為自治AP上的訪客配置Web身份驗證

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[AP配置](#)
[配置無線客戶端](#)
[驗證](#)
[疑難排解](#)
[自訂](#)

簡介

本檔案介紹如何使用內嵌於AP本身的內部網頁在自主存取點(AP)上設定訪客存取。

必要條件

需求

思科建議您在嘗試此設定之前瞭解以下主題：

- 如何為基本操作配置自治AP
- 如何在自治AP上配置本地RADIUS伺服器
- 作為第3層安全措施的Web身份驗證的工作原理

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行Cisco IOS®映像15.2(4)JA1的AIR-CAP3502I-E-K9
- Intel Centrino Advanced-N 6200 AGN無線介面卡（驅動程式13.4.0.9版）
- Microsoft Windows 7請求方實用程式

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

Web驗證是第3層(L3)安全功能，可讓自治AP封鎖IP流量(DHCP和網域名稱伺服器(DNS)相關封包除外)，直到訪客在開啟瀏覽器時，使用者端重新導向到的Web輸入網站中提供有效的使用者名稱和密碼。

使用Web身份驗證時，必須為每個訪客定義單獨的使用者名稱和密碼。訪客由本地RADIUS伺服器或外部RADIUS伺服器以使用者名稱和密碼進行驗證。

此功能是在Cisco IOS版本15.2(4)JA1中導入。

AP配置

注意：本文檔假設AP上的網橋虛擬介面(BVI) 1的IP地址為192.168.10.2 /24，並且DHCP池在AP內部定義為IP地址192 2.168.10.10到192.168.10.254（192.168.10.1到192.168.10.10的IP地址除外）。

完成以下步驟，為訪客接入配置AP：

1. 增加新的服務集識別符號(SSID)（區分大小寫），將其命名為Guest，並為Web身份驗證進行配置：

```
<#root>

ap(config)#

dot11 ssid Guest


ap(config-ssid)#

authentication open


ap(config-ssid)#

web-auth


ap(config-ssid)#

guest-mode


ap(config-ssid)#
```

```
exit
```

2. 建立身份驗證規則，您必須在其中指定代理身份驗證協定，並將其命名為web_auth：

```
<#root>

ap(config)#

ip admission name web_auth proxy http
```

3. 將SSID (Guest)和驗證規則(web_auth)應用於無線電介面。此範例使用802.11b/g無線電：

```
<#root>

ap(config)#

interface dot11radio 0


ap(config-if)#

ssid Guest


ap(config-if)#

ip admission web_auth


ap(confi-if)#

no shut


ap(config-if)#

exit
```

4. 定義方法清單，指定驗證使用者身份證明的位置。將方法清單名稱與web_auth身份驗證規則連結，並將其命名為web_list：

```
<#root>

ap(config)#

ip admission name web_auth method-list authentication web_list
```

5. 完成以下步驟，以便在AP和本地RADIUS伺服器上配置身份驗證、授權和記帳(AAA)，並將方法清單與AP上的本地RADIUS伺服器連結：

A. 啟用AAA：

```
<#root>

ap(config)#

aaa new-model
```

B. 配置本地RADIUS伺服器：

```
<#root>

ap(config)#

radius-server local


ap(config-radsrv)#

nas 192.168.10.2 key cisco


ap(config-radsrv)#

exit
```

C. 建立訪客帳戶，並指定其生存期（以分鐘為單位）。使用一個使用者名稱和口令user1建立一個使用者帳戶，並將生存時間值設定為60分鐘：

```
<#root>

ap(config)#

dot11 guest


ap(config-guest-mode)#

username  user1 lifetime 60 password user1


ap(config-guest-mode)#
```

```
exit


ap(config)#
```

您可以使用相同的程式建立其他使用者。

注意：必須啟用radius-server local才能建立訪客帳戶。

D. 將AP定義為RADIUS伺服器：

```
<#root>

ap(config)#

radius-server host 192.168.10.2 auth-port 1812
 acct-port 1813 key cisco
```

E. 將Web驗證清單與本機伺服器連結：

```
<#root>

ap(config)#

aaa authentication login web_list group radius
```

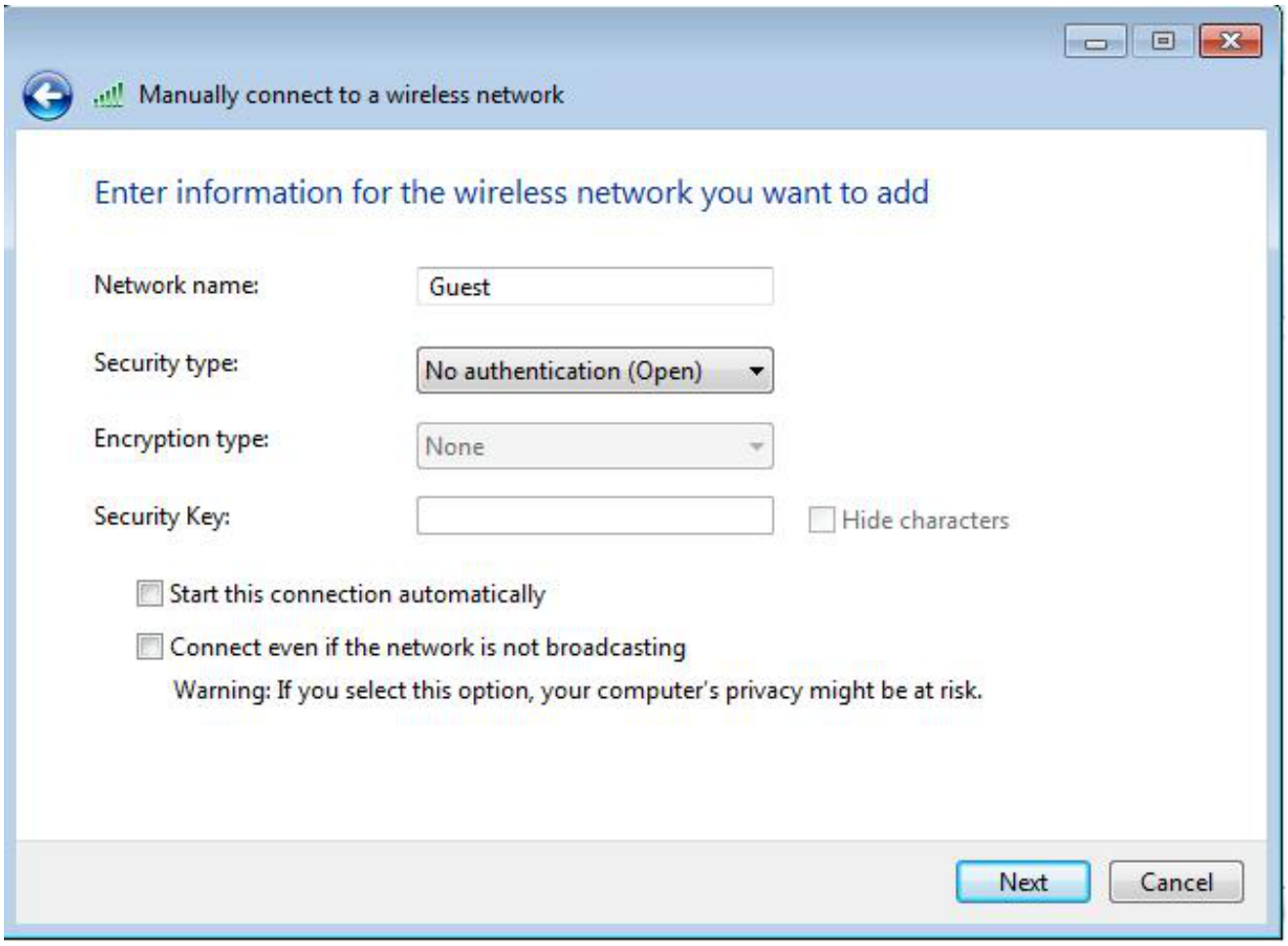
附註：您可以使用外部RADIUS伺服器來託管訪客使用者帳戶。為此，請配置radius-server host命令以指向外部伺服器而不是AP IP地址。

配置無線客戶端

要配置無線客戶端，請完成以下步驟：

1. 要使用名為Guest的SSID在Windows請求方實用程式上配置無線網路，請導航到Network and Internet > Manage Wireless Networks，然後按一下Add。

2. 選擇手動連線到無線網路並輸入必要資訊，如下圖所示：



3. 按「Next」（下一步）。

驗證

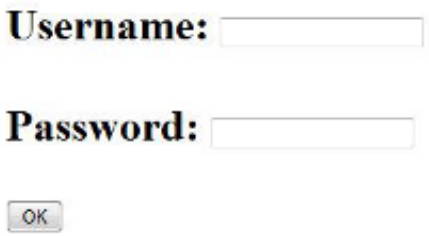
配置完成後，客戶端可以正常連線到SSID，您將在AP控制檯上看到以下內容：

```
<#root>

%DOT11-6-ASSOC: Interface Dot11Radio0, Station ap 0027.10e1.9880
 Associated KEY_MGMT[NONE]

ap#

show dot11 ass


802.11 Client Stations on Dot11Radio0:

SSID [Guest] :

MAC Address    IP address   IPV6 address  Device    Name  Parent  State

0027.10e1.9880  0.0.0.0     ::           ccx-client  ap   self    Assoc
```

客戶端的動態IP地址為192.168.10.11。但是，嘗試對客戶端的IP地址執行ping操作時失敗，因為客戶端未經過完全身份驗證：

```
<#root>

ap#

PING 192.168.10.11


 Type escape sequence to abort.

 Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:

 .....

 Success rate is 0 percent (0/5)
```

例如，如果客戶端打開瀏覽器，並且嘗試訪問http://1.2.3.4，則客戶端被重定向到內部登入頁：

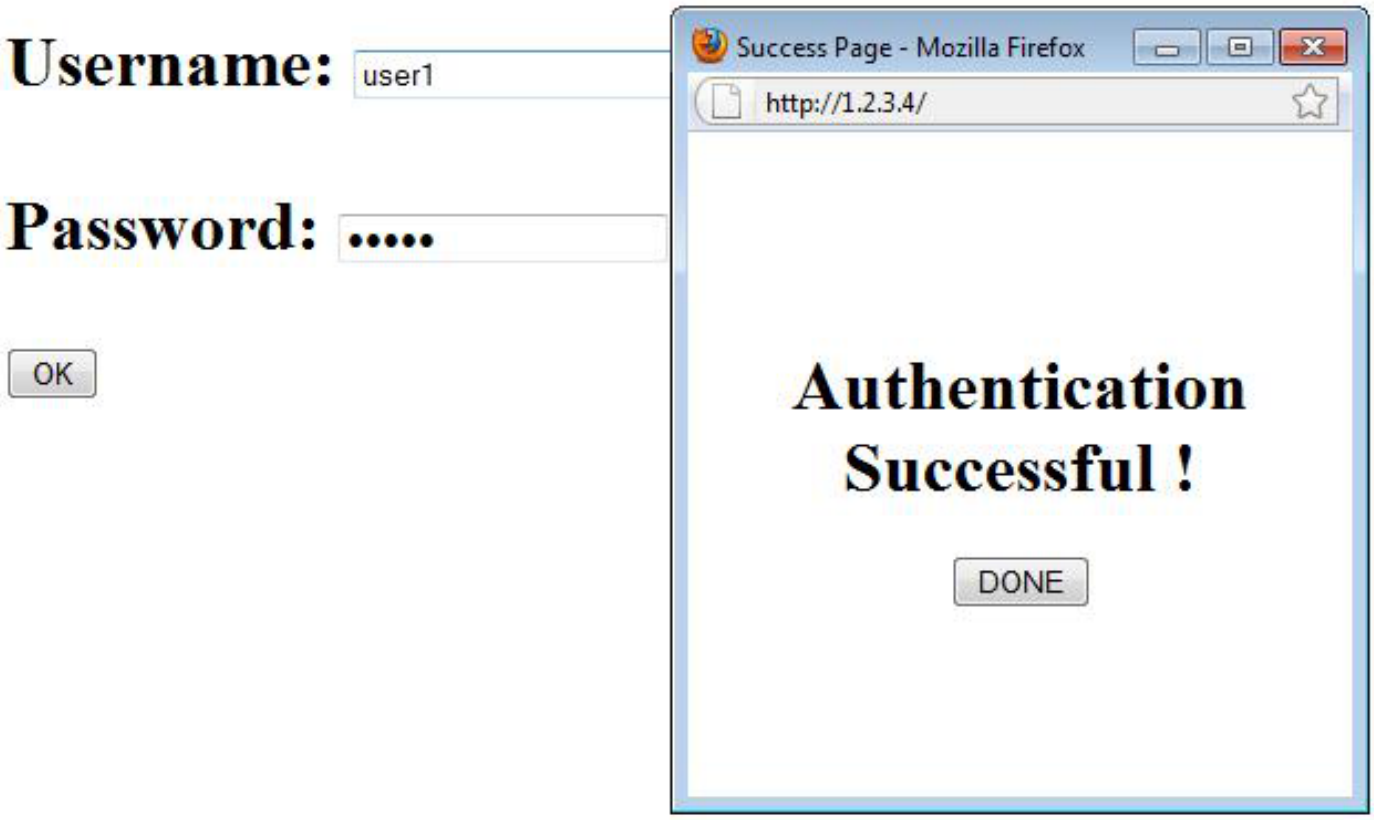


注意：本測試使用直接輸入的隨機IP地址(此處輸入的URL是1.2.3.4)完成，無需透過DNS轉換URL，因為測試中沒有使用DNS。在正常情況下，使用者會輸入首頁URL，並且允許DNS流量，直到客戶端將HTTP GET消息傳送到解析地址（被AP攔截）為止。該AP偽裝了網站地址

，並將客戶端重定向到內部儲存的登入頁。

客戶端重定向到登入頁後，將根據AP配置輸入使用者憑證並根據本地RADIUS伺服器進行驗證。在身份驗證成功後，完全允許來自和流向客戶端的流量。

以下是成功驗證後傳送給使用者的訊息：



在身份驗證成功後，您可以檢視客戶端IP資訊：

<#root>

ap#

show dot11 ass

802.11 Client Stations on Dot11Radio0:

SSID [Guest] :

MAC Address IP address IPV6 address Device Name Parent State

```
0027.10e1.9880  192.168.10.11     ::       ccx-client  ap    self   Assoc
```

在成功完成身份驗證後，對客戶端的ping操作應該可以正常工作：

<#root>

ap#

ping 192.168.10.11

```
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6 ms
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

注意：在Web身份驗證期間AP之間的漫遊無法提供流暢的體驗，因為客戶端必須登入到其連線的每個新AP。

自訂

與路由器或交換機上的IOS類似，您可以使用自定義檔案自定義頁面；但是，無法重定向到外部網頁。

使用以下命令以自定義門戶檔案：

- ip admission proxy http login page file
- ip admission proxy http expired page檔案
- ip admission proxy http success page檔案
- ip admission proxy http failure page file

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。