

在WAP125或WAP581接入點上配置HTTP/HTTPS服務任務

目標

超文本傳輸協定安全(HTTPS)是一種比HTTP更安全的傳輸協定。配置HTTP/HTTPS伺服器時，可以通過HTTP和HTTPS連線管理接入點。某些Web瀏覽器使用HTTP，而其它瀏覽器使用HTTPS。存取點必須具有有效的安全通訊端層(SSL)憑證才能使用HTTPS服務。

為什麼需要配置HTTP/HTTPS服務任務？

此功能對於阻止惡意主機訪問基於Web的實用程式非常有用。使用管理訪問控制清單，您可以指定最多10個IP地址，5個用於IPv4,5個用於IPv6以訪問基於Web的實用程式。

本文檔旨在向您展示如何在WAP125上配置HTTP/HTTPS服務任務，從而向您展示如何強化您的網路。

適用裝置

- WAP125
- WAP581

軟體版本

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

收集支援資訊

步驟1.登入到WAP的基於Web的實用程式。預設使用者名稱和密碼為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 the text "English" with a downward arrow indicating a dropdown menu. Below these fields is a blue button with the text "Login" in white.

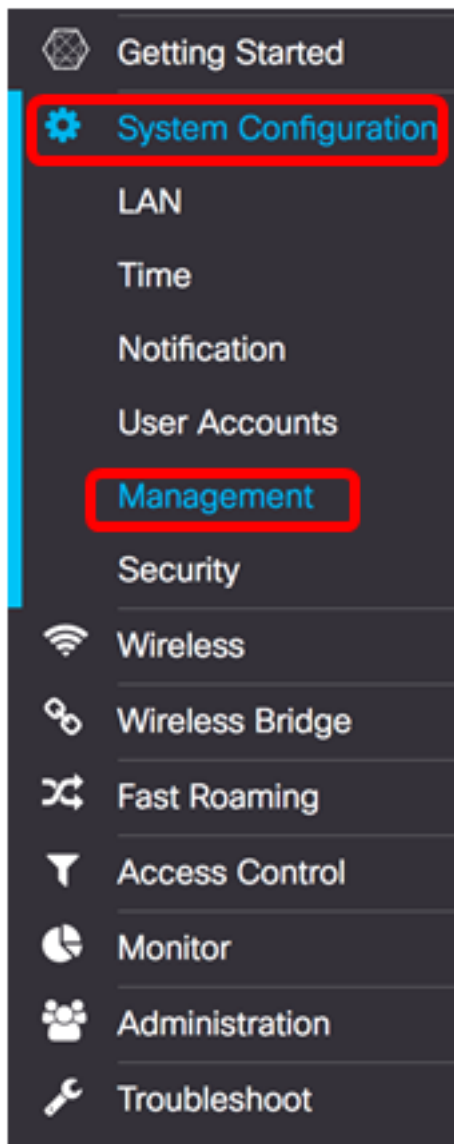
©2017 Cisco Systems, Inc. All Rights Reserved.

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.

附註：如果您已更改密碼或建立新帳戶，請輸入您的新憑據。

步驟2.選擇System Configuration > Management。

附註：可用選項可能會因裝置的具體型號而異。本示例使用WAP125。



步驟3. 在Connect Session Settings底下的*Maximum Sessions*欄位中，輸入介於1到10之間的值，以設定同時進行Web作業階段的最大數量。每次使用者登入到裝置時都會建立會話。如果達到最大會話數，則拒絕嘗試使用HTTP或HTTPS服務登入裝置的下一個使用者。預設值為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...](#)

步驟4.在 *Session Timeout* 欄位中，輸入介於2到60分鐘之間的值，以設定Web作業階段可以保持空閒的時間。預設值為10分鐘。

附註：在此示例中，使用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...](#)

HTTP服務

步驟5.選中 **Enable** HTTP Service 覈取方塊以允許通過HTTP連線Web會話。

Connect Session Settings

Maximum Sessions: ?

Session Timeout: ? Min.

HTTP/HTTPS Service

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

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

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

步驟6。(可選) 按一下 **More** 檢視更多選項並配置埠號。

Connect Session Settings

Maximum Sessions: ?

Session Timeout: ? Min.

HTTP/HTTPS Service

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

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

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

步驟7. 在 *HTTP Port* 欄位中，輸入用於HTTP連線的邏輯埠號。埠值範圍為1025到65535。HTTP連線的預設公認埠為80。

HTTP Port

HTTP Port: 

80

Redirect HTTP to HTTPS:



OK

cancel

步驟8. (可選) 勾選**Redirect HTTP to HTTPS**覈取方塊以允許瀏覽器在建立Web作業階段時將您重新導向到更安全的通訊協定HTTPS。

附註：僅當步驟4中禁用了HTTP服務覈取方塊時，此選項才可用。在此示例中，選中此選項。

HTTP Port

HTTP Port: 

80

Redirect HTTP to HTTPS:



OK

cancel

步驟9. 按一下**OK**以返回Management頁面並繼續設定。

HTTP Port

HTTP Port: 

Redirect HTTP to HTTPS:





HTTPS服務

步驟10.選中**Enable** HTTPS Service 覆取方塊以允許通過安全協定HTTPS建立Web會話。預設情況下啟用此選項。

附註：如果禁用此選項，則使用HTTPS的所有現有連線都將斷開。

Connect Session Settings

Maximum Sessions: 

Session Timeout:  Min.

HTTP/HTTPS Service

HTTP Service:	<input checked="" type="checkbox"/> Enable	<input type="button" value="More..."/>
HTTPS Service:	<input checked="" type="checkbox"/> Enable	<input type="button" value="More..."/>
Management ACL Mode:	<input type="checkbox"/> Enable	<input type="button" value="More..."/>

步驟11.按一下**More**以定義供HTTPS使用的連線埠，並選擇要用於HTTPS的傳輸層安全版本。

Connect Session Settings

Maximum Sessions: 

Session Timeout: 

Min.

HTTP/HTTPS Service

HTTP Service: Enable

More...

HTTPS Service: Enable

More...

Management ACL Mode: Enable

More...

步驟12.在HTTPS埠區域下，選中通過HTTPS使用的以下安全協定的覈取方塊：

- TLSv1.0 — 傳輸層安全第1版(TLSv1)是一個加密協定，它為Internet上的通訊提供安全性和資料完整性。
- TLSv1.1 — 改進版本的TSLv1提高了資料安全和通訊完整性。
- SSLv3 — 安全通訊端第3層版本(SSLv3)是透過HTTPS使用以透過Internet建立安全作業階段和通訊的通訊協定。

附註：在此示例中，所有覈取方塊均處於選中狀態。

HTTPS Port

TLSv1.0 TLSv1.1 SSLv3

HTTPS Port: 

OK

cancel

步驟13.在「*HTTPS Port*」欄位中，輸入用於HTTPS連線的邏輯連線埠號碼。預設公認埠為443。

HTTPS Port

TLSv1.0 TLSv1.1 SSLv3

HTTPS Port : 

OK

cancel

步驟14.按一下OK以繼續。

HTTPS Port

TLSv1.0 TLSv1.1 SSLv3

HTTPS Port : 

OK

cancel

管理ACL模式

步驟15.選中**Enable ACL Mode**釐取方塊以指定允許訪問基於Web的實用程式的IP地址的訪問控制清單(ACL)。如果禁用此功能，則此操作將授予對基於Web的實用程式的訪問許可權。

Connect Session Settings

Maximum Sessions: ?

Session Timeout: ?

Min.

HTTP/HTTPS Service

HTTP Service: Enable

More...

HTTPS Service: Enable

More...

Management ACL Mode: Enable

More...

步驟16. 按一下**More**以指定允許訪問基於Web的實用程式的IPv4和IPv6地址清單。

Connect Session Settings

Maximum Sessions: ?

Session Timeout: ?

Min.

HTTP/HTTPS Service

HTTP Service: Enable

More...

HTTPS Service: Enable

More...

Management ACL Mode: Enable

More...

步驟17. 在*IPv4 Address*和*IPv6 Address*欄位中，以相應的格式輸入將授予對基於Web的實用程式的訪問許可權的管理IP地址。

提示：將靜態IP地址分配給管理IP地址。

附註：在本示例中，192.168.2.123用作IPv4管理地址，fdad:b197:cb72:0000:0000:0000:0000:0000用作IPv6管理地址。

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


步驟18. 按一下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: 

OK

cancel

步驟19. 按一下 **Save** 按鈕以儲存已設定的設定。

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...](#)

現在，您應該已經在WAP125或WAP581接入點上成功配置HTTP/HTTPS服務任務。