

Configuration Guide

For Accessing the Switch Securely

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

1910012326 REV1.0.0

January 2018

CONTENTS

| Overview | 1 |
|---|----|
| Accessing the Switch via SSH | 2 |
| Password Authentication Mode | 2 |
| Configuring the SSH Server | 3 |
| Configuring the SSH Client | 5 |
| Key Authentication Mode | 6 |
| Configuring the SSH Server | 7 |
| Generating the SSH Key on the PC | 9 |
| Downloading the Public Key onto the Switch | 12 |
| Configuring the SSH Client | 16 |
| Accessing the Switch via HTTPS | 20 |
| Using the Built-In Certificate of the Switch | 21 |
| Configuring the HTTPS Server | 21 |
| Accessing the Switch Using the Built-In Certificate | 22 |
| Using a Self-Signed Certificate | 23 |
| Configuring the HTTPS Server | 23 |
| Generating the Certificate and Private Key on the PC | 24 |
| Downloading the Certificate and the Private Key onto the Switch | 31 |
| Accessing the Switch Using the Self-Signed Certificate | 36 |

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.





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

 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.

| Elevera 0.0 | | CCLI Carry or Clabally | |
|-------------|-----------------|------------------------|--|
| Figure 2-2 | Configuring the | SSH Server Globally | |

| Global Config | | | |
|----------------------|--------|-----------------|--|
| SSH: | Enable | | |
| Protocol V1: | Enable | | |
| Protocol V2: | Enable | | |
| Idle Timeout: | 120 | seconds (1-120) | |
| Maximum Connections: | 5 | (1-5) | |
| Port: | 22 | (1-65535) | |
| | | | |

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

Figure 2-3 Configuring the Encryption Algorithms

| Encryption Algorit | hm |
|--------------------|--------|
| AES128-CBC: | Enable |
| AES192-CBC: | Enable |
| AES256-CBC: | Enable |
| Blowfish-CBC: | Enable |
| CAST128-CBC: | Enable |
| 3DES-CBC: | Enable |
| | |

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

Figure 2-4 Configuring the Data Integrity Algorithms

| Data Integrity Al | gorithm | | |
|-------------------|---------|--|-------|
| HMAC-SHA1: | Enable | | |
| HMAC-MD5: | Enable | | |
| | | | Apply |

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

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

 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).

| Category: Basic options for your PuTTY session Session Specify the destination you want to connect to Terminal Host Name (or IP address) Port 192.168.0.1 | Reputitive Configuration | ? × |
|--|--|---|
| Image: Section type: Connection type: Image: Section type: Image: Section type: Image: Section t | PuTTY Configuration Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation | Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port 192.168.0.1 Connection type: Raw Telnet Rlogin Ssriel Saved Sessions |
| Selection Colours Operation Default Settings Proxy Telnet Rlogin Default Settings ● SSH Default Settings Open Cancel | Iranslation Selection Colours Onection Data Proxy Telnet Rlogin SSH Serial | Default Settings Load Save |

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

 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 |
|------------|----------------------------|----------|
| | | |

| Global Config | | |
|----------------------|--------|-----------------|
| SSH: | Enable | |
| Protocol V1: | Enable | |
| Protocol V2: | Enable | |
| Idle Timeout: | 120 | seconds (1-120) |
| Maximum Connections: | 5 | (1-5) |
| Port: | 22 | (1-65535) |
| | | Apply |

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

Figure 2-8 Configuring the Encryption Algorithms

| Encryption Algorith | m |
|---------------------|--------|
| AES128-CBC: | Enable |
| AES192-CBC: | Enable |
| AES256-CBC: | Enable |
| Blowfish-CBC: | Enable |
| CAST128-CBC: | Enable |
| 3DES-CBC: | Enable |
| | |

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

Figure 2-9 Configuring the Data Integrity Algorithms

| Data Integrity A | lgorithm | |
|------------------|----------|-------|
| HMAC-SHA1: | Enable | |
| HMAC-MD5: | Enable | |
| | | Apply |

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

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

 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.

| 😰 PuTTY Key Generator | ? | X |
|---|----------|------|
| File Key Conversions Help | | |
| Key No key. | | |
| Actions | | |
| Generate a public/private key pair | nerate | |
| Load an existing private key file | oad | |
| Save the generated key Save public key Save p | rivate k | cey |
| Parameters | | |
| Type of key to generate: | SH-1 (F | RSA) |
| Number of bits in a generated key: 2048 | 3 | |

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

| 😴 PuTTY Key Generato | or | | | 8 | x |
|--|---|--------------------------------|----------------------------|----------------------------------|-----|
| <u>File Key Conversion</u> | ns <u>H</u> elp | | | | |
| Key <u>P</u> ublic key for pasting i | nto OpenSSH auth | orized_keys file | •: | | |
| ssh-rsa AAAAB3NzaC1yc2EA weLM/Q7UUSavS+0 +zlgzuUuug6oFQFGj0 brMQfbGJMsNf | AAABJQAAAQEAr olc2UE5iJ5JXo QXXDUzA5hZqcL | nY5tkNOu6jDku iS9SgqaYCry00 | uTd6vmraDZ2 QJ1D0zRFEb4 | tzr8Q00QAS5xQI 4+vx/W5tzrVHTv | • |
| Key fingerprint: | ssh-rsa 2048 5c:b | 9:50:b8:b5:a9: | :83:0a:e7:8a:8 | 88:b0:4a:e5:c7:66 | |
| Key comment: | rsa-key-2017121 | D | | | |
| Key p <u>a</u> ssphrase: | ••••• | | | | |
| Confirm passphrase: | ••••• | | | | |
| Actions | | | | | |
| Generate a public/priv | ate key pair | | | <u>G</u> enerate | |
| Load an existing privat | e key file | | | <u>L</u> oad | |
| Save the generated ke | ey - | Save p | <u>u</u> blic key | <u>S</u> ave private ke | у |
| Parameters | | | | | |
| Type of key to generat <u>R</u> SA <u></u> | e: <u>D</u> SA © <u>B</u> | ECDSA (| © ED <u>2</u> 5519 |) SSH- <u>1</u> (RS | SA) |
| Number of <u>b</u> its in a ger | nerated key: | | | 2048 | |

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

| 😴 Save public key as: | |
|--|-------------------------|
| 💭 🗸 📙 D:\PuTTY\keygen | - 4 Search keygen |
| Organize 🔻 New folder | }≡ ▼ 🔞 |
| ★ Favorites ▲ Name ▲ Desktop ▲ Downloads ▲ Recent Places | Date modified Type Size |
| □ Libraries □ Documents □ Music □ Pictures □ Videos | |
| F Computer Local Disk (C:) Ca Local Disk (D:) | |
| File name: public | • |
| Save as type: All Files (*.*) | • |
| Hide Folders | Save |

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**.

| 😴 Save private key as: | | | | | l | x |
|--|---------------|--------------------|--------------|---------------|--------|---|
| 🕞 🖓 🖟 D:\PuTTY\keygen | | | - 4 ∳ | Search keygen | | ٩ |
| Organize 🔻 New folder | | | | | | 0 |
| ★ Favorites ▲ Name | Date modified | Туре | Size | | | |
| E Desktop Downloads Recent Places | No items r | natch your search. | | | | |
| E Documents Music Pictures | | | | | | |
| Videos | | | | | | |
| Local Disk (C:) | | | | | | |
| File name: private | | | | | | • |
| Save as type: PuTTY Private Key Files (*.ppk | () | | | | | • |
|) Hide Folders | | | [| Save | Cancel | |

Figure 2-13 Saving the Private Key

2.2.3 Downloading the Public Key onto the Switch

Using the GUI

 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

| Import Key File | | | | |
|-----------------------|---------------------------------------|--------|---|--------|
| Choose the SSH public | c key file to be imported to the swit | ch. | | |
| Key Type: | SSH-2 RSA/DSA | • | _ | |
| Key File: | | Browse | | |
| | | | | Import |

 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.

| Choose File to Upload | | | | | | | | | X |
|-----------------------|---------------|---|------------------|-------------------|----------------------------|---------------|------|--------|---|
| D:\PuTTY\key | /gen | | | | - - - - - - - - - - | Search ke | ygen | | ٩ |
| Organize 🔻 New folder | | | | | | | | | 0 |
| ★ Favorites | Name | ^ | Date modified | Туре | Size | | | | |
| Marktop | 🔹 private.ppk | | 2017/12/10 16:05 | PuTTY Private Key | 1 | KB | | | |
| \rm Downloads | D public | | 2017/12/10 16:04 | File | 1 | KB | | | |
| Recent Places | | | | | | | | | |
| P | | | | | | | | | |
| Documents | | | | | | | | | |
| Music | | | | | | | | | |
| E Pictures | | | | | | | | | |
| Videos | | | | | | | | | |
| | | | | | | | | | |
| Normal Computer | | | | | | | | | |
| Local Disk (C:) | | | | | | | | | |
| Local Disk (D:) | | | | | | | | | |
| local Disk (E:) | | | | | | | | | |
| | | | | | | | | | |
| File nan | ne: public | | | | - | All Files (*. | *) | | • |
| | | | | | | 0.000 | | Cancel | |
| | | | | | | Upen | | Cancel | |

Figure 2-15 Downloading the Public Key onto the Switch

Using the CLI

- 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.

| GLOBAL TFTP | DHCP SYSLOG |
|---|---------------|
| Start Services TFTP Server TFTP Client SNTP server Syslog Server DHCP Server DNS Server | |
| Enable IPv6 | |
| | |
| | |
| | |
| | |

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

| D:\PuTTY\keygen | | Browse | |
|---|---|--------------|--|
| IFTP Security None Standard High Read Only Advanced TFTP Options ✓ Option negotiation PXE Compatibility ✓ Show Progress bar ✓ Translate Unix file na Bind TFTP to this ad △ Allow "\'As virtual root Use anticipation wind □ Hide Window at start □ Create "dir.txt" files □ Create md5 files □ Beep for long transfe | TFTP configuration Timeout (seconds) Max Retransmit Tftp port local ports pool dress 127.0.0.1 ot dow of 0 Bytes up | 3 6 69 | |
| OK Defa | ault Help | Cancel | |

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.

| * | 🔖 Tftpd32 by Ph. J | ounin | | | |
|---|--------------------|-----------------|--------------------|------------------|------------------------------|
| | Current Directory | D:\PuTTY\keygen | | • | Browse |
| | Server interfaces | 192.168.0.2 | Realtek PCIe GBE F | amily Controller | Show Dir |
| | Tftp Server Log vi | ewer | | | |
| | peer | file | start time progre | ss bytes | total timeo |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | 1 | | | | |
| | About | | Settings | | Help |

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

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 |
|-------------|-----------------------------|
| 119010 2 10 | |

| Reputitive Putty Configuration | ? 💌 |
|---|--|
| Pully Configuration Category: Session Category: Session Category: Session Category: Session Category: Category: Selection Colours Colours Connection Proxy Telnet Rlogin €. SSH Serial | Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port 192.168.0.1 Connection type: Raw Telnet Rlogin SSH Segial Load, save or delete a stored session Saved Sessions Default Settings Default Settings Default Settings Default Settings Delete Close window on exit: Always Never Only on clean exit |
| About <u>H</u> elp | Open Cancel |

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

| Real PuTTY Configuration | ? × |
|--|--|
| Category: | Options controlling SSH connections |
| ···· Logging ⊡·· Terminal ···· Keyboard ··· Bell ···· Features | Data to send to the server Remote command: |
| → Features → Window → Appearance → Behaviour → Translation → Selection → Colours → Colours → Connection → Data → Proxy → Telnet → Rlogin → Serial | Protocol options Don't start a shell or command at all Enable compression SSH protocol version: 2 1 (INSECURE) Sharing an SSH connection between PuTTY tools Share SSH connections if possible Permitted roles in a shared connection: Upstream (connecting to the real server) Downstream (connecting to the upstream PuTTY) |
| About Help | Open Cancel |

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

Figure 2-21 Configuring the SSH Authentication

| Real PuTTY Configuration | n | | ? × |
|--------------------------|------|-------------------------------------|---|
| Category: | | | |
| Category: | A E | Options controlling SSH authenticat | ion ? only) y) I-2) SSH-2 Browse |
| X11 Tunnels | | | |
| Bugs More bugs | | | |
| About | Help | Open | Cancel |

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

| 🕵 Select private key file | | | | | | | X |
|-----------------------------|------------------|---|------------------|-------------------|------------------|-------------------------------|------|
| D:\PuTTY\ke | eygen | | | | - - ↓ + † | Search keygen | Q |
| Organize 🔻 New folde | er | | | | | :≕ ▼ □ | 0 |
| ☆ Favorites | Name | ^ | Date modified | Туре | Size | | |
| Desktop | 🖹 private.ppk | | 2017/12/10 16:05 | PuTTY Private Key | 11 | KB | |
| Downloads Secent Places | | | | | | _ | |
| | | | | | | | |
| Documents | | | | | | | |
| d Music ■ | | | | | | | |
| Pictures | | | | | | | |
| Videos | | | | | | | |
| Computer | | | | | | | |
| Local Disk (C:) | | | | | | | |
| Local Disk (E:) | | | | | | | |
| 👝 Local Disk (F:) | | | | | | | |
| File na | ame: private.ppk | | | | • | PuTTY Private Key Files (*.pp | k) 🔻 |
| | | | | | | Open 🔻 Canc | el |
| | | | | | | | |

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

 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

| Global Config | | | |
|----------------|---------|-----------|-------|
| HTTPS: | Senable | | |
| SSL Version 3: | Enable | | |
| TLS Version 1: | Enable | | |
| Port: | 443 | (1-65535) | |
| | | | Apply |

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

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

| CipherSuite Config | | | |
|----------------------------|--------|--|--|
| RSA_WITH_RC4_128_MD5: | Enable | | |
| RSA_WITH_RC4_128_SHA: | Enable | | |
| RSA_WITH_DES_CBC_SHA: | Enable | | |
| RSA_WITH_3DES_EDE_CBC_SHA: | Enable | | |
| | | | |

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

 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 |
|--------------|-----------------------|
| i igui o o i | roocooning the ownton |

| \$ There is a problem with this website's security certificate. |
|---|
| The security certificate presented by this website was not issued by a trusted certificate authority. The security certificate presented by this website was issued for a different website's address. |
| Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server. |
| We recommend that you close this webpage and do not continue to this website. |
| Click here to close this webpage. |
| Solution Continue to this website (not recommended). |
| |
| |
| |

 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.

| Username | | | | | | |
|-------------|--|--|--|--|--|--|
| Password | | | | | | |
| Remember Me | | | | | | |
| Log In | | | | | | |

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

 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

| Global Config | | | |
|----------------|----------|-----------|-------|
| HTTPS: | Enable | | |
| SSL Version 3: | C Enable | | |
| TLS Version 1: | Enable | | |
| Port: | 443 | (1-65535) | |
| | | | Apply |

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

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

| CipherSuite Config | | | |
|----------------------------|----------|--|--|
| RSA_WITH_RC4_128_MD5: | ✓ Enable | | |
| RSA_WITH_RC4_128_SHA: | Enable | | |
| RSA_WITH_DES_CBC_SHA: | Enable | | |
| RSA_WITH_3DES_EDE_CBC_SHA: | Enable | | |
| | | | |

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

 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.

| ð | ✓ X Certificate and Key management | | | | | | | |
|---|------------------------------------|-----------------|---------------|--------------|-----------|------------|--|--|
| F | ile Import | Token Extra | Help | | | | | |
| | Private Keys | Certificate sig | ning requests | Certificates | Templates | Revocation | n lists | |
| | | | | | | | New Key | |
| | | | | | | | Export | |
| | | | | | | | Import | |
| | | | | | | | Import PFX (PKCS#12) | |
| | | | | | | | Show Details | |
| | | | | | | | Delete | |
| | | | | | | | ACCH ACCH ACCH ACCH ACCH ACCH ACCH ACCH | |

Figure 3-8 Launching the XCA Software

 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.

| 🔗 Open XCA Database | - orthogen - testerer - tester | | × |
|---------------------------------------|--------------------------------|------------|-----------------|
| C C C C C C C C C C C C C C C C C C C | | ✓ 4 Search | h xcadatabase 🔎 |
| Organize 🔻 New folder | | | := - 🔞 |
| Name | Date modified | d Type | Size |
| | No items match you | ır search. | |
| •3 ⊦ | | | |
| p≡ c ≝ □ | | | |
| | | | |
| ¶in N I≣ | | | |
| File name xcadata | | | |
| Save as type: XCA Databases | (*.xdb) | | |
|) Hide Folders | | Sa | Cancel |

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 | Kev |
|--------|------|--------------|-------|---------|------|
| riguio | 0 10 | or cutting u | 11011 | invato | 1.09 |

| 🔗 X Certifica | te and Key mar | nagement | | ? × |
|---------------|----------------------------|----------------------|------------------|--------|
| New ke | y e a name to th | e new key and select | the desired keys | size |
| Key prope | erties | | | |
| Name | tplink | | | |
| Keytype | RSA | | | |
| Keysize | 2048 bit |] | | - |
| 🕅 Remember | r as default | | | |
| | | | Create | Cancel |

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

| X Certificate and Key management | | | | | | | |
|---|----------------------|--|--|--|--|--|--|
| <u>F</u> ile I <u>m</u> port <u>T</u> oken Extra <u>H</u> elp | | | | | | | |
| Private Keys Certificate signing requests Certificates Templates Revocation lists | | | | | | | |
| Internal name Type Size Use Password | New Key | | | | | | |
| tplink RSA 2048 bit 1 Common | Export | | | | | | |
| | Import | | | | | | |
| | Import PFX (PKCS#12) | | | | | | |
| | Show Details | | | | | | |
| | Delete | | | | | | |
| | XCH | | | | | | |
| Database: E:/xcadatabase/xcadata.xdb | | | | | | | |

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 |
|-------------|------------------------|
|-------------|------------------------|

| 🞸 X Certificate and Key management | ? × |
|--|-----------------------------------|
| Export private key [RSA] | |
| Filename E:/xcadatabase/tplink.pem | |
| Unencrypted private key in text format | Export Format PEM private (*.pem) |
| | OK Cancel |

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.

| irce | Subject | Extensions | Key usage | Netscape | Advanced | | | |
|---|---|------------------|-------------------|----------|----------|------------------|-------------------|---------------------------------------|
| | | | | | | | | |
| ianina | request | | | | | | | |
| Sig | n this Certific | ate signing red | juest | | | | | ~ |
| / Cor | oy extension | s from the requ | Jest | | | Show | v request | |
| Mo | dify subject (| of the request | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| igning | | | | | | | | |
| igning | eate a self sig | gned certificate | with the serial | 1 | | | | |
| igning) Cre | eate a self sig | ned certificate | with the serial | 1 | | | | |
| igning) Cre | eate a self sig e this Certific | ned certificate | with the serial | 1 | | | | Ŧ |
| igning) Cre) Use | eate a self sig e this Certific e algorithm | aned certificate | with the serial | 1 | SHA 256 | | | |
| igning Cre Use | eate a self sig e this Certific e algorithm | aned certificate | with the serial | 1 | SHA 256 | | | · · · · · · · · · · · · · · · · · · · |
| igning Cre Use nature | eate a self sig e this Certific e algorithm te for the ne | aned certificate | with the serial | 1 | SHA 256 | | | ~ |
| igning Cre Use nature empla | eate a self sig e this Certific e algorithm te for the ne ult] CA | ned certificate | with the serial | 1 | SHA 256 | | | · · · · · · · · · · · · · · · · · · · |
| igning Cre Use nature empla | eate a self sig e this Certific e algorithm te for the ne alt] CA | ate for signing | e with the serial | 1 | SHA 256 | Apply extension: | s) (Apply subject | T 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.

| X Certificate and Key r Create x509 Ce | nanagement ertificate | | | | | |
|---|--------------------------|-----------|----------|------------------------|---------------------|------------------|
| Source Subject | Extensions k | Key usage | Netscape | Advanced | | |
| Distinguished name | | | | | | |
| Internal name | tplink | | | organizationName | tplinkSMB | |
| countryName | CN | | | organizationalUnitName | tplinkswitch | |
| stateOrProvinceName | Guangdong | | | commonName | tplinkdocument | |
| localityName | Shenzhen | | | emailAddress | support@tp-link.com | |
| Тур | e | | | Content | | Add |
| | | | | | | |
| Private key tplink (RSA:2048 bit) | | | | • | Used keys too Ge | nerate a new key |
| | | | | | | |

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.

| 🗸 X Certificate and Key management | | | | | | |
|---|--------------------------------------|--|--|--|--|--|
| <u>F</u> ile I <u>m</u> port <u>T</u> oken Extra <u>H</u> elp | | | | | | |
| Private Keys Certificate signing requests Certificates Templates Revocation | on lists | | | | | |
| Internal name commonName CA Serial Expiry date | New Certificate | | | | | |
| | Export | | | | | |
| | Import | | | | | |
| | Show Details | | | | | |
| | Delete | | | | | |
| | Import PKCS#12 | | | | | |
| | Import PKCS#7 | | | | | |
| | Plain View | | | | | |
| 4 | Zaseminosta Dinoloso Jine Jine | | | | | |
| Database: E:/xcadatabase/xcadata.xdb | | | | | | |

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

| 🔗 X Certificate and Key management | ? × |
|------------------------------------|---------------------------|
| Certificate export | Bullen 7 Ter |
| Name tplink | |
| Filename E:/xcadatabase/tplink.crt | |
| PEM Text format with headers | |
| | Export Format PEM (*.crt) |
| | OK Cancel |

3.2.3 Downloading the Certificate and the Private Key onto the Switch

Using the GUI

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

| Figure 3-17 | Downloading the Certificate and Key |
|-------------|-------------------------------------|
|-------------|-------------------------------------|

| Load Certificate | | |
|-------------------|--------|------|
| Certificate File: | Browse | |
| | | Load |
| Load Key | | |
| Key File: | Browse | |
| | | Load |

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

| Choose File to Upload | | | X |
|--|--------------------------------|----------------------|-------|
| COO V E:\xcadatabase | ✓ ✓ Search | xcadatabase | ٩ |
| Organize 🔻 New folder | | !≡ ▼ 🔳 | 0 |
| Name | Date modified | Туре | Size |
| Libraries | 2017/12/24 19:49 | Security Certificate | |
| bocuments tplink.pem | 2017/12/24 19:49 | PEM File | |
| E Pictures | | | |
| Videos | | | |
| P Computer ▲ Local Disk (C:) Local Disk (D:) R Local Disk (F:) C Nutried | | | |
| Vetwork | | | Þ |
| File name: tplink.crt | All Files Ope | (*.*) Cancel | • |

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

| Load Certificate | | | |
|-------------------|------------|--------|------|
| Certificate File: | tplink.crt | Browse | |
| | | | Load |
| Load Key | | | |
| Key File: | | Browse | |
| | | | Load |

 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.

| Choose File to Upload | | | | x |
|-----------------------|--------------------|----------------------------|----------------------|------|
| E:\xcadat | abase | ✓ 4y Search x | cadatabase | ٩ |
| Organize 🔻 New fo | older | | | 0 |
| | ^ Name | Date modified | Туре | Size |
| Documents | 🔄 tplink.crt | 2017/12/24 19:49 | Security Certificate | |
| Music | tplink.pem | 2017/12/24 19:49 | PEM File | |
| Pictures | | | | |
| Videos | | | | |
| 🖳 Computer | | | | |
| 🏭 Local Disk (C:) | E | | | |
| 👝 Local Disk (D:) | | | | |
| Real Disk (E:) | | | | |
| 👝 Local Disk (F:) | | | | |
| 🗣 Network | ▼ < | | | F |
| File | e name: tplink.pem | ✓ All Files (¹ | *,*) | • |
| | | Оре | Cancel | |

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 I | Key | | |
|-------------------------------|------------|--------|------|
| Load Certificate | | | |
| Certificate File: | | Browse | |
| | | | Load |
| Load Key | | | |
| Key File: | tplink.pem | Browse | |
| | | | Load |

Using the CLI

- 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

| GLOBAL TFTP DHCP SYSLOG | | | | | | | |
|-------------------------|-----------------|--|--|--|--|--|--|
| | | | | | | | |
| | Start Services | | | | | | |
| | ✓ TFTP Server | | | | | | |
| | TFTP Client | | | | | | |
| | SNTP server | | | | | | |
| | 🔲 Syslog Server | | | | | | |
| | DHCP Server | | | | | | |
| | DNS Server | | | | | | |
| | | | | | | | |
| | 🔲 Enable IPv6 | | | | | | |
| L | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

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 |
|-------------|--|
|-------------|--|

| P Security None Standard High Read Only anced TFTP Options Option negotiation PXE Compatibility Show Progress bar |
|---|
| Option negotiation PXE Compatibility Show Progress bar |
| Translate Unix file names Bind TFTP to this address 127.0.0.1 Allow "\' As virtual root Use anticipation window of 0 Bytes Hide Window at startup Create "dir.txt" files Create md5 files Beep for long transfer |

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

_ _ _ _ _

 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.

| Ŵ | Tftpd32 by Ph. | Jounin | | | |
|---|-------------------|----------------|------------------------|------------------|-------------|
| | Current Directory | E:\xcadatabase | | • | Browse |
| | Server interfaces | 192.168.0.2 | Realtek PCIe GBE Famil | y Controller 📃 💌 | Show Dir |
| | Tftp Server Log | viewer | | | |
| | peer | file | start time progress | bytes | total timeo |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | 1 | | | | |
| | About | | Settings | | Help |

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

 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 |
|-------------|------------------------|
| 119010020 | ribbeedding the Ownton |

| ne security certificate pro ne security certificate pro | esented by this website v esented by this website v | as not issued by a truste as issued for a different | d certificate authority. website's address. |
|--|--|--|--|
| curity certificate proble rver. | ms may indicate an atten | pt to fool you or interce | pt any data you send to t |
| le recommend that yo | ou close this webpage a | nd do not continue to | this website. |
| Click here to close this | webpage. | | |
| Continue to this webs | ite (not recommended). | | |
| More information | | _ | |

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.

| User | admin | | | | |
|-------------|-------|--|--|--|--|
| \diamond | aumin | | | | |
| Pass | word | | | | |
| <u>ි</u> | | | | | |
| Remember Me | | | | | |
| Log In | | | | | |

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. **Ptp-link** is a registered trademark of TP-Link Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-Link Technologies Co., Ltd. Copyright © 2018 TP-Link Technologies Co., Ltd. All rights reserved.

https://www.tp-link.com