

# Configure the HTTP/HTTPS Service Task on a WAP125 or WAP581 Access Point

## Objective

HyperText Transfer Protocol Secure (HTTPS) is a transfer protocol that is more secure than HTTP. The access point can be managed through both HTTP and HTTPS connections when the HTTP/HTTPS servers are configured. Some web browsers use HTTP while others use HTTPS. An access point must have a valid Secure Socket Layer (SSL) certificate to use HTTPS services.

### Why do we need to configure the HTTP/HTTPS Service Task?

This feature is useful to keep out rogue hosts from accessing the web-based utility. Using the Management Access Control List, it allows you to specify up to 10 IP addresses, five for IPv4 and five for IPv6 to have access to the web-based utility.

The objective of this document is to show you how to fortify your network by showing you how to configure the HTTP/HTTPS Service Task on the WAP125.

## Applicable Devices

- WAP125
- WAP581

## Software Version

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

## Gather the Support Information

Step 1. Log in to the web-based utility of your WAP. The default username and password is cisco/cisco.



## Wireless Access Point

A login form for a Cisco Wireless Access Point. It features a red rounded rectangular border. Inside, there are three input fields: the first contains the text "cisco", the second contains a masked password ".....|", and the third contains "English" with a dropdown arrow. Below these fields is a blue "Login" button.

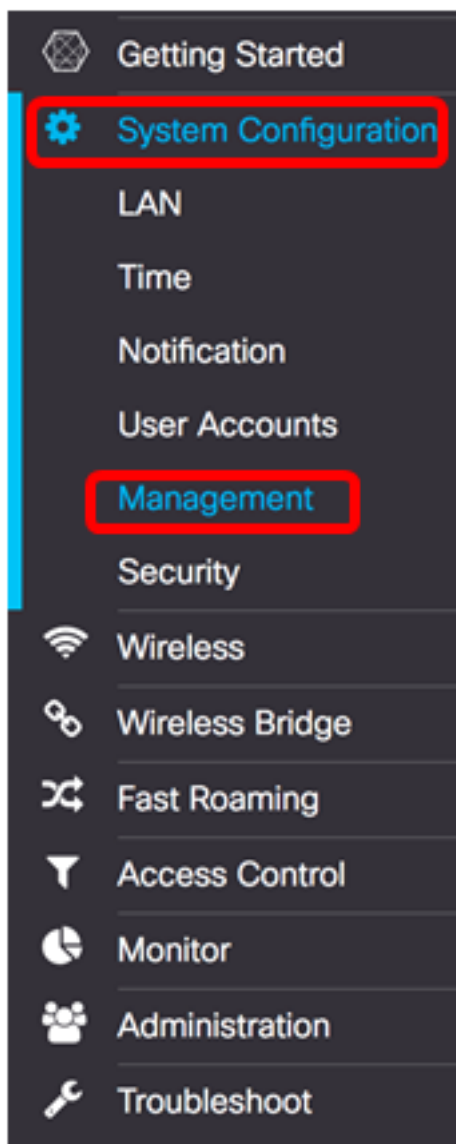
©2017 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

**Note:** If you already have changed the password or created a new account, enter your new credentials instead.

Step 2. Choose **System Configuration > Management**.

**Note:** The available options may vary depending on the exact model of your device. In this example, WAP125 is used.



Step 3. In the *Maximum Sessions* field under Connect Session Settings, enter a value from 1 to 10 to set the maximum number of simultaneous web sessions. A session is created each time a user logs on to the device. If the maximum session is reached then the next user who attempts to log on into the device with HTTP or HTTPS service is rejected. The default is 5.

### Connect Session Settings

Maximum Sessions:

Session Timeout:  Min.

### HTTP/HTTPS Service

HTTP Service:  Enable [More...](#)

HTTPS Service:  Enable [More...](#)

Management ACL Mode:  Enable [More...](#)

Step 4. In the *Session Timeout* field, enter a value between 2 and 60 minutes to set the time the web session can remain idle. The default value is 10 minutes.

**Note:** In this example, 13 is used.

### Connect Session Settings

Maximum Sessions:

Session Timeout:  Min.

### HTTP/HTTPS Service

HTTP Service:  Enable [More...](#)

HTTPS Service:  Enable [More...](#)

Management ACL Mode:  Enable [More...](#)

#### HTTP Service

Step 5. Check the **Enable** HTTP Service check box to allow web sessions to be connected through HTTP.

### Connect Session Settings

Maximum Sessions:  ?

Session Timeout:  ? Min.

### HTTP/HTTPS Service

HTTP Service:  Enable [More...](#)

HTTPS Service:  Enable [More...](#)

Management ACL Mode:  Enable [More...](#)

Step 6. (Optional) Click **More** to view more options and configure a port number.

### Connect Session Settings

Maximum Sessions:  ?

Session Timeout:  ? Min.

### HTTP/HTTPS Service

HTTP Service:  Enable [More...](#)

HTTPS Service:  Enable [More...](#)

Management ACL Mode:  Enable [More...](#)

Step 7. In the *HTTP Port* field, enter a logical port number to use for HTTP connections. The port value ranges from 1025 to 65535. The default well-known port for HTTP connections is 80.

## HTTP Port

---

HTTP Port: 

80

Redirect HTTP to HTTPS:



OK

cancel

Step 8. (Optional) Check the **Redirect HTTP to HTTPS** check box to allow the browser to redirect you to a more secure protocol, HTTPS upon establishing a web session.

**Note:** This option is only available if HTTP Service check box is disabled in Step 4. In this example, this option is checked.

## HTTP Port

---

HTTP Port: 

80

Redirect HTTP to HTTPS:



OK

cancel

Step 9. Click **OK** to return to the Management page and continue with the configuration.

## HTTP Port

HTTP Port: 

Redirect HTTP to HTTPS:



OK

cancel

## HTTPS Service

Step 10. Check the **Enable** HTTPS Service check box to allow web sessions to be established through a secured protocol, HTTPS. This option is enabled by default.

**Note:** If this option is disabled, any existing connections using the HTTPS are disconnected.

### Connect Session Settings

Maximum Sessions: 

Session Timeout: 

Min.

### HTTP/HTTPS Service

HTTP Service:

Enable

More...

HTTPS Service:

Enable

More...

Management ACL Mode:  Enable

More...

Step 11. Click **More** to define a port to be used by HTTPS and to choose Transport Layer Security Versions to be used on HTTPS.

## Connect Session Settings

Maximum Sessions: ?

Session Timeout: ?

Min.

## HTTP/HTTPS Service

HTTP Service:  Enable

More...

HTTPS Service:  Enable

More...

Management ACL Mode:  Enable

More...

Step 12. Under the HTTPS Port area, check the check boxes of the following security protocols that are used over HTTPS:

- TLSv1.0 — Transport Layer Security version 1 (TLSv1) is a cryptographic protocol that provides security and data integrity for communication over the Internet.
- TLSv1.1 — An improved version of the first version of the TSLv1, improves the data security and integrity for communication.
- SSLv3 — Secured Socket Layer version 3 (SSLv3) is a protocol that is used over HTTPS to establish secured sessions and communication over the Internet.

**Note:** In this example, all check boxes are checked.

## HTTPS Port

TLSv1.0  TLSv1.1  SSLv3

HTTPS Port : ?

OK

cancel

Step 13. In the *HTTPS Port* field, enter a logical port number to use for HTTPS connections. The default well-known port is 443.



## HTTPS Port

---

TLSv1.0     TLSv1.1     SSLv3

HTTPS Port : 

OK

cancel

Step 14. Click **OK** to continue.

## HTTPS Port

---

TLSv1.0     TLSv1.1     SSLv3

HTTPS Port : 

OK

cancel

### Management ACL Mode

Step 15. Check the **Enable** ACL Mode check box to specify an Access Control List (ACL) of IP addresses that are permitted to access the web-based utility. If this feature is disabled, then this grants access to the web-based utility.

## Connect Session Settings

Maximum Sessions: 

Session Timeout:   Min.

## HTTP/HTTPS Service

HTTP Service:  Enable [More...](#)

HTTPS Service:  Enable [More...](#)

Management ACL Mode:  Enable [More...](#)

Step 16. Click **More** to specify a list of IPv4 and IPv6 addresses permitted to access the web-based utility.

## Connect Session Settings

Maximum Sessions: 

Session Timeout:   Min.

## HTTP/HTTPS Service

HTTP Service:  Enable [More...](#)

HTTPS Service:  Enable [More...](#)

Management ACL Mode:  Enable [More...](#)

Step 17. In the *IPv4 Address* and *IPv6 Address* fields, enter the administrative IP addresses in the respective formats that will be granted access to the web-based utility.

**Tip:** Assign static IP addresses to the administrative IP addresses.

**Note:** In this example, 192.168.2.123 is used as the IPv4 administrative address and fdad:b197:cb72:0000:0000:0000:0000:0000 is used as the IPv6 administrative address.

# Management Access Control

IPv4 Address 1: ? 192.168.2.123

IPv4 Address 2: ?

IPv4 Address 3: ?

IPv4 Address 4: ?

IPv4 Address 5: ?

IPv6 Address 1: ? fdad:b197:cb72:0000:0000:0000:0000

IPv6 Address 2: ?

IPv6 Address 3: ?

IPv6 Address 4: ?


IPv6 Address 5: ?


OK cancel


Step 18. Click **OK**.


## Management Access Control


---


IPv4 Address 1: 


IPv4 Address 2: 


IPv4 Address 3: 


IPv4 Address 4: 


IPv4 Address 5: 

IPv6 Address 1: 

IPv6 Address 2: 

IPv6 Address 3: 

IPv6 Address 4: 

IPv6 Address 5: 

---

Step 19. Click **Save** button to save the configured settings.

## Management

Save

### Connect Session Settings

Maximum Sessions:

Session Timeout:  Min

### HTTP/HTTPS Service

HTTP Service:  Enable [More...](#)

HTTPS Service:  Enable [More...](#)

Management ACL Mode:  Enable [More...](#)

You should now have successfully configured the HTTP/HTTPS Service Task on your WAP125 or WAP581 access point.