Internal Web Authentication for Guest Access on Autonomous APs Configuration Example

Document ID: 116897

Contributed by Mohammad Aldehnee, Cisco TAC Engineer.
Dec 17, 2013

Contents

Introduction

This document describes how to configure for guest access on autonomous Access Points (APs) with the use of the internal web page that is embedded in the AP itself.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics before you attempt this configuration:

- How to configure autonomous APs for basic operation
- How to configure the local RADIUS server on autonomous APs
- How web authentication as a Layer 3 security measure works

Components Used

The information in this document is based on these software and hardware versions:

- AIR−CAP3502I−E−K9 that runs Cisco IOS® image 15.2(4)JA1
- Intel Centrino Advanced−N 6200 AGN wireless adapter (Driver Version 13.4.0.9)
- Microsoft Windows 7 supplicant utility

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Web authentication is a Layer 3 (L3) security feature that enables the autonomous APs to block IP traffic (except DHCP and Domain Name Server (DNS)−related packets) until the guest provides a valid username and password in the web portal to which the client is redirected when a browser is opened.

With web authentication, a separate username and password must be defined for each guest. The guest is authenticated with the username and password either by the local RADIUS server or an external RADIUS server.

This feature was introduced in Cisco IOS Release 15.2(4)JA1.

AP Configuration

Note: This document assumes that Bridge Virtual Interface (BVI) 1 on the AP has an IP address of 192.168.10.2 /24, and that the DHCP pool is defined internally on the AP for IP addresses 192.168.10.10 through 192.168.10.254 (IP addresses 192.168.10.1 through 192.168.10.10 are excluded).

Complete these steps in order to configure the AP for guest access:

1. Add a new Service Set Identifier (SSID) , name it ***Guest,*** and configure it for web authentication:

```
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. Create an authentication rule, where you must specify the proxy authentication protocol, and name it ***web_auth***:

```
ap(config)#ip admission name web_auth proxy http
```

3. Apply the SSID (***Guest***) and the authentication rule (***web_auth***) to the radio interface. This example uses 802.11b/g radio:

```
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. Define the method list that specifies where the user credentials are authenticated. Link the method list name with the ***web_auth*** authentication rule, and name it ***web_list***:

```
ap(config)#ip admission name web_auth method-list authentication web_list
```

5. Complete these steps in order to configure Authentication, Authorization, and Accounting (AAA) on the AP and local RADIUS server, and link the method list with the local RADIUS server on the AP:

   A. Enable AAA:

```
ap(config)#aaa new-model
```

   B. Configure the local RADIUS server:

```
ap(config)#radius-server local

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   C. Create the guest accounts, and specify their lifetime (in minutes). Create one user account with a username and password of ***user1***, and set the lifetime value to 60 minutes:

```
ap(config)#dot11 guest

ap(config-guest-mode)#username  user1 lifetime 60 password user1

ap(config-guest-mode)#exit

ap(config)#
```

   You can create other users with the same process.

   Note: You must enable ***radius-server local*** in order to create guest accounts.

   D. Define the AP as a RADIUS server:

```
ap(config)#radius-server host 192.168.10.2 auth-port 1812
 acct-port 1813 key cisco
```

E. Link the web authentication list with the local server:

```
ap(config)#aaa authentication login web_list group radius
```

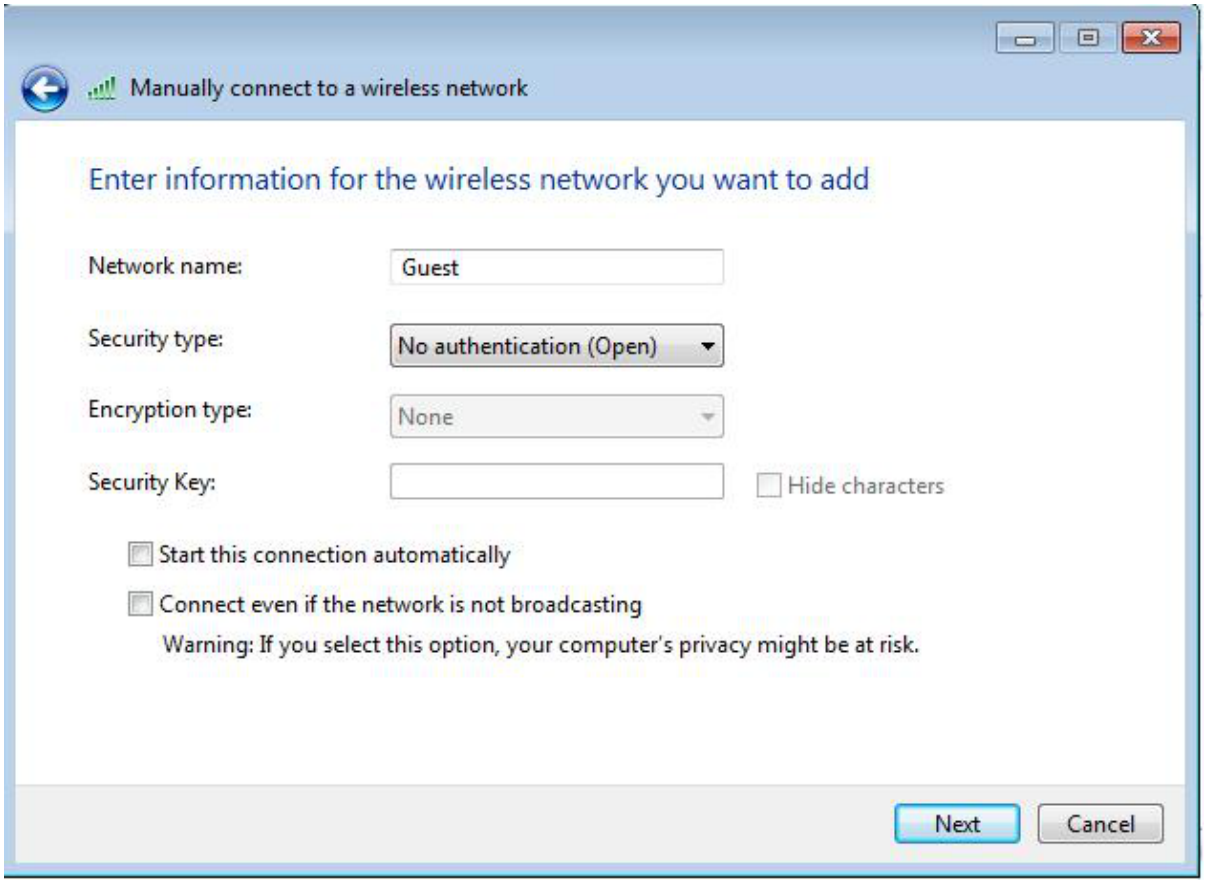
Note: You can use an external radius server in order to host the guest user accounts. In order to do this, configure the ***radius−server host*** command to point to the external server instead of the AP IP address.

Configure the Wireless Client

Complete these steps in order to configure the wireless client:

1. In order to configure the wireless network on your windows supplicant utility with the SSID named ***Guest***, navigate to ***Network and Internet > Manage Wireless Networks***, and click ***Add***.

2. Select ***Manually connect to a wireless network***, and enter the required information, as shown in this image:



3. Click ***Next***.

Verify

After the configuration is complete, the client can connect to the SSID normally, and you see this on the AP

console:

```
%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
```

The client has a dynamic IP address of 192.168.10.11. However, when you attempt to ping the IP address of the client, it fails because the client is not fully authenticated:

```
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)
```

If the client opens a browser, and attempts to reach ***http://1.2.3.4*** for example, the client is redirected to the internal login page:

Username:

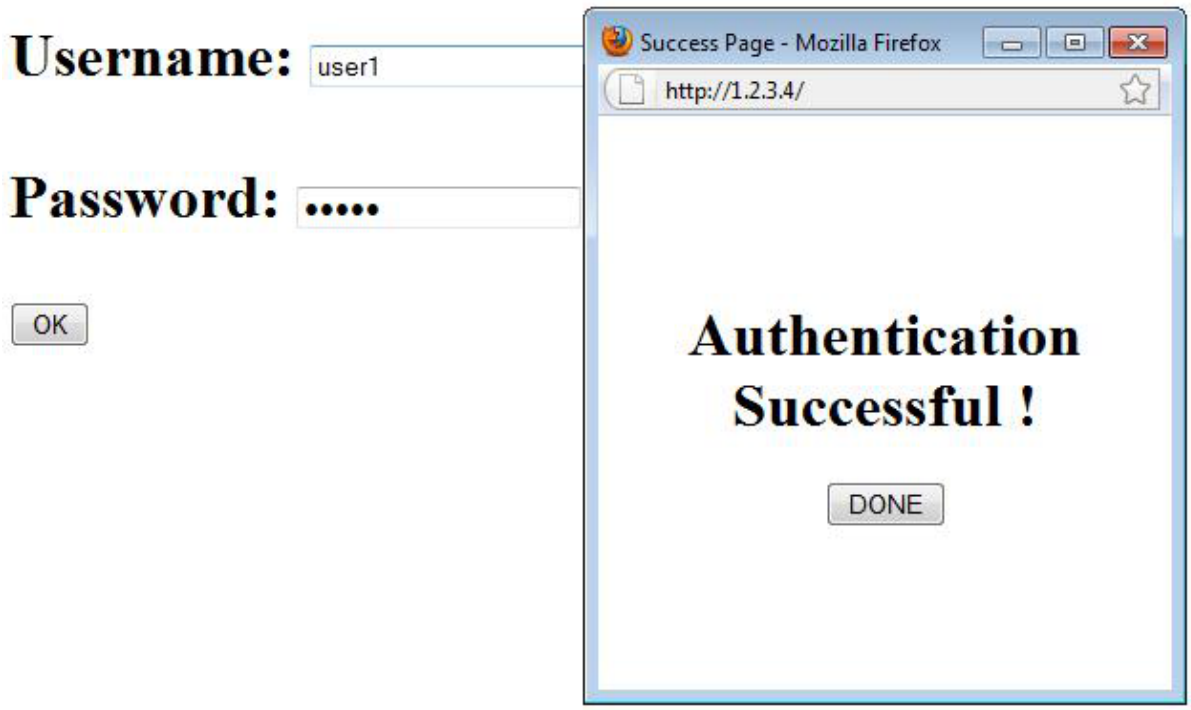
Password:

OK

Note: This test is completed with a random IP address entered directly (here the URL entered is ***1.2.3.4***) without the need for translation of a URL through the DNS, because the DNS was not used in the test. In normal scenarios, the user enters the home page URL, and the DNS traffic is allowed until the client sends the HTTP GET message to the resolved address, which is intercepted by the AP. The AP spoofs the web site address, and redirects the client to the login page stored internally.

Once the client is redirected to the login page, the user credentials are entered and verified against the local RADIUS server, as per the AP configuration. After successful authentication, the traffic that comes from and goes to the client is fully allowed.

Here is the message that is sent to the user after successful authentication:



After successful authentication, you can view the client IP information:

```
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
```

Pings to the client after successful authentication is complete should work properly:

```
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
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Note: Roaming between APs during web authentication does not provide a smooth experience, because the clients must log in to each new AP to which they connect.

Customization

Similar to the IOS on routers or switches, you can customize your page with a custom file; however, it is not possible to redirect to an external web page.

Use these commands in order to customize the portal files:

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

Updated: Dec 17, 2013 Document ID: 116897