

# Konfigurieren der HTTP/HTTPS-Dienstaufgabe auf einem WAP125 oder WAP581 Access Point

## Ziel

HyperText Transfer Protocol Secure (HTTPS) ist ein Übertragungsprotokoll, das sicherer ist als HTTP. Der Access Point kann sowohl über HTTP- als auch über HTTPS-Verbindungen verwaltet werden, wenn die HTTP-/HTTPS-Server konfiguriert sind. Einige Webbrowser verwenden HTTP, während andere HTTPS verwenden. Ein Access Point muss über ein gültiges SSL-Zertifikat (Secure Socket Layer) verfügen, um HTTPS-Dienste verwenden zu können.

## Warum müssen wir die HTTP/HTTPS-Dienstaufgabe konfigurieren?

Diese Funktion ist hilfreich, um nicht autorisierte Hosts vom Zugriff auf das webbasierte Dienstprogramm abzuhalten. Mithilfe der Verwaltungszugriffskontrollliste können Sie bis zu 10 IP-Adressen, fünf für IPv4 und fünf für IPv6 für den Zugriff auf das webbasierte Dienstprogramm angeben.

In diesem Dokument wird erläutert, wie Sie Ihr Netzwerk stärken können, indem Sie zeigen, wie Sie die HTTP/HTTPS-Dienstaufgabe auf dem WAP125 konfigurieren.

## Anwendbare Geräte

- WAP125
- WAP581

## Softwareversion

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

## Sammeln der Support-Informationen

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm Ihres WAP an. Der Standard-Benutzername und das Kennwort lautet `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 is a dropdown menu currently showing "English". Below these fields is a blue "Login" button.

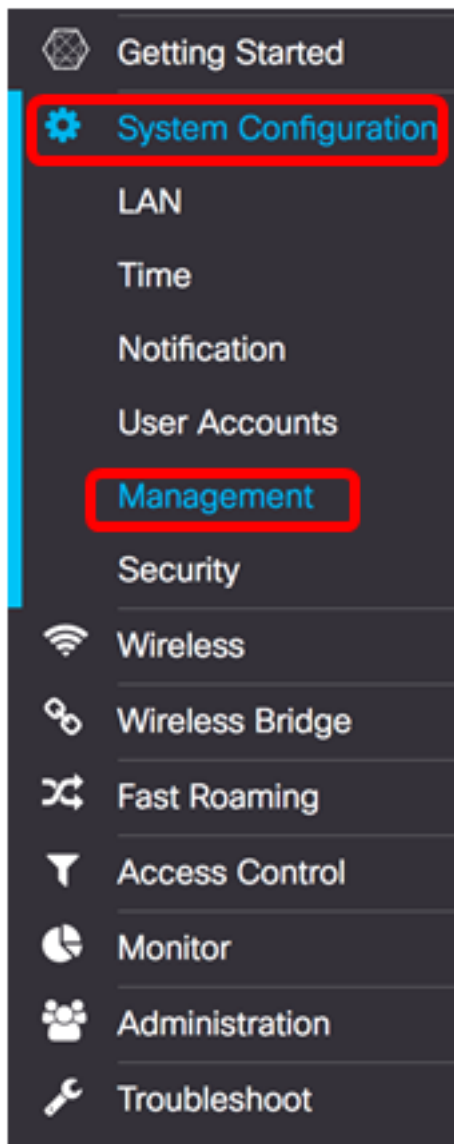
©2017 Cisco Systems, Inc. All Rights Reserved.

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.

**Hinweis:** Wenn Sie das Kennwort bereits geändert oder ein neues Konto erstellt haben, geben Sie stattdessen Ihre neuen Anmeldeinformationen ein.

Schritt 2: Wählen Sie **Systemkonfiguration > Management aus**.

**Hinweis:** Die verfügbaren Optionen können je nach Gerät variieren. In diesem Beispiel wird WAP125 verwendet.



Schritt 3: Geben Sie im Feld *Maximale Sitzungen* unter Sitzungseinstellungen verbinden einen Wert zwischen 1 und 10 ein, um die maximale Anzahl gleichzeitiger Websitzungen festzulegen. Bei jeder Anmeldung eines Benutzers am Gerät wird eine Sitzung erstellt. Wenn die maximale Sitzung erreicht ist, wird der nächste Benutzer, der versucht, sich mit dem HTTP- oder HTTPS-Dienst am Gerät anzumelden, abgelehnt. Der Standardwert ist 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...](#)

Schritt 4: Geben Sie im Feld *Session Timeout* (Sitzungszeitüberschreitung) einen Wert zwischen 2 und 60 Minuten ein, um die Zeit festzulegen, in der die Websitzung inaktiv bleiben kann. Der Standardwert ist 10 Minuten.

**Hinweis:** In diesem Beispiel wird 13 verwendet.

### 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

Schritt 5: Aktivieren Sie das Kontrollkästchen **HTTP-Dienst aktivieren**, um die Verbindung von Websitzungen über HTTP zuzulassen.

## Connect Session Settings

Maximum Sessions: 

Session Timeout: 

Min.

## HTTP/HTTPS Service

HTTP Service:

Enable

More...

HTTPS Service:

Enable

More...

Management ACL Mode:  Enable

More...

Schritt 6: (Optional) Klicken Sie auf **More** (Mehr), um weitere Optionen anzuzeigen und eine Portnummer zu konfigurieren.

## Connect Session Settings

Maximum Sessions: 

Session Timeout: 

Min.

## HTTP/HTTPS Service

HTTP Service:

Enable

More...

HTTPS Service:

Enable

More...

Management ACL Mode:  Enable

More...

Schritt 7: Geben Sie im Feld *HTTP-Port* eine logische Portnummer für HTTP-Verbindungen ein. Der Port-Wert liegt zwischen 1025 und 65535. Der allgemein bekannte Standard-Port für HTTP-Verbindungen ist 80.

## HTTP Port

---

HTTP Port: 

80

Redirect HTTP to HTTPS:



OK

cancel

Schritt 8: (Optional) Aktivieren Sie das Kontrollkästchen **HTTP zu HTTPS umleiten**, damit der Browser Sie beim Einrichten einer Websitzung zu einem sichereren Protokoll umleiten kann.

**Hinweis:** Diese Option ist nur verfügbar, wenn das Kontrollkästchen HTTP-Service in Schritt 4 deaktiviert ist. In diesem Beispiel ist diese Option aktiviert.

## HTTP Port

---

HTTP Port: 

80

Redirect HTTP to HTTPS:



OK

cancel

Schritt 9: Klicken Sie auf **OK**, um zur Seite "Verwaltung" zurückzukehren und mit der Konfiguration fortzufahren.

## HTTP Port

HTTP Port: 

Redirect HTTP to HTTPS:



## HTTPS-Service

Schritt 10: Aktivieren Sie das Kontrollkästchen **Enable** HTTPS Service (HTTPS-Dienst **aktivieren**), um die Einrichtung von Websitzungen über das sichere Protokoll HTTPS zu ermöglichen. Diese Option ist standardmäßig aktiviert.

**Hinweis:** Wenn diese Option deaktiviert ist, werden alle vorhandenen HTTPS-Verbindungen getrennt.

## Connect Session Settings

Maximum Sessions: 

Session Timeout: 

Min.

## HTTP/HTTPS Service

HTTP Service:

 Enable

HTTPS Service:

 Enable

Management ACL Mode:  Enable

Schritt 11: Klicken Sie auf **More** (Mehr), um einen Port für HTTPS festzulegen und für HTTPS die für HTTPS zu verwendenden Transportschichtversionsnummern auszuwählen.

## Connect Session Settings

Maximum Sessions: ?

Session Timeout: ?

Min.

## HTTP/HTTPS Service

HTTP Service:  Enable

More...

HTTPS Service:  Enable

More...

Management ACL Mode:  Enable

More...

Schritt 12: Aktivieren Sie im Bereich HTTPS-Port die Kontrollkästchen der folgenden Sicherheitsprotokolle, die über HTTPS verwendet werden:

- TLSv1.0 - Transport Layer Security Version 1 (TLSv1) ist ein Verschlüsselungsprotokoll, das Sicherheit und Datenintegrität für die Kommunikation über das Internet bietet.
- TLSv1.1 - Eine verbesserte Version der ersten Version des TLSv1 verbessert die Datensicherheit und -integrität für die Kommunikation.
- SSLv3 - Secure Socket Layer Version 3 (SSLv3) ist ein Protokoll, das über HTTPS sichere Sitzungen und die Kommunikation über das Internet herstellt.

**Hinweis:** In diesem Beispiel sind alle Kontrollkästchen aktiviert.

## HTTPS Port

TLSv1.0  TLSv1.1  SSLv3

HTTPS Port : ?

OK

cancel

Schritt 13: Geben Sie im Feld *HTTPS-Port* eine logische Portnummer für HTTPS-Verbindungen ein. Der allgemein bekannte Standard-Port ist 443.



## HTTPS Port

---

TLSv1.0     TLSv1.1     SSLv3

HTTPS Port : 

OK

cancel

Schritt 14: Klicken Sie auf **OK**, um fortzufahren.

## HTTPS Port

---

TLSv1.0     TLSv1.1     SSLv3

HTTPS Port : 

OK

cancel

## Management-ACL-Modus

Schritt 15: Aktivieren Sie das Kontrollkästchen **Enable ACL Mode** (ACL-Modus **aktivieren**), um eine Zugriffskontrollliste (ACL) für IP-Adressen anzugeben, die für den Zugriff auf das webbasierte Dienstprogramm zulässig sind. Wenn diese Funktion deaktiviert ist, wird dem webbasierten Dienstprogramm Zugriff gewährt.

## Connect Session Settings

Maximum Sessions: 

Session Timeout:   Min.

## HTTP/HTTPS Service

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

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

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

Schritt 16: Klicken Sie auf **More (Mehr)**, um eine Liste der IPv4- und IPv6-Adressen anzugeben, die für den Zugriff auf das webbasierte Dienstprogramm zulässig sind.

## Connect Session Settings

Maximum Sessions: 

Session Timeout:   Min.

## HTTP/HTTPS Service

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

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

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

Schritt 17: Geben Sie in die Felder *IPv4-Adresse* und *IPv6-Adresse* die administrativen IP-Adressen in den entsprechenden Formaten ein, die Zugriff auf das webbasierte Dienstprogramm erhalten.

**Tipp:** Weisen Sie den administrativen IP-Adressen statische IP-Adressen zu.

**Hinweis:** In diesem Beispiel wird 192.168.2.123 als IPv4-Administrationsadresse und fdad:b197:cb72:0000:0000:0000:0000:0000 als IPv6-Administrator verwendet. Adresse.

## 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


Schritt 18: Klicken Sie auf **OK**.


## 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: 

---

Schritt 19: Klicken Sie auf die Schaltfläche **Speichern**, um die konfigurierten Einstellungen zu speichern.

## 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...](#)

Sie sollten jetzt die HTTP/HTTPS-Dienstaufgabe auf Ihrem WAP125- oder WAP581-Access Point erfolgreich konfiguriert haben.