols, such as telnet. In an SSH login session, the PC acts as the SSH client, and the switch acts as the SSH server.

- HTTPS

  HTTPS (HTTP Secure) is an adaptation of HTTP (Hypertext Transfer Protocol) for secure communication. HTTPS creates a secure channel over an insecure network. If adequate cipher suites are used and the server's certificate is verified and trusted, the communication data can be protected from eavesdroppers and man-in-the-middle attacks. HTTPS is also referred to as HTTP over TLS, or HTTP over SSL, because in HTTPS, communication data is encrypted by TLS (Transport Layer Security) or SSL (Secure Sockets Layer). Nowadays, HTTPS is widely used on the internet for secure communication between websites and web browsers. In a local network, HTTPS can also be used for secure access to network devices, such as switches.

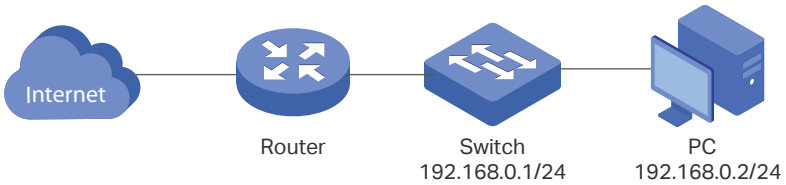
2 Accessing the Switch via SSH

SSH login supports the following two modes:

- Password Authentication Mode: In this mode, username and password are required for authentication. It is easier, but less secure to access the switch in password authentication mode.
- Key Authentication Mode: In this mode, a key pair including a public key and a private key is required. The server authenticates the client by matching up the public key of the server with the private key of the client. This mode is more secure than the password authentication mode. You can use either SSH-1 RSA or SSH-2 RSA/DSA to generate a key pair.

The following figure shows the typical network topology in this scenario.

Figure 2-1 Accessing the Switch Securely



Demonstrated with T2600G-28TS V3, the following sections provide configuration procedure in two modes: password authentication mode and key authentication mode.

2.1 Password Authentication Mode

In the password authentication mode, follow these steps to access the switch via SSH:

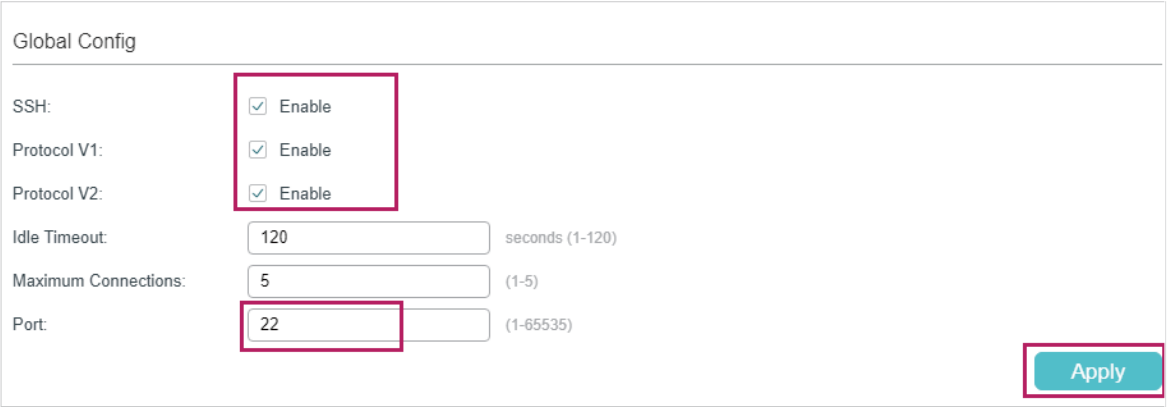
1) Configure the SSH server.
2) Configure the SSH client.

2.1.1 Configuring the SSH Server

Using the GUI

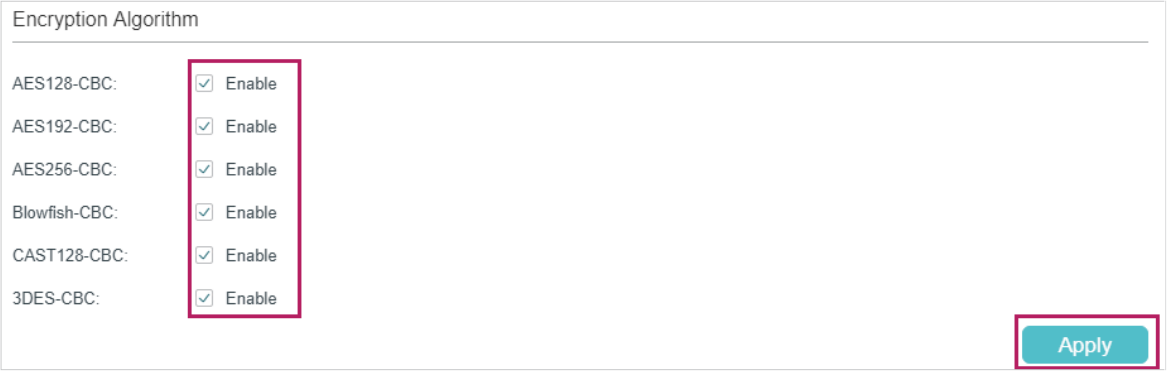
1) On the switch, choose the menu **SECURITY** > **Access Security** > **SSH Config** to load the following page. In the **Global Config** section, enable SSH, Protocol V1, and Protocol V2. In the **Port** field, enter the port of SSH server (**22** by default). Click **Apply**.

Figure 2-2 Configuring the SSH Server Globally



2) In the **Encryption Algorithm** section, enable all the encryption algorithms and click **Apply**.

Figure 2-3 Configuring the Encryption Algorithms



3) In the **Data Integrity Algorithm** section, enable all the data integrity algorithms and click **Apply**.

Figure 2-4 Configuring the Data Integrity Algorithms

Using the CLI

1) Enable the SSH server globally and configure the SSH version.

T2600G-28TS#configure

T2600G-28TS(config)#ip ssh server

T2600G-28TS(config)#ip ssh version v1

T2600G-28TS(config)#ip ssh version v2

2) Configure encryption algorithms.

T2600G-28TS(config)#ip ssh algorithm AES128-CBC

T2600G-28TS(config)#ip ssh algorithm AES192-CBC

T2600G-28TS(config)#ip ssh algorithm AES256-CBC

T2600G-28TS(config)#ip ssh algorithm Blowfish-CBC

T2600G-28TS(config)#ip ssh algorithm Cast128-CBC

T2600G-28TS(config)#ip ssh algorithm 3DES-CBC

3) Configure data integrity algorithms.

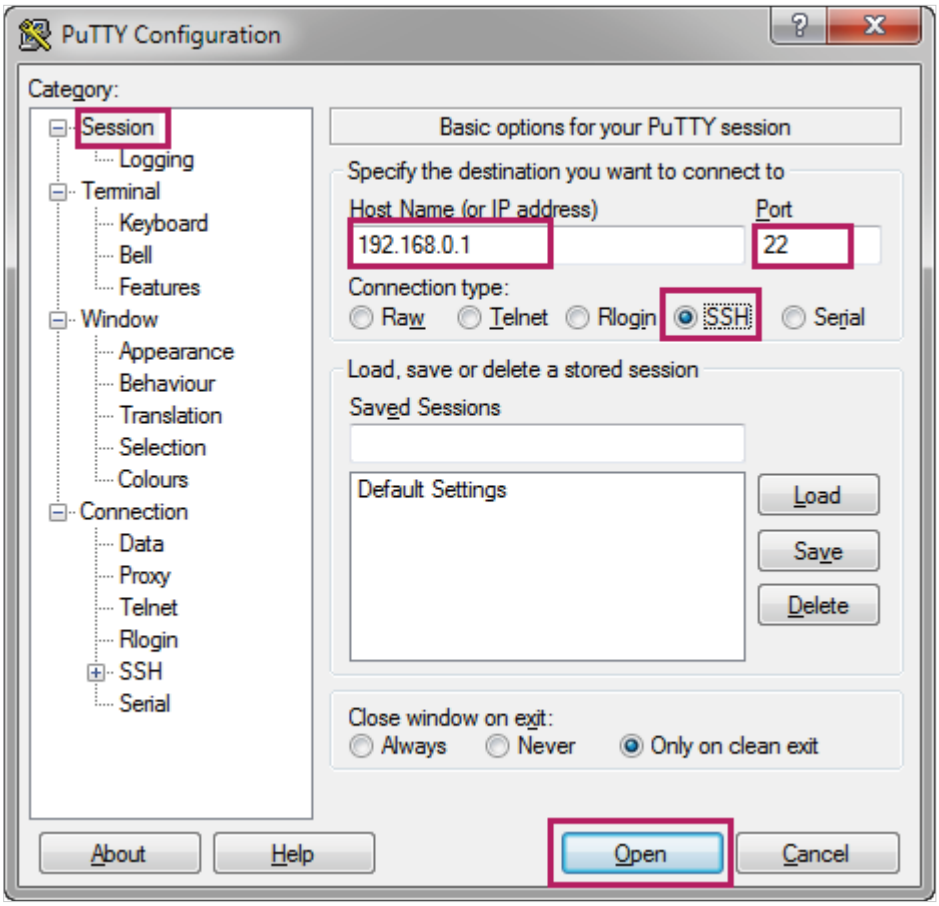
T2600G-28TS(config)#ip ssh algorithm HMAC-SHA1

T2600G-28TS(config)#ip ssh algorithm HMAC-MD5

2.1.2 Configuring the SSH Client

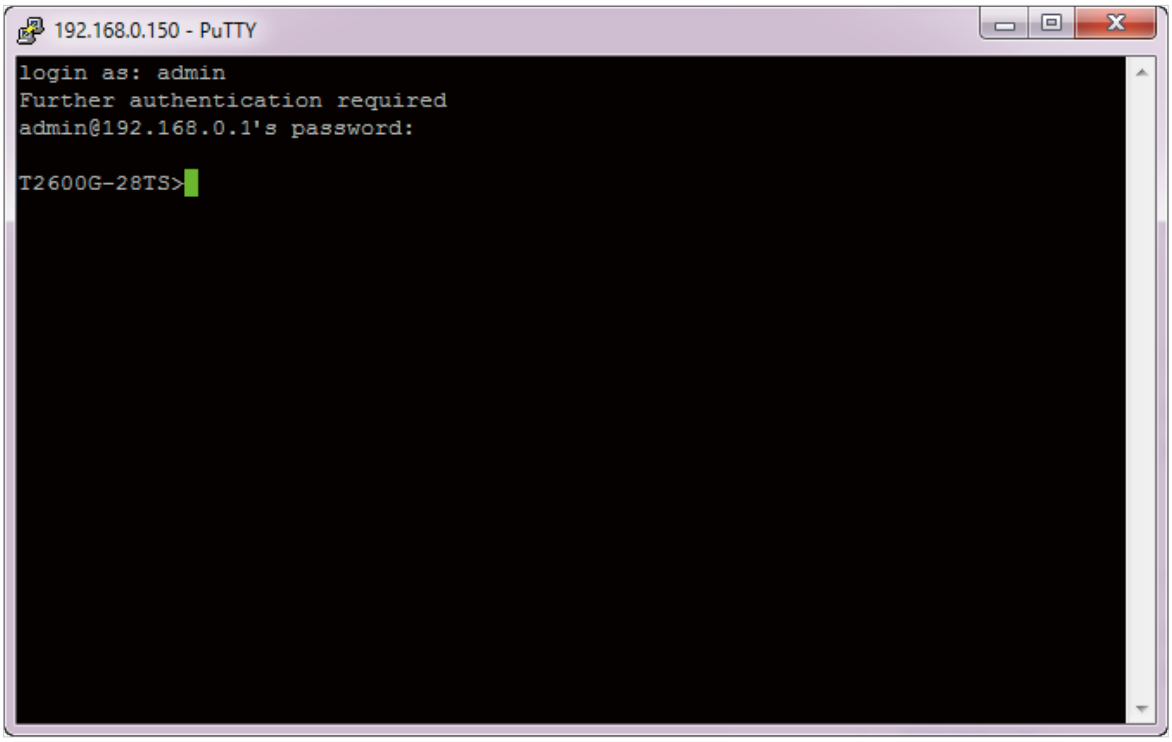
1) On the PC, go to the website *https://www.ssh.com/ssh/putty/download* to download **putty-0.70-installer.msi**, the SSH client software. Run the PuTTY setup wizard by double clicking **putty-0.70-installer.msi**. Follow the prompts to install the software on the PC. Double click **putty.exe** in the installation path to launch the software. Choose the menu **Session** to load the following page. Specify the connection type as **SSH**. In the **Host Name (or IP address)** field, enter the IP address of the switch (**192.168.0.1** by default). In the Port field, enter the port number you set on the SSH server in 2.1.1. Configuring the SSH Server (**22** by default).

Figure 2-5 Configuring Basic Options for Your PuTTY Session



2) Click **Open** to load the following page. If any PuTTY security alert pops up, click **Yes** to continue with the connection. Input the user account and password. Then you can manage the switch in the command line.

Figure 2-6 Logging in to the Switch



2.2 Key Authentication Mode

In the key authentication mode, you can use either SSH-1 RSA or SSH-2 RSA/DSA to generate a key pair, here we take SSH-2 RSA/DSA as an example. Follow these steps to access the switch via SSH:

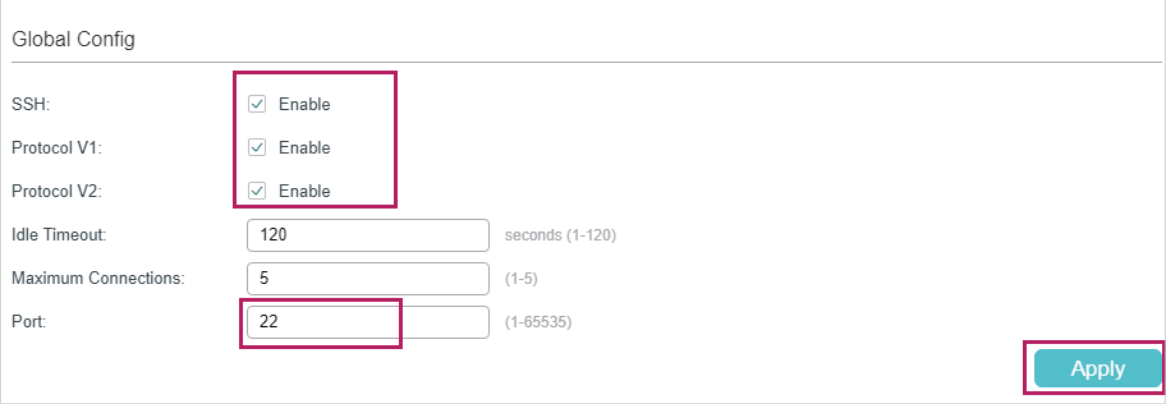
1) Configure the SSH server.
2) Generate the SSH key on the PC.
3) Download the public key onto the switch.
4) Configure the SSH client.

2.2.1 Configuring the SSH Server

Using the GUI

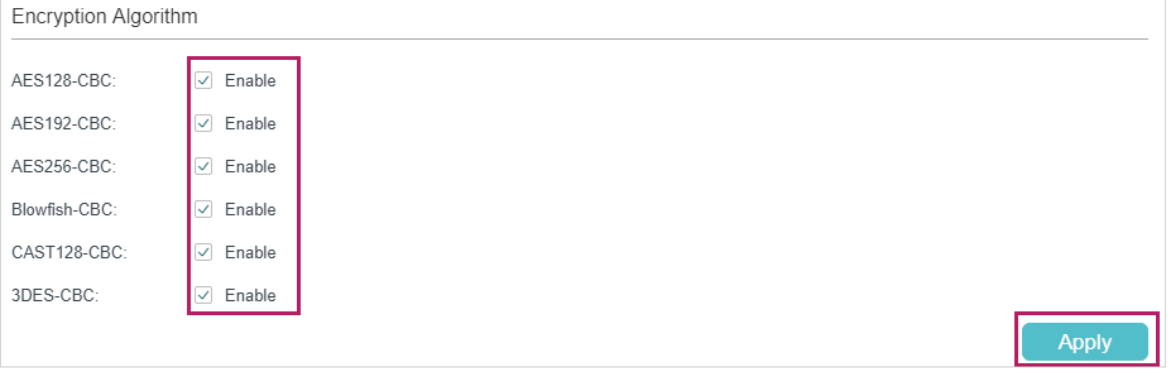
1) On the switch, choose the menu **SECURITY** > **Access Security** > **SSH Config** to load the following page. In the **Global Config** section, enable SSH, Protocol V1, and Protocol V2. In the **Port** field, enter the port of SSH server (**22** by default). Click **Apply**.

Figure 2-7 Configuring the SSH Server Globally



2) In the **Encryption Algorithm** section, enable all the encryption algorithms and click **Apply**.

Figure 2-8 Configuring the Encryption Algorithms



3) In the **Data Integrity Algorithm** section, enable all the data integrity algorithms and click **Apply**.

Figure 2-9 Configuring the Data Integrity Algorithms

Using the CLI

1) Enable the SSH server globally and configure the SSH version.

T2600G-28TS#configure

T2600G-28TS(config)#ip ssh server

T2600G-28TS(config)#ip ssh version v1

T2600G-28TS(config)#ip ssh version v2

2) Configure encryption algorithms.

T2600G-28TS(config)#ip ssh algorithm AES128-CBC

T2600G-28TS(config)#ip ssh algorithm AES192-CBC

T2600G-28TS(config)#ip ssh algorithm AES256-CBC

T2600G-28TS(config)#ip ssh algorithm Blowfish-CBC

T2600G-28TS(config)#ip ssh algorithm Cast128-CBC

T2600G-28TS(config)#ip ssh algorithm 3DES-CBC

3) Configure data integrity algorithms.

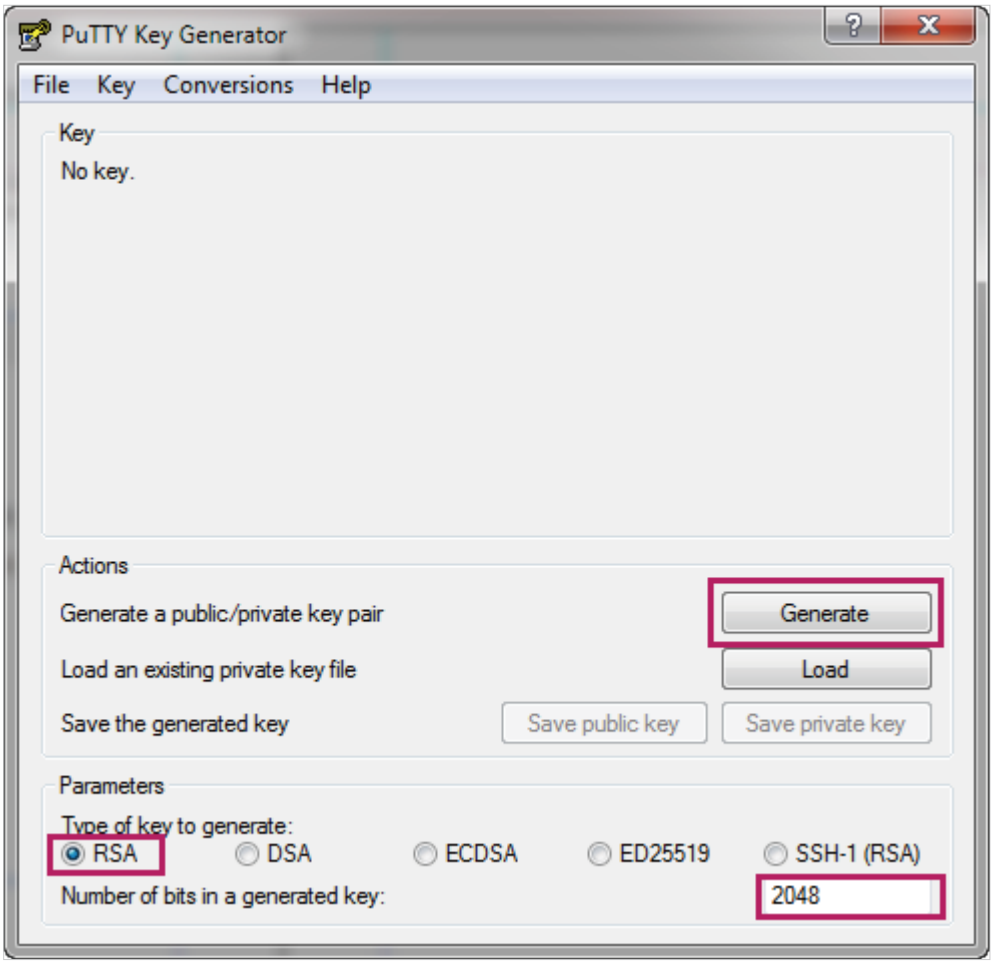
T2600G-28TS(config)#ip ssh algorithm HMAC-SHA1

T2600G-28TS(config)#ip ssh algorithm HMAC-MD5

2.2.2 Generating the SSH Key on the PC

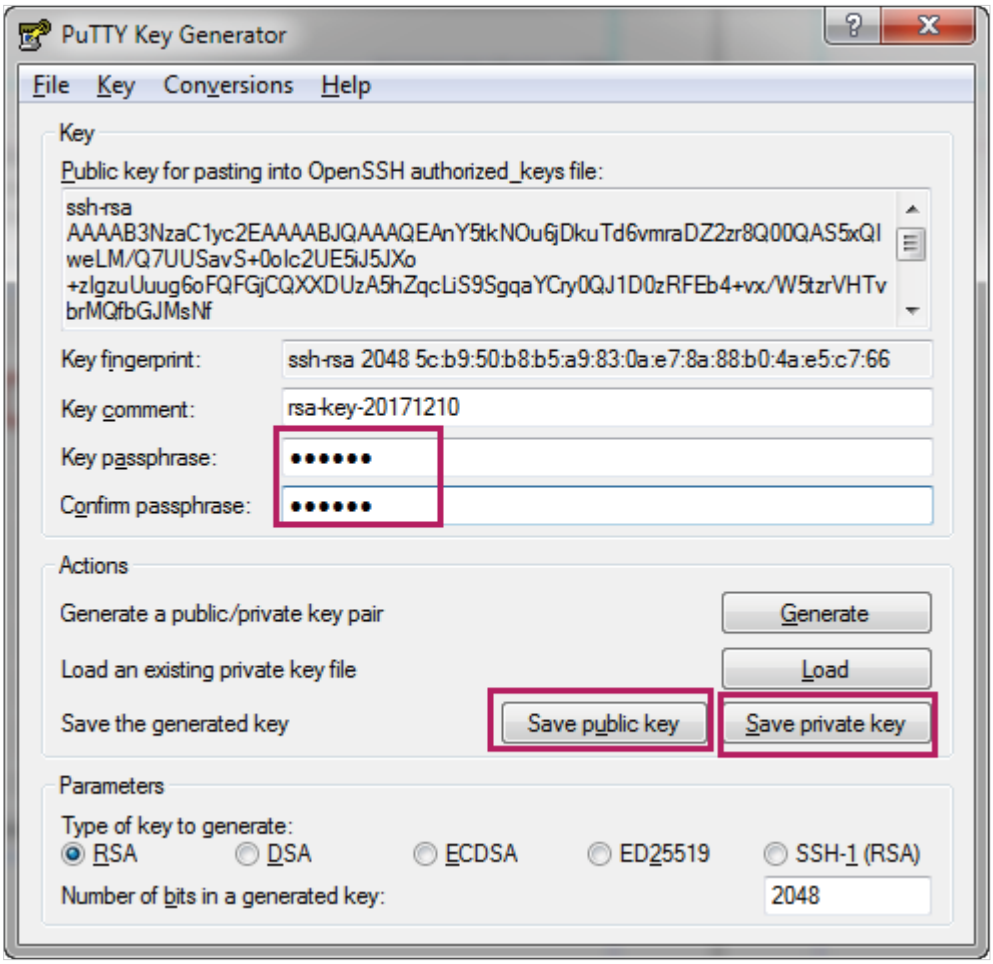
1) On the PC, go to the website *https://www.ssh.com/ssh/putty/download* to download **putty-0.70-installer.msi**, the SSH client software. Run the PuTTY setup wizard by double clicking **putty-0.70-installer.msi**. Follow the prompts to install the software on the PC. Double click **puttygen.exe** in the installation path to launch the software. Specify the type of key to generate as **RSA** or **DSA**. Specify the number of bits in a generated key according to your needs, here we specify the number as **2048**. Click **Generate** to generate a key pair.

Figure 2-10 Generating a Key Pair



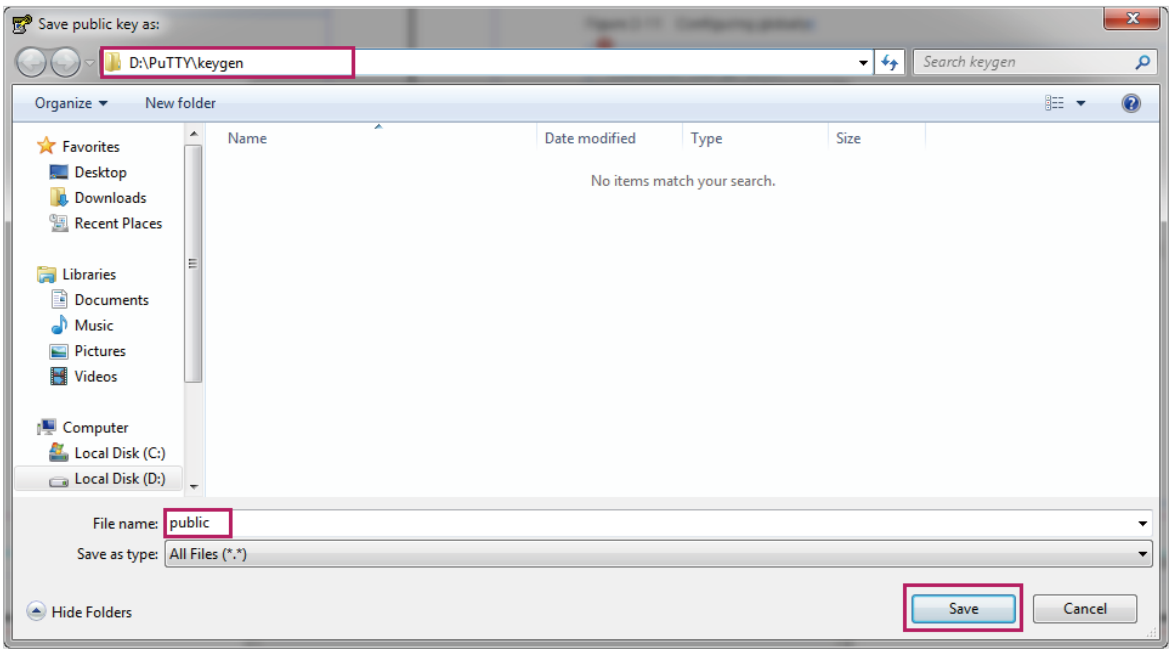
2) In the process of the key pair generation, move the mouse over the blank area quickly to generate some randomness. After the process, the following page is displayed. Enter a key passphrase and confirm the passphrase to protect the private key.

Figure 2-11 Configuring the Key Passphrase



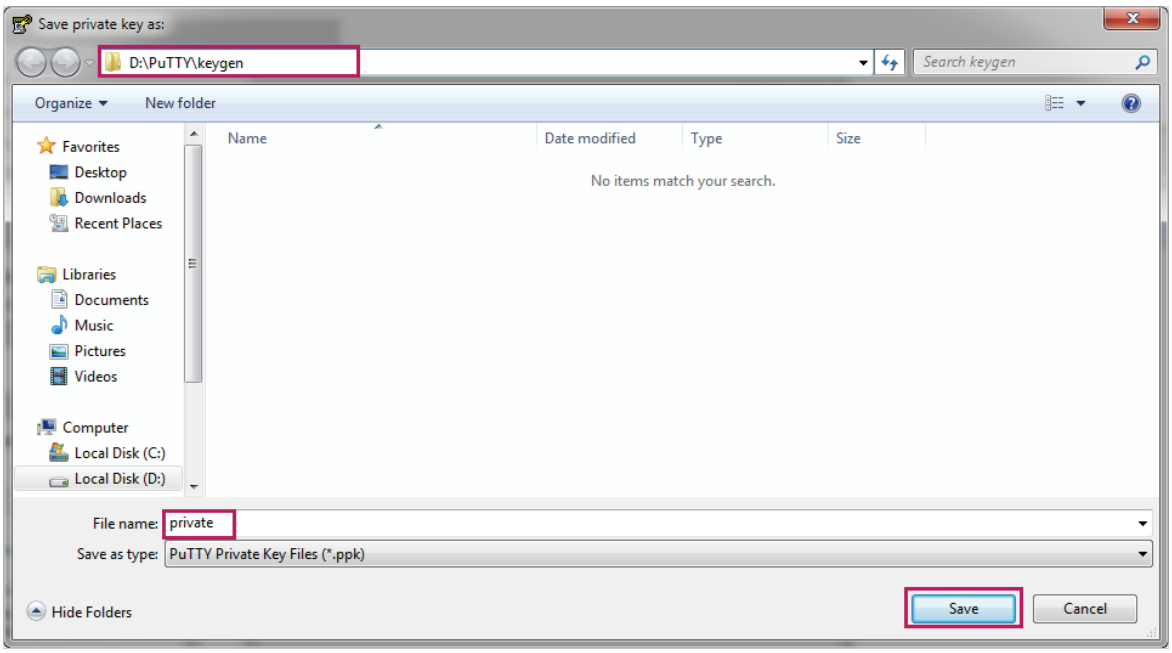
3) Click **Save public key** to load the following page. Specify a file path for the public key file. Enter a file name for the public key file. Click **Save**.

Figure 2-12 Saving the Public Key



4) Click **Save private key** to load the following page. Specify a file path for the private key file. Enter a file name for the private key file, Click **Save**.

Figure 2-13 Saving the Private Key

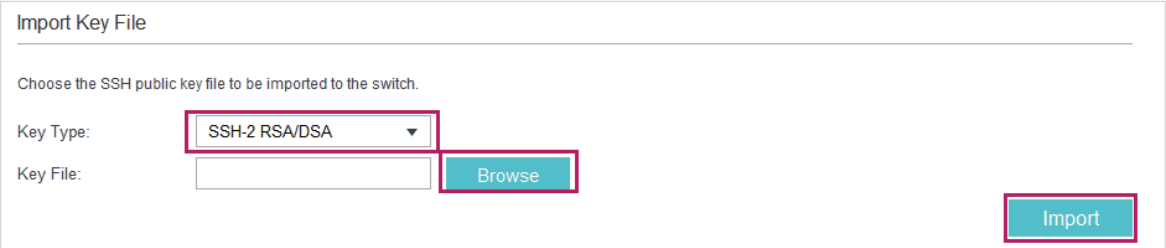


2.2.3 Downloading the Public Key onto the Switch

Using the GUI

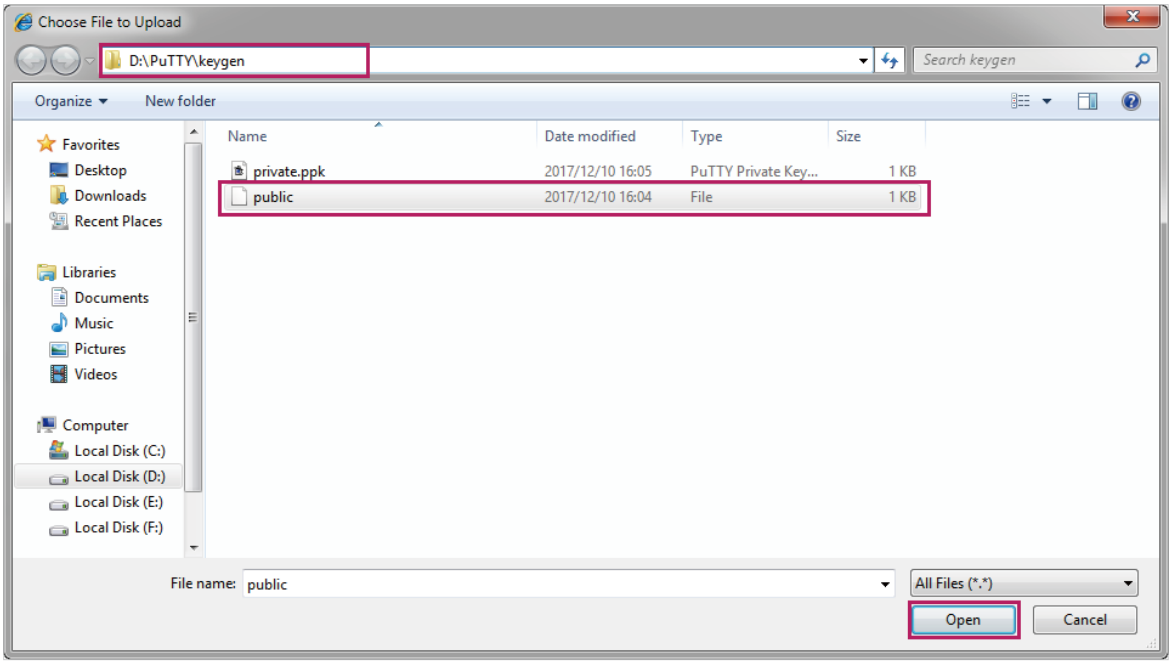
1) On the switch, choose the menu **SECURITY** > **Access Security** > **SSH Config** to load the following page. In the **Import Key File** section, select the key type as **SSH-2 RSA/DSA**.

Figure 2-14 Specifying the Key Type



2) Click **Browse** to load the following page. Enter the public key file path in the address bar. Select the public key file we previously saved. Click **Open**. Click **Import** to download the public key onto the switch.

Figure 2-15 Downloading the Public Key onto the Switch

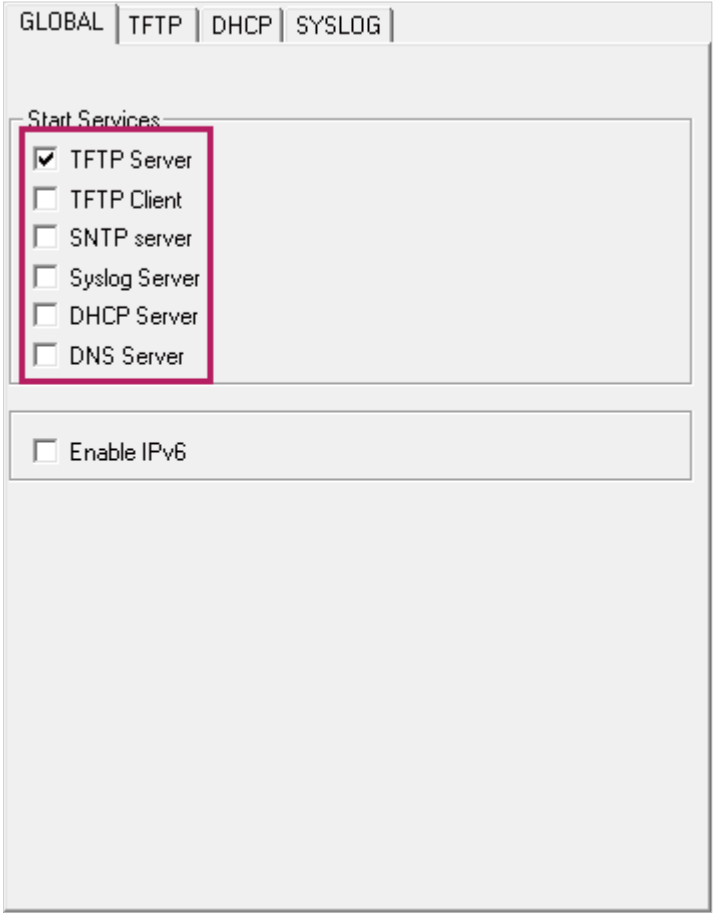


Using the CLI

1) As the switch downloads the public key file from a TFTP server, we can launch a 3rd-party TFTP server software on the PC, such as tftpd32. Go to the following website *http://tftpd32.jounin.net/tftpd32_download.html* to download tftpd32 standard edition (zip), uncompress the package and launch the software by double clicking tftpd32.exe.

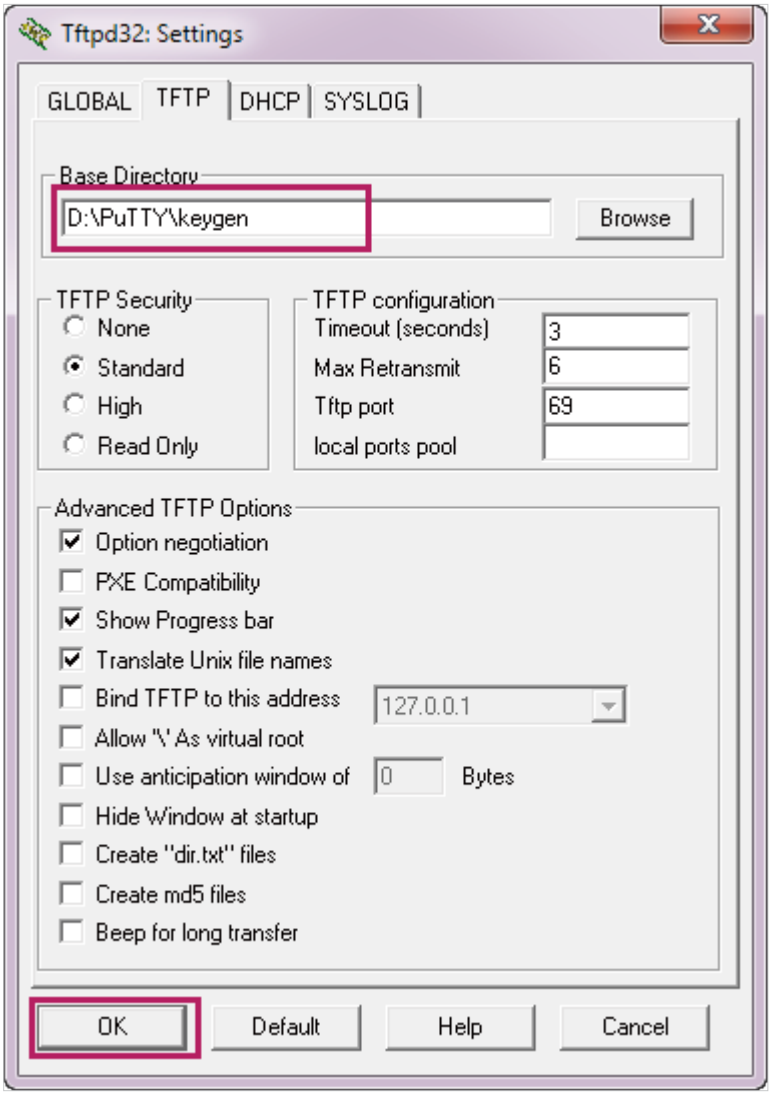
2) Click **Settings** and choose the menu **GLOBAL** to load the following page. Enable the TFTP server and disable the other functions.

Figure 2-16 Configuring the TFTP Server Gloabally



3) Choose the menu **TFTP** to load the following page. Specify the base directory as the key file path where the public key is saved. Click **OK**.

Figure 2-17 Configuring the Path for the TFTP Server

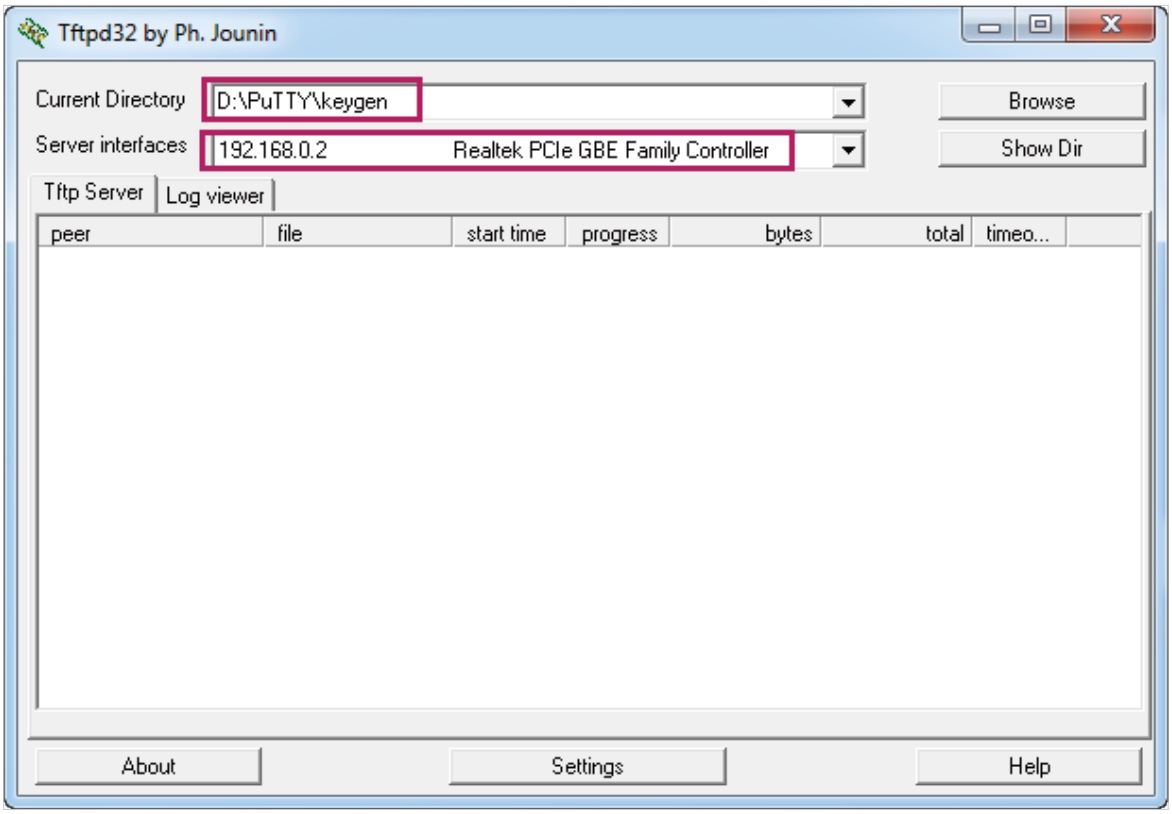


Note:

The base directory path should not include any blanks. Otherwise, the TFTP server cannot find the file.

4) Restart the TFTP software to apply the new settings, and load the following page. Specify the current directory as the key file path where the public key is saved. Select the server interface as **192.168.0.2** from the drop-down list, which is the IP address of the PC.

Figure 2-18 Configuring the Interface for the TFTP Server



5) On the switch, download the public key file via the TFTP protocol.

T2600G-28TS#configure

T2600G-28TS(config)#ip ssh download v2 public ip-address 192.168.0.2

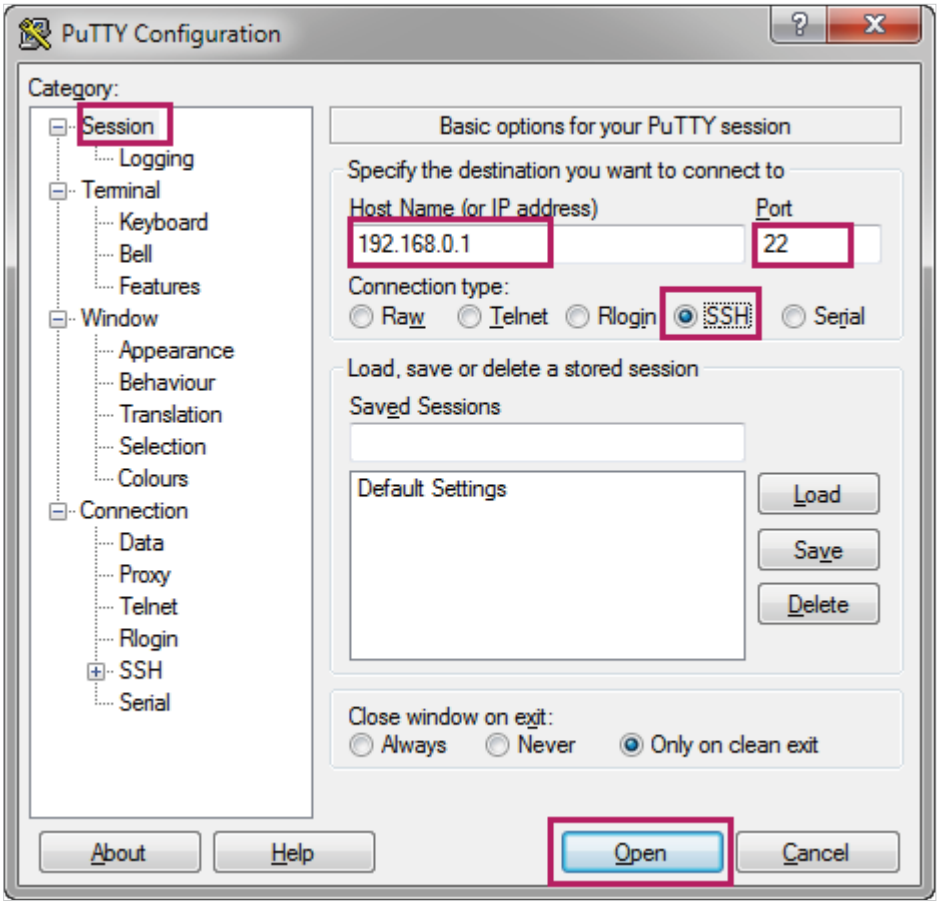
Start to download SSH key file.....

Download SSH key file OK.

2.2.4 Configuring the SSH Client

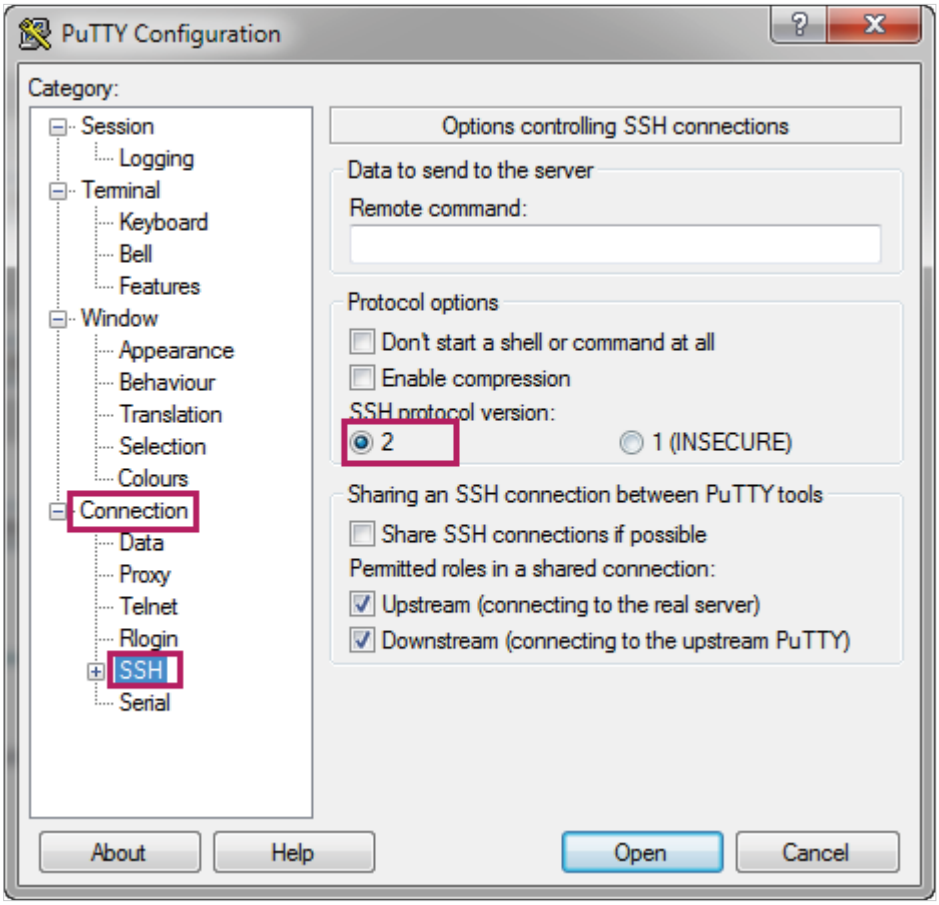
1) On the PC, double click **putty.exe** in the installation path to launch the software. Choose the menu **Session** to load the following page. Specify the connection type as **SSH**. In the **Host Name (or IP address)** field, enter the IP address of the switch (**192.168.0.1** by default). In the Port field, enter the port number you set on the SSH server in 2.2.1. Configuring the SSH Server (**22** by default).

Figure 2-19 Configuring the SSH Session



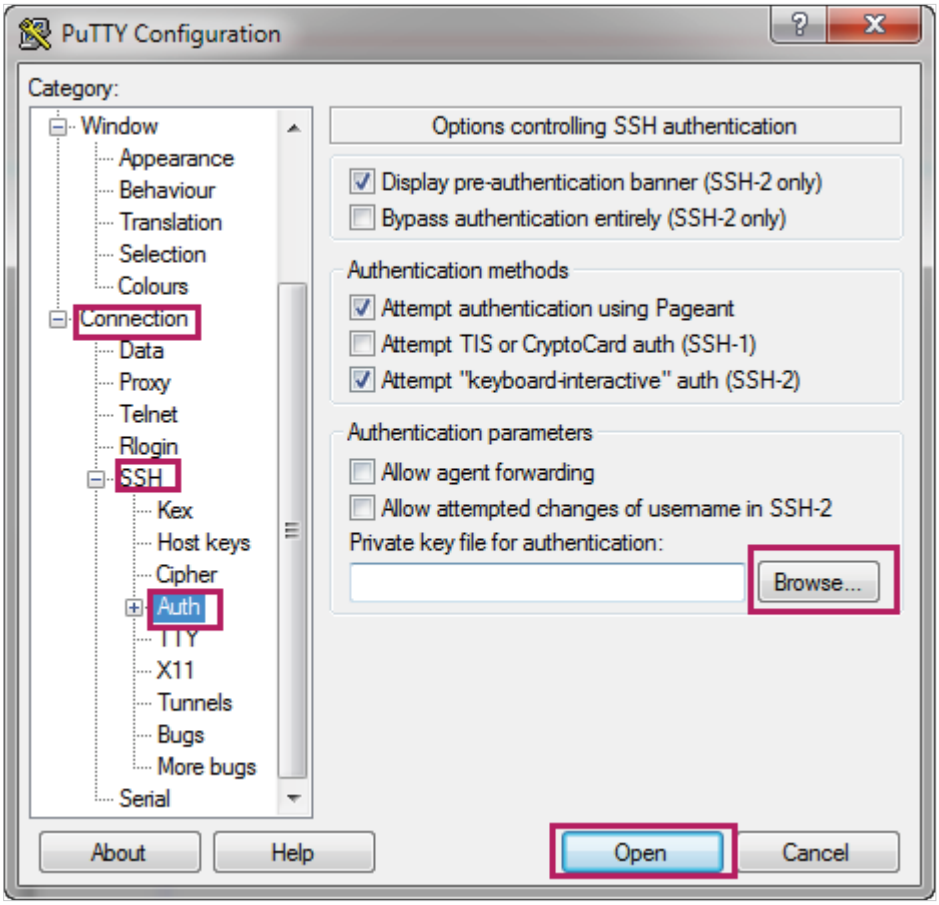
2) Choose the menu **Connection > SSH** to load the following page. Specify the SSH protocol version as **2**.

Figure 2-20 Configuring the SSH Protocol Version



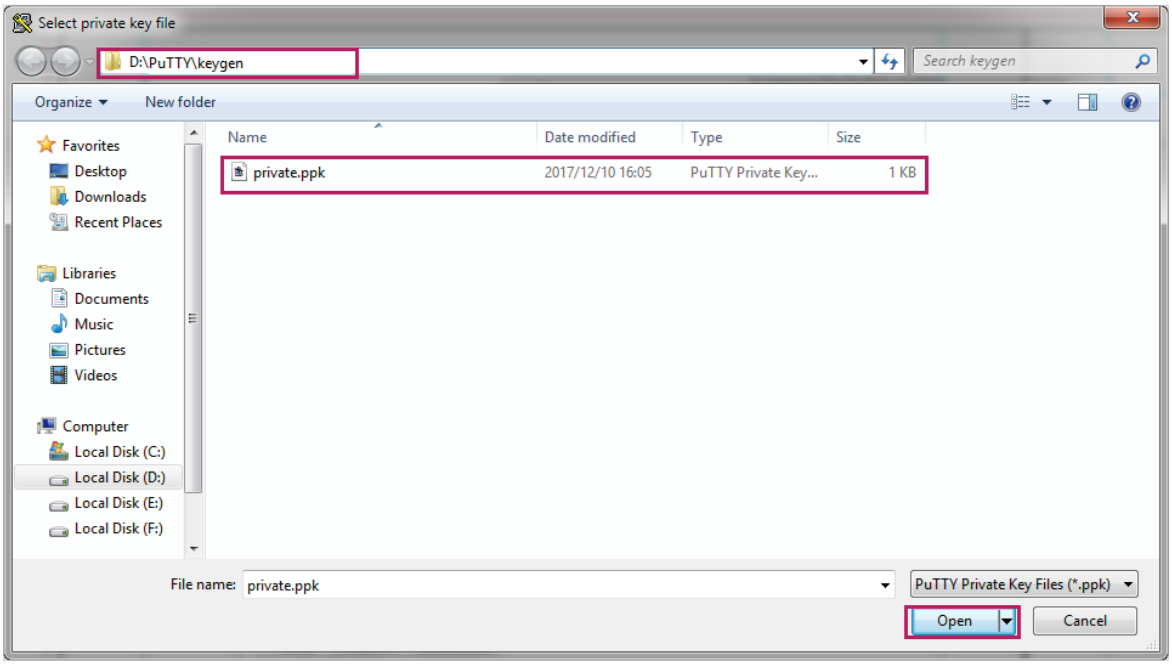
3) Choose the menu **Connection > SSH > Auth** to load the following page.

Figure 2-21 Configuring the SSH Authentication



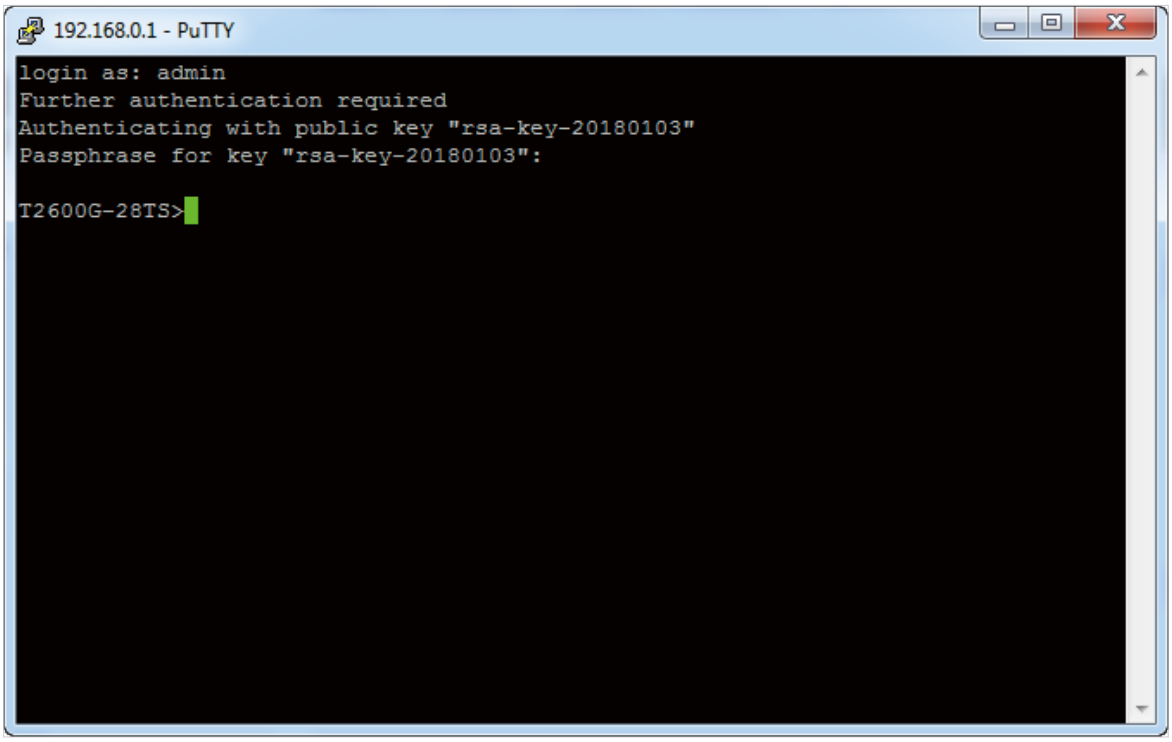
4) Click **Browse** to load the following page. Enter the private key file path in the address bar. Select the private key file we previously saved. Click **Open.**

Figure 2-22 Configuring the Private Key



5) Click **Open** to load the following page. If any PuTTY security alert pops up, click **Yes** to continue with the connection. Input the username, which is **admin** by default. Input the key passphrase configured in key pair generation process. Then you can manage the switch by using the CLI.

Figure 2-23 Logging in to the Switch



3 Accessing the Switch via HTTPS

On the internet, HTTPS is widely used for communication between a website and a web browser to enhance access security. When you browse a website using HTTPS, the web browser acts as the HTTPS client and the website acts as the HTTPS server. The communication process is as follows:

1) The server sends its certificate to the client. The certificate is typically awarded to the server by an official CA (Certificate Authentication).
2) The client identifies the server on the condition that the client trusts the CA and certificates signed by the CA.
3) The client uses the public key contained in the certificate to encrypt data sent to the server.
4) The server decrypts the cipher text using the corresponding private key.

In the local network, you can also use HTTPS to access and manage the switch securely. This communication process is similar to that between a website and a web browser. The difference is that your PC acts as the HTTPS client and the switch acts as the HTTPS server. Besides, you can use the built-in certificate of the switch or a self-signed certificate free of charge instead of an authoritatively signed certificate.

You can access the switch securely via the following two methods:

- Using the built-in certificate of the switch

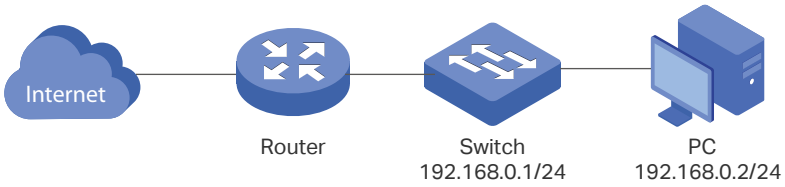
  You can access the switch via HTTPS without generating any certificate by using the built-in certificate of the switch. This method is much more convenient, however, it only takes effect in the premise that you trust the built-in certificate of the switch.

- Using a self-singed certificate

  You can run your own CA, generate a self-signed certificate and download the certificate onto the switch. Then you can access the switch securely using the self-signed certificate.

The following figure shows the typical network topology in this scenario.

Figure 3-1 Accessing the Switch Securely



Demonstrated with T2600G-28TS V3, the following sections provide configuration procedure in two ways: using the built-in certificate of the switch and using a self-signed certificate.

3.1 Using the Built-In Certificate of the Switch

To access the switch using the built-in certificate, follow these steps:

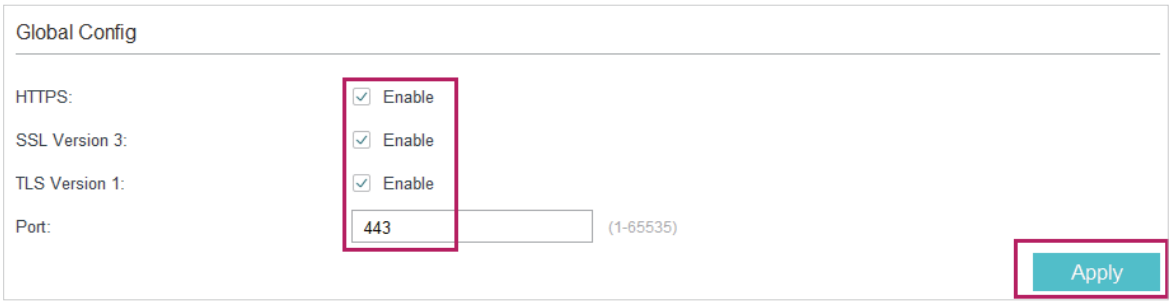
1) Configure the HTTPS server.
2) Access the switch using the built-in certificate.

3.1.1 Configuring the HTTPS Server

Using the GUI

1) On the switch, choose the menu **SECURITY** > **Access Security** > **HTTPS Config** to load the following page. In the **Global Config** section, enable HTTPS, SSL Version 3, and TLS Version 1.In the **Port** field, enter the port of HTTPS server (**443** by default). Click **Apply**.

Figure 3-2 Configuring the HTTPS Server Globally



2) In the **CipherSuite Config** section, enable all the suites. Click **Apply**.

Figure 3-3 Configuring the Cipher Suites for the HTTPS Server

Using the CLI

1) Enable the HTTPS server globally and configure the HTTPS version.

```
T2600G-28TS#configure
T2600G-28TS(config)#ip http secure-server
T2600G-28TS(config)#ip http secure-protocol ssl3 tls1
```

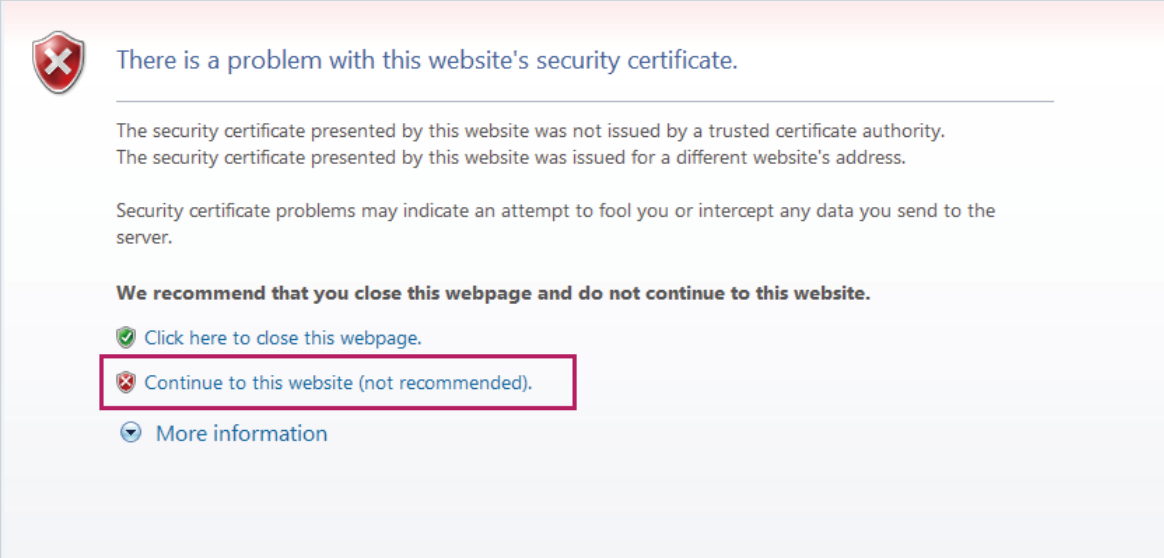
2) Configure the HTTPS cipher suites.

```
T2600G-28TS(config)#ip http secure-ciphersuite 3des-ede-cbc-sha rc4-128-md5 rc4-128-sha des-cbc-sha
```

3.1.2 Accessing the Switch Using the Built-In Certificate

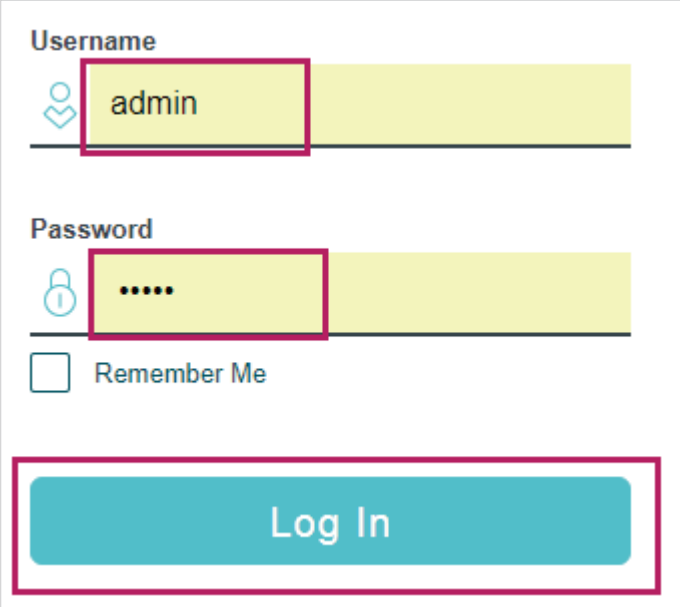
1) Launch the web browser on the PC. Here we take Internet Explorer for example. Enter **https://192.168.0.1** in the address bar of the browser, and press the **Enter** key. **https** indicates the access to the switch via HTTPS. **192.168.0.1** is the IP address of the switch. The following warning information will be displayed.

Figure 3-4 Accessing the Switch



2) Click **Continue to this website (not recommended)**. The following web page will be displayed. Enter the username and the password, and click **Log In** to access and manage the switch securely.

Figure 3-5 Logging in to the Switch



3.2 Using a Self-Signed Certificate

To use the self-signed certificate to access the switch, follow these steps:

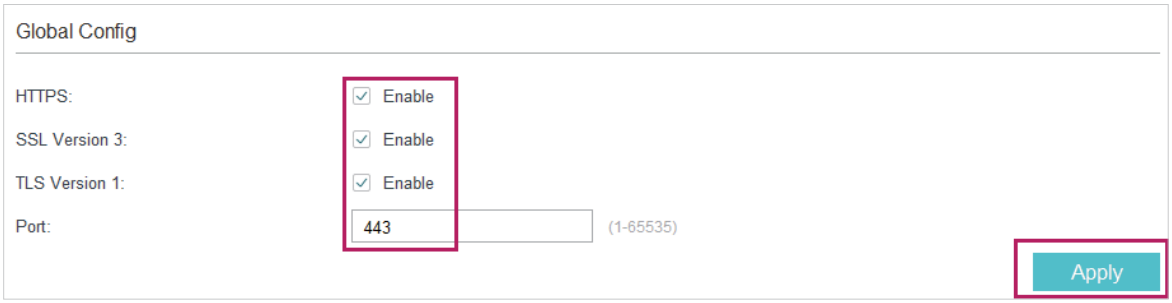
1) Configure the HTTPS server.
2) Generate the certificate and private key on the PC.
3) Download the certificate and private key onto the switch.
4) Access the switch using the self-signed certificate.

3.2.1 Configuring the HTTPS Server

Using the GUI

1) On the switch, choose the menu **SECURITY** > **Access Security** > **HTTPS Config** to load the following page. In the **Global Config** section, enable HTTPS, SSL Version 3 , and TLS Version 1. In the **Port** field, enter the port of HTTPS server (**443** by default). Click **Apply**.

Figure 3-6 Configuring the HTTPS Server Globally



2) In the **CipherSuite Config** section, enable all the suites. Click **Apply**.

Figure 3-7 Configuring the Cipher Suites for the HTTPS Server

Using the CLI

1) Enable the HTTPS server globally and configure the HTTPS version.

```
T2600G-28TS#configure
T2600G-28TS(config)#ip http secure-server
T2600G-28TS(config)#ip http secure-protocol ssl3 tls1
```

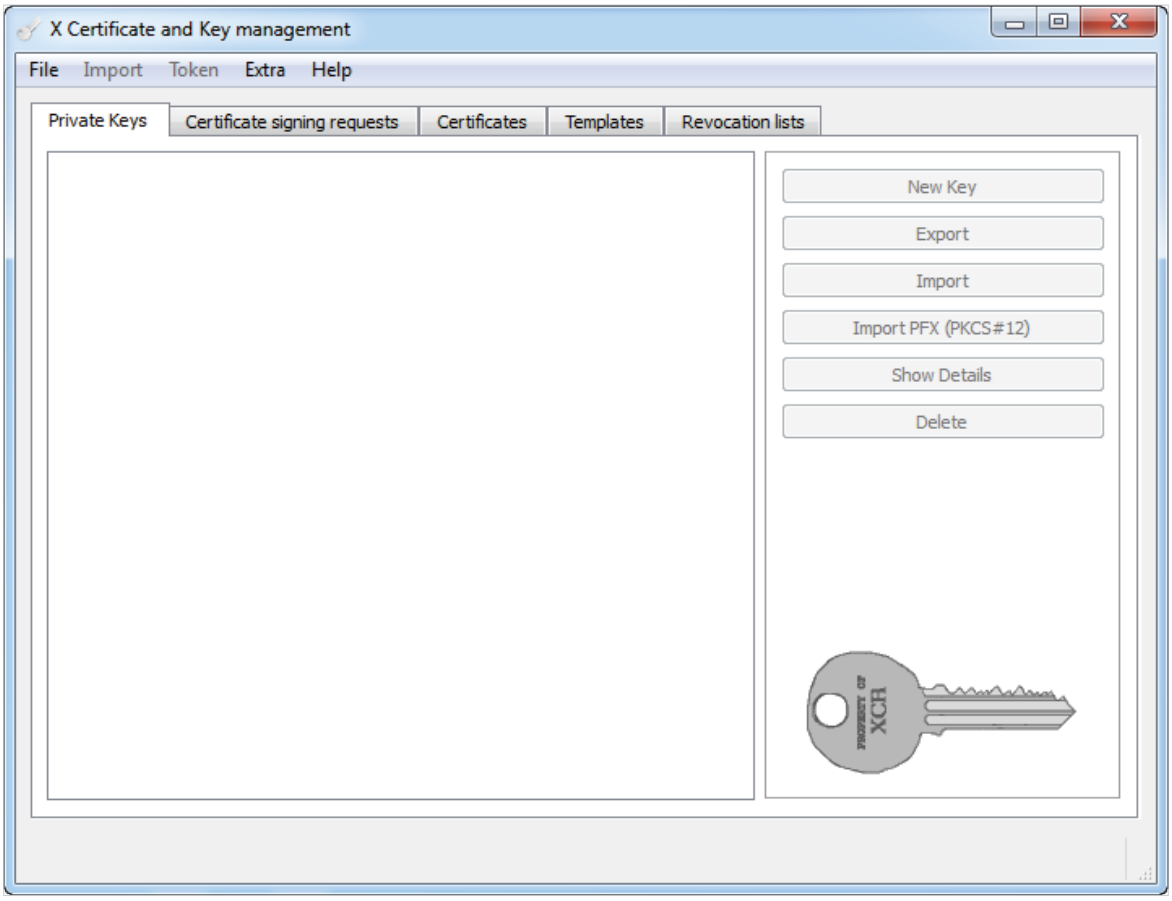
2) Configure the HTTPS cipher suites.

T2600G-28TS(config)#ip http secure-ciphersuite 3des-ede-cbc-sha rc4-128-md5 rc4-128-sha des-cbc-sha

3.2.2 Generating the Certificate and Private Key on the PC

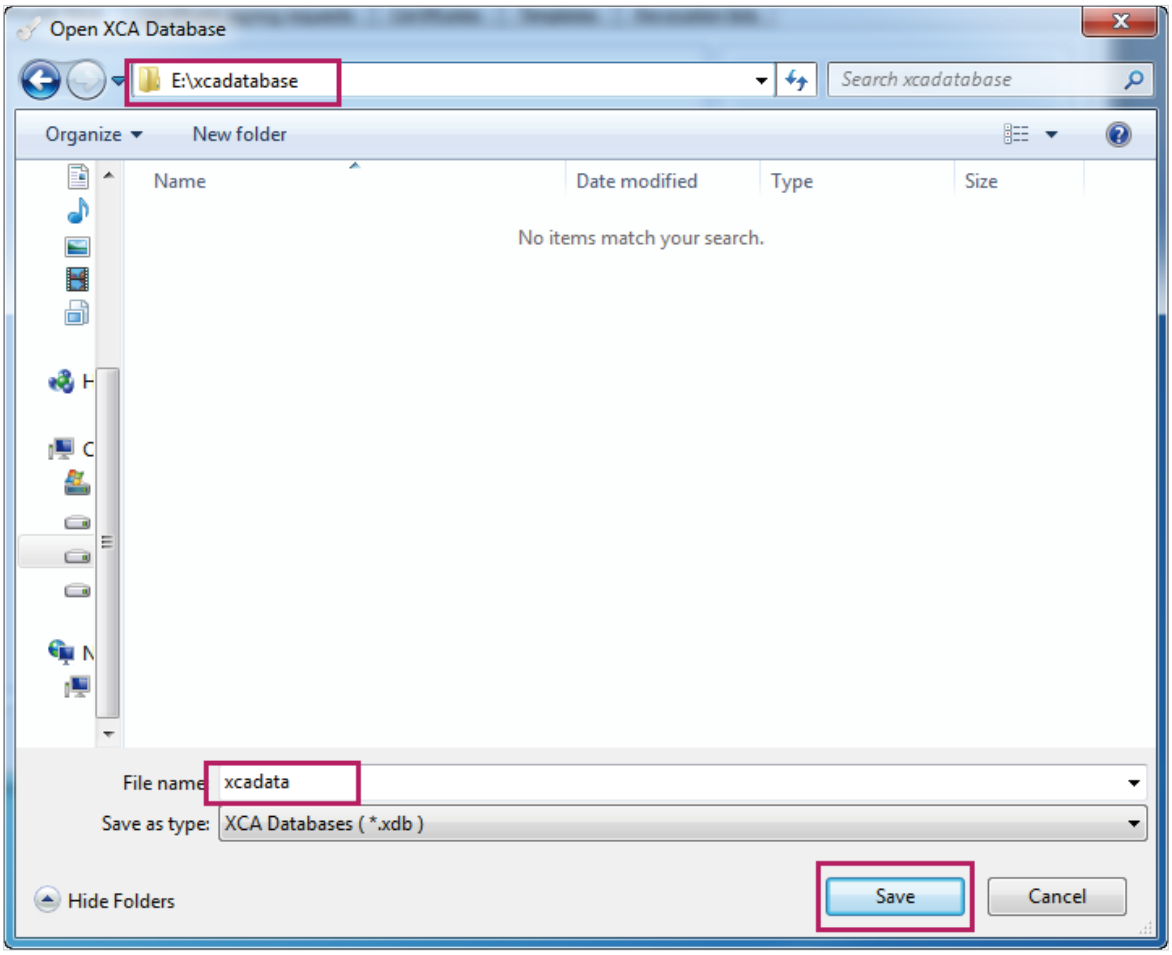
1) On the PC, go to the website *https://sourceforge.net/projects/xca* to download the xca software, which is used to generate the certificate and the private key. Follow the prompts to install the software and launch the software on the PC. The following page will be displayed.

Figure 3-8 Launching the XCA Software



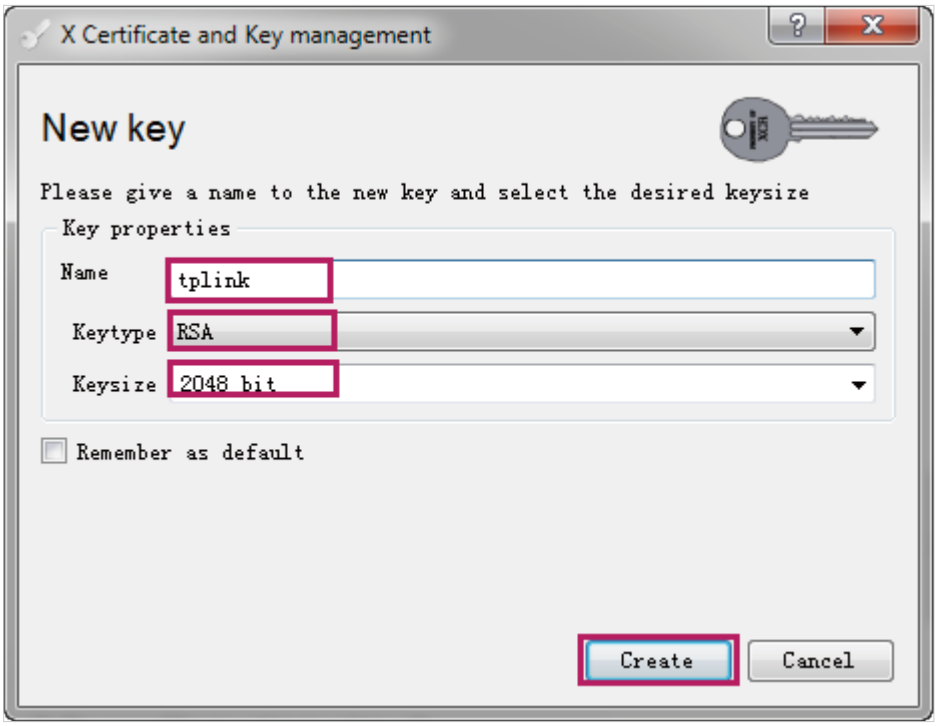
2) Choose the menu **File** > **New DataBase** to load the following page. Specify a file path for the database file. Enter a file name for the XCA database, here we specify the file name as xcadata. Select the file type as **XCA Databases**. Click **Save**.

Figure 3-9 Creating a NewDdatabase



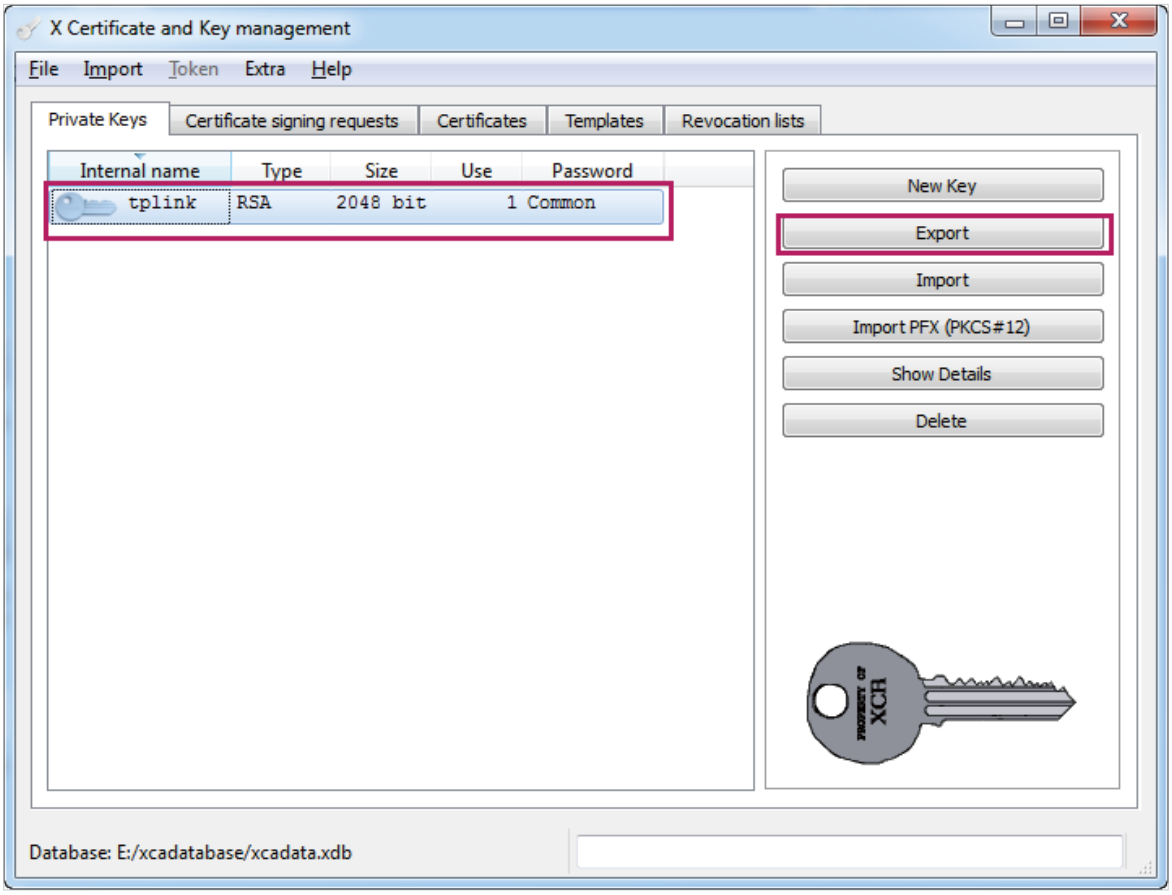
3) Choose the menu **Private Keys > New Key** to load the following page. Enter a name for the key, here we specify the file name as **tplink**. Select the key type as **RSA**. Select the key size as **2048 bit**. Click **Create**.

Figure 3-10 Creating a New Private Key



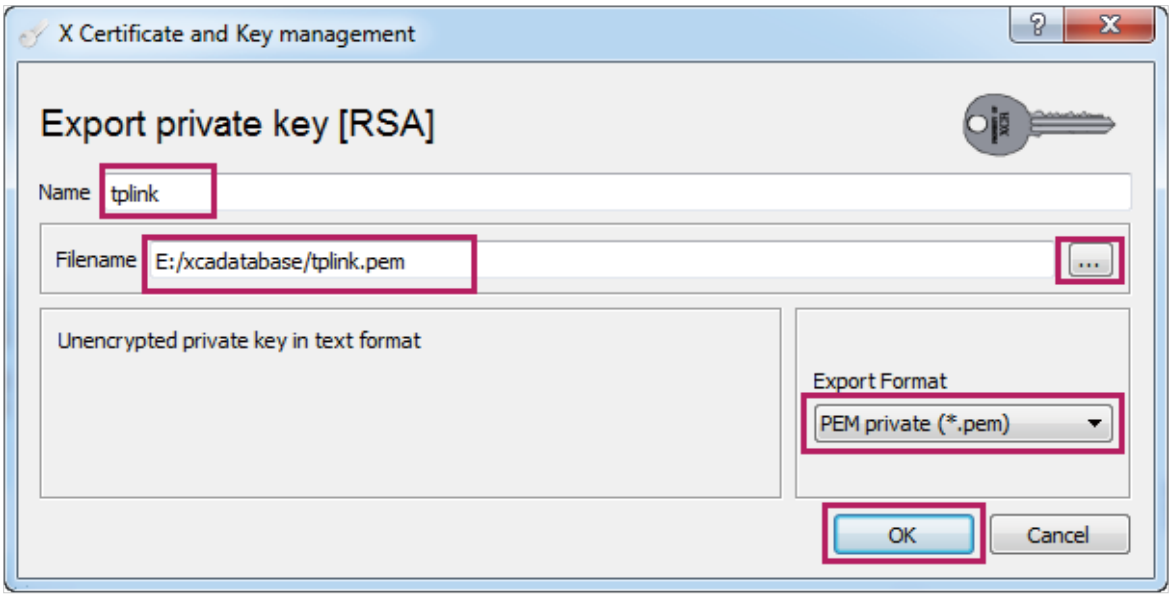
4) Choose the menu **Private Keys** to load the following page. Select the private key we generated previously.

Figure 3-11 Exporting the Private Key



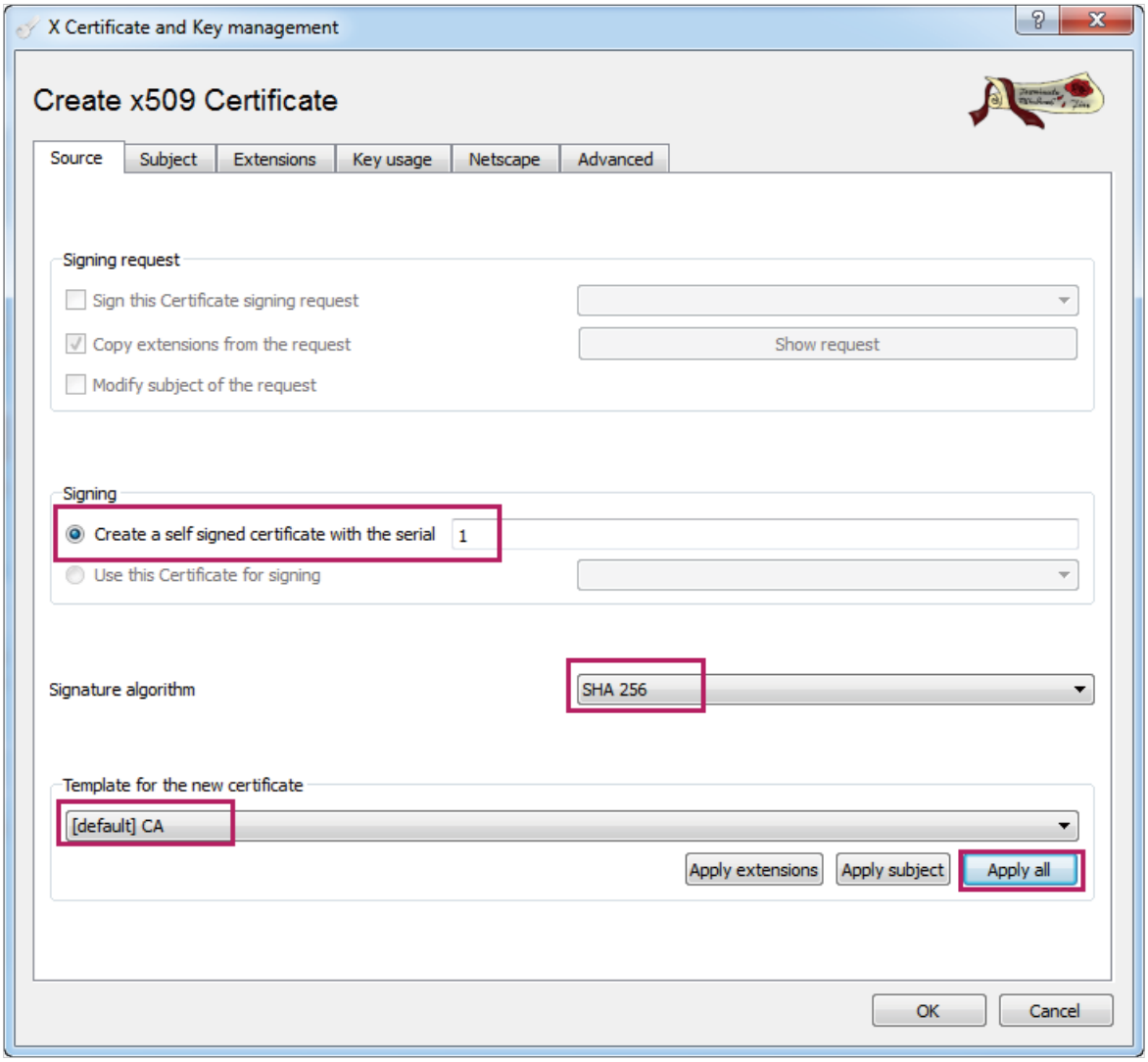
5) Click **Export** to load the following page. Click ... and specify a file path and a file name for the private key file. Select the export format as **PEM private (*.pem)** . Click **OK**.

Figure 3-12 Saving the Private Key



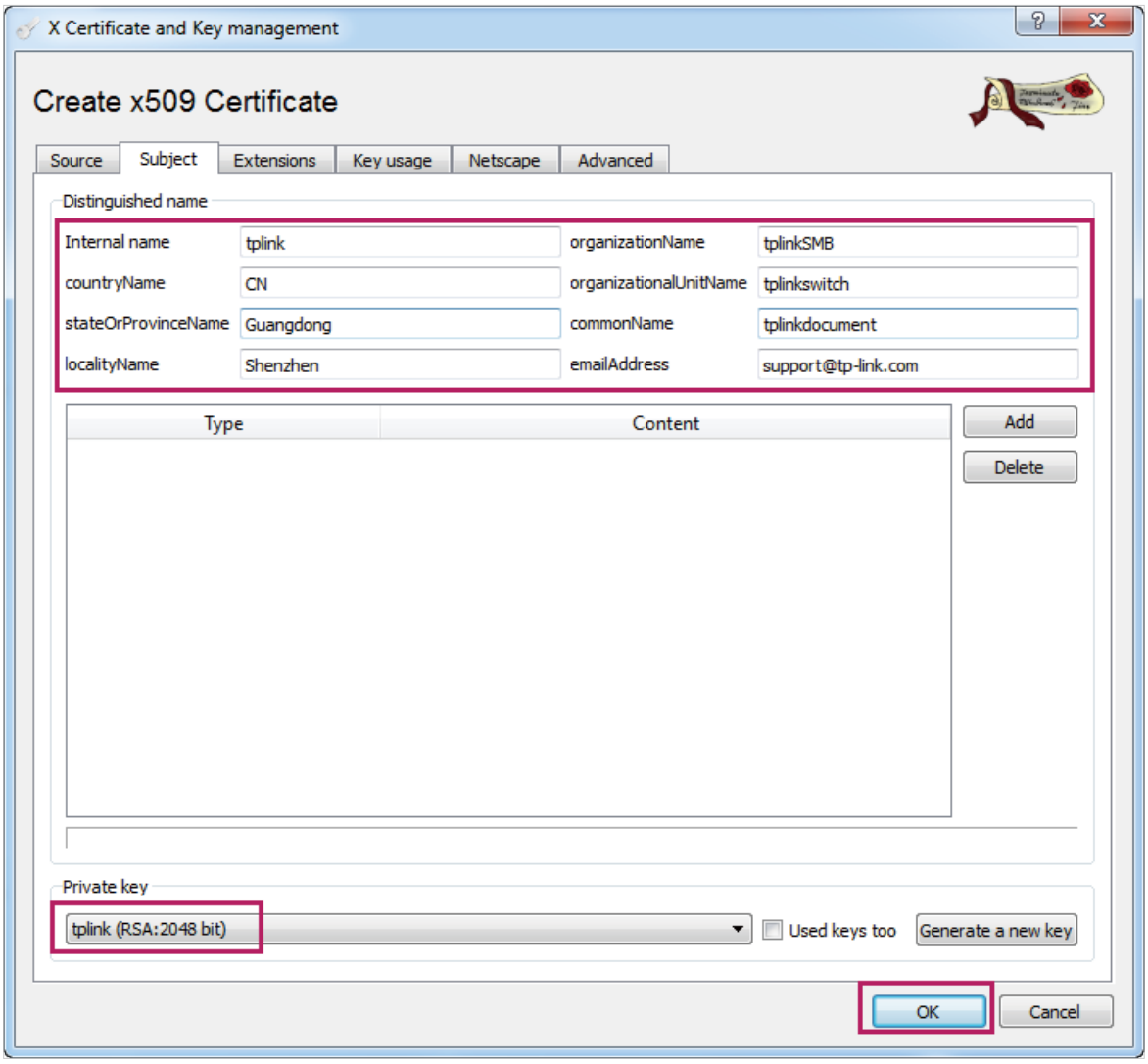
6) Choose the menu **Certificate > New Certificate** to load the following page. Choose the menu **Source**. Select **Create a self signed certificate with the serial** and specify the serial number as **1**. Select the signature algorithm according to your needs, here we select the signature algorithm as **SHA 256**. Select the template for the new certificate as **[default] CA**. Click **Apply all**.

Figure 3-13 Creating a New Certificate



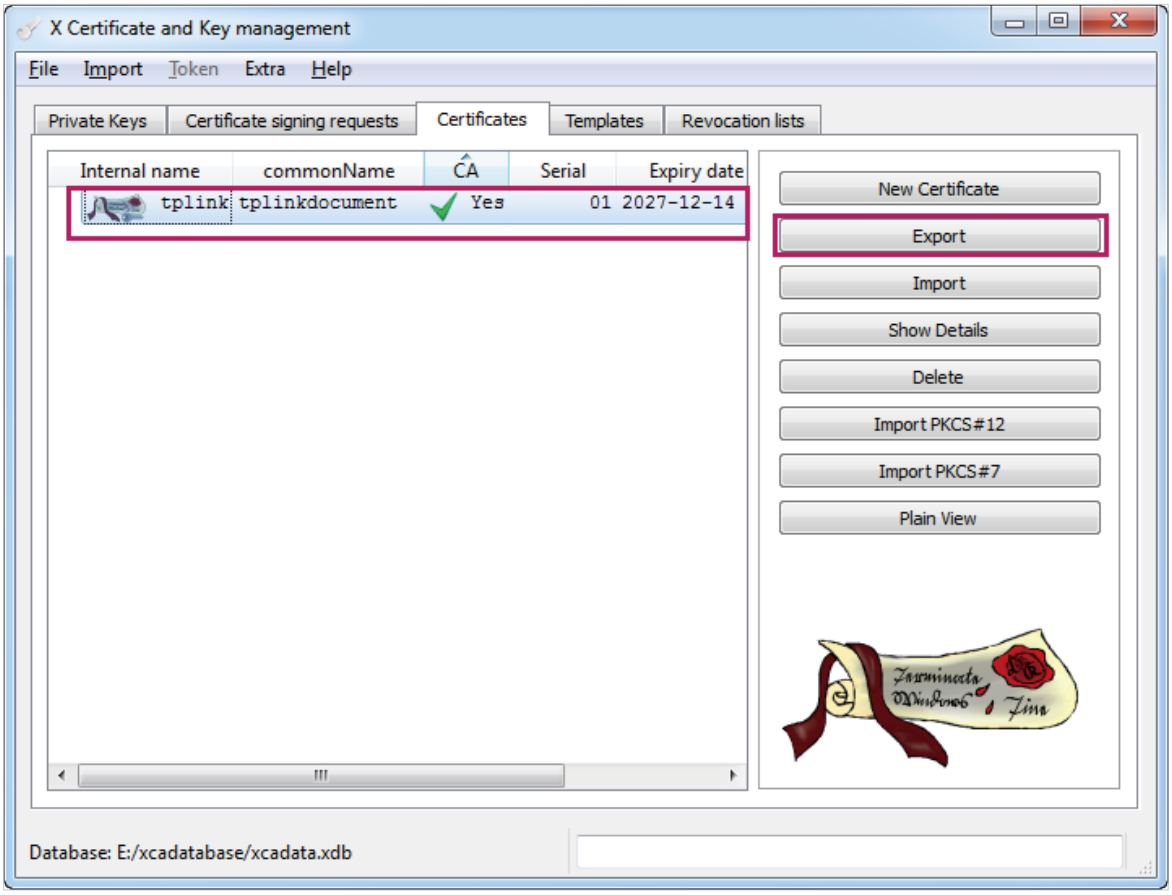
7) Choose the menu **Subject** to load the following page. Specify the distinguished name entries, such as the internal name, according to your needs. These entries will be contained in the certificate to be generated. Select the private key as **tplink (RSA:2048 bit)**. This is the private key we generated previously. Click **OK**.

Figure 3-14 Specifying the Distinguished Name Entries



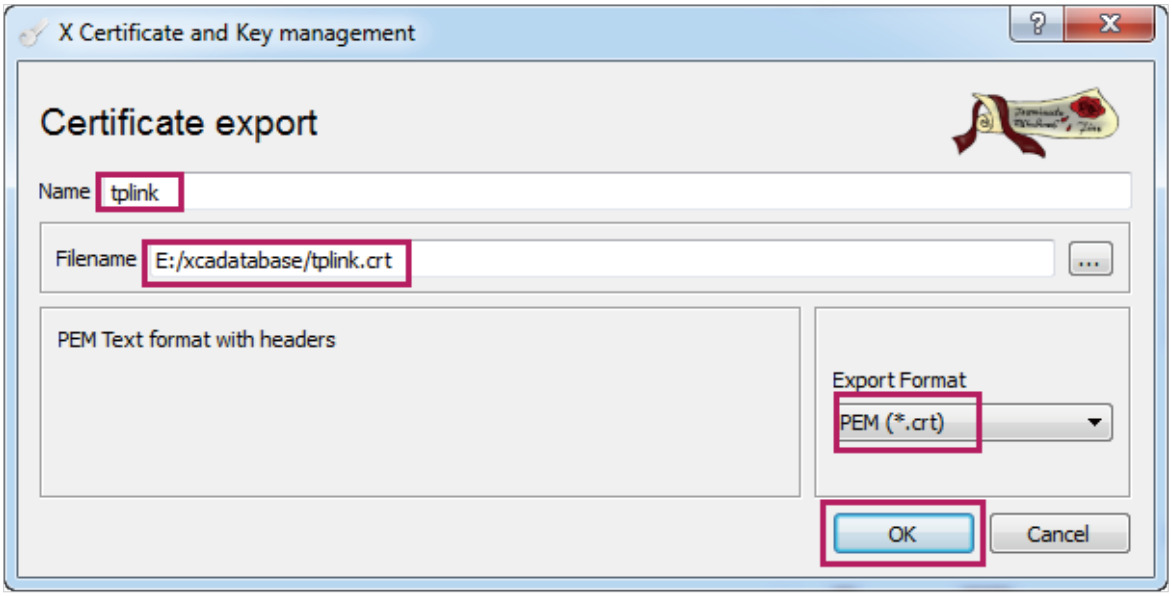
8) Choose the menu **Certificates** to load the following page. Select the certificate we have just generated.

Figure 3-15 Exporting the Certificate



9) Click **Export** to load the following page. Click ... and specify the file path and the file name for the certificate file. Here, the file path is set the same with the key file. Select the export format as **PEM (*.crt)**. Click **OK**.

Figure 3-16 Saving the Certificate

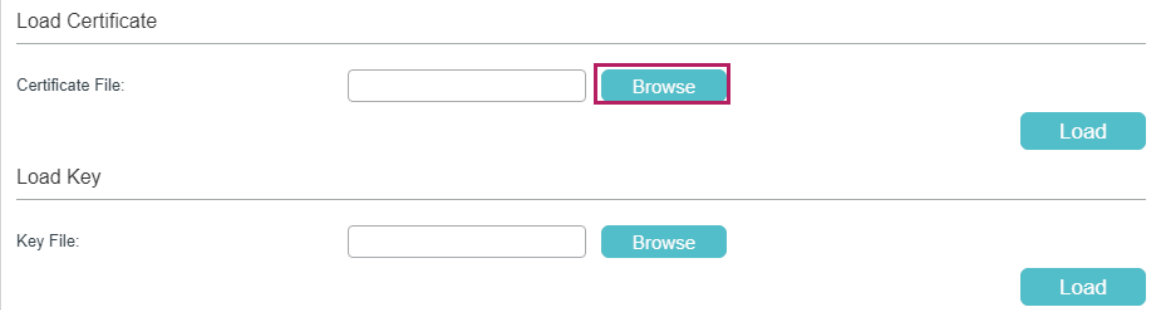


3.2.3 Downloading the Certificate and the Private Key onto the Switch

Using the GUI

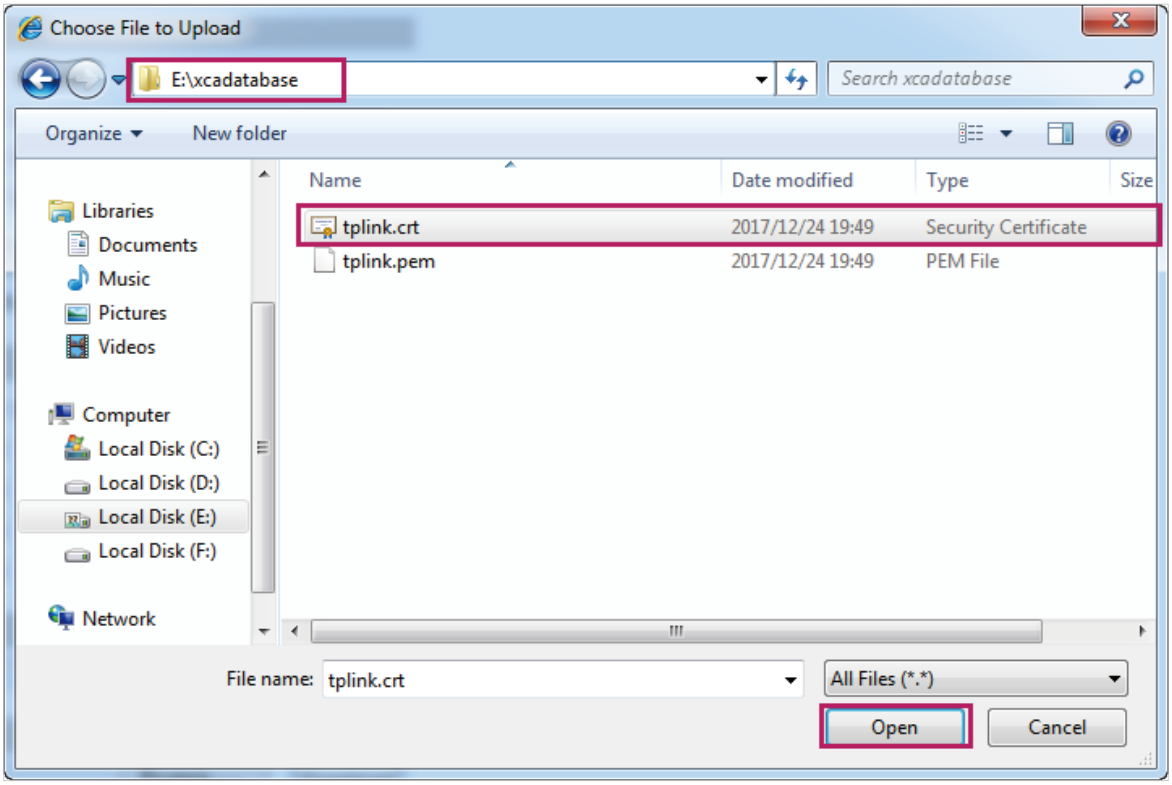
1) On the switch, choose the menu **SECURITY** > **Access Security** > **HTTPS Config** to load the following page.

Figure 3-17 Downloading the Certificate and Key



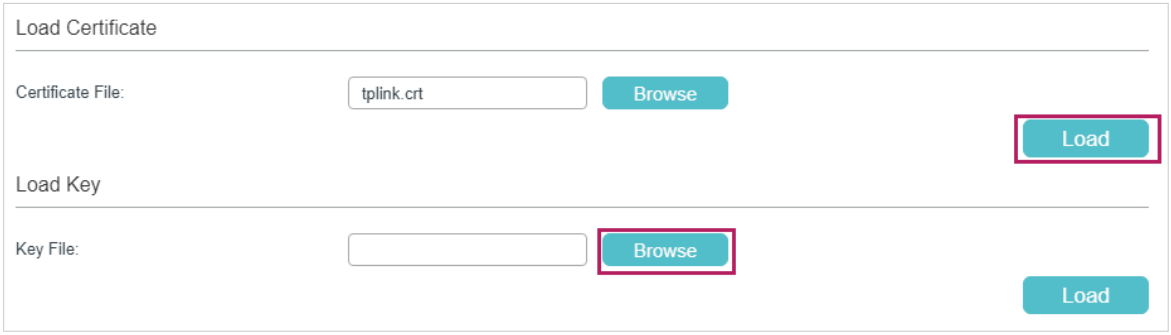
2) In the **Load Certificate** section, click **Browse** to load the following page. Enter the certificate file path in the address bar. Select the certificate file we previously exported. Click **Open**.

Figure 3-18 Specifying the Certificate to Download



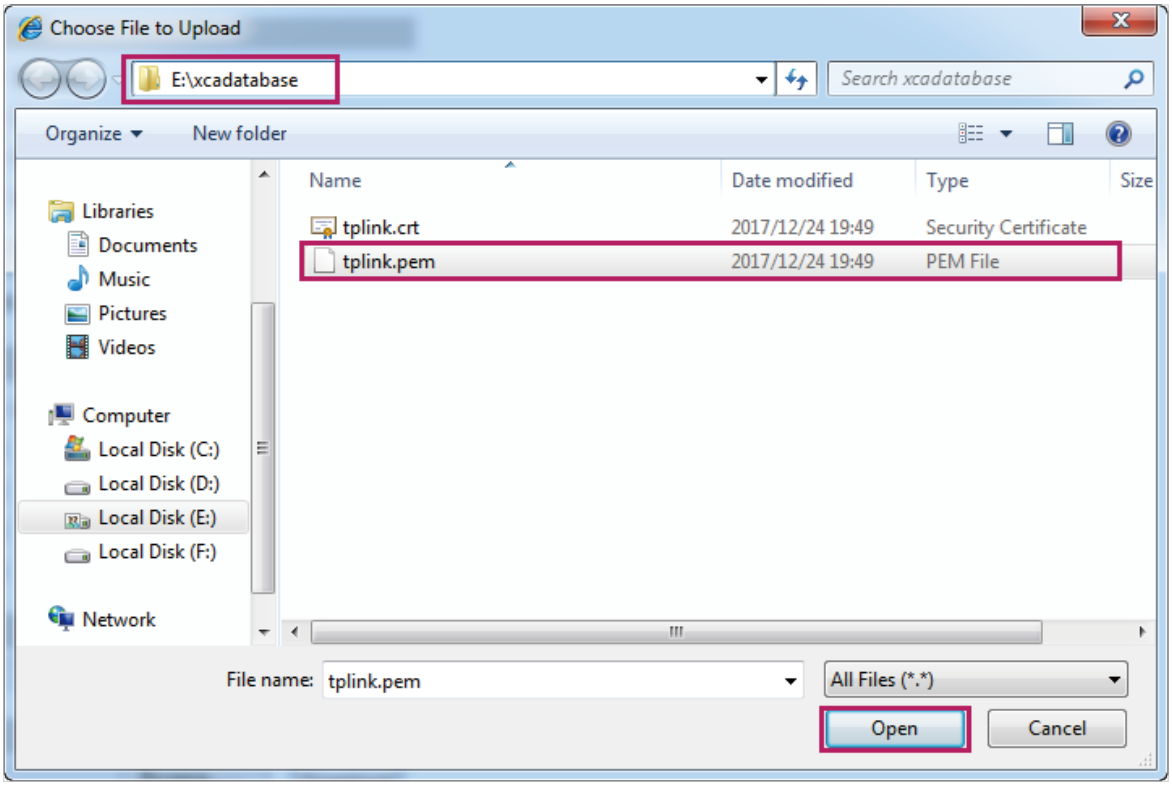
3) The following page will be displayed. In the **Load Certificate** section, click **Load** to download the certificate onto the switch.

Figure 3-19 Downloading the Certificate



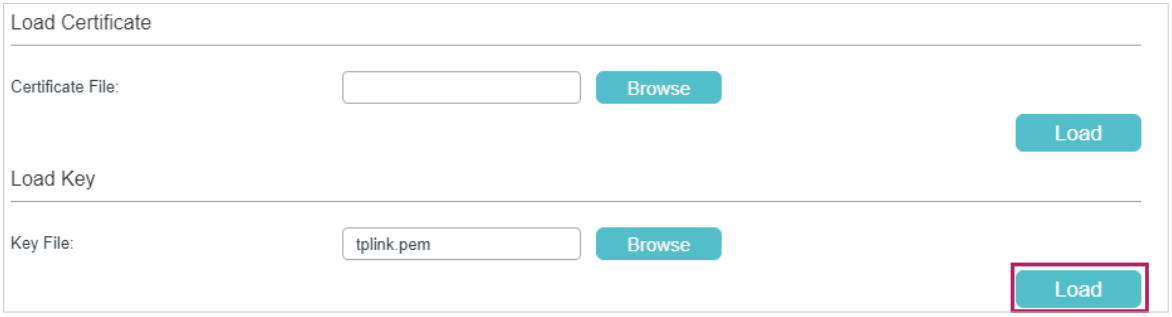
4) In the **Load Key** section, click **Browse** to load the following page. Enter the private key file path in the address bar. Select the private key file we previously exported. Click **Open**.

Figure 3-20 Specifying the Key to Download



5) The following page will be displayed. In the **Load Key** section, click **Load** to download the key onto the switch.

Figure 3-21 Downloading the Key

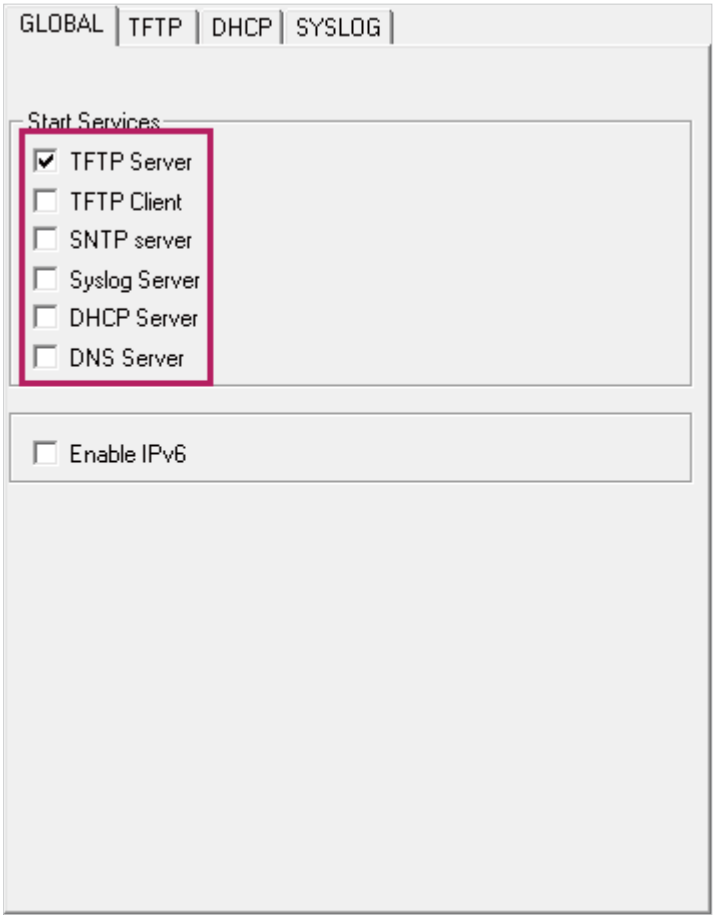


Using the CLI

1) As the switch downloads the public key file from a TFTP server, we can launch a 3rd-party TFTP server software on the PC, such as tftpd32. Go to the following website *http://tftpd32.jounin.net/tftpd32_download.html* to download tftpd32 standard edition (zip), uncompress the package and launch the software by double clicking **tftpd32.exe**.

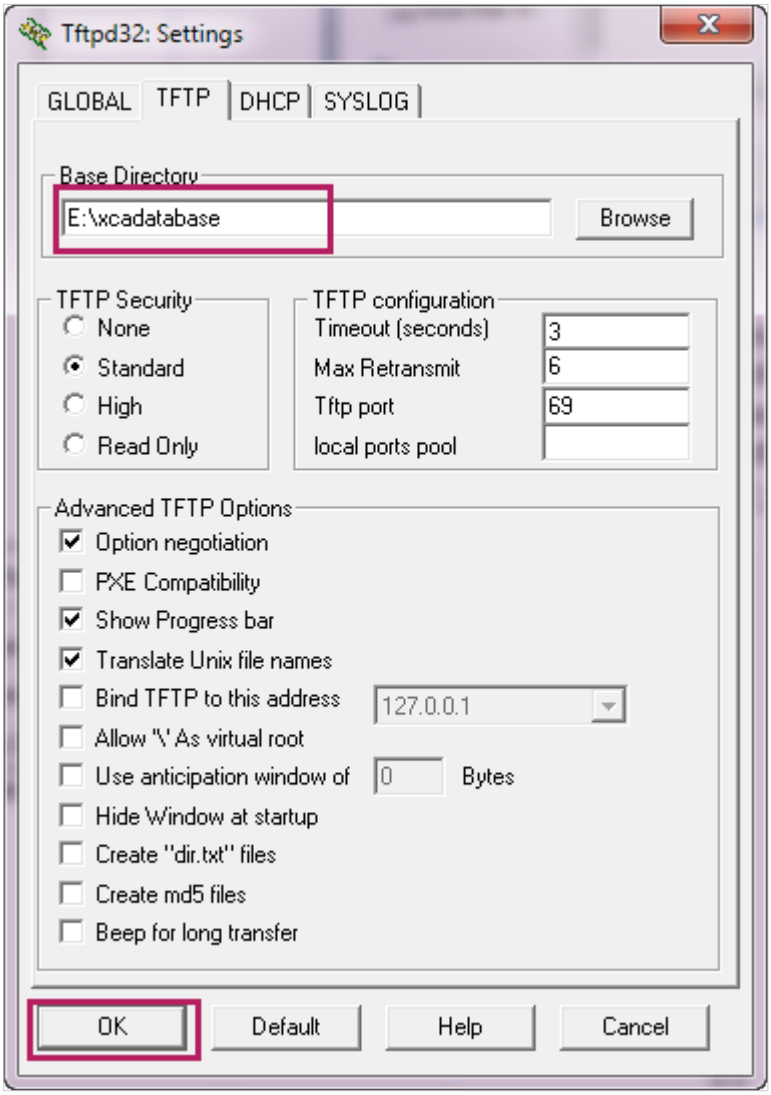
2) Click **Settings** and choose the menu **GLOBAL** to load the following page. Enable the TFTP server and disable the other functions.

Figure 3-22 Configuring the TFTP Server Gloabally



3) Choose the menu **TFTP** to load the following page. Specify the base directory as the key file and certificate file path. Click **OK**.

Figure 3-23 Configuring the Path for the TFTP Server

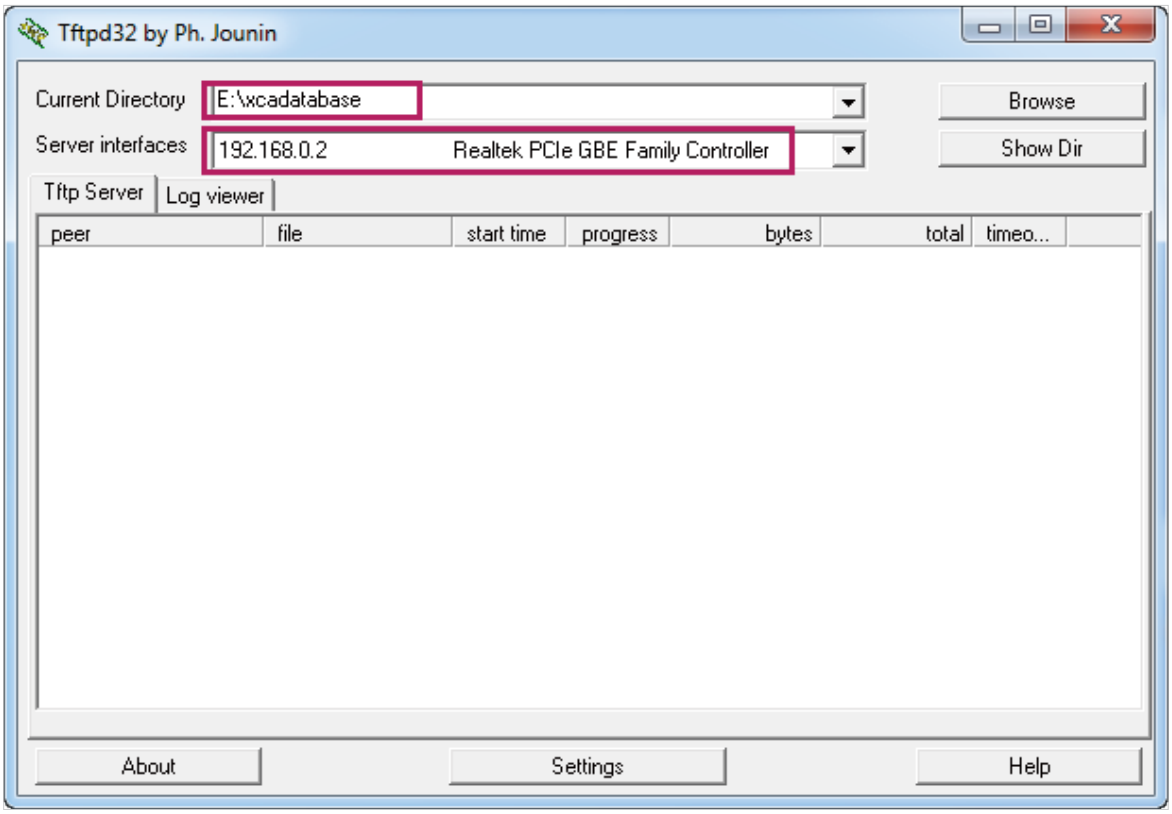


Note:

The base directory path should not include any blanks. Otherwise, the TFTP server cannot find the file.

4) Restart the TFTP software to apply the new settings, and load the following page. Specify the current directory as the key file and certificate file path. Select the server interface as **192.168.0.2** from the drop-down list. This should be the IP address of the PC.

Figure 3-24 Configuring the Interface for the TFTP Server



5) Download the certificate onto the switch.

T2600G-28TS(config)#ip http secure-server download certificate tplink.crt ip-address 192.168.0.2

Start to download SSL certificate.....

Download SSL certificate OK.

6) Download the key file onto the switch.

T2600G-28TS(config)#ip http secure-server download key tplink.pem ip-address 192.168.0.2

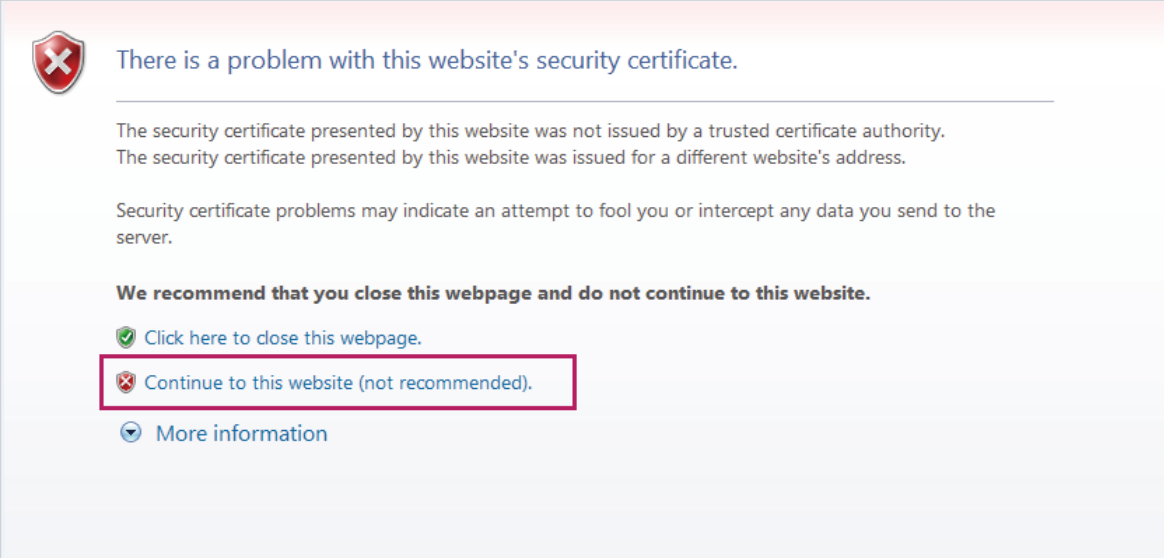
Start to download SSL key.....

Download SSL key OK.

3.2.4 Accessing the Switch Using the Self-Signed Certificate

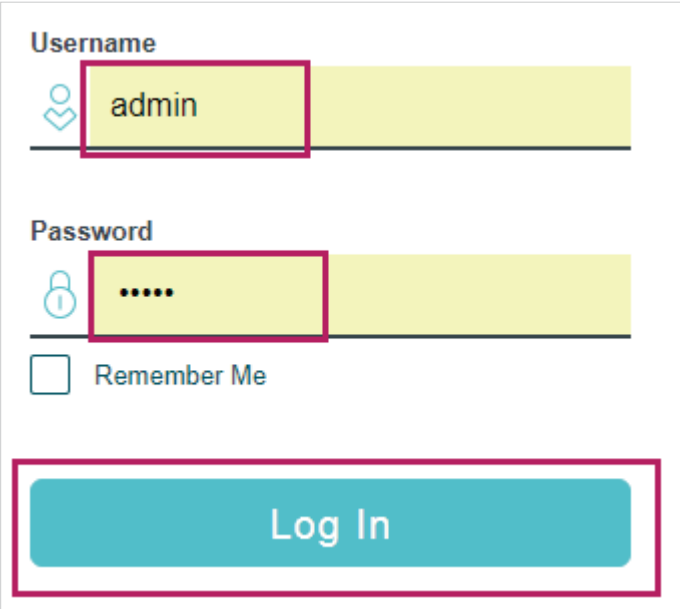
1) Launch the web browser on the PC. Here we take Internet Explorer for example. Enter **https://192.168.0.1** in the address bar of the browser, and press the **Enter** key. **https** indicates the access to the switch via HTTPS. **192.168.0.1** is the IP address of the switch. The following warning information will be displayed.

Figure 3-25 Accessing the Switch



2) The self-signed certificate, which is previously generated, should be trusted. You can just ignore this warning and click **Continue to this website (not recommended)**. The following web page will be displayed. Enter the username and the password, and click **Log In** to access and manage the switch securely.

Figure 3-26 Logging in to the Switch



COPYRIGHT & TRADEMARKS

https://www.tp-link.com