ArubaOS 6.1.3.6-AirGroup

ARUBA networks

Deployment 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

Contents

Introducing Aruba AirGroup

Aruba AirGroup is a unique enterprise-class capability that leverages zero configuration networking to allow mobile device technologies, such as the AirPrint™ wireless printer service and the AirPlay™ mirroring service, to communicate over a complex access network topology.

Zero Configuration Networking

Zero configuration networking enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as a wireless network of the user.

Bonjour®, the zero configuration implementation introduced by Apple®, is supported by many Apple product lines, including devices using the OS X operating system, iPhone®, iPod Touch®, iPad®, Apple TV®, and AirPort Express®. Bonjour is included with popular software programs such as Apple iTunes, Safari, and iPhoto. Bonjour can also be installed on computers running Microsoft Windows® and is supported by most new network-capable printers.

Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these devices. However, addresses used by this protocol are link-scope multicast addresses, so each query or advertisement is limited to a specific VLAN. In large universities and enterprise networks, it is common for Bonjour-capable devices to connect to the network using different VLANs. As a result, an iPad on one enterprise VLAN will not be able to discover the Apple TV that resides on another VLAN. Broadcast and multicast traffic is filtered out of a wireless LAN network in an effort to reduce network traffic. This inhibits Bonjour (mDNS) services, which rely on multicast traffic.

AirGroup Solution

Aruba addresses the mDNS challenge by introducing the patent-pending AirGroup solution. AirGroup leverages key elements of Aruba's solution portfolio including the ArubaOS operating system software for Aruba mobility controllers and Aruba ClearPass Policy Manager.

Aruba AirGroup maintains seamless connectivity between clients and services across VLANs. The mDNS traffic is minimized to preserve valuable wired network bandwidth.

NOTE

The AirGroup feature is disabled by default. For information on enabling this feature after upgrading to a version of ArubaOS that supports AirGroup, see "Enabling or Disabling AirGroup" on page 20.

With Aruba AirGroup:

- An AirGroup operator—an end user such as a student can register personal devices. The devices registered by the operator can then automatically be shared with each other.
- Each operator can define a group of users, such as friends and roommates, who are allowed to share the operator's registered devices.
- AirGroup administrators can register and manage an organization's shared devices such as printers or conference room Apple TVs. The administrator can grant global access to each device, or limit access according to user name, role, or user location.

This deployment guide provides configuration information for network administrators to enable AirGroup on an Aruba mobility controller and ClearPass Policy Manager and to register devices with ClearPass Guest. Additional information on AirGroup is available in the ArubaOS 6.1.3.6-AirGroup release notes.

AirGroup also enables context awareness for services across the network:

- AirGroup is aware of personal devices. An Apple TV in a dorm room, for example, can be associated with the student who owns it.
- AirGroup is aware of shared resources, such as an Apple TV in a meeting room, a printer available to multiple users, or AirPlay in a classroom where a laptop screen is projected on HDTV monitor.
- AirGroup is aware of the location of services—for example, an iPad is presented with the closest printer location instead of all the printers in the building. If a user in a conference room wants to use an Apple TV receiver to project a MacBook screen on an HDTV monitor, the location-aware mobility controller shows the Apple TV that is closest to that user.

AirGroup Services

AirGroup supports zero configuration services. The services are pre-configured and are available as a part of the factory default configuration. The adminsitrator can enable or disable individual services by using the controller WebUI.

Services enable by default:

- AirPlay— Apple AirPlay allows wireless streaming of music, video, and slideshows on your iOS device to Apple TVs and other devices that support the AirPlay feature.
- AirPrint— Apple AirPrint allows you to print from an iPad, iPhone or iPod touch directly to any AirPrint compatible printers.

Services disable by default:

- iTunes— iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt— This service is used for remote login, remote management, and FTP utilities on Apple devices.
- Sharing— Applications, such as disk sharing and file sharing, use the service ID that are part of this service, on one or more Apple devices.
- Chat— The iChat (Instant Messenger) application on Apple devices uses this service.

NOTE

AirGroup also supports custom and allowall services. For more information, see Defining an AirGroup Service on page 21 and Configuring the allowall Service on page 25.

The AirGroup Solution Components

The Aruba AirGroup Solution includes the Aruba mobility controller, ClearPass Policy Manager, and ClearPass Guest.

Table 1 describes the requirements for each component:

Table 1 *AirGroup Solution Component Supported Versions*

Component	Minimum Version
ArubaOS (Mobility Controller)	ArubaOS 6.1.3.6-AirGroup
ClearPass Policy Manager and ClearPass Guest	6.0.2

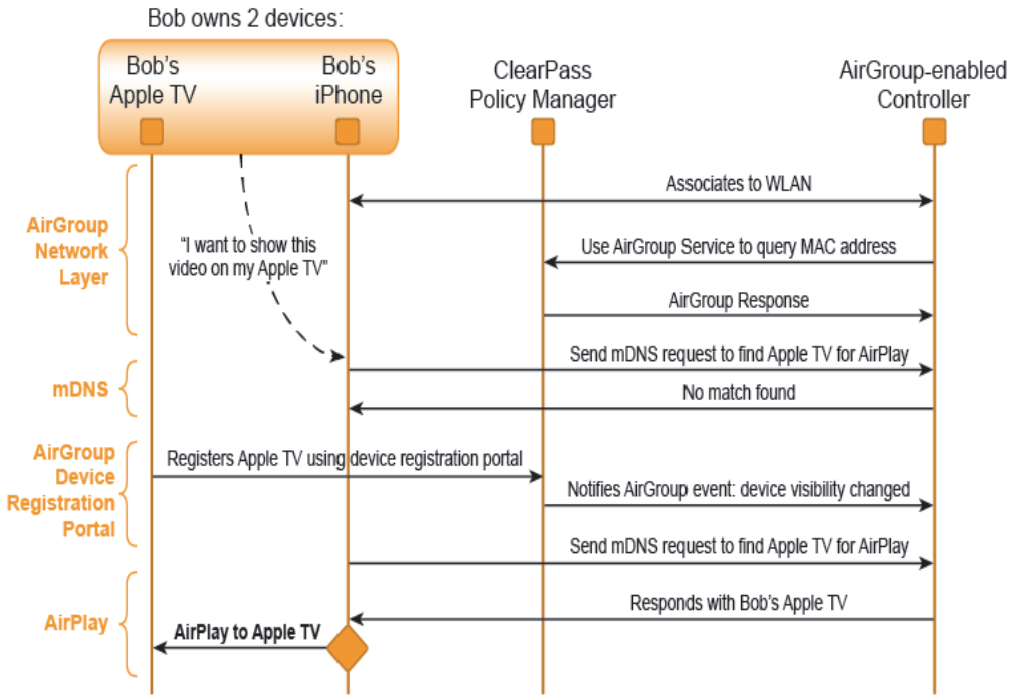
AirGroup and ClearPass Policy Manager

The AirGroup feature and ClearPass Policy Manager work together to allow users to share personal devices.

- An AirGroup administrator uses ClearPass Policy Manager to authorize end users to register their personal devices.
- An AirGroup operator—the end user registers devices (such as an Apple TV).
- Aruba mobility controllers query ClearPass Policy Manager to associate the access privileges of each mobile device to its allowed services.

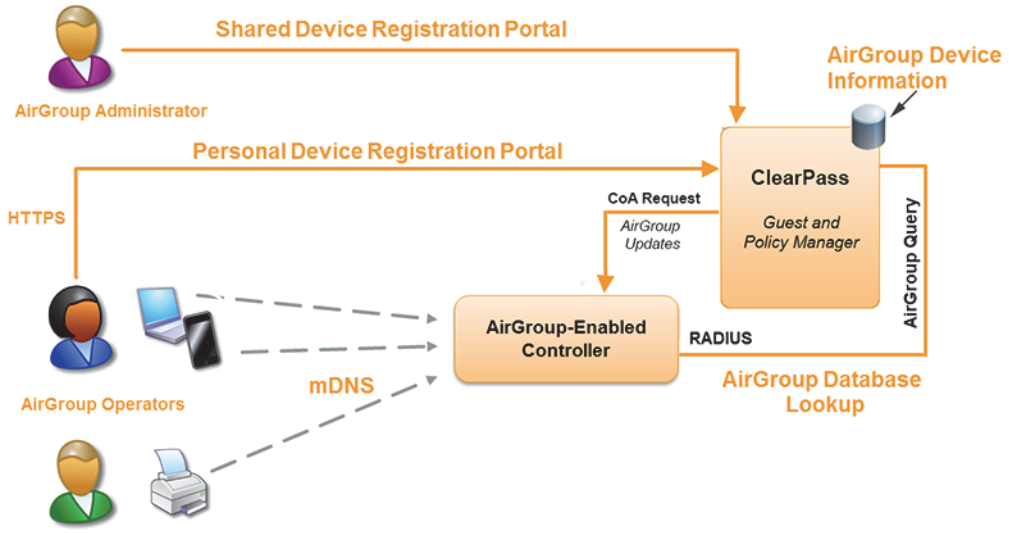
Figure 1 shows the AirGroup workflow that allows a user to register personal devices and then, use AirPlay to send an image from an iPhone to an Apple TV.

Figure 1 *AirGroup Enables Personal Device Sharing*



Aruba AirGroup enables context awareness for services across the network and supports a typical customer environment with shared, local, and personal services available to mobile devices. For example, in Figure 2, an AirGroup administrator registers the shared devices in ClearPass, and AirGroup operators register their personal devices in the ClearPass Guest portal. The AirGroup-enabled controller sends AirGroup queries to ClearPass for the registered devices' information. ClearPass sends the Change of Authorization (CoA) to inform the AirGroup controller about the registered devices.

Figure 2 *AirGroup in a Typical Wireless Deployment*



AirGroup deployments that include both ClearPass Policy Manager and an AirGroup controller support more features than deployments with only an AirGroup controller.

Typical Deployment Models

AirGroup can be deployed with ClearPass Policy Manager (recommended for large WLANs), or optionally without ClearPass in smaller networks. For networks without ClearPass Policy Manager, some of the features that require Policy Manager interaction are not available. The two AirGroup deployment models are described in the following sections:

- Integrated Deployment Model on page 10
- Overlay Deployment Model on page 11

Integrated Deployment Model

In the integrated deployment model, AirGroup features are integrated with the WLAN controller that terminates all APs and provides WLAN services. This deployment model also supports optional integration with ClearPass Policy Manager. If AirGroup is deployed in an integrated environment, upgrade the controller to the version ArubaOS 6.1.3.6-AirGroup or later. For more information, see Chapter 2, “Integrated Deployment Model” on page 19.

6.1.3.6-AirGroup supports a multi-controller AirGroup cluster. The AirGroup cluster can consist of multiple controllers in various configuration combinations such as master-master, master-local, and local-local. Figure 3 shows an example of a master-local setup with shared, local, and personal services that are available to mobile devices. With AirGroup, the context-based policies determine the services visible to the end-user devices.

Figure 3 *Integrated AirGroup Network Topology*

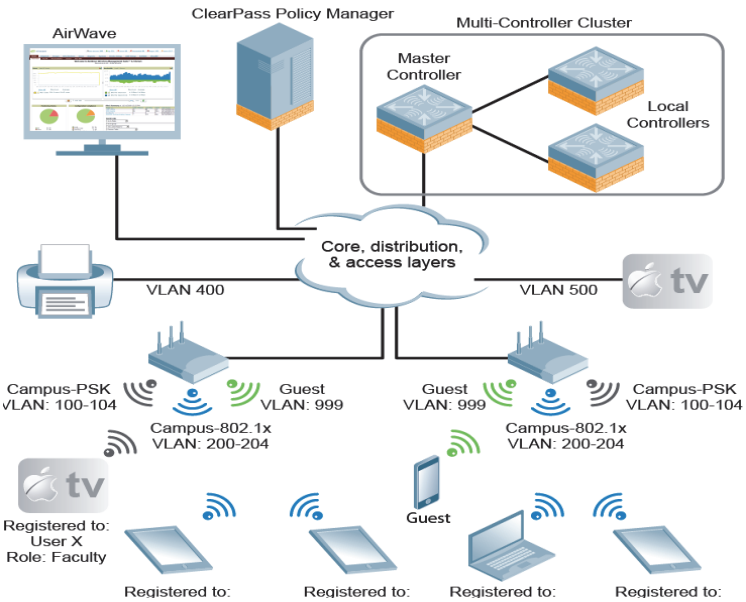


Table 2 *Sample policies for Aruba AirGroup*

mDNS Services	Faculty	Student	Visitor
	User X's iPad	**User B's MacBook**	**Windows Laptop**
Apple TV in the lab, registered to user role "Faculty"	Yes	No	No
Apple TV in the dorm room, registered to User B	No	Yes	No
Apple TV in a lecture hall accessible to Faculty	Yes	No	No
Printer located in a lab accessible to faculty and students	Yes	Yes	No

Overlay Deployment Model

In the overlay model:

- One access controller terminates APs and provides WLAN services
- A second dedicated AirGroup controller acts as an overlay that provides AirGroup functionality

This model allows you to deploy AirGroup without upgrading the existing production controller managing your network. The production WLAN controller does not require a code upgrade. However, the overlay AirGroup controller requires ArubaOS 6.1.3.6-AirGroup.

CAUTION

The overlay deployment model does **not** support Broadcast/Multicast optimization or location-based device discovery or role-based access controls through ClearPass Policy Manager. Use the integrated deployment model instead to access these features.

The production WLAN controller must be configured with ACL redirect rules to send mDNS traffic from user VLANs to the overlay controller, which are connected through an L2 GRE tunnel. If you use this model,

ensure that no user VLANs (wired or wireless) terminate on the AirGroup overlay controller. To terminate user VLANs on the overlay controller, ensure that no VLANs create a loop.

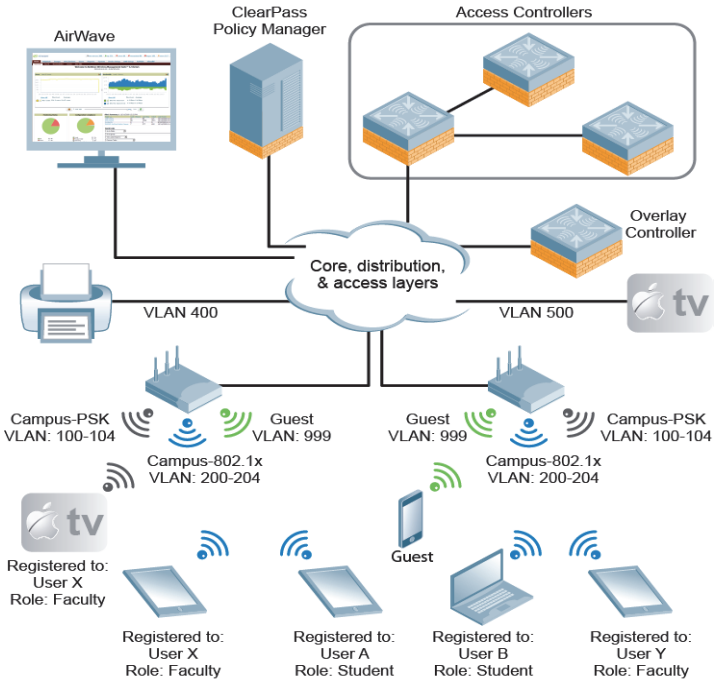
This model does not support the Broadcast/Multicast (BC/MC) optimization feature, which drops downstream multicast packets from the AirGroup controller to the WLAN controller. However, disabling this setting can increase client traffic. To limit the impact of this change, enable the **Drop Broadcast and Multicast** and **Convert Broadcast ARP Requests to Unicast** settings in the Virtual AP profiles. This restricts broadcasts to the wired network, but still allows the overlay deployment model to support wired Bonjour devices. This setting prevents the overlay controller from pro-actively discovering any newly created or enabled AirGroup services. However, the overlay controller discovers the AirGroup services when the device advertises AirGroup services.

The overlay controller is not able to gather information about the location of a device and user name or user role, so this deployment model does not support ClearPass Policy Manager location-based device discovery or role-based access controls. If your network requires these types of policy controls, use the integrated deployment model instead. See Chapter 3, "Overlay Deployment Model" on page 33 for more information on configuring this deployment model.

NOTE

In an overlay model, register the users and servers with ClearPass Policy Manager to discover personal and shared servers of the users.

Figure 4 *Overlay AirGroup Network Topology*



What's New in ArubaOS 6.1.3.6-AirGroup

The following new features are introduced in the ArubaOS 6.1.3.6-AirGroup:

Multi-Controller AirGroup Cluster

ArubaOS 6.1.3.6-AirGroup supports multiple mobility controllers running AirGroup to form a cluster. This feature enables an iPad users on one controller to discover Apple TV available on another controller, when both controllers are part of the same cluster.

Multi-Controller AirGroup Cluster—Terminologies

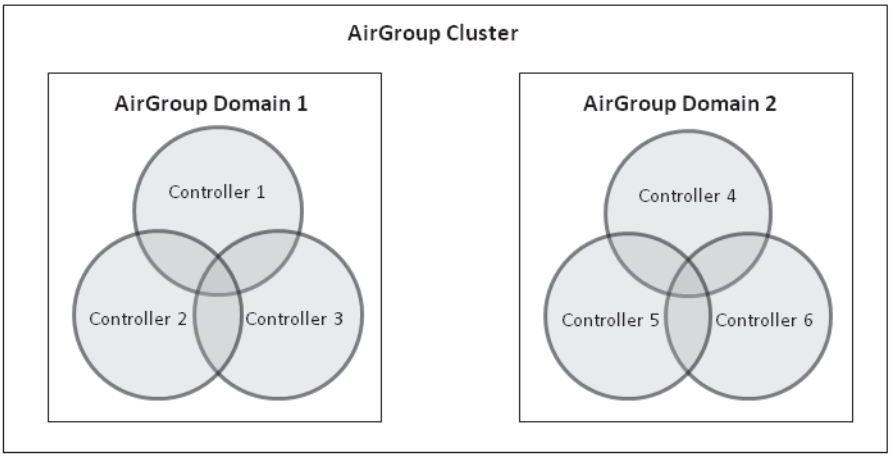
AirGroup Domain

An AirGroup domain is a set of controllers that are part of an AirGroup cluster. An administrator can configure multiple AirGroup domains for a site-wide deployment. Individual local controllers can independently choose relevant multiple AirGroup domains to form a multi-controller AirGroup cluster.

AirGroup Cluster

One or more AirGroup domain makes an AirGroup cluster. An AirGroup domain can include a list of likely controllers which may participate in the multi-controller AirGroup cluster. Figure 5 shows the AirGroup cluster and domain relationship:

Figure 5 *AirGroup cluster and domain relationship*



Active-Domain

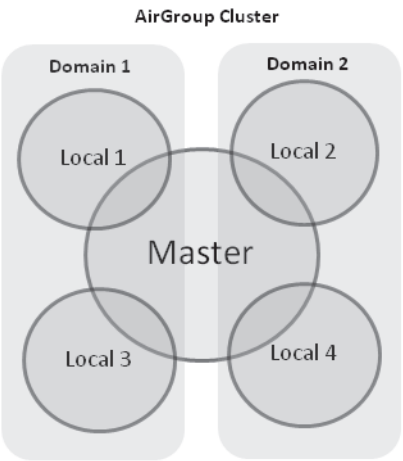
AirGroup allows one or more AirGroup domains to be a part of the AirGroup active-domain list of a controller. A master or local controller may participate in one or more AirGroup clusters based on its active-domain list. The mobility controller must set the corresponding domain as active for the controller to be part of the AirGroup cluster.

In Figure 5, under **AirGroup Domain 1**, all three controllers belong to **AirGroup Domain 1**. Based on this, the active-domain is 1 for these controllers.

Sample AirGroup Cluster Topology

Figure 6 shows a typical master-local multi-controller deployment. In this topology, five local controllers terminate on a single master controller.

Figure 6 *Typical Master-Local Multi-Controller Deployment*



Based on the requirement, the administrator can have the following setup:

Domain Definition

The administrator can define two domains with the following controllers in each domain:

- **Domain 1**: Local 1 (L1), Master (M), Local 3 (L3)
- **Domain 2**: Local 2 (L2), M, Local 4 (L4)

To configure an AirGroup domain, see Configuring an AirGroup Domain on page 27.

Active-Domain Definition

Based on the domain definition, each controller belongs to the following active-domain list:

- **Active-Domain 1**: L1, M, L3
- **Active-Domain 2**: L2, M, L4

To configure an active domain, see Configuring an AirGroup active-domain on page 29.

AirGroup Controller Communication

Based on the domain and active-domain definitions, the AirGroup controller communication takes place in the following manner:

- L1, M, and L3 can communicate with each other as they are part of active-domain 1.
- L2, M, and L4 can communicate with each other as they are part of active-domain 2.
- M can communicate with L1, L2, L3, and L4 as M is part of active-domain 1 and 2.
- L1 and L3 cannot communicate with L3 and L4 because they do not have a common active-domain and they do not share the same VLAN.

AirGroup Server Discovery

- Any iPad user in L1, M, and L3 can discover any Apple TV or AirPrint Printer in L1, M, and L3.
- Any iPad user in L2, M, and L4 can discover any Apple TV or AirPrint Printer in L2, M, and L4.
- Any iPad user in M can discover any Apple TV or AirPrint Printer in L1, L2, L3, and L4 and vice-versa.
- iPad users in L1 and L3 cannot discover any Apple TV or AirPrint Printer in L2 and L4 and vice-versa.

Scalability

In a multi-controller deployment, there is a scaling limit of 2000 AirGroup servers and 6000 AirGroup users for all controllers in a cluster. If you require more servers and users than the prescribed limit, configure

multiple clusters so that each cluster is within the prescribed limit. For detailed scalability information, see AirGroup Scalability Limits on page 67.

An AirGroup domain is a set of controllers that are part of an AirGroup cluster. An AirGroup cluster can have one or several AirGroup domains. An AirGroup domain can include a list of likely controllers which may participate in the multi-controller AirGroup cluster. Depending on the deployment setup, the IP address in the AirGroup domain could either be the controller IP or VRRP IP address. The configuration elements are defined by an administrator on a master controller, for all its associated local controllers, sharing the same configuration with the master controller. The actual AirGroup multi-controller cluster may include one or several local controllers, and this cluster is defined by including one or several relevant AirGroup domains, on the respective local controller, in the active-domain list. As a result, a master or local controller may participate in one or more AirGroup clusters based on its active-domain list.

Incorrect or incomplete configuration of the controllers participating in an AirGroup cluster can lead to disjointed clusters. In a disjoined cluster, an AirGroup user will not have a seamless view of the AirGroup servers spanning multiple controllers. Ensure that all the participating controllers in an AirGroup cluster are configured appropriately.

The AirGroup domain configurations are restricted to the master controller. This ensures all local controllers in a master-local setup have unique AirGroup domain names. If duplicate AirGroup domain names on multiple master controllers are encountered, then ensure that the duplicate AirGroup domain names have the same values to participate in a single AirGroup cluster.

ArubaOS 6.1.3.6-AirGroup supports multiple AirGroup instances per VLAN. In a multi-controller deployment, AirGroup is enabled on more than one controller, and they share one or more VLANs.

NOTE

Any controller that shares VLANs with another controller must be part of the same AirGroup multi-controller cluster.

When an AirGroup controller has the list of all the controllers in the multi-controller table, it will set up a Layer-2 GRE tunnel with all the controllers in the table. The Layer-2 GRE tunnel carries AirGroup specific packets only.

For configuration details, see Configuring an AirGroup Domain on page 27.

Master-Local Controller Synchronization

Staring from ArubaOS 6.1.3.6-AirGroup, administrators can configure AirGroup from the master controller to ease deployment. The master controller then synchronizes the AirGroup configuration elements with all the local controllers it manages. For more information, see Master-Local Controller Synchronization on page 19.

Pre-configured AirGroup Services

The following services are pre-configured and made available as part of the factory default configuration:

- AirPlay
- AirPrint
- iTunes
- RemoteMgmt
- Sharing
- Chat

For more information, see Defining an AirGroup Service on page 21.

New Commands Introduced in ArubaOS 6.1.3.6-AirGroup

The following new commands are introduced in ArubaOS 6.1.3.6-AirGroup command-line interface:

Table 3 *New CLI Commands*

Command	Description

`[no] airgroup domain <string>`
`[no] ip-address <A.B.C.D>`
`[no] description <string>`
	This command configures a cluster of mobility controllers to be a part of a domain.

`[no] airgroup active-domain <string>`	This command configures an AirGroup active-domain for an AirGroup cluster.
`[no] airgroup cppm-server query-interval <1..24>`	This command configures the CPPM query interval in the controller.
`airgroup global-credits <query-packets> <response-packets>`	In an AirGroup network, AirGroup devices generate excess mDNS query and response packets. Using this command, the AirGroup controller restricts these packets by assigning tokens. The controller processes these mDNS packets based on this token value. The controller rejects any packets beyond this token limit. The token renews every 15 seconds. The renewal time is not a configurable parameter.
`clear airgroup statistics blocked-queries`	This command clears the statistics of service IDs which were queried but not available in the AirGroup service table.
`clear airgroup statistics blocked-service-id`	This command clears the statistics for the list of blocked services.
`clear airgroup statistics cppm_entries`	This command clears the statistics that are displayed for **show airgroup cppm entries**.
`clear airgroup statistics internal-state`	This command clears internal state statistics of mDNS module.
`clear airgroup statistics multi-controller`	This command clears the statistics maintained for multi-controller message exchanges.
`clear airgroup statistics query`	This command clears statistics maintained in the user and server table.
`clear airgroup statistics service`	This command clears statistics maintained in the AirGroup service table.
`clear airgroup users`	This command removes the current AirGroup user entries from the user table.
`show airgroup active-domains`	This command displays a list of AirGroup active-domains configured.
`show airgroup multi-controller-table`	This command displays the IP address of all the controllers configured as part of a cluster.
`show airgroup domain`	This command displays a list of AirGroup domains configured.
`show airgroup cppm-server query-interval`	This command displays the CPPM query interval value configured.
`show airgroup blocked-queries`	This command displays the service IDs which were queried but not available in the AirGroup service table.

Table 3 *New CLI Commands*

Command	Description
`show airgroup global-credits`	This command displays tokens assigned to query and response packets. It displays configured and current global tokens.

ClearPass Policy Manager and ClearPass Guest Features

The ClearPass Policy Manager portal for WLAN administrators allows to register shared devices such as conference room Apple TVs and printers. The ClearPass Guest portal for WLAN users allows end users to register their personal devices. For more information on configuration, see Chapter 5, "Configuring ClearPass and ClearPass Guest" on page 45.

In the integrated deployment model, AirGroup features are integrated with the WLAN controller that terminates all APs and provides WLAN services. This deployment model also supports optional integration with ClearPass Policy Manager. When you implement AirGroup in an integrated deployment, upgrade the controller to a version of ArubaOS 6.1.3.6-AirGroup or later, and trunk all VLANs with wired devices (such as printers) to the AirGroup controller.

NOTE

If your deployment requires ClearPass Policy Manager integration, complete the steps described in Chapter 5, "Configuring ClearPass and ClearPass Guest" , before performing the steps described in this chapter.

Master-Local Controller Synchronization

You can configure AirGroup from the master controller to ease the deployment. The master controller then synchronizes the AirGroup configuration elements with all the local controllers it manages. AirGroup configurations can belong to one of two categories:

Master — These configuration commands are specific to master controller and will initially not be available on the local controllers. The master controller pushes the AirGroup configuration commands to all the applicable local controllers.

- AirGroup custom service definition. For more information, see Defining an AirGroup Service on page 21.
- AirGroup disallow user-role (service filtering) definition. For more information, see Configuring the disallow-role for an AirGroup Service on page 22.
- AirGroup disallow VLAN (service filtering) definition. For more information, see Restricting AirGroup Servers on a VLAN based on an AirGroup Service on page 23.
- AirGroup CPPM enforce registration. For more information, see Configuring CPPM to Enforce Registration on page 43.
- AirGroup definition. For more information, see Configuring The AirGroup-CPPM Interface on page 37.
- AirGroup multi-controller domain definition. For more information, see Configuring an AirGroup Domain on page 27.
- AirGroup CPPM query interval definition. For more information, see Configuring CPPM Query Interval on page 37.

Local — There are a few configuration limitations on the local controller. The local controller can only include the existing AirGroup domains in the AirGroup active-domain list, applicable for this controller. The local controller cannot define or edit an AirGroup domain.

These configuration commands are applicable to both master and local controllers. The master controller does not push the following AirGroup configuration commands to all the applicable local controllers.

- AirGroup enable/disable parameter. For more information, see Enabling or Disabling AirGroup on page 20.
- AirGroup service enable/disable parameter. For more information, see Enabling or Disabling an AirGroup Service on page 25.
- AirGroup allowall service definition. For more information, see Configuring the allowall Service on page 25.

- AirGroup disallow VLAN (global) definition. For more information, see Restricting AirGroup Servers for a VLAN on page 22.
- AirGroup multi-controller active-domain definition. For more information, see Configuring an AirGroup active-domain on page 29.

Configuring an AirGroup Integrated Deployment Model

Use the following procedures to enable the AirGroup feature and configure AirGroup services.

Enabling or Disabling AirGroup

The first step is to enable AirGroup in your mobility controller.

Using the WebUI

To enable or disable the AirGroup service using the controller WebUI:

1. Navigate to **Configuration > Advanced Services > AirGroup** page.
2. Select the **AirGroup Settings** tab.
3. Under **Global Settings > AirGroup Status**, select **enable** from the drop-down menu.
4. Click **Apply**.

Using the CLI

Access the controller's command-line interface, and use the following command:

```
(host) (config) # airgroup [enable|disable]
```

Command Mode

Configuration mode on master and local controller.

Viewing AirGroup Status on Controller

Using the WebUI

To view the current status of the AirGroup in the controller using the controller WebUI:

1. Navigate to **Configuration > Advanced Services > AirGroup** page.
2. Select the **AirGroup Settings** tab to view the AirGroup status in the controller.

Using the CLI

Use the following command to verify the current status of the AirGroup configuration and AirGroup services configured in your WLAN controller.

```
(host) #show airgroup status

AirGroup Feature
----------------
Status
------
Enabled

AirGroup Enforce Registration
-----------------------------
Status
------
Enabled
```

```
AirGroup Service Information
----------------------------
Service         Status
-------         ------
airplay         Enabled
airprint        Enabled
itunes          Disabled
remotemgmt      Enabled
sharing         Enabled
chat            Enabled
allowall        Enabled
```

Command Mode

Enable mode on master and local controllers.

Defining an AirGroup Service

The AirGroup solution defines the concept of configurable AirGroup services. One or more mDNS services can be configured on the mobility controller. When you define an mDNS service as an AirGroup service, you can implement policies to restrict its availability to a specific user role or VLAN.

In ArubaOS 6.1.3.6-AirGroup, the following services are preconfigured and made available as part of the factory default configuration:

- AirPlay
- AirPrint
- iTunes
- RemoteMgmt
- Sharing
- Chat

Using the WebUI

To define an AirGroup service using the controller WebUI:

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. On the **AirGroup service details** tab, click **Add New**.
3. Enter the name of the AirGroup profile in the **Name** field.
4. Enter the description for the AirGroup profile in the **Description** field.
5. Enter the roles that need to be restricted in the **Disallow Roles** field.
6. Enter the VLANs that need to be restricted in the **Disallow VLANs** field.
7. Enter the Service ID of the AirGroup service in the **Services IDs** field.
8. Click **OK** and then click **Apply**.

The following table describes the configuration parameters of an AirGroup service:

Table 4 *AirGroup Service Parameters*

Parameter	Description
Name	Name of the AirGroup Service.
Description	Enter the description for the AirGroup Service.

Table 4 *AirGroup Service Parameters*

Parameter	Description
Disallow Roles	User Roles restricted from accessing the service.
Disallow VLANs	User VLANs restricted from accessing the service.
Service IDs	An AirGroup service ID is the name of a Bonjour service offered by a Bonjour-enabled device or application. Bonjour defines service ID strings using the following format: <underscore>servicename<period><underscore>protocol.local Example: `_airplay._tcp.local` The service ID string is case sensitive and should be entered without any modification, with the exception of the **.local** portion of the service ID, which is not required.

Using the CLI

Use the **airgroupservice** command to define an AirGroup service using the command-line interface.

```
airgroupservice <name>
```

Sample Configuration

The following example configures the *iPhoto* service with access to the *_dpap._tcp* service ID to share photos across MacBooks:

```
(host) (config) #airgroupservice iPhoto
(host) (config-airgroupservice) #description "Share Photos"
(host) (config-airgroupservice) #id _dpap._tcp
```

Command Mode

Configuration mode on master controllers.

Configuring the disallow-role for an AirGroup Service

By default, an AirGroup service is accessible to all user devices associated to your controller. The **disallow-role** option prevents devices with specified user roles from accessing AirGroup services.

```
airgroupservice <string>
   disallow-role <string>
```

Sample Configuration

```
(host) (config) #airgroupservice iPhoto
(host) (config-airgroupservice) #disallow-role guest
```

Command Mode

Configuration mode on master controllers.

Restricting AirGroup Servers for a VLAN

By default, an AirGroup service is accessible to user devices in all VLANs configured on your controller. Use the following command to enable or disable AirGroup access to devices in a specific VLAN:

```
airgroup vlan <VLAN ID> allow|disallow
```

Sample Configuration

```
(host) (config) #airgroup vlan 5 disallow
```

Command Mode

Configuration mode on master and local controllers.

Restricting AirGroup Servers on a VLAN based on an AirGroup Service

To prevent user devices on a specific VLAN from accessing a specific AirGroup service, use the **disallow-vlan** option.

```
airgroupservice <string>
   disallow-vlan <string>
```

Sample Configuration

```
(host) (config) #airgroupservice airplay
(host) (config-airgroupservice) #disallow-vlan 5
```

Command Mode

Configuration mode on master controllers.

Viewing AirGroup Disallowed VLAN Policy Details

Use the following command to view the status of a disallowed VLAN policy.

```
show airgroupservice
```

Sample Configuration

```
(host) # show airgroupservice
AirGroupService Details
-----------------------
Service     Description        Disallowed-Role  Disallowed-VLAN  ID
-------     -----------        ---------------  ---------------  --
airplay     AirPlay                                              _airplay._tcp
                                                                 _raop._tcp
                                                                 _appletv-v2._tcp
airprint    AirPrint                                             _ipp._tcp
                                                                 _printer._tcp
                                                                 _canon-bjnp1._tcp
                                                                 _ica-networking2._tcp
itunes      iTunes                                               _home-sharing._tcp
                                                                 _apple-mobdev._tcp
remotemgmt  Remote management                                    _ssh._tcp
                                                                 _sftp-ssh._tcp
                                                                 _ftp._tcp
                                                                 _telnet._tcp
sharing     Sharing                                              _odisk._tcp

#query-hits  #servers
-----------  --------
11018        108
0            0

AirGroupService Details
-----------------------
Service   Description         Disallowed-Role  Disallowed-VLAN  ID
-------   -----------         ---------------  ---------------  --
                                                                _afpovertcp._tcp
                                                                _xgrid._tcp
chat      Chat                                                  _presence._tcp
allowall  Remaining-Services                                    _net-assistant._udp
                                                                _rbnsrv._tcp
#query-hits  #servers
-----------  --------
32411        99
1007         59
```

```
Num Services:7
Num Service-ID:19
```

The output of this command includes the following information:

Table 5 *show airgroupservice*

Column	Description
Service	Name of the AirGroup service.
Description	The description for the AirGroup service.
Disallowed-Role	User Roles restricted from accessing the service.
Disallowed-VLAN	User VLANs restricted from accessing the service.
ID	An AirGroup service ID is the name of a Bonjour service offered by a Bonjour-enabled device or application.
#query-hits	Displays the number of mDNS query hits for a particular service.
#servers	Displays the number of AirGroup servers advertising this service.

Command Mode

Configuration mode on master controller.

Viewing AirGroup Disallowed VLAN

Use the following command to view the status of disallowed VLANs:

```
show airgroup vlan
```

Sample Configuration

```
(host) #show airgroup vlan

VLAN Table
----------
VLAN-Id   IP-Address     Status
-------   ----------     ------
1         10.17.72.1     Allowed
5         2.2.2.2        Disallowed
7         3.3.3.3        Allowed
default   169.254.53.53  N/A
```

The output of this command includes the following information:

Table 6 *show airgroup vlan*

Column	Description
VLAN-Id	Identification number of the AirGroup VLAN.
IP-Address	IP address of the VLAN interface.
Status	Status of AirGroup access to devices for the VLAN.

Command Mode

Configuration mode on master and local controllers.

Configuring the allowall Service

The **allowall** service is a pre-configured AirGroup service that enables support for DNS records that are not part of any other defined AirGroup service.

Using the WebUI

Use the following steps to configure the allowall service using the controller WebUI:

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. In the **AirGroup service details** tab, select the check box next to **allowall** service and click **Enable**.
3. Click **Apply**.

Using the CLI

Use the following command to enable or disable the allowall service:

```
airgroup service allowall enable|disable
```

Sample Configuration

```
(host) (config) #airgroup service allowall enable
```

Command Mode

Configuration mode on master and local controllers.

Enabling or Disabling an AirGroup Service

Using the WebUI

To enable/disable an AirGroup service using the controller WebUI:

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. On the **AirGroup service details** tab, select the AirGroup service and click **Enable** or **Disable**.
3. Click **Apply**.

Using the CLI

Use the following command to enable or disable an AirGroup service:

```
airgroup service <string> enable|disable
```

Sample Configuration

```
(host) (config)#airgroup service airplay disable
```

Command Mode

Configuration mode on master and local controllers.

Viewing AirGroup Service Status

Using the WebUI

Use the following steps to view the status of AirGroup services using the controller WebUI:

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. Under the **AirGroup service details** tab, view the status of all the AirGroup services.

Using the CLI

Use the following command to verify the status of an AirGroup Service:

```
show airgroup status
```

Sample Configuration

```
(host) #show airgroup status

AirGroup Feature
----------------
Status
------
Enabled

AirGroup Enforce Registration
-----------------------------
Status
------
Enabled

AirGroup Service Information
----------------------------
Service         Status
-------         ------
airplay         Enabled
airprint        Enabled
itunes          Disabled
remotemgmt      Enabled
sharing         Enabled
chat            Enabled
allowall        Enabled
```

The output of this command includes the following information:

Table 7 *show airgroup status*

Column	Description
`AirGroup Feature Status`	Displays the status of AirGroup in the controller.
`AirGroup Enforce Registration Status`	Displays the status of AirGroup server registration with the CPPM server.
`AirGroup Service Information`	Displays the status of all the AirGroup services.

Command Mode

Enable mode on master and local controller.

Viewing Blocked Services

The **airgroup service <servicename> disable** command blocks an AirGroup service by blocking the service IDs for that service. When an AirGroup service is enabled, service IDs of that service are enabled automatically. To view the list of blocked services, use the **show airgroup blocked-service-id** command.

Using the CLI

```
show airgroup blocked-service-id
```

Sample Configuration

```
(host) #show airgroup blocked-service-id
```

```
AirGroup Blocked Service IDs
----------------------------
Origin      Service ID            #response-hits
------      ----------            --------------
2.2.2.254   _colorPrinter._udp    5

Num Blocked Service-ID:1
```

The output of this command includes the following information:

Table 8 *show airgroup blocked-service-id*

Column	Description
`Origin`	Source IP address of the AirGroup server which advertises this service.
`Service ID`	An AirGroup service ID is the name of a Bonjour service offered by a Bonjour-enabled device or application.
`#response-hits`	Number of mDNS response messages received for this service ID.

Command Mode

Enable mode on master and local controller.

Viewing AirGroup Service Details

Using the WebUI

To view the AirGroup service details using the controller WebUI:

1. Navigate to the **Configuration > Advanced Services > AirGroup service details** tab.
2. Click on any of the service name to view the service details.

Using the CLI

Use the following command to view the service details of all AirGroup services:

```
show airgroupservice
```

Sample Configuration

For sample configuration, see Viewing AirGroup Disallowed VLAN Policy Details on page 23.

To view the description of the column headings, see Table 5 on page 24.

Command Mode

Enable mode on master controllers.

Configuring an AirGroup Domain

An administrator can configure multiple AirGroup domains for a site-wide deployment. Individual local controller can independently choose relevant multiple AirGroup domains to form a multi-controller AirGroup cluster.

The following procedure configures a cluster of mobility controllers to be a part of a domain:

Using the WebUI

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. Select the **AirGroup Settings** tab.

3. Under the **AirGroup Domains** section, click **Add New**.
4. In the **Name** field, enter the domain name.
5. In **Description** field, enter a short description of the domain name.
6. Select the **Active-Domain Status** check box to enlist the domain in the active-domain list of a controller.
7. Under the **Ip Address** section, enter the controller or VRRP IP to be a part of this domain and click **Add**.
8. Click **Ok** and **Apply**.

Using the CLI

```
[no] airgroup domain <string>
   [no] ip-address <A.B.C.D>
   [no] description <string>
```

Sample Configuration

```
(host) (config) #airgroup domain Campus1
(host) (config-airgroup-domain) #ip-address 10.10.10.1
(host) (config-airgroup-domain) #ip-address 11.11.11.1
(host) (config-airgroup-domain) #description AirGroup_campus1
```

Command Mode

Configuration mode on master controllers.

Viewing an AirGroup Domain

The following procedure displays a list of AirGroup domains configured:

Using the WebUI

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. Select the **AirGroup Settings** tab.
3. Under the **AirGroup Domains** section, view a list of all AirGroup domains configured in the controller.

Using the CLI

```
show airgroup domain
```

Sample Configuration

```
(host) #show airgroup domain
AirGroup Domains
----------------
Name       Description        IP-Address
----       -----------        ----------
Campus1    AirGroup_campus1   10.10.10.1
                              11.11.11.1
Campus2    AirGroup_campus2   9.9.9.1
                              8.8.8.1
```

The output of this command includes the following information:

Table 9 *show airgroup domain*

Column	Description
Name	Name of the domain.

Table 9 *show airgroup domain*

Column	Description
`Description`	Short description of the domain.
`IP-Address`	Controller or VRRP IP address.

Command Mode

Enable mode on master controllers.

Configuring an AirGroup active-domain

AirGroup allows one or more AirGroup domains to be a part of the AirGroup active-domain list of a controller. A master or local controller may participate in one or more AirGroup cluster based on its active-domain list. The mobility controller must set the corresponding domain as active for the controller to be part of the AirGroup cluster.

The following procedure configures an AirGroup active-domain for AirGroup cluster:

Using the WebUI

See the WebUI procedure under Configuring an AirGroup Domain on page 27.

Using the CLI

```
[no] airgroup active-domain <string>
```

Sample Configuration

```
(host) (config) #airgroup active-domain campus1
(host) (config) #airgroup active-domain campus2
```

Command Mode

Configuration mode on master and local controllers.

Viewing AirGroup active-domains

The following procedure displays a list of AirGroup active-domains configured:

Using the WebUI

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. Select the **AirGroup Settings** tab.
3. Under the **AirGroup Domains** section, the **Active-Domain** and **Status** column displays a list of AirGroup active-domains configured.

Using the CLI

```
show airgroup active-domains
```

Sample Configuration

```
(host) #show airgroup active-domains
AirGroup Active-Domains
-----------------------
Domain Name  Status
-----------  ------
Campus1      Included
```

```
Campus2      Included
Num active-domains:2
```

The output of this command includes the following information:

Table 10 *show airgroup active-domains*

Column	Description
`Domain Name`	Name of the domain.
`Status`	Status of the domain if it is part of the active-domain list.

Command Mode

Enable mode on master and local controllers.

Viewing AirGroup Multi-Controller Table

All controllers communicate with each other based on the multi-controller table in an AirGroup cluster. This table is a combination of controllers specified in each domain, as part of active-domains.

The following procedure displays the IP address of all the controllers participating in an AirGroup multi-controller environment:

Using the CLI

```
show airgroup multi-controller-table
```

Sample Configuration

```
(host) #show airgroup multi-controller-table
AirGroup Multi-Controller-Table
-------------------------------
IP-Address Request with Tag Tx  Unicast Response with tag Tx  Raw Response Tx
---------- -------------------  ----------------------------  ---------------
10.1.0.255 123                  0                             0
10.1.1.0   123                  0                             0

Request with Tag Rx  Unicast Response with tag Rx  Raw Response Rx
-------------------  ----------------------------  ---------------
0                    0                             0
59                   0                             21
Num IP-Address:2
```

The output of this command includes the following information:

Table 11 *show airgroup multi-controller-table*

Column	Description
`IP-Address`	Displays the IP address of all the controllers participating in an AirGroup multi-controller environment.
`Request with Tag Tx`	Number of AirGroup multi-controller queries transmitted with meta-tag information by the controller to other controllers in its multi-controller domain.
`Unicast Response with tag Tx`	Number of AirGroup multi-controller responses transmitted with meta-tag information by the controller to other controllers in its multi-controller domain.

Table 11 *show airgroup multi-controller-table*

Column	Description
`Raw Response Tx`	Number of mDNS responses transmitted by the controller in response to multi-controller queries from other controllers in the domain.
`Request with Tag Rx`	Number of AirGroup multi-controller queries received with meta-tag information by the controller from other controllers in its multi-controller domain.
`Unicast Response with tag Rx`	Number of AirGroup multi-controller responses received with meta-tag information by the controller from other controllers in its multi-controller domain.
`Raw Response Rx`	Number of mDNS responses received by the controller in response to multi-controller queries sent by the controller.

Command Mode

Enable mode on master and local controllers.

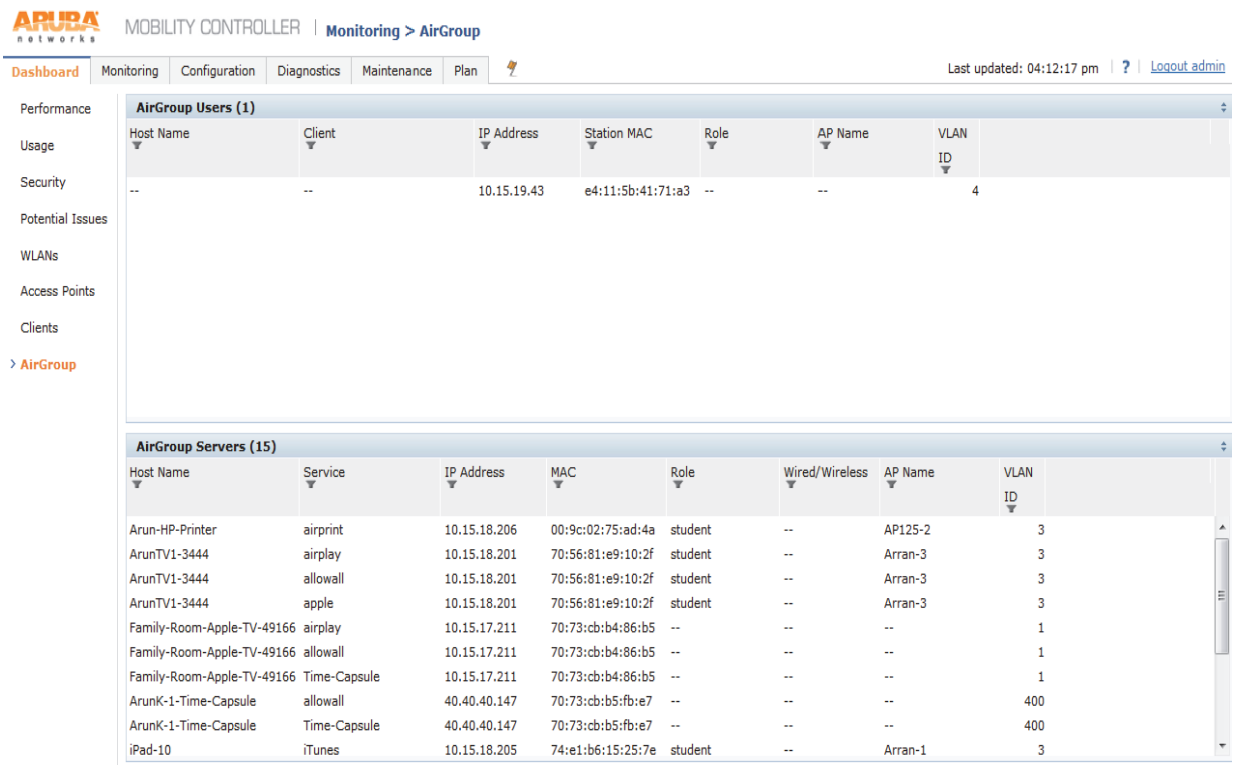
NOTE

Any controller that shares one or more VLANs with another controller must be part of the same AirGroup multi-controller cluster.

Controller Dashboard Monitoring

The AirGroup page on the controller's **Dashboard** tab lets you view AirGroup users, servers, and the services that they advertise. To view the AirGroup page, open the Aruba controller WebUI and navigate to **Dashboard > AirGroup**.

Figure 7 *Controller Dashboard Monitoring*



The overlay deployment model uses one access controller to terminate APs and provide WLAN services, and a second dedicated mDNS proxy controller to act as an overlay that provides AirGroup functionality. This model allows you to deploy AirGroup without upgrading the existing production controller managing your network. Although the production WLAN controller does not require a code upgrade, the overlay AirGroup controller requires a version of ArubaOS that supports the AirGroup feature.

The production WLAN controller must be configured with ACL redirect rules to send mDNS traffic from user VLANs to the overlay controller, which is connected through a L2 GRE tunnel. If you use this model, ensure that no user VLANs (wired or wireless) terminate on the AirGroup overlay controller. If you must terminate user VLANs on the overlay controller, ensure that no VLANs create a loop.

NOTE

Multi-Controller AirGroup clusters are not supported in overlay deployment model. Use the Integrated Deployment Model on page 10 to support Multi-Controller AirGroup clusters.

Refer to the following sections to configure the WLAN Controller and the AirGroup Controller in an overlay deployment:

- Configuring the WLAN Controller on page 33
- Configuring the AirGroup Controller on page 34

Configuring the WLAN Controller

To configure the mobility access controller that terminates the APs:

1. Create an L2 GRE tunnel from the mobility access controller to the AirGroup controller and identify the user VLAN that carries the mDNS packets to the AirGroup controller:

```
interface tunnel <tunnel_id>
description <description>
tunnel source <tunnel source IP> or controller-ip
tunnel mode gre 0
tunnel destination <mDNS proxy IP>
trusted
tunnel vlan <List of user VLANs>
```

2. Add a session ACL for user roles to redirect all mDNS packets from clients to the tunnel. (This ACL must be moved to the top of the ACL list):

```
ip access-list session <redirect_ACL>
          user any udp 5353  redirect tunnel <tunnel_id>
user-role <user_role>
          access-list session <redirect_ACL>
          access-list session allowall
          access-list session v6-allowall
```

3. Enable the **Convert Broadcast ARP Requests to Unicast** option in a Virtual AP profile to enable ARP conversion on individual virtual APs. When you enable this feature in a Virtual AP profile, broadcast ARPs destined for the wireless clients that are part of the user and station tables are converted to unicast ARP requests.

```
wlan virtual-ap <vap_profile>
broadcast-filter arp
```

4. Disable the **Drop broadcast and multicast** option in the Virtual AP profile. If this option is enabled, it drops broadcast and multicast traffic (except DHCP offers and acknowledgements), which affects the mDNS queries from the AirGroup controller and the wired network.

```
wlan virtual-ap <vap_profile>
no broadcast-filter all
```

5. Disable BC/MC optimization on user VLANs using the **interface vlan <vlan_id> no bcmc-optimization** command, and then execute the **show interface vlan <vlan_id>** command to verify that
BC/MC optimization is disabled:

```
(host)(config) #interface vlan <vlan_id>
   no bcmc-optimization

(host)(config) #show interface vlan <vlan_id>
   VLAN1 is up line protocol is up
   Hardware is CPU Interface, Interface address is 00:0B:86:0E:4A:00 (bia
   00:0B:86:0E:4A:00)
   Description: 802.1Q VLAN
   Internet address is 10.15.17.165  255.255.255.0
   IPv6 is enabled, link-local address is fe80::b:8600:10e:4a00
   IPv6 Router Advertisements are disabled
   Routing interface is enable, Forwarding mode is enable
   Directed broadcast is disabled, BCMC Optimization disabled ProxyARP disabled
   Suppress ARP disabled
   Encapsulation 802, loopback not set
   MTU 1500 bytes
   IGMP Snooping is enabled on this interface
   Last clearing of "show interface" counters 0 day 4 hr 24 min 23 sec
   link status last changed 0 day 4 hr 22 min 35 sec
   Proxy Arp is disabled for the Interface
```

NOTE

Any wired mDNS devices, such as Apple TV or printers which are directly connected to the access controller in an overlay deployment, must be connected to untrusted ports. The mDNS packets from these wired devices is tunneled to an overlay controller by using Access Control List (ACL) redirect in a user role and only when the users are connected to untrusted ports.
If the devices are connected to trusted ports, then the mDNS packets are directly forwarded to the users and the policies are not applied to these packets.

Configuring the AirGroup Controller

To configure an overlay AirGroup controller:

1. Create an L2 GRE tunnel from the mDNS proxy controller to the mobility access controller. If your deployment has multiple access controllers, repeat this process to create a tunnel for each one.

```
interface tunnel <tunnel_id>
description <description>
tunnel source <tunnel source IP> or controller-ip
tunnel mode gre 0
tunnel destination <access controller IP>
trusted
tunnel vlan <List of user VLANs>
```

2. Create user VLANs and VLAN interfaces on the proxy controller and access controller.

```
vlan <vlan_id>
interface vlan <vlan_id>
ip address <ipaddr> <mask>
```

3. Assign valid IP addresses to the user VLAN interfaces.
4. Add these user VLANs to the L2 GRE tunnel interface.
5. Configure AirGroup services that need to be allowed on the network.

   Use the following command to enable a service:

```
airgroup service <string> enable
Example: airgroup service airplay enable
```

   Use the following command to disable a service:

```
airgroup service <string> disable
Example: airgroup service airplay disable
```

Configure the AirGroup and ClearPass Policy Manager (CPPM) interface to allow an AirGroup controller and CPPM to exchange information about the owner, visibility, and status for each mobile device on the network. The following procedures configure the AirGroup-CPPM interface:

Configuring CPPM Query Interval

The AirGroup CPPM query interval is used to refresh the CPPM entries at periodic intervals. The minimum value is 1 hour and the maximum value is 24 hours. The default value is 10 hours.

Using the WebUI

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. Select the **AirGroup Settings** tab.
3. Under **Global Settings > AirGroup CPPM query interval**, enter a value in the range of 1 to 24 hours.

Using the CLI

```
[no] airgroup cppm-server query-interval <1..24>
```

Sample Configuration

```
(host) (config) #airgroup cppm-server query-interval 9
```

Command Mode

Configuration mode on master controllers.

Viewing CPPM Query Interval

The following procedure displays the configured CPPM query interval value.

Using the WebUI

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. Select the **AirGroup Settings** tab.
3. In the **Global Settings** section the **AirGroup CPPM query interval** displays the value in hours.

Using the CLI

```
show airgroup cppm-server query-interval
```

Sample Configuration

```
(host) #show airgroup cppm-server query-interval
CPPM Server Query Interval
```

```
-------------------------
Timer Value  Unit
-----------  ----
9            hours
```

The output of this command includes the following information:

Table 12 *show airgroup cppm-server query-interval*

Column	Description
`Timer Value`	Displays the number of hours.
`Unit`	Displays the unit in hours.

Command Mode

Enable mode on master controllers.

Defining CPPM and RFC3675 Server

You must define one or more CPPM servers to be used by the AirGroup RADIUS client, and an RFC 3576 (dynamic authorization) server. If multiple CPPM servers are defined, the servers are listed in a sequential order. The AirGroup RADIUS client will use the first available server on this list.

The following table describes the configuration parameters for a CPPM server.

Table 13 *CPPM Server Configuration Parameters*

Parameter	Description
Host	IP address or fully qualified domain name (FQDN) of the authentication server. The maximum supported FQDN length is 63 characters.
Key	Shared secret between the controller and the authentication server. The maximum length is 128 characters.
Authentication Port	Authentication port on the server. Default: 1812
Accounting Port	Accounting port on the server. Default: 1813
Retransmits	Maximum number of retries sent to the server by the controller before the server is marked as down. Default: 3
Timeout	Maximum time, in seconds, that the controller waits before timing out the request and resending it. Default: 5 seconds
NAS ID	Network Access Server (NAS) identifier to use in RADIUS packets.
NAS IP	NAS IP address to send in RADIUS packets. You can configure a “global” NAS IP address that the controller can use for communications with all CPPM servers. Note, however, that the controller will only use this global NAS IP If you do not configure a server-specific NAS IP. To set the global NAS IP in the WebUI, navigate to the **Configuration > Security > Authentication > Advanced** page. To set the global NAS IP in the CLI, enter the **ip radius nas-ip <A.B.C.D>** command.

Table 13 *CPPM Server Configuration Parameters (Continued)*

Parameter	Description
Source Interface	Enter a VLAN number ID. This value allows you to use source IP addresses to differentiate RADIUS requests, and associates a VLAN interface with the RADIUS server to allow the server-specific source interface to override the global configuration. • If you associate a Source Interface (by entering a VLAN number) with a configured server, then the source IP address of the packet will be that interface's IP address. • If you do not associate the Source Interface with a configured server (leave the field blank), the IP address of the global Source Interface will be used.
Use MD5	Use a MD5 hash of the cleartext password.
Use IP address for calling station ID	Select this check box to use an IP address instead of a MAC address for the calling station ID.
Mode	Enables or disables the server.

Configuring a CPPM Server

You can configure a CPPM server for AirGroup using the WebUI or CLI.

NOTE

Server-derived user roles or VLANs configured in this server group are not applicable to AirGroup.

Using the WebUI

To configure a CPPM server using the controller WebUI:

1. Navigate to the **Configuration > Security > Authentication > Servers**.
2. Select **Radius Server** to display the CPPM Server List.
3. To configure a CPPM server, enter the name for the server and click **Add**.
4. Select the name to configure server parameters. Select the **Mode** check box to activate the authentication server.
5. Click **Apply** to apply the configuration.

Using the CLI

Use the following commands to configure a CPPM server using the CLI:

```
aaa authentication-server radius <name>
   host <ipaddr>
   key <key>
   enable
```

Sample Configuration

```
(host)(config) #aaa authentication-server radius emp_accounts
(host)(RADIUS Server "emp_accounts") #host 10.100.8.32
(host)(RADIUS Server "emp_accounts") #key employee123
(host)(RADIUS Server "emp_accounts") #enable
```

Command Mode

Configuration mode on master controllers.

Configuring the CPPM Server Group

Using the WebUI

To configure a CPPM server group using the controller WebUI:

1. Navigate to the **Configuration > Security > Authentication > Servers**.
2. Select **Server Group** to display the Server Group list.
3. Enter the name of the new server group and click **Add**.
4. Select the name to configure the server group.
5. Under **Servers**, click **New** to add a server to the group.
   a. Select a server from the drop-down menu and click **Add Server**.
   b. Repeat the above step to add other servers to the group.
6. Click **Apply**.

Using the CLI

Use the following commands to configure a CPPM server group using the CLI:

```
aaa server-group <name>
   auth-server <name>
```

Sample Configuration

```
(host) (config) #aaa server-group employee
(host) (Server Group "employee") #auth-server emp_accounts
```

Command Mode

Configuration mode on master controllers.

Configuring an RFC 3576 Server

Using the WebUI

To configure an RFC 3576 server using the controller WebUI:

1. Navigate to the **Configuration > Security > Authentication > Servers**.
2. Select **RFC 3576 Server**.
3. Enter the **IP address** and click **Add**.
4. Select the IP address to enter the shared secret key in the **Key** text box.
5. Retype the shared secret key in the **Retype** text box.

Using the CLI

Use the following commands to configure an RFC 3576 server using the CLI:

```
aaa rfc-3576-server <server_ip>
   key <string>
```

Sample Configuration

```
(host) (config) #aaa rfc-3576-server 10.100.8.32
(host) (RFC 3576 Server "10.100.8.32") #key employee123
```

Command Mode

Configuration mode on master controllers.

Assigning CPPM and RFC 3576 Servers to AirGroup

Use the following procedures to assign CPPM and RFC 3576 servers to AirGroup.

> **NOTE**
> An AirGroup RFC 3576 server cannot use the same port as an authentication module RFC 3576 server. To avoid conflicts, use a non-standard port for the AirGroup RFC 3576 server.

Using the WebUI

Use the following procedure to configure the AirGroup AAA profile using the controller WebUI:

1. Navigate to the **Configuration > Advanced Services > All Profiles** page.
2. Expand the **Other Profiles** menu and select **AirGroup AAA Profile**.
3. In the **Configure dead time for a down Server** text box in the **Profile Details** window, enter the maximum period after which a client sending no user traffic should be considered idle.
4. Enter the UDP port number in the **Configure UDP port to receive RFC 3576 server requests** field. If your network uses an RFC 3576 server for authentication, select a different port for the AirGroup 3576 server. The default in ClearPass Guest is 5999.
5. Next, identify the AirGroup CPPM server group. In the **Profiles** list, select the Server Group under the **AirGroup AAA Profile** menu.
6. In the **Profile Details** window, click the **Server Group** drop-down list to select the desired CPPM server group.
7. Click **Apply.**
8. Identify the RFC 3576 server. In the Profiles list, select RFC 3576 Server under the **AirGroup AAA Profile** menu.
9. Enter the IP address of the RFC 3576 server in the Add a p**rofile** text box.
10. Click **Add** and **Apply**.

Using the CLI

Execute the following commands to configure the AirGroup AAA profile using the command-line interface:

```
airgroup cppm-server aaa
   rfc-3576-server <ip address>
   rfc-3576_udp_port <port number>
   server-dead-time <time>
   server-group <server group name>
```

> **NOTE**
> If your network uses an RFC 3576 server for authentication, select a different port for the AirGroup 3576 server. The default in ClearPass Guest is 5999.

Sample Configuration

```
(host) (config) # airgroup cppm-server aaa
(host) (Airgroup AAA profile) #rfc-3576-server 10.15.16.25
(host) (Airgroup AAA profile) #rfc3576_udp_port 21334
(host) (Airgroup AAA profile) #server-dead-time 10
(host) (Airgroup AAA profile) #server-group employee
```

Command Mode

Configuration mode on master controllers.

Change of Authorization (CoA)

To enable change of authorization (CoA) for the RFC 3576 server:

1. Configure the ClearPass Policy Manager and the AirGroup controller with the same RFC-3576 UDP port you defined in the procedures "Using the WebUI" on page 41 or "Using the CLI" on page 41.
2. Configure a firewall policy to permit CoA traffic using the **firewall cp permit proto 17 ports <rfc-3576-udp port> <rfc-3576-udp port>** command. The **<rfc-3576-udp port>** port number in this command must be the same RFC-3576 UDP port number you defined in the procedures Using the WebUI on page 41 or Using the CLI on page 41. The default in ClearPass Guest is 5999.

Viewing the CPPM Server Configuration

Using the WebUI

To view the CPPM server configuration using the controller WebUI:

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. Select the **AirGroup Settings** tab.
3. The **AirGroup CPPM server aaa** section displays the CPPM Server configuration.

Using the CLI

Use the following CLI command to view data for the ClearPass Policy Manager servers:

```
(host) #show airgroup cppm-server aaa
Config-cppm-server-aaa
----------------------
Parameter                                                  Value
---------                                                  -----
Server Group                                                RADIUS_4
RFC 3576 server                                             Test1
Configure dead time for a down Server                       10
Configure UDP port to receive RFC 3576 server requests      N/A
```

The output of this command includes the following information:

Table 14 *show airgroup cppm-server aaa*

Column	Description
`Parameter`	AAA parameters for AirGroup.
`Value`	Displays the value entered for each AAA parameter.

Command Mode

Configuration mode on master controllers.

Verifying CPPM Device Registration

Use the **show airgroup cppm entries** command to display information for devices registered in ClearPass Policy Manager.

```
(host) #show airgroup cppm entries

ClearPass Guest Device Registration Information
-----------------------------------------------
Device             device-owner  shared location-id AP-name  shared location-id AP-FQLN
```

```
------              ------------  --------------------------  --------------------------
98:d6:bb:25:8b:9f  ade

shared location-id AP-group  shared user-list  shared role-list
---------------------------  ----------------  ----------------

Num CPPM Entries:1
```

The output of this command includes the following information:

Table 15 *show airgroup cppm entries*

Column	Description
`Device`	Displays the MAC address of the AirGroup device
`device-owner`	Displays the user name of the AirGroup device.
`shared location-id AP-name`	Displays the location ID based on an AP name. **NOTE:** The geographical location of AirGroup device can be tracked with respect to its RF neighbors. AirGroup devices connected to APs can be located based on nearby APs. In this case, an AirGroup user's AP could be any of the APs in AirGroup server's neighbor AP list, in addition to the server's own associated AP to receive the service advertisements from the corresponding AirGroup server.
`shared location-id AP-FQLN`	Displays the location ID based on the Fully Qualified Location Name (FQLN) value of an AP. AP FQLN is configured in the format **<apname>.<floor>.<building>.<campus>**
`shared location-id AP-group`	Displays the location ID based on the name of an AP group.
`shared user-list`	Displays one or more primary login IDs of an AirGroup user.
`shared role-list`	Displays the name of the controller role.
`#CPPM-Req`	Displays the number of requests sent by AirGroup controller to CPPM server to populate the policy details for the given client.
`#CPPM-Resp`	Displays the number of responses received from the CPPM server for policy details of the given client.

Configuring CPPM to Enforce Registration

The AirGroup solution allows users to view all mDNS devices by default.AirGroup provides a set of policy definitions to allow or disallow one of more AirGroup servers from being visible to specific AirGroup users.

If an AirGroup server is not registered on a CPPM server, by default, the server will be visible to all AirGroup users. The administrator has to register an AirGroup server to allow or disallow this server from being visible to specific AirGroup users.

The following procedure registers an AirGroup server on a CPPM server:

Using the WebUI

To configure using the controller WebUI:

1. Navigate to the **Configuration > Advanced Services > AirGroup** page.
2. Select the **AirGroup Settings** tab.

3. Under **Global Settings > AirGroup CPPM enforce registration**, select **enable** from the drop-down menu.

Using the CLI

Use the following command to force AirGroup servers to register with CPPM. This option is disabled by default:

```
(host) (config) #airgroup cppm-server enforce-registration
```

To verify the CPPM Registration Enforcement status, use the following command:

```
(host) #show airgroup status

AirGroup Feature
----------------
Status
------
Enabled

AirGroup Enforce Registration
-----------------------------
Status
------
Enabled

AirGroup Service Information
----------------------------
Service         Status
-------         ------
airplay         Enabled
airprint        Enabled
itunes          Disabled
remotemgmt      Enabled
sharing         Enabled
chat            Enabled
allowall        Enabled
```

To view the description of the column headings, see Table 7 on page 26.

Command Mode

Configuration mode on master controllers.

This chapter describes how to configure the ClearPass Guest user interface and the AirGroup protocol that communicates with the Aruba controller. These interfaces are key components of the Aruba AirGroup solution.

ClearPass Guest is used to:

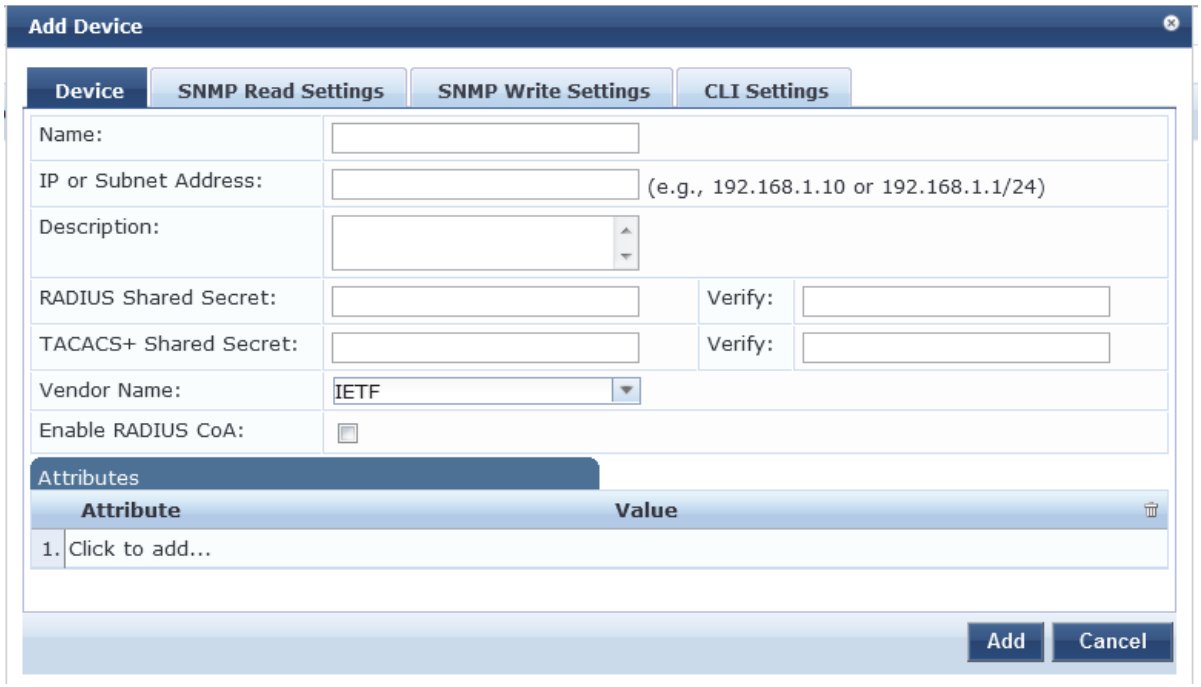
- Add new AirGroup controllers
- Enable the controllers to receive dynamic notifications of AirGroup Events
- Configure AirGroup logging in ClearPass Guest
- Perform some of the steps to create AirGroup administrators and operators
- Authenticate AirGroup users via LDAP
- Register and manage AirGroup devices

Configuring Network Access Devices

Each AirGroup-enabled Aruba controller must be defined as a network access device in ClearPass Policy Manager.

1. In ClearPass Policy Manager, navigate to **Configuration** > **Network** > **Devices**.
2. Click the **Add Device** link in the upper-right corner. The **Add Device** form opens.

Figure 8 *Add Device Form*



3. Complete the details on the **Device** tab of the form. Ensure that you specify the correct **RADIUS Shared Secret** for the controller.
4. Click **Add**.

Enabling Support for Dynamic Notifications

With more than one controller requesting AirGroup policy information for the same user, CPPM sends a Change of Authorization (CoA) request to all applicable controllers for this user. CPPM maintains a dynamic list of such controllers for each user from whom a RADIUS MAC authentication request was observed earlier, so that CPPM can send a CoA request to all these controllers in future.

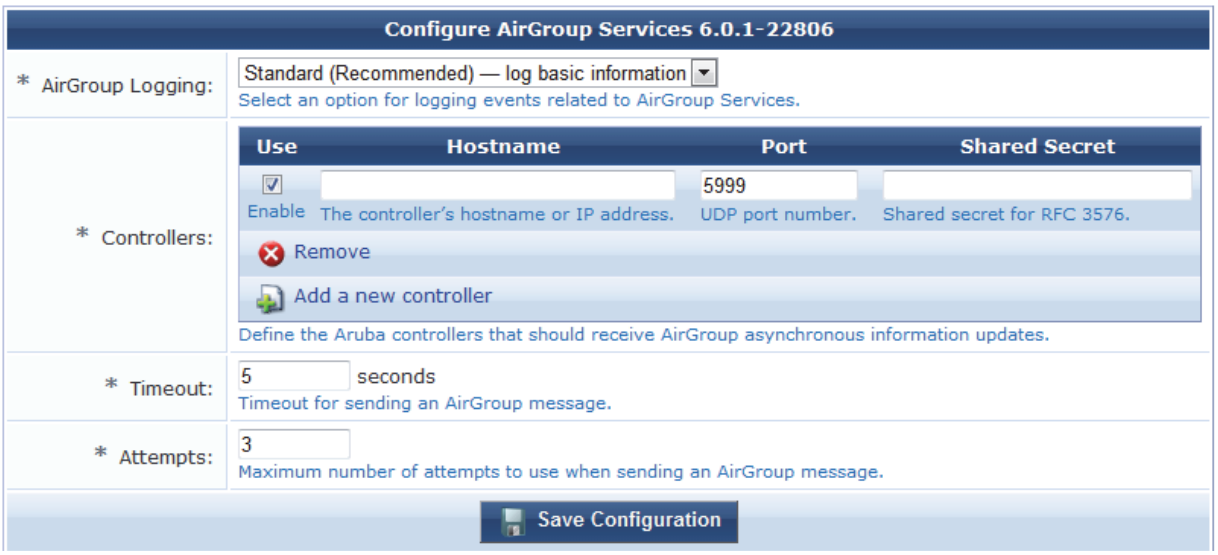
CPPM maintains an idle time-out mechanism for each user. This removes the controller from the user list for users when a RADIUS MAC authentication request was not observed in the last 24 hours. The idle time out value is not a configurable parameter and is set to 24 hours.

To enable support for dynamically notifying the controller of AirGroup events when new devices are added, each AirGroup-enabled Aruba controller must be defined in ClearPass Guest.

To enable support for dynamic notifications and configure AirGroup logging:

1. In ClearPass Guest, navigate to **Administration > AirGroup Services** and click the **Configure AirGroup Services** command link. The **Configure AirGroup Services** form opens.

Figure 9 *Configure AirGroup Services Form*



2. In the **AirGroup Logging** drop-down list, choose one of the following options to configure AirGroup logging levels in the ClearPass Guest application logs:
   - **Disabled — Do not log AirGroup related events**
   - **Standard (Recommended) — Log basic information**
   - **Extended — Log additional information**
   - **Debug — Log debug information**
   - **Trace — Log all debug information**
3. In the **Controllers** section, click the **Add a new controller** link to add a new AirGroup controller and receive dynamic notifications of AirGroup events. The row expands to include fields for entering the controller's properties.
4. Specify the following properties for each AirGroup-enabled controller:
   a. **Hostname or IP address**
   b. **Port number** – This should be AirGroup cppm-server aaa rfc3576-server, the UDP port number of the AirGroup process on the controller. This is the same port number you defined when configuring the CPPM interface. The default in ClearPass Guest is 5999. See "Assigning CPPM and RFC 3576 Servers to AirGroup" in the "Configuring The AirGroup-CPPM Interface" chapter.
   c. **Shared secret** – This is the rfc-3576_udp_port shared secret used for AirGroup.

5. In the **Timeout** row, enter the number of seconds after which an attempt to send an AirGroup message should time out.
6. In the **Attempts** row, enter the maximum number of times the system should attempt to send an AirGroup message.
7. Click **Save Configuration**.

Creating AirGroup Users

AirGroup users, both administrators and operators, use ClearPass Guest to register and manage devices:

- AirGroup Administrators can use the **Create Device** form in ClearPass Guest to define and manage the organization's shared devices. Devices can be shared globally, or shared with restrictions based on the username, role name, or location of a user trying to access the device.
- AirGroup Operators can use the **Create Device** form in ClearPass Guest to define and manage a limited number of personal devices. An operator's devices are automatically shared with all other devices owned by the same operator. Devices may also be shared with specific users.

Each AirGroup user needs a ClearPass Guest operator login with the appropriate AirGroup profile. Because ClearPass Policy Manager profiles and ClearPass Guest profiles are different, a local user with an AirGroup role is defined in ClearPass Policy Manager, and ClearPass Guest uses translation rules to map the role to the appropriate AirGroup profile. The AirGroup roles, profiles, and translation rules are automatically included in CPPM and Guest, when AirGroup is enabled.

To view details for the profiles, navigate to **ClearPass Guest > Administration > Operator Logins > Profiles**. In the **Operator Profiles** list, click to expand the row of either AirGroup profile, then click the **Show Details** option.

Figure 10 *The Operator Profiles List in ClearPass Guest, Showing Details*

Name	Description
AirGroup Administrator	Operators with this profile can manage multiple devices that are shared with all users based on location.

Hide Details | Edit | Delete | Duplicate | Show Usage

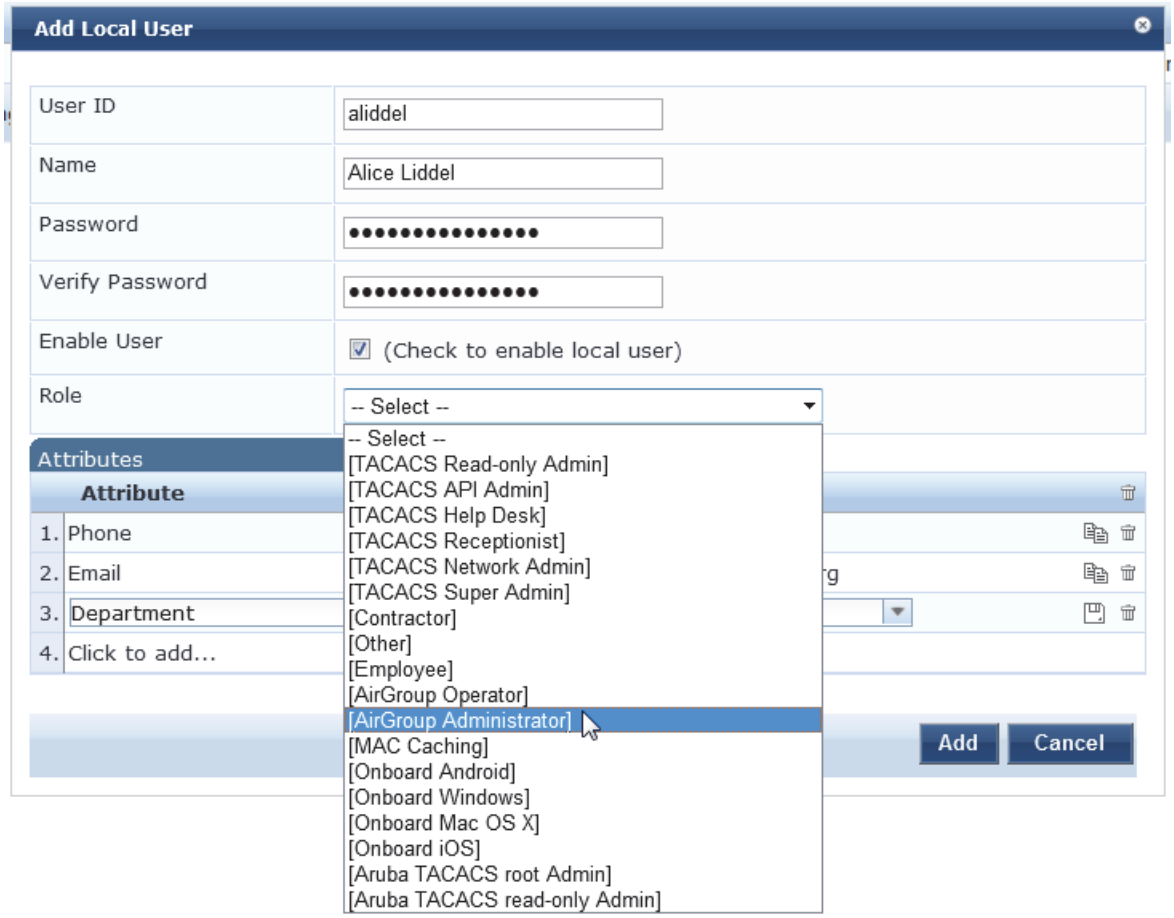
Operator Profile	
Name:	**AirGroup Administrator**
Description:	Operators with this profile can manage multiple devices that are shared with all users based on location.
Operator logins:	Enabled
Privileges:	**Guest Manager** — **Custom** Create New MAC Authentication — Full Access Full User Control — Full Access List MAC Authentication accounts — Full Access Remove Accounts — Full Access
Skin:	
Start Page:	List Devices
Language:	(Default)
Time Zone:	(Default)

AirGroup Operator	Operators with this profile can self-provision up to 5 devices within their personal WLAN.
Help Desk	A help desk operator logs in to troubleshoot problems reported by end user.
IT Administrators	Default administrative profile.

To create a new AirGroup user:

1. In **ClearPass Policy Manager**, navigate to **Configuration > Identity > Local Users**, and click the **Add User** link in the top-right corner. The **Add Local User** form opens.

Figure 11 *Add Local User Form*



2. In the **User ID** field, enter the username for AirGroup login.
3. In the **Name** field, enter the name of the user.
4. In the **Password** and **Verify Password** field, enter a password for the user. (For security, regardless of how many characters you enter in the **Password** field, it is automatically masked with 15 dots when you move to the next field.)
5. In the **Role** drop-down list, select the **AirGroup Administrator** or **AirGroup Operator** role.
6. In the **Attributes** area of the form, use the **Click to add** link to add **Phone**, **Email**, **Sponsor**, **Title**, **Department**, or **Designation** attributes for the user, then enter values for the attributes.
7. When your entries on the form are complete, click **Add**. The form closes and the new user is displayed in the **Local Users** list. The new user you created can now log in to ClearPass Guest to manage and register shared devices.

To change your entries after the user is created, you can click the row in the **Local Users** list and modify the properties in the **Edit Local User** form.

Configuring an AirGroup Operator Device Limit

By default, an AirGroup operator can create up to five personal devices. You can modify the default device limit for an AirGroup Operator profile. If you wish to keep the default AirGroup Operator profile and add a profile with a different limit, see "Creating Additional Profiles with Different Device Limits".

Changing the Device Limit for the AirGroup Operator Profile

To change the default device limit for the standard AirGroup Operator profile:

1. In ClearPass Guest, navigate to **Administration > Operator Logins > Profiles**, then select the **AirGroup Operator** profile in the list.
2. Click the **Edit** link. The **Edit Operator Profile** form opens.
3. In the **Account Limit** field, specify an appropriate value. This is the maximum number of personal devices that an operator with this profile can create.
4. Click **Save Changes**. The number you specified will be the device limit for all users with the AirGroup Operator profile.

Creating Additional Profiles with Different Device Limits

If you need to provide different device limits to different users, you can create a set of operator profiles and configure each profile with a different account limit. This makes it easy to assign operator profiles for small groups, larger groups, or events. To create each new profile, create a copy of the standard AirGroup Operator profile with a new name, update the **Account Limit** field in the new profile, and apply the appropriate translation rule.

To create the new AirGroup Operator profile with a different device limit:

1. In ClearPass Guest, navigate to **Administration > Operator Logins > Profiles**, then click the **AirGroup Operator** profile in the list. The row expands to include option links.
2. Click the **Duplicate** link. The status of the operation is displayed while the profile is being duplicated. When it is complete, the **Copy of AirGroup Operator** profile is included below the original in the Operator Profiles list.
3. In the **Copy of AirGroup Operator** row, click the **Edit** link. The **Edit Operator Profile** form opens.
4. In the **Name** field, give the profile a name that clearly identifies what it is—for example, **AirGroup Operator - Device Limit 25**, or **AirGroup Operator 10 Devices**.
5. In the **Description** field, modify the text to match the new number of devices.
6. To make the profile available as soon as you complete the form, mark the **Allow operator logins** check box in the **Enabled** row. You can leave the check box unmarked to create a profile that will be used later, then come back to this form to enable it when it is needed.
7. In the **Privileges** area, use the **AirGroup Services** drop-down list to specify the level of access for the operator.
8. In the **Account Limit** field, specify an appropriate value. This is the maximum number of personal devices that an operator with this profile can create.
9. Click **Save Changes**. The number you specified will be the device limit for all users assigned this operator profile.

After you create the AirGroup operator profile, provide a matching translation rule:

1. In **ClearPass Guest**, navigate to **Administration > Operator Logins > Translation Rules**, and then click the **Copy of ClearPass AirGroup Operator** rule in the list. The row expands to include option links.
2. Click the **Duplicate** link. The status of the operation is displayed while the rule is being duplicated. When it is complete, the **Copy of ClearPass AirGroup Operator** rule is included below the original in the Operator Translation Rules list.

3. In the **Copy of ClearPass AirGroup Operator** row, click the **Edit** link. The row expands to include the Edit Translation Rule form.
4. In the **Name** field, specify a name that indicates the rule, so that it can match the appropriate operator profile. For example, **ClearPass AirGroup Operator - Device Limit 25**.
5. To make the rule available as soon as you complete the form, select the check box in the **Enabled** row. If the check box is not selected, the rule will appear in the rules list but will not be active until you come back to this form to enable it.
6. In the **Matching Rule** drop-down list, choose **equals**.
7. In the Value field, modify the pre-populated value to match the new operator profile you created—for example, **[AirGroup Operator - Device Limit 25]**.
8. Leave the value in the **On Match** field set to **Assign fixed operator profile**.
9. In the **Operator Profile** field, use the drop-down list to choose the new operator profile you created—for example, **AirGroup Operator - Device Limit 25**. Verify if the operator profile's device limit matches the device limit set in the name of the associated rule.
10. When you have completed the form, click **Save Changes**. The Action column in the Translation Rules list is updated to show the new operator profile with the modified device limit assigned to the new translation rule with the matching device limit.

Authenticating AirGroup Users Through LDAP

ClearPass Guest supports LDAP authentication for AirGroup administrators and operators. To provide AirGroup services to LDAP-authenticated users, in ClearPass Guest:

- Use the **Administrator > Operator Logins > Servers** list view to define the LDAP server for AirGroup.
- Define the appropriate translation rules to categorize the LDAP users:
  - Network administrators (for example, IT staff) responsible for provisioning shared devices across the organization should be assigned the **AirGroup Administrator** operator profile.
  - Other users (for example, staff or students) who should only be allowed to provision personal devices should be assigned the **AirGroup Operator** profile.

Refer to the *Operator Logins* chapter of the *ClearPass Guest Deployment Guide* for details on external operator authentication and custom LDAP translation processing.

Registering Devices in ClearPass Guest

After configuration is complete, administrators and operators can register devices.

Registering Groups of Devices or Services

AirGroup administrators can provision their organization's shared devices and manage access. This functionality is only available to AirGroup administrators.

To register and manage an organization's shared devices and configure device access:

1. Log in as the AirGroup administrator. In **ClearPass Guest**, navigate to **Guest > Create Device**. The Register Shared Device form opens.

Figure 12 *Register Shared Device Form*

2. In the **Device Name** field, enter the name used to identify the device.
3. In the **MAC Address** field, enter the MAC address of the device.
4. In the **Shared Locations** field, enter the locations where the device can be shared. To allow the device to be shared with all locations, leave this field blank.

   Each location is entered as a tag=value pair describing the MAC address of the access point (AP) closest to the registered device. Use commas to separate the tag=value pairs in the list. Tag=value pair formats are shown in the following table.

Table 16 *Tag=Value Pair Formats*

Location Attribute	Tag=Value Format	Description
AP-Name based	ap-name=<name>	When the location is set to ap-name, all AirGroup users connected to this AP and to APs which are in the same RF neighborhood can access the shared device.
AP-Group based	ap-group=<group>	When the location attribute is set to ap-group, all AirGroup users associated to APs in the specified AP group can access the shared device.
AP-FQLN based	fqln=<fqln>	When the location attribute is set to ap-FQLN, all AirGroup users connected to APs on the same floor, and to the APs on a floor above or below the configured APs can access the shared device.

   - AP FQLNs should be configured in the format **`<ap-name>.floor <number>.<building>.<campus>`**
   - The `<ap-name>` should not include periods (.)

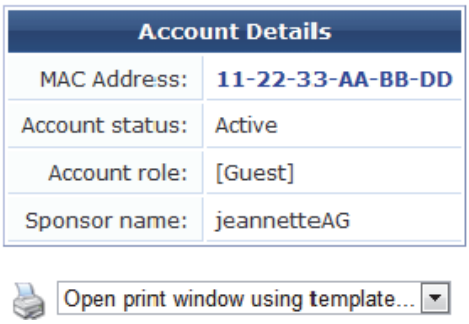
   Example:

   `AP105-1.Floor 1.TowerD.Aruba`

5. In the **Shared With** field, enter the usernames of your organization's staff or students who are allowed to use the device. Use commas to separate usernames in the list. To make the device available to all the organization's users, leave this field blank.

6. In the **Shared Roles** field, enter the user roles that are allowed to use the device. Use commas to separate the roles in the list. To make the device available to all roles, leave this field blank.
7. Click **Register Shared Device**. The **Finished Creating Guest Account** page opens. This page displays **Account Details** and provides printer options.

Figure 13 *Account Details Form*



To view and edit your organization's shared AirGroup devices:

1. In **ClearPass Guest**, navigate to **Guest > List Devices**, or click the **Manage my AirGroup Devices** link on the Create AirGroup Device page. The AirGroup Devices page opens. This page lists all the shared AirGroup devices for the organization. You can remove a device; edit a device's name, MAC address, shared locations, shared-user list, or shared roles; print device details; or add a new device.
2. To work with a device, click the device's row in the list. The form expands to include the **Remove**, **Edit**, and **Print** options.

Registering Personal Devices

AirGroup operators can register and provision a limited number of their own personal devices for sharing.

To register your personal devices and define a group who can share them:

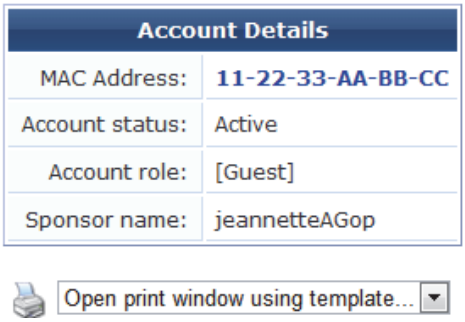
1. Log in as the AirGroup operator. In **ClearPass Guest**, navigate to **Guest > Create Device**. The **Register Device** form opens.

Figure 14 *Register Device Form*

2. In the **Your Name** field, enter your username for your organization.
3. In the **Device Name** field, enter the name used to identify the device.
4. In the **MAC Address** field, enter the device's MAC address.
5. In the **Shared With** field, enter the usernames of your friends or colleagues who are allowed to use the device. Use commas to separate usernames in the list. You may enter up to ten usernames.

6. Click **Register Device**. The **Finished Creating Guest Account** page opens. This page displays **Account Details** and provides printer options.

Figure 15 *Account Details Form*



To view and edit your personal AirGroup devices, navigate to **Guest > List Devices**, or click the **Manage my AirGroup Devices** link on the Create AirGroup Device page. The List Device page lets you remove a device; edit a device's name, MAC address, or shared-user list; print device details; or add a new device.

To view and edit your personal AirGroup devices:

1. Navigate to **Guest > List Devices**, or click the **Manage my AirGroup Devices** link on the Create AirGroup Device page. The AirGroup Devices page opens. This page lists all your personal AirGroup devices. You can remove a device; edit a device's name, MAC address, or shared-user list; print device details; or add a new device.
2. Click the device row in the list. The form expands to include the **Remove**, **Edit**, and **Print** options.

Controller Troubleshooting Steps

Use the following procedure to troubleshoot potential errors in the controller:

1. Execute the **show airgroup internal-state statistics** CLI command and ensure that the **Sibyte Messages Sent/Recv** counters increment over a period of time.
2. Enable mDNS logs using the **logging level debugging system process mdns** command, and capture the output of **show log system all** at the time the issue was seen. Review any obvious error print statements.
3. Save the output of **show airgroup cache entries** and **change airgroup cppm** entries and look for any discrepancies.

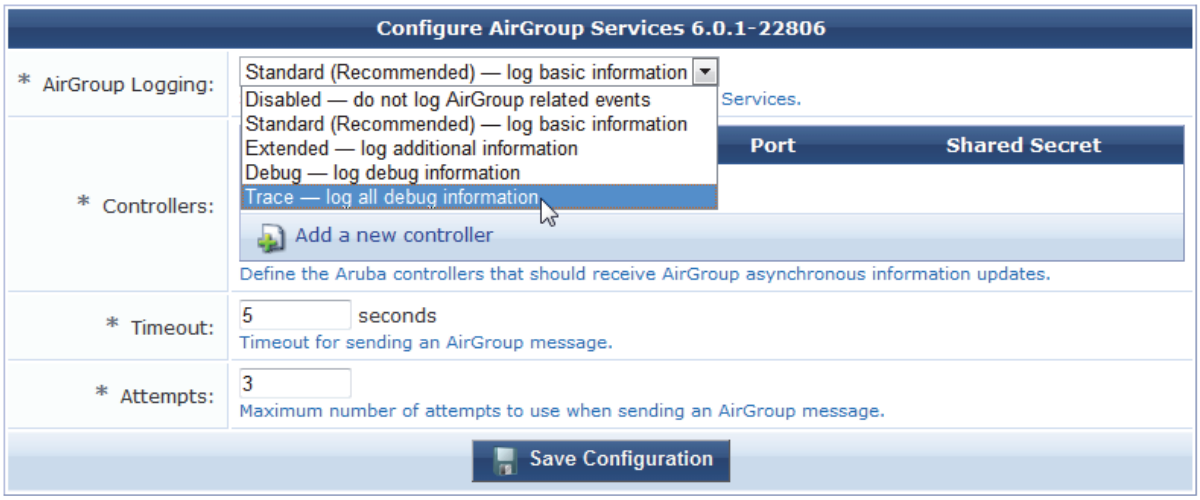
ClearPass Guest Troubleshooting Steps

ClearPass Guest includes AirGroup-related events in the application log files. You can configure logging levels to provide debugging information.

To show debugging information in event logs:

1. In **ClearPass Guest**, go to **Administration > AirGroup Services** and click the **Configure AirGroup Services** command link. The **Configure AirGroup Services** form opens.

Figure 16 *Configure AirGroup Services Form*



2. In the **AirGroup Logging** drop-down list, choose either **Debug—log debug information** or **Trace—log all debug information**. When one of these options is selected, debugging information is provided in the events log.
3. Click **Save Configuration**.

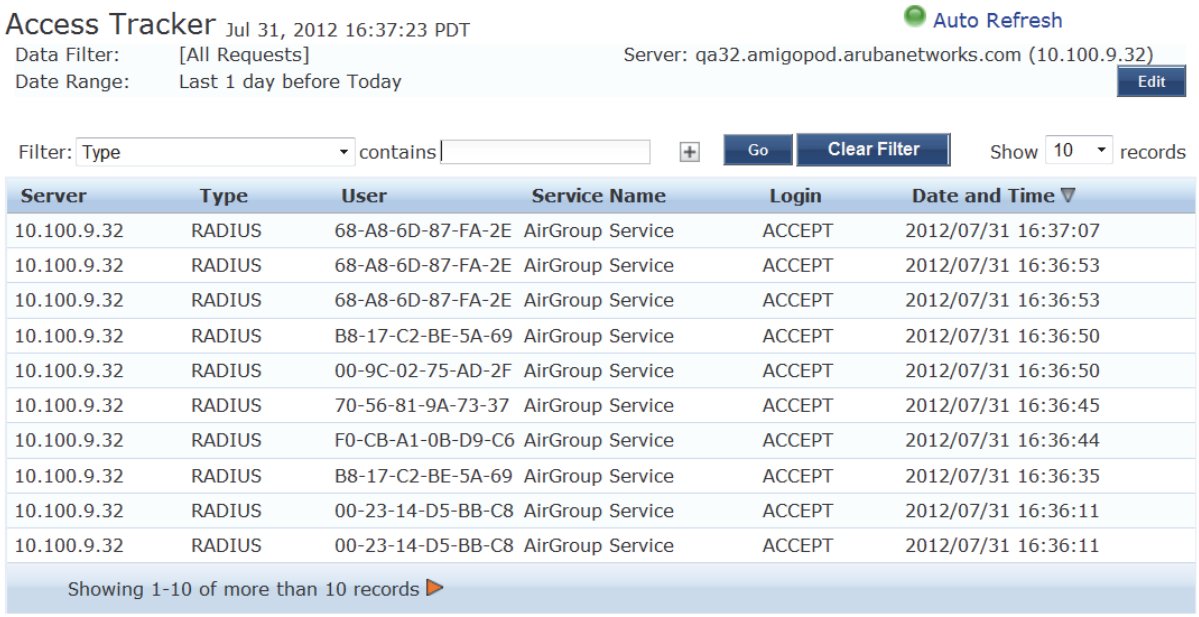
ClearPass Policy Manager Troubleshooting Steps

Monitoring and reporting services in ClearPass Policy Manager provide insight into system events and performance.

To show incoming AirGroup requests from the controller:

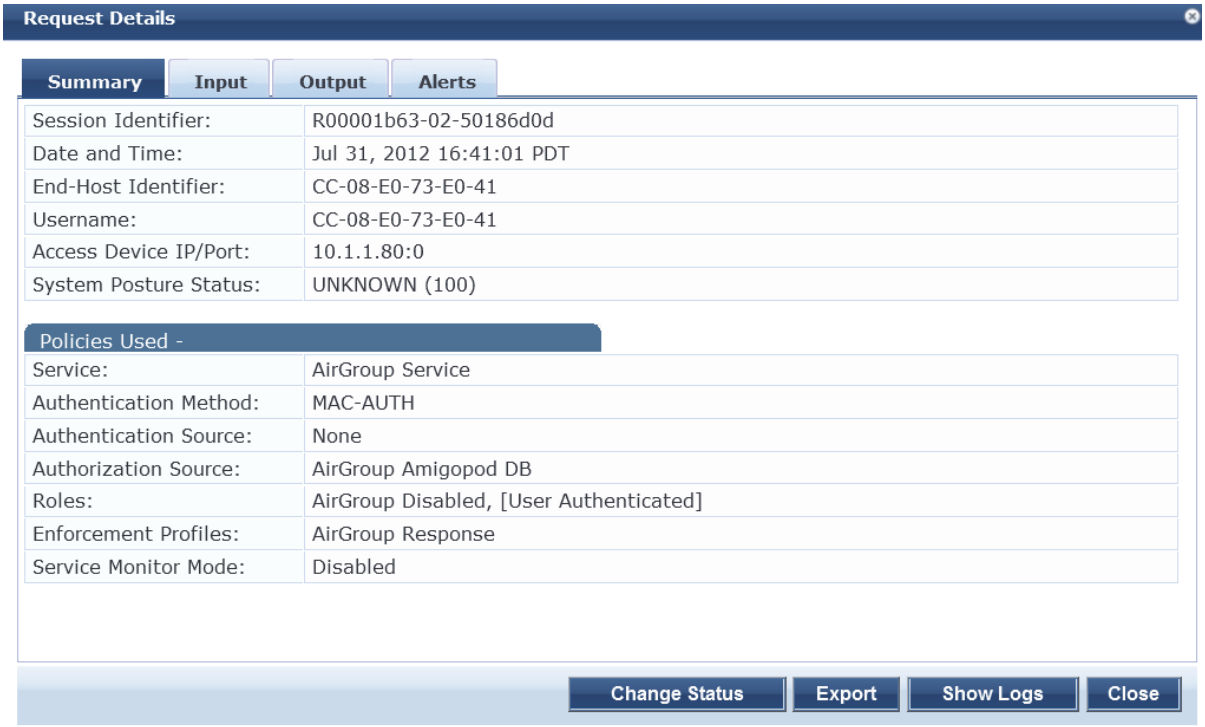
1. In **ClearPass Policy Manager**, navigate to **Monitoring > Live Monitoring > Access Tracker**. The **Access Tracker** list view opens.

Figure 17 *Access Tracker List*



2. Click an event's row to view details. The **Summary** tab of the **Request Details** view opens. Additional details may be viewed on the **Input**, **Output**, or **Alerts** tabs, or you can click the **Show Logs** button to view logging details.

Figure 18 *Request Details Form*



Log Messages

Display AirGroup logs by issuing the following commands:

- **show log all**
- **show log system all**
- **show log user all**
- **show log user-debug all**

The log debug messages for the mDNS process are not enabled by default. To enable specific logging levels, use the following CLI commands:

- To view high level mDNS debug messages:

  ```
  # logging level debugging system process mdns
  ```

- To view mDNS packet processing messages:

  ```
  # logging level debugging system process mdns subcat messages
  ```

- To view mDNS CLI configuration messages:

  ```
  # logging level debugging system process mdns subcat configuration
  ```

- To view mDNS Auth and CPPM user messages:

  ```
  # logging level debugging user process mdns
  ```

Show Commands

Use the following show commands to view AirGroup configuration data and statistics.

Viewing AirGroup mDNS Cache

```
(host)# show airgroup cache entries
Cache Entries
-------------
Name            Type    Class  TTL   Origin       Expiry   Last Update
----            ----    -----  ---   ------       ------   -----------
_ssh._tcp.local PTR     IN     4500  10.15.16.50  3765.38  Tue Feb 19 22:25:38 2013
_ssh._tcp.local PTR     IN     4500  10.15.16.28  3844.92  Tue Feb 19 22:25:34 2013
_ssh._tcp.local PTR     IN     4500  10.15.16.30  3702.80  Tue Feb 19 22:25:59 2013
_ssh._tcp.local PTR     IN     4500  10.15.16.27  3614.83  Tue Feb 19 22:25:37 2013
Num Cache Entries:4
```

The output of this command includes the following information:

Table 17 *show airgroup cache entries*

Column	Description
Name	Name of the service ID.
Type	Type of mDNS record.
Class	Class of the record. This is usually IN.
TTL	Time to live value of the service ID in seconds.
Origin	Source IP of the AirGroup server.
Expiry	Expiry period of the mDNS record in seconds.
Last Update	Time stamp of the last cache update.

Viewing AirGroup mDNS Statistics

```
# show airgroup internal-state statistics
PAPI Messages
-------------
Msg ID Name Sent Since last Read Sent Total  Recv Since Last Read  Recv Total
------ ---- -------------------- ----------  --------------------  ----------
7003    Request switch ip  1                     1           0            0
7005    Set switch ip      0                     0           1            1
7006    Request vlan info  1                     1           0            0
7007    Set vlan info      0                     0           1            1
7031    vlan oper state    1                     1           0            0
14001   mdns cli request   0                     0           36           36
10001   mdns host update   472                   472         0            0
10003   mdns client info   479                   479         479          479

RADIUS Client Messages
----------------------
Type           Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
----           --------------------  ----------  --------------------  ----------
Auth Req/Resp  646                   27471       0                     12
RFC3576        N/A                   N/A         0                     0
```

```
Sibyte Messages
---------------
Opcode  Name  Sent Since Last Read Sent Total   Recv Since Last Read  Recv Total
------  ----  ---------- --------- -----------  ---------- ---------  ----------
7       app   0                    9            0                     0
188     MDNS  62                   10081        652                   29025

Internal Statistics
-------------------
Functionality                Hit Count Since Last Read  Hit Count Total
-------------                -------------------------  ---------------
Response - Cache Update      5556                       179860
Response                     634                        24786

Average Time in microsec (since last read)  Average Time in microsec (alltime)
------------------------------------------  ----------------------------------
1153                                        1114
10687                                       8664

Multi-controller Cluster Messages
---------------------------------
Type                  Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
----                  --------------------  ----------  --------------------  ----------
Unicast Response with tag  0                     0           0                     0
Request with tag           0                     2149        0                     2067
Raw Response               0                     1000        0                     1321
```

The output of this command includes the following information:

Table 18 *show airgroup internal-state statistics*

Column	Description
PAPI Messages	Statistics of Performance Application Programming Interface (PAPI) messages between mDNS and other processes.
RADIUS Client Messages	Statistics of RADIUS messages sent and received by AirGroup.
Sibyte Messages	Statistics of mDNS messages sent and received from the datapath.
Internal Statistics	Statistics about the number of mDNS response and query messages received and the time taken to process each of these messages.
Multi-controller Cluster Messages	Statistics about the mDNS query and response messages among controllers in a multi-controller cluster.

Viewing AirGroup VLANs

```
# show airgroup vlan
VLAN Table
----------
Vlan-Id  IP-Address
-------  ----------
1        10.17.72.1
2        2.2.2.2
3        3.3.3.3
default  169.254.53.53
```

To view the description of the column headings, see Table 6 on page 24.

Viewing AirGroup Server Status

```
# show airgroup servers
AirGroup Servers
MAC                IP             Host Name       Service  VLAN  Wired/Wireless
---                --             ---------       -------  ----  --------------
00:11:22:33:44:13  10.15.122.172  MDNSDevice-190  airplay  122   N/A
00:11:22:33:44:b4  10.15.122.77   MDNSDevice-095  airplay  122   N/A
00:11:22:33:44:cb  10.15.122.100  MDNSDevice-118  airplay  122   N/A

Role  Username  AP-Name  query-rec-dropped  query-rec-filtered  query-rec-responded
----  --------  -------  -----------------  ------------------  -------------------
                         0                  0                   0
                         0                  0                   0
                         0                  0                   0

last-query
----------

Num Servers:3
```

The output of this command includes the following information:

Table 19 *show airgroup servers*

Column	Description
MAC	Displays the MAC address of the AirGroup server.
IP	Displays the IP address of the AirGroup server.
Host Name	Displays the hostname of the AirGroup server.
Service	Displays the AirGroup service hosted by the server.
VLAN	Displays the VLAN ID of the AirGroup server.
Wire/Wireless	Indicates if the AirGroup server is connected to a Wired LAN or Wireless LAN. **NOTE:** The column displays **Wired** when the server is connected to an untrusted wired port. When the server is connected to a trusted wired port, the column displays it as **N/A**.
Role	Displays the user role of the AirGroup server.
Username	Displays the user name of the AirGroup server.
AP-Name	Displays the AP name to which the AirGroup server is connected.
query-rec-dropped	Number of mDNS queries dropped from the AirGroup server.
query-rec-filtered	Number of mDNS queries filtered as a result of the policies.
query-rec-responded	Number of mDNS queries responded from the AirGroup server.
last-query	Time stamp of the last query received.

Viewing AirGroup Users

```
# show airgroup users
AirGroup Users
```

```
--------------
MAC                IP             Host Name   VLAN  Role  Username  AP-Name
---                --             ---------   ----  ----  --------  -------
00:11:22:33:44:63  10.15.122.252              122
f0:de:f1:0e:c6:31  10.15.122.245              122
00:11:22:33:44:de  10.15.122.119              122

query-rec-dropped  query-rec-filtered  query-rec-responded  last-query
-----------------  ------------------  -------------------  ----------
0                  0                   0                    Sun Feb 10 23:10:08 2013
2014               2014                201400               Sun Feb 10 23:37:48 2013
0                  0                   0                    Wed Dec 31 16:00:00 1969

Num Users:3
```

The output of this command includes the following information:

Table 20 *show airgroup users*

Column	Description
MAC	Displays the MAC address of the AirGroup user.
IP	Displays the IP address of the AirGroup user.
Host Name	Displays the hostname of the AirGroup user.
VLAN	Displays the VLAN ID of the AirGroup user.
Role	Displays the user role of the AirGroup user.
Username	Displays the user name of the AirGroup user.
AP-Name	Displays the AP name to which the AirGroup user is connected.
query-rec-dropped	Number of mDNS queries dropped from the AirGroup user.
query-rec-filtered	Number of mDNS queries filtered as a result of the policies.
query-rec-responded	Number of mDNS queries responded from the AirGroup user.
last-query	Time stamp of the last query received.

Viewing Service Queries Blocked by AirGroup

This command displays the service ID which were queried but not available in the AirGroup service table.

```
(host) #show airgroup blocked-queries
AirGroup dropped Query IDs
--------------------------
Service ID                                                          #query-hits
----------                                                          -----------
_smb._tcp                                                           545
_adisk._tcp                                                         545
_airport._tcp                                                       545
_touch-remote._tcp                                                  1102
_00000000-54ce-c0a7-a21f-369c70ae4de6._sub._home-sharing._tcp       1125
_00000000-54ce-c0a7-a21f-369c70ae4de6._sub._hs-dpap._tcp            906
6.d.8.7.7.9.e.f.f.f.3.f.0.4.2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa  2
_osxsvr._tcp                                                        4
```

```
a.c.e.3.a.1.e.f.f.f.7.4.8.f.2.e.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa  1
Num dropped Query IDs:9
```

The output of this command includes the following information:

Table 21 *show airgroup blocked-queries*

Column	Description
`Service ID`	An AirGroup service ID is the name of a Bonjour service offered by a Bonjour-enabled device or application.
`#query-hits`	Displays the number of mDNS query hits for a service blocked by AirGroup.

Viewing Blocked Services

The **airgroup service <servicename> disable** command blocks an AirGroup service by blocking the service IDs for that service. When an AirGroup service is enabled, service IDs of that service are enabled automatically. To view the list of blocked services, use the **show airgroup blocked-service-id** command.

```
(host) #show airgroup blocked-service-id
AirGroup Blocked Service IDs
----------------------------
Origin      Service ID            #response-hits
------      ----------            --------------
2.2.2.254   _colorPrinter._udp    5

Num Blocked Service-ID:1
```

The output of this command includes the following information:

Table 22 *show airgroup blocked-service-id*

Column	Description
`Origin`	Source IP address of the AirGroup server which advertises this service.
`Service ID`	An AirGroup service ID is the name of a Bonjour service offered by a Bonjour-enabled device or application.
`#response-hits`	Number of mDNS response messages received for this service ID.

AirGroup Global Tokens

In an AirGroup network, AirGroup devices generate excess mDNS query and response packets. Using **airgroup global-credits** command, the AirGroup controller restricts these packets by assigning tokens. The controller processes these mDNS packets based on this token value. The controller rejects any packets beyond this token limit. The token renews every 15 seconds. The renewal time is not a configurable parameter.

In the following example, the AirGroup controller restricts the number of query packets to 151 and response packets to 25 from AirGroup devices in a time frame of 15 seconds.

```
(host) #airgroup global-credits 151 25
```

The following command displays tokens assigned to query and response packets. It displays configured and current global tokens.

```
(host) #show airgroup global-credits
Global Credits - Default
------------------------
```

```
Type              Value
----              -----
Query Packets     151
Response Packets  25

Global Credits - Current
------------------------
Type              Value
----              -----
Query Packets     145
Response Packets  16
```

The output of this command includes the following information:

Table 23 *show airgroup global-credits*

Column	Description
`Type`	Displays the mDNS packet type.
`Value`	Displays the limit of the token.

Consider the best practices and limitations in this chapter before proceeding with your AirGroup deployment. Any recommendation that is not specific to any deployment model applies to both overlay and integrated deployments.

Firewall Configuration Changes

Best practices recommend the following firewall settings.

Disable Inter-User Firewall Settings

Some firewall settings can prevent untrusted clients from communicating with each other. When these settings are enabled, an untrusted client such as an iPad may not be able to send its image to an Apple TV on the same controller.

Use the following commands to disable the virtual AP global firewall options, and allow Bonjour services to use the AirGroup feature.

- `firewall deny-inter-user-bridging`
- `firewall deny-inter-user-traffic`
- `ipv6 firewall deny-inter-user-bridging`

ValidUser ACL Configuration

The **ValidUser** Access Control list (ACL) must allow mDNS packets with the source IP as a link local address. Do not use a validUser ACL if the user VLAN interfaces of the AirGroup controller are not configured with an IP address.

Allow GRE and UDP 5353

mDNS discovery uses the predefined port **UDP 5353**. If there is a firewall between the AirGroup controller and WLAN controller, ensure that your firewall policies allow GRE and UDP 5353.

Recommended Ports

The ArubaOS role-based access controls for wireless clients use ACLs to allow or deny user traffic on specific ports. Even though mDNS discovery uses the predefined port UDP 5353, application-specific traffic for services like AirPlay may use dynamically selected port numbers. Best practices are to add or modify ACLs to allow traffic on the ports described in Table 24 and Table 25.

NOTE

AirPlay operates using dynamic ports, but printing protocols like AirPrint use fixed ports.

Ports for AirPlay Service

Enable the following ports for the AirPlay service.

Table 24 *Ports for AirPlay Service*

Protocol	Ports
TCP	• 5000 • 7000 • 7100 • 8612 • 49152-65535
UDP	• 7010 • 7011 • 8612 • 49152-65535

Ports for AirPrint Service

Enable the ports in Table 25 to allow AirGroup devices to access AirPrint services.

Table 25 *Ports for AirPrint Service*

Protocol	Print Service	Port
TCP	Datastream	9100
TCP	IPP	631
TCP	HTTP	80
TCP	Scanner	9500
TCP	HTTP-ALT	8080

AirGroup Services for Large Deployments

By default, all Bonjour services are enabled in AirGroup. Large deployments with many wireless and wired users often support a large number of advertised Bonjour services, which can consume a significant amount of system resources. For large scale deployments, best practices to specifically enable the AirPlay and AirPrint services, then disable the **allowall** service and block all other Bonjour services. See Chapter 2, "Integrated Deployment Model" on page 19 for the full list of AirGroup configuration options.

Recommendations for Deploying an Overlay Model

If you are deploying AirGroup in a master-local topology with multiple local controllers that share the same user VLANs, best practices are to use AirGroup in overlay mode on a separate controller. See Chapter 3, "Overlay Deployment Model" on page 33 for a full list of configuration options.

If your deployment uses a dedicated AirGroup overlay controller:

- Do not terminate any user (wired or wireless) VLANs on the AirGroup overlay controller.
- Ensure that only the mDNS traffic from the user VLANs are tunneled to the AirGroup overlay controller.

- Disable the BC/MC optimization in your WLAN access controller. If you do not disable this feature, it blocks multicast traffic on the VLAN and mDNS packets cannot be redirected to the overlay controller. After BC/MC optimization is disabled, configure broadcast controls on a virtual AP to restrict multicasts to the wired network and so wired devices like Apple TVs and AirPrint printers can continue to be served by AirGroup. In the virtual-ap profile, enable the **broadcast-filter-all** and **broadcast-filter-arp** options. For more information on disabling BC/MC optimization refer to step 5 on page 34.

Limitations of Deploying Overlay Model

The overlay controller does not maintain context about devices. In this deployment model, the controller is not aware of a device's user name, user role, or the location of the AP to which the device is attached. This limits the rich policy enforcement framework that AirGroup provides in conjunction with CPPM-based device registration. If Policy control is essential, best practices is to use the integrated deployment model.

AirGroup Scalability Limits

Table 26 displays the total number of AirGroup servers (Apple TV, AirPrint Printer) and iPad users supported in individual controllers:

Table 26 *AirGroup Server and User Limits in Controllers*

	Aruba 3200	Aruba 3400	Aruba 3600	M3
Number of AirGroup servers	500	1000	2000	2000
Number of AirGroup users	1500	3000	6000	6000

NOTE

In a multi-controller deployment, there is a scaling limit of 2000 AirGroup servers and 6000 AirGroup users for all controllers in a cluster. If you require more servers and users than the prescribed limit, configure multiple clusters so that each cluster is within the prescribed limit.

The scaling limits on ArubaOS 6.1.3.6-AirGroup is measured based on the following metrics:

- Memory Utilization
- CPU Utilization

Memory Utilization

The memory utilization is affected by the number of AirGroup servers and users in an AirGroup cluster. In an AirGroup cluster, the total number of AirGroup servers and users cannot exceed the limit defined by the top-end controller. For example, in an AirGroup cluster of one Aruba 3200 controller and two M3 controllers, the cluster limit is determined as per the scaling limit of the top-end controller which is the M3 controller. For the Aruba 3200 controller in the cluster, the controller platform limit of the Aruba 3200 controller is applied. Based on the memory utilization, Table 26 summarizes the maximum number of AirGroup servers and users for all supported controller platforms.

CPU Utilization

The CPU utilization can be measured by the rate at which the controller receives mDNS packets. The rate of mDNS packets in the cluster depends on the number of AirGroup servers, users, and number of applications installed on these devices. The rate of mDNS packets handled by supported controller platform varies. Table 27 displays the total number of mDNS packets received per second by supported controller platforms:

Table 27 *mDNS Packet Limits in Controllers*

	Aruba 3200	Aruba 3400	Aruba 3600	M3
mDNS packets per second (pps)	10	10	20	20

Use the following command to determine the number of mDNS packets received per second by the controller:

```
show airgroup internal-state statistics
```

NOTE

Issue this command multiple times to measure the time difference and the mDNS packet count.

General AirGroup Limitations

The AirGroup feature has the following limitations:

- AirGroup is supported only in tunnel and decrypt-tunnel forwarding modes.
- If you use ClearPass Policy Manager to define AirGroup users, shared user and role lists and location attributes cannot exceed 240 characters:
- The RTSP protocol does not support AirPlay on an Apple TV receiver if you enable NAT on the user VLAN interface.
- The location-based access feature only supports AP FQLNs (Fully Qualified Location Names) configured in the format `<ap name>.floor <number>.<building>.<campus>`. AP names cannot contain periods.