1 HTTP Commands

Command	Function
enable service web-server	Enable the Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) service.
http check-version	Detect upgrade files on an HTTP server.
http port	Configure a port for the HTTP service.
http secure-port	Configure a port for the HTTPS service.
http update	Configure a file for manual upgrade.
http update mode	Configure the manual upgrade mode for HTTP upgrade.
http update server	Configure the server address and port number for HTTP upgrade.
http update set oob	Configure HTTP upgrade using the MGMT port.
http update source_ip	Configure the source IP address for HTTP upgrade.
http update time	Configure HTTP automatic detection time.
show web-server https certificate information	Display information about the HTTPS service certificate.
show web-server status	Display the configuration and status of the Web service.
webmaster level	Configure a username and a password for Web login and authentication.
web-server http redirect-to-https	Configure automatic HTTP redirection to HTTPS.
web-server https certificate	Install an HTTPS certificate.
web-server https generate self-signed-certificate	Generate an HTTPS service self-signed certificate again.

1.1 enable service web-server

Function

Run the **enable service web-server** command to enable the Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) service.

Run the **no** form of this command to disable the HTTP and HTTPS service.

Run the **default** form of this command to restore the default configuration of the HTTP and HTTPS service.

The HTTP and HTTPS services are disabled by default.

Syntax

enable service web-server [**all** | **http** | **https**]

no enable service web-server [**all** | **http** | **https**]

default enable service web-server [**all** | **http** | **https**]

Parameter Description

all | **http** | **https**: Enables the service. Here, **all** indicates that both the HTTP and HTTPS services are enabled; **http** indicates that only the HTTP service is enabled; **https** indicates that only the HTTPS service is enabled. Both the HTTP and HTTPS services are enabled by default.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- If no keyword is configured or the **all** keyword is configured at the end of the command, both the HTTP and HTTPS services are enabled; if the **http** keyword is configured, only the HTTP service is enabled; if the **https** keyword is configured, only the HTTPS service is enabled.
- The **no enable service web-server** command or the **default enable service web-server** command is configured to disable the HTTP service. If no keyword is entered at the end of the **no enable service web-server** or **default enable service web-server** command, both the HTTP and HTTPS services are disabled.

Examples

The following example enables both the HTTP and HTTPS services.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# enable service web-server all
```

Notifications

If the port is 80 and the HTTP service fails, the following notification will be displayed:

```
%notice:Failed to open tcp listen, port=[80].
```

Common Errors

If the port is occupied by other modules, the Web service may not be enabled.

Platform Description

N/A

Related Commands

N/A

1.2 http check-version

Function

Run the **http check-version** command to detect upgrade files on an HTTP server.

Detecting available upgrade files on an HTTP server is enabled by default.

Syntax

http check-version [**extend**]

Parameter Description

extend: Detects upgrade files on more than one HTTP server.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example detects upgrade files on an HTTP server.

```
Hostname> enable
Hostname# http check-version
Business modules need to be updated: character-db, route-db
app name:web
    app-name           version          filename
----- -----------------
character-db     2014.02.09.14.02.09 app_sub_1.exe
character-db     2014.02.09.14.02.09 app_file_list.txt
character-db     2014.02.09.14.02.09 app_sub_3.exe
character-db     2014.02.09.14.02.09 app_sub_2.exe
route-db         2013.12.01.00       route-choose.db
```

Notifications

If no service module is registered with the upgrade module, the following notification will be displayed:

```
%notice: No bussiness modules registration.
```

If the device cannot establish a connection with the server or the communication with the server fails, the following notification will be displayed:

```
%notice: Communicate with the server failed.
```

If the memory of the device is insufficient, the following notification will be displayed:

```
%warning: Out of memory, application memory failure.
```

If the format of the response packet of the server is incorrect, the following notification will be displayed:

```
%notice: The server response message format is wrong.
```

If the service module is being upgraded or has not registered a version number, the following notification will be displayed:

```
%notice: Suspend, some business modules are upgrading or haven't registered
release.
```

If the versions of all service modules are the latest, the following notification will be displayed:

```
%notice: All bussiness modules are the latest versions.
```

Common Errors

Communication with the server fails during running of this command, possibly because the network fails or the DNS service is not enabled.

Platform Description

N/A

Related Commands

N/A

1.3 http port

Function

Run the **http port** command to configure a port for the HTTP service.

Run the **no** form of this command to restore the default port number.

The default port number of the HTTP service is **80**.

Syntax

http port *port-number*

no http port

Parameter Description

port-number: Port number of the HTTP service. The range is 80 and from 1025 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the port number of the HTTP service to 8080.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http port 8080
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 http secure-port

Function

Run the **http secure-port** command to configure a port for the HTTPS service.

Run the **no** form of this command to restore the default port number.

The default port number of the HTTPS service is **443**.

Syntax

http secure-port *port-number*

no http secure-port

Parameter Description

port-number: Port number of the HTTPS service. The range is 443 and from 1025 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the port number of the HTTPS service to 4443.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http secure-port 4443
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 http update

Function

Run the **http update** command to configure a file for manual upgrade.

No file for manual upgrade is configured by default.

Syntax

http update [**extend**] { **all** | *module* }

Parameter Description

extend: Configures multiple servers.

all: Upgrades all the service modules.

Module: Name of the service module to be upgraded. More names can be entered and are separated by spaces.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example manually downloads the latest upgrade file **route-db** from the remote server.

```
Hostname> enable
Hostname# http update route-db
Downloading updated files, please wait...
Press Ctrl+C to quit
route-db: download and notify successfully.
```

Notifications

If no service module is registered with the upgrade module, the following notification will be displayed:

```
%notice: No bussiness modules registration.
```

If the specified service module is not registered, the following notification will be displayed:

```
%notice: The bussiness modules haven't registered.
```

If the current upgrade module is being upgraded, the following notification will be displayed:

```
%notice: There are business modules in the upgrading, please wait for a moment.
```

If the device cannot establish a connection with the server or the communication with the server fails, the following notification will be displayed:

```
%notice: Communicate with the server failed.
```

If the memory of the device is insufficient, the following notification will be displayed:

```
%warning: Out of memory, application memory failure.
```

If the format of the response packet of the server is incorrect, the following notification will be displayed:

```
%notice: The server response message format is wrong.
```

If the service module is being upgraded or has not registered a version number, the following notification will be displayed:

```
%notice: Suspend, some business modules are upgrading or haven't registered
release.
```

If the versions of all service modules are the latest, the following notification will be displayed:

```
%notice: All bussiness modules are the latest versions.
```

Common Errors

Communication with the server fails during running of this command, possibly because the network fails or the DNS service is not enabled.

Platform Description

N/A

Related Commands

N/A

1.6 http update mode

Function

Run the **http update mode** command to configure the manual upgrade mode for HTTP upgrade.

Run the **no** form of this command to switch to the automatic upgrade mode.

The default HTTP upgrade mode is manual upgrade.

Syntax

http update mode manual

no http update mode

Parameter Description

manual: Specifies the manual upgrade mode.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the **no http update mode** command is run to switch the HTTP upgrade mode to automatic upgrade mode, the system detects upgrade files on the server by default, automatically downloads the files, and performs an upgrade when the scheduled timer expires.

Examples

The following example configures automatic upgrade mode for HTTP upgrade.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update mode manual
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 http update server

Function

Run the **http update server** command to configure the server address and port number for HTTP upgrade.

Run the **no** form of this command to remove this configuration and restore the default configuration.

The default server address for HTTP upgrade is **0.0.0.0** and the default port number is **80**.

Syntax

http update server { *host-name* | *ipv4-address* } [**port** *port-number* | **extend** | **uri**]

no http update server

Parameter Description

host-name: Domain name of the server.

ipv4-address: Server address.

port *port-number*: Configures the server port number. Here, *port-number* indicates the port number. The range is from 1 to 65535.

extend: Configures multiple servers.

uri: Configures URI. URI indicates the local path for storing the Web package.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- The server address may not be configured because the local upgrade record file records the addresses of possible upgrade servers.
- The DNS feature needs to be enabled on the device and the DNS address needs to be configured by default.
- The server address does not support IPv6.
- During an HTTP upgrade, the device connects to the server address configured by this command. If the server address cannot be connected, the device attempts to connect to server addresses recorded in the local file in turn. If none of them are connected, the upgrade cannot be performed.

Examples

The following example sets the address of the HTTP upgrade server to 10.83.132.1 and the port number to 90.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update server 10.83.132.1 port 90
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 http update set oob

Function

Run the **http update set oob** command to configure HTTP upgrade using the MGMT port.

Run the **no** form of this command to configure HTTP upgrade using a common port and restore the default configuration.

The upgrade using a common port instead of a MGMT port is configured by default.

Syntax

http update set oob

no http update set oob

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is available on only the devices that support the MGMT port.

Examples

The following example configures HTTP upgrade using the MGMT port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update set oob
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 http update source_ip

Function

Run the **http update source_ip** command to configure the source IP address for HTTP upgrade.

Run the **no** form of this command to restore the default configuration, that is, no source IP address is specified.

Syntax

http update source_ip *ipv4-address*

no http update source_ip

Parameter Description

ipv4-address: IPv4 source address.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure a source IP address for HTTP upgrade.

Examples

The following example sets the source IP address bound for HTTP upgrade to 192.168.1.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update source_ip 192.168.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 http update time

Function

Run the **http update time** command to configure HTTP automatic detection time.

Run the **no** form of this command to remove the configured HTTP automatic detection time and restore the default configuration.

The HTTP automatic detection time is random in the range from 00:00 to 23:59 by default.

Syntax

http update time daily *hh*:*mm*

no http update time

Parameter Description

hh:*mm*: Upgrade time, in the format of hour:minute (24-hour system). Here, *hh* indicates hours, and *mm* indicates minutes.

range *hh:mm hh:mm*: Time span for automatic upgrade.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the automatic HTTP detection time.

The device connects to the Web server as scheduled to check for available upgrade files. You can view obtained files on the Web page.

Examples

The following example sets the HTTP automatic detection time to 23:40.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http update time daily 23:40
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 show web-server https certificate information

Function

Run the **show web-server https certificate information** command to display information about the HTTPS service certificate.

Syntax

show web-server https certificate information

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays information about the HTTPS service certificate.

```
Hostname> enable
Hostname# show web-server https certificate information
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Self-Signed-CA472E87
        Validity
            Not Before: Feb 20 07:26:51 2019 GMT
            Not After : Feb 17 07:26:51 2029 GMT
        Subject: CN=Self-Signed-CA472E87
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ec:39:13:5a:09:da:97:d1:83:8f:a7:77:cf:b4:
                    88:96:a0:85:23:68:4d:5a:c6:d3:4b:d9:c0:d6:1b:
                    f4:42:29:ce:33:2e:2f:79:5e:cc:bb:bd:5f:63:5b:
                    41:f3:9f:fb:82:c7:ca:8a:21:a9:c2:fb:36:db:62:
                    08:3c:05:b8:a2:47:07:1a:20:99:80:24:63:a4:08:
                    66:22:86:b6:aa:46:43:8a:91:7d:99:f3:8a:7c:58:
                    ac:1f:ef:6c:4c:d1:d6:bf:ef:a1:77:64:4b:53:16:
```

```
                29:2f:1c:e8:ec:d6:6b:b6:34:64:32:00:1f:09:30:
                69:8d:2e:85:d5:6a:db:45:cb:b8:fd:38:ba:bd:68:
                1d:de:38:65:ef:3f:c6:90:bf:ca:1a:9e:df:c3:75:
                5f:20:bd:61:b4:bd:43:6b:77:ef:25:c6:43:0a:0f:
                dc:5a:0e:28:53:37:14:77:8b:bd:ea:14:54:c5:e1:
                45:27:c9:14:63:37:67:bc:0f:09:15:1f:73:ae:bb:
                46:b1:ad:cd:23:89:fd:2c:0c:9f:a3:34:62:f0:14:
                0d:c8:92:09:68:df:8f:69:fb:1c:49:91:d8:1c:f7:
                ee:67:a3:25:c5:9a:e2:f6:1c:a8:8c:af:7e:08:29:
                44:32:b1:d8:a9:86:04:a2:80:65:24:47:56:f4:fd:
                e4:19
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
Signature Algorithm: sha256WithRSAEncryption
     16:b8:e2:1e:45:13:56:9c:48:ef:ec:40:fb:9a:e3:4c:da:e4:
     95:c4:3b:92:10:9a:27:a0:da:ab:45:86:4c:39:fd:73:0c:e8:
     98:8b:0e:a4:28:72:66:0a:74:cc:9c:91:71:2f:94:dd:4b:4b:
     a2:54:e5:8f:47:82:bd:82:4d:70:93:6e:af:72:ce:cf:db:e2:
     36:b1:64:1a:1f:5e:c1:d9:57:12:15:5f:81:d3:ab:40:66:2a:
     3d:ab:d4:fb:24:a6:dd:1f:82:a2:33:9d:3d:da:a7:75:fa:0d:
     e6:be:1f:3b:a9:7f:d0:94:67:bf:e7:8b:19:32:5c:ea:0f:ae:
     3e:1e:41:55:06:c9:cb:42:b9:45:de:0e:d9:48:a5:75:90:5b:
     d7:89:ff:60:f2:31:ed:d7:52:0a:3d:91:87:c3:9a:85:76:8a:
     44:6f:c5:4e:9b:65:f6:78:cf:ee:7b:28:f5:10:c8:d1:39:3f:
     13:a7:96:f1:4b:11:5f:34:96:8f:13:b1:b6:de:9c:23:9e:f6:
     9d:b8:a3:f7:03:07:76:ce:bd:f6:76:1d:fc:5d:83:1e:8e:74:
     fb:78:b6:4a:ad:73:ce:e7:71:72:7d:0a:1e:49:5d:9e:65:30:
     aa:6f:b4:2f:9d:c3:e5:e6:38:de:0b:26:20:69:98:e4:6d:99:
     d2:15:ec:bd
```

Table 1-1Output Fields of the show web-server https certificate information Command

Field	Description
Certificate	Certificate information

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 show web-server status

Function

Run the **show web-server status** command to display the configuration and status of the Web service.

Syntax

show web-server status

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration and status of the Web service.

```
Hostname> enable
Hostname# show web-server status
http server status : enabled
http server port : 80
https server status: enabled
https server port: 443
http redirect to https: false
```

Table 1-1 Output Fields of the show web-server status Command

Field	Description
http server status	HTTP service status
http server port	HTTP service port
https server status	HTTPS service status
https server port	HTTPS service port
http redirect to https	Whether automatic HTTP redirection to HTTPS is enabled

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 webmaster level

Function

Run the **webmaster level** command to configure a username and a password for Web login and authentication.

Run the **no** form of this command to restore the default configuration.

The privilege level bound to a user is 0, username is **admin**, and plaintext password is **admin** by default.

Syntax

webmaster level *privilege-level* **username** *username* { **password** [**0** | **7**] *password* | **secret** [**0** | **8**] *secret* }

no webmaster level *privilege-level* [**username** *username*]

Parameter Description

privilege-level:-level: privilege level bound to a user.

username: Username.

0 | **7**: Specifies the encryption type of a password. The value **0** indicates no encryption and **7** indicates simple encryption. The default value is **0**.

password: User password. Enter the ciphertext when the encryption type is **7**; otherwise, enter the plaintext.

0 | **8**: Specifies the encryption type of a password. The value **0** indicates no encryption and **8** indicates encryption using the SHA-256 algorithm. The default value is **0**.

secret: User password. Enter the SHA-256 ciphertext when the encryption type is **8**; otherwise, enter the plaintext.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- After logging in to the Web server, you need to be authenticated before logging in to the Web page.
- This command is used to configure a username and a password for logging in to the Web page.

- The **no webmaster level** *privilege-level* command is run to delete all the usernames and passwords of the specified permission level.
- The **no webmaster level** *privilege-level* **username** *name* command is run to delete the specified username and password.
- Usernames and passwords involve three permission levels: Up to 10 usernames and passwords are configured for each permission level.
- The system creates account **admin** by default. The account cannot be deleted and only its password can be changed. The administrator account **admin** corresponds to the level 0 privilege. Account **admin** owns all the function privileges on the Web client and can edit other management accounts and authorize the accounts to access pages. New accounts correspond to the level 1 privilege.

Examples

The following example sets the privilege level bound to a user for logging in to the Web page to **0**, username to **Hostname**, and password to **admin**, and configures SHA-256 encryption.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# webmaster level 0 username Hostname secret admin
```

Notifications

When the default account **admin** is deleted, the following notification will be displayed:

```
%notice: Cannot cancel the default user configure!
```

When the number of configured usernames exceeds 10 at each permission level, the following notification will be displayed:

```
%notice: configure webmaster level %d server reached max 10, add failed.
```

When the configured username reaches or exceeds 32 characters, the following notification will be displayed:

```
%notice: Username too long. Please enter less than 32 characters.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 web-server http redirect-to-https

Function

Run the **web-server http redirect-to-https** command to configure automatic HTTP redirection to HTTPS.

Run the **no** form of this command to restore the default configuration.

Run the **default** form of this command to restore the default configuration.

Automatic HTTP redirection to HTTPS is disabled by default.

Syntax

web-server http redirect-to-https

no web-server http redirect-to-https

no web-server http redirect-to-https

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- When a user uses a browser to access the Web management system through HTTP upon configuration of HTTP redirection to HTTPS, the Web server address automatically redirects to HTTPS.
- The **no web-server http redirect-to-https** or **default web-server http redirect-to-https** command is used to disable automatic HTTP redirection to HTTPS.
- HTTP automatically redirects to HTTPS only when the HTTP and HTTPS services are enabled..
- If an IP address to be accessed is a Network Address Port Translation (NAPT) address, the redirection function may fail. In this case, to access the device through HTTP, disable the NAPT feature; to access the device through HTTPS, use HTTPS directly.

Examples

The following example configures HTTP redirection to HTTPS when a user accesses the Web page through HTTP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-server http redirect-to-https
```

Notifications

If the HTTPS service is not enabled when HTTP redirection to HTTPS is configured, the following notification will be displayed:

```
%notice: available unless https is enabled.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 web-server https certificate

Function

Run the **web-server https certificate** command to install an HTTPS certificate.

Run the **no** form of this command to restore the default configuration.

No HTTPS service certificate is installed by default.

Syntax

web-server https certificate { **pem** *cert-filename* **private-key** *key-filename* | **pfx** *cert-filename* } [**password** *password-text*]

no web-server https certificate

Parameter Description

pem: Imports the certificate file and private key file in the pem format.

pfx: Imports the certificate file in the pfx format from which a private key is exported.

Cert-filename:-filename: Name of the certificate file under the **flash:** drive.

Key-filename:-filename: Name of the private key file under the **flash:** drive.

password-text: Decryption password of the private key file or decryption password of the private key exported from the pfx certificate.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- Run the **copy** command to copy the certificate/private key file to the **flash:** partition before running the **web-server https certificate** command to install the HTTPS service certificate. After installation, you can delete the certificate/private key file from the **flash:** partition.
- You can run the **no web-server https certificate** command to remove the installed HTTPS service certificate. After deletion, the HTTPS service will use the self-signed certificate.
- This command is not displayed in the configuration.
- After the HTTPS service certificate is installed, the browser may require you to add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.

Examples

The following example configures the device to install the HTTP certificate: Install the certificate file **usercert.pfx** under the **flash:** partition. The password for exporting the certificate file is 123456.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-server https certificate pfx usercert.pfx password 123456
```

```
*Feb 28 14:38:37: %HTTPD-CERT_CHANGE: HTTPS certificate changed.
% The certificate was successfully installed.
```

Notifications

When the certificate is installed, the following notification will be displayed:

```
% The certificate was successfully installed.
```

When the size of the file name exceeds 64 bytes, the following notification will be displayed:

```
% Operation failed: filename too long, should be less than 64 bytes.
```

When the certificate fails to match the private key file, the following notification will be displayed:

```
% Operation failed: certificate does not matched with private key.
```

When the certificate file does not exist or is empty, the following notification will be displayed:

```
% Operation failed: certificate file not found or is empty.
```

When the private key file does not exist or is empty, the following notification will be displayed:

```
% Operation failed: private key file not found or is empty.
```

When the password is incorrect, the following notification will be displayed:

```
% Operation failed: please input correct password.
```

When an error is reported during parsing of the certificate file or private key file, the following notification will be displayed:

```
% Operation failed: verify file failed.
```

When the certificate is not installed but the certificate deletion command is run, the following notification will be displayed:

```
% Operation failed: no certificate installed.
```

When the certificate is deleted, the following notification will be displayed:

```
% The installed certificate was successfully deleted.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 web-server https generate self-signed-certificate

Function

Run the **web-server https generate self-signed-certificate** command to generate an HTTPS service self-signed certificate again.

The HTTPS service uses the self-signed certificate by default.

Syntax

web-server https generate self-signed-certificate

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

- This command is an interactive command. After running this command, enter the information to generate a self-signed certificate as prompted including the number of RSA key modulus digits and certificate username, or press **Ctrl+C** to cancel the operation.
- If the device is installed with a third-party HTTPS service certificate, the device uses the HTTPS certificate preferentially. The re-generated self-signed certificate does not replace the current HTTPS service certificate.
- When the **show running-config** command is run, this command is not displayed.
- After the HTTPS service certificate is generated again, the browser may require you add the trust certificate again before you continue access to the Web management page of the device. You are advised to open the Web management page again after closing the browser.

Examples

The following example generates an HTTPS service self-signed certificate again.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-server https generate self-signed-certificate
RSA key modulus bits (1024~4096) [2048]:
Common Name (e.g. server IP) [Self-Signed-600B16C2]:
% Generate self-signed certificate successfully.
```

Notifications

When the modulus length of the entered RSA key is not in the range from 1024 to 4096 or is not a number, the following notification will be displayed:

```
% Invalid number.
```

If you press **Ctrl+C** when an input prompt is displayed, the operation will be canceled and the following notification will be displayed:

```
% Operation cancelled.
```

When the length of the entered certificate username exceeds 64 bytes, the following notification will be displayed:

```
% Input too long, should not exceed 64 bytes.
```

When a self-signed certificate is generated, the following notification will be displayed:

```
% Generate self-signed certificate successfully.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A