



Configuring Security Solutions

This chapter describes security solutions for wireless LANs. This chapter contains these sections:

- [Cisco WLAN Solution Security, page 5-2](#)
- [Configuring the System for SpectraLink NetLink Telephones, page 5-4](#)
- [Using Management over Wireless, page 5-6](#)
- [Configuring DHCP, page 5-7](#)
- [Customizing the Web Authentication Login Screen, page 5-8](#)
- [Configuring Identity Networking, page 5-16](#)

Cisco WLAN Solution Security

Cisco WLAN Solution Security includes the following sections:

- [Security Overview, page 5-2](#)
- [Layer 1 Solutions, page 5-2](#)
- [Layer 2 Solutions, page 5-2](#)
- [Layer 3 Solutions, page 5-3](#)
- [Rogue Access Point Solutions, page 5-3](#)
- [Integrated Security Solutions, page 5-4](#)

Security Overview

The Cisco WLAN Solution Security solution bundles potentially complicated Layer 1, Layer 2, and Layer 3 802.11 Access Point security components into a simple policy manager that customizes system-wide security policies on a per-WLAN basis. The Cisco WLAN Solution Security solution provides simple, unified, and systematic security management tools.

One of the biggest hurdles to WLAN deployment in the enterprise is WEP encryption, which is weak standalone encryption method. A newer problem is the availability of low-cost access points, which can be connected to the enterprise network and used to mount man-in-the-middle and denial-of-service attacks. Also, the complexity of add-on security solutions has prevented many IT managers from embracing the benefits of the latest advances in WLAN security.

Layer 1 Solutions

The Cisco WLAN Solution Operating System Security solution ensures that all clients gain access within an operator-set number of attempts. Should a client fail to gain access within that limit, it is automatically excluded (blocked from access) until the operator-set timer expires. The Operating System can also disable SSID broadcasts on a per-WLAN basis.

Layer 2 Solutions

If a higher level of security and encryption is required, the network administrator can also implement industry-standard security solutions, such as: 802.1X dynamic keys with EAP (extensible authentication protocol), or WPA (Wi-Fi protected access) dynamic keys. The Cisco WLAN Solution WPA implementation includes AES (advanced encryption standard), TKIP + Michael (temporal key integrity protocol + message integrity code checksum) dynamic keys, or WEP (Wired Equivalent Privacy) static keys. Disabling is also used to automatically block Layer 2 access after an operator-set number of failed authentication attempts.

Regardless of the wireless security solution selected, all Layer 2 wired communications between Cisco Wireless LAN Controllers and Cisco 1000 Series lightweight access points are secured by passing data through LWAPP tunnels.

Layer 3 Solutions

The WEP problem can be further solved using industry-standard Layer 3 security solutions, such as VPNs (virtual private networks), L2TP (Layer Two Tunneling Protocol), and IPSec (IP security) protocols. The Cisco WLAN Solution L2TP implementation includes IPSec, and the IPSec implementation includes IKE (internet key exchange), DH (Diffie-Hellman) groups, and three optional levels of encryption: DES (ANSI X.3.92 data encryption standard), 3DES (ANSI X9.52-1998 data encryption standard), or AES/CBC (advanced encryption standard/cipher block chaining). Disabling is also used to automatically block Layer 3 access after an operator-set number of failed authentication attempts.

The Cisco WLAN Solution IPSec implementation also includes industry-standard authentication using: MD5 (message digest algorithm), or SHA-1 (secure hash algorithm-1).

The Cisco WLAN Solution supports local and RADIUS MAC (media access control) filtering. This filtering is best suited to smaller client groups with a known list of 802.11 access card MAC addresses.

Finally, the Cisco WLAN Solution supports local and RADIUS user/password authentication. This authentication is best suited to small to medium client groups.

Rogue Access Point Solutions

This section describes security solutions for rogue access points.

Rogue Access Point Challenges

Rogue access points can disrupt WLAN operations by hijacking legitimate clients and using plaintext or other denial-of-service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as passwords and username. The hacker can then transmit a series of clear-to-send (CTS) frames, which mimics an access point informing a particular NIC to transmit and instructing all others to wait, which results in legitimate clients being unable to access the WLAN resources. WLAN service providers thus have a strong interest in banning rogue access points from the air space.

The Operating System Security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points, automatically discover rogue access points, and locate them as described in the [“Tagging and Containing Rogue Access Points”](#) section on page 5-3.

Tagging and Containing Rogue Access Points

When the Cisco WLAN Solution is monitored using WCS, WCS generates the flags as rogue access point traps, and displays the known rogue access points by MAC address. The operator can then display a map showing the location of the Cisco 1000 Series lightweight access points closest to each rogue access point, allowing Known or Acknowledged rogue access points (no further action), marking them as Alert rogue access points (watch for and notify when active), or marking them as contained rogue access points. Between one and four Cisco 1000 Series lightweight access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point.

When the Cisco WLAN Solution is monitored using a GUI or a CLI, the interface displays the known rogue access points by MAC address. The operator then has the option of marking them as Known or Acknowledged rogue access points (no further action), marking them as Alert rogue access points (watch

for and notify when active), or marking them as Contained rogue access points (have between one and four Cisco 1000 Series lightweight access points discourage rogue access point clients by sending the clients deauthenticate and disassociate messages whenever they associate with the rogue access point).

Integrated Security Solutions

- Cisco WLAN Solution Operating System Security is built around a robust 802.1X AAA (authorization, authentication and accounting) engine, which allows operators to rapidly configure and enforce a variety of security policies across the Cisco WLAN Solution.
- The controllers and lightweight access points are equipped with system-wide authentication and authorization protocols across all ports and interfaces, maximizing system security.
- Operating System Security policies are assigned to individual WLANs, and lightweight access points simultaneously broadcast all (up to 16) configured WLANs. This can eliminate the need for additional access points, which can increase interference and degrade system throughput.
- The controllers securely terminates IPsec VPN clients, which can reduce the load on centralized VPN concentrators.
- Operating System Security uses the RRM function to continually monitor the air space for interference and security breaches, and notify the operator when they are detected.
- Operating System Security works with industry-standard authorization, authentication, and accounting (AAA) servers, making system integration simple and easy.
- The Operating System Security solution offers comprehensive Layer 2 and Layer 3 encryption algorithms which typically require a large amount of processing power. Rather than assigning the encryption tasks to yet another server, the controller can be equipped with a VPN/Enhanced Security Module that provides extra hardware required for the most demanding security configurations.

Configuring the System for SpectraLink NetLink Telephones

For best integration with the Cisco Wireless LAN Solution, SpectraLink NetLink Telephones require an extra Operating System configuration step: enable long preambles. The radio preamble (sometimes called a header) is a section of data at the head of a packet that contains information that wireless devices need when sending and receiving packets. Short preambles improve throughput performance, so they are enabled by default. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles.

Use one of these methods to enable long preambles:

- [Using the GUI to Enable Long Preambles, page 5-5](#)
- [Using the CLI to Enable Long Preambles, page 5-5](#)

Using the GUI to Enable Long Preambles

Use this procedure to use the GUI to enable long preambles to optimize the operation of SpectraLink NetLink phones on your wireless LAN.

-
- Step 1** Log into the controller GUI.
- Step 2** Follow this path to navigate to the 802.11b/g Global Parameters page:

Wireless > Global RF > 802.11b/g Network

If the Short Preamble Enabled box is checked, continue with this procedure. However, if the Short Preamble Enabled box is unchecked (which means that long preambles are enabled), the controller is already optimized for SpectraLink NetLink phones and you do not need to continue this procedure.

- Step 3** Uncheck the Short Preamble Enabled check box to enable long preambles.
- Step 4** Click **Apply** to update the controller configuration.



Note If you do not already have an active CLI session to the controller, Cisco recommends that you start a CLI session to reboot the controller and watch the reboot process. A CLI session is also useful because the GUI loses its connection when the controller reboots.

- Step 5** Reboot the controller using Commands > Reboot > Reboot. Click **OK** in response to this prompt:

Configuration will be saved and switch will be rebooted. Click ok to confirm.

The controller reboots.

- Step 6** Log back into the controller GUI and verify that the controller is properly configured. Follow this path to navigate to the 802.11b/g Global Parameters page:

Wireless > Global RF > 802.11b/g Network

If the Short Preamble Enabled box is unchecked, the controller is optimized for SpectraLink NetLink phones.

Using the CLI to Enable Long Preambles

Use this procedure to use the CLI to enable long preambles to optimize the operation of SpectraLink NetLink phones on your wireless LAN.

-
- Step 1** Log into the controller CLI.
- Step 2** Enter **show 802.11b** and check the Short preamble mandatory parameter. If the parameter indicates that short preambles are enabled, continue with this procedure. This example shows that short preambles are enabled:

```
Short Preamble mandatory..... Enabled
```

However, if the parameter shows that short preambles are disabled (which means that long preambles are enabled), the controller is already optimized for SpectraLink NetLink phones and you do not need to continue this procedure. This example shows that short preambles are disabled:

```
Short Preamble mandatory..... Disabled
```

- Step 3** Enter **config 802.11b disable network** to disable the 802.11b/g network. (You cannot enable long preambles on the 802.11a network.)
- Step 4** Enter **config 802.11b preamble long** to enable long preambles.
- Step 5** Enter **config 802.11b enable network** to re-enable the 802.11b/g network.
- Step 6** Enter **reset system** to reboot the controller. Enter **y** when this prompt appears:
- ```
The system has unsaved changes. Would you like to save them now? (y/n)
```
- The controller reboots.
- Step 7** To verify that the controller is properly configured, log back into the CLI and enter **show 802.11b** to view these parameters:
- ```
802.11b Network..... Enabled
Short Preamble mandatory..... Disabled
```
- These parameters show that the 802.11b/g network is enabled and that short preambles are disabled.
-

Using Management over Wireless

The Cisco WLAN Solution Management over Wireless feature allows Cisco WLAN Solution operators to monitor and configure local controllers using a wireless client. This feature is supported for all management tasks except uploads to and downloads from (transfers to and from) the controller.

Before you can use the Management over Wireless feature, you must properly configure the controller using one of these sections:

- [Using the GUI to Enable Management over Wireless, page 5-6](#)
- [Using the CLI to Enable Management over Wireless, page 5-7](#)

Using the GUI to Enable Management over Wireless

-
- Step 1** In the Web User Interface, use the **Management/Mgmt Via Wireless** links to navigate to the **Management Via Wireless** page.
- Step 2** In the **Management Via Wireless** page, verify that the **Enable Controller Management to be accessible from Wireless Clients** selection box is checked. If the selection box is not checked, continue with Step 2. Otherwise, continue with Step 3.
- Step 3** In the **Management Via Wireless** page, check the **Enable Controller Management to be accessible from Wireless Clients** selection box to select Management over Wireless for the WLAN.
- Step 4** Click **Apply** to enable Management over Wireless for the WLAN.
- Step 5** Use a wireless client web browser to connect to the Cisco Wireless LAN Controller Management Port or DS Port IP Address, and log into the Web User Interface to verify that you can manage the WLAN using a wireless client.
-

Using the CLI to Enable Management over Wireless

-
- Step 1** In the CLI, use the **show network** command to verify whether the Mgmt Via Wireless Interface is Enabled or Disabled. If Mgmt Via Wireless Interface is Disabled, continue with Step 2. Otherwise, continue with Step 3.
- Step 2** To Enable Management over Wireless, enter **config network mgmt-via-wireless enable**.
- Step 3** Use a wireless client to associate with an access point connected to the controller that you want to manage.
- Step 4** Enter **telnet controller-ip-address** and log into the CLI to verify that you can manage the WLAN using a wireless client.
-

Configuring DHCP

Follow the steps in one of these sections to configure your wireless LAN to use a DHCP server:

- [Using the GUI to Configure DHCP, page 5-7](#)
- [Using the CLI to Configure DHCP, page 5-8](#)

Using the GUI to Configure DHCP

Follow these steps to use the GUI to configure DHCP.

-
- Step 1** In the Web User Interface, navigate to the **WLANs** page.
- Step 2** Locate the WLAN which you wish to configure for a DHCP server, and click the associated **Edit** link to display the **WLANs > Edit** page.
- Step 3** Under **General Policies**, check the **DHCP Relay/DHCP Server IP Addr** to verify whether you have a valid DHCP server assigned to the WLAN. If you have no DHCP server assigned to the WLAN, continue with Step 4. Otherwise, continue with Step 9.
- Step 4** Under **General Policies**, deselect the **Admin Status Enabled** box.
- Step 5** Click **Apply** to disable the WLAN.
- Step 6** In the **DHCP Relay/DHCP Server IP Addr** box, enter a valid DHCP server IP Address for this WLAN.
- Step 7** Under **General Policies**, select the **Admin Status Enabled** box.
- Step 8** Click **Apply** to assign the DHCP server to the WLAN and to enable the WLAN. You are returned to the **WLANs** page.
- Step 9** In the upper-right corner of the **WLANs** page, click **Ping** and enter the DHCP server IP Address to verify that the WLAN can communicate with the DHCP server.
-

Using the CLI to Configure DHCP

Follow these steps to use the CLI to configure DHCP.

-
- Step 1** In the CLI, enter **show wlan** to verify whether you have a valid DHCP server assigned to the WLAN. If you have no DHCP server assigned to the WLAN, continue with Step 2. Otherwise, continue with Step 4.
- Step 2** If necessary, use these commands:
- **config wlan disable** *wlan-id*
 - **config wlan dhcp_server** *wlan-id dhcp-ip-address*
 - **config wlan enable** *wlan-id*
- In these commands, *wlan-id* = 1 through 16 and *dhcp-ip-address* = DHCP server IP Address.
- Step 3** Enter **show wlan** to verify that you have a DHCP server assigned to the WLAN.
- Step 4** Enter **ping dhcp-ip-address** to verify that the WLAN can communicate with the DHCP server.
-

Customizing the Web Authentication Login Screen

Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic (except DHCP-related packets) from a particular client until that client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define usernames and passwords for each client, and when clients attempt to join the wireless LAN, they must enter a valid username and password when prompted by a login window. These sections describe the default web authentication operation and how to customize the Web Authentication Login window.

- [Default Web Authentication Operation, page 5-9](#)
- [Customizing Web Authentication Operation, page 5-11](#)
- [Example: Sample Customized Web Authentication Login Window, page 5-15](#)

Default Web Authentication Operation

When web authentication is enabled, clients might receive a web-browser security alert the first time that they attempt to access a URL. [Figure 5-1](#) shows a typical security alert.

Figure 5-1 Typical Web-Browser Security Alert



Figure 5-2 After the client user clicks **Yes** to proceed (or if the client’s browser does not display a security alert) the web authentication system redirects the client to a login window.
Typical Web Authentication Login Window

The client must respond with a username and password that you define using the Local Net Users > New Web User page, or using the **config netuser add** CLI command.

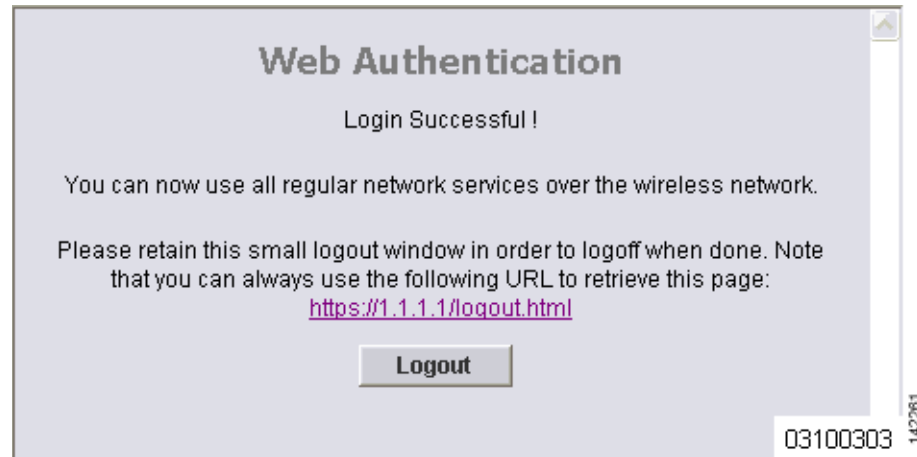
The default Web Authentication Login window contains Cisco WLAN Solution-specific text and a logo in four customizable areas:

- The Cisco WLAN Solution logo in the upper-right corner can be hidden.
- The window title, “Welcome to the Cisco WLAN Solution wireless network.”
- The message “Cisco WLAN Solution is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.”
- A blank area on the right side of the screen for a logo or other graphic.

The “[Customizing Web Authentication Operation](#)” section explains how to customize the Cisco WLAN Solution logo, window title, message, and logo.

When the client enters a valid username and password, the web authentication system displays a successful login window and redirects the authenticated client to the requested URL. [Figure 5-3](#) shows a typical successful login window.

Figure 5-3 Typical Successful Login Window



The default login successful window contains a pointer to a virtual gateway address URL, redirect <https://1.1.1.1/logout.html>. You define this redirect through the Virtual Gateway IP Address parameter in the configuration wizard, the Virtual Gateway Address parameter on the Interfaces GUI page, or by entering the **config interface create** command in the CLI.

Customizing Web Authentication Operation

This section explains how to customize web authentication operation using the controller CLI. These sections describe the customization tasks:

- [Hiding and Restoring the Cisco WLAN Solution Logo, page 5-11](#)
- [Changing the Web Authentication Login Window Title, page 5-11](#)
- [Changing the Web Message, page 5-12](#)
- [Changing the Logo, page 5-12](#)
- [Creating a Custom URL Redirect, page 5-14](#)
- [Verifying Web Authentication Changes, page 5-14](#)

Hiding and Restoring the Cisco WLAN Solution Logo

Use this command to delete or restore the Cisco WLAN Solution logo:

```
config custom-web weblogo {disable | enable}
```

Changing the Web Authentication Login Window Title

Use this command to change the Web Authentication Login window title:

```
config custom-web webtitle title
```

Use this command to reset the Web Authentication Login window title back to the default setting:

```
clear webtitle
```

Changing the Web Message

Use this command to change the Web Authentication Login window message:

```
config custom-web webmessage message
```

To reset the Web Authentication Login window message to the Cisco WLAN Solution default (“Cisco WLAN Solution is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work”), use this command:

```
clear webmessage
```

Changing the Logo

These sections explain how to change the logo on the right side of the Web Authentication Login window:

- [Preparing the TFTP Server, page 5-12](#)
- [Copying the Logo or Graphic to the TFTP Server, page 5-12](#)
- [Downloading the Logo or Graphic, page 5-13](#)
- [Hiding the Logo, page 5-13](#)

Preparing the TFTP Server

Follow these steps to prepare a TFTP server to load the logo:

-
- Step 1** Make sure you have a TFTP server available to load the logo.
- If you are downloading through the Service port, the TFTP server **MUST** be on the same subnet as the Service port, because the Service port is not routable.
 - If you are downloading through the DS (Distribution System) network port, the TFTP server can be on the same or a different subnet, because the DS port is routable.
- Step 2** On the CLI, enter **ping ip-address** to ensure that the controller can contact the TFTP server.



Note The TFTP server cannot run on the same computer as WCS. WCS and the TFTP server use the same communication port.

Copying the Logo or Graphic to the TFTP Server

Follow these steps to copy the logo to the TFTP server:

-
- Step 1** Create a logo in .JPG, .GIF, or .PNG format with a maximum file size of 30 kilobits. For the best fit in the space available, make the logo around 180 pixels wide and 360 pixels high.
- Step 2** Make sure the image filename does not contain spaces.
- Step 3** Copy the image file to the default directory on your TFTP server.
-

Downloading the Logo or Graphic

Follow these steps to download the image file to the controller:

- Step 1** On the CLI, enter **transfer download start** and answer **n** to the prompt to view the current download settings:

```
transfer download start
Mode..... TFTP
Data Type..... Code
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... <directory path>
TFTP Filename..... <filename.jpg|.gif|.png>
Are you sure you want to start? (y/n) n
Transfer Canceled
>
```

- Step 2** Use these commands to change the download settings:

```
transfer download mode tftp
transfer download datatype image
transfer download serverip tftp-server-ip-address
transfer download filename {filename.gif|filename.jpg|filename.png}
transfer download path absolute-tftp-server-path-to-file
```



Note Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

- Step 3** Enter **transfer download start** to view the updated settings, and answer **y** to the prompt to confirm the current download settings and start the download:

```
transfer download start
Mode..... TFTP
Data Type..... Login Image
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... <directory path>
TFTP Filename..... <filename.jpg|.gif|.png>
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Image transfer starting.
Image installed.
```

Hiding the Logo

To remove the logo from the Web Authentication Login window, enter **clear webimage**.

Creating a Custom URL Redirect

Use this command to redirect all web authentication clients to a specific URL (including http:// or https://) after they authenticate:

```
config custom-web redirecturl url
```

For example, if you want to redirect all clients to www.AcompanyBC.com, use this command:

```
config custom-web redirecturl www.AcompanyBC.com
```

To change the redirect back to the default setting, enter **clear redirect-url**.

Verifying Web Authentication Changes

Enter **show custom-web** to verify your web authentication operation changes. This example shows the output from the command when the web authentication settings are at defaults:

```
>show custom-web
Cisco Logo..... Enabled
CustomLogo..... Disabled
Custom Title..... Disabled
Custom Message..... Disabled
Custom Redirect URL..... Disabled
External Web Authentication Mode..... Disabled
External Web Authentication URL..... Disabled
```

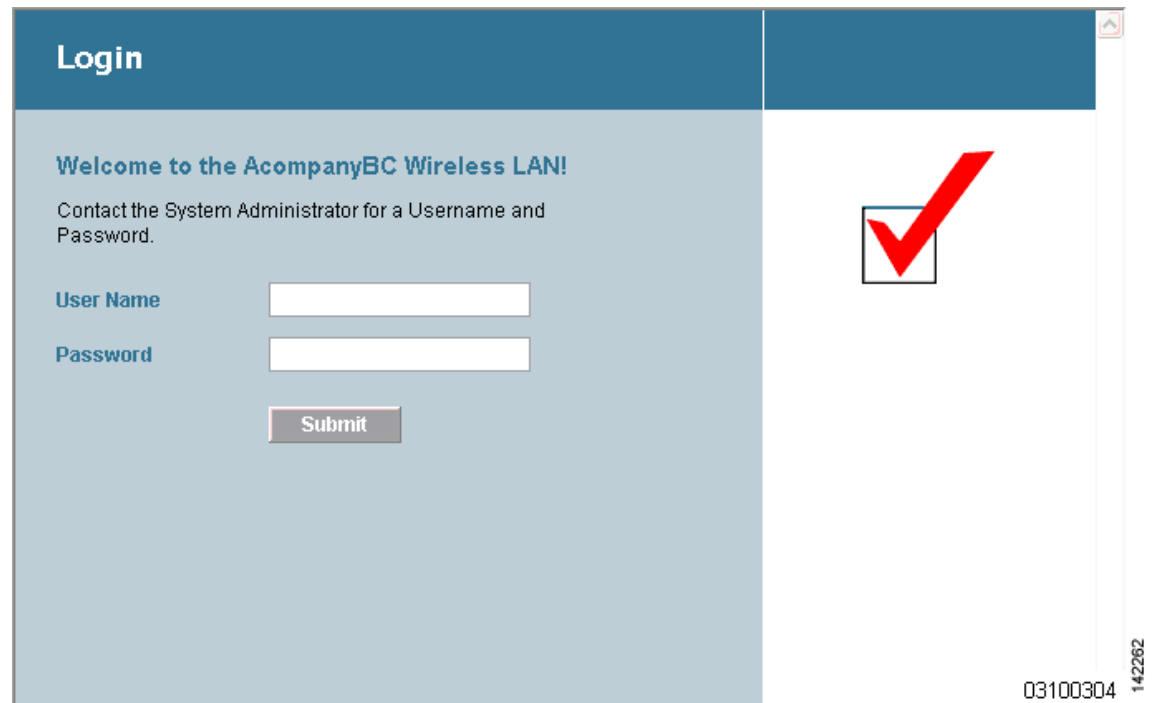
This example shows the output from the command when the web authentication settings have been modified:

```
>show custom-web
Cisco Logo..... Disabled
CustomLogo..... 00_logo.gif
Custom Title..... Welcome to the AcompanyBC Wireless LAN!
Custom Message..... Contact the System Administrator for a
Username and Password.
Custom Redirect URL..... http://www.AcompanyBC.com
External Web Authentication Mode..... Disabled
External Web Authentication URL..... Disabled
```

Example: Sample Customized Web Authentication Login Window

Figure 5-4 shows a customized Web Authentication Login window and the CLI commands used to create it.

Figure 5-4 Example of a Customized Web Authentication Login Window



These are the CLI commands used to create the window in Figure 5-4:

```
>config custom-web weblogo disable
>config custom-web webtitle Welcome to the AcompanyBC Wireless LAN!
>config custom-web webmessage Contact the System Administrator for a Username and
Password.
>transfer download start
Mode..... TFTP
Data Type..... Login Image
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... /
TFTP Filename..... Logo.gif
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Image transfer starting.
Image installed.
>config custom-web redirecturl http://www.AcompanyBC.com
>show custom-web
Cisco Logo..... Disabled
CustomLogo..... 00_logo.gif
Custom Title..... Welcome to the AcompanyBC Wireless LAN!
Custom Message..... Contact the System Administrator for a
Username and Password.
Custom Redirect URL..... http://www.AcompanyBC.com
External Web Authentication Mode..... Disabled
External Web Authentication URL..... Disabled
```

Configuring Identity Networking

These sections explain the Identity Networking feature, how it is configured, and the expected behavior for various security policies:

- [Identity Networking Overview, page 5-16](#)
- [RADIUS Attributes Used in Identity Networking, page 5-17](#)

Identity Networking Overview

In most wireless LAN systems, each WLAN has a static policy that applies to all clients associated with an SSID. Although powerful, this method has limitations since it requires clients to associate with different SSIDs to inherit different QoS and security policies.

However, the Cisco Wireless LAN Solution supports Identity Networking, which allows the network to advertise a single SSID but allows specific users to inherit different QoS or security policies based on their user profiles. The specific policies that you can control using identity networking include:

- **Quality of Service.** When present in a RADIUS Access Accept, the [QoS-Level](#) value overrides the QoS value specified in the WLAN profile.
- **ACL.** When the ACL attribute is present in the RADIUS Access Accept, the system applies the [ACL-Name](#) to the client station after it authenticates. This overrides any ACLs that are assigned to the interface.
- **VLAN.** When a VLAN [Interface-Name](#) or [VLAN-Tag](#) is present in a RADIUS Access Accept, the system places the client on a specific interface.



Note The VLAN feature only supports MAC filtering, 802.1X, and WPA. The VLAN feature does not support Web Auth or IPsec.

- Tunnel Attributes.



Note When any of the other RADIUS attributes in this section are returned, the Tunnel Attributes must also be returned.

In order for this feature to be enabled, on a per WLAN basis, the Enable AAA Override configuration flag must be enabled.

The Operating System's local MAC Filter database has been extended to include the interface name, allowing local MAC filters to specify to which interface the client should be assigned. A separate RADIUS server can also be used, but the RADIUS server must be defined using the Security menus.

RADIUS Attributes Used in Identity Networking

This section explains the RADIUS attributes used in Identity Networking.

QoS-Level

This attribute indicates the Quality of Service level to be applied to the mobile client's traffic within the switching fabric, as well as over the air. This example shows a summary of the QoS-Level Attribute format. The fields are transmitted from left to right.

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   | Length   |                               Vendor-Id   |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+
|                               QoS Level                               |
+-----+-----+-----+-----+-----+-----+

```

- Type – 26 for Vendor-Specific
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – Three octets:
 - 0 – Bronze (Background)
 - 1 – Silver (Best Effort)
 - 2 – Gold (Video)
 - 3 – Platinum (Voice)

ACL-Name

This attribute indicates the ACL name to be applied to the client. A summary of the ACL-Name Attribute format is shown below. The fields are transmitted from left to right.

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   | Length   |                               Vendor-Id   |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+
|                               ACL Name...                               |
+-----+-----+-----+-----+-----+-----+

```

- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0
- Value – A string that includes the name of the ACL to use for the client

Interface-Name

This attribute indicates the VLAN Interface a client is to be associated to. A summary of the Interface-Name Attribute format is shown below. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   |   Length   |   Vendor-Id   |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Interface Name... |
+-----+-----+-----+-----+-----+-----+

```

- Type – 26 for Vendor-Specific
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5
- Vendor length – >0
- Value – A string that includes the name of the interface the client is to be assigned to.



Note This Attribute only works when MAC Filtering is enabled, or if 802.1X or WPA is used as the security policy.

VLAN-Tag

This attribute indicates the group ID for a particular tunneled session, and is also known as the Tunnel-Private-Group-ID attribute.

This attribute might be included in the Access-Request packet if the tunnel initiator can predetermine the group resulting from a particular connection and should be included in the Access-Accept packet if this tunnel session is to be treated as belonging to a particular private group. Private groups may be used to associate a tunneled session with a particular group of users. For example, it may be used to facilitate routing of unregistered IP addresses through a particular interface. It should be included in Accounting-Request packets which contain Acct-Status-Type attributes with values of either Start or Stop and which pertain to a tunneled session.

A summary of the Tunnel-Private-Group-ID Attribute format is shown below. The fields are transmitted from left to right.

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|   Type   |   Length   |   Tag   |   String... |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 81 for Tunnel-Private-Group-ID.
- Length – >= 3

- Tag – The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. If the value of the Tag field is greater than 0x00 and less than or equal to 0x1F, it should be interpreted as indicating which tunnel (of several alternatives) this attribute pertains. If the Tag field is greater than 0x1F, it should be interpreted as the first byte of the following String field.
- String – This field must be present. The group is represented by the String field. There is no restriction on the format of group IDs.

Tunnel Attributes



Note

When any of the other RADIUS attributes in this section are returned, the Tunnel Attributes must also be returned.

Reference RFC2868 defines RADIUS tunnel attributes used for authentication and authorization, and RFC2867 defines tunnel attributes used for accounting. Where the IEEE 802.1X Authenticator supports tunneling, a compulsory tunnel may be set up for the Supplicant as a result of the authentication.

In particular, it may be desirable to allow a port to be placed into a particular Virtual LAN (VLAN), defined in IEEE8021Q, based on the result of the authentication. This can be used, for example, to allow a wireless host to remain on the same VLAN as it moves within a campus network.

The RADIUS server typically indicates the desired VLAN by including tunnel attributes within the Access-Accept. However, the IEEE 802.1X Authenticator may also provide a hint as to the VLAN to be assigned to the Supplicant by including Tunnel attributes within the Access-Request.

For use in VLAN assignment, the following tunnel attributes are used:

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Note that the VLANID is 12-bits, taking a value between 1 and 4094, inclusive. Since the Tunnel-Private-Group-ID is of type String as defined in RFC2868, for use with IEEE 802.1X, the VLANID integer value is encoded as a string.

When Tunnel attributes are sent, it is necessary to fill in the Tag field. As noted in RFC2868, section 3.1:

- The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. Valid values for this field are 0x01 through 0x1F, inclusive. If the Tag field is unused, it must be zero (0x00).
- For use with Tunnel-Client-Endpoint, Tunnel-Server-Endpoint, Tunnel-Private-Group-ID, Tunnel-Assignment-ID, Tunnel-Client-Auth-ID or Tunnel-Server-Auth-ID attributes (but not Tunnel-Type, Tunnel-Medium-Type, Tunnel-Password, or Tunnel-Preference), a tag field of greater than 0x1F is interpreted as the first octet of the following field.
- Unless alternative tunnel types are provided, (e.g. for IEEE 802.1X Authenticators that may support tunneling but not VLANs), it is only necessary for tunnel attributes to specify a single tunnel. As a result, where it is only desired to specify the VLANID, the tag field should be set to zero (0x00) in all tunnel attributes. Where alternative tunnel types are to be provided, tag values between 0x01 and 0x1F should be chosen.

