

Cloudpath and Brocade/Motorola Wireless Integration

This document describes the steps required to integrate a Brocade/Motorola Wireless System with Ruckus Cloudpath. This is not a definitive guide as different situations and requirements require different configurations. This is a guide to get you as close as possible to a finished product.

For this setup, we are using Ruckus Cloudpath version 5.1 and Moto Wing 5.5 on a 7131 AP acting as a virtual controller. We will use an Onboarding SSID and a Secure SSID.

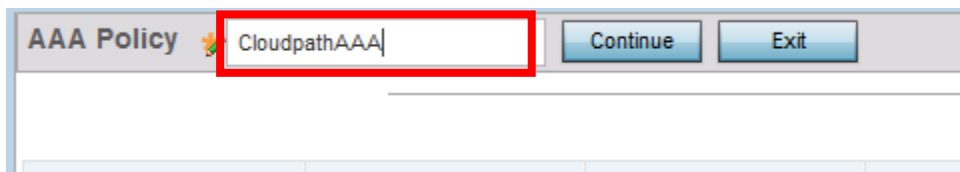
First we need to configure the AAA Policy in the Brocade/Motorola (Moto) controller.

Configure Cloudpath as a AAA Server in the controller:

Go to Configuration -> Network -> AAA Policy

Select Add at the bottom Right

Name the new AAA Policy and click continue

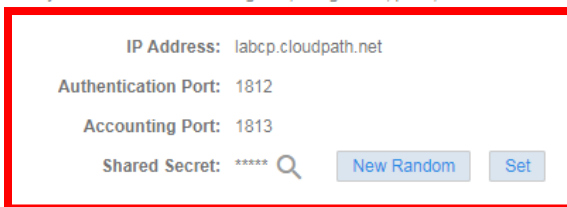


AAA Policy

All the information required on the next tabs comes from Cloudpath (Configuration -> Radius Server).

RADIUS Server Settings

This system will need to be configured, using the IP, ports, and shared secret below, as the RADIUS server within your WLAN infrastructure or wired switches.



IP Address: labcp.cloudpath.net
Authentication Port: 1812
Accounting Port: 1813
Shared Secret: *****

IP Address in Cloudpath is the hostname in Controller, Authentication Port, and Shared Secret. Click the spy glass to see and copy the key.

On the Radius Authentication Tab, click Add.

Authentication Server

Server Id 1 (1 to 6)

Settings

Host Hostname

Port (1 to 65,535)

Server Type

Secret Show

Request Proxy Mode

Proxy Mint Host

Request Attempts (1 to 10)

Request Timeout Seconds (1 to 60)

Retry Timeout Factor (50 to 200)

DSCP (0 to 63)

Network Access Identifier Routing

NAI Routing Enable

Realm

Realm Type Prefix Suffix

Strip Realm

OK Reset Exit

Click OK to Save and the Exit.

On the Radius Accounting Tab, Click Add.

Accounting Server

Server Id 1 (1 to 6)

Settings

Host cloudpath.netadmin.us Hostname Alias

Port 1813 (1 to 65,535)

Server Type Host

Secret ***** Show

Request Proxy Mode None

Proxy Mint Host

Request Attempts 3 (1 to 10)

Request Timeout 5 Seconds (1 to 60)

Retry Timeout Factor 100 (50 to 200)

DSCP 34 (0 to 63)

Network Access Identifier Routing

NAI Routing Enable

Realm

Realm Type Prefix Suffix

Strip Realm

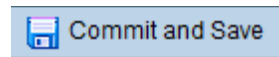
If a part of the username (prefix or suffix depending on realm_type) matches this parameter this server is selected for authentication.

OK Reset Exit

Click OK to Save and then Exit.

Click Exit to complete the AAA Policy.

Click Commit and Save to implement and save the changes.

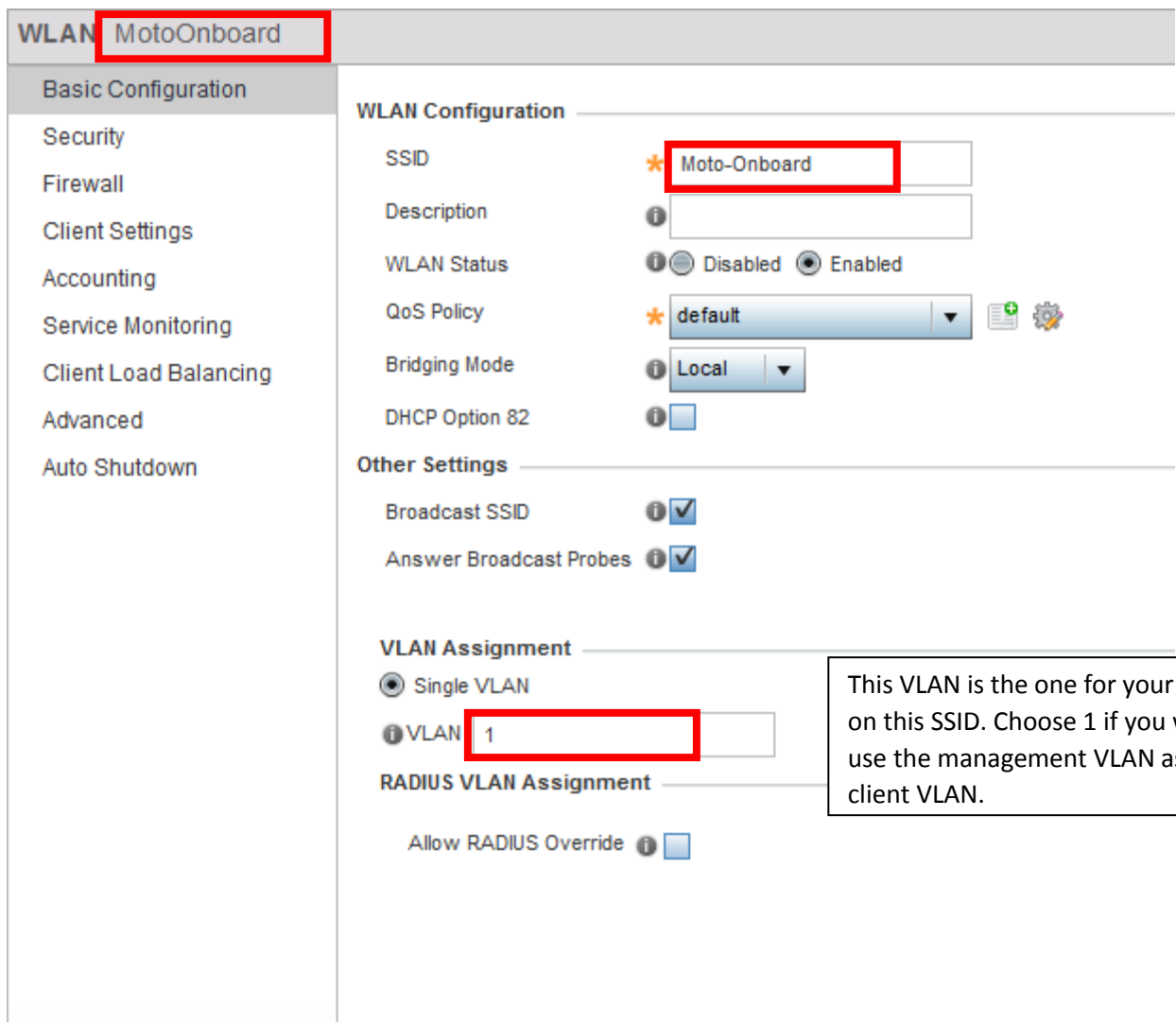


Next we will create an SSID to connect to and configure the settings for Cloudpath.

Note: If you have an existing SSID you want to use, just modify it for use with Cloudpath.

Create an Onboarding SSID:

On the Basic Configuration Tab:

A screenshot of a network configuration interface. The top bar shows "WLAN" and "MotoOnboard" (highlighted with a red box). A left sidebar lists configuration tabs: Basic Configuration, Security, Firewall, Client Settings, Accounting, Service Monitoring, Client Load Balancing, Advanced, and Auto Shutdown. The main area is titled "WLAN Configuration" and contains several sections: "WLAN Configuration" with fields for SSID (Moto-Onboard, highlighted with a red box), Description, WLAN Status (radio buttons for Disabled and Enabled), QoS Policy (default), Bridging Mode (Local), and DHCP Option 82; "Other Settings" with checkboxes for Broadcast SSID and Answer Broadcast Probes; "VLAN Assignment" with radio buttons for Single VLAN and a field for VLAN (1, highlighted with a red box); and "RADIUS VLAN Assignment" with a checkbox for Allow RADIUS Override. A callout box on the right states: "This VLAN is the one for your clients on this SSID. Choose 1 if you want to use the management VLAN as the client VLAN."

Click OK to Save

On the Security Tab

WLAN MotoOnboard

Basic Configuration

Security

Firewall

Client Settings

Accounting

Service Monitoring



Client Load Balancing

Advanced

Auto Shutdown

Select Authentication



EAP EAP-PSK EAP-MAC **MAC** PSK / None

AAA Policy  



Reauthentication (30 to 86,400)

Captive Portal

Enforcement Captive Portal Enable Captive Portal if P

Captive Portal Policy  

Passpoint Policy

Passpoint Policy  

MAC Registration

Enable

Radius Group Name

Expiry Time (1 to 1,500 days)

Agreement Refresh (0 to 144,000 days)

External Controller

Enable

Host Hostname

Proxy Mode

Select Encryption

TKIP-CCMP WEP 128 WEP 64 **Open**

WPA2-CCMP KeyGuard

No Encryption

Create a Captive Portal by clicking on the create icon next to the box. When created select it from the drop down. See the section below for instructions.

Click OK to Save

On the Accounting Tab

WLAN MotoOnboard

Basic Configuration
Security
Firewall
Client Settings
Accounting
Service Monitoring
Client Load Balancing
Advanced
Auto Shutdown

Syslog Accounting

Enable Syslog Accounting

Syslog Host Hostname ▾

Syslog Port

Proxy Mode ▾

Format ▾

Case ▾

RADIUS Accounting

Enable RADIUS Accounting

AAA Policy

Select the AAA Policy from the list below (policy shared with WLAN Authentication)

Cloudpath-AAA

[Create](#)
[Edit](#)

Click OK to Save and Exit

Create a Secure SSID:

Go to Configuration -> Wireless -> Wireless LANs

Click Add. On the Basic Configuration Tab:

The screenshot shows the configuration page for a WLAN named 'CP-Moto'. The interface is divided into several sections:

- WLAN Configuration:**
 - SSID: CP-Moto
 - Description: (empty)
 - WLAN Status: Enabled
 - QoS Policy: default
 - Bridging Mode: Local
 - DHCP Option 82: (unchecked)
- Other Settings:**
 - Broadcast SSID: (checked)
 - Answer Broadcast Probes: (checked)
- VLAN Assignment:**
 - Single VLAN: (selected)
 - VLAN: 1
- RADIUS VLAN Assignment:**
 - Allow RADIUS Override: (unchecked)

A red box highlights the SSID 'CP-Moto' and the VLAN '1' field. A text box on the right provides instructions: 'This VLAN is the one for your clients on this SSID. Choose 1 if you want to use the management VLAN as the client VLAN.'

Click OK to Save.

On the Security Tab:

WLAN CP-Moto

Basic Configuration

Security

Firewall

Client Settings

Accounting

Service Monitoring

Client Load Balancing

Advanced

Auto Shutdown

Select Authentication

EAP EAP-PSK EAP-MAC MAC PSK / None

AAA Policy

Reauthentication 3600 (30 to 8400)

Captive Portal

Enforcement Captive Portal Enable Captive Portal if Primary Authentication Fails

Captive Portal Policy

Passpoint Policy

Passpoint Policy

MAC Registration

Enable

Radius Group Name

Expiry Time (1 to 1,500 days)

Agreement Refresh (0 to 144,000 days)

External Controller

Enable

Host Hostname

Proxy Mode

This is the AAA Policy created earlier in the document.

Select Encryption

TKIP-CCMP

WPA2-CCMP

WEP 128

KeyGuard

WEP 64

Open

Click OK to Save.

On the Accounting Tab:

WLAN CP-Moto

- Basic Configuration
- Security
- Firewall
- Client Settings
- Accounting**
- Service Monitoring
- Client Load Balancing
- Advanced
- Auto Shutdown

Syslog Accounting

Enable Syslog Accounting

Syslog Host Hostname ▾

Syslog Port ▲ ▼

Proxy Mode ▾

Format ▾

Case ▾

RADIUS Accounting

Enable RADIUS Accounting

AAA Policy

Select the AAA Policy from the list below (policy shared with WLAN Authentication)

Cloudpath-AAA

[Create](#)
[Edit](#)

Click OK to Save and Exit

Create a Captive Portal:

This can also be done from Configuration -> Services -> Captive Portals

On the Basic Configuration Tab, complete the marked fields.

Captive Portal Policy Cloudpath-Portal

Basic Configuration Web Page

Settings

Captive Portal Server Mode Internal (Self) Centralized Centralized Controller

Hosting VLAN Interface (0 to 4,096)

Captive Portal Server Host Hostname

Connection Mode HTTP HTTPS

Simultaneous Users (1 to 8,192)

Security

AAA Policy

Access

Access Type No authentication required Generate Logging Record and Allow Access Custom User Information for RADIUS Authentication RADIUS Authentication email Email option is part of experimental feature

RADIUS Lookup Information

Terms and Conditions page

Client Settings

Radius VLAN Assignment

Post Authentication VLAN ID (1 to 4,096) Alias S

Client Access Time (10 to 10,080 minutes)

Inactivity Timeout Minutes (5 to 1,440)

DNS Whitelist

DNS Whitelist

Accounting

Enable RADIUS Accounting

OK Reset Exit

Create a Whitelist by clicking on the create icon next to the box. When created select it from the drop down. See the section below for instructions.

Click OK to Save

On the Web Page Tab, complete the marked fields.

Captive Portal Policy Onboarding-Portal ?

Basic Configuration **Web Page**

Web Page Source Internal Advanced Externally Hosted

| | |
|---------------------|---|
| Login URL | https://labcp.cloudpath.net/enroll/Lab/Moto/process?mac_address= |
| Agreement URL | https://labcp.cloudpath.net/enroll/Lab/Moto/process?mac_address= |
| Welcome URL | https://labcp.cloudpath.net/enroll/Lab/Moto/submit-registration |
| Fail URL | |
| Acknowledgement URL | |
| No Service | |

A set of pre-existing web pages outside of the Controller are specified by the provided URLs. Four separate URLs point to external web pages for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt.

Login URL:

https://labcp.cloudpath.net/enroll/Lab/Moto/process?mac_address=WING_TAG_CLIENT_MAC

Agreement URL:

https://labcp.cloudpath.net/enroll/Lab/Moto/process?mac_address=WING_TAG_CLIENT_MAC

Welcome URL

<https://labcp.cloudpath.net/enroll/Lab/Moto/submit-registration>


Note: The yellow highlighted part is the Cloudpath Enrollment Portal URL. (Configuration -> Workflows)

Create a Whitelist:

This can also be done from Configuration -> Services -> DNS Whitelist

Name **CP-Whitelist** ?

DNS Entries

| DNS Entry | Match Suffix | |
|---------------------|--------------|---|
| labcp.cloudpath.net | X |  |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

+ Add Row

OK Reset Exit

This is the hostname of the Cloudpath server to allow access before authentication. If you need to allow other sites, that is done here.

Click OK to Save and Exit.

Cloudpath Configuration

Below is the Workflow configuration used in Cloudpath for this setup:


Enrollment Process


The screenshot displays the 'Enrollment Process' configuration in a tabbed interface. The tabs are 'Properties', 'Enrollment Process', 'Look & Feel', 'Snapshot(s)', and 'Advanced'. The 'Enrollment Process' tab is active, showing a flow of three steps:

- Step 1:** Require the user to accept the AUP **Moto AUP**
- Step 2:** **Prompt the user** for credentials from **Lab AD**
- Result:** Move user to **Moto** and assign certificate using **BYOD Policy Template**.


Device Configuration Summary

Summary Information

Name: Moto 

Network(s) To Install: Moto-Secure 

Conflicting SSID(s): <None>

Certificates: Only talk to RADIUS servers with a common name matching 'labcp.cloudpath.net'.
Install client certificate (if applicable).
Install & trust root CA 'Lab Root CA I'. 37440B...40B980 

Operating Systems: Windows, Mac OS X, Linux, Android, Apple iOS, Windows Mobile, Other, Chrome 