



amigopod



Cisco WLC Integration Guide

Revision Ver 0.93b by jhao

Date 23 Sept 2011

Copyright © 2011 Aruba Networks, Inc.

Aruba Networks HQ Aruba Networks Headquarters
1344 Crossman Ave
Sunnyvale, CA 94089-1113
United States of America

Web www.arubanetworks.com

Phone 1-866-WIFI-LAN

Table of Contents

Introduction	3
Test Environment	3
Integration	5
Cisco WLC Configuration	6
Step 1 – Create New VLAN (Optional)	7
Step 2 – Add IP Addressing to VLAN (Optional)	8
Step 3 – Create RADIUS Authentication Server	9
Step 4 – Create RADIUS Accounting Server	10
Step 5 – Create PreAuthentication Access Control List (Pre Auth ACL)	11
Step 6 – Create the new Wireless LAN	12
Step 7 – Configure the General WLAN settings	13
Step 8 – Configure the Security WLAN settings	14
Step 9 – Configure the AAA WLAN settings	15
Step 10 – Configure the AAA Override setting	16
Amigopod Configuration.....	17
Step1 – Create RADIUS NAS for Cisco WLC.....	18
Step 2 – Restart RADIUS Services	19
Step 3 – Configure Cisco Web Login Page	20
Step 4 – Confirm External Captive Portal URL	22
Step 5 – Create a test user account	23
Testing the Configuration	25
Step 1 - Connect to the Amigopod wireless network	25
Step 2 – Confirm DHCP IP Address received.....	26
Step 3 – Launch Web Browser and login	26
Step 4 – Confirm RADIUS debug messages on Amigopod	28

Introduction

This document outlines the configuration process on both the Cisco Wireless LAN Controller (WLC) and the Amigopod appliance to create a fully integrated Visitor Management solution. The solution leverages the captive portal functionality built into the Cisco WLC software image.

The captive portal functionality allows a wireless client to authenticate using a web-based portal. Captive portals are typically used in public access wireless hotspots or for hotel in-room Internet access. After a client associates to the wireless network, their device is assigned an IP address. The client must start a web browser and pass an authentication check before access to the network is granted.

Captive portal authentication is the simplest form of authentication to use and requires no software installation or configuration on the client. The username/password exchange is encrypted using standard SSL encryption.

However, portal authentication does not provide any form of encryption beyond the authentication process; to ensure privacy of client data, some form of link-layer encryption (such as WEP or WPA-PSK) should be used when sensitive data will be sent over the wireless network.

Amigopod extends the standard Cisco WLC captive portal functionality by providing many advanced features such as a fully branded user interface, SMS integration for delivery of receipts, bulk upload of visitors for conference management, self provisioning of users for public space environments to name a few.

Test Environment

The test environment referenced throughout this integration guide is based on an Cisco WLC 4402 controller. Although this low end hardware platform has been used, the testing and therefore this procedure is valid for all hardware variants from Cisco in its WLC range including the WiSM blade that installs as a module in the Catalyst 6500 switching platform.

The WLC range is based on the Cisco acquisition of Airespace and therefore this integration guide is valid for any solution based on the Airespace technology. Other Cisco wireless reference designs such as Autonomous IOS Access Points and the preceding WLSM architecture do not natively support the required Captive Portal functionality and therefore are not covered in this Integration Guide.

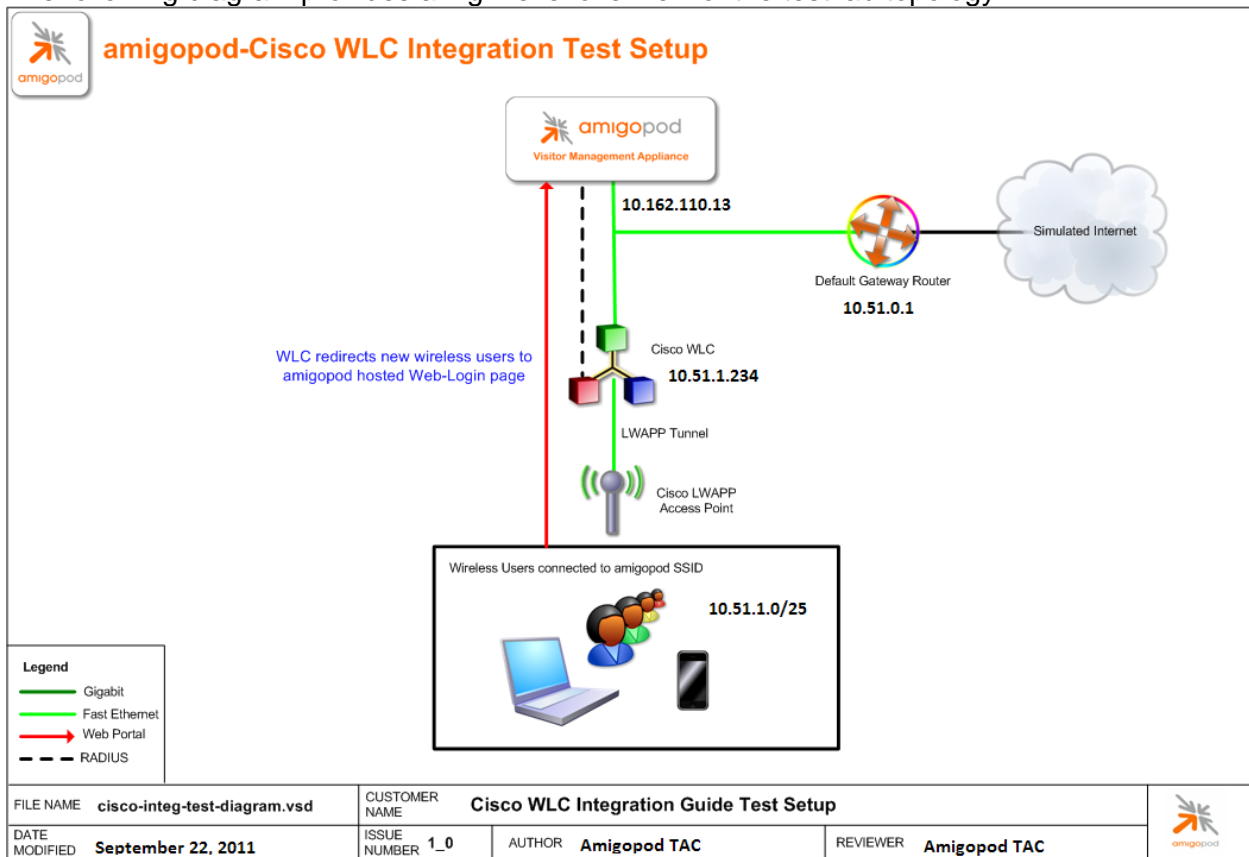
The following table shows the software versions used during the integration testing. This document will be updated in the future if changes in either Amigopod or Cisco subsequent releases affect the stability of this integration. It is advised that the customer always check for the latest integration guide available from either Amigopod or Cisco.

Dated Tested: September 2011
Amigopod Version: Kernel→3.3.5, Radius Services→ 3.3.1
Plugins Required: Standard build
Cisco WLC Version: 4.2.209.0
Integration: HTTP Captive Portal

An Amigopod VM Server was deployed in its own VLAN/subnet with layer 3 access to the LAN interface of the Cisco WLC controller. DHCP was provided on the Wireless Guest Network and routing was enabled between subnets

Cisco WLC IP Address 10.51.1.234
Internet Gateway Address 10.51.0.1
Amigopod IP Address 10.162.111.13
Amigopod RADIUS port Auth 1812 Acc 1813 (default settings)
DHCP Server 10.51.0.10
Client DHCP Range 10.51.1.1-128

The following diagram provides a high level overview of the test lab topology:



Integration

Although the Cisco WLC supports both internal and external Captive portal functionality, this integration guide will focus on the latter as the internal Captive portal dictates the use of the internal login page native to the controller. This login page is very basic and doesn't allow for the significant customization possible with the Amigopod Web Logins feature.

Note: Cisco now allows for fully customized captive portal pages to be uploaded to the controller and managed via templates on the Cisco WCS management platform but this process requires a significant amount of web design experience to produce a professional result. One of Amigopod's strongest features is the Skin Plugin technology where the presentation of the User Interface is separated from the mechanics of the underlying application. This allows Amigopod to supply end users with a ready branded Skin for all Amigopod interaction including both Visitor and Operator pages.

This integration guide will also leverage the Cisco WLC's ability to define and reference external RADIUS servers for the authentication and accounting of visitor accounts. In the standalone Cisco WLC Guest provisioning solution the local database in each controller is used to store user credentials, limiting the scalability of the solution to resources of the local deployment. With the introduction of Amigopod, all visitor accounts are created, authenticated and accounted for on the Amigopod internal RADIUS Server.

Cisco WLC Configuration

The following configuration procedure assumes that the Cisco WLC has been powered up and a basic IP configuration has been applied through the CLI to allow the Administrator to access the Web User Interface. The following table reviews the IP Addressing used in the example environment. This should be replaced with the site specific configuration information of each customer deployment:

Cisco WLC Address	10.51.1.234
Internet Gateway Address	10.51.0.1
Amigopod IP Address	10.162.110.13
Amigopod RADIUS port	Auth 1812 Acc 1813 (default settings)
DHCP Server	10.51.0.10
Client DHCP Range	10.51.1.1-128

Note: In this particular guide, we use the management interface as our WLAN interface. In an actual deployment, oftentimes you'll find a specific interface/VLAN created and designated for use with the Guest WLAN. These will be deployment specific details and the WLC configuration will need to be adjusted to accommodate the desired deployment configuration.

Step 1 - Create New VLAN (Optional)

A new vlan can to be created to bind to the new Wireless LAN that will be used for the Visitor users. From the *Controller*→*Interfaces* screen, click on the *Add* button and enter the new VLAN ID and name you wish to use and then click the *Apply* button.

This step is considered optional as depending on the complexity of the site deployment, the administrator may simply decide associated the new Wireless LAN with the default *Management* interface and all wireless traffic will be forwarded onto this LAN. The network design of each site will dictate whether a new VLAN is required for separation of traffic.

The configuration example used has taken this more simplistic approach of associated the new Wireless LAN with the default *Management* interface.

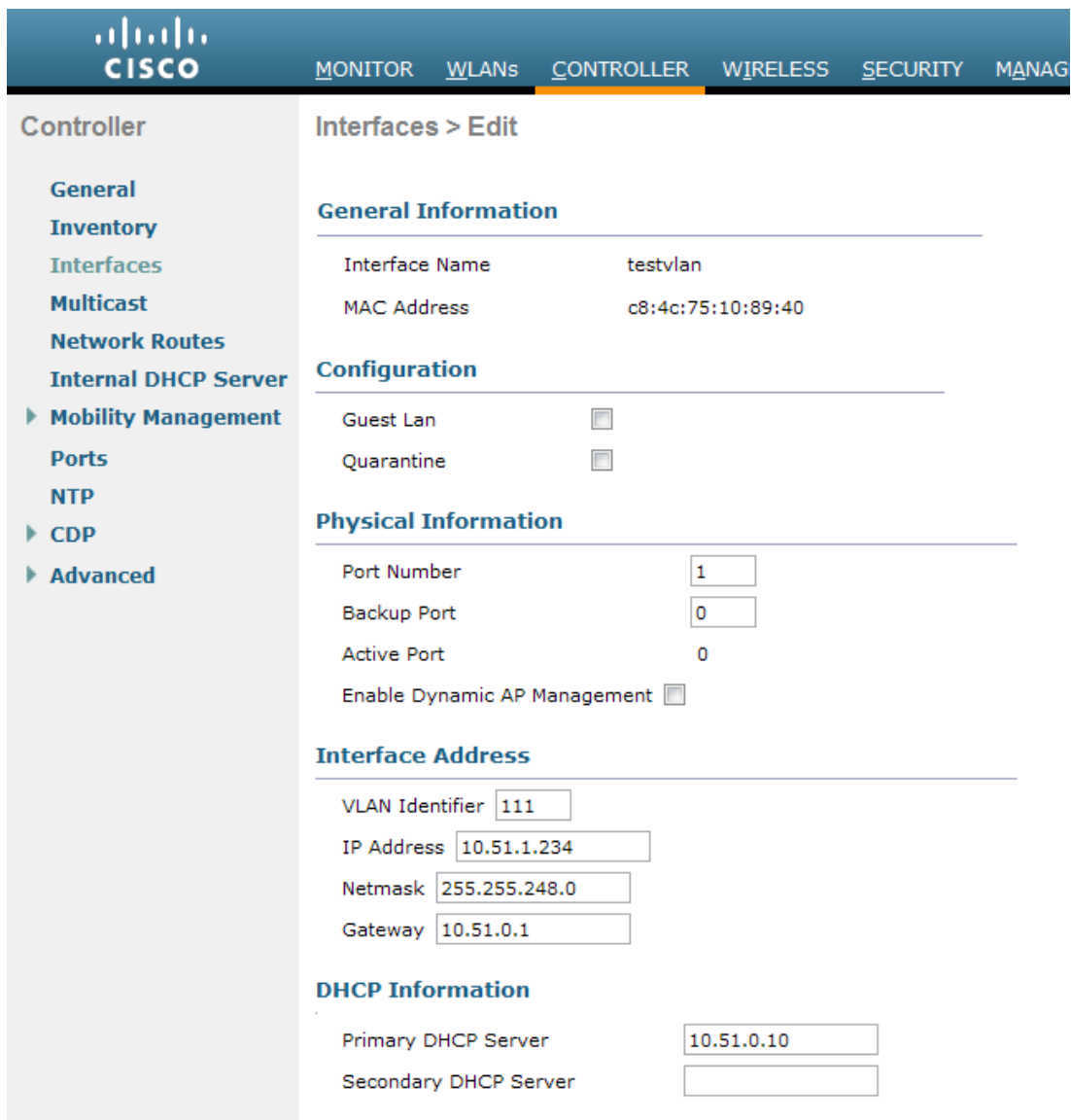


The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes the Cisco logo and tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANA. The left sidebar shows the Controller configuration menu with options: General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled 'Interfaces > New' and contains two input fields: 'Interface Name' with the value 'testvlan' and 'VLAN Id' with the value '111'.

IMPORTANT: Click the *Apply* button to save the changes.

Step 2 - Add IP Addressing to VLAN (Optional)

Now the VLAN has been created, an IP address needs to be assigned to the VLAN interface on the controller. This IP Address will not act as the default gateway for all wireless traffic on the Visitor SSID – this will be provided by an upstream router terminating the VLAN defined in the previous step. From the *Controller* → *Interfaces* screen, select the *Edit* button for the newly created VLAN (VLAN 111 in this optional example). Enter the designated IP Address details for the Wireless Visitor network. Make sure to enter the appropriate DHCP server details for the interface so the controller knows where to forward any wireless DHCP requests. Also define which of the front panel interfaces will be connected to this defined VLAN. These front panel interfaces are configured with dot1q trunking enabled by default.



The screenshot displays the Cisco Controller's web interface for configuring a VLAN interface. The navigation menu on the left includes options like General, Inventory, Interfaces, and Mobility Management. The main content area is titled 'Interfaces > Edit' and is divided into several sections: General Information, Configuration, Physical Information, Interface Address, and DHCP Information. The 'Interface Address' section contains input fields for VLAN Identifier (111), IP Address (10.51.1.234), Netmask (255.255.248.0), and Gateway (10.51.0.1). The 'DHCP Information' section has input fields for Primary DHCP Server (10.51.0.10) and Secondary DHCP Server.

General Information	
Interface Name	testvlan
MAC Address	c8:4c:75:10:89:40

Configuration	
Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>

Physical Information	
Port Number	1
Backup Port	0
Active Port	0
Enable Dynamic AP Management	<input type="checkbox"/>

Interface Address	
VLAN Identifier	111
IP Address	10.51.1.234
Netmask	255.255.248.0
Gateway	10.51.0.1

DHCP Information	
Primary DHCP Server	10.51.0.10
Secondary DHCP Server	

IMPORTANT: Click the *Apply* button to save the changes.

Step 3 - Create RADIUS Authentication Server

In order for the Cisco WLC to successfully authenticate the guest users that will be provisioned on the Amigopod system, a **RADIUS Authentication Server** needs to be defined on the controller. From the *Security*→*AAA*→*RADIUS* menu option, select *Authentication* and then click the *New* button in the top corner.

Enter the IP Address of your Amigopod deployment in the *Server IP Address* field. This can be found on the console of the Amigopod server. There is no need to change the default RADIUS *Port Number* as this is the default port used by Amigopod.

The screenshot shows the Cisco WLC configuration interface for creating a new RADIUS Authentication Server. The left sidebar shows the navigation menu with 'Security' expanded and 'RADIUS' selected. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

Server Index (Priority)	2
Server IP Address	10.162.110.13
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

IMPORTANT: Enter and **REMEMBER** the *Shared Secret* used for authenticating the controller to the Amigopod RADIUS server as this **MUST MATCH** the configured Shared Secret that will be input during the configuration of the Amigopod software.

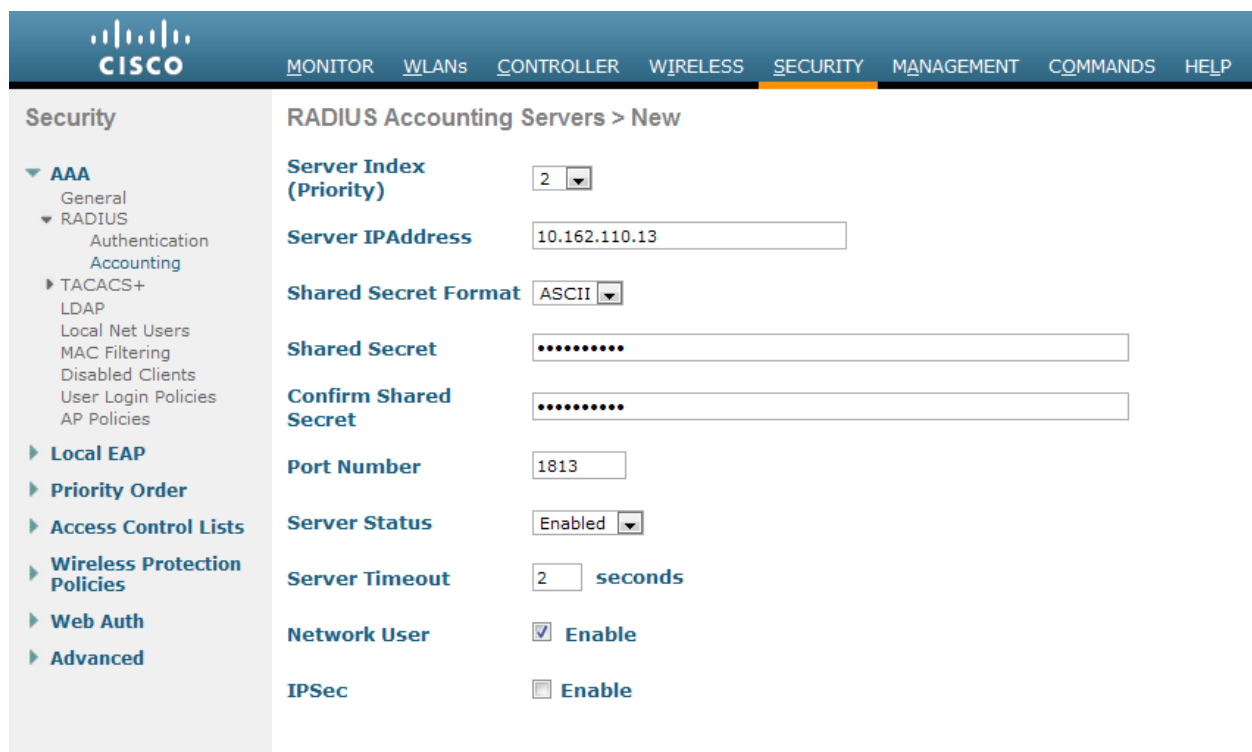
IMPORTANT: Please ensure that the **Network User** check box is selected so that this RADIUS server can be used to authenticate Clients connecting to the WLC.

IMPORTANT: Click the *Apply* button to save the changes.

Step 4 - Create RADIUS Accounting Server

In order for the Cisco WLC to successfully send accounting data associated with traffic being generated by the guest users, a **RADIUS Accounting Server** needs to be defined on the controller. From the *Security* → *AAA* → *RADIUS* menu option, select *Accounting* and then click the *New* button in the top corner.

Enter the IP Address of your Amigopod deployment in the *Server Address* field. This can be found on the console of the Amigopod server. There is no need to change the default RADIUS *Port Number* as this is the default port used by Amigopod.



The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, and HELP. The left sidebar shows the configuration tree with 'Security' expanded to 'AAA' > 'RADIUS' > 'Accounting'. The main content area is titled 'RADIUS Accounting Servers > New' and contains the following configuration fields:

Server Index (Priority)	2
Server IP Address	10.162.110.13
Shared Secret Format	ASCII
Shared Secret
Confirm Shared Secret
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

IMPORTANT: Enter and **REMEMBER** the *Shared Secret* used for authenticating the controller to the Amigopod RADIUS server as this **MUST MATCH** the configured Shared Secret that will be input during the configuration of the Amigopod software.

IMPORTANT: Please ensure that the **Network User** check box is selected so that this RADIUS server can be used to perform accounting for Clients connecting to the WLC

IMPORTANT: Click the *Apply* button to save the changes.

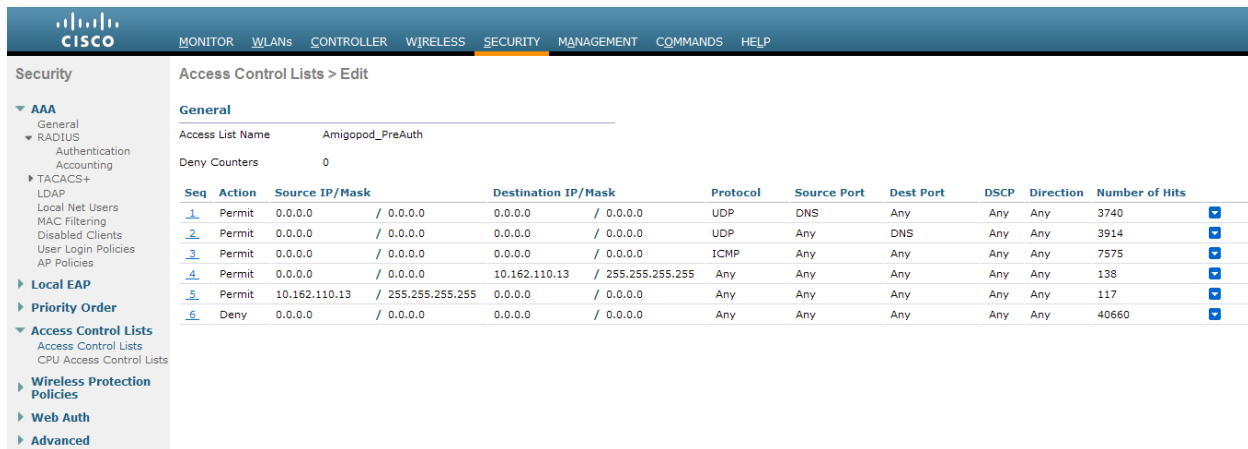
Step 5 - Create PreAuthentication Access Control List (Pre Auth ACL)

The PreAuth ACL controls the network access of a wireless visitor prior to being authenticated by Amigopod. This can often include a walled garden of local servers or other site specific hosts that Guests may be permitted access to without authentication.

In this guide, we will configure the minimum recommended number of ACLs to allow proper DNS lookup and redirection of HTTP/HTTPS requests to the Amigopod Captive Portal. The PreAuth ACL configured in this example only represented the minimum recommended ACLs and can be customized to the desired deployment depending on customer needs.

IMPORTANT: The Cisco ACL is a pure ACL implementation and is not a stateful firewall. Explicit rules for both inbound and outbound traffic must be defined otherwise you may encounter issues during testing.

From the *Security* → *Access Control Lists* menu option, select the *New* button from the top corner. Enter a name for the PreAuth ACL and click the *Apply* button to save the changes. Under the *Security* → *Access Control Lists* screen displayed from the previous step, click the highlighted name of the newly created ACL (*Amigopod_PreAuth* in the example).



The screenshot shows the Cisco configuration interface for the Amigopod_PreAuth ACL. The left sidebar shows the navigation menu with 'Security' selected. The main content area shows the 'Access Control Lists > Edit' page for the 'Amigopod_PreAuth' ACL. The 'General' tab is active, showing the 'Access List Name' as 'Amigopod_PreAuth' and 'Deny Counters' as '0'. Below this is a table of ACL rules with columns for Seq, Action, Source IP/Mask, Destination IP/Mask, Protocol, Source Port, Dest Port, DSCP, Direction, and Number of Hits. The rules are as follows:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	3740
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	3914
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	7575
4	Permit	0.0.0.0 / 0.0.0.0	10.162.110.13 / 255.255.255.255	Any	Any	Any	Any	Any	138
5	Permit	10.162.110.13 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	117
6	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	40660

As can be seen from the *Amigopod_PreAuth* ACL example above:

Rule 1 enables ICMP in any direction (Optional, good for troubleshooting)

Rules 2 and 3 enable DNS communication TO and FROM port 53 (DNS) of your DNS server to any port (the DNS client will generate the request from a random port). Without both rules, the client will receive a browser error indicating a timeout occurred and that the DNS name could not be resolved.

Rule 4 enables communication TO the amigopod server (10.162.110.13) NOTE: This rule can be further refined to restrict access FROM the guest network and or include protocol restrictions such as HTTP/HTTPS.

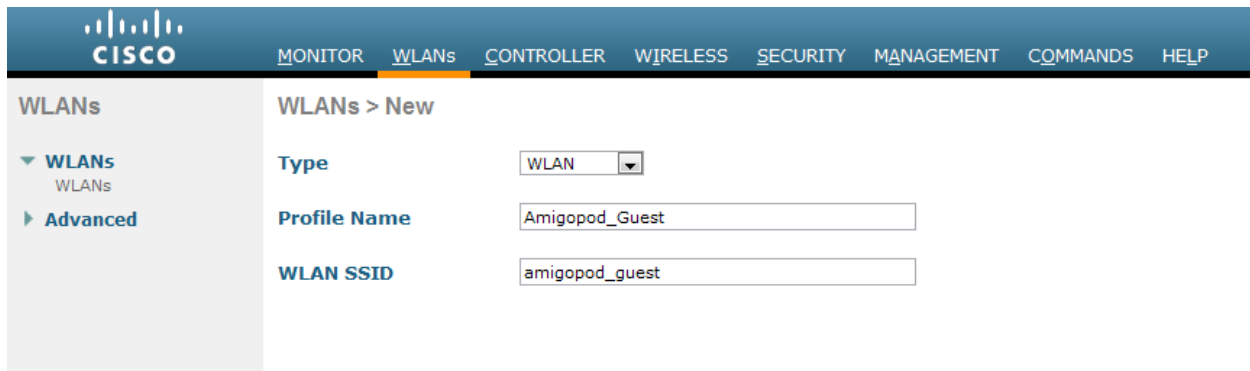
Rule 5 enables communication FROM the amigopod server (10.162.110.13) NOTE: This rule can be further refined to restrict access TO the guest network and or include protocol restrictions such as HTTP/HTTPS.

Rule 6 is a deny all statement that prevents all other traffic from the guest from reaching anything (Optional – there is an implicit deny all at the end of the ACL).

IMPORTANT: Remember to *Save Configuration* when done creating ACL rules.

Step 6 - Create the new Wireless LAN

A WLAN needs to be defined to service the Guests and in the example below you can see the configured ssid is *amigopod_guest*. Under the *WLANs menu option* select the *New...* button to display the configuration screen shown below.



The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes the Cisco logo and tabs for MONITOR, WLANs (selected), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. On the left, a sidebar shows 'WLANs' with sub-options for 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > New' and contains three configuration fields: 'Type' set to 'WLAN', 'Profile Name' set to 'Amigopod_Guest', and 'WLAN SSID' set to 'amigopod_guest'.

Configure the SSID *Profile Name* and the *WLAN SSID* setting to match your desired configuration for your deployment. In the example both the profile name and the SSID have been set to *Amigopod_Guest* and *amigopod_guest* respectively. Click the *Apply* button to commit the changes.

Note: For the purposes of this guide, the Layer 2 Security settings have been configured with Open authentication (no encryption). This may not be suitable for all deployments based on the desired Layer 2 security policy.

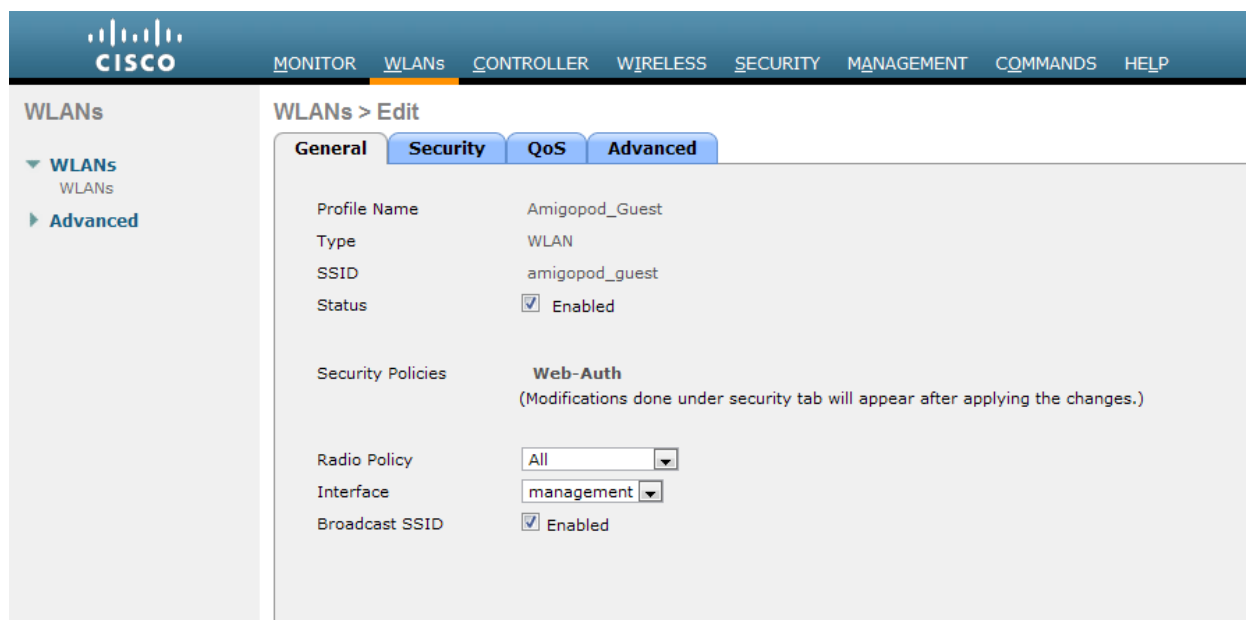
IMPORTANT: Click the *Apply* button to save the changes.

Step 7 - Configure the General WLAN settings

Under the *WLANs* → *Edit* → *General* settings tab the WLAN can be enabled and disabled and also associated with a specific VLAN.

IMPORTANT: This is where you will map the desired VLAN/subnet for the desired guest network to the WLAN. Select the desired VLAN via the Interface dropdown.

In the example, the default *management* VLAN is being used.



The screenshot displays the Cisco WLAN configuration interface. The top navigation bar includes the Cisco logo and menu items: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows a tree view with 'WLANs' expanded to 'Advanced'. The main content area is titled 'WLANs > Edit' and features four tabs: General, Security, QoS, and Advanced. The 'General' tab is active, showing the following configuration details:

Profile Name	Amigopod_Guest
Type	WLAN
SSID	amigopod_guest
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Web-Auth (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	management
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

IMPORTANT: Click the *Apply* button to save the changes.

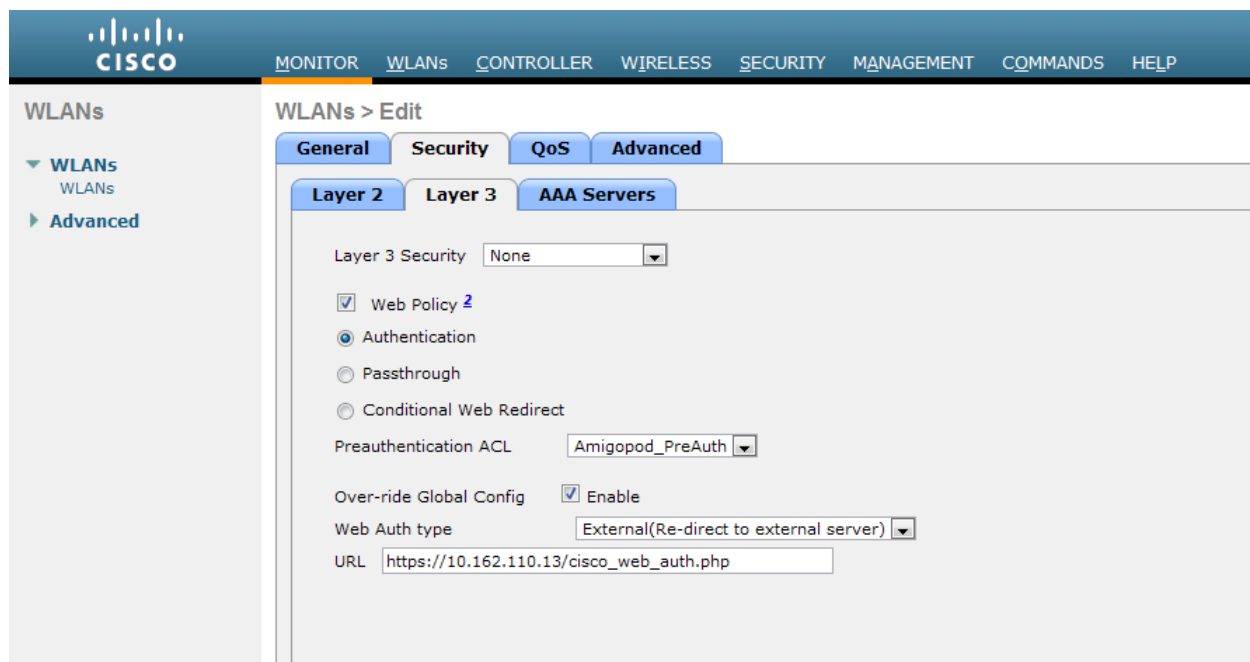
Step 8 - Configure the Security WLAN settings

Under the *WLANs* → *Edit* → *Security* tab WLAN security settings can be configured. Layer 2 encryption technologies such as WEP and WPA can be applied through the *Layer 2* sub tab and are specific to each site security policy and are therefore considered outside the scope of this configuration guide.

IMPORTANT: Under the *Security* → *Layer 3*, critical settings for the Captive Portal feature **must** be configured.

Now available in WLC code 4.2.x versions the *Over-ride global config* is now supported on a per SSID basis. In the example we will configure the *Web Auth Type* to **External** and enter the URL of the desired Amigopod captive portal login page (See Step 3 in the Amigopod Configuration section)

IMPORTANT: The *PreAuth ACL* must be configured to permit the traffic from the wireless client to be redirected to the Amigopod captive portal. Select the appropriate ACL from the drop down list. (previously created ACL in Step 5 – *Amigopod_PreAuth*)



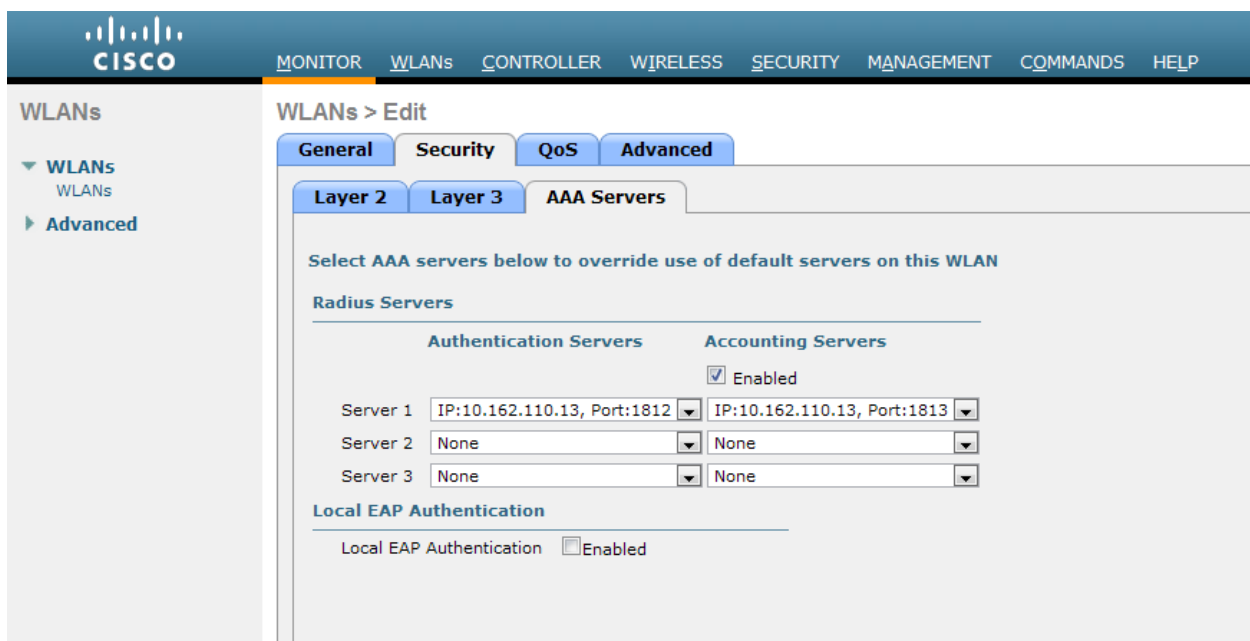
The screenshot displays the Cisco WLC configuration interface for editing WLAN settings. The navigation menu at the top includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows the WLANs configuration tree with options for WLANs and Advanced. The main content area is titled 'WLANs > Edit' and features tabs for General, Security, QoS, and Advanced. Under the Security tab, there are sub-tabs for Layer 2, Layer 3, and AAA Servers. The Layer 3 Security settings are visible, including a dropdown for Layer 3 Security (set to None), checkboxes for Web Policy (checked), Authentication (selected), Passthrough, and Conditional Web Redirect. The Preauthentication ACL is set to Amigopod_PreAuth. The Over-ride Global Config checkbox is checked and labeled 'Enable'. The Web Auth type is set to External(Re-direct to external server), and the URL is https://10.162.110.13/cisco_web_auth.php.

IMPORTANT: Click the *Apply* button to save the changes.

Step 9 - Configure the AAA WLAN settings

Under the *Security->AAA Servers* tab the desired RADIUS authentication and accounting servers need to be selected. These fields refer back to the RADIUS authentication and Accounting servers that were previously created in Step 3 and Step 4 (RADIUS Authentication and RADIUS Accounting)

IMPORTANT: Please ensure that the appropriate entries for *Authentication Servers* and *Accounting Servers* are selected as shown below and that the *Enabled* checkbox has been selected. Radius Authentication and Accounting features will not work properly unless they are configured correctly.



The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows WLANs > Edit. The main content area has tabs for General, Security, QoS, and Advanced. Under the Security tab, there are sub-tabs for Layer 2, Layer 3, and AAA Servers. The AAA Servers section is active, showing a heading "Select AAA servers below to override use of default servers on this WLAN". Below this is the "Radius Servers" section, which is divided into "Authentication Servers" and "Accounting Servers". There is a checked "Enabled" checkbox. The configuration table is as follows:

	Authentication Servers	Accounting Servers
Server 1	IP:10.162.110.13, Port:1812	IP:10.162.110.13, Port:1813
Server 2	None	None
Server 3	None	None

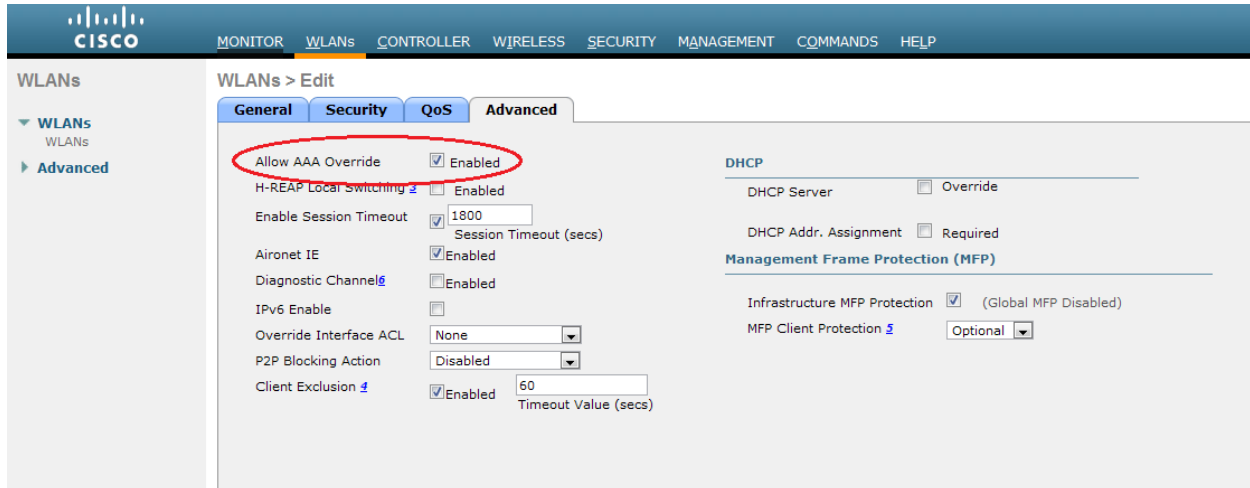
Below the Radius Servers section is the "Local EAP Authentication" section, which has an unchecked "Enabled" checkbox.

IMPORTANT: Click the *Apply* button to save the changes.

Step 10 - Configure the AAA Override setting

Under the *WLAN->Edit->Advanced* locate and enable the **Allow AAA Override** feature. This is critical for the Amigopod to be able to send an override to the Cisco WLC to terminate the user session based on the desired account lifetime in the Amigopod user interface.

IMPORTANT: Without AAA Override enabled you will not be able to disconnect users from the Amigopod user interface.



The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > Edit' and has four tabs: 'General', 'Security', 'QoS', and 'Advanced'. The 'Advanced' tab is selected. In the 'Advanced' section, the 'Allow AAA Override' checkbox is checked and highlighted with a red circle. Other settings include 'H-REAP Local Switching' (checked), 'Enable Session Timeout' (checked, 1800), 'Aironet IE' (checked), 'Diagnostic Channel' (checked), 'IPv6 Enable' (unchecked), 'Override Interface ACL' (None), 'P2P Blocking Action' (Disabled), and 'Client Exclusion' (checked, 60). On the right, the 'DHCP' section has 'DHCP Server' (unchecked), 'DHCP Addr. Assignment' (unchecked), and 'Management Frame Protection (MFP)' section with 'Infrastructure MFP Protection' (checked) and 'MFP Client Protection' (Optional).

IMPORTANT: Click the *Apply* button to save the changes.

Amigopod Configuration

The following configuration procedure assumes that the Amigopod software or appliance has been installed properly and the basic IP configuration has been applied through the setup wizard to allow the Administrator to access the Web User Interface. The following table reviews the IP Addressing used in the example environment but this would be replaced with the site specific configuration information of each customer deployment:

Cisco WLC Address	10.51.1.234
Internet Gateway Address	10.51.0.1
Amigopod IP Address	10.162.110.13
Amigopod RADIUS port	Auth 1812 Acc 1813 (default settings)
DHCP Server	10.51.0.10
Client DHCP Range	10.51.1.1-128

Please refer to the Amigopod Quick Start Guide for more information on the basic configuration of the Amigopod software.

Step1 - Create RADIUS NAS for Cisco WLC

In order for the Cisco WLC to authenticate users it **must** be able to communicate with the Amigopod RADIUS Server. In Step 3 of the Cisco WLC configuration, a RADIUS Authentication Server was defined. This step configures the matching Amigopod NAS definition for the Cisco WLC. The RADIUS key used in Step 3 **MUST** to be configured exactly the same here for the RADIUS transactions to be successful.

Navigate to *RADIUS* → *NAS List* and click on the **Create** button to create a new NAS device. Enter the IP Address of the Cisco WLC, select the *NAS Type* as **Cisco Systems (RFC3576 Support)** and enter the *Shared Secret* from Step 3 of the Cisco WLC Configuration into the *Shared Secret* field.

NOTE: You may now opt for Amigopod to automatically create a customized Web Login page for this NAS device at this time, or you may customize your own later.

- Advertising Services
- RADIUS
 - Start Here
 - Authentication
 - Database List
 - Dictionary
 - NAS List
 - Server Control
 - Server Configuration
 - User Roles
- Reporting
- Support
- Logout

Each network access server that will use this RADIUS server for authentication or accounting purposes should be defined here.

The screenshot shows the 'Create Network Access Server' form. The fields are as follows:

- Name:** Cisco WLC
- IP Address:** 10.51.1.234
- NAS Type:** Cisco Systems (RFC 3576 support)
- Shared Secret:** [Redacted]
- Confirm Shared Secret:** [Redacted]
- Description:** [Empty text area]
- Web Login:** Create a RADIUS Web Login page for this network access server
- Form Address:** Override vendors private IP

Buttons at the bottom: Create NAS Device, Reset Form, Cancel.

* required field

IMPORTANT: Click the *Create NAS Device* button to commit the change to the RADIUS database.


NOTE: The Amigopod Server will automatically attempt to ping the new NAS device. If ICMP is disabled or filtered then this may generate a warning. Please ensure that the Amigopod Server is able to communicate with the Cisco WLC before proceeding.

Step 2 - Restart RADIUS Services

IMPORTANT: A restart of the RADIUS Service is required for the new NAS configuration to take affect.

Click the **Restart RADIUS Server** link shown below and wait a few moments for the process to complete.

- Home
- Guests
- Administrator
- Customization
- Advertising Services
- RADIUS
 - Start Here
 - Authentication
 - Database List
 - Dictionary
 - [NAS List](#)
 - Server Control
 - Server Configuration
 - User Roles
- Reporting
- Support
- Logout

 The local RADIUS server needs to be restarted to complete the changes made.

Each network access server that will use this RADIUS server for authentication or accounting purposes should be defined here.

Name	Hostname	Type	Comments
Aruba650_Master	10.162.105.33	aruba_3576	
Cisco WLC	10.51.1.234	cisco_3576	

[Edit](#) [Delete](#) [Ping](#)

The Network Access Server is responding to pings:

```
PING 10.51.1.234 (10.51.1.234) 56(84) bytes of data:
64 bytes from 10.51.1.234: icmp_seq=1 ttl=249 time=1.51 ms

--- 10.51.1.234 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.517/1.517/1.517/0.000 ms
```

Step 3 - Configure Cisco Web Login Page

If you opted for a Web Login (Captive Portal) page to automatically be created for you during Step 1 you should now see it under *Customization -> Web Logins*. The automatically generated Cisco WLC web login page can be modified to suit the local deployment by adding custom HTML code or by defining a unique Amigopod skin for each captive portal page hosted by the Amigopod install as shown below:

From the *Customization -> Web Logins* page select the *Cisco WLC Login* entry and Click the *Edit* button.

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the amigopod you are able to provide a customised graphical login page for visitors accessing the network

Use this list view to define new web login pages, and to make changes to existing web login pages.

[Create a new web login page](#)

Name	Page Title	Page Name	Page Skin
Aruba650_Master Login Auto-generated web login for NAS Aruba650_Master	Login	welcome	(Default)
Cisco WLC Login Auto-generated web login for NAS Cisco WLC	Login	cisco_web_auth	(Default)
MOPS Enrollment Mobile Device Provisioning enrollment page.	Employee Smartphone and Tablet Registration	device_provisioning	(Default)

3 web logins [Reload](#) 20 rows per page

[Back to customization](#)

[Back to main](#)

IMPORTANT: The Cisco WLC Login template assumes the Virtual Interface address is the default Cisco setting of 1.1.1.1. You will need to update this to the actual configured Virtual Interface address per your actual WLC configuration.

NOTE: The Virtual Interface IP address is used only in communications between the controller and wireless clients. It never appears as the source or destination address of a packet that goes out a network port and onto the switched network. For the system to operate correctly, the virtual interface IP address must be configured (it cannot be 0.0.0.0), and no other device on the network may share the same address as the virtual interface (besides other Cisco WLC devices). Therefore, the virtual interface must be configured with an unassigned and unused IP address, such as 1.1.1.1. The virtual interface IP address is not pingable and should not exist in any routing table in your network. In addition, the virtual interface cannot be mapped to a backup port.

NOTE: All controllers within a mobility group must be configured with the same virtual interface IP address. Otherwise, inter-controller roaming may appear to work, but the hand-off will not complete, and the client loses connectivity for a period of time.

From the *RADIUS Web Login Editor* page you may customize your Web Login page and/or select the *Skin* that you would like presented as the branding for this particular Captive Portal page.

IMPORTANT: You should select a page name and make note of it. You will need to return to *Step 8 Configure the Security WLAN settings* of the *Cisco WLC Configuration* in order to update the configuration with the appropriate page. Please note that “.php” will automatically be appended to the end of your page name selected and that the URL entered in Step 8 of the *Cisco WLC Configuration* must include the “.php” suffix.

- Home
- Guests
- Administrator
- Customization
 - Start Here
 - Content Manager
 - Email Receipt
 - Fields
 - Forms & Views
 - Guest Manager
 - Guest Self-Registration
 - Hotspot Manager
 - IP Phones
 - Mobile Devices
 - Print Templates
 - SMS Receipt
 - [Web Logins](#)
- Advertising Services
- RADIUS
- Reporting
- Support
- Logout

Use this form to make changes to the RADIUS Web Login Cisco WLC Login.

RADIUS Web Login Editor	
* Name:	<input type="text" value="Cisco WLC Login"/> <small>Enter a name for this web login page.</small>
Page Name:	<input type="text" value="cisco_web_auth"/> <small>Enter a page name for this web login. The web login will be accessible from "page_name.php"</small>
Description:	<input type="text" value="Auto-generated web login for NAS Cisco WLC"/> <small>Comments or descriptive text about the web login.</small>
* Vendor Settings:	<input type="text" value="Cisco Systems"/> <small>Select a predefined group of settings suitable for standard network configurations.</small>
Address:	<input type="text" value="1.1.1.1"/> <small>Enter the IP address or hostname of the vendor's product here.</small>
Secure Login:	<input type="text" value="Use vendor default"/> <small>Select a security option to apply to the web login process.</small>
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials <small>In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.</small>

You may also modify the sample HTML in the *Header HTML*, *Footer HTML* and *Login Message* section to customize for your local environment.

IMPORTANT: Click the *Save Changes* button to commit the changes.

Step 4 - Confirm External Captive Portal URL


If you did not choose to manually configure a page name then the URL that needs to be configured in the Cisco WLC External Captive Portal section covered in *Step 8 Configure the Security WLAN settings* of the *Cisco WLC Configuration* can be determined by clicking on the test button shown on the screen below under the *Customization* → *Web Logins* screen:


- Home
- Guests
- Administrator
- Customization
 - Start Here
 - Content Manager
 - Email Receipt
 - Fields
 - Forms & Views
 - Guest Manager
 - Guest Self-Registration
 - Hotspot Manager
 - IP Phones
 - Mobile Devices
 - Print Templates
 - SMS Receipt
 - Web Logins
- Advertising Services
- RADIUS
- Reporting
- Support
- Logout




Many NAS devices support Web-based authentication for visitors.


By defining a web login page on the amigopod you are able to provide a customised graphical login page for visitors accessing the network


Use this list view to define new web login pages, and to make changes to existing web login pages.


 Modified RADIUS Web Login: Cisco WLC Login

 [Create a new web login page](#)

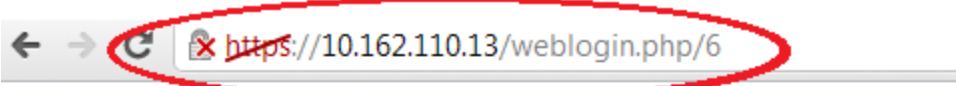
Name	Page Title	Page Name	Page Skin
 Aruba650_Master Login Auto-generated web login for NAS Aruba650_Master	Login	welcome	(Default)
 Cisco WLC Login Auto-generated web login for NAS Cisco WLC	Login		(Default)
 MDPS Enrollment Mobile Device Provisioning enrollment page.	Employee Smartphone and Tablet Registration	device_provisioning	(Default)

3 web logins  [Reload](#) 20 rows per page

 [Back to customization](#)

 [Back to main](#)

A test page will be presented and the URL can be seen in the address bar of your browser



Please login to the network using your amigopod username and password.

Login

* Username:

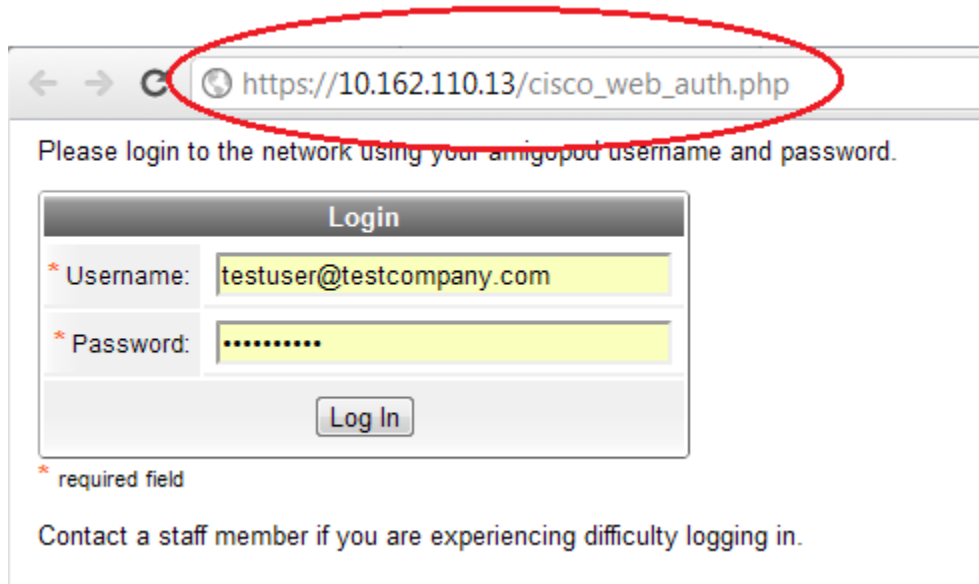
* Password:

* required field

Contact a staff member if you are experiencing difficulty logging in.

Note: Make note of the URL presented in the web browser after the *Test* button has been clicked. This URL is automatically generated but should remain static and will be required for configuration of the captive portal settings on the Cisco WLC.

Note: If you manually configured the page name in *Step 3 Configure Cisco WLC Login Page*. You should see the page name you selected in the URL. This URL will be required for configuration of the captive portal settings on the Cisco WLC.



← → ↻ https://10.162.110.13/cisco_web_auth.php

Please login to the network using your amigopod username and password.

Login

* Username:

* Password:

* required field

Contact a staff member if you are experiencing difficulty logging in.

Step 5 - Create a test user account

Within the Amigopod RADIUS Server a test user account can be created using the Amigopod *Guest Account Manager*. From the *Guest Account Management* menu, select the *Create New Guest Account* option. Enter the test user details as detailed on the form below and click the *Create Account* button to save the new test user account.

Guest Account Management

Use the commands below to manage your network's guest user accounts.

- Create New Guest Account**
Set up a new account for guest access to your network.
- Create Multiple Guest Accounts**
Create multiple guest accounts, each with a randomly-assigned username and password.
- List Guest Accounts**
View a list of all current guest accounts. You can modify and remove individual user accounts here.
- Edit Multiple Guest Accounts**
View a list of all current guest accounts. You can modify and

Note: Make note of the randomly generated *Visitor Password* as this will be required during the integration testing. You may edit this password by going to *List Accounts* and editing the account and change the password to a more user friendly string.

New guest account being created by **admin**.

New Visitor Account

* Sponsor's Name:
Name of the person sponsoring this visitor account.

* Visitor's Name:
Name of the visitor.

* Company Name:
Company name of the visitor.

* Email Address:
The visitor's email address. This will become their username to log into the network.

Account Activation:
Select an option for changing the activation time of this account.

Account Expiration:
Select an option for changing the expiration time of this account.

* Expire Action:
Select an option for controlling the expiration of this account. Note that a logout can only occur if the NAS is RFC-3576 compliant.

* Account Role:
Role to assign to this visitor account.

Password: **5=Vh**

* Terms of Use: I am the sponsor of this visitor account and accept the [terms of use](#)

IMPORTANT: The new Guest **USERNAME** will be their **Email Address**.

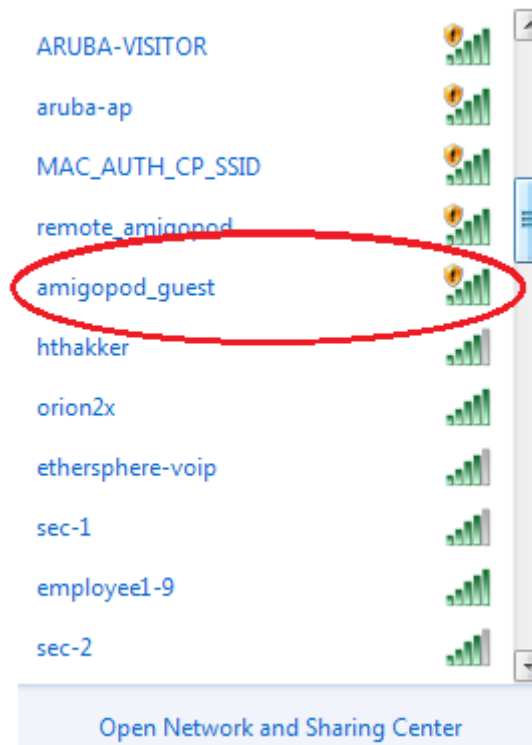
Testing the Configuration

Now that the configuration of both the Cisco WLC and the Amigopod solution is complete, the following steps can be followed to verify the setup.

Step 1 - Connect to the Amigopod wireless network

Use a test laptop to attempt to connect to the advertised *amigopod_guest* wireless network. The screen capture below shows the interface used on a Windows 7 based laptop. Although the process differs from laptop to laptop depending on the wireless card drivers installed and different operating systems in use, the basic premise of connecting to the Guest Wireless network should be fundamentally the same. Refer to your laptop manufacturer's documentation on the procedure for connecting to wireless networks if you experience an issue connecting to the guest network..

Note: If the *amigopod_guest* wireless network is not visible from the test laptop, double check the configuration of the Cisco WLC and potentially source a second wireless test device to see if the problem is laptop specific.



Step 2 - Confirm DHCP IP Address received

Using the Windows Command Prompt or equivalent in the chosen operating system, confirm that a valid IP Address has been received from the DHCP server defined on the Cisco WLC.

Issue the *ipconfig* command from the Windows Command Prompt to display the IP information received from the DHCP process. As can be seen below on the Wireless adaptor an IP Address of *192.168.10.253* has been received.

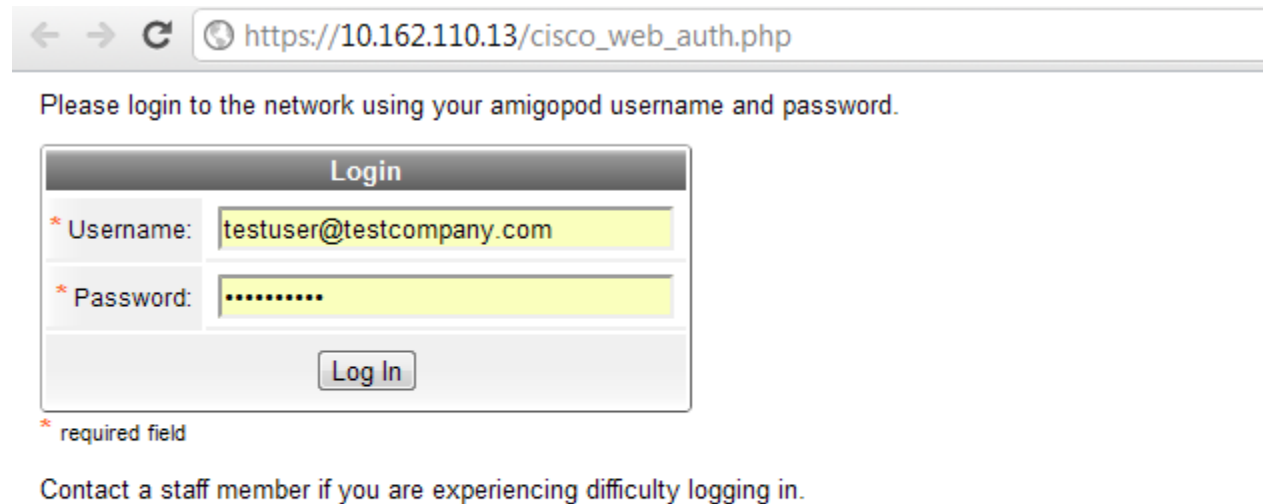
```
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : dev.airwave.com
Link-local IPv6 Address . . . . . : fe80::f8a9:eec4:8678:4308%12
IPv4 Address. . . . . : 10.51.1.115
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.51.0.1
```

Note: On Mac OS X and Linux operating system variants use a Terminal window and enter the *ifconfig* command to obtain the interface configuration information.

```
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    ether 60:33:4b:10:76:53
    inet6 fe80::6233:4bff:fe10:7653%en1 prefixlen 64 scopeid 0x5
    inet 10.51.1.120 netmask 0xffff0000 broadcast 10.51.255.255
    media: autoselect
    status: active
```

Step 3 - Launch Web Browser and login

When the web browser on the test laptop is launched the Cisco WLC will automatically capture the session and redirect the user to the Amigopod hosted login page as shown below:



Please login to the network using your amigopod username and password.

Login	
* Username:	testuser@testcompany.com
* Password:	*****
<input type="button" value="Log In"/>	

* required field

Contact a staff member if you are experiencing difficulty logging in.

Enter the test user credentials you noted in *Step 5 Create a test user account* of the Amigopod configuration instructions and click *Login*.

At this point the test user should be successfully authenticated and allowed onto the network.

COMMON TROUBLESHOOTING ISSUES:

DNS: If the client is unable to resolve the DNS entry of the initial http request then the redirect will not function properly. Please ensure that the client (and DNS Server) is able to resolve DNS lookups and that the ACL is configured properly to allow communication **TO** and **FROM** the DNS server to the Guest Network.

WEB BROWSER: Common Web browser issues include the web browser home page set to intranet site not available in guest network DNS. Also common issues involve Proxy Server configurations in browser using non standard HTTP ports.


Step 4 - Confirm RADIUS debug messages on Amigopod


Once the test laptop has successfully authenticated and now able to browse the Internet, an entry should appear in the RADIUS logs confirming the positive authentication of the test user – in the example: testuser@testcompany.com.


Select the *RADIUS*→*Server Control* menu option and the following screen should be displayed showing the status of the RADIUS server and a tail of the log file, including an entry for the positive authentication transaction.


- Home
- Guests
- Administrator
- Customization
- Advertising Services
- RADIUS
 - Start Here
 - Authentication
 - Database List
 - Dictionary
 - NAS List
 - **Server Control**
 - Server Configuration
 - User Roles
- Reporting
- Support
- Logout


Control the local RADIUS server using these command links.


 The RADIUS server is currently running.

 **Restart RADIUS Server**
Restart the local RADIUS server.

 **Stop RADIUS Server**
Stop the local RADIUS server.

 **Debug RADIUS Server**
Run the local RADIUS server and see detailed log output.

 **View Failed Authentications**
View a list of recent failed authentications.

 **Test RADIUS Authentication**
Check a username and password, or verify the RADIUS attributes for a user role.

RADIUS Server Time

The RADIUS server time is currently: **Fri Sep 23 2011 17:35:09 GMT-0700 (Pacific Daylight Time) -0700**

RADIUS Log Snapshot

The most recent entries in the RADIUS server log file are shown below.

```
Fri Sep 23 17:34:57 2011 : Auth: Login OK: [testuser@testcompany.com] (from client Cisco WLC port 0 cli 10.51.1.120)
```

This is a useful tool to remember when troubleshooting user authentication issues. A more advanced debugging tool is also available from this screen using the *Debug RADIUS Server* feature.