ARUBA WIRELESS AND CLEARPASS 6 INTEGRATION GUIDE
Copyright

© 2013 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®, RFProtect®, 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
6. **Troubleshooting** .................................................................................................................. 62

5. **Advanced Features** ............................................................................................................. 55

   *Controller Management Login Authentication with ClearPass Policy Manager*.................. 55

   *RADIUS Enforcement (Generic) configuration*..................................................................... 55

4. **Testing the MAC Caching** ................................................................................................. 54

3. **Testing the 802.1x and Guest SSID** ................................................................................ 48

   Step 9: Test the 802.1x SSID.................................................................................................... 51

   Step 10: Testing the Guest SSID........................................................................................... 51

2. **ClearPass Policy Manager Setup** .................................................................................... 39

   Guest SSID Login service configuration ............................................................................. 44

1. **Aruba Wireless and ClearPass 6.0.1 Integration Guide** ..................................................... 10

   Purpose ..................................................................................................................................... 10

   Assumptions ............................................................................................................................ 10

   Step 1: AOS Controller Configuration ................................................................................... 10

   Step 2: Adding a RFC 3576 Server ...................................................................................... 12

   Step 3: Creating a new Server Group for ClearPass ............................................................. 14

   Step 4: Create a Captive Portal role ...................................................................................... 20

   Step 5: Pre-configured Firewall Policies ............................................................................ 25

   Step 6: Creating AAA Profiles for the ClearPass Guest and 802.1x SSID ......................... 26

   Step 7: Associating a 802.1x SSID and Guest SSID with AAA Profiles .............................. 32

   Step 8: ClearPass Guest Setup ............................................................................................ 34

Basic Guest Registration and Login configuration ................................................................. 34

Contents

Audience ................................................................................................................................. 8

Typographic Conventions ...................................................................................................... 8

Contacting Support ................................................................................................................ 9

1. **Aruba Wireless and ClearPass 6.0.1 Integration Guide** ..................................................... 10

   Purpose ..................................................................................................................................... 10

   Assumptions ............................................................................................................................ 10

   Step 1: AOS Controller Configuration ................................................................................... 10

   Step 2: Adding a RFC 3576 Server ...................................................................................... 12

   Step 3: Creating a new Server Group for ClearPass ............................................................. 14

   Step 4: Create a Captive Portal role ...................................................................................... 20

   Step 5: Pre-configured Firewall Policies ............................................................................ 25

   Step 6: Creating AAA Profiles for the ClearPass Guest and 802.1x SSID ......................... 26

   Step 7: Associating a 802.1x SSID and Guest SSID with AAA Profiles .............................. 32

   Step 8: ClearPass Guest Setup ............................................................................................ 34

Basic Guest Registration and Login configuration ................................................................. 34

2. **ClearPass Policy Manager Setup** .................................................................................... 39

   Guest SSID Login service configuration ............................................................................. 44

3. **Testing the 802.1x and Guest SSID** ................................................................................ 48

   Step 9: Test the 802.1x SSID.................................................................................................... 51

   Step 10: Testing the Guest SSID........................................................................................... 51

4. **Testing the MAC Caching** ................................................................................................. 54

5. **Advanced Features** ............................................................................................................. 55

   *Controller Management Login Authentication with ClearPass Policy Manager*.................. 55

   *RADIUS Enforcement (Generic) configuration*..................................................................... 55

6. **Troubleshooting** .................................................................................................................. 62
Figure 1 Adding a RADIUS Server .......................................................... 11
Figure 2 RADIUS Server list ................................................................. 11
Figure 3 RADIUS server IP and Key entry ............................................. 11
Figure 4 RFC 3576 Server list ................................................................. 12
Figure 5 Adding a RF 3576 Server .......................................................... 13
Figure 6 RFC 3576 Server IP ................................................................. 13
Figure 7 Enter the RADIUS shared key ................................................. 14
Figure 8 ClearPass Server Group ............................................................ 14
Figure 9 Adding a ClearPass Server Group ............................................. 15
Figure 10 ClearPass Server Group list .................................................... 15
Figure 11 Adding a ClearPass RADIUS Server ...................................... 16
Figure 12 Selecting the newly created ClearPass Server Group ............... 16
Figure 13 Select Add Server ClearPass button ...................................... 17
Figure 14 L3 Authentication tab .............................................................. 17
Figure 15 Select Captive Portal Authentication Profile ............................. 18
Figure 16 Enter a new Captive Portal profile name ................................ 18
Figure 17 Select the newly created Captive Portal Authentication Profile .... 19
Figure 18 Captive Portal Authentication Profile login page IP ................. 19
Figure 19 Changing "default" server group to the newly created Captive Portal Authentication Profile server name... 20
Figure 20 The newly created Captive Portal Authentication Profile server Group ................................................................. 20
Figure 21 User Roles tab ........................................................................ 21
Figure 22 Adding a User Role ................................................................. 21
Figure 23 Create new User Role Policy ................................................... 22
Figure 24 Entering the Policy Name and Policy Type ............................... 22
Figure 25 Entering the ACL (Access Control List) field names ............... 23
Figure 26 Firewall policy rule Add button .............................................. 23
Figure 27 Adding a svc-https (tcp 443 Service ACL) ............................. 24
Figure 28 Accepting the ACL rows created .......................................... 24
Figure 29 User Roles Add page listings ................................................. 24
Figure 30 Firewall logon-control (session) policy .................................. 25
Figure 31 Firewall "captiveportal (session)" policy ................................................................. 25
Figure 33 Firewall Policies list ................................................................................................. 26
Figure 33 Aruba_admin captive portal being chosen ............................................................... 26
Figure 34 Select the previously configured Captive Portal Profile ........................................ 26
Figure 35 Adding a ClearPass Guest Profile ............................................................................ 27
Figure 36 Changing the default Initial role ............................................................................ 27
Figure 37 RADIUS Interim Accounting option ..................................................................... 28
Figure 38 Log Accounting Interim-Update Packets option in CPPM ...................................... 28
Figure 39 MAC Authentication Profile setting = default ....................................................... 29
Figure 40 MAC Authentication Server Group option .............................................................. 29
Figure 41 RADIUS Accounting Server Group option ............................................................. 30
Figure 42 RFC 3576 for this AAA Profile ............................................................................... 31
Figure 43 IP address of your ClearPass server ...................................................................... 31
Figure 44 Configuring no MAC Authentication Profile ......................................................... 32
Figure 45 Advanced Services All Profiles menu ................................................................. 32
Figure 46 Advanced Services Wireless LAN Profile ............................................................ 33
Figure 47 Advanced Services Virtual AP Profile ................................................................. 33
Figure 48 Virtual AP Profile modifications .......................................................................... 34
Figure 49 Policy Manager login ......................................................................................... 34
Figure 50 ClearPass Policy Manager Dashboard .................................................................. 35
Figure 51 ClearPass Guest Quick Link .................................................................................. 35
Figure 52 ClearPass Guest administration page .................................................................... 36
Figure 53 ClearPass Guest Self-Registration selection ......................................................... 36
Figure 54 ClearPass Guest Self-Registration menu .............................................................. 37
Figure 55 NAS Vendor Settings ......................................................................................... 37
Figure 56 Enable guest login to a Network Access Server ................................................... 38
Figure 57 ClearPass Policy Manager Network Devices selection ........................................ 39
Figure 58 Add a ClearPass Policy Manager Network Device .............................................. 39
Figure 59 Configuring a ClearPass Policy Manager Network Device .................................. 40
Figure 60 Aruba 802.1X Wireless 'Start Here' selection ....................................................... 40
Figure 61 Naming a 802.1X Wireless Service .................................................................... 41
Figure 62 802.1X Authentication Methods and Sources ....................................................... 41
Figure 63 802.1X Role Mapping Policy .............................................................................. 42
Figure 64 802.1X Enforcement configuration ...................................................................... 42
Figure 65 ClearPass Policy Manager Reorder menu ............................................................. 43
Preface

Audience

This Aruba Wireless and ClearPass 6 Integration Guide is intended for system administrators and people who are integrating Aruba Networks Wireless Hardware with ClearPass 6.0.1.

Typographic Conventions

The following conventions are used throughout this manual to emphasize important concepts.

<table>
<thead>
<tr>
<th>Type Style</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Italics</em></td>
<td>Used to emphasize important items and for the titles of books.</td>
</tr>
<tr>
<td><strong>Boldface</strong></td>
<td>Used to highlight navigation in procedures and to emphasize command names and parameter options when mentioned in text.</td>
</tr>
<tr>
<td>Sample template code or HTML text</td>
<td>Code samples are shown in a fixed-width font.</td>
</tr>
</tbody>
</table>
| <angle brackets>            | When used in examples or command syntax, text within angle brackets represents items you should replace with information appropriate to your specific situation. For example: ping <ipaddr>
                                In this example, you would type “ping” at the system prompt exactly as shown, followed by the IP address of the system to which ICMP echo packets are to be sent. Do not type the angle brackets. |
## Contacting Support

<table>
<thead>
<tr>
<th>Main Site</th>
<th>arubanetworks.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Site</td>
<td>support.arubanetworks.com</td>
</tr>
<tr>
<td>Airheads Social Forums and Knowledge Base and Knowledge Base</td>
<td>community.arubanetworks.com</td>
</tr>
<tr>
<td>North American Telephone</td>
<td>1-800-943-4526 (Toll Free)</td>
</tr>
<tr>
<td></td>
<td>1-408-754-1200</td>
</tr>
<tr>
<td>International Telephones</td>
<td><a href="http://www.arubanetworks.com/support-services/aruba-support-program/contact-support/">http://www.arubanetworks.com/support-services/aruba-support-program/contact-support/</a></td>
</tr>
<tr>
<td>Software Licensing Site</td>
<td><a href="https://licensing.arubanetworks.com/">https://licensing.arubanetworks.com/</a></td>
</tr>
<tr>
<td>Wireless Security Incident Response Team (WSIRT)</td>
<td><a href="http://www.arubanetworks.com/support-services/security-bulletins/">http://www.arubanetworks.com/support-services/security-bulletins/</a></td>
</tr>
</tbody>
</table>

### Support Email Addresses

- **Americas and APAC**
  - support@arubanetworks.com
- **EMEA**
  - emea_support@arubanetworks.com
- **WSIRT Email**
  - wsirt@arubanetworks.com

Please email details of any security problem found in an Aruba product.
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.
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**.
Click on the new server name that shows up in the RADIUS Server list on that page:

Figure 2 RADIUS Server list

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.

Figure 3 RADIUS server IP and Key entry
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.

Figure 4 RFC 3576 Server list

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

**Figure 8 ClearPass Server Group**

Enter a reference name for your ClearPass Server Group in the empty box and click **Add**.
Select the newly created Server Group on the right under Server Group:

Click **New** and select the ClearPass RADIUS server from the previous step.
2. Click **Add Server**. Click **Apply** at the bottom of the page to save the changes.
Figure 13 Select Add Server ClearPass button

Captive Portal profile

Click on the **L3 Authentication tab**.

Figure 14 L3 Authentication tab

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

Select the newly created Captive Portal Authentication Profile under Captive Portal Authentication Profile on the right.
Figure 17 Select the newly created Captive Portal Authentication Profile

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

3. 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.

Figure 18 Captive Portal Authentication Profile login page IP

Click Apply at the bottom to save the changes.

4. 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.
Figure 19 Changing "default" server group to the newly created Captive Portal Authentication Profile server name

Security > Authentication > L3 Authentication

![Diagram showing server group change]

Figure 20 The newly created Captive Portal Authentication Profile server Group

Security > Authentication > L3 Authentication

![Diagram showing server group change]

Step 4: 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.
Enter a name like `<CPG-Login>` for the **Role Name** under **Firewall Policies**, Click **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:
Enter and select the following information:

- **Policy Name**: `<CP6-web-ACL>`
- **Policy Type**: `<Session>`

Click **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>`

Figure 25 Entering the ACL (Access Control List) field names

Security > User Roles > Add Role > Add New Policy

![Policy Name and Policy Type](image)

<table>
<thead>
<tr>
<th>IP Version</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Log</th>
<th>Mirror</th>
<th>Queue</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>host</td>
<td>service</td>
<td>svc-http (tcp 80)</td>
<td>permit</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Figure 26 Firewall policy rule Add button

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

Choose **Service**: `svc-https (tcp 443)`
Figure 27 Adding a svc-https (tcp 443) Service ACL

Security > User Roles > Add Role > Add New Policy

![Policy Table](image)

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

Figure 28 Accepting the ACL rows created

Security > User Roles > Add Role > Add New Policy

![ACL Rows](image)

Click **Done**

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

Figure 29 User Roles Add page listings

Security > User Roles > Add Role

![User Roles Add Page](image)
Step 5: 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).

Figure 30 Firewall logon-control (session) policy

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).

Figure 31 Firewall “captiveportal (session)” policy
Click **Done** in the **Firewall Policies** section. Your Firewall Policy should look like this:

![Firewall Policies](image)

**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.

![Captive Portal Profile](image)

Click the **Change** button.

![Captive Portal Profile](image)

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

![Captive Portal Profile](image)

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

**Step 6: 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.
Figure 35 Adding a ClearPass Guest Profile

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 Step 4: Create a Captive Portal role page 20.

Figure 36 Changing the default Initial role

**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.
Figure 37 RADIUS Interim Accounting option

<table>
<thead>
<tr>
<th>Security &gt; Authentication &gt; Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Profiles</td>
</tr>
<tr>
<td>L2 Authentication</td>
</tr>
<tr>
<td>L3 Authentication</td>
</tr>
<tr>
<td>User Rules</td>
</tr>
<tr>
<td>Advanced</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AAA Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>108_7_coppm_health</td>
</tr>
<tr>
<td>108_7_onboard_issued</td>
</tr>
<tr>
<td>108_7_onboard_dottx_aaa</td>
</tr>
<tr>
<td>110_101_coppm_dottx_aaa</td>
</tr>
<tr>
<td>110_104_coppm_dottx_aaa</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AAA Profile &gt; cp-60_cpg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial role</td>
</tr>
<tr>
<td>108_7_coppm_cp</td>
</tr>
<tr>
<td>802.1X Authentication Default Role</td>
</tr>
<tr>
<td>guest</td>
</tr>
<tr>
<td>RADIUS Interim Accounting</td>
</tr>
<tr>
<td>Wired to Wireless Roaming</td>
</tr>
<tr>
<td>Device Type Classification</td>
</tr>
</tbody>
</table>

Note: 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".

Figure 38 Log Accounting Interim-Update Packets option in CPPM

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

MAC Authentication Profile: default
Figure 39 MAC Authentication Profile setting = default

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

Figure 40 MAC Authentication Server Group option

RADIUS Accounting Server Group: *(Your ClearPass 6.0.1 Server Group)*
Figure 41 RADIUS Accounting Server Group option

Click on RFC 3576 for this AAA Profile.
Figure 42 RFC 3576 for this AAA Profile

Security > Authentication > Profiles

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

Figure 43 IP address of your ClearPass server

Click **Apply** to save these settings.

Repeat Creating AAA Profiles for the ClearPass Guest and 802.1x SSID, page 26, 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:
Step 7: 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.

Figure 45 Advanced Services All Profiles menu
Expand the **Wireless LAN** section.

Figure 46 Advanced Services Wireless LAN Profile

`Advanced Services > All Profile Management`

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

Figure 47 Advanced Services Virtual AP Profile

`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 8: ClearPass Guest Setup**

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

**Basic Guest Registration and Login configuration**


Figure 49 Policy Manager login
After you login, you will see the ClearPass Policy Manager Dashboard.

Figure 50 ClearPass Policy Manager Dashboard

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

Figure 51 ClearPass Guest Quick Link

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

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.
Figure 56 Enable guest login to a Network Access Server

Click **Save Changes**.
2. **ClearPass Policy Manager Setup**

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

Figure 57 ClearPass Policy Manager Network Devices selection

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

Figure 58 Add a ClearPass Policy Manager Network Device

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**
Click **Add**.

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

Give the service a name such as <WLAN Enterprise Service>.
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**.

Figure 62 802.1X Authentication Methods and Sources

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.

Figure 63 802.1X Role Mapping Policy

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

Figure 64 802.1X Enforcement configuration

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.

Figure 65 ClearPass Policy Manager Reorder menu

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.
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**.

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

Repeat those steps for the **Guest MAC Authentication** service:

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 Role** in the top right corner of the page.
Enter <TestRole> as the name, and click **Save**.

Figure 71 Adding a Identity Role

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: check box <(Check to enable local user)>
- Role: select <TestRole> from the drop down menu
Figure 72 Guest SSID Local User conditions

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.

![Figure 73 Configuring Enforcement Profiles](image)

Click Add Enforcement Profile 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:
Click **Next**.

Click on "Enter role here" and enter `<authenticated>` in the **Value** field as the role to be passed back. Then click on the disk icon to save the line.

Click **Save**.

**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:

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

Click **Save** in the lower right corner of the page.
Step 9: 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.


Figure 78 Live Monitoring Access Tracker menu

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

Figure 79 802.1x SSID RADIUS, ACCEPT WLAN Enterprise Service

Step 10: 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.


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.

Figure 80 MAC Auth REJECT for the MAC Caching on the Guest SSID

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?
Figure 81 ClearPass Guest Login

Network Login

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

![Network Login](image)

* required field

Need an account? [Click Here](#)

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

Figure 82 ClearPass Guest Registration

Guest Registration

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

![Visitor Registration](image)

* 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.

Figure 83 ClearPass Guest Registration Receipt

Guest Registration Receipt

The details for your guest account are shown below.

![Visitor Registration Receipt](image)

Clicking [Log In](#) button will automatically submit these credentials to the wireless controller's internal captive portal, which will 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:

Figure 84 RADIUS, ACCEPT configuration for a newly created 802.1x SSID Guest account

<table>
<thead>
<tr>
<th>Server</th>
<th>Type</th>
<th>User</th>
<th>Service Name</th>
<th>Login</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.20</td>
<td>RADIUS</td>
<td><a href="mailto:test@test.com">test@test.com</a></td>
<td>Guest Access With MAC Caching</td>
<td>ACCEPT</td>
<td>2012/11/07 15:52:34</td>
</tr>
<tr>
<td>10.1.20</td>
<td>RADIUS</td>
<td>7a-12:ab:3d:08:ab</td>
<td>Guest MAC Authentication</td>
<td>REJECT</td>
<td>2012/11/07 15:50:33</td>
</tr>
</tbody>
</table>

**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.
4. Testing the MAC Caching

The next steps test the MAC Caching.

1. SSH to your controller and run:
   ```
   show user-table | include <test@test.com>
   ```
   command where `<test@test.com>` is the 802.1x SSID guest user created, in order to find the MAC address of the test device.

2. Disable the wireless on the test device and run:
   ```
   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.

Figure 85 Successful MAC authentication
5. 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 from Figure 86 Adding a Controller Management Local User, using whatever you want for the password (this will be the login and password for managing the controller).

Figure 86 Adding a Controller Management Local User

Click Add to save this user account.

RADIUS Enforcement (Generic) configuration

Navigate to Configuration->Start Here.

Scroll down the right main column and click on RADIUS Enforcement (Generic).

Figure 87 RADIUS Enforcement (Generic) template

Service

Give the service a name such as <Aruba Controller Management Login>.

Add the Service Rules from Figure 88 RADIUS Enforcement (Generic) Service Rules configuration below for each Service Rule by selecting from each of their corresponding drop down arrow menu settings.
Remember to click the disk at the end of each Service Rule in order to save the line configuration.

Click Next.

Authentication

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

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

Click Next.

Roles

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 the following configuration:

Authorization: SomeADServer:MemberOf:Contains:IT-Admins;

Role Name: ControllerMgmt

Click Next.
**Enforcement**

On the **Enforcement** tab, Click **Add new Enforcement Policy**.

Give the new Enforcement Policy a name like <Controller Login Enforcement>.

Figure 90 RADIUS Enforcement (Generic) Enforcement configuration

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

Figure 91 RADIUS Enforcement (Generic) Enforcement Profile Template and Name

Click **Next**.

Add each Attribute from Figure 92 RADIUS Enforcement (Generic) Enforcement Attribute configuration below by selecting from each of their corresponding drop down arrow menu settings except for **Value**. Enter **root** in the **Value** field column.

**Note:** **Aruba-User-Role** is changed to **Aruba-Admin-Role**

Figure 92 RADIUS Enforcement (Generic) Enforcement Attribute configuration
Remember to click the disk at the end of each Attribute in order to save the line configuration.

Click Next.

Figure 93 RADIUS Enforcement (Generic) Enforcement configuration Summary

Click Save. This will return you to the Enforcement Policy creation.

Change the Default Profile to Deny Access Profile.

Click Next.

On the Rules tab, click Add Rule.

Enter the values from Figure 94 RADIUS Enforcement (Generic) Rule Conditions and Enforcement Profiles below for each Rules Editor Condition column by selecting their corresponding drop down arrow menu settings.
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.

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

**Note:** Reorder the service so that it is **above** the **Guest Access With MAC Caching** service.

![Reorder Services Diagram]

Click **Save**.

**Management Authentication Servers**

Login to the Aruba Controller Interface

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

```
<table>
<thead>
<tr>
<th>Allow Local Authentication</th>
<th>Default Role</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>no-access</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>MSCHAPv2</td>
<td>✓</td>
</tr>
</tbody>
</table>
```

**Server Group** > cp60-sg

**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 **Type** = RADIUS and **Login** = ACCEPT for the controller-root test user:

```
<table>
<thead>
<tr>
<th>Server</th>
<th>Type</th>
<th>User</th>
<th>Service Name</th>
<th>Login</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.20</td>
<td>RADIUS</td>
<td>controller-root</td>
<td>Aruba Controller Management Login</td>
<td>ACCEPT</td>
<td>2012/11/01 16:36:50</td>
</tr>
</tbody>
</table>
```
6. **Troubleshooting**

*Problem:*

MAC Caching is not working.

*Solution:*

Check the Endpoints Repository, navigate to **Configuration->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.