

ARUBA WIRELESS AND CLEARPASS 6 INTEGRATION GUIDE



Technical Note

Copyright

© 2012 Aruba Networks, Inc. Aruba Networks trademarks include  airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFPProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site::

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.



www.arubanetworks.com
1344 Crossman Avenue
Sunnyvale, California 94089
Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

1. Aruba Wireless and ClearPass 6.0.1 Integration Guide	4
Purpose.....	4
Assumptions	4
Step 1: AOS Controller Configuration	4
Step 2: Adding a RFC 3576 Server	5
Step 3: Creating a new Server Group for ClearPass.....	7
Step 4: Pre-configured Firewall Policies	18
Step 5: Creating AAA Profiles for the ClearPass Guest and 802.1x SSID.....	19
Step 6: Associating a 802.1x SSID and Guest SSID with AAA Profiles.....	24
Step 7: ClearPass Guest Setup.....	26
Basic Guest Registration and Login configuration.....	26
2. ClearPass Policy Manager Setup	30
Guest SSID Login service configuration.....	35
3. Testing the 802.1x and Guest SSID	38
Step 8: Test the 802.1x SSID	41
Step 9: Testing the Guest SSID.....	41
Testing the MAC Caching.....	43
<i>Controller Management Login Authentication with ClearPass Policy Manager</i>	44
Troubleshooting.....	48

1. Aruba Wireless and ClearPass 6.0.1 Integration Guide

Purpose

The purpose of this document is to provide instructions for integrating Aruba Networks Wireless Hardware with ClearPass 6.0.1. This will include basic topics for 802.1x, RADIUS, and Guest integration in an environment using an Aruba Networks WLAN Solution.

Assumptions

1. Aruba Networks wireless controller is setup and running the latest code.
2. At least one access point is provisioned on the controller for testing.
3. 802.1x SSID is already configured.
4. Guest SSID with Captive Portal is already configured.
5. DHCP and DNS are appropriately configured.
6. ClearPass 6.0.1 server (VM or Physical Appliance) initial setup is complete. This includes network settings, time and date, and system name.
7. Aruba Wireless controller can communicate with ClearPass 6.0.1.
8. The Guest SSID VLAN can communicate with ClearPass 6.0.1.
9. All systems are appropriately licensed.
10. Only one interface is configured on ClearPass.

Step 1: AOS Controller Configuration

Login to the controller GUI as an admin user. Navigate to **Configuration->Security->Authentication->Servers** tab. Click on **RADIUS Server** and create a new RADIUS server by entering the new RADIUS server reference name in the empty Add box and clicking **Add**.

The screenshot shows the Aruba AOS Controller GUI. The navigation path is Configuration > Security > Authentication > Servers. The 'Servers' tab is active, showing a list of RADIUS servers. A red arrow points to the 'RADIUS Server' link in the left-hand navigation pane. Below this list is an 'Add' button with an empty text box next to it, also highlighted with a red arrow. The main content area displays a table of existing RADIUS servers with columns for Instance and Actions (Show Reference, Delete).

Instance	Actions
108_7_cppm_rad	Show Reference Delete
110_101_cppm_rad	Show Reference Delete
110_104_cppm_rad	Show Reference Delete
110_106_cppm_rad	Show Reference Delete
110_33_amg_rad	Show Reference Delete
110_8_amg_rad	Show Reference Delete
111_109_cp6_rad	Show Reference Delete

Click on the new server name that shows up in the RADIUS Server list on that page:

oring **Configuration** Diagnostics Maintenance Plan Save Configuration

Security > Authentication > Servers

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

- Server Group
 - RADIUS Server
 - 108_7_cppm_rad
 - 110_101_cppm_rad
 - 110_104_cppm_rad
 - 110_106_cppm_rad
 - 110_33_amg_rad
 - 110_8_amg_rad
 - 111_109_cp6_rad

RADIUS Server Instance

- 108_7_cppm_rad
- 110_101_cppm_rad
- 110_104_cppm_rad
- 110_106_cppm_rad
- 110_33_amg_rad
- 110_8_amg_rad
- 111_109_cp6_rad
- cp60-radius

Add

Enter the IP address for ClearPass in the **Host** field. Enter aruba123 for the **key**. Click **Apply** at the bottom of the page to save these configuration settings.

RADIUS Server > cp60-radius Show Reference Save As Reset

Host	<input type="text" value="10.1.1.20"/>	Key	<input type="password" value="....."/> Retype: <input type="password" value="....."/>
Auth Port	<input type="text" value="1812"/>	Acct Port	<input type="text" value="1813"/>
Retransmits	<input type="text" value="3"/>	Timeout	<input type="text" value="5"/> sec
NAS ID	<input type="text"/>	NAS IP	<input type="text"/>
Source Interface	<input type="text"/>	Use MD5	<input type="checkbox"/>
Use IP address for calling station ID	<input type="checkbox"/>	Mode	<input checked="" type="checkbox"/>

Step 2: Adding a RFC 3576 Server

The next step is to add an RFC 3576 server entry for ClearPass.

Click on **RFC 3576 Server**.

Configuration | **Configuration** | Diagnostics | Maintenance

Security > Authentication > Servers

Servers | AAA Profiles | L2 Authentication

- + Server Group
- + RADIUS Server
- + LDAP Server
- + Internal DB
- + Tacacs Accounting Server
- + TACACS Server
- + XML API Server
- + **RFC 3576 Server**

Enter the **IP address** of ClearPass in the entry box and click **Add**.

MOBILITY CONTROLLER | ravi650

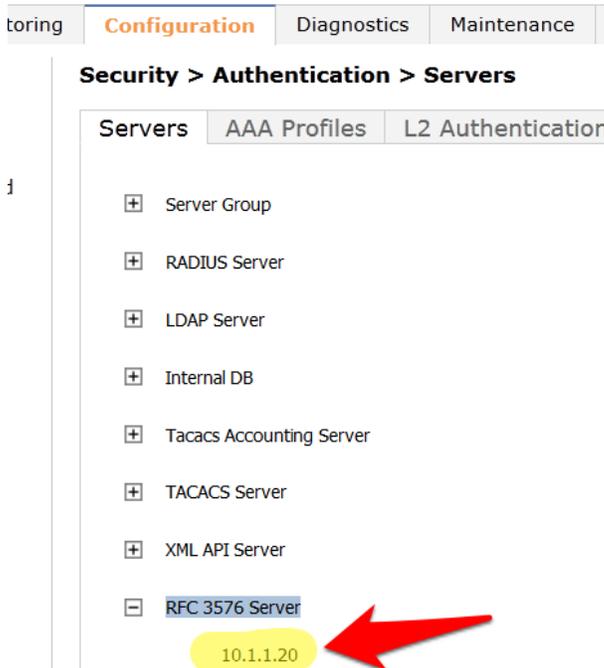
Configuration | **Configuration** | Diagnostics | Maintenance | Plan | Save Configuration

Security > Authentication > Servers

Servers | AAA Profiles | L2 Authentication | L3 Authentication | User Rules

RFC 3576 Server	
Instance	
	10.162.108.7
	10.162.108.9
	10.162.110.19
	10.162.110.24
	10.162.110.25
	10.162.110.26
	10.162.110.33
	10.162.110.36
	10.162.110.37
	10.162.110.8
	10.162.111.109
	10.2.50.178
	10.6.52.81
10.162.108.7	10.1.1.20
10.162.108.9	
10.162.110.19	
10.162.110.24	

Click on the IP address of ClearPass that appears in the left column under RFC 3576 Server.



You will be presented with a screen in the right column that looks like this:



1. You **MUST** enter the RADIUS shared key into the key boxes. Enter aruba123 in both boxes and click **Apply** at the bottom of the page to save the changes.

Note: This step is extremely important!

Step 3: Creating a new Server Group for ClearPass

The next step is to create a new Server Group for ClearPass. Click on Server Group.

oring **Configuration** Diagnostics Maintenance Plan

Security > Authentication > Servers

Servers AAA Profiles L2 Authentication L3 A

- + Server Group 
- + RADIUS Server
- + LDAP Server
- + Internal DB
- + Tacacs Accounting Server
- + TACACS Server
- + XML API Server
- + RFC 3576 Server
- + Windows Server

Enter the a reference name for your ClearPass Server Group in the empty box and click **Add**.

oring **Configuration** Diagnostics Maintenance Plan **Save Configuration**

Security > Authentication > Servers

Servers AAA Profiles L2 Authentication L3 Authentication Use

- Server Group
 - 108_7_cppm_srv
 - 110_101_cppm_srv
 - 110_104_cppm_srv
 - 110_106_cppm_srv
 - 110_33_amg_srv
 - 110_8_amg_srv
 - 111_109_cp6_srv
 - default
 - internal

Server Group

Instance
108_7_cppm_srv
110_101_cppm_srv
110_104_cppm_srv
110_106_cppm_srv
110_33_amg_srv
110_8_amg_srv
111_109_cp6_srv
default
internal
cp60-sg <input type="text" value="cp60-sg"/> Add



Select the newly created Server Group on the right under Server Group:

oring **Configuration** Diagnostics Maintenance

Security > Authentication > Servers

Servers AAA Profiles L2 Authent

- [-] Server Group
 - 108_7_cppm_srv
 - 110_101_cppm_srv
 - 110_104_cppm_srv
 - 110_106_cppm_srv
 - 110_33_amg_srv
 - 110_8_amg_srv
 - 111_109_cp6_srv
 - cp60-sg** 

Click **New** and select the ClearPass RADIUS server from the previous step.

oring **Configuration** Diagnostics Maintenance Plan **Save Configuration**

Security > Authentication > Servers

Servers AAA Profiles L2 Authentication L3 Authentication Use

- [-] Server Group
 - 108_7_cppm_srv
 - 110_101_cppm_srv
 - 110_104_cppm_srv
 - 110_106_cppm_srv 
 - 110_33_amg_srv
 - 110_8_amg_srv
 - 111_109_cp6_srv
 - cp60-sg

Server Group > cp60-sg

Fail Through

Servers

Name	Server
New	

Server Rules

Priority	Attribute	Oper
New		

Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration

Security > Authentication > Servers

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Server Group

- 108_7_cppm_srv
- 110_101_cppm_srv
- 110_104_cppm_srv
- 110_106_cppm_srv
- 110_33_amg_srv
- 110_8_amg_srv
- 111_109_cp6_srv
- cp60-sg
- default
- internal

Server Group > cp60-sg

Fail Through

Servers

Name	Server-Type	trim-FQDN	Match-Rule	Actions
Server Name	Trim FQDN	Match Rules		
Internal (Local)	<input type="checkbox"/>			Ma Au A
108_7_cppm_rad (Radius)				
110_101_cppm_rad (Radius)				
110_104_cppm_rad (Radius)				
110_106_cppm_rad (Radius)				
110_33_amg_rad (Radius)				
110_8_amg_rad (Radius)				
111_109_cp6_rad (Radius)				
cp60-radius (Radius)				

Operation Operand T

2. Click **Add Server**. Click **Apply** at the bottom of the page to save the changes.

Server Group > cp60-sg Show Reference Save As Reset

Fail Through

Servers

Name	Server-Type	trim-FQDN	Match-Rule	Actions
Server Name	Trim FQDN	Match Rules		
cp60-radius (Radius)	<input type="checkbox"/>	Match Type Authstring	Operator contains	Match String <input type="text"/>
		Add Rule	Delete Rule	

Add Server Cancel

Server Rules

Priority	Attribute	Operation	Operand	Type	Action	Value	Validated	Actions
New								

Captive Portal profile

Click on the **L3 Authentication** tab.

Configuration | Diagnostics | Maintenance | Plan | Save Configuration

Security > Authentication > Servers

Servers | AAA Profiles | L2 Authentication | **L3 Authentication** | User Rule

Server Group

- 108_7_cppm_srv
- 110_101_cppm_srv
- 110_104_cppm_srv
- 110_106_cppm_srv
- 110_33_amg_srv
- 110_8_amg_srv
- 111_109_cp6_srv
- cp60-sg**
- default
- internal

Server Group > cp60-sg

Fail Through

Servers

Name	Server-Type
cp60-radius (Radius)	

Server Rules

Priority	Attribute	Operation
New		

Click on **Captive Portal Authentication Profile**.

MOBILITY CONTROLLER | ravi650

Configuration | Diagnostics | Maintenance | Plan

Security > Authentication > L3 Authentication

Servers | AAA Profiles | L2 Authentication | **L3 Authentication**

- + **Captive Portal Authentication Profile** ←
- + WISPr Authentication Profile
- + VPN Authentication Profile
- + Stateful NTLM Authentication Profile
- + VIA Authentication Profile
- + VIA Connection Profile
- + VIA Web Authentication

Enter a new Captive Portal profile name in the empty box and click **Add**.

Configuration | Diagnostics | Maintenance | Plan | Save Configuration

Security > Authentication > L3 Authentication

Servers | AAA Profiles | L2 Authentication | L3 Authentication | User F

- Captive Portal Authentication Profile
 - 108_7_cppm_cp
 - 110_33_amg_cp
 - 110_8_onboard_prov_cp
 - 111_109_cpg6
 - default
 - Aruba_admin**

Captive Portal Authentication Profile Instance

- 108_7_cppm_cp
- 110_33_amg_cp
- 110_8_onboard_prov_cp
- 111_109_cpg6
- default

Select the newly created **Captive Portal Authentication Profile** under **Captive Portal Authentication Profile** on the right.

Configuration | Diagnostics | Maintenance | Plan | Save Configuration

Security > Authentication > L3 Authentication

Servers | AAA Profiles | L2 Authentication | L3 Authentication | User Rules | Adv

- Captive Portal Authentication Profile
 - 108_7_cppm_cp
 - 110_33_amg_cp
 - 110_8_onboard_prov_cp
 - 111_109_cpg6
 - Aruba_admin**
 - default

Captive Portal Authentication Profile Instance

- 108_7_cppm_cp
- 110_33_amg_cp
- 110_8_onboard_prov_cp
- 111_109_cpg6
- Aruba_admin**
- default

There are two things we need to change on this profile.

- Change the **Login page** to http://10.1.1.20/guest/guest_register_login.php (replacing the 10.1.1.20 with the IP address of your ClearPass 6.0.1 server).

Captive Portal Authentication Profile > Aruba_admin Show Reference Save As Reset

Default Role	guest	Default Guest Role	guest
Redirect Pause	10 sec	User Login	<input checked="" type="checkbox"/>
Guest Login	<input type="checkbox"/>	Logout popup window	<input checked="" type="checkbox"/>
Use HTTP for authentication	<input type="checkbox"/>	Logon wait minimum wait	5 sec
Logon wait maximum wait	10 sec	logon wait CPU utilization threshold	60 %
Max Authentication failures	0	Show FQDN	<input type="checkbox"/>
Use CHAP (non-standard)	<input type="checkbox"/>	Login page	10.162.111.119
Welcome page	/auth/welcome.html	Show Welcome Page	<input checked="" type="checkbox"/>
Add switch IP address in the redirection URL	<input type="checkbox"/>	Adding user vlan in redirection URL	<input type="checkbox"/>
Add a controller interface in the redirection URL	<input type="text"/>	Allow only one active user session	<input type="checkbox"/>
White List	<input type="text"/> Delete Add	Black List	<input type="text"/> Delete Add
Show the acceptable use policy page	<input type="checkbox"/>		

Click **Apply** at the bottom to save the changes.

- Click on **Server Group** under the **Captive Portal Authentication Profile** and change the **Server Group** from **default** to the Server Group that you created for ClearPass in the previous steps and click **Apply** at the bottom of the page to save the changes.

Security > Authentication > L3 Authentication

Servers AAA Profiles L2 Authentication L3 Authentication User Rules

[-] Captive Portal Authentication Profile

- + 108_7_cppm_cp
- + 110_33_amg_cp
- + 110_8_onboard_prov_cp
- + 111_109_cpg6
- [-] Aruba_admin
 - Server Group default
- + default

Server Group > default

Fail Through

Servers

Name

Internal

New

Server Rules

Priority **Attribute** **Operation** **Op**

1 role value-of

New

Security > Authentication > L3 Authentication

The screenshot shows the configuration for a Captive Portal Authentication Profile. The 'Server Group' is set to 'cp60-sg'. A table lists the servers associated with this group:

Name	Server-Type	Fail Through
cp60-radius	Radius	No

Below the servers table, there is a 'Server Rules' section with a table that has columns for Priority, Attribute, Operation, and Open. A 'New' button is visible below the table.

Create a Captive Portal role

Now we need to create our Captive Portal role, which is the role that clients will receive when they connect to the Guest SSID.

Navigate to **Configuration->Security->Access Control->User Roles** tab. Click **Add** to create a new User Role.

The screenshot shows the 'User Roles' configuration page. The 'Add' button at the bottom left is highlighted with a red arrow.

Name	Firewall Policies	Bandwidth Contract	Actions
108_7_cppm_cp	logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
110_33_amg_logon	logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
110_8_onboard_prov_logon	110_8_onboard_prov_cp_list_operations/,logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
111_109_cpg6_logon	logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
authenticated	allowall/,v6-allowall/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
default-via-role	allowall/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
default-vpn-role	allowall/,v6-allowall/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
denyall	Not Configured	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
guest	http-acl/,https-acl/,dhcp-acl/,icmp-acl/,dns-acl/,v6-http-acl/,v6-https-acl/,v6-dhcp-acl/,v6-icmp-acl/,v6-dns-acl/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
guest-logon	v6-logon-control/,captiveportal6/,logon-control/,captiveportal/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
logon	ocsp-acl/,captiveportal6/,logon-control/,captiveportal/,vpnlogon/,v6-logon-control/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete
voice	sip-acl/,noe-acl/,svp-acl/,vocera-acl/,skinny-acl/,h323-acl/,dhcp-acl/,tftp-acl/,dns-acl/,icmp-acl/	Up:Not Enforced Down:Not Enforced	Show Reference Edit Delete

Enter a name like “CPG-Login” for the Role Name under **Firewall Policies**, Click **Add**.

Security > User Roles > Add Role

User Roles System Roles Policies Time Ranges Guest Access

Role Name

Firewall Policies

Name	Rule Count
<input type="button" value="Add"/>	

For the first policy, it is essentially important that we add an ACL that will allow our **Guest user** to access ClearPass 6.0.1, which is where the Captive Portal webpage will be hosted.

Choose the radio button for **Create New Policy**, and click the **Create** button:

Security > User Roles > Add Role

User Roles System Roles Policies Time Ranges Guest Access

Role Name

Firewall Policies

Name	Rule Count
<input type="button" value="Add"/>	

Choose From Configured Policies

Create New Policy From Existing Policy

Create New Policy

Enter and select the following information:

- **Policy Name:** "CP6-web-ACL"
- **Policy Type:** "Session"

Click **Add**.

Security > User Roles > Add Role > Add New Policy

User Roles System Roles Policies Time Ranges Guest Access

Policy Name

Policy Type

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time
<input type="button" value="Add"/>								

Select and enter the following information for the first line of the ACL:

- **IP Version:** "IPv4"
- **Source:** "User"
- **Destination:** host
 - **Host IP:** (the IP address of your ClearPass server)
- **Service:** "service"
 - **Service:** "svc-http (tcp 80)"
- **Action:** "permit"

Security > User Roles > Add Role > Add New Policy

User Roles System Roles Policies Time Ranges Guest Access

Policy Name

Policy Type

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time
IPv4	user	host Host IP 10.162.111.119	service Service svc-http (tcp 80) New	permit				

Click **Add** at the far right underneath this rule.

« Back

Classify Media	TOS	802.1p Priority	Action
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Done

Click **Add** again to add another line to this ACL, identical to the previous line except:

Choose **Service**: “svc-https (tcp 443)”

Security > User Roles > Add Role > Add New Policy

User Roles System Roles Policies Time Ranges Guest Access

Policy Name CP6-web-ACL
Policy Type Session

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time R
IPv4	user	host 10.162.111.119	svc-http	permit			low	

IP Version	Source	Destination	Service	Action
IPv4	user	host Host IP 10.162.111.119	service Service svc-https (tcp 443) New	permit

Click **Add** at the far right underneath this rule.

Security > User Roles > Add Role > Add New Policy

User Roles System Roles Policies Time Ranges Guest Access

Policy Name CP6-web-ACL
Policy Type Session

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue
IPv4	user	host 10.162.111.119	svc-http	permit			low
IPv4	user	host 10.162.111.119	svc-https	permit			low

Click **Done**

You will be brought back to the Add Role page where you were creating your CPG-Login User Role.

User Roles System Roles Policies Time Ranges Guest Access

Role Name

Firewall Policies

Name	Rule Count
CP6-web-ACL	2

Step 4: Pre-configured Firewall Policies

The Firewall Policy that you just created has been added to the list. Now we need to add two more pre-configured Firewall Policies.

Click **Add** under **Firewall Policies**. Select the radio button for “Choose From Configured Policies” and select the policy called “logon-control (session)”.

Firewall Policies

Name	Rule Count
CP6-web-ACL	2

Choose From Configured Policies
 Create New Policy From Existing P
 Create New Policy

- validuser (session)
- captiveportal (session)
- captiveportal_testlab_178 (session)
- captiveportal6 (session)
- citrix-acd (session)
- control (session)
- cplogout (session)
- dhcp-acd (session)
- dns-acd (session)
- h323-acd (session)
- http-acd (session)
- https-acd (session)
- icmp-acd (session)
- logon-control (session)
- noe-acd (session)

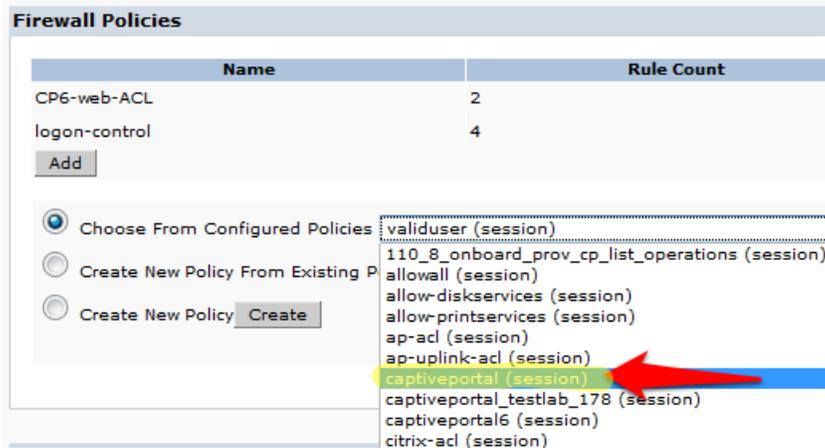
Re-authentication Interval

Disabled

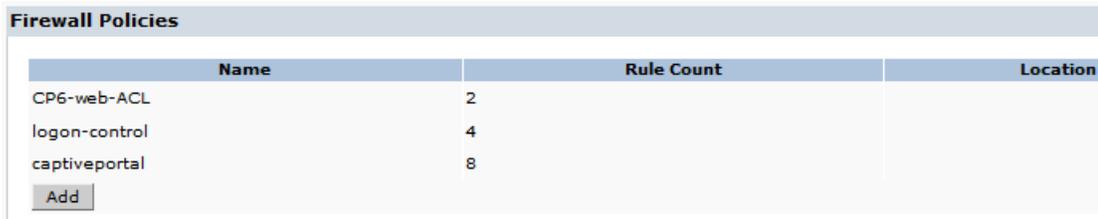
Click **Done** in the **Firewall Policies** section.

Click **Add** again in the **Firewall Policies** section.

Select the radio button for “Choose From Configured Policies” and select the policy called “captiveportal (session)”.



Click **Done** in the **Firewall Policies** section. Your Firewall Policy should look like this:



NOTE: The Firewall policy order **MUST** place “captive portal” at the **bottom** of the list!

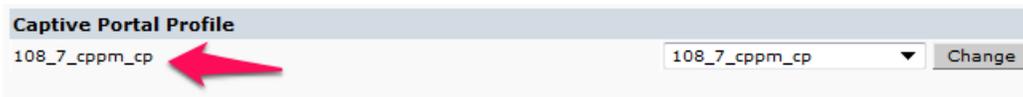
Scroll down this page to the **Captive Portal Profile** section.

Select the previously configured Captive Portal Profile from the drop-down list.

Click the **Change** button.



Verify that the “Not Assigned” has changed to the name of your Captive Portal Profile.



Click **Apply** at the bottom of the page to save the newly created User Role.

Step 5: Creating AAA Profiles for the ClearPass Guest and 802.1x SSID

The next step is to create AAA Profiles for the ClearPass Guest and 802.1x SSID.

Navigate to **Configuration->Security->Authentication->AAA Profiles tab**.

Click **Add**, enter a name for the ClearPass Guest Profile, and then click **Add** again.

Configuration Diagnostics Maintenance Plan Save Configuration

Security > Authentication > Profiles

Servers **AAA Profiles** L2 Authentication L3 Authentication User Rules Advanced

AAA Profile

- + 108_7_cppm_health
- + 108_7_onboard_issid
- + 108_7_onboard_dot1x_aaa
- + 110_101_cppm_dot1x_aaa
- + 110_104_cppm_dot1x_aaa
- + 110_106_cppm_dot1x_aaa
- + 110_33_amg_aaa
- + 110_8_onboard_dot1x_aaa
- + 110_8_onboard_prov_aaa
- + 111_109_cpg_aaa
- + default
- + default-dot1x
- + default-dot1x-psk
- + default-mac-auth
- + default-open
- + default-xml-api
- + NoAuthAAAProfile

AAA Profiles Summary

Name	
108_7_cppm_health	108_7_cpp
108_7_onboard_issid	logon
108_7_onboard_dot1x_aaa	logon
110_101_cppm_dot1x_aaa	logon
110_104_cppm_dot1x_aaa	logon
110_106_cppm_dot1x_aaa	logon
110_33_amg_aaa	110_33_ar
110_8_onboard_dot1x_aaa	logon
110_8_onboard_prov_aaa	110_8_ont
111_109_cpg_aaa	111_109_c
default	guest-logo
default-dot1x	logon
default-dot1x-psk	guest-logo
default-mac-auth	logon
default-open	logon
default-xml-api	logon
NoAuthAAAProfile	logon

Add

Now in the left column, click on the new profile that you just created. Change the Initial role to the role that you created in the previous step.

AAA Profile > cp-60_cpg

Initial role	logon
802.1X Authentication Default Role	108_7_cppm_cp
RADIUS Interim Accounting	110_33_amg_logon 110_8_onboard_prov_logon 111_109_cpg6_logon
Wired to Wireless Roaming	ap-role authenticated
Device Type Classification	default-via-role default-vpn-role denyall nquest

Tech Tip: On this page you will see an option for “RADIUS Interim Accounting”. This should be checked if you want live utilization updates in ClearPass, usually used to control guest users based on Bandwidth Utilization.

Security > Authentication > Profiles

Servers **AAA Profiles** L2 Authentication L3 Authentication User Rules Advanced

AAA Profile

- + 108_7_cppm_health
- + 108_7_onboard_issid
- + 108_7_onboard_dot1x_aaa
- + 110_101_cppm_dot1x_aaa
- + 110_104_cppm_dot1x_aaa
- + 110_106_cppm_dot1x_aaa

AAA Profile > cp-60_cpg

Initial role	108_7_cppm_cp
802.1X Authentication Default Role	guest
RADIUS Interim Accounting	<input checked="" type="checkbox"/>
Wired to Wireless Roaming	<input checked="" type="checkbox"/>
Device Type Classification	<input checked="" type="checkbox"/>

This also needs to be enabled on ClearPass.

In ClearPass Policy Manager, navigate to:

Administration->Server Manager->Server Configuration->Select Server->Service Parameters->RADIUS Server->Log Accounting Interim-Update Packets="TRUE".

The screenshot shows the ClearPass Policy Manager interface. The left sidebar contains a navigation menu with 'Administration' selected. The main content area shows the configuration for 'Server Configuration - burns.corp.airwave.com (10.162.111.119)'. The 'Service Parameters' tab is active, and the 'Accounting' section is expanded. The 'Log Accounting Interim-Update Packets' setting is highlighted with a red box, and a red arrow points to the 'TRUE' option in the dropdown menu. A 'Back to Server Configuration' link is visible below the setting.

System	Services Control	Service Parameters	System Monitoring	Network Int
Cleanup Time		5		s
Local DB Authentication Source Connection Count		32		
AD/LDAP Authentication Source Connection Count		64		
SQL DB Authentication Source Connection Count		32		
EAP-TLS Fragment Size		1024		b
Use Inner Identity in Access-Accept Reply		FALSE		
Reject if OSCP response does not have Nonce		TRUE		
TLS Session Cache Limit		3750		s
Thread Pool				
Maximum Number of Threads		10		tl
Number of Initial Threads		5		tl
EAP-FAST				
Master Key Expire Time		1	weeks	
Master Key Grace Time		3	weeks	
PACs are valid across cluster		true		
Accounting				
Log Accounting Interim-Update Packets		FALSE		

Set the subsections of the profile as described below, clicking **Apply** after each change:

MAC Authentication Profile: "default"

Security > Authentication > Profiles

The screenshot shows the 'Security > Authentication > Profiles' page. The 'AAA Profiles' tab is active. A list of AAA profiles is shown on the left, including '108_7_cppm_health', '108_7_onboard_1ssid', '108_7_onboard_dot1x_aaa', '110_101_cppm_dot1x_aaa', '110_104_cppm_dot1x_aaa', '110_106_cppm_dot1x_aaa', '110_33_amg_aaa', '110_8_onboard_dot1x_aaa', '110_8_onboard_prov_aaa', '111_109_cpg_aaa', and 'cp-60_cpg'. The 'MAC Authentication Profile' section is highlighted. A dropdown menu is open, showing the selected profile as 'default'. A red arrow points to the 'default' option in the dropdown.

MAC Authentication Server Group: *(Your ClearPass 6.0.1 Server Group)*

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profile

- 108_7_cppm_health
- 108_7_onboard_1ssid
- 108_7_onboard_dot1x_aaa
- 110_101_cppm_dot1x_aaa
- 110_104_cppm_dot1x_aaa
- 110_106_cppm_dot1x_aaa
- 110_33_amg_aaa
- 110_8_onboard_dot1x_aaa
- 110_8_onboard_prov_aaa
- 111_109_cpg_aaa
- cp-60_cpg
 - MAC Authentication Profile default
 - MAC Authentication Server Group cp60-sg

MAC Authentication Server Group > cp60-sg

Fail Through

Servers

Name	Radius
cp60-radius	cp60-sg

New

Server Rules

Priority	Attribute	Operation	Operation
New			

RADIUS Accounting Server Group: *(Your ClearPass 6.0.1 Server Group)*

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profile

- 108_7_cppm_health
- 108_7_onboard_1ssid
- 108_7_onboard_dot1x_aaa
- 110_101_cppm_dot1x_aaa
- 110_104_cppm_dot1x_aaa
- 110_106_cppm_dot1x_aaa
- 110_33_amg_aaa
- 110_8_onboard_dot1x_aaa
- 110_8_onboard_prov_aaa
- 111_109_cpg_aaa
- cp-60_cpg
 - MAC Authentication Profile default
 - MAC Authentication Server Group cp60-sg
 - 802.1X Authentication Profile
 - 802.1X Authentication Server Group
 - RADIUS Accounting Server Group cp60-sg

RADIUS Accounting Server Group > cp60-sg

Fail Through

Servers

Name	Radius
cp60-radius	cp60-sg

New

Server Rules

Priority	Attribute	Operation	Operation
New			

Click on **RFC 3576** for this AAA Profile.

Security > Authentication > Profiles

Servers AAA Profiles L2 Authentication

- AAA Profile
 - 108_7_cppm_health
 - 108_7_onboard_1ssid
 - 108_7_onboard_dot1x_aaa
 - 110_101_cppm_dot1x_aaa
 - 110_104_cppm_dot1x_aaa
 - 110_106_cppm_dot1x_aaa
 - 110_33_amg_aaa
 - 110_8_onboard_dot1x_aaa
 - 110_8_onboard_prov_aaa
 - 111_109_cpg_aaa
 - cp-60_cpg
 - MAC Authentication Profile
 - MAC Authentication Server Group default
 - 802.1X Authentication Profile
 - 802.1X Authentication Server Group
 - RADIUS Accounting Server Group
 - XML API server
 - RFC 3576 server
 - 10.162.111.119

From the **Add a profile** list, select the IP address of your ClearPass server and click the **Add** button.

RFC 3576 servers	
	Name
10.162.111.119	

Add a profile:

Click **Apply** to save these settings.

Repeat Creating AAA Profiles for the ClearPass Guest and 802.1x SSID, page 19, to create the AAA Profile for the 802.1x SSID. The only difference is that this AAA Profile will have 802.1x settings but no MAC Authentication Profile. See example below:

- [-] AAA Profile
 - [+] cp60-AAA
 - [-] cp60-dot1x-aaa
 - MAC Authentication Profile
 - MAC Authentication Server Group default
 - 802.1X Authentication Profile default
 - 802.1X Authentication Server Group cp60-sg
 - RADIUS Accounting Server Group
 - [+] XML API server
 - [-] RFC 3576 server
 - [+] 10.162.110.103

Step 6: Associating a 802.1x SSID and Guest SSID with AAA Profiles

The next step is to associate our 802.1x SSID and Guest SSID with the AAA Profiles we just created.

Navigate to **Configuration->Advanced Services->All Profiles**.



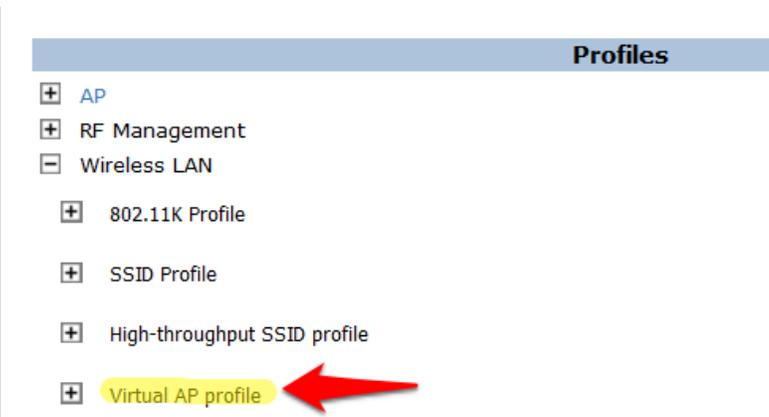
Expand the **Wireless LAN** section.

Advanced Services > All Profile Management

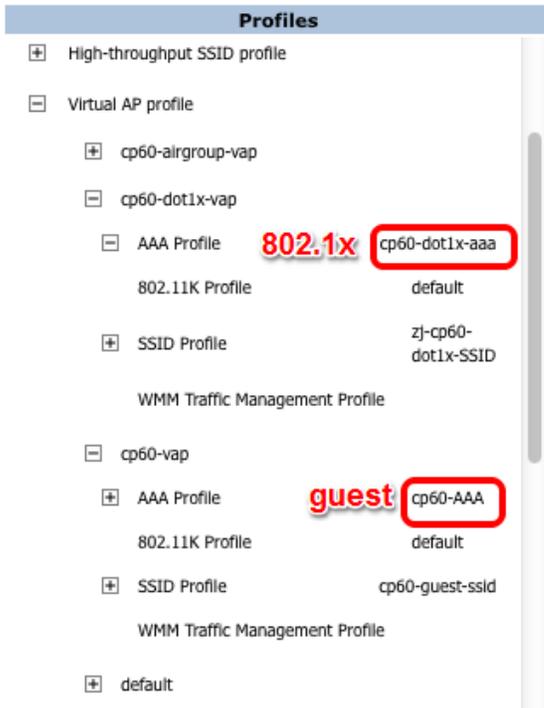


Expand the **Virtual AP profile** and locate your Guest and 802.1x SSID profiles.

Advanced Services > All Profile Management



Modify each Virtual AP profile to use the appropriate AAA Profile that you created in the previous section.



Make sure to click **Apply** after each change.

Click the **Save Configuration** button at the top of the page once the changes are completed.

Step 7: ClearPass Guest Setup

In this step we will configure basic Guest Registration and Login.

Basic Guest Registration and Login configuration

Log into ClearPass Policy Manager (<https://your-cp-ip-here/tips>).

Operator Login

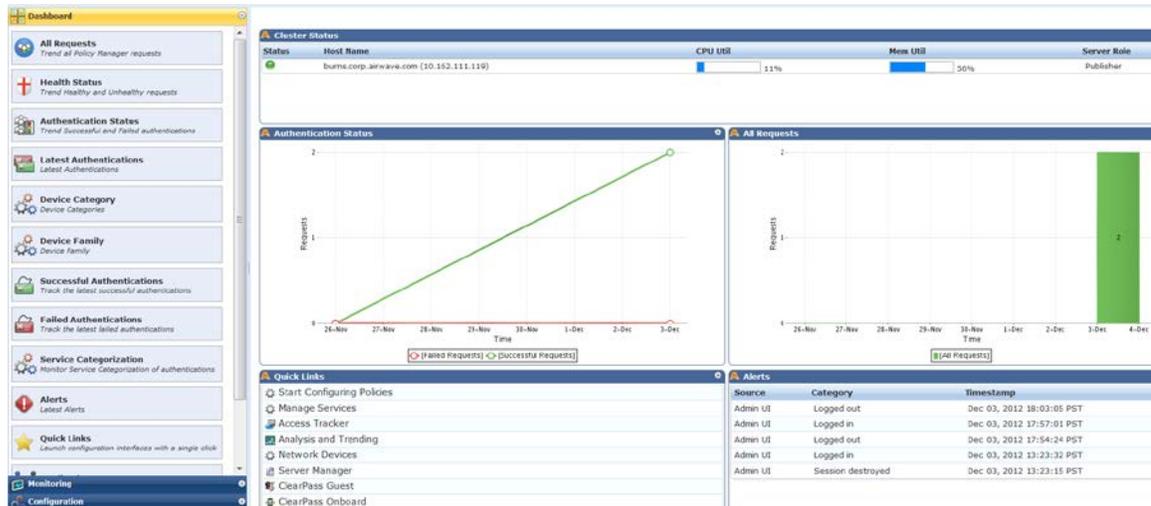
* Username:

* Password:

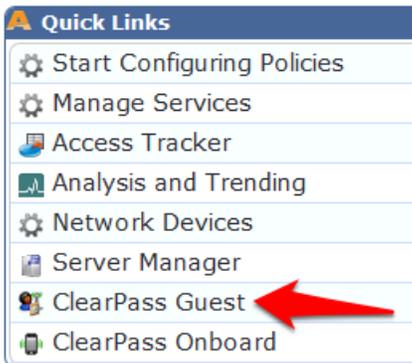
Log In

* required field

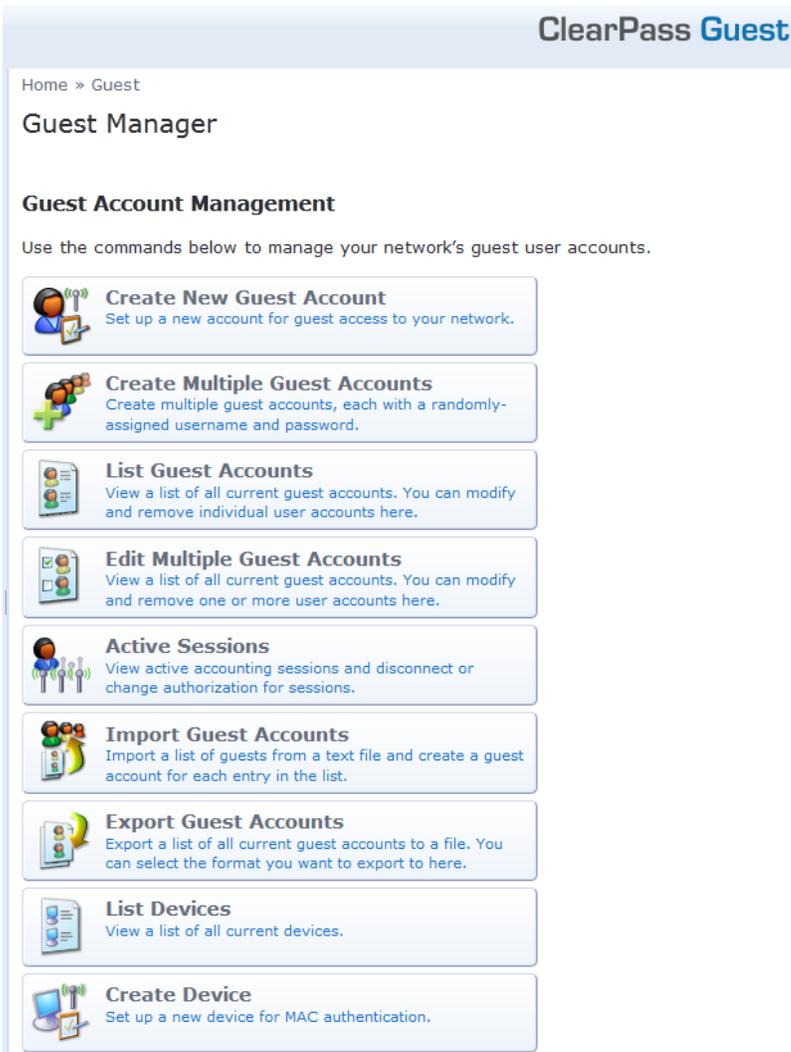
After you login, you will see the ClearPass Policy Manager Dashboard.



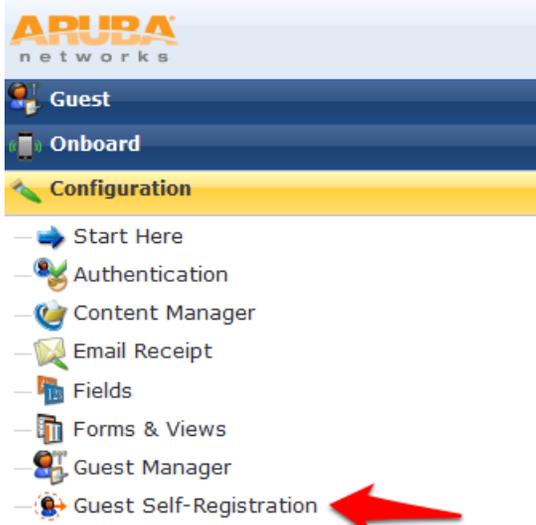
One of the Dashboard objects is Quick Links. Click on the quick link for ClearPass Guest



Clicking this link will automatically log you into the ClearPass Guest administration page. Alternatively you could enter the url for the Guest page (<https://your-cp-ip-here/guest>).



Navigate to **Configuration->Guest Self-Registration.**



Click on the preconfigured **Guest Self-Registration** profile. This will reveal several options. Click **Edit**.

Home » Configuration » Guest Self-Registration

Guest Self-Registration

Use this list view to manage the pages used for guest self-registration.

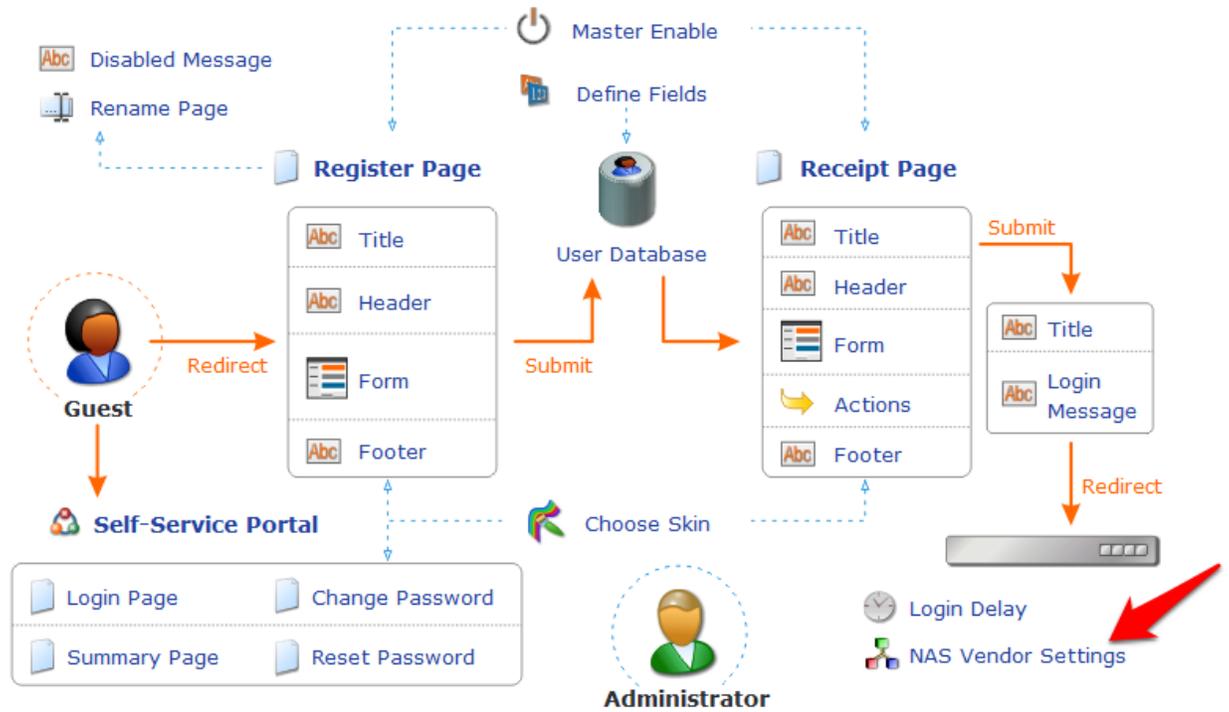
Quick Help			
Name	Register Page	Skin	Parent
Guest Self-Registration Default settings for visitor self-registration.	guest_register	(Default)	(No Parent)
Edit Delete Duplicate Disable Go To			
1 self-registration Reload			20 rows per page

[Back to configuration](#)

[Back to main](#)

In this guest registration profile, it is necessary to enable web login. Click **NAS Vendor Settings** from the edit diagram:

Guest Self-Registration 'Guest Self-Registration'



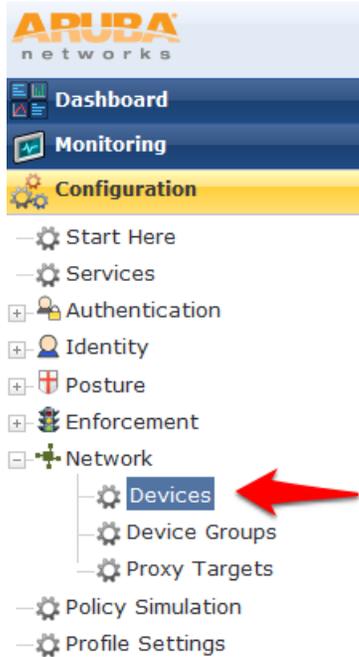
On the **NAS Login** settings page, check the checkbox to “Enable guest login to a Network Access Server.” It will prepopulate the settings with Aruba Networks NAS settings.

Customize Guest Registration	
NAS Login	
Options controlling logging into a NAS for self-registered guests.	
Enabled:	<input checked="" type="checkbox"/> Enable guest login to a Network Access Server
* Vendor Settings:	Aruba Networks Select a predefined group of settings suitable for standard network configurations.
IP Address:	securelogin.arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default Select a security option to apply to the web login process.
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials 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.
Default Destination	
Options for controlling the destination clients will redirect to after login.	
Default URL:	<input type="text"/> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
<input type="button" value="Save Changes"/> <input type="button" value="Save and Continue"/>	

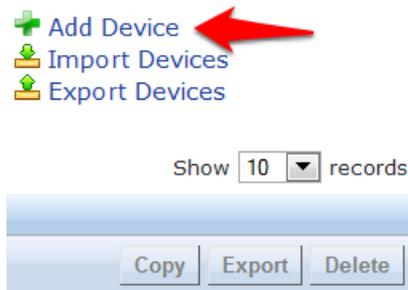
Click **Save Changes**.

2. ClearPass Policy Manager Setup

In ClearPass Policy Manager, navigate to **Configuration->Network->Devices**.



Click **Add Device** in the top right corner of the page.



Enter a **Name** and the **IP or Subnet address** for your Wireless Controller. For the RADIUS Shared Secret, enter aruba123 (the same shared secret we used in the Controller setup for RADIUS and RFC 3576). Select “Aruba” as the **Vendor Name**, and check the box to “**Enable RADIUS CoA:**”

Add Device

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings

Name:

IP or Subnet Address: (e.g., 192.168.1.10 or 192.168.1.1/24)

Description:

RADIUS Shared Secret: Verify:

TACACS+ Shared Secret: Verify:

Vendor Name:

Enable RADIUS CoA: RADIUS CoA Port:

Attributes

Attribute	Value
1. Click to add...	

Add **Cancel**

Click **Add**.

Navigate to **Configuration->Start Here** and select Aruba 802.1X Wireless.

ARUBA networks

Dashboard | Monitoring | **Configuration**

Start Here | Services | Authentication | Identity | Posture

Configuration » Start Here

Choose a deployment type to start

Aruba 802.1X Wireless

For wireless end-hosts connecting through Aruba WLAN Mobility Controllers).

Give the service a name such as “WLAN Enterprise Service”.

Services



Service	Authentication	Roles	Enforcement	Summary
Type:	Aruba 802.1X Wireless			
Name:	WLAN Enterprise Service			
Description:	Aruba 802.1X Wireless Access Service			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints			
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	
3. Radius:Aruba	Aruba-Essid-Name	EXISTS		
4. Click to add...				

Click **Next**.

On the **Authentication** tab, Click the “Select to Add” down arrow and choose “[Local User Repository] [Local SQL DB]” as the “Authentication Sources”.

Service	Authentication	Roles	Enforcement	Summary
Authentication Methods:				
		[EAP PEAP] [EAP FAST] [EAP TLS] [EAP TTLS]		<input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>
		<input type="text" value="--Select to Add--"/>		
Authentication Sources:				
		[Local User Repository] [Local SQL DB]		<input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>
		<input type="text" value="--Select to Add--"/>		
Strip Username Rules:		<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip use		

Click **Next**.

For initial testing, **Role mapping Policy** will not be used. Click **Next** on the **Roles** tab at the bottom right corner of the page to continue.

Configuration » Services » Add

Services



Service	Authentication	Roles	Enforcement	Summary
Role Mapping Policy:			--Select--	
Role Mapping Policy Details				
Description:	-			
Default Role:	-			
Rules Evaluation Algorithm:	-			
Conditions				

On the **Enforcement** tab, no changes are necessary. Click **Next** at the bottom right corner of the page to continue.

Configuration » Services » Add

Services

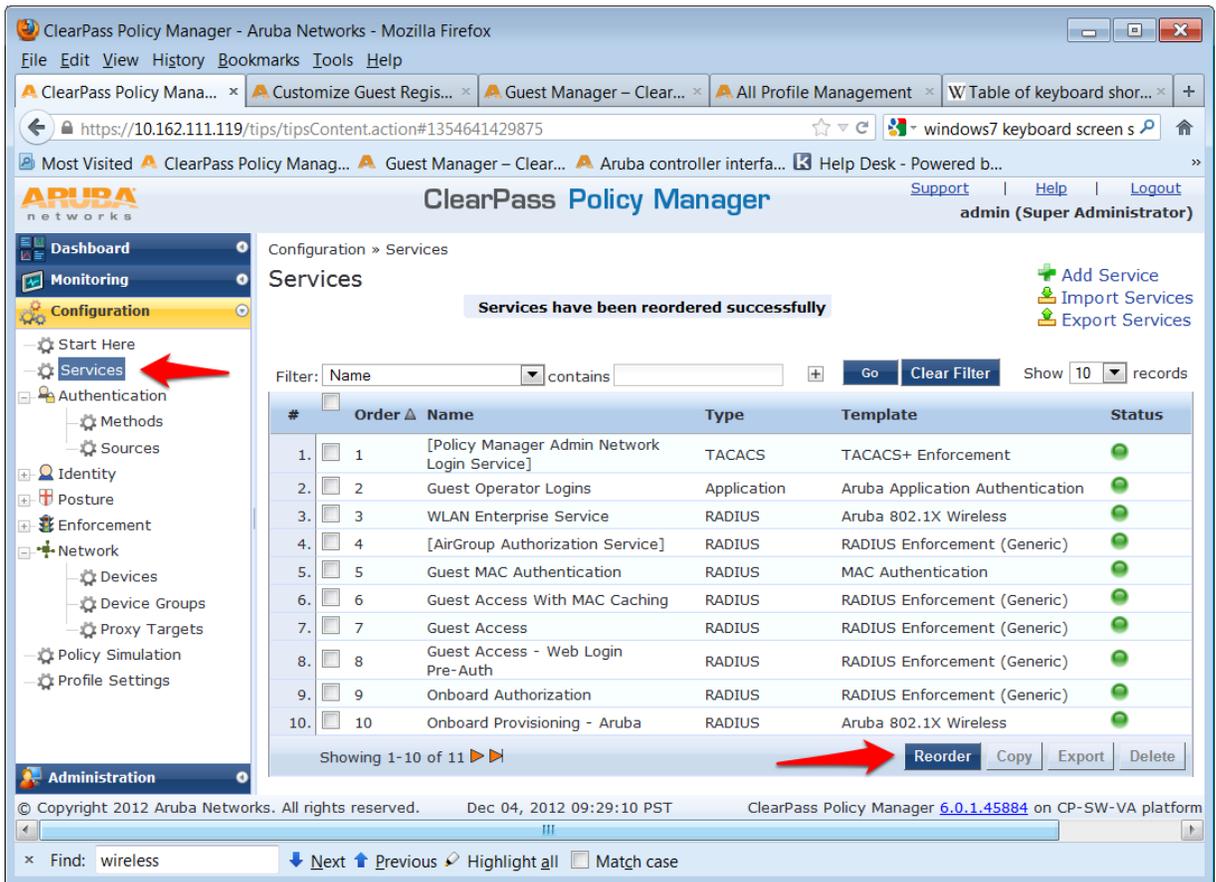


Service	Authentication	Roles	Enforcement	Summary
Use Cached Results:	<input type="checkbox"/>	Use cached Roles and Posture attributes		
Enforcement Policy:			[Sample Allow Access Policy]	
Enforcement Policy Details				
Description:	Sample policy to allow network access			
Default Profile:	[Allow Access Profile]			
Rules Evaluation Algorithm:	evaluate-all			
Conditions				
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday,				

Review the summary and click **Save**.

Important! You must move the WLAN Enterprise Service above any generic RADIUS services that are not filtering via service rules. ClearPass 6.0.1 does not ship with any generic RADIUS services that have no service rules.

Navigate to **Configuration->Services** and select **Reorder** to move “WLAN Enterprise Service” above ANY generic RADIUS services that are not filtering via service rules.



Select "WLAN Enterprise Service" and click on the **Move up** button to position " above ANY generic RADIUS services that are not filtering via service rules.

Note: Do NOT move any services you create ABOVE the initial services that are installed with ClearPass Policy Manager. **IF** you add a service and move it ABOVE the initial services installed your newly created service **could** intercept RADIUS requests that "Guest Mac authentication", which is Mac caching, or Onboarding, and AirGroup.

Configuration » Services » Reorder

Reorder Services

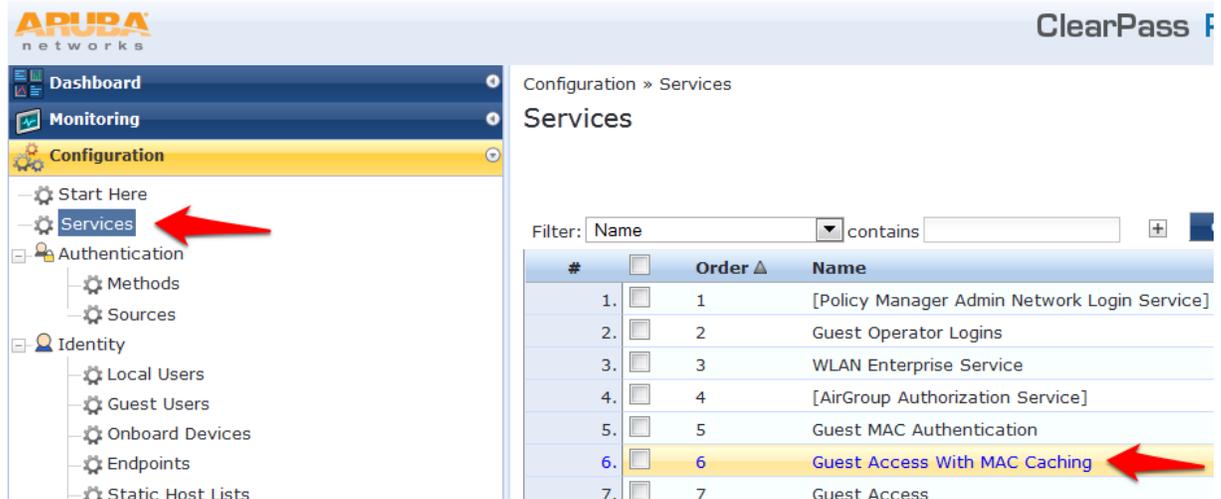
Order	Name
1	[Policy Manager Admin Network Login Service]
2	Guest Operator Logins
3	[AirGroup Authorization Service]
4	Guest MAC Authentication
5	Guest Access With MAC Caching
6	Guest Access
7	Guest Access - Web Login Pre-Auth
8	Onboard Authorization
9	Onboard Provisioning - Aruba
10	[Aruba Device Access Service]
11	WLAN Enterprise Service

Service Details:	
Name:	WLAN Enterprise Service
Template:	Aruba 802.1X Wireless
Type:	RADIUS
Description:	Aruba 802.1X Wireless Access Service
Status:	Enabled
Service Rule	
<pre>((Radius:IETF:NAS-Port-Type EQUALS Wireless-802.11 (19)) AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Frame AND (Radius:Aruba:Aruba-Essid-Name EXISTS)) AND (Connection:Protocol EQUALS RADIUS))</pre>	

If you are running the beta version of 6.0, you may not have the Guest MAC Authentication services. If this is the case, please [download](#) the non-beta version of 6.0, as it will include these services by default.

Guest SSID Login service configuration

To configure the Guest SSID Login service, navigate to **Configuration->Services**. Click on “Guest Access With MAC Caching.”



The screenshot shows the Aruba ClearPass configuration interface. On the left is a navigation menu with 'Configuration' selected and 'Services' highlighted by a red arrow. The main area displays a list of services under the heading 'Services'. A table lists services with columns for '#', 'Order', and 'Name'. The service 'Guest Access With MAC Caching' is highlighted in yellow and pointed to by a red arrow.

#	Order	Name
1.	1	[Policy Manager Admin Network Login Service]
2.	2	Guest Operator Logins
3.	3	WLAN Enterprise Service
4.	4	[AirGroup Authorization Service]
5.	5	Guest MAC Authentication
6.	6	Guest Access With MAC Caching
7.	7	Guest Access

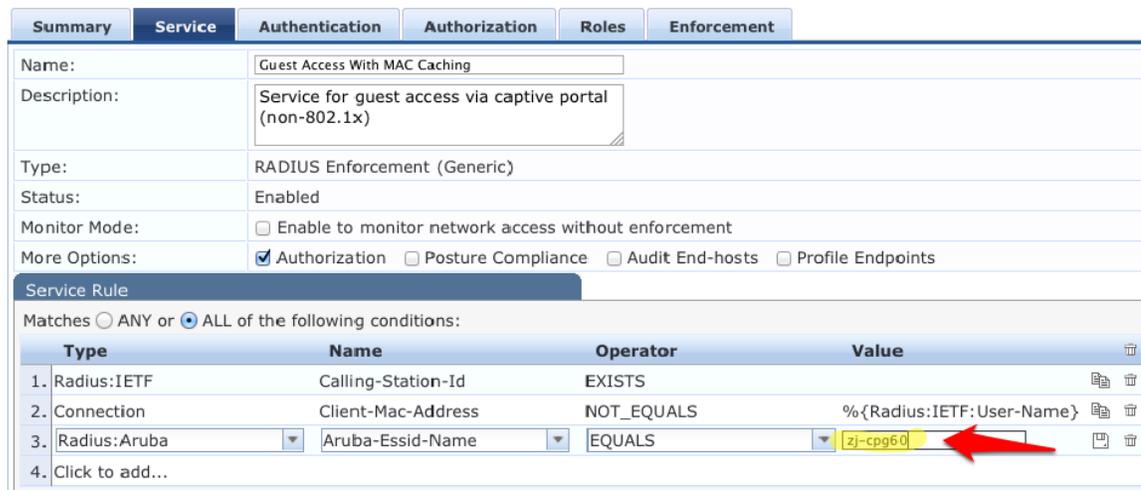
Click on the **Service** tab.

In order to get this service to respond to the guest SSID, click the “Radius:Aruba, Aruba-Essid-Name, EQUALS, Guest SSID Name” row under **Service Rule** sub-tab to modify.

Replace the “Guest SSID Name” with the actual guest SSID used on the controller.

In the example below, the guest SSID is “zj-cpg60.”

Services - Guest Access With MAC Caching



The screenshot shows the configuration page for the 'Guest Access With MAC Caching' service. The 'Service Rule' section is active, showing a table of conditions. The third condition is selected, showing 'Radius:Aruba' as the operator, 'Aruba-Essid-Name' as the name, and 'EQUALS' as the operator. The value is 'zj-cpg60', which is highlighted in yellow and pointed to by a red arrow.

Type	Name	Operator	Value
1. Radius:IETF	Calling-Station-Id	EXISTS	
2. Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
3. Radius:Aruba	Aruba-Essid-Name	EQUALS	zj-cpg60
4. Click to add...			

Click **Save** to register the modifications to the service.

Repeat those steps for the “Guest MAC Authentication” service:

Services - Guest MAC Authentication

Summary	Service	Authentication	Authorization	Roles	Enforcement
Name:	Guest MAC Authentication				
Description:	Service performing authentication for cached MAC entries for guest accounts				
Type:	MAC Authentication				
Status:	Enabled				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement				
More Options:	<input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints				
Service Rule					
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:					
Type	Name	Operator	Value		
1. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}		
2. Radius:Aruba	Aruba-Essid-Name	EQUALS	zj-cpg60		
3.	Click to add...				

The next step is to add a User Role. Even though no role mapping is in use in the WLAN Enterprise Service, a user role must be created for any local user account added into the Local User Repository.

Navigate to **Configuration->Identity->Roles**

Click **Add Device** in the top right corner of the page.

Add Device

 Import Devices

 Export Devices

Show records

Enter "TestRole" as the name, and click **Save**.

Dashboard

Monitoring

Configuration

- Start Here
- Services
- Authentication
 - Methods
 - Sources
- Identity**
 - Local Users
 - Guest Users
 - Onboard Devices
 - Endpoints
 - Static Host Lists
 - Roles**
 - Role Mappings

Configuration » Identity » Roles

Roles

Filter: Name contains

#	<input type="checkbox"/>	Name
1.	<input type="checkbox"/>	TestRole
2.	<input type="checkbox"/>	[TACACS Super Admin]
3.	<input type="checkbox"/>	[TACACS Receptionist]
4.	<input type="checkbox"/>	[TACACS Read-only Admin]
5.	<input type="checkbox"/>	[TACACS Network Admin]
6.	<input type="checkbox"/>	[TACACS Help Desk]
7.	<input type="checkbox"/>	[TACACS API Admin]
8.	<input type="checkbox"/>	[Other]
9.	<input type="checkbox"/>	[Onboard Windows]

Navigate to **Configuration->Identity->Local Users**. Click **Add User**. Enter the following information:

- User ID: test
- Name: Test User
- Password: test123
- Verify Password: test123
- Enable User: *checked*
- Role: TestRole

Add Local User

User ID	<input type="text" value="test"/>
Name	<input type="text" value="TestUser"/>
Password	<input type="password" value="....."/>
Verify Password	<input type="password" value="....."/>
Enable User	<input checked="" type="checkbox"/> (Check to enable local user)
Role	<input type="text" value="TestRole"/>

Attributes

Attribute	Value
1. Click to add...	

Add **Cancel**

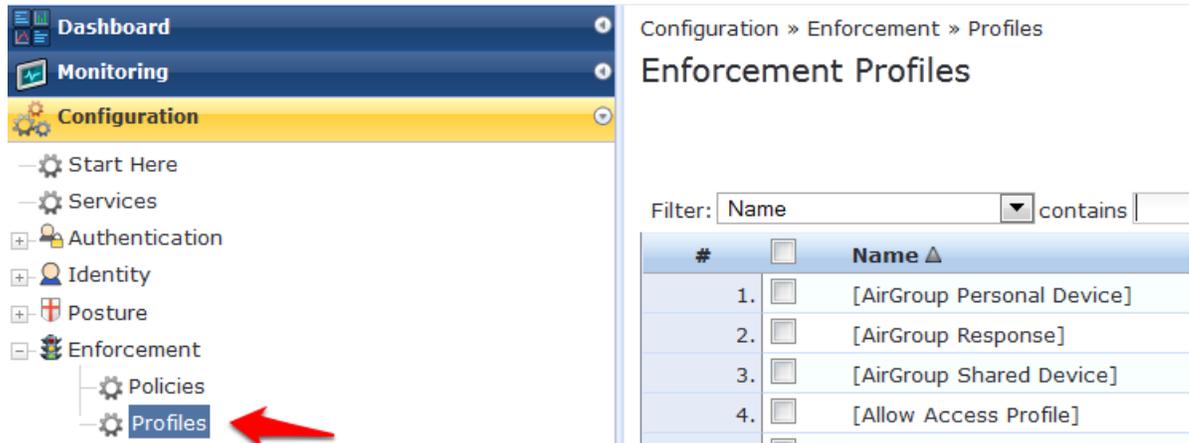
Click **Add**.

3. Testing the 802.1x and Guest SSID

At this point testing of the 802.1x and Guest SSID could commence. However, when 802.1x is tested with the Test User account, the user will authenticate but receive the guest role on the controller. This is because an Aruba User Role is not being passed back for the Test User. When the controller receives the RADIUS Accept from a successful authentication, the controller will give the client the default 802.1x role set in the AAA Profile.

In order to pass back an Aruba User Role, an Enforcement Profile must be built and the Sample Allow Access Policy must be modified to send this Enforcement Profile.

Navigate to **Configuration->Enforcement->Profiles**.



Configuration » Enforcement » Profiles

Enforcement Profiles

Filter: Name [v] contains []

#	<input type="checkbox"/>	Name ▲
1.	<input type="checkbox"/>	[AirGroup Personal Device]
2.	<input type="checkbox"/>	[AirGroup Response]
3.	<input type="checkbox"/>	[AirGroup Shared Device]
4.	<input type="checkbox"/>	[Allow Access Profile]

Click **Add Enforcement Policy** in the top right corner of the page.

Give it a name like “Aruba Authenticated Role”. Make sure the Template selected is Aruba RADIUS Enforcement:

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile | Attributes | Summary

Template:  Aruba RADIUS Enforcement

Name: Aruba Authenticated Role

Description:

Type: RADIUS

Action: Accept Reject Drop

Device Group List:

--Select--

Remove
View Details
Modify

Click **Next**.

Click on “Enter role here” and enter “authenticated” as the role to be passed back. Then click on the disk



icon to save the line.

Click **Save**.

Enforcement Profiles

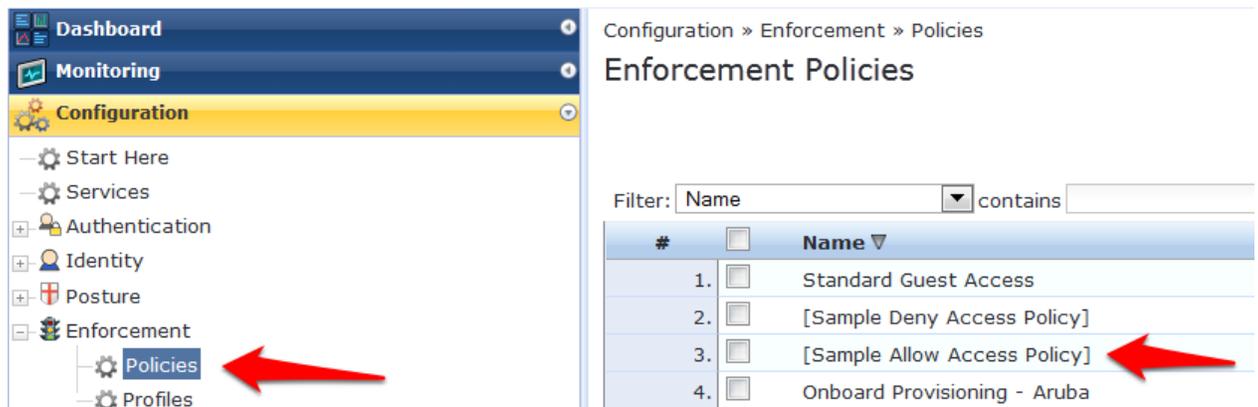


Tech Tip: Get used to clicking that disk icon. Whenever you edit a line like this, click the disk icon to save the line, or else your change may not get saved.

Click **Next**.

Click **Save**.

Navigate to **Configuration->Enforcement->Policies**. Click on the “Sample Allow Access Policy” to edit.



Click on the **Rules** tab. Click on the only Condition in the list to highlight it, and click **Edit Rule**.



Select the “Aruba Authenticated Profile” from the “— Select to Add—” drop down menu to the list of Enforcement Profiles that will be executed when a user successfully authenticates:

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value	
1. Date	Day-of-Week	BELONGS_TO	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday	
2. Click to add...				

Enforcement Profiles

Profile Names:

[RADIUS] Allow Access Profile

[RADIUS] Aruba Authenticated Role

--Select to Add--

Move Up

Move Down

Remove

Save **Cancel**

Click **Save** the the **Rules Editor** window.

Click **Save** in the lower right corner of the page.

Step 8: Test the 802.1x SSID

Connect to the 802.1x SSID, and login with the local user account (NOT the guest account) created in the ClearPass Policy Manager setup.

Navigate to **Monitoring->Live Monitoring->Access Tracker**.



A RADIUS ACCEPT for the WLAN Enterprise Service server should be visible.

Access Tracker Nov 01, 2012 15:09:01 PDT Auto Refresh

Data Filter: [All Requests] Server: (10.1.1.20)
Date Range: Last 1 day before Today Edit

Filter: Type contains Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time
10.1.1.20	RADIUS	test	WLAN Enterprise Service	ACCEPT	2012/11/01 15:08:46

Step 9: Testing the Guest SSID

At this point, both the 802.1x SSID and the Guest SSID can be tested. Start by testing the Guest SSID.

In ClearPass Policy Manager navigate to **Monitoring->Live Monitoring->Access Tracker**.

When your device first connects to the Guest SSID you will notice a MAC Auth REJECT. This is for the MAC Caching on the Guest SSID.

Access Tracker Nov 07, 2012 15:51:05 PST Auto Refresh

Data Filter: [All Requests] Server: (10.1.1.20)
Date Range: Last 1 day before Today Edit

Filter: Type contains Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	REJECT	2012/11/07 15:50:33

Open up a web browser on your device that just connected. It should redirect you to the Guest Login page. Select "Click Here" after **Need an account?**

Network Login

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

Network Login	
* Username:	<input type="text"/>
* Password:	<input type="password"/>
* Terms:	<input type="checkbox"/> I accept the terms of use
	

* required field

Need an account? [Click Here](#)

You will be then be presented with the Guest Account Creation page.

Guest Registration

Please complete the form below to gain access to the network.

Visitor Registration	
* Your Name:	<input type="text"/> <small>Please enter your full name.</small>
* Email Address:	<input type="text"/> <small>Please enter your email address. This will become your username to log into the network.</small>
* Confirm:	<input type="checkbox"/> I accept the terms of use
	

* required field

Enter the information (Email Address will become the guest username), check the box to accept the terms of use, and click Register.

You will then be presented with the Guest Registration Receipt that shows the guest username and password.

Guest Registration Receipt

The details for your guest account are shown below.

Visitor Registration Receipt	
Sponsor's Name:	admin
Visitor's Name:	Test User
Account Username:	 test@test.com
Visitor Password:	 76435597
Expiration Time:	Friday, 02 November 2012, 01:24 PM
	

Clicking “Log In” will automatically submit these credentials to the wireless controller’s internal captive portal, which will in turn create a RADIUS request with the Authentication Method PAP. This request will hit the Guest SSID Login Service that was created in ClearPass Policy Manager in the previous step.

After logging in on the test device, return to Access Tracker in ClearPass Policy Manager.

Notice the RADIUS ACCEPT entry for [test@test.com](#):

Filter: contains Show records

Server	Type	User	Service Name	Login	Date and Time ▾
10.1.1.20	RADIUS	test@test.com	Guest Access With MAC Caching	ACCEPT	2012/11/07 15:52:34
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	REJECT	2012/11/07 15:50:33

STOP! Wait 3 minutes before proceeding to the next step. For MAC Caching, the service queries the Insight Database. Information is pushed to the Insight Database every 3 minutes.

Testing the MAC Caching

The next steps test the MAC Caching.

1. SSH to your controller and run the “show user-table | include [test@test.com](#)” in order to find the MAC address of the test device.
2. Disable the wireless on the test device and run the “aaa user delete mac 00:aa:22:bb:44:cc” command where “00:aa:22:bb:44:cc” is the MAC address returned from the show user-table command.
3. Re-enable the wireless on the test device. Now in Access Tracker you will see a successful MAC authentication.

Filter: contains Show records

Server	Type	User	Service Name	Login	Date and Time ▾
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	ACCEPT	2012/11/07 15:57:55
10.1.1.20	RADIUS	test@test.com	Guest Access With MAC Caching	ACCEPT	2012/11/07 15:52:34
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	REJECT	2012/11/07 15:50:33

Advanced Features

Controller Management Login Authentication with ClearPass Policy Manager

In ClearPass Policy Manager, navigate to **Configuration->Identity->Roles**.

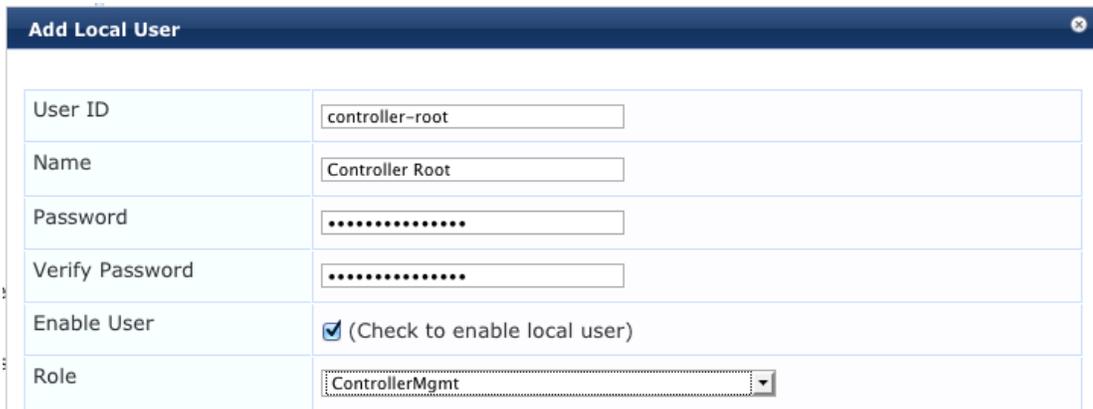
Click **Add Roles**.

Create a new role called "ControllerMgmt."

Navigate to **Configuration->Identity->Local Users**.

Click **Add User**.

Enter the information in the image below, using whatever you want for the password (this will be the login and password for managing the controller):

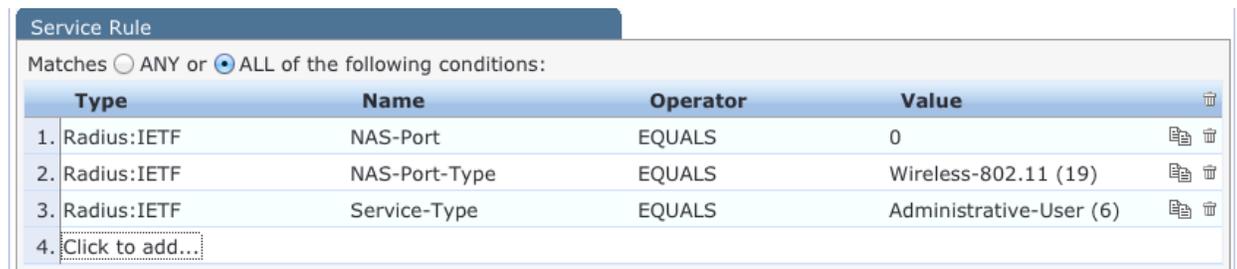


User ID	controller-root
Name	Controller Root
Password
Verify Password
Enable User	<input checked="" type="checkbox"/> (Check to enable local user)
Role	ControllerMgmt

Click **Add** to save this user account.

Navigate to **Configuration->Start Here**.

Click on RADIUS Enforcement (Generic). Give the service a name such as "Aruba Controller Management Login." Add the Service Rules in the image below:



Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port	EQUALS	0	
2. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	
3. Radius:IETF	Service-Type	EQUALS	Administrative-User (6)	
4. Click to add...				

Remember to click the disk at the end of each line in order to save the line.

Click **Next**.

For "Authentication Methods", Click the "Select to Add" down arrow and choose "[MACHAP]."

For "Authentication Sources," Click the "Select to Add" down arrow and choose [Local User Repository] [Local SQL DB]

Summary	Service	Authentication	Roles	Enforcement
Authentication Methods:	[MSCHAP]		<input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>	Add new Authentication Method
Authentication Sources:	[Local User Repository] [Local SQL DB]		<input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/>	Add new Authentication Source
Strip Username Rules:	<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes			

Click **Next**.

Tech Tip: You could use a Role Mapping Policy, but it is not required. It would be required if the Authentication source was Active Directory, in which case you would create a Role Mapping rule that would look for Authorization: SomeADServer:MemberOf:Contains:IT-Admins; Role Name: ControllerMgmt.

Click **Next**.

On the **Enforcement** tab, Click **Add new Enforcement Policy**. Give the new Enforcement Policy a name like “Controller Login Enforcement.”

Enforcement	Rules	Summary
Name:	Controller Login Enforcement	
Description:		
Enforcement Type:	<input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+ <input type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application	
Default Profile:	--Select to Add--	<input type="button" value="View Details"/> <input type="button" value="Modify"/> Add new Enforcement Profile

Click **Add new Enforcement Profile**. Use the Aruba RADIUS Enforcement template. Enter a name for the Enforcement Profile such as “Aruba MGMT Root User.”

Click **Next**. Match the Attribute to the following image

(**Note:** “Aruba-User-Role” is changed to “Aruba-Admin-Role”):

Profile	Attributes	Summary									
<table border="1"> <thead> <tr> <th>Type</th> <th>Name</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>1. Radius:Aruba</td> <td>Aruba-Admin-Role (4)</td> <td>= root</td> </tr> <tr> <td>2. Click to add...</td> <td></td> <td></td> </tr> </tbody> </table>			Type	Name	Value	1. Radius:Aruba	Aruba-Admin-Role (4)	= root	2. Click to add...		
Type	Name	Value									
1. Radius:Aruba	Aruba-Admin-Role (4)	= root									
2. Click to add...											

Remember to click the Save Disk at the end of the line.

Click **Next**.

Click **Save**. This will return you to the Enforcement Policy creation. Change the **Default Profile** to “Deny Access Profile.”

Enforcement	Rules	Summary
Name:	Controller Login Enforcement	
Description:		
Enforcement Type:	<input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+ <input type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application	
Default Profile:	[Deny Access Profile]	View Details Modify Add new Enforcement Profile

Click **Next**.

On the **Rules** tab, click **Add Rule**.

Enter the Rule **Conditions** and **Enforcement Profiles** as shown in the image below:

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Tips	Role	EQUALS	ControllerMgmt
2. Click to add...			

Enforcement Profiles

Profile Names:

- [RADIUS] Aruba MGMT Root User

--Select to Add--

Buttons: Move Up, Move Down, Remove

Buttons: Save, Cancel

Click **Save**. Click **Next**.

Click **Save** to log the Enforcement Policy.

The newly created Enforcement Policy should automatically be selected for the Service in the Service creation flow.

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	Controller Login Enforcement		Modify	Add new Enforcement Policy
Enforcement Policy Details				
Description:				
Default Profile:	[Deny Access Profile]			
Rules Evaluation Algorithm:	first-applicable			
Conditions		Enforcement Profiles		
1. (Tips:Role EQUALS ControllerMgmt)		Aruba MGMT Root User		

Click **Next**.

Click **Save**.

Note: Reorder the service so that it is **above** the Guest – MAC caching generic service.

Click **Save**.

Login to the wireless controller GUI.

Navigate to **Configuration->Management->Administration**.

1. Change Default Role to “no-access.”
2. Check the checkbox for **Enable**.
3. Check the checkbox for **MSCHAPv2**.
4. Change the **Server Group** to the ClearPass Policy Manager server group created earlier in this document.

Management Authentication Servers

Allow Local Authentication

Default Role	no-access	Enable	<input checked="" type="checkbox"/>
MSCHAPv2	<input checked="" type="checkbox"/>		

Server Group > cp60-sg

Show Reference Save As Reset

Important! Leave the **Allow Local Authentication** box checked. If this box is unchecked and there is a problem with the Management Authentication configuration, you will not be able to login to the controller if **Allow Local Authentication** is unchecked.

Click **Apply** to save these settings.

Logout of the controller and test login with the controller-root test user created earlier.

In Access Tracker you should see the RADIUS ACCEPT for the controller-root test user:

Filter: Type contains [] + Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time
10.1.1.20	RADIUS	controller-root	Aruba Controller Management Login	ACCEPT	2012/11/01 16:36:50

Troubleshooting

Problem:

MAC Caching is not working.

Solution:

Check the Endpoints Repository (Identity->Endpoints) for the device in question. Click on the device and verify that the device status is set to Known. If it is not, verify that the correct controller-ip vlan has been set on the wireless controller.

Problem:

During creation of Enforcement Policy, an error appears when trying to save: Name contains special characters...

Solution:

Creation of the Enforcement Policy has timed out. Click Cancel, then create the Enforcement Policy again.