

Cisco (WLC managed)

Modified on: Wed, 19 Aug, 2015 at 9:48 AM

IMPORTANT NOTICE: Your device must be running WLC 7.6 firmware or above to continue.

Open a web browser and log in to your Cisco WLC interface

Click on "Security" on the top menu and then "Radius" on the left menu

RADIUS Authentication Servers

Call Station ID Type [?](#)

Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
--------------	------------	--------------	----------------	------	-------	--------------

Click "AAA Servers" on the left menu and then under RADIUS choose "Authentication". Set the correct settings:

- **Called Station ID Type:** select **AP MAC Address** from the drop down menu
- **MAC Delimiter:** select **Hyphen**

Click the "New" button at the top right and configure with the below settings:

RADIUS Authentication Servers > New

Server Index (Priority)	1 ▼
Server IP Address	[.....]
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 type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

- **Server IP Address:** *insert radius_server_ip here*
- **Shared Secret Format:** ASCII
- **Shared Secret:** *insert radius_secret here*
- **Confirm Shared Secret:** *insert radius_secret here*
- **Port:** enter 1812
- **Server Status:** Enabled
- **Network User:** Unticked (Disabled)
- **Management:** Unticked (Disabled)

Press **Apply** to Save

Click the "New" button again at the top right and configure with the below settings:

- **Server IP Address:** *insert radius_server2_ip here*
- **Shared Secret Format:** ASCII
- **Shared Secret:** *insert radius_secret here*
- **Confirm Shared Secret:** *insert radius_secret here*
- **Port:** enter 1812
- **Server Status:** Enabled
- **Network User:** Unticked (Disabled)
- **Management:** Unticked (Disabled)

Press **Apply** to Save

Click on "**Accounting**" on the left, "**New**" at the top right and configure with the below settings:

RADIUS Accounting Servers > New

Server Index (Priority)	<input type="text" value="1"/>
Server IP Address	<input type="text" value="..."/>
Shared Secret Format	<input type="text" value="ASCII"/>
Shared Secret	<input type="password" value="....."/>
Confirm Shared Secret	<input type="password" value="....."/>
Port Number	<input type="text" value="1813"/>
Server Status	<input type="text" value="Enabled"/>
Server Timeout	<input type="text" value="2"/> seconds
Network User	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

- **Server IP Address:** *insert radius_server_ip here*
- **Shared Secret Format:** ASCII
- **Shared Secret:** *insert radius_secret here*
- **Confirm Shared Secret:** *insert radius_secret here*
- **Port:** enter **1813**
- **Server Status:** Enabled
- **Network User:** Unticked (Disabled)

Press **Apply** to Save

Click the "**New**" button again at the top right and configure with the below settings:

- **Server IP Address:** *insert radius_server2_ip here*
- **Shared Secret Format:** ASCII
- **Shared Secret:** *insert radius_secret here*
- **Confirm Shared Secret:** *insert radius_secret here*
- **Port:** enter **1813**
- **Server Status:** Enabled
- **Network User:** Unticked (Disabled)

Press **Apply** to Save

Click "**Access Control Lists**" on the left menu and then "**New**", and configure with the settings:

- **Access Control List Name:** Guest Wi-Fi
- **ACL Type:** IPv4

Press **Apply** to Save

Then, click on the ACL you just created (blue link). Click on "**Add New Rule**" and enter the following:

- **Sequence:** 1
- **Source:** IP Address
- **IP Address:** *insert walled_garden_ip here*
- **Netmask:** 255.255.255.255
- **Action:** Permit

Press **Apply** to Save

Click "**Add New Rule**" and enter the following:

- **Sequence:** 2
- **Destination:** IP Address
- **IP Address:** *insert walled_garden_ip here*
- **Netmask:** 255.255.255.255
- **Action:** Permit

Press **Apply** to Save

Click "**Add New Rule**" and enter the following:

- **Sequence:** 3
- **Source:** IP Address
- **IP Address:** *insert walled_garden2_ip here*
- **Netmask:** 255.255.255.255
- **Action:** Permit

Press **Apply** to Save

Click "**Add New Rule**" and enter the following:

- **Sequence:** 4

- **Destination:** IP Address
- **IP Address:** *insert walled_garden2_ip here*
- **Netmask:** 255.255.255.255
- **Action:** Permit

Press **Apply** to Save

Important Note - If you are using you APs in FlexConnect Mode then you will need to complete the previous steps under the "**FlexConnect ACLs**" Section instead of the "**Access Control Lists**"

From the left Hand Menu, click "**Web Auth**" on the left menu and enter the following:

Web Login Page

Web Authentication Type	External (Redirect to external server) ▼
Redirect URL after login	http://*Pre-defined URL*/access/?res=success
External Webauth URL	http://*Pre-defined URL*/access/

- **Web Authentication Type:** External
- **Redirect URL after login:** *insert redirect_url here*
- **External Webauth URL:** *insert access_url here*

Press **Apply** to Save

Click on "**WLANs**" at the top and then "**WLANs**" on the left hand menu, then select "**Create New**" and Click "**Go**" on the right to create a new profile.

WLANs

Current Filter: None

[\[Change Filter\]](#) [\[Clear Filter\]](#)

[Create N](#)

WLANs > New

Type	WLAN ▼
Profile Name	White Label WiFi
SSID	White Label WiFi
ID	5 ▼

Enter the following:

- **Type:** WLAN
- **Profile Name:** Guest Wi-Fi
- **SSID:** Enter whatever wireless network name (SSID) you want

Press **Apply** to Save

Now click on the new SSID profile you just created to edit the settings, and on the **General Tab**:

WLANs > Edit 'White Label WiFi'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	White Label WiFi			
Type	WLAN			
SSID	White Label WiFi			
Status	<input checked="" type="checkbox"/> Enabled			
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)			
Radio Policy	All ▼			
Interface/Interface Group(G)	management ▼			
Multicast Vlan Feature	<input type="checkbox"/> Enabled			
Broadcast SSID	<input checked="" type="checkbox"/> Enabled			
NAS-ID	ciscowlc			

Enter the following details:

- **Status:** Enabled
- **Broadcast SSID:** Enabled

On the **Security** tab, then the **Layer 2** tab

Enter the following details:

- **Layer 2 Security:** None

On the **Layer 3** tab:

- **Layer 3 Security:** Web Policy
- **Authentication:** Ticked (Enabled)
- **Pre-authentication ACL (IPv4):** Guest Wi-Fi

Important Note - Again if you are using your APs in Flex Connect Mode then you will need to use the drop down box next too "**WebAuth FlexACL**" for the right policy to be applied correctly.

On the **AAA Servers** tab:

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface Enabled

Authentication Servers **Accounting Servers**

	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Server 1	IP: 192.168.1.10, Port: 1812	IP: 192.168.1.10, Port: 1813
Server 2	IP: 192.168.1.10, Port: 1812	IP: 192.168.1.10, Port: 1813
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Radius Server Accounting

Interim Update Interim Interval 600

- **Authentication Servers:** Enabled
- **Server 1:** IP: *insert radius_server_ip here*, Port: 1812
- **Server 2:** IP: *insert radius_server2_ip here*, Port: 1812
- **Accounting Servers:** Enabled
- **Server 1:** IP: *insert radius_server_ip here*, Port: 1813
- **Server 2:** IP: *insert radius_server2_ip here*, Port: 1813
- **Interim Update:** Ticked, Interval: 600
- **Authentication priority order for web-auth user (Not Used):** LOCAL, LDAP
- **Authentication priority order for web-auth user (Order Used For Authentication):** RADIUS

On the Advanced tab:

- **Allow AAA Override:** Enabled
- **Enable Session Timeout:** Ticked
- **Session Timeout (secs):** 43200

WLANs > Edit 'White Label WiFi'

General	Security	QoS	Policy-Mapping	Advanced
Allow AAA Override				<input checked="" type="checkbox"/> Enabled

Press **Apply** to Save

Select the **Management Tab** and then **HTTP-HTTPS** option from the left hand menu. Under WebAuth SecureWeb use the drop down box to select **Disabled**

Select the **Controller Tab** and change the option **Fast SSID change** to **Enabled**

Controller

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- ▶ Internal DHCP Server
- ▶ Mobility Management
- Ports
- ▶ NTP
- ▶ CDP
- ▶ IPv6
- ▶ mDNS
- ▶ Advanced

General

Name	<input type="text" value="ciscowlc"/>
802.3x Flow Control Mode	Disabled ▼
LAG Mode on next reboot	Disabled ▼ (LAG
Broadcast Forwarding	Enabled ▼
AP Multicast Mode ¹	Multicast ▼ <input type="text" value="239.0.0.0"/> Multicast Gro
AP Fallback	Enabled ▼
Fast SSID change	Enabled ▼
Default Mobility Domain Name	<input type="text" value="test"/>
RF Group Name	<input type="text" value="test"/>
User Idle Timeout (seconds)	<input type="text" value="3600"/>
ARP Timeout (seconds)	<input type="text" value="300"/>
Web Radius Authentication	PAP ▼
Operating Environment	Commercial (0 to 40 C)
Internal Temp Alarm Limits	0 to 65 C
WebAuth Proxy Redirection Mode	Disabled ▼
WebAuth Proxy Redirection Port	<input type="text" value="0"/>
Maximum Allowed APs ²	<input type="text" value="0"/>
Global IPv6 Config	Enabled ▼
HA SKU secondary unit	Disabled ▼

1. Multicast is not supported with FlexConnect on this platform.
 2. Value zero implies there is no restriction on maximum allowed APs.

Press **Apply** to Save

Finally, click **Save Configuration** at the top right to ensure all settings are saved. Once this is complete you will need to **reboot your controller** for all the features to work.

Troubleshooting

When setting up a Cisco WLC with the WiFi solution it's important to allow traffic to and from our Radius servers *insert radius_server_ip here* and *insert radius_server2_ip here* inbound and outbound using UDP on the clients Firewall, if this isn't completed then the authentication wont complete correctly.