

Wireless LAN Controller Web Passthrough Configuration Example

Document ID: 107474

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Web Passthrough on Wireless LAN Controllers

Configure the WLC for Web Passthrough

- Create a VLAN Interface
- Add a WLAN Instance
- Reboot the WLC

Configure Client Machine for Web Passthrough

- Client Configuration

Verify and Troubleshoot Web Passthrough

- Verify the Client
- Verify the Web Passthrough Authentication
- Troubleshoot Web Passthrough

Customize the Web Passthrough Login Page

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document shows how to configure the web passthrough feature on a Wireless LAN Controller (WLC).

Prerequisites

Requirements

This document assumes that initial configurations are already done on the WLC.

Components Used

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

- A 4400 series WLC that runs 5.0.148.0 code
- Cisco Secure Access Control Server (ACS) version 4.2 installed on Microsoft Windows 2003 Server
- Cisco Aironet 1230 Series Lightweight Access Point
- Cisco Aironet 802.11 a/b/g CardBus Wireless Adapter installed with Aironet Desktop Utility version 3.6

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.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Web Passthrough on Wireless LAN Controllers

Web passthrough is a solution that is typically used for guest access. The process of web passthrough is similar to that of web authentication except that no authentication credentials are required for web passthrough.

Note: For more information on web authentication, refer to *Wireless LAN Controller Web Authentication Configuration Example*.

In web passthrough the wireless users are redirected to the usage policy page when they try to use the Internet for the first time. Once the users accept the policy they can browse the Internet. This redirection to the policy page is taken care of by the WLC.

In this example, a VLAN interface is created on a separate subnet on the WLC. Then a separate WLAN/SSID is created and configured with web passthrough and mapped to this VLAN interface. Remember that web passthrough does not provide any data encryption.

Configure the WLC for Web Passthrough

In this section, you are presented with the information to configure the WLC for web passthrough.

These are the IP addresses used in this document:

- The IP address of the WLC is **10.77.244.204**, which is the management interface.
- The IP address of the the ACS server is **10.77.244.196**.

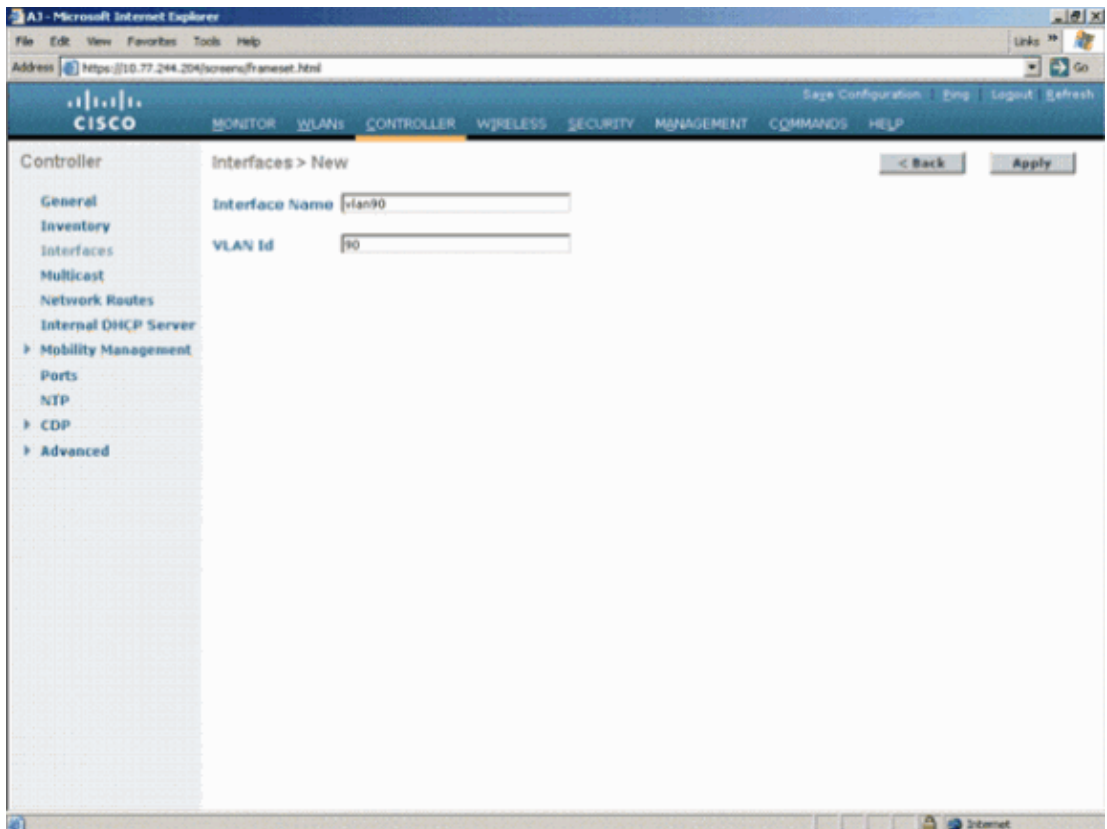
Create a VLAN Interface

Complete these steps:

1. In the main controller window, choose **Controller** from the menu at the top, choose **Interfaces** from the menu on the left, and click **New** on the upper right side of the window.

The window in Figure 1 appears. This example uses Interface Name *vlan90* with a VLAN ID of *90*:

Figure 1



2. Click **Apply** in the upper right side.

The Interfaces >Edit window appears with some parameters to be defined.

This example uses these values for the parameters:

- ◆ IP Address;0.10.10.2
- ◆ Netmask;255.255.255.0 (24 bits)
- ◆ Gateway;0.10.10.1
- ◆ Port Number;90

Note: Make sure this is the active port number on the WLC which is connected to the switch.

- ◆ Primary DHCP Server;0.77.244.204

Note: This parameter should be the IP address of your RADIUS or DHCP server. In this example, the management address of the WLC is used as the DHCP server because the Internal DHCP scope is configured on the WLC. For more information on how to configure the DHCP server on the WLC, refer to the Set Up DHCP and DNS Servers on the WLC section of the document Wireless LAN Controller Web Authentication Configuration Example.

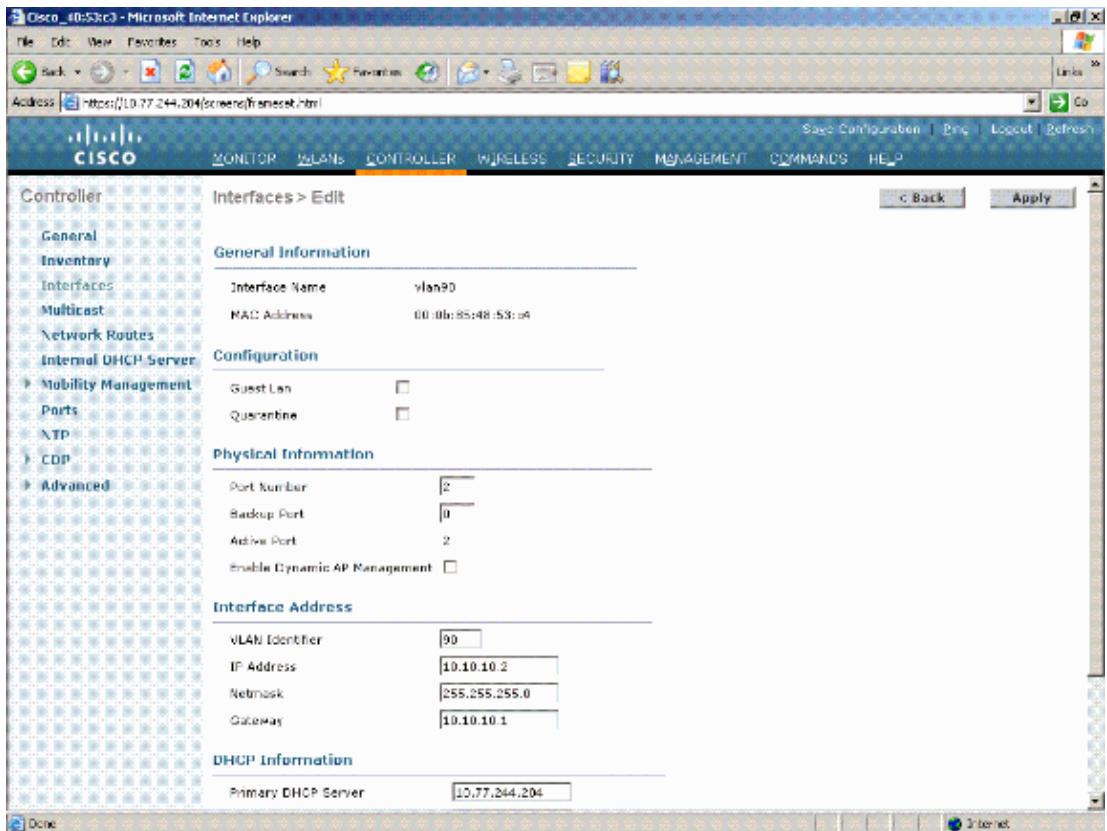
- ◆ Secondary DHCP Server .0.0.0

Note: The example does not have a secondary DHCP server, so 0.0.0.0 is used. If your configuration has a secondary DHCP server, add the server IP address in this field.

- ◆ ACL Name None

Figure 2 shows these parameters:

Figure 2



3. Click **Apply** in order to save the changes.

Add a WLAN Instance

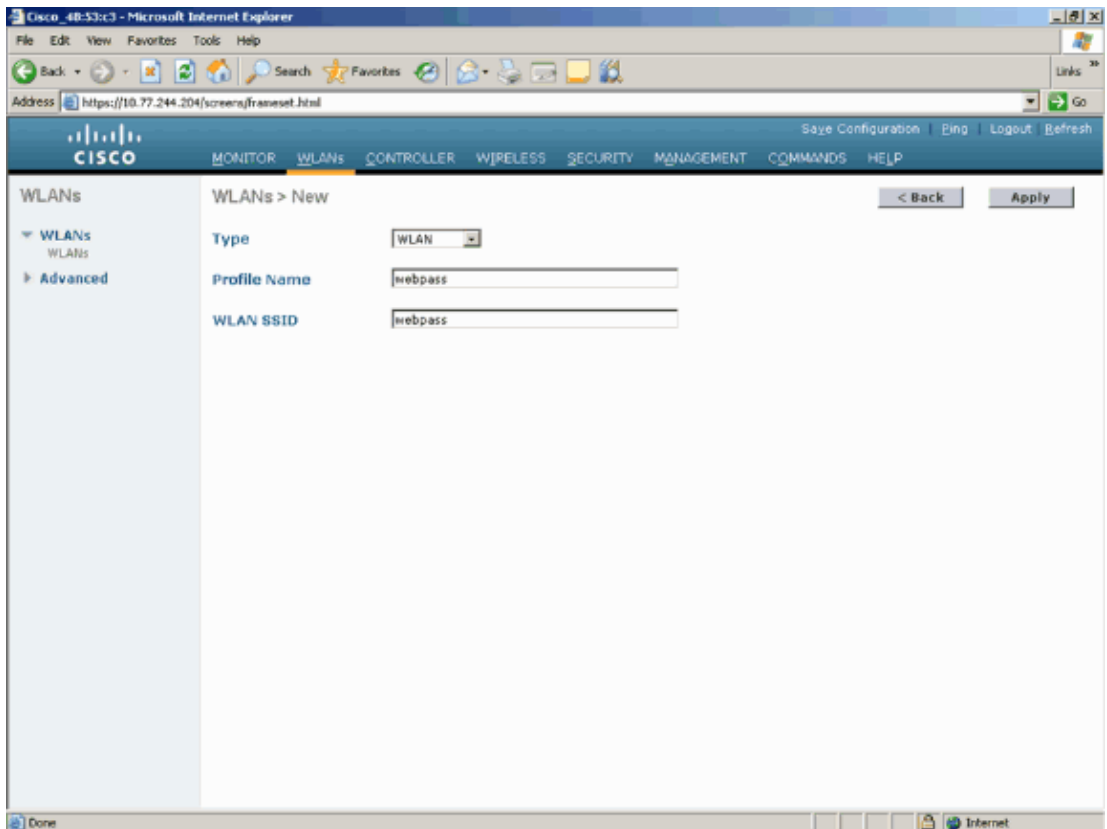
Now that you have a VLAN interface that is dedicated for web passthrough, you must create a new WLAN/SSID.

Complete these steps in order to create a new WLAN/SSID:

1. Open the WLC browser, click **WLAN** in the menu at the top, and click **New** on the upper right side.

The window shown in Figure 3 appears.

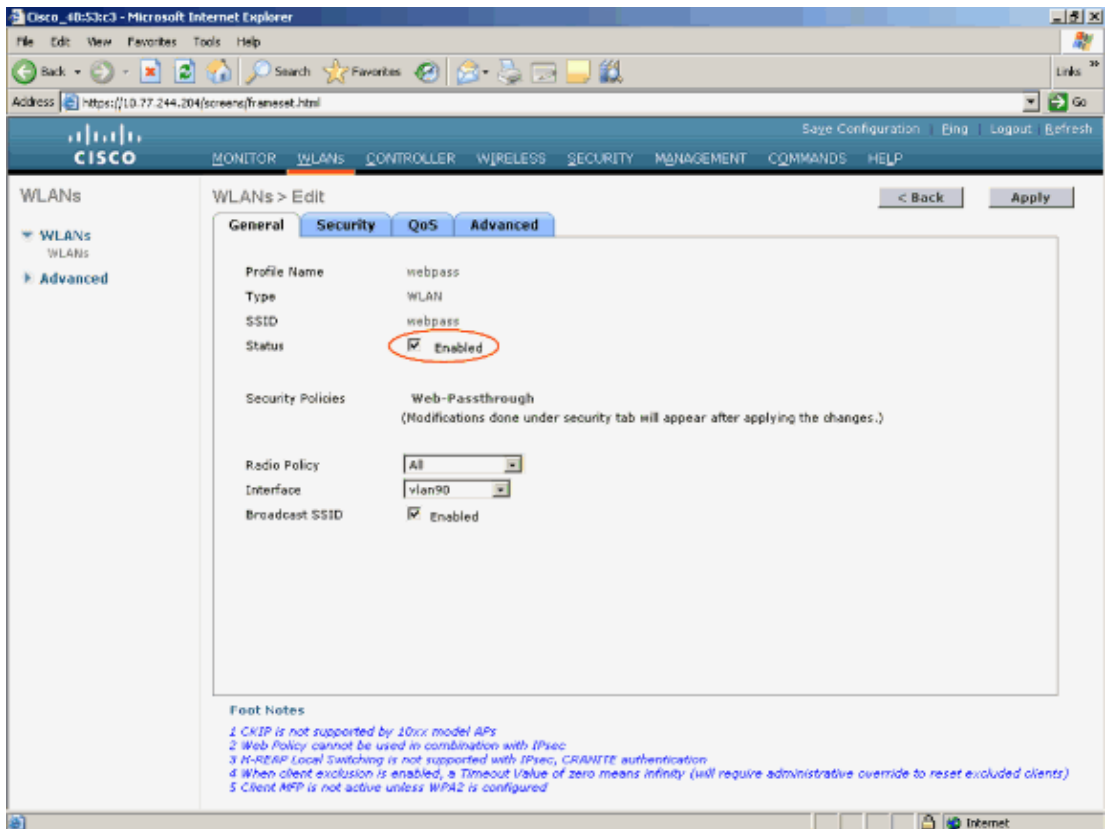
Figure 3



2. Choose **WLAN** as the Type. Select a profile name and WLAN SSID for web passthrough. This example uses **webpass** for both the Profile Name and WLAN SSID.
3. Click **Apply** in the upper right corner.

A new **WLANs> Edit** window appears, as shown in Figure 4. This window is different for WLC versions earlier than 4.2.

Figure 4

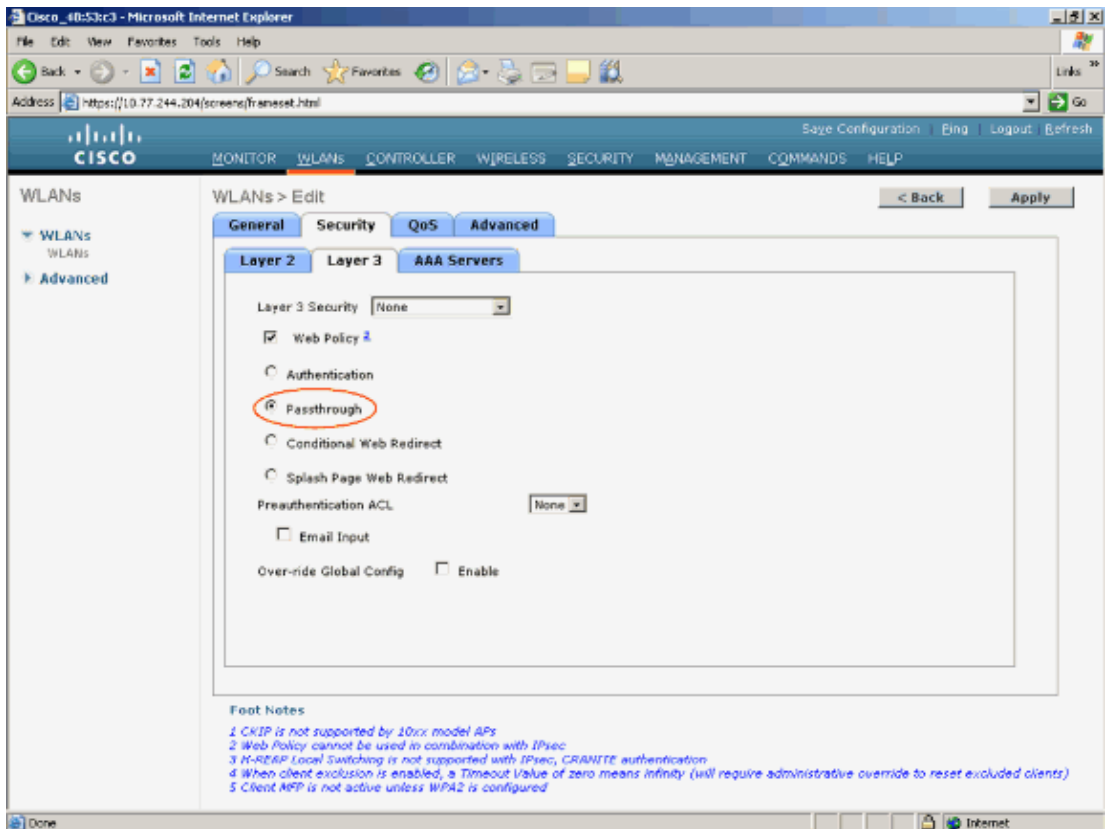


4. Check the status box of the WLAN to enable the WLAN. From the Interface menu, select the name of the VLAN interface that you created previously. In this example, the Interface name is `vlan90`, as shown in Figure 4.

Note: Leave the default value for the other parameters on this screen.

5. Select the **Security** tab. The window shown in Figure 5 appears.

Figure 5



Complete these steps to configure web passthrough:

- a. Click the **Layer 2** tab and set the security as **None** .

Note: You cannot configure web passthrough as Layer 3 security with 802.1x or WPA/WPA2 as Layer 2 security for a WLAN. Refer to Wireless LAN Controller Layer 2 Layer 3 Security Compatibility Matrix for more information on the Wireless LAN Controller Layer 2 and Layer 3 security compatibility.

- b. Click the **Layer 3** tab. Check the **Web Policy** check box and choose the **Passthrough** option, as shown in Figure 5.
- c. Click **Apply** in order to save this WLAN to the running configuration on the WLAN switch.

You are returned to the WLAN summary window.

- d. Make sure that the web passthrough is enabled under the Security Policies column of the WLAN table for the SSID *webpass* .

Reboot the WLC

You must reboot the WLC because one or more of the WLAN changes cannot be made while the system is active. The changes must be made before or during the boot. Complete these steps in order to reboot the WLC:

1. In the main controller window, choose **Commands** from the menu at the top.
2. In the new window, choose **Reboot** from the menu on the left.

You are prompted to save and reboot if there are unsaved changes in your configuration.

3. Click **Save and Reboot** in order to save the configuration and reboot the switch.
4. Monitor your system reboot from the console connection.

When the WLC is up, you can create your web authentication subscriber.

Configure Client Machine for Web Passthrough

Once the WLC is configured, the client should also be configured appropriately for web passthrough. In this section, you are presented with the information to configure your client for web passthrough using the Cisco Aironet Desktop Utility.

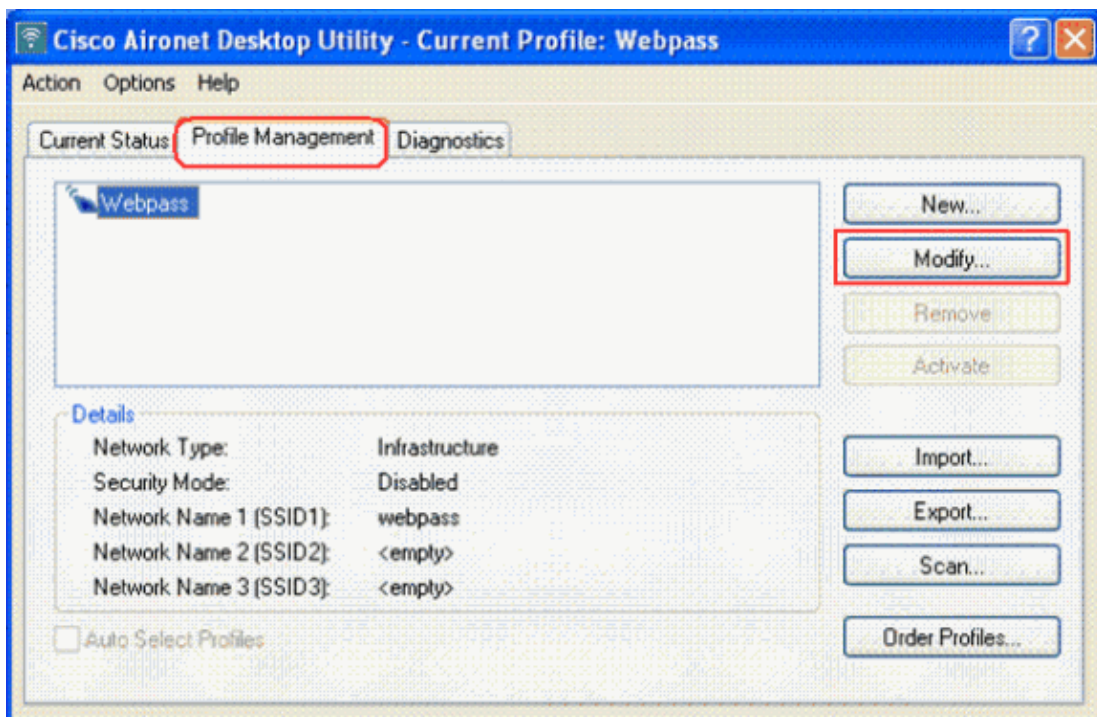
Client Configuration

Make sure that the drivers for the client adapter and the Cisco Aironet Desktop Utility are installed on the client computer. Complete these steps:

1. Click the shortcut icon for Aironet Utility on the desktop.
2. On the Cisco Aironet Desktop Utility screen, click the **Profile Management** tab.
3. Click on the existing profile and click the **Modify** button.

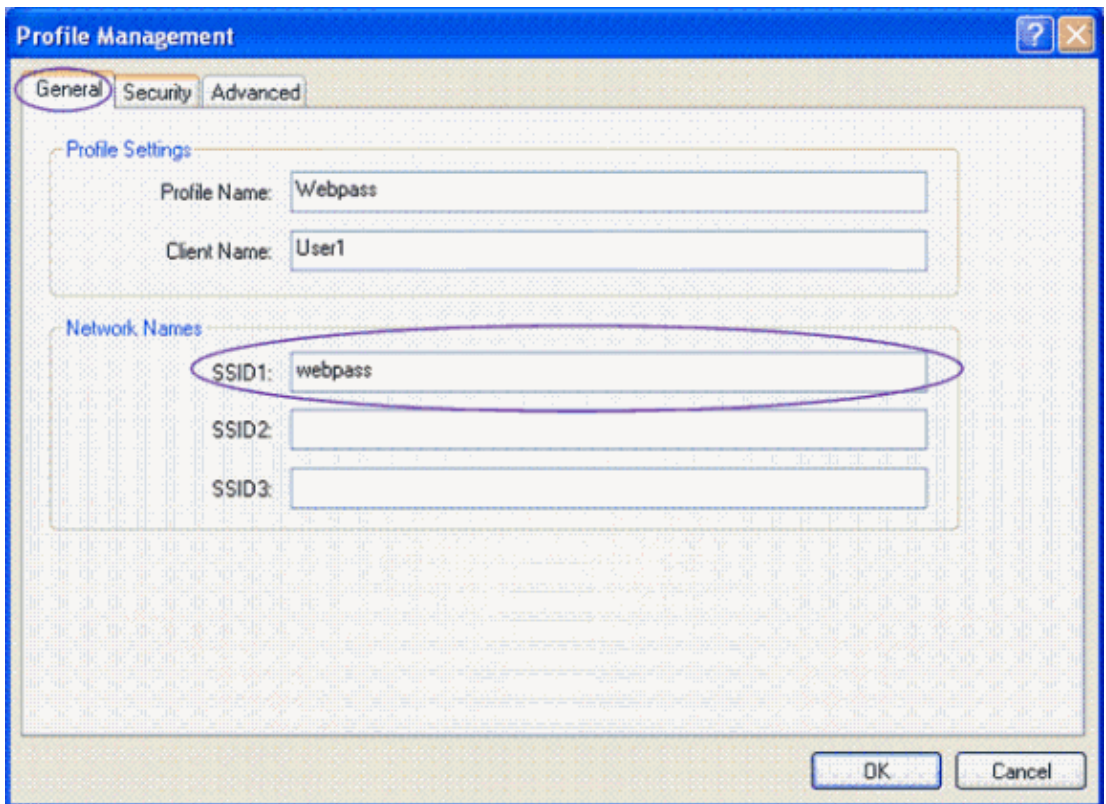
Figure 6 shows how to perform steps 2 and 3.

Figure 6



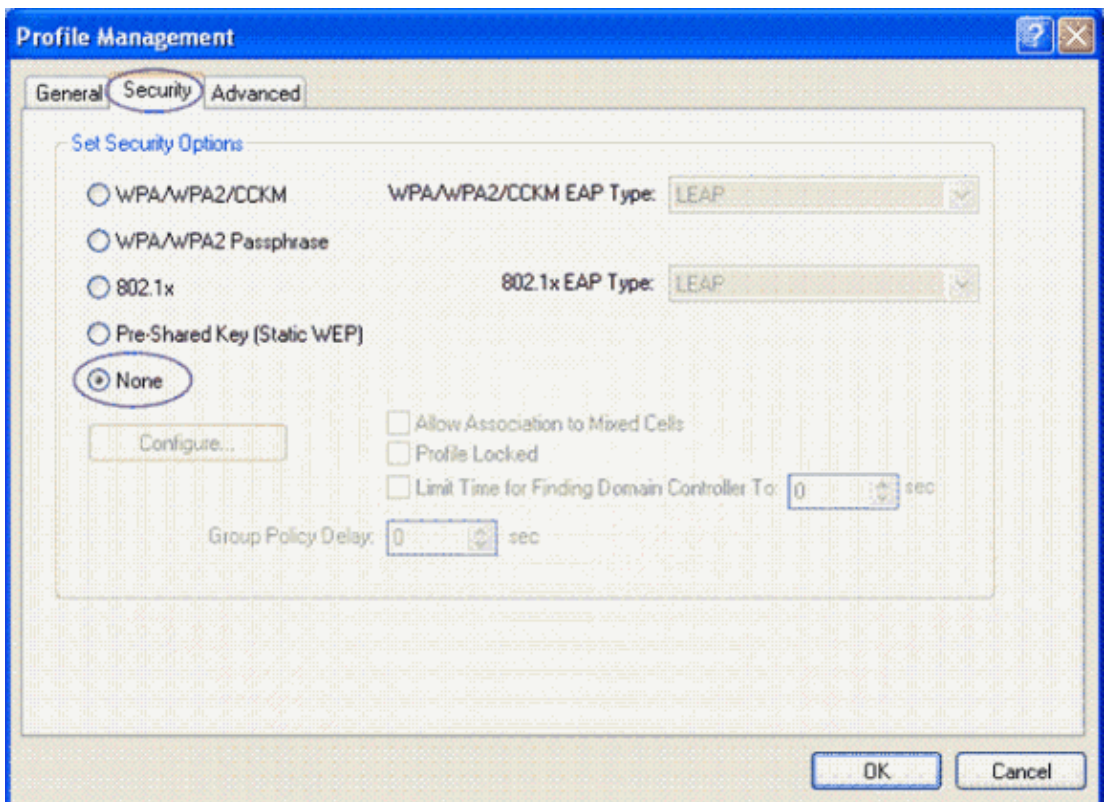
4. Under the General tab, choose a Profile Name. Enter the SSID configured on the WLC for web passthrough, as shown in **Figure 7** . In this example, the SSID is *webpass* .

Figure 7



5. Select the **Security** tab. Choose the security option as *None* , as shown in **Figure 8** .

Figure 8



6. Click **OK**.

This brings you back to the main screen of the Desktop Utility.

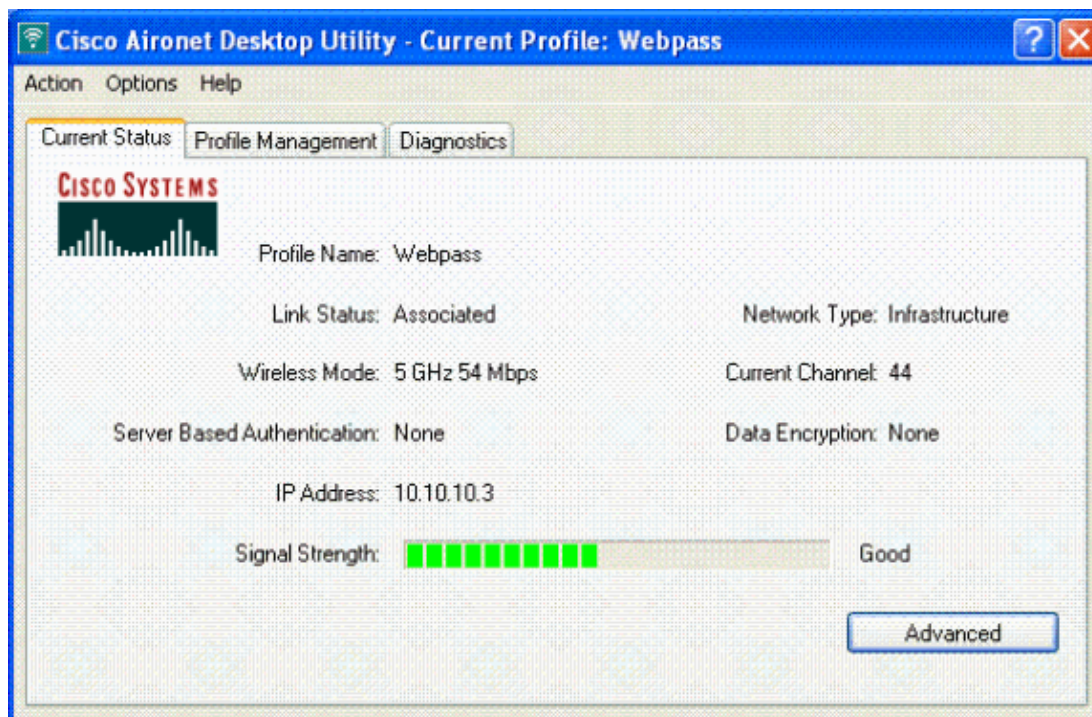
Note: If your wireless client is also a VPN end point and you have web passthrough configured as a security feature for WLAN, then the VPN tunnel is not established until you go through the web passthrough process explained here. In order to establish a VPN tunnel, the client must first go through the process of web passthrough with success. Only then is VPN tunneling successful.

Verify and Troubleshoot Web Passthrough

Verify the Client

If the wireless connection is successful you should have obtained a valid IP address from the **WLC**. Click the **Current Status** Tab to verify this. Ensure that the IP address is from the correct subnet. In this example, it is *vlan90* configured with the *10.10.10.0/24* network. **Figure 9** shows a sample successful wireless connection.

Figure 9



In order to determine the WLC to which the client is associated, click the **Advanced** button at the bottom of the screen, as shown in **Figure 9**. Here, the WLC IP address and MAC address is shown as AP IP address and AP MAC address.

Verify the Web Passthrough Authentication

Complete these steps:

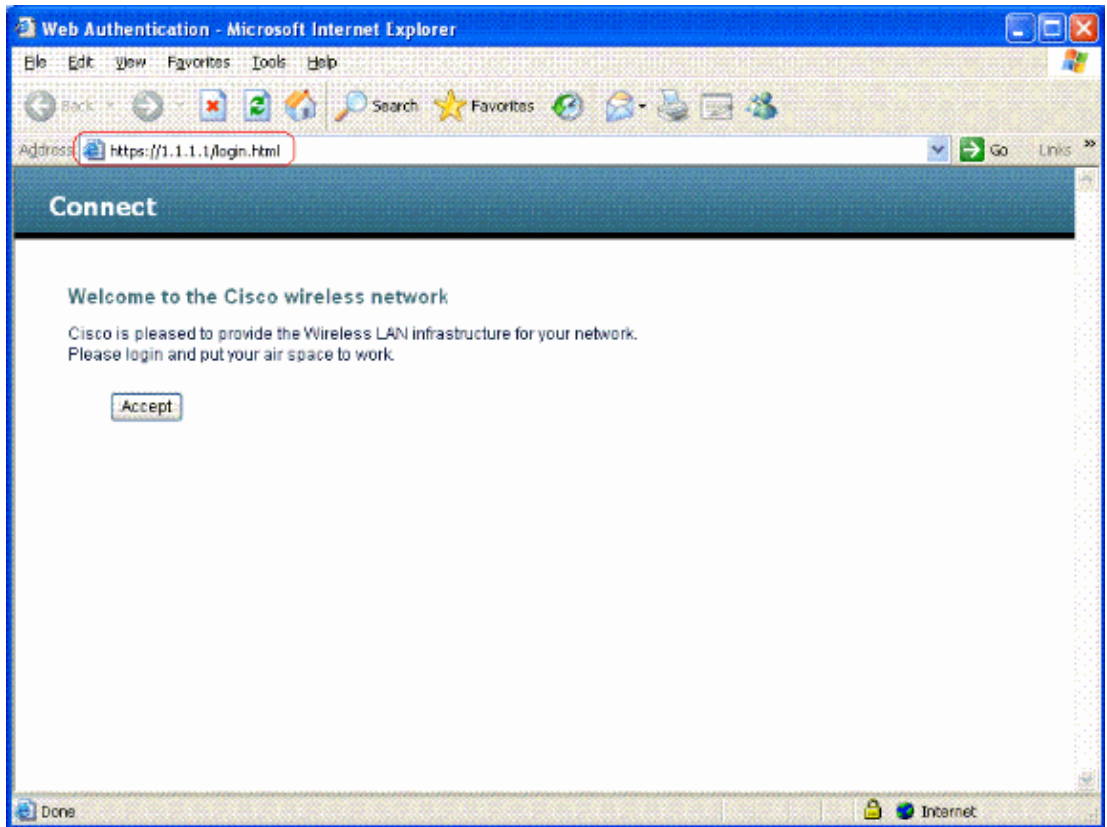
1. Open a browser window and enter the virtual IP address that is configured on the WLC.

Here, the secure `https://1.1.1.1/login.html` is used. This step is important in versions earlier than 3.0, but the step is not necessary in later versions. In later versions, any URL brings you to the web passthrough page.

A security alert window displays.

2. Click **Yes** in order to proceed. Figure 10 shows the web passthrough page displayed on the client.

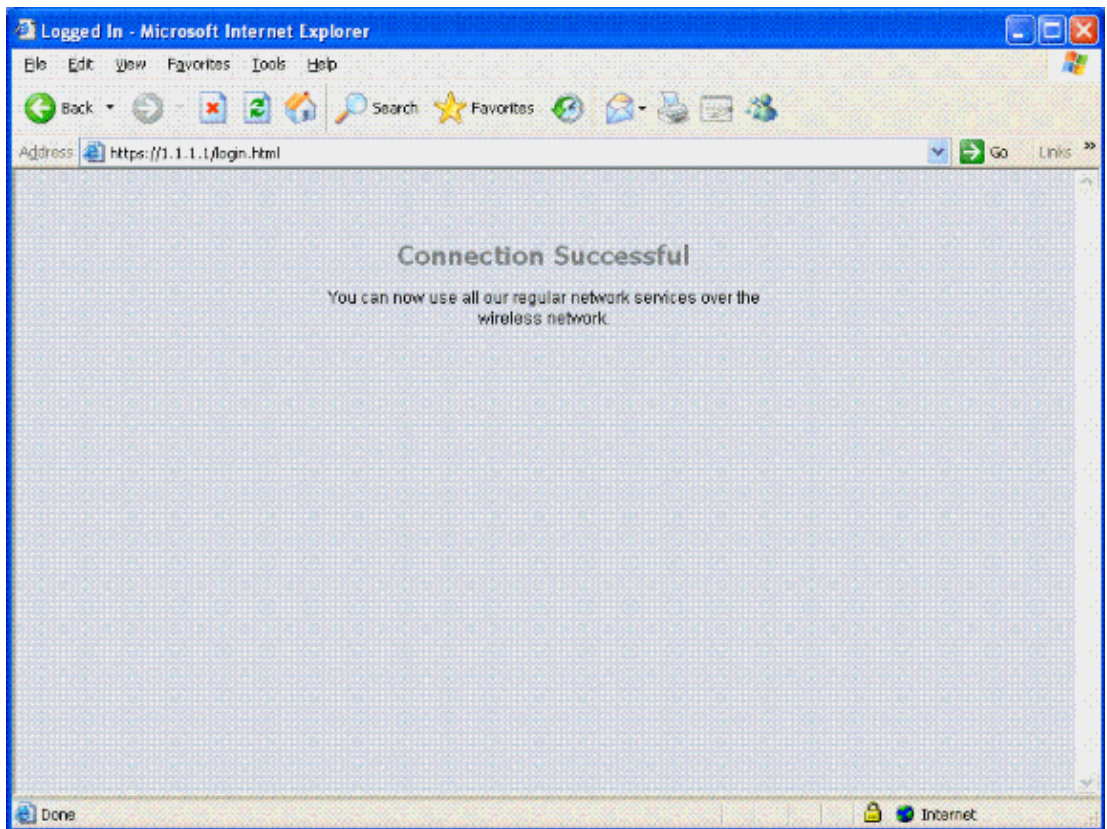
Figure 10



3. When the web passthrough window appears, click the **Accept** button. A window displays that shows the successful connection. Internet connection can now be used.

Figure 11 shows the successful connection window.

Figure 11



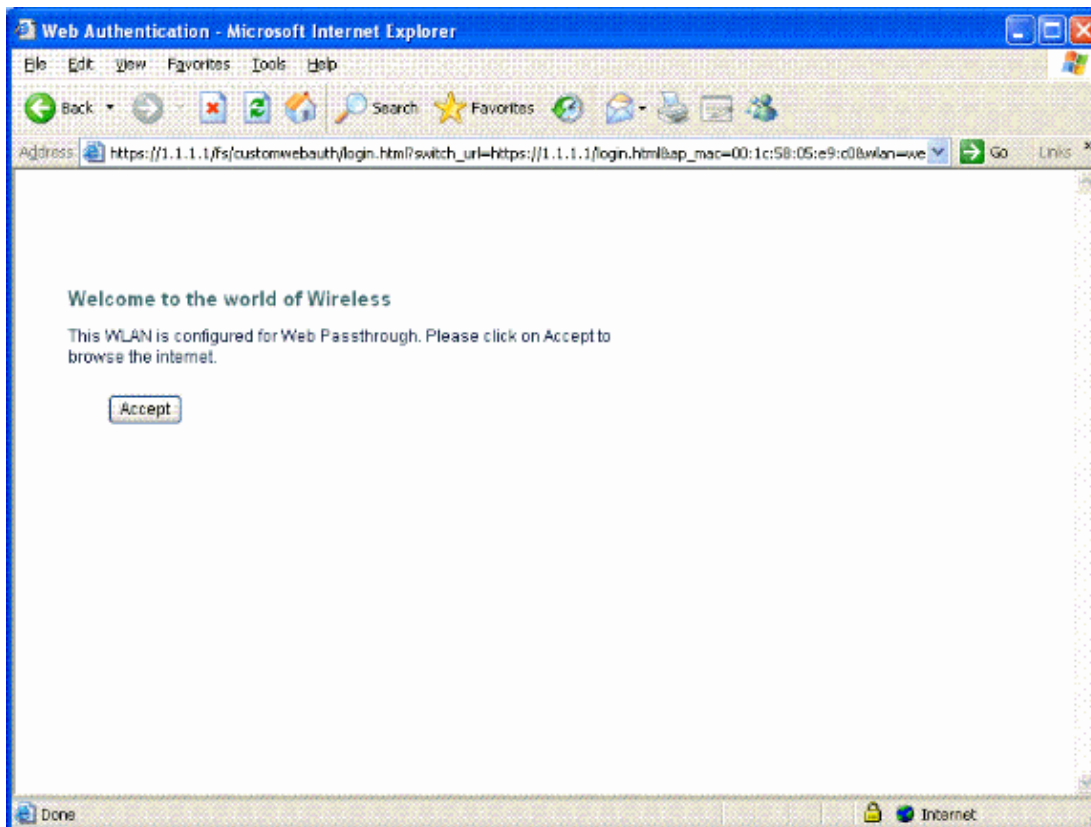
Troubleshoot Web Passthrough

Troubleshooting web passthrough is similar to that of web authentication. For troubleshooting purposes, refer to the Troubleshoot Internal Web Authentication section of the document Wireless LAN Controller Web Authentication Configuration Example.

Customize the Web Passthrough Login Page

The default web passthrough page can be customized to suit your needs. For more information on how to customize the web passthrough page, refer to the Configure Web Passthrough in the WLC section of the document Wireless LAN Controller Web Authentication Configuration Example. **Figure 12** shows a sample customized page.

Figure 12



NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Wireless

Wireless – Mobility: WLAN Radio Standards

Wireless – Mobility: Security and Network Management

Wireless – Mobility: Getting Started with Wireless

Wireless – Mobility: General

Related Information

- [Wireless LAN Controller Web Authentication Configuration Example](#)
- [Cisco Wireless LAN Controller Configuration Guide, Release 5.0](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 01, 2008

Document ID: 107474