

# Configurare l'attività Servizio HTTP/HTTPS su un access point WAP125 o WAP581

## Obiettivo

HyperText Transfer Protocol Secure (HTTPS) è un protocollo di trasferimento più sicuro di HTTP. Il punto di accesso può essere gestito tramite connessioni HTTP e HTTPS quando i server HTTP/HTTPS sono configurati. Alcuni browser Web utilizzano HTTP mentre altri utilizzano HTTPS. Per utilizzare i servizi HTTPS, un punto di accesso deve disporre di un certificato SSL (Secure Sockets Layer) valido.

### Perché è necessario configurare l'attività servizio HTTP/HTTPS?

Questa funzione è utile per impedire agli host non autorizzati di accedere all'utility basata sul Web. Utilizzando l'elenco di controllo di accesso di gestione, è possibile specificare fino a 10 indirizzi IP, cinque per IPv4 e cinque per IPv6 per accedere all'utility basata sul Web.

L'obiettivo di questo documento è mostrare come fortificare la rete mostrando come configurare l'attività di servizio HTTP/HTTPS su WAP125.

## Dispositivi interessati

- WAP125
- WAP581

## Versione del software

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

## Raccolta delle informazioni sul supporto

Passaggio 1. Accedere all'utilità basata sul Web di WAP. Il nome utente e la password predefiniti sono 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.

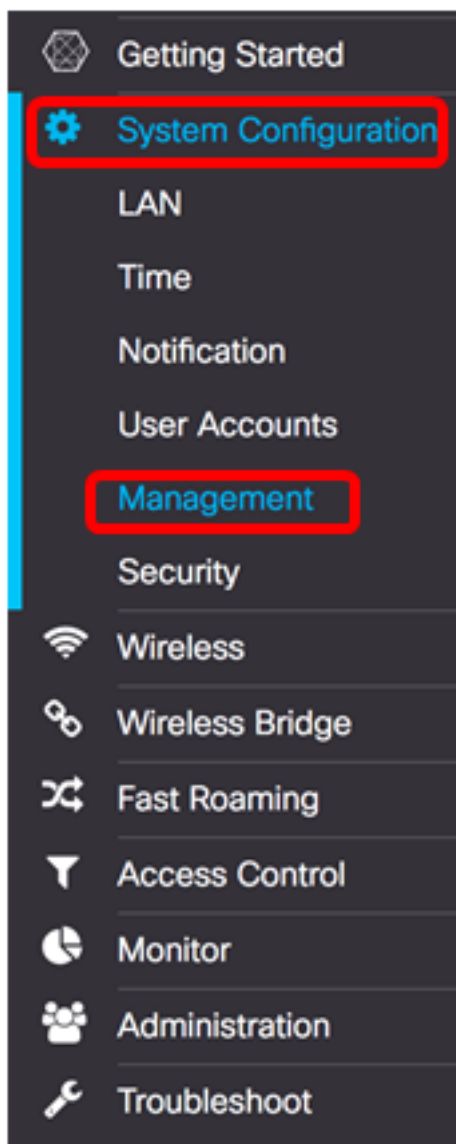
©2017 Cisco Systems, Inc. All Rights Reserved.

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.

**Nota:** Se la password è già stata modificata o è stato creato un nuovo account, immettere le nuove credenziali.

Passaggio 2. Scegliere **Configurazione di sistema > Gestione**.

**Nota:** Le opzioni disponibili possono variare a seconda del modello esatto del dispositivo. Nell'esempio viene utilizzato WAP125.



Passaggio 3. Nel campo *Maximum Sessions* in *Connect Session Settings*, immettere un valore da 1 a 10 per impostare il numero massimo di sessioni Web simultanee. Ogni volta che un utente accede al dispositivo viene creata una sessione. Se viene raggiunta la sessione massima, l'utente successivo che tenta di accedere al dispositivo con il servizio HTTP o HTTPS viene rifiutato. Il valore predefinito è 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...](#)

Passaggio 4. Nel campo *Timeout sessione*, immettere un valore compreso tra 2 e 60 minuti per impostare il tempo di inattività della sessione Web. Il valore predefinito è 10 minuti.

**Nota:** nell'esempio viene utilizzato 13.

### Connect Session Settings

Maximum Sessions:

Session Timeout:  Min.

### HTTP/HTTPS Service

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

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

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

#### Servizio HTTP

Passaggio 5. Selezionare la casella di controllo **Abilita** servizio HTTP per consentire la connessione delle sessioni Web tramite 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...](#)

Passaggio 6. (Facoltativo) Fare clic su **More** per visualizzare altre opzioni e configurare un numero di porta.

### Connect Session Settings

Maximum Sessions: ?

Session Timeout: ?  Min.

### HTTP/HTTPS Service

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

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

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

Passaggio 7. Nel campo *Porta HTTP*, immettere un numero di porta logica da utilizzare per le connessioni HTTP. Il valore della porta è compreso tra 1025 e 65535. Il valore predefinito della porta conosciuta per le connessioni HTTP è 80.

## HTTP Port

---

HTTP Port: 

80

Redirect HTTP to HTTPS:



OK

cancel

Passaggio 8. (Facoltativo) Selezionare la casella di controllo **Reindirizza HTTP a HTTPS** per consentire al browser di reindirizzare l'utente a un protocollo più sicuro, HTTPS, quando viene stabilita una sessione Web.

**Nota:** Questa opzione è disponibile solo se la casella di controllo Servizio HTTP è disattivata nel passaggio 4. In questo esempio, questa opzione è selezionata.

## HTTP Port

---

HTTP Port: 

80

Redirect HTTP to HTTPS:



OK

cancel

Passaggio 9. Fare clic su **OK** per tornare alla pagina Gestione e continuare con la configurazione.

## HTTP Port

HTTP Port: 

Redirect HTTP to HTTPS:



## Servizio HTTPS

Passaggio 10. Selezionare la casella di controllo **Abilita** servizio HTTPS per consentire la creazione di sessioni Web tramite un protocollo protetto, HTTPS. Questa opzione è attivata per default.

**Nota:** Se questa opzione è disattivata, tutte le connessioni esistenti che utilizzano HTTPS verranno disconnesse.

## Connect Session Settings

Maximum Sessions: 

Session Timeout: 

Min.

## HTTP/HTTPS Service

HTTP Service:



Enable

HTTPS Service:



Enable

Management ACL Mode:  Enable

Passaggio 11. Fare clic su **More** per definire una porta che deve essere utilizzata da HTTPS e per scegliere le versioni di Transport Layer Security da utilizzare su 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...

Passaggio 12. Nell'area Porta HTTPS, selezionare le caselle di controllo dei seguenti protocolli di sicurezza utilizzati su HTTPS:

- TLSv1.0 — Transport Layer Security versione 1 (TLSv1) è un protocollo crittografico che fornisce sicurezza e integrità dei dati per la comunicazione su Internet.
- TLSv1.1: una versione migliorata della prima versione di TSLv1, migliora la sicurezza e l'integrità dei dati per la comunicazione.
- SSLv3 — Secure Sockets Layer versione 3 (SSLv3) è un protocollo utilizzato su HTTPS per stabilire sessioni protette e comunicazioni su Internet.

**Nota:** In questo esempio, tutte le caselle di controllo sono selezionate.

## HTTPS Port

TLSv1.0

TLSv1.1

SSLv3

HTTPS Port : ?

OK

cancel

Passaggio 13. Nel campo *Porta HTTPS*, immettere un numero di porta logica da utilizzare per le connessioni HTTPS. La porta conosciuta predefinita è 443.



## HTTPS Port

---

TLSv1.0     TLSv1.1     SSLv3

HTTPS Port : 

OK

cancel

Passaggio 14. Fare clic su **OK** per continuare.

## HTTPS Port

---

TLSv1.0     TLSv1.1     SSLv3

HTTPS Port : 

OK

cancel

### Modalità ACL di gestione

Passaggio 15. Selezionare la casella di controllo **Abilita** modalità ACL per specificare un elenco di controllo di accesso (ACL) di indirizzi IP a cui è consentito accedere all'utility basata sul Web. Se questa funzione è disattivata, viene concesso l'accesso all'utility basata sul Web.

## Connect Session Settings

Maximum Sessions: 

Session Timeout: 

Min.

## HTTP/HTTPS Service

HTTP Service:  Enable

More...

HTTPS Service:  Enable

More...

Management ACL Mode:  Enable

More...

Passaggio 16. Fare clic su **Altro** per specificare un elenco di indirizzi IPv4 e IPv6 autorizzati ad accedere all'utility basata sul Web.

## Connect Session Settings

Maximum Sessions: 

Session Timeout: 

Min.

## HTTP/HTTPS Service

HTTP Service:  Enable

More...

HTTPS Service:  Enable

More...

Management ACL Mode:  Enable

More...

Passaggio 17. Nei campi *Indirizzo IPv4* e *Indirizzo IPv6*, immettere gli indirizzi IP amministrativi nei rispettivi formati a cui verrà concesso l'accesso all'utility basata sul Web.

**Suggerimento:** Assegnare indirizzi IP statici agli indirizzi IP amministrativi.

**Nota:** Nell'esempio, 192.168.2.123 viene usato come indirizzo amministrativo IPv4 e fdad:b197:cb72:0000:0000:0000:0000:0000 viene usato come indirizzo amministrativo IPv6.

## 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


Passaggio 18. Fare clic su 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: 

---

Passaggio 19. Fare clic su **Salva** per salvare le impostazioni configurate.

## 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...](#)

A questo punto è necessario aver configurato correttamente l'attività del servizio HTTP/HTTPS sul punto di accesso WAP125 o WAP581.