


AirGroup Configuration How-To with ClearPass 6.0.1



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®, 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

Audience.....	7
Typographic Conventions.....	7
Contacting Support.....	8
1. AirGroup Configuration How-to with ClearPass 6.0.1.....	9
Assumptions:.....	9
Step 1: Controller Configuration	9
Step 2: ClearPass Setup	11
Testing.....	17
Troubleshooting	18

Figure 1 Configuring a UDP port for AirGroup's RFC 3576.....	10
Figure 3 Airgroup AAA profile RFC 3576 server.....	11
Figure 4 Configure AirGroup Services	11
Figure 5 Add a new controller for AirGroup Services.....	12
Figure 6 Configure AirGroup Services controller settings.....	12
Figure 8 Adding a new Local User in CPPM.....	13
Figure 9 Create an AirGroup Administrator.....	14
Figure 10 Create an AirGroup Operator.....	14
Figure 11 Local Users GUI screen	15
Figure 12 Create a device	15
Figure 13 Register Shared Device.....	16

Audience

This AirGroup Configuration How-To with ClearPass 6.0.1 is intended for system administrators and people who are setting up AirGroup configuration with ClearPass 6.0.1.

Typographic Conventions

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

Type Style	Description
<i>Italics</i>	Used to emphasize important items and for the titles of books.
Boldface	Used to highlight navigation in procedures and to emphasize command names and parameter options when mentioned in text.
Sample template code or HTML text	Code samples are shown in a fixed-width font
<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

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	http://www.arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	https://licensing.arubanetworks.com/
End of Support information	www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support-services/security-bulletins/

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. AirGroup Configuration How-to with ClearPass 6.0.1

The purpose of this document is to walk through how-to setup AirGroup configuration with ClearPass 6.0.1. This document will use the Integrated Deployment Model.

Assumptions:

1. Controller is running the latest AirGroup AOS Technology Release (at the time of this document it was 6.1.3.4-Airgroup).
2. ClearPass 6.0.1 non-Beta version is installed.
3. **IPv6 is disabled** on the controller (command: `no ipv6 enable`).
4. Aruba Wireless and ClearPass 6 Integration Guide setup has already been completed.
5. An SSID with a PSK is setup for testing.
6. An up-to-date AppleTV is available for testing.
7. An Apple computer running Mountain Lion (10.8.2) or an iOS device running iOS 6 is available for testing.

Step 1: Controller Configuration

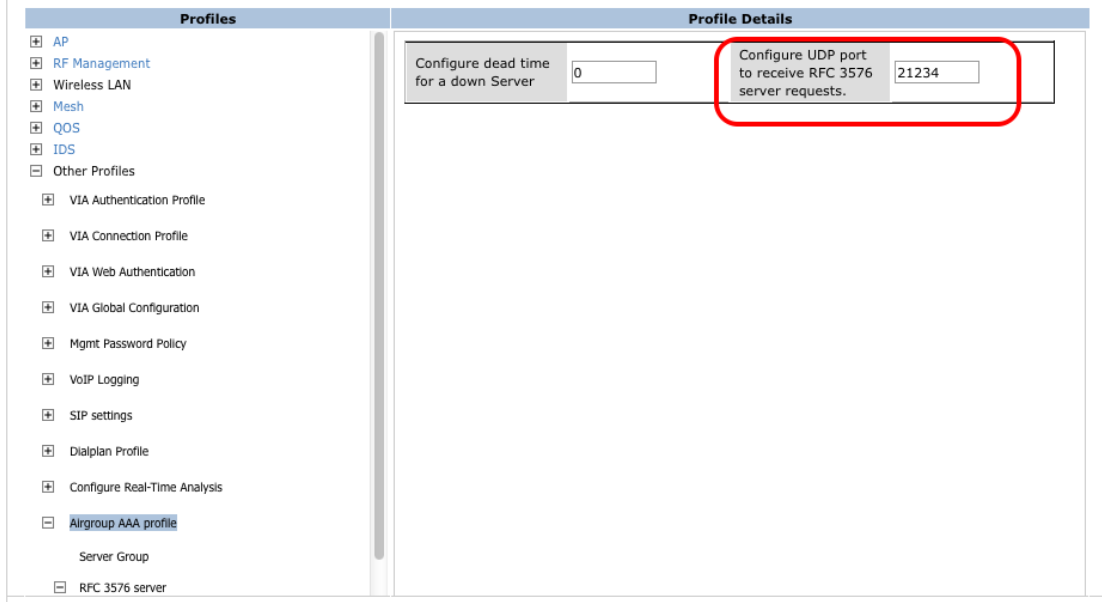
Use SSH to login to the controller and run the following command in configure terminal mode:

```
airgroup enable
firewall cp permit proto 17 ports 21234 21234
```

In the controller GUI, navigate to **Configuration->Advanced Services->All Profiles**. Expand **Other Profiles**. Click on **Airgroup AAA profile**. You must configure a UDP port for AirGroup's RFC 3576. You cannot use the default 3799. In the sample below, UDP port 21234 is used. Enter the port number in the 'Configure UDP port to receive RFC 3576 server requests' field and click **Apply**.

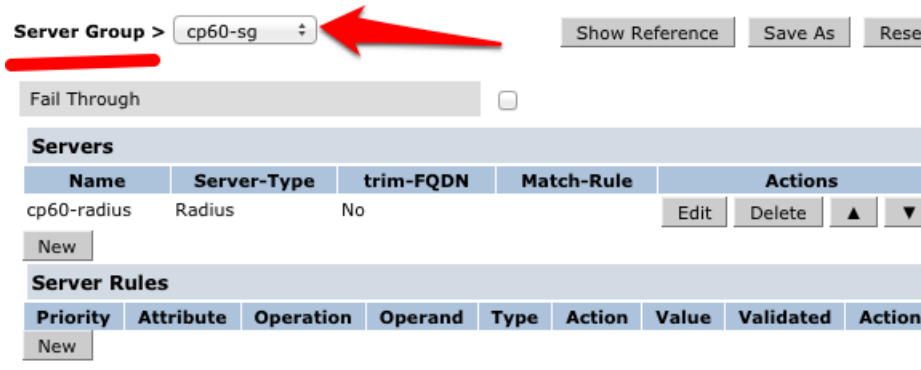
Figure 1 Configuring a UDP port for AirGroup's RFC 3576

Advanced Services > All Profile Management



Click on **Server Group** under **Airgroup AAA profile**. Select the ClearPass 6 server group that was created in the Aruba Wireless and ClearPass 6 Integration Guide.

Figure 2 ClearPass 6 server group previously created

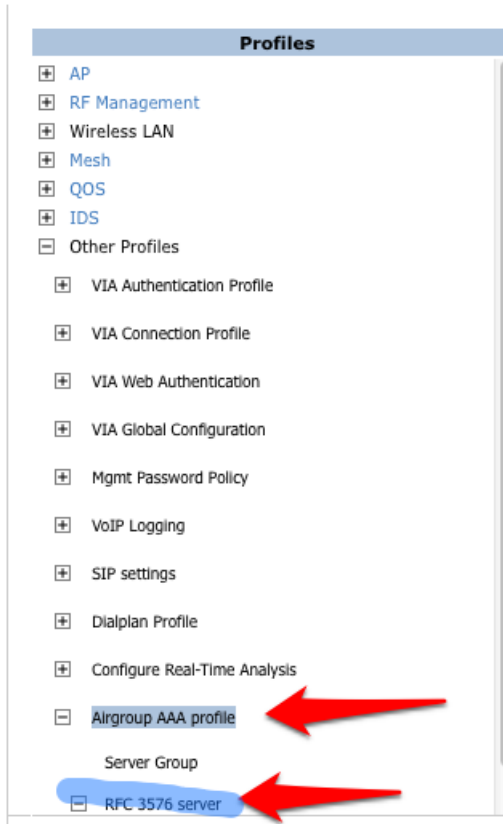


Click **Apply**.

Click on RFC 3576 server under **Airgroup AAA profile**.

Figure 3 Airgroup AAA profile RFC 3576 server

Advanced Services > All Profile Management



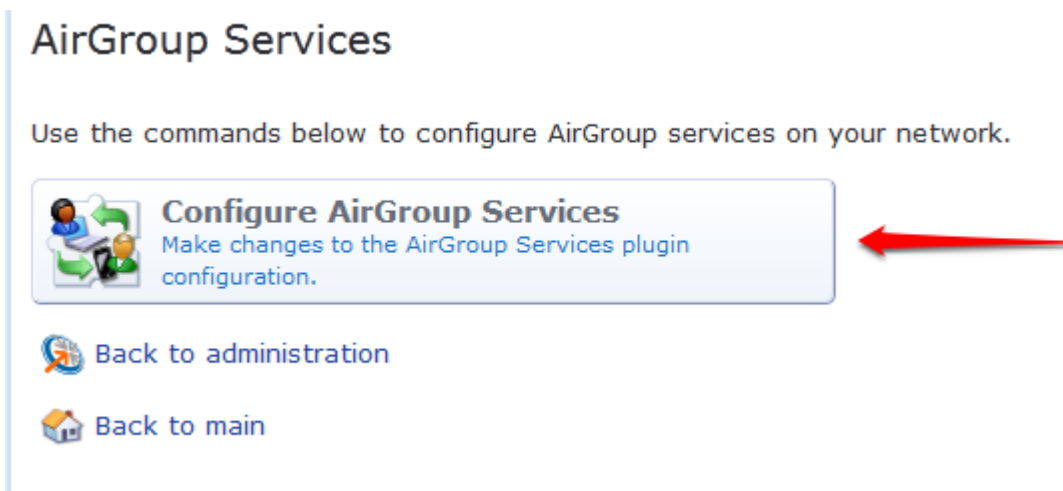
Again, use the RFC 3576 server that points to ClearPass 6 which was created in the previous setup guide.

Click **Apply**.

Step 2: ClearPass Setup

Open up ClearPass Guest and navigate to **Administration->AirGroup Services**. Click 'Configure AirGroup Services'.

Figure 4 Configure AirGroup Services



Click 'Add a new controller'.

Figure 5 Add a new controller for AirGroup Services

AirGroup Services 6.0.1-22806 Configuration

Set the configuration options for AirGroup Services 6.0.1-22806.

Configure AirGroup Services 6.0.1-22806															
* AirGroup Logging:	Standard (Recommended) – log basic information <small>Select an option for logging events related to AirGroup Services.</small>														
* Controllers:	<table border="1"><thead><tr><th>Use</th><th>Hostname</th><th>Port</th><th>Shared Secret</th></tr></thead><tbody><tr><td colspan="4">There are no items to display.</td></tr><tr><td colspan="4">Add a new controller</td></tr></tbody></table> <small>Define the Aruba controllers that should receive AirGroup asynchronous information updates.</small>			Use	Hostname	Port	Shared Secret	There are no items to display.				Add a new controller			
Use	Hostname	Port	Shared Secret												
There are no items to display.															
Add a new controller															
* Timeout:	5 seconds <small>Timeout for sending an AirGroup message.</small>														
* Attempts:	3 <small>Maximum number of attempts to use when sending an AirGroup message.</small>														
Save Configuration															

* required field

Enter the appropriate information.

Note: The port used in these setup instructions is 21234 and the shared secret was configured in the previous setup guide (where aruba123 was used as an example).

Figure 6 Configure AirGroup Services controller settings

AirGroup Services 6.0.1-22806 Configuration

Set the configuration options for AirGroup Services 6.0.1-22806.

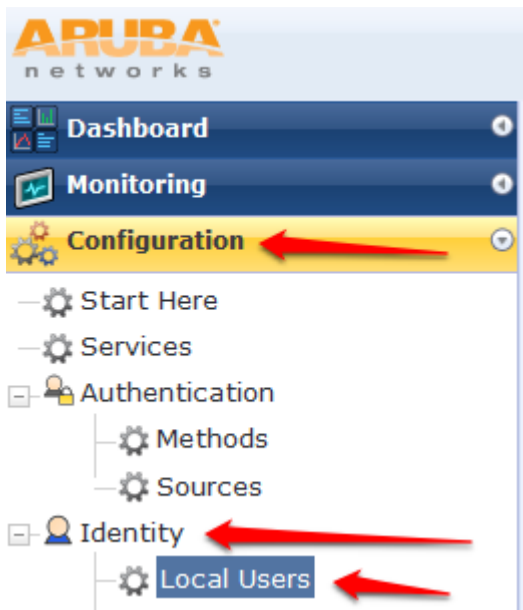
Configure AirGroup Services 6.0.1-22806																							
* AirGroup Logging:	Standard (Recommended) – log basic information <small>Select an option for logging events related to AirGroup Services.</small>																						
* Controllers:	<table border="1"><thead><tr><th>Use</th><th>Hostname</th><th>Port</th><th>Shared Secret</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td>10.1.1.10</td><td>21234</td><td>●●●●●●●●</td></tr><tr><td colspan="4"><small>Enable The controller's hostname or IP address. UDP port number. Shared secret for RFC 3576.</small></td></tr><tr><td colspan="4">Remove</td></tr><tr><td colspan="4">Add a new controller</td></tr></tbody></table> <small>Define the Aruba controllers that should receive AirGroup asynchronous information updates.</small>			Use	Hostname	Port	Shared Secret	<input checked="" type="checkbox"/>	10.1.1.10	21234	●●●●●●●●	<small>Enable The controller's hostname or IP address. UDP port number. Shared secret for RFC 3576.</small>				Remove				Add a new controller			
Use	Hostname	Port	Shared Secret																				
<input checked="" type="checkbox"/>	10.1.1.10	21234	●●●●●●●●																				
<small>Enable The controller's hostname or IP address. UDP port number. Shared secret for RFC 3576.</small>																							
Remove																							
Add a new controller																							
* Timeout:	5 seconds <small>Timeout for sending an AirGroup message.</small>																						
* Attempts:	3 <small>Maximum number of attempts to use when sending an AirGroup message.</small>																						
Save Configuration																							

* required field

Click **Save Configuration**.

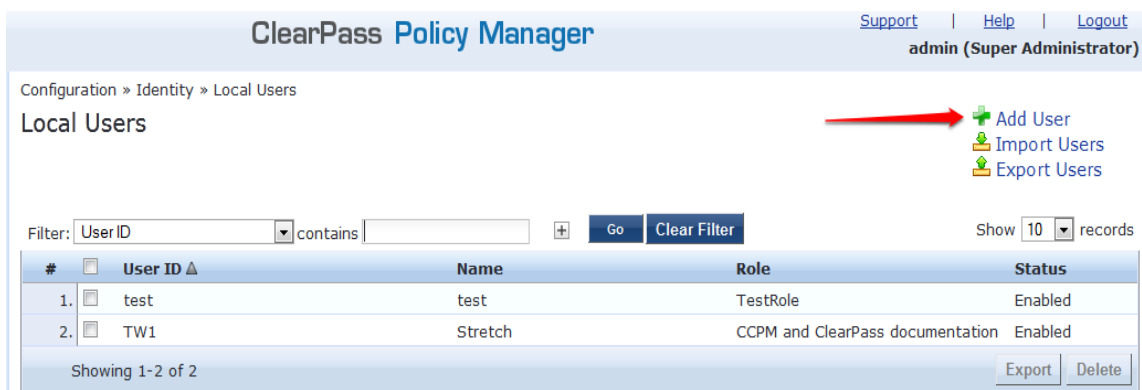
In order to demonstrate AirGroup, either an AirGroup Administrator or AirGroup Operator account must be created. Go to the ClearPass Policy Manager GUI, and navigate to **Configuration->Identity->Local Users**.

Figure 7 Configuration ->Identity->Local Users selection




Click **Add User**.

Figure 8 Adding a new Local User in CPPM



Create an **AirGroup Administrator**:

Figure 9 Create an AirGroup Administrator

User ID	airgroup-admin
Name	AirGroup Admin
Password
Verify Password
Enable User	<input checked="" type="checkbox"/> (Check to enable local user)
Role	[AirGroup Administrator] 


Attributes	
Attribute	Value
1.	Click to add...

Add **Cancel**

In this example, as in past documentation, the password used is test123. Click **Add**.

Now click **Add User**, and create an **AirGroup Operator**:

Figure 10 Create an AirGroup Operator

User ID	airgroup-oper
Name	AirGroup Operator
Password
Verify Password
Enable User	<input checked="" type="checkbox"/> (Check to enable local user)
Role	[AirGroup Operator] 

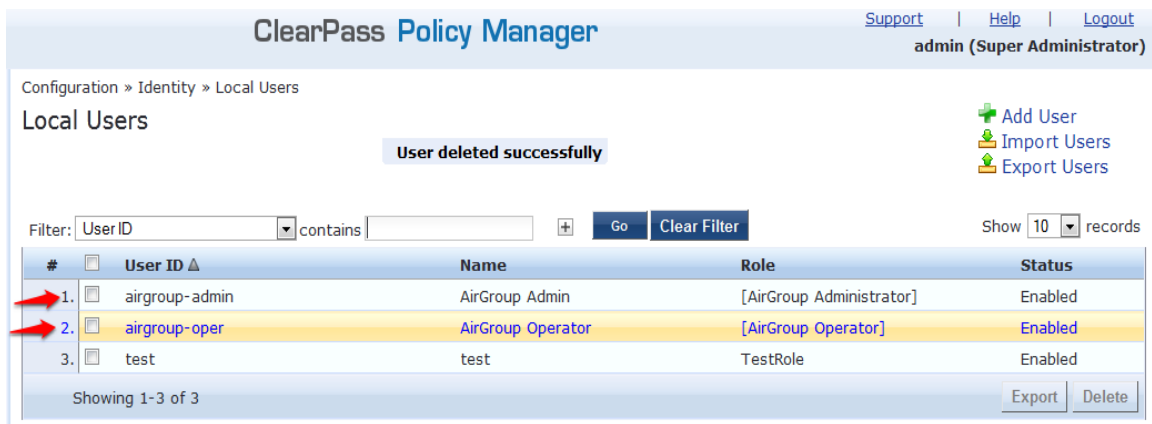
Attributes	
Attribute	Value
1.	Click to add...

Add **Cancel**

Click **Add** to save the 'AirGroup Operator' login.

The 'AirGroup Administrator' and 'AirGroup Operator' IDs will be displayed in the **Local Users** GUI screen.

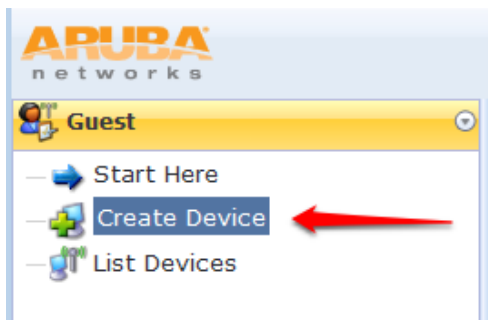
Figure 11 Local Users GUI screen



Navigate to the ClearPass Guest GUI and click the **Logout** button so that you are presented with the ClearPass Guest Login page. Enter the airgroup-admin login and password.

Click on **Create Device**.

Figure 12 Create a device



The following page is displayed:

Figure 13 Register Shared Device

Register Shared Device	
* Device Name:	<input type="text"/> Enter a name to identify the device.
* MAC Address:	<input type="text"/> Enter the MAC address of the device.
Shared Locations:	<input type="text"/> Enter a list of location IDs where this device will be shared. Use a comma-separated list of tag=value pairs; tag may be AP-Name, AP-Group, or FQLN. A fully qualified location name is '<ap-name>.floor<N>.<building-name>.<campus>'. Leave blank to share with all locations.
Shared With:	<input type="text"/> Enter up to 10 usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.
Shared Roles:	<input type="text"/> List the user roles that will be able to use this device. Use a comma-separated list, e.g. role1,role2,role3, or blank for all roles.
	

For testing purposes, add your test AppleTV device name and MAC address; but leave the other fields blank.

Click **Register Shared Device**.

Testing

Disconnect your AppleTV and OSX Mountain Lion/iOS 6 devices if they were previously connected to the wireless network. Remove their entries from the controller's user table as follows:

Find the MAC address

```
"show user table"
```

Delete them from the table

```
"aaa user delete mac 00:aa:22:bb:33:cc"
```

Reconnect both devices. You should be able to connect to the AppleTV from the other device. In order to limit access to the AppleTV, open up the ClearPass Guest GUI, logging in as the user that created the device (airgroup-admin or aigroup-oper were the example usernames in this document) and navigate to **List Devices**. Click on the test AppleTV. Click **Edit**. Now add a username to the Shared With field that is **not** the username being used to login with the OSX Mountain Lion/iOS 6 device.

Disconnect and remove the OSX Mountain Lion/iOS 6 device from the controller's user table. Reconnect the device, again **not** using the username that you added to the Shared With field. The AppleTV **should not** be available to this device.

Disconnect the OSX Mountain Lion/iOS 6 device and delete it from the controller's user table. Reconnect using the username that was added to the Shared With field. The OSX Mountain Lion/iOS 6 device should once again have access to the AppleTV.

Troubleshooting

Problem:

Limiting devices has no affect.

Solution:

Make sure that IPv6 is disabled.

Problem:

OSX Laptop running Mountain Lion can AirPlay to the AppleTV, but iOS devices cannot.

Solution:

Make sure that IPv6 is disabled.