aruba
a Hewlett Packard
Enterprise company

AirGroup Service

Version 2.2

Authors:
Chris Peacock
Lance Bockenstedt

Deployment Guide

Copyright Information

Open Source Code

aruba
a Hewlett Packard
Enterprise company
www.arubanetworks.com
3333 Scott Blvd
Santa Clara, CA 95054
Phone: 1-800-WIFI-LAN (+800-943-4526)
Fax 408.227.4550

Contents

Revision History

The following table lists the revisions of this document:

Revision	Date	Change Description
2.0.0		Initial Publication
2.0.1	May 27, 2019	Document Updates
2.1	Nov 5, 2019	Best Practices/Design Updates
2.2	May 4, 2020	Bug List Added/Design Updates

Table 1 *Revision History*

AirGroup Overview

AirGroup is an Enterprise class Zero-Configuration-Networking for Bonjour , Digital Living Network Alliance (DLNA) services, and Simple Service Discovery Protocol (SSDP). AirGroup provides context-awareness of services across network and is supported in tunnel and decrypt-tunnel forwarding modes.

AirGroup supports both wired and wireless devices and employs ClearPass Policy Manager for device registration and sharing policies. The following preconfigured services are supported:

- AirPlay (used by iOS devices to stream to Apple TV)
- AirPrint (used by iOS devices to print to compatible printers)
- Amazon TV
- DIAL (used by streaming devices like Google Chromecast, Roku, Amazon Fire TV)
- DLNA Media (used by applications like Windows Media Player)
- DLNA Print (used by DLNA compatible printers)
- GoogleCast (used by Google Chromecast)
- iTunes (used by Apple devices)
- RemoteMgmt (used by Apple devices)
- Sharing (used by Apple devices)

When AirGroup is enabled upon start-up or mDNS process restart, MD/AirGroup controller sends out multicast mDNS query packets across all VLANs in order to learn about the services offered on the network.

Based on the mDNS responses received from different servers, AirGroup maintains a cache table listing all the servers and corresponding services learned on the network.

The following features will occur when AirGroup is enabled and the controller is properly configured:

- Suppresses all mDNS responses (Broadcast Filter All required)
- Controller CPPM interaction
- Device visibility queries from controller/IAP: The controller/IAP periodically sends RADIUS messages to CPPM with the MAC address of an AirGroup user and receives AirGroup-specific information pertaining to that MAC address, such as device owner and shared locations, users and roles.
- Asynchronous information updates from CPPM: Whenever AirGroup-specific information related to a MAC address changes, CPPM sends a RADIUS CoA (Change of Authorization) request to the controller to notify it of the changes.

- With Mobility Master, ClearPass sends the RADIUS CoA request to the Mobility Master, which then sends the update to the Managed Device.

Deployment Use Cases

AirGroup Service is often used for VLAN based service filtering: mDNS and SSDP services can be filtered per VLAN.

By default, all services are visible across all VLANs

Services can be filtered per user role

- Filtering with roles can be applied for both servers and users separately

Services can be filtered based on user Group (defined in AD, others)

Registration of personal devices on the network:

- An AirGroup operator (end user) can register his/her devices for personal use
- Enabling sharing of devices with a user or a group of users
- Location based sharing by AP-name

AirGroup Features in ArubaOS 8

- AirGroup changes in ArubaOS 8.2 onward:
- Define more than one hop for ap-name based location policy
- Distributed mode support
- Support for disallowed named VLAN policy for users and servers
- Extension of support for disallowed VLAN policy for users in addition to servers
- Extension of support for disallowed role policy for servers in addition to users
- Enhanced visibility of servers, users, traffic trend, and bandwidth utilization in Dashboard
- Support for wired users
- AirGroup Islands

AirGroup Features Deprecated with ArubaOS 8 from ArubaOS 6

- Domain is no longer supported in Mobility Master-Managed Device topology.
  - NOTE: Domain is supported in 7200 Series Master Controller Mode and standalone controller topology.
- Global credits mechanism is removed.
- Active wireless discovery mechanism is removed.
- Location discovery parameter is deprecated.
- mDNS Multicast Response Propagation

AirGroup Server/User roles

- AirGroup classifies all mDNS/SSDP devices as either AirGroup servers, AirGroup users or both
- Servers are devices which advertise at least one AirGroup service (Apple TV, Google Chrome Cast, Amazon Fire Stick) – Servers can be users / devices
- Users are devices which query for AirGroup services (MacBook, iOS Device, Android tablet, Amazon Fire Tablet/Stick)

Modes of Operation

See design section below on when and where to use each mode of operation

Centralized Mode

In Centralized mode, the AirGroup service runs on the Mobility Master. The Mobility Master-Managed Device deployment model supports Centralized mode, Distributed mode, or both.

Distributed Mode

In Distributed mode, the AirGroup service runs on the node (Mobility Controller) where an AirGroup profile is configured. The 7030 and 7200 Series Master Controller Mode deployment model or the standalone controller deployment model supports only the Distributed mode.

NOTE

With Distributed mode with MM, it is expected that you will NOT see AirGroup entries showing up on the MM from the CLI, they only show up on the MC, however they are present in the MM GUI.

AirGroup Deployment Models

Mobility Master-Managed Device

- Centralized/Distributed mode (and can be mixed with Mobility Master configuration)
  - This means at /MD/ArubaU you can define common AirGroup policy and options (ClearPass/VLAN’s to be excluded/Services
  - At /MD/ArubaU/SantaClara – you can set the mode to centralized
  - At /MD/ArubaU/Whitby – you can set the mode to distributed

Master Controller Mode (MCM) (Distributed mode)

Standalone Controller (Distributed mode)

You can mix and match deployment models which is referred to as Mixed Mode. While not a mode you can select from a configuration, you can have some controllers running in Distributed mode and some running in centralized mode.

Mobility Master Managed Devices

The Mobility Master is the root of a network hierarchy. A single Mobility Master oversees a number of managed devices that can be collocated or off campus. In the Mobility Master-managed deployment model, AirGroup configuration is allowed on the Mobility Master and Managed Device.

7030/7200 Series Master Controller Mode

ArubaOS 8.0.1.0 supports 7200 series controllers to run as a master controller. In the Master Controller Mode deployment model, AirGroup configuration is allowed on the managed devices (AOS 8 hierarchical configuration model) and device nodes (device nodes are located within managed devices), e.g. /md/ArubaU/SantaClara. However, server-based policy configuration is allowed only on device nodes. This deployment model does not support Centralized AirGroup dashboard.

Standalone Controller

AirGroup supports domains for standalone controllers. This feature, for example, allows iPad users on one standalone controller to discover an Apple TV available on another standalone controller, if both standalone controllers are part of the same domain. In standalone controller deployment model, all AirGroup configuration is allowed only on the managed device.

Scalability Limit in Standalone or Distributed Controller AOS 8

Standalone Controller Model	AOS 8.x AirGroup Servers	AOS 8.x AirGroup Users
7240	10000	20000
7220	7000	15000
7210	5000	10000
7205	2000	6000
7030	1000	3000
7024	600	1400
7010	500	1500
7005	300	700

mDNS Packet Limits in Standalone Controller or Distributed Mode

Standalone Controller Model or Distributed Mode	mDNS packets per second (pps)
Mobility Master – in Centralized Mode (10k)	1750
7280	150
7240	150
7220	90
7210	90
7205	60
7030	75
7024	75
7010	45
7005	45

NOTE

Note 1: This data is taken from the 8.4.0.0 User Guides

You can use the following command to determine the number of mDNS packets received per second on a Mobility Master or Instant Virtual Controller. Packets are processed on FIFO so no weight is placed on either a query or response.

show airgroup internal-state statistics

Below is a partial output of the command:

Opcode 193 is a cumulative number of messages processed which is broken out into request and response just below. To calculate PPS, run the command several times in a row at a scheduled interval. You can then average requests over the period of time the command is run. For example:

Run every 5 seconds – divide opcode 193 by 5 (for 5 secs or whatever interval you select) each time to give you PPS and overage that number over the number of samples taken. You must cumulate all message types to accurately account for total PPS. MDNS & DLNA are shown below.

Note: This is an estimate of the PPS and depending on controller load some messages may be lost if the controller is running at or near capacity. Output from the dropped packets command is cumulative since the last time the stat was cleared. It is not representative of PPS being dropped but rather a total counter. If there are no packets dropped then the AirGroup process has never ran beyond PPS capacity since the last time the counter was cleared.

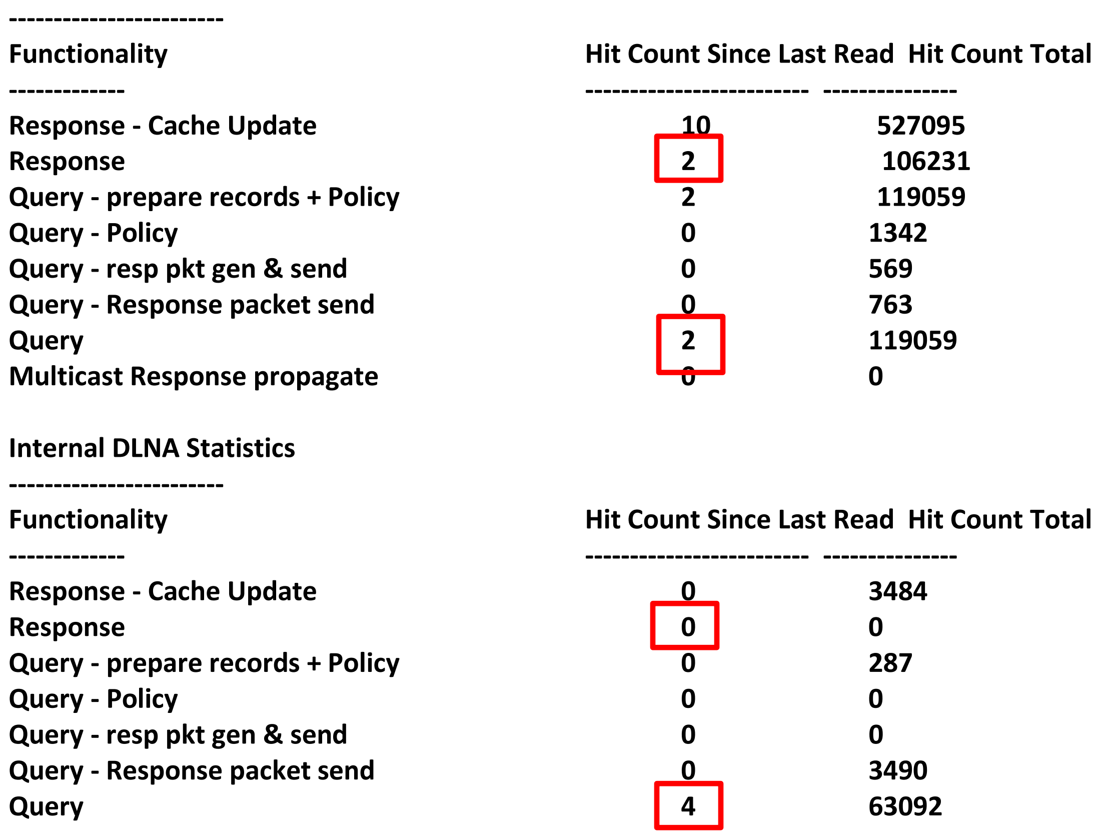
```
MDNS Messages
-------------
Opcode  Name                    Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
------  ----                    --------------------  ----------  --------------------  ----------
7       app                     0                     8           0                     0
193     N/A                     148                   1007        814                   4535
Rx      Request                 N/A                   N/A         301                   1852
Rx      Response                N/A                   N/A         513                   2663
Tx      Request-Refresh         72                    326         N/A                   N/A
Tx      Request-discovery       4                     130         N/A                   N/A
Tx      Request-wildcard        0                     0           N/A                   N/A
Tx      Response-Solicited      66                    377         N/A                   N/A
Tx      Response-Solicited-Fragment  6                173         N/A                   N/A
Tx      Response-Unsolicited    0                     0           N/A                   N/A
Tx/Rx   Total                   962                   0           N/A                   N/A


DLNA Messages
-------------
Opcode  Name             Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
------  ----             --------------------  ----------  --------------------  ----------
193     N/A              0                     2065        22                    7471
Rx      Query            N/A                   N/A         0                     795
Rx      Notify Announce  N/A                   N/A         22                    4315
Rx      Notify Bye       N/A                   N/A         0                     0
Tx      Response         0                     1889        N/A                   N/A

MDNS CPU and Throttling details
------------------------------
CPU Utilization      (%)  Throttling State         Description          Query Dropped  Resp Dropped
--------------------------  ----------------   -----------       ----------------  ----------------
0.02(3)              MDNS_NO_THROTTLING        No packets dropped   0              0
```

NOTE: On IAP – you will need to add up the query and response counters and average them manually. There is not a cumulative counter.

Internal MDNS Statistics



```
-----------------------
Functionality                                  Hit Count Since Last Read  Hit Count Total
-------------                                  -------------------------  ---------------
Response - Cache Update                         10                         527095
Response                                        2                          106231
Query - prepare records + Policy                2                          119059
Query - Policy                                  0                          1342
Query - resp pkt gen & send                     0                          569
Query - Response packet send                    0                          763
Query                                           2                          119059
Multicast Response propagate                    0                          0

Internal DLNA Statistics
-----------------------
Functionality                                  Hit Count Since Last Read  Hit Count Total
-------------                                  -------------------------  ---------------
Response - Cache Update                         0                          3484
Response                                        0                          0
Query - prepare records + Policy                0                          287
Query - Policy                                  0                          0
Query - resp pkt gen & send                     0                          0
Query - Response packet send                    0                          3490
Query                                           4                          63092
```

AirGroup Best Practices

Plan AirGroup Deployment (Centralized/Distributed/Scale)

- Scale – number of users, devices, severs, etc.
- Centralized – high speed campus
- Distributed – WAN link

Enable AirGroup service

Disabling the allowall service is recommended

- Create rules for just the applications you want including App IDs for Chromecast applications.

Monitor to see services in play

Filter services to those needed or desired

Auto associate ap-name doesn't apply for wired devices

- If you want to apply policies to wired devices, use MAC address-based policy with ClearPass or CLI

Custom services can also be created if needed

- The CLI of the controller will show what AirGroup services have been denied if you do not know what service is being used. **show airgroup blocked-service-id**

Auto-associate ap-name for wireless is mandatory for optimum performance

- When the AirGroup Server table is large, there can be significant delays while the Mobility Master responds to a client request. This problem is noticeable when the controller must cross reference every service with an AP-Group and forward an advertisement for that server. Limiting to AP-Name decreases the lookup time when the AirGroup Server table is large (more than 200 table entries)

Disallow all VLANs and Roles that do not need AirGroup Services

- This is done to prevent excessive load on the mDNS process and limit the number of servers and users the system must manage

AirGroup Islands do not support roaming servers or clients

- AirGroup Islands are designed to prevent connectivity and management between two or more Islands. This is different than AirGroup Domains that have been deprecated in Centralize/Distributed deployments with Mobility Master.

Wired servers are required to be on a VLAN that the controller or controllers (cluster) has an L2 connection to. See Wired AirGroup Server section below

- Do not share the wired Server VLAN across multiple clusters

Wired servers cannot be seen by more than 1 cluster

- Do not share the wired Server VLAN across multiple clusters

ClearPass Policy Manager is required in deployments with greater than 50 wired servers. This is because we must limit the number of AirGroup Server responses a client receives and ClearPass Policy Manager is the tool to use to limit the number of AirGroup Services a client is presented.

Chromecast Best Practices

Chromecast devices have some unique requirements in later versions of code. Due to Chromecast not responding to queries from devices that are not in the same subnet as the device, we must use the controller or mobility master to assist. No single version or device has been identified or the specific scenarios where this is triggered is known. However, when devices refuse connections from other subnets there are a few options that are listed below.

Distributed mode:

- IP address must be configured on the MD in the same VLAN as the device

Centralized mode:

- Option 1: Same as distributed mode where ap IP address is needed on the MD in the same VLAN as the Chromecast device.
- Option 2: A common VLAN/IP can be configured on the MM that the MD can use to aid in the process.

➢ NOTE: Option 2 is only a configuration optimization that is allowed in the hierarchy. Each controller must have an IP in the VLAN where the device exists. This feature is only to have less configuration on each MD but the same process still applies weather you use options 1 or 2 in centralized mode.

➢ NOTE: Chromecast does not function with a publicly addressable IPV4 address. There is not known way to make this work and it is not an issue with AirGroup.

Wired AirGroup Servers

Wired AirGroup Servers are supported with the following restrictions:

Wired AirGroup VLAN must not be seen by more than 1 cluster

- Each cluster should have it's own wired VLAN for AirGroup Servers that it is L2 adjacent to. See figure below

When using wired AirGroup Servers in a cluster, all cluster members will see the multicast packets to and from the device. Each cluster member will process or forward the packet to the Mobility Master for processing. This will have a performance and scale impact as the controllers or Mobility Master will need to process duplicate packets

The AP Multicast Aggregator can be configured in the AP System Profile. The purpose of this feature is to have the AP capture mDNS advertisements and forward them to the controller.

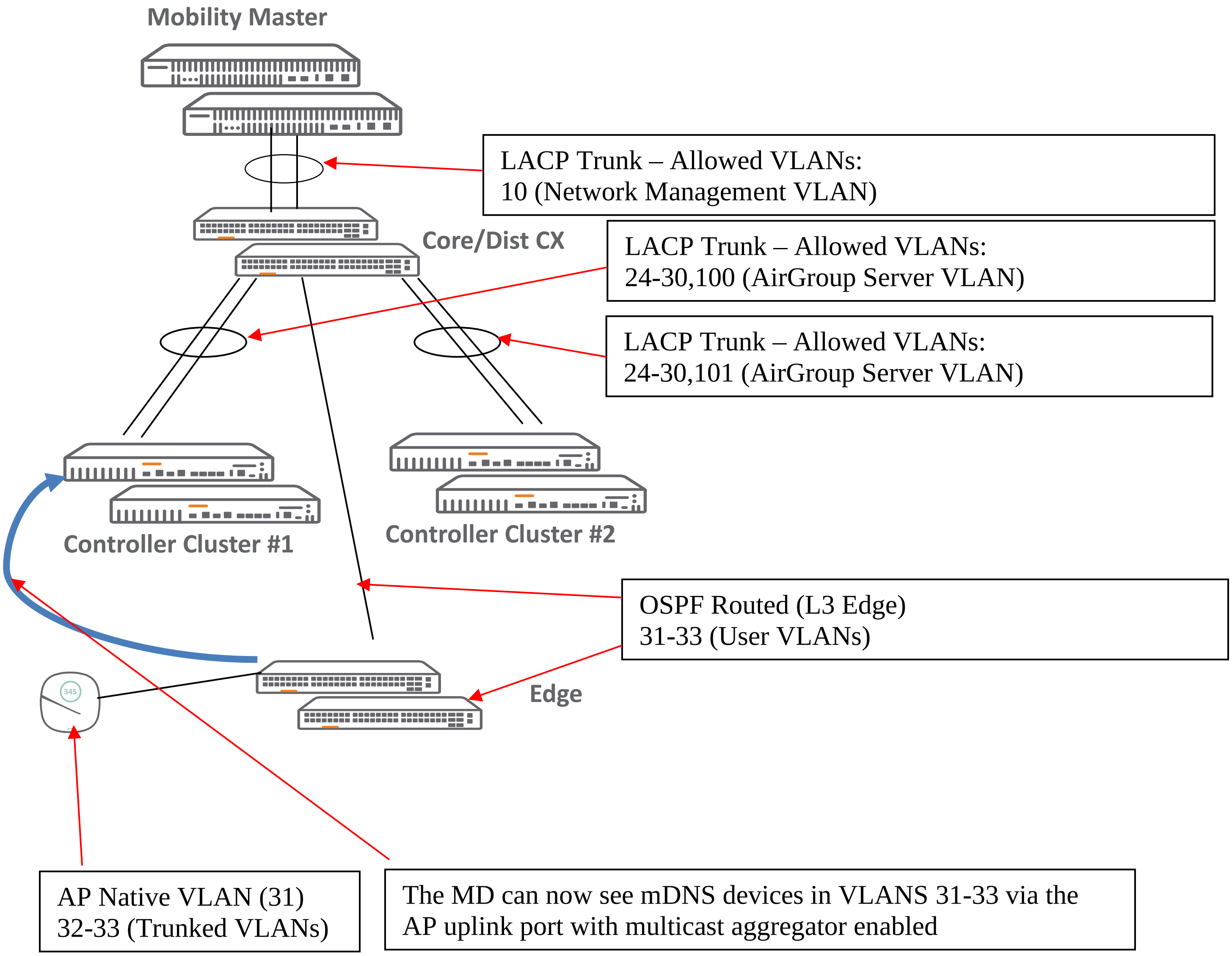
Can be configured to forward mDNS packets from the native VLAN or a Trunked VLAN

1 AP on the L2 network being Aggregated is elected to perform this operation

- Example: If you have 20 Aps configured the same L2 networks only 1 AP will be elected to forward the mDNS packets. If that AP goes offline a new device will be elected. We do not duplicate the messages from every AP or to each controller in a cluster.

Designed to detect AirGroup capable services on wired VLANs that the MD or MM is not L2 adjacent to.

- See drawing below:



LACP Trunk – Allowed VLANs:
10 (Network Management VLAN)

LACP Trunk – Allowed VLANs:
24-30,100 (AirGroup Server VLAN)

LACP Trunk – Allowed VLANs:
24-30,101 (AirGroup Server VLAN)

OSPF Routed (L3 Edge)
31-33 (User VLANs)

AP Native VLAN (31)
32-33 (Trunked VLANs)

The MD can now see mDNS devices in VLANS 31-33 via the AP uplink port with multicast aggregator enabled

Scalability Limits

AirGroup scalability limits in ArubaOS8 are based on the following attributes:

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 standalone controller. For example, an AirGroup cluster of one 7005 standalone controller and two 7210 standalone controllers, the cluster limit is determined as per the scaling limit of the top-end standalone controller which is the 7210 standalone controller. For the 7005 standalone controller in the cluster, the platform limit of the 7005 standalone controller is applied.

CPU Utilization

The CPU utilization is measured by the rate at which a standalone controller receives mDNS packets per second. The rate of mDNS packets per second in the cluster depends on the number of AirGroup servers, users, and number of applications installed on these devices. When the number of mDNS packets per second exceeds the limit, AirGroup drops the additional packets.

Bluetooth-Based Discovery and AirGroup for Apple TV

Apple devices support Bluetooth-based device discovery mechanism, which allows an Apple device to discover an Apple TV that is within the Bluetooth range.

AirGroup supports only mDNS-based device discovery and does not support Bluetooth-based device discovery mechanism.

Apple TV Generation 3 and on if using wireless, will form an ad-hoc network between the client and the Apple TV, which will bypass the AirGroup services

- Ad-hoc can be disabled under the management profile for organized-owed Apple TV’s (AirPlay Security)
    - Apple School Manager
    - Apple Configurator 2 – 10.14 (Mojave) is required

NFC Discovery and AirGroup for Android

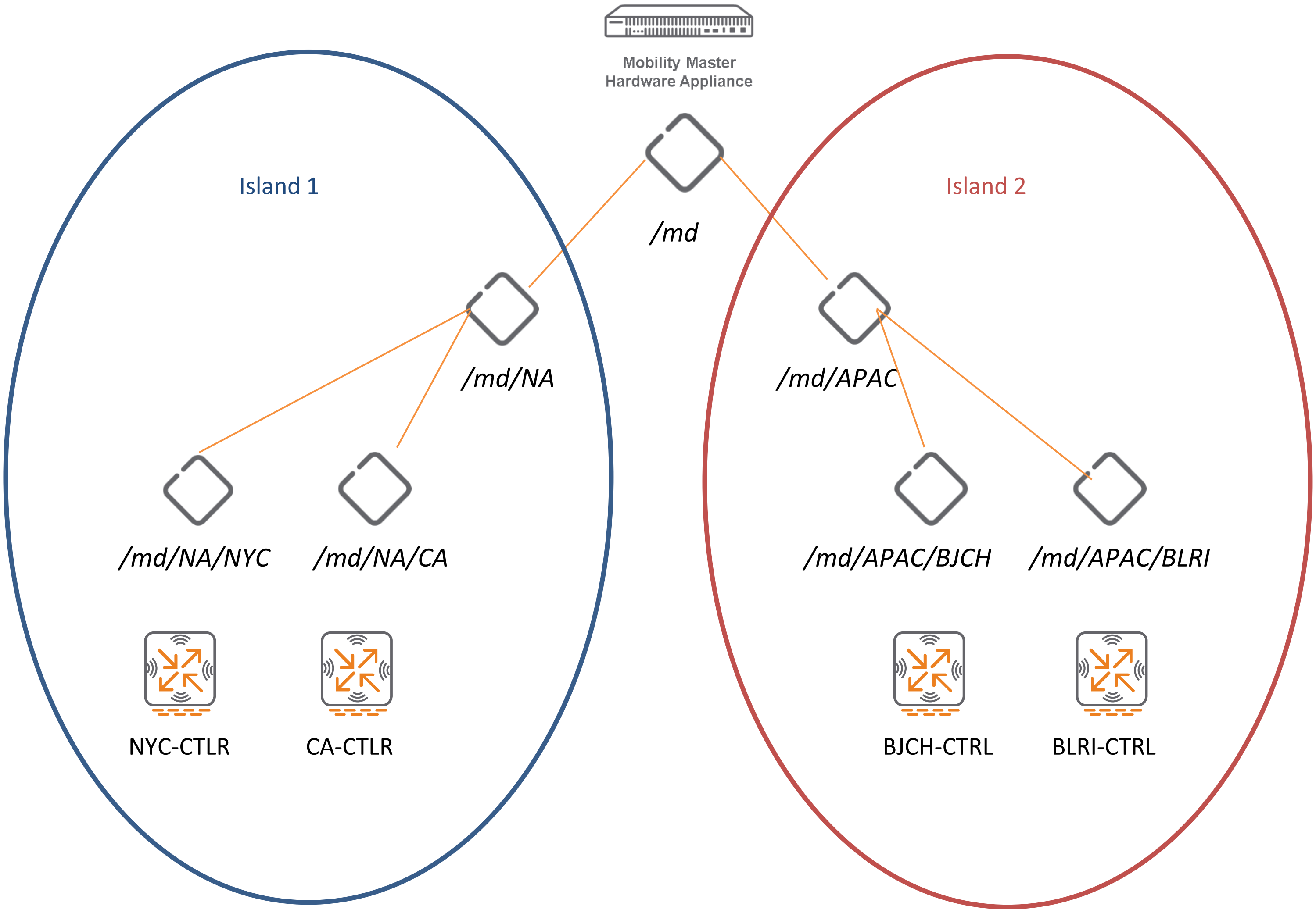
Newer Android devices which support NFC technology when within range of a Chromecast, device will bypass the wireless infrastructure and create peer to peer links.

AirGroup Islands

AirGroup Islands have been introduced to allow for areas of AirGroup management across regions

- Discovery will not work across Islands regardless of the mode AirGroup is running
- Roaming servers are not supported between Islands

Each Island is configured by a profile in the Mobility Master and applied to a group in the hierarchy



Deployment Models

Higher ED

Higher Ed deployments are very similar to those for large campus with the exception of device registration (recommended for Higher Ed customers). Higher ED customers will typically have far more devices that are not owned by IT or controlled by IT. Any of these can be changed based on individual requirements. It is highly recommended customers use these best practices:

- Use device registration with ClearPass
- Do not use AirGroup Islands. See AirGroup Islands
- Enable only the AirGroup Services that are in use (AirPrint, AirPlay, Chromecast, etc)
- Run AirGroup in centralized mode
- Use Multicast aggregator feature of the access point to bring AirGroup service advertisements back to the controller or have a controller L2 adjacent to the VLANs with AirGroup devices. See Wired AirGroup Servers section
- Design Mobility Masters to prevent or mitigate AirGroup services roaming between Mobility Master pairs

Large Campus

Large Campus is very similar to Higher Ed except we don't always need device registration. See below for a starting point of best practices. Any of these can be changed based on individual requirements. It is highly recommended customers use these best practices:

- Use AirGroup Islands to have different administrative domains and there are no roaming devices between Islands. See AirGroup Islands
- Enable only the AirGroup Services that are in use (AirPrint, AirPlay, Chromecast, etc)
- Run AirGroup in centralized mode
- Use Multicast aggregator feature of the access point to bring AirGroup service advertisements back to the controller or have a controller L2 adjacent to the VLANs with AirGroup devices. See Wired AirGroup Servers section

Distributed Enterprise

Distributed enterprise is a deployment like retail or many small offices. Any of these can be changed based on individual requirements. It is highly recommended customers use these best practices:

- Do not use AirGroup Islands. See AirGroup Islands
- Enable only the AirGroup Services that are in use (AirPrint, AirPlay, Chromecast, etc)
- Run AirGroup in distributed mode – single controller
- Deploy Controller so it is L2 adjacent to the AirGroup servers

Multi-National

Multi-National deployment typically have several Mobility Masters and many controllers in different countries / regulatory domains. Typically these deployments don't have devices that roam between domains and have different administrators. Any of these can be changed based on individual requirements. It is highly recommended customers use these best practices:

- Use AirGroup Islands to have different administrative domains and there are no roaming devices between Islands. See AirGroup Islands
- Enable only the AirGroup Services that are in use (AirPrint, AirPlay, Chromecast, etc)
- Run AirGroup in centralized mode
- Design Mobility Masters to prevent or mitigate AirGroup services roaming between Mobility Master pairs

Challenges with mDNS

Multicast DNS (mDNS) is a host name resolution service implemented by Apple as an alternative to the popular DNS service. It was primarily intended for local shared networks where devices could find each other without requiring additional infrastructure on the network such as a DNS server. In large universities and enterprise networks, it is common for Bonjour-capable (mDNS) 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.

As mDNS capable products such as iPods, iPads, iPhones and MacBooks started penetrating enterprise networks, they presented certain challenges:

In K-12 schools, universities and enterprise networks, it is common for mDNS devices to connect to the network across VLANs. As a result, an iPad on one VLAN cannot discover an Apple TV that resides on another VLAN because mDNS traffic in its native form is limited to a Layer 2 network and does not propagate across VLANs.

In most networks, broadcast and multicast traffic are usually filtered out from a WLAN to preserve the airtime and battery life. This limitation inhibits the performance of mDNS services because they rely on multicast traffic.

Even if broadcast/multicast traffic were allowed on the WLAN, they would present the following challenges:

- These devices create a significant amount of mDNS traffic thus increasing the load on the WLAN.
- When mDNS traffic is generated, all mDNS-capable devices on the WLAN need to wake up and process these frames, thus bringing down their battery life
- Other users on the same VLAN can discover personal devices, which might not be desirable.

The Solution: Aruba AirGroup

AirGroup is an Aruba solution that helps address the above issues as follows:

AirGroup maintains seamless connectivity between clients and services across VLANs and SSIDs.

Even if broadcast and multicast controls are enabled on an SSID, AirGroup creates special exceptions to send select mDNS traffic across the WLAN to learn about mDNS services.

AirGroup on a controller/IAP sends unicast mDNS responses to clients requesting mDNS services on the WLAN. Because there is no downstream multicast traffic on the WLAN, airtime and client battery life are significantly improved.

AirGroup on a controller has support of DLNA (Digital Living Network Alliance) devices. DLNA is a network standard that is derived from UPnP (Universal Plug and Play) in addition to the existing mDNS protocol. DLNA uses the Simple Service Discovery Protocol (SSDP) for service discovery on the network. DLNA provides the ability to share digital media between multimedia devices like Windows and Android, similar to how mDNS supports Zero Configuration Networking to Apple® devices and services.

You can also integrate AirGroup with the ClearPass to provide the following benefits:

Users can register their personal devices on the network such that they have exclusive access to these devices. They can also define a group of users who can share the registered devices.

Administrators can register and manage an organization’s shared devices, such as conference room printers or classroom Apple TVs. An administrator can grant global access to each device (for example, Apple TV access for both teachers and students), or restrict access according to the user name, role, or user location.

AirGroup is disabled by default with ArubaOS 8.x.

Use the following commands to disable the virtual AP global firewall options and allow mDNS/SSDP/DLNA services to use the AirGroup feature.

```
!
no firewall deny-inter-user-bridging
no firewall deny-inter-user-traffic
no ipv6 firewall deny-inter-user-bridging
!
```

- Valid User ACL configuration: The Valid User Access Control List (ACL) must allow mDNS packets with the source IP as a link local address. Do not use a valid User ACL if the user VLAN interfaces of the AirGroup controller are not configured with an IP address.
- Port recommendations: 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 as described below.

Ports for AirPlay Service	
Protocol	**Port**
TCP	554
TCP	5000
TCP	7000
TCP	7100
TCP	8612
TCP	49162-65535
UDP	554
UDP	7010
UDP	7011
UDP	8612
UDP	49512-65535

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

Ports for AirPrint Service		
Protocol	**Print Service**	**Port**
TCP	DataStream	9100
TCP	IPP	631
TCP	HTTP	80
TCP	Scanner	9500
TCP	HTTP-ALT	8080

Pre-Deployment Checklist for AirGroup

If you are considering deploying AirGroup in very large networks where thousands of AirGroup devices are expected to connect at any given time, two things need to be taken into consideration:

- **The expected number of AirGroup servers on the network** - For example, the 7xxx series controllers have a scaling limit of 2000 AirGroup servers per controller.
- **The rate of mDNS packet transactions observed on the controller** - If the number of AirGroup devices is expected to approach controller platform limits, it is important to determine the amount of AirGroup traffic passing the controller during peak network usage, as controllers are limited by the maximum number of mDNS packets they can process per second.

For details on AirGroup user/server scalability limits and mDNS packet rate limits on different controllers, please see the AirGroup Scalability Limits section.

Before enabling AirGroup on the network, ask the following questions:

How many controllers are present? If AirGroup functionality is required across controllers (i.e., an iPad on one controller being able to see and access an Apple TV on a different controller), then an AirGroup domain needs to be configured, if deployed without a Mobility Master or Master Controller Mode (Standalone Mode).

What does the campus topology look like? In a campus with multiple buildings, it may not be desired for AirGroup users in one building to see AirGroup services from a different building. This is not a problem if the topology is designed such that there is a single controller per building and no AirGroup domains are configured. In case of a single controller serving multiple buildings, APs in geographically separate buildings can be assigned to different AP Groups such that each building falls under a different AP Group. AirGroup servers can then be shared per AP Group(s).

For large networks:

What is the expected number of AirGroup servers and users on the network?

What services need to be enabled? It is recommended to start enabling only the most commonly used services such as AirPlay, AirPrint, etc. and disable the allowall service. Based on whether the number of AirGroup servers on the network reaches maximum platform capacity not, more AirGroup services can be enabled.

How many VLANs does the controller know? In a large network where thousands of AirGroup servers and users are expected, it is recommended to enable AirGroup on a select number of VLANs and then gradually enable more VLANs while simultaneously monitoring the size of the AirGroup server table and the mDNS packet rate per second. VLANs with wired AirGroup servers need to be trunked to the controller in order for the controller to discover services on these VLANs.

AirGroup Configuration for Aruba Instant

This section describes the configuration of AirGroup in an Instant network, along with optional ClearPass configuration for the following software versions:

8.3.x.x

8.4.x.x

The optional ClearPass configuration includes:

Adding the network device

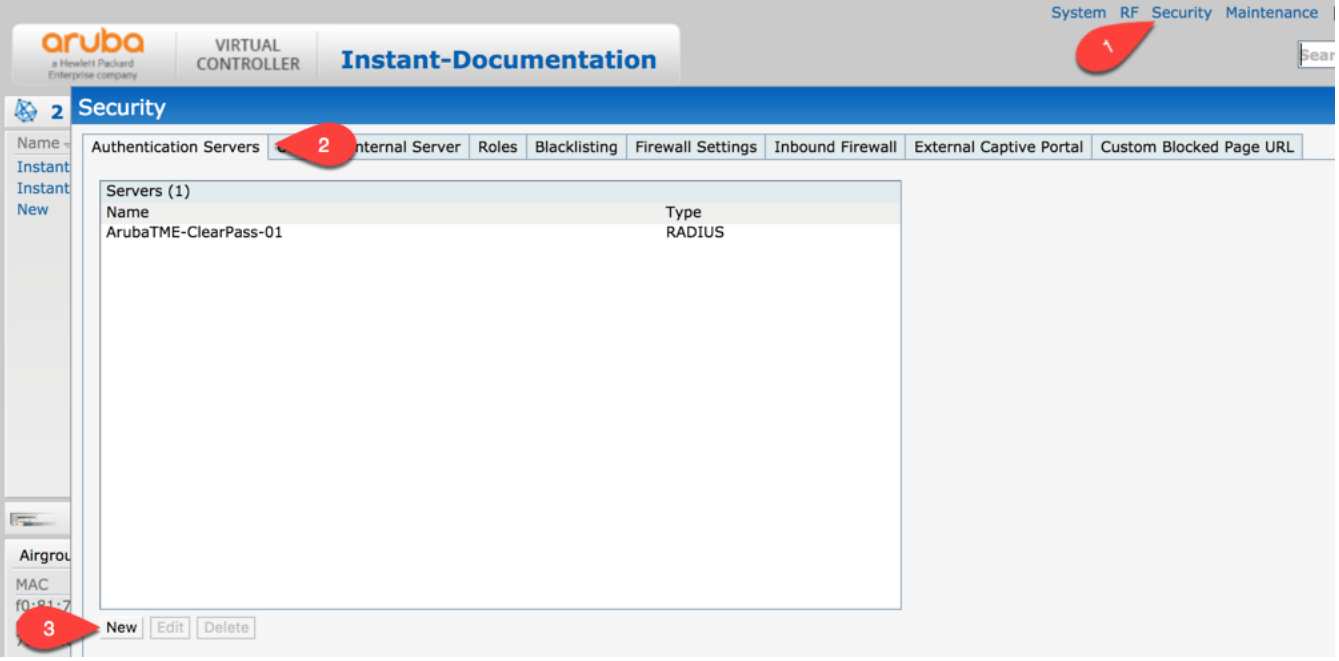
Adding the Virtual Controller to the AirGroup service on ClearPass Guest

AirGroup Instant 8.3.x.x

ClearPass (Optional)

Define the Authentication Server:

- Navigate to **Security**
- Select **Authentication Servers**
- Click **New**



Servers (1)

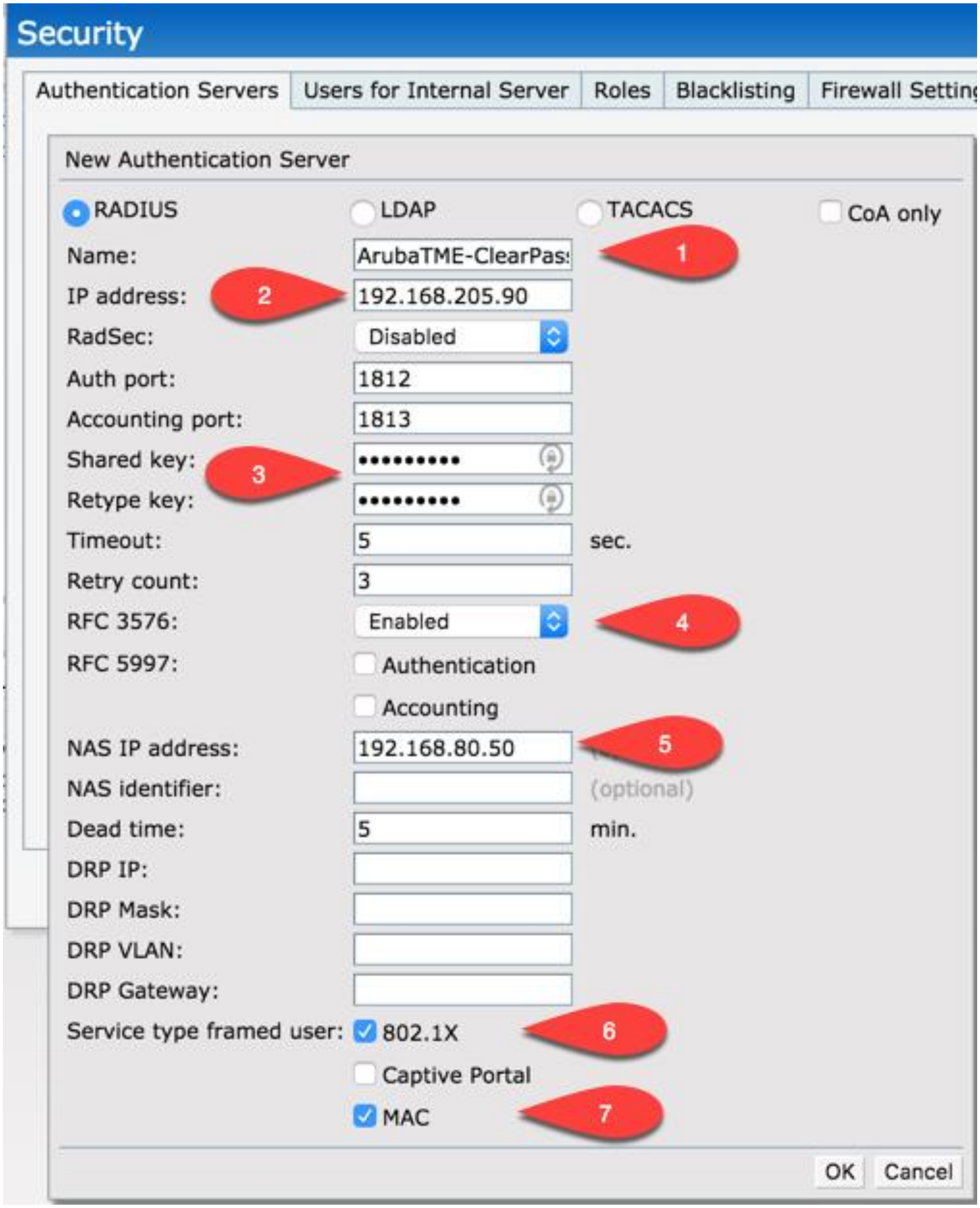
Name	Type
ArubaTME-ClearPass-01	RADIUS

Define the ClearPass Authentication Server:

- Provide a **Server name**
- Provide the **IP address** of the server
- Provide the **Shared Secret**
- Enable **RFC 3576**
- Provide **the NAS IP** address
  - In this example this is the IP of the Virtual Controller
- Select the **services** to be used for this server

- In this example this server is also being used for User Authentication (Dot1x) and for MAC Authentication (MAC Auth))

- Click on **Ok**



Security

Authentication Servers | Users for Internal Server | Roles | Blacklisting | Firewall Setting

New Authentication Server

● RADIUS ○ LDAP ○ TACACS □ CoA only

Name: ArubaTME-ClearPas:

IP address: 192.168.205.90

RadSec: Disabled

Auth port: 1812

Accounting port: 1813

Shared key: ••••••••••

Retype key: ••••••••••

Timeout: 5 sec.

Retry count: 3

RFC 3576: Enabled

RFC 5997: □ Authentication □ Accounting

NAS IP address: 192.168.80.50

NAS identifier: (optional)

Dead time: 5 min.

DRP IP:

DRP Mask:

DRP VLAN:

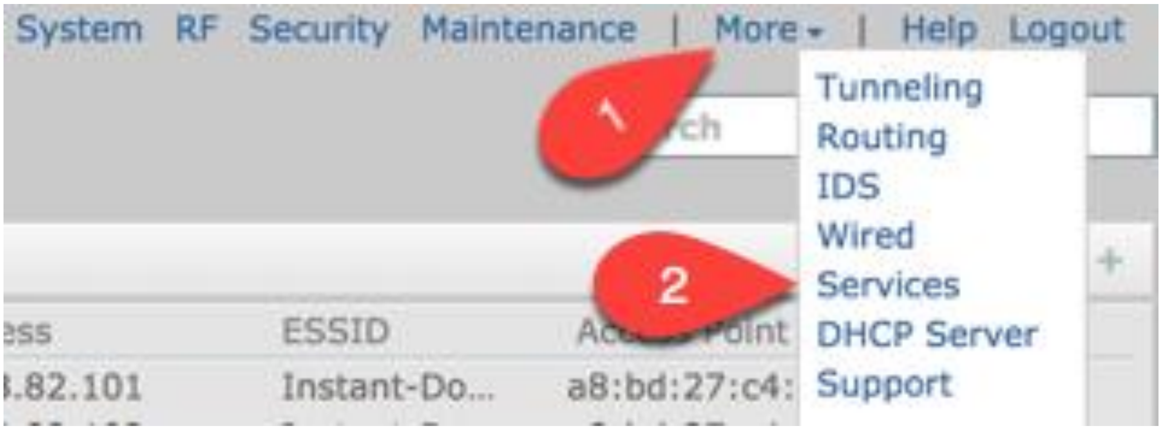
DRP Gateway:

Service type framed user: ☑ 802.1X □ Captive Portal ☑ MAC

AirGroup Service

Define the AirGroup Service:

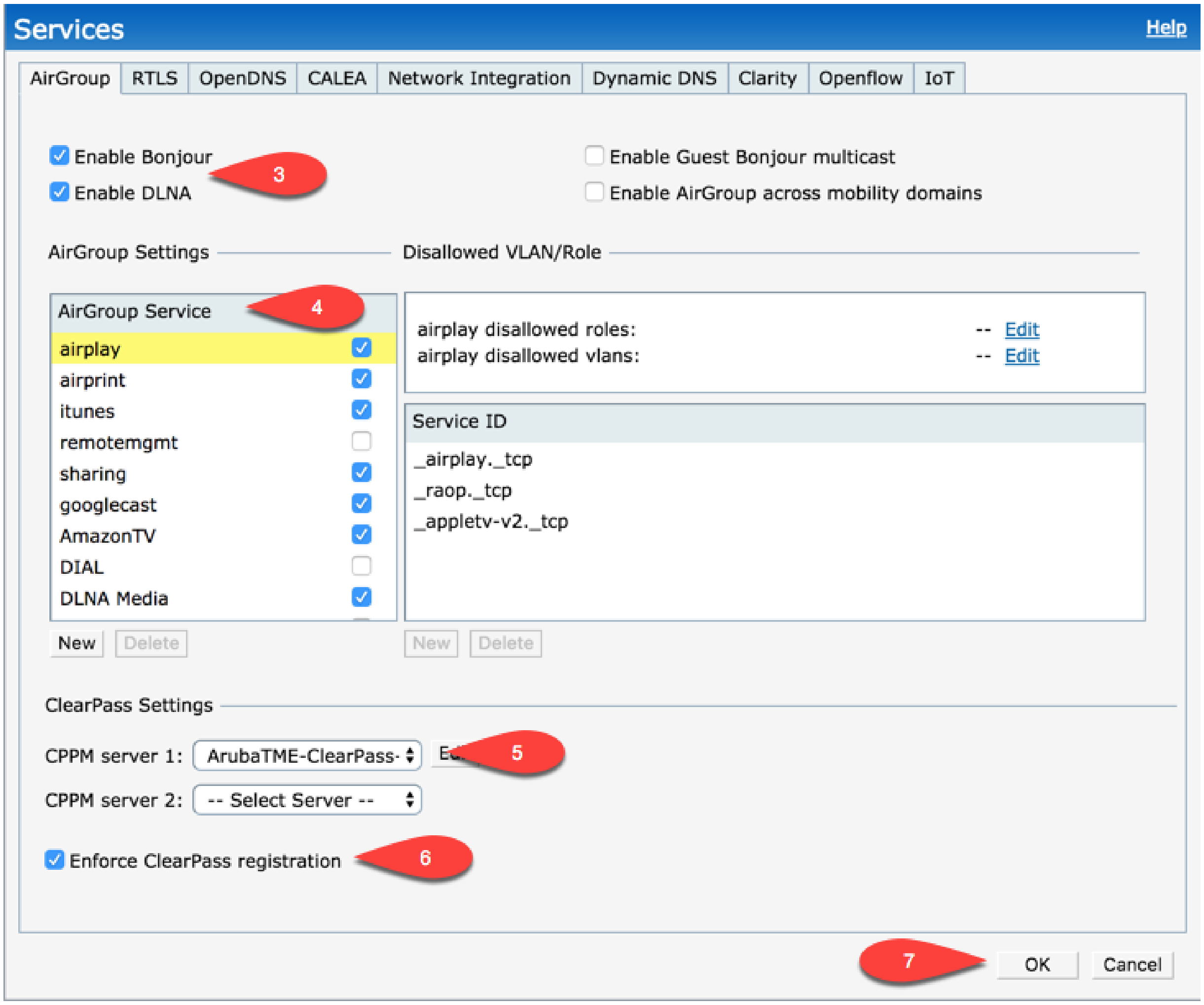
- Click on **More**
- Click on **Services**



The First tab you are presented with is AirGroup Service

Continued on the next page

- Choose the **Services** to enable
  - Bonjour
  - DLNA
- Choose the **AirGroup Service** under **Settings**
  - In this example the following services were enabled;
  - AirPlay/AirPrint/sharing/Googlecast/Amazon TV/DLNA Media
- Choose the **CPPM Server 1** (ClearPass) Settings
  - Choose the drop down and select the server which was created earlier
- If you wish to enforce AirGroup device Registration check the **Enforce ClearPass registration**
- Click **ok**



☑ Enable Bonjour
☑ Enable DLNA
□ Enable Guest Bonjour multicast
□ Enable AirGroup across mobility domains

AirGroup Settings

AirGroup Service	
airplay	☑
airprint	☑
itunes	☑
remotemgmt	□
sharing	☑
googlecast	☑
AmazonTV	☑
DIAL	□
DLNA Media	☑

Disallowed VLAN/Role

airplay disallowed roles: -- Edit
airplay disallowed vlans: -- Edit

Service ID
_airplay._tcp
_raop._tcp
_appletv-v2._tcp

ClearPass Settings

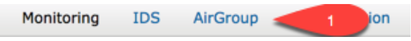
CPPM server 1: ArubaTME-ClearPass-
CPPM server 2: -- Select Server --

☑ Enforce ClearPass registration

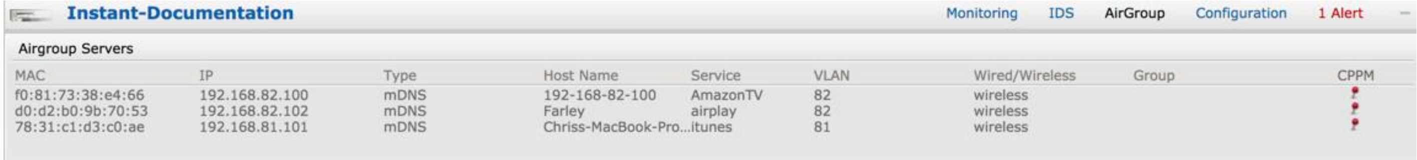
You have now defined the AirGroup Service, and as you start to connect devices you will see them showing up.

AirGroup Server Verification

1. Click on **AirGroup** on the line next to Monitoring



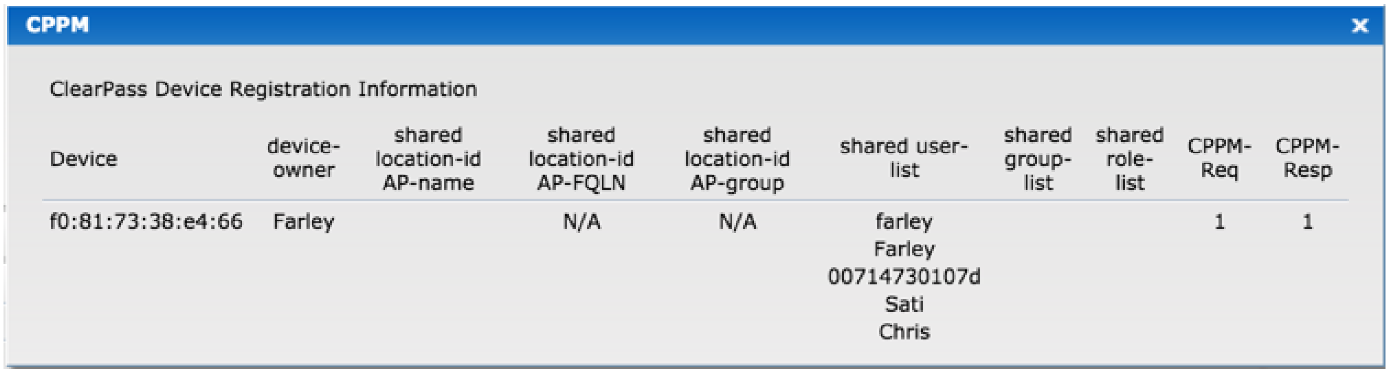
Here you can see the AirGroup servers listed



Airgroup Servers

MAC	IP	Type	Host Name	Service	VLAN	Wired/Wireless	Group	CPPM
f0:81:73:38:e4:66	192.168.82.100	mDNS	192-168-82-100	AmazonTV	82	wireless		📍
d0:d2:b0:9b:70:53	192.168.82.102	mDNS	Farley	airplay	82	wireless		📍
78:31:c1:d3:c0:ae	192.168.81.101	mDNS	Chriss-MacBook-Pro...	itunes	81	wireless		📍

Click on the pin under CPPM (ClearPass) you can see the shared user list from ClearPass begin returned.



ClearPass Device Registration Information

Device	device-owner	shared location-id AP-name	shared location-id AP-FQLN	shared location-id AP-group	shared user-list	shared group-list	shared role-list	CPPM-Req	CPPM-Resp
f0:81:73:38:e4:66	Farley		N/A	N/A	farley Farley 00714730107d Sati Chris			1	1

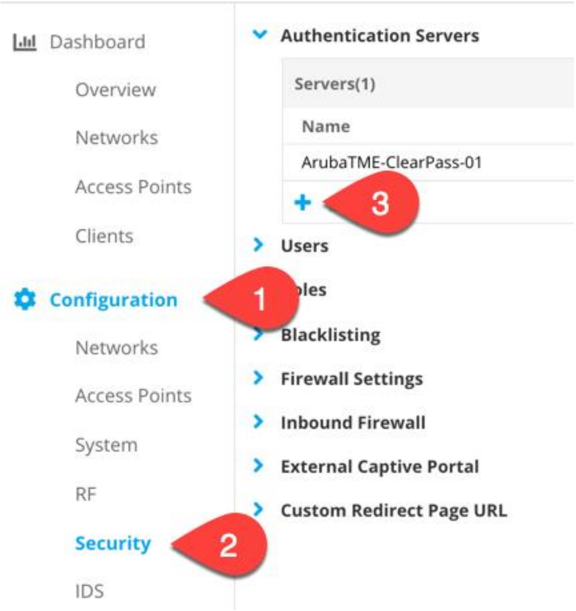
You can refer to the Verifying AirGroup Service for additional commands from the CLI for command outputs. These are consistent across Mobility Managed and Instant Deployments.

AirGroup Instant 8.4.x.x

ClearPass (Optional)

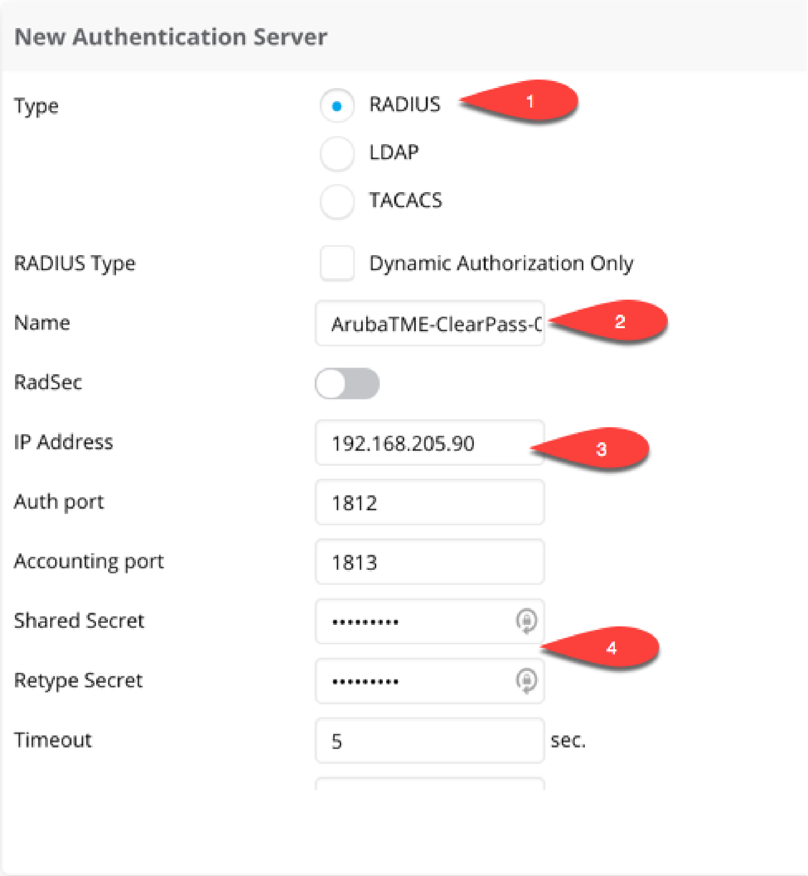
Define the Authentication Server:

1. Navigate to **Configuration**
2. Select **Security**
3. Click **plus** (+) sign



Define the ClearPass Authentication Server with Instant version 8.4.x.x:

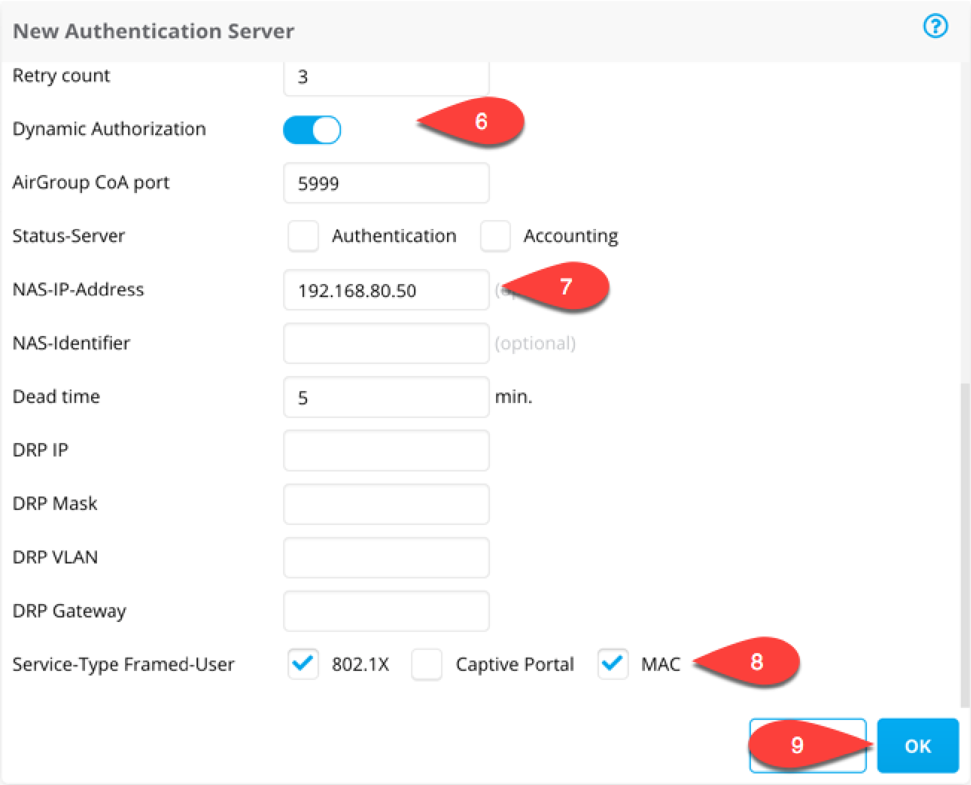
1. Choose **RADIUS**
2. Provide a **Server name**
3. Provide the **IP address** of the server
4. Provide the **Shared Secret**



New Authentication Server

Type	● RADIUS ○ LDAP ○ TACACS
RADIUS Type	□ Dynamic Authorization Only
Name	ArubaTME-ClearPass-C
RadSec	
IP Address	192.168.205.90
Auth port	1812
Accounting port	1813
Shared Secret	•••••••••
Retype Secret	•••••••••
Timeout	5 sec.

5. **Scroll the page down**



New Authentication Server

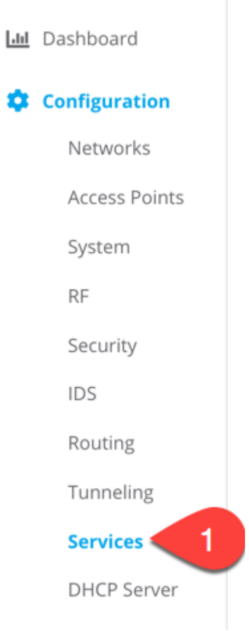
Retry count	3
Dynamic Authorization	●
AirGroup CoA port	5999
Status-Server	□ Authentication □ Accounting
NAS-IP-Address	192.168.80.50
NAS-Identifier	(optional)
Dead time	5 min.
DRP IP	
DRP Mask	
DRP VLAN	
DRP Gateway	
Service-Type Framed-User	☑ 802.1X □ Captive Portal ☑ MAC

6. Enable **Dynamic Authorization**
7. Provide the **NAS IP address**
   a. In this example this is the IP of the Virtual Controller
8. Select the services to be used for this server (**Service-Type Framed-User**)
   a. In this example this server is also being used for User Authentication (Dot1x) and for MAC Authentication (MAC Auth))
9. Click on **Ok**

AirGroup Service

Define the AirGroup service.

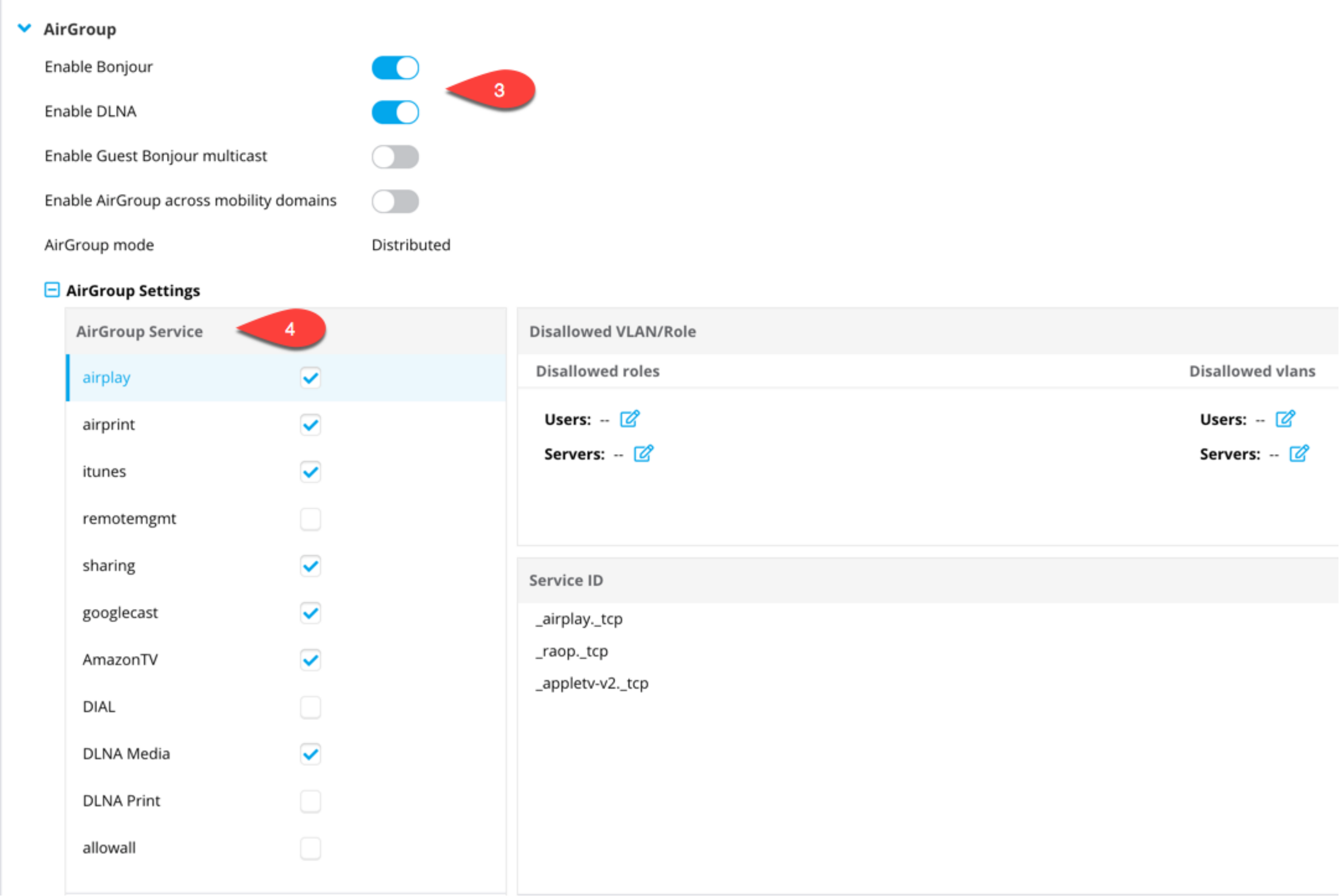
1. Under **Configuration**
2. Click on **Services**



The First tab you are presented with is AirGroup Service

Continued on the next page

3. Choose the Services to enable
    a. Bonjour
    b. DLNA
4. Choose the AirGroup Services under Settings
    a. In this example the following services were enabled;
        i. AirPlay/AirPrint/sharing/Googlecast/Amazon TV/DLNA Media



AirGroup

Enable Bonjour	On
Enable DLNA	On
Enable Guest Bonjour multicast	Off
Enable AirGroup across mobility domains	Off
AirGroup mode	Distributed

AirGroup Settings

AirGroup Service	
airplay	☑
airprint	☑
itunes	☑
remotemgmt	□
sharing	☑
googlecast	☑
AmazonTV	☑
DIAL	□
DLNA Media	☑
DLNA Print	□
allowall	□

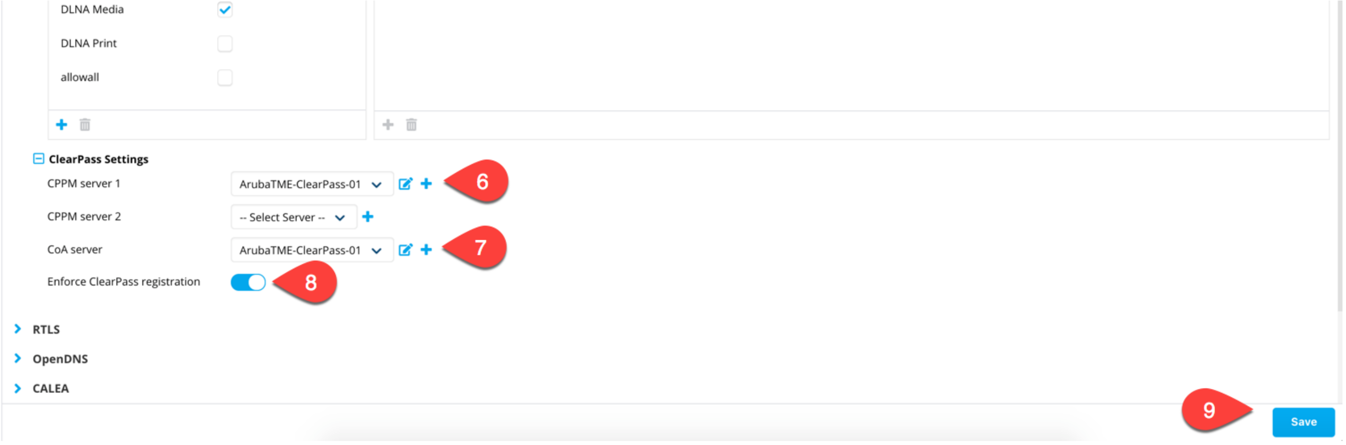
Disallowed VLAN/Role

Disallowed roles	Disallowed vlans
Users: --	Users: --
Servers: --	Servers: --

Service ID

_airplay._tcp
_raop._tcp
_appletv-v2._tcp

5. **Scroll the page down**
6. Choose the **CPPM Server 1** (ClearPass Server)
   a. Choose the drop down and select the server which was created earlier
7. Choose the **CoA Server**
   a. Choose the drop down and select the server which was created earlier
8. If you wish to enforce AirGroup device Registration check the **Enforce ClearPass registration**
9. Click **Save**



DLNA Media ☑

DLNA Print □

allowall □

ClearPass Settings

CPPM server 1: ArubaTME-ClearPass-01

CPPM server 2: -- Select Server --

CoA server: ArubaTME-ClearPass-01

Enforce ClearPass registration: on

RTLS

OpenDNS

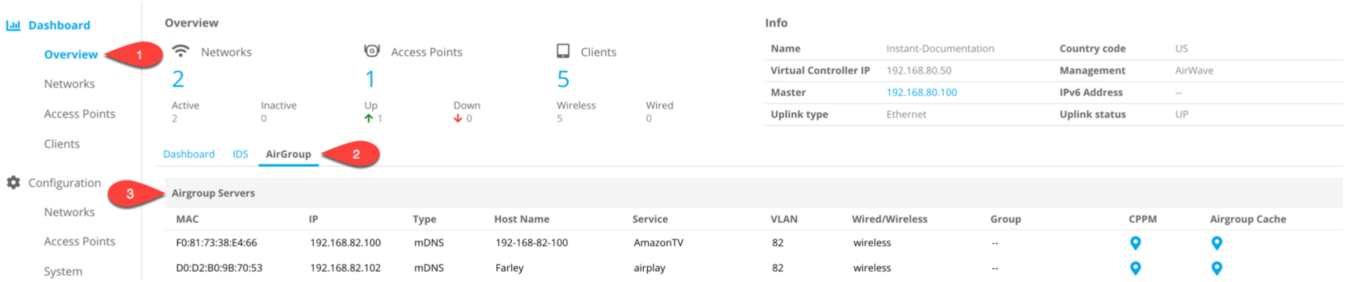
CALEA

You have now defined the AirGroup Service, and as you start to connect devices you will see them showing up

AirGroup Server Verification

1. Click on **Dashboard**
2. Click on **Overview**
3. Click on **AirGroup**

Here you can see the AirGroup servers listed



Overview

Networks 2 — Active 2, Inactive 0

Access Points 1 — Up 1, Down 0

Clients 5 — Wireless 5, Wired 0

Info

Name	Instant-Documentation	Country code	US
Virtual Controller IP	192.168.80.50	Management	AirWave
Master	192.168.80.100	IPv6 Address	--
Uplink type	Ethernet	Uplink status	UP

Airgroup Servers

MAC	IP	Type	Host Name	Service	VLAN	Wired/Wireless	Group	CPPM	Airgroup Cache
F0:81:73:38:E4:66	192.168.82.100	mDNS	192-168-82-100	AmazonTV	82	wireless	--	●	●
D0:D2:B0:9B:70:53	192.168.82.102	mDNS	Farley	airplay	82	wireless	--	●	●

You can refer to the Verifying AirGroup Service for additional commands from the CLI for command outputs. These are consistent across Mobility Managed and Instant Deployments.

AirGroup Configuration on the Mobility Master

This section describes the configuration of the following items in a controller-based network, with optional ClearPass-specific configuration

The AirGroup Profile

The AirGroup Service

The optional ClearPass configuration includes:

Adding the network device

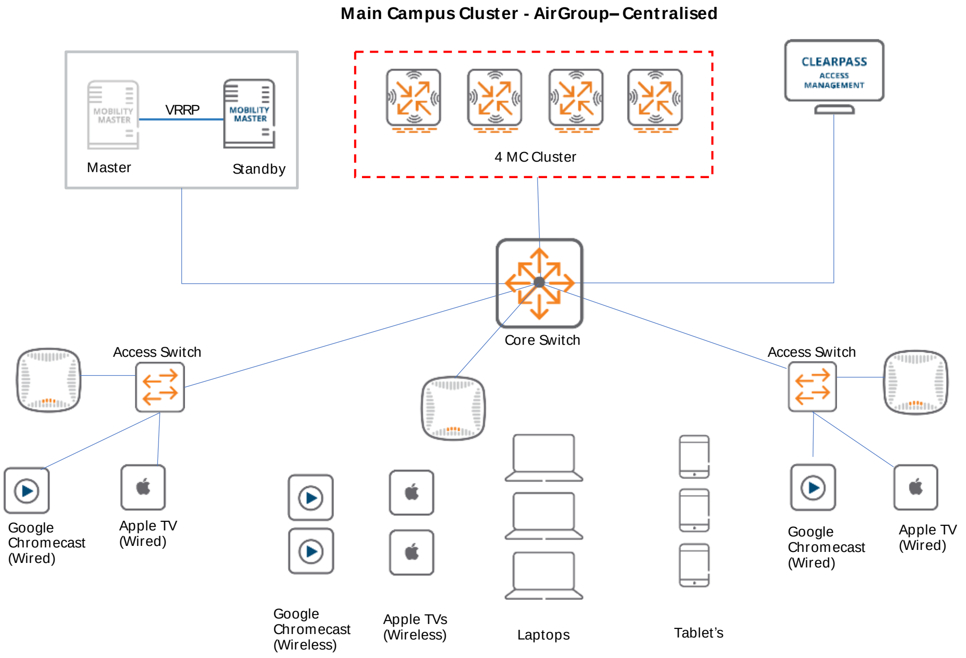
Adding the Mobility Master/Controller to the AirGroup service on ClearPass Guest

The following parameters are recommended if your deploying AirGroup with ClearPass but are not required if you're not deploying AirGroup with ClearPass.

Steps to be performed when AirGroup is deployed with ClearPass

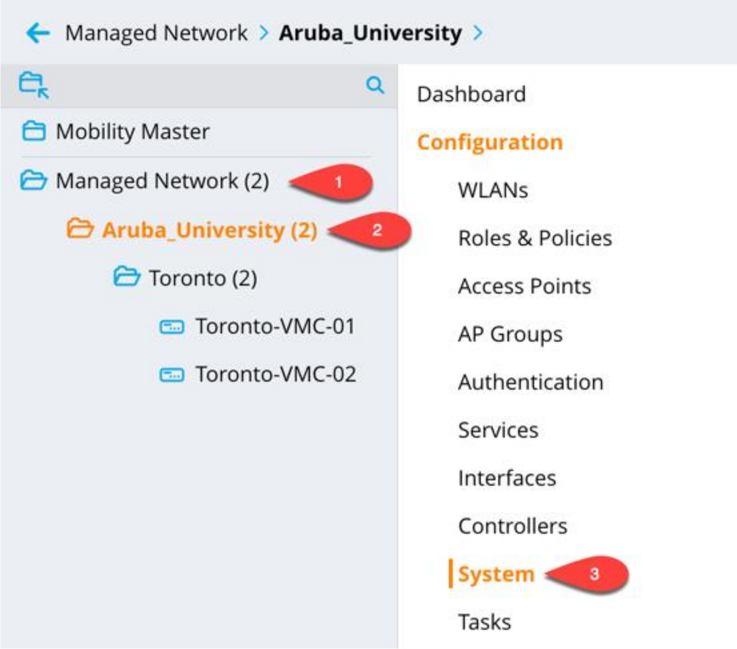
1. Define an RFC 3576 Server
2. Define an Authentication Server Group and assign a server to the group
3. Map the AirGroup Profile

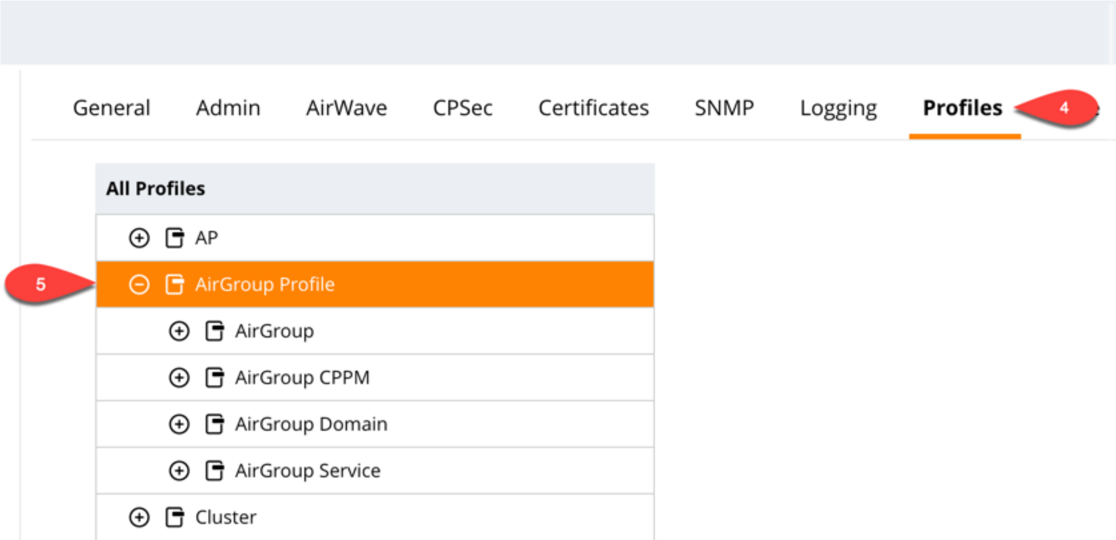
Network Topology



The AirGroup Profile

1. Navigate to Managed Network-><group>
2. Select Configuration
3. Select the System
4. Select the Profiles TAB
5. Under all Profiles choose AirGroup Profile

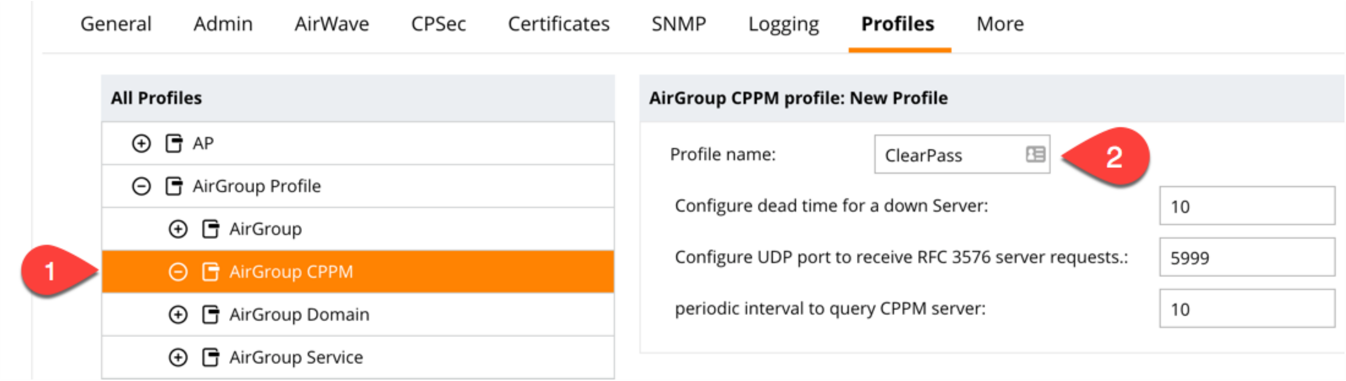




The AirGroup CPPM Profile

Defining AirGroup CPPM Profile

1. Click on **AirGroup CPPM**
2. Click on the blue **plus** (+) sign
1. In the **Profile name box**, use a descriptive profile name (in this example **ClearPass**)
2. Then click on **Submit**



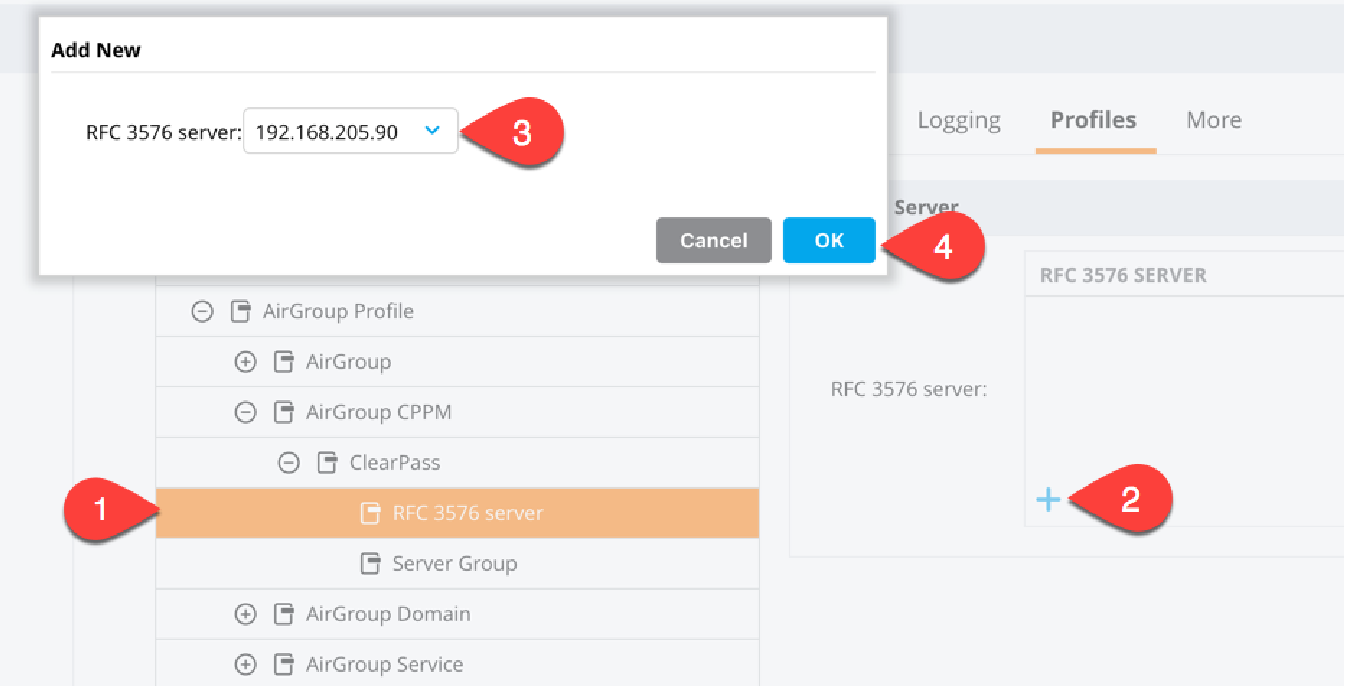
AirGroup CPPM profile: New Profile

Profile name:	ClearPass
Configure dead time for a down Server:	10
Configure UDP port to receive RFC 3576 server requests.:	5999
periodic interval to query CPPM server:	10

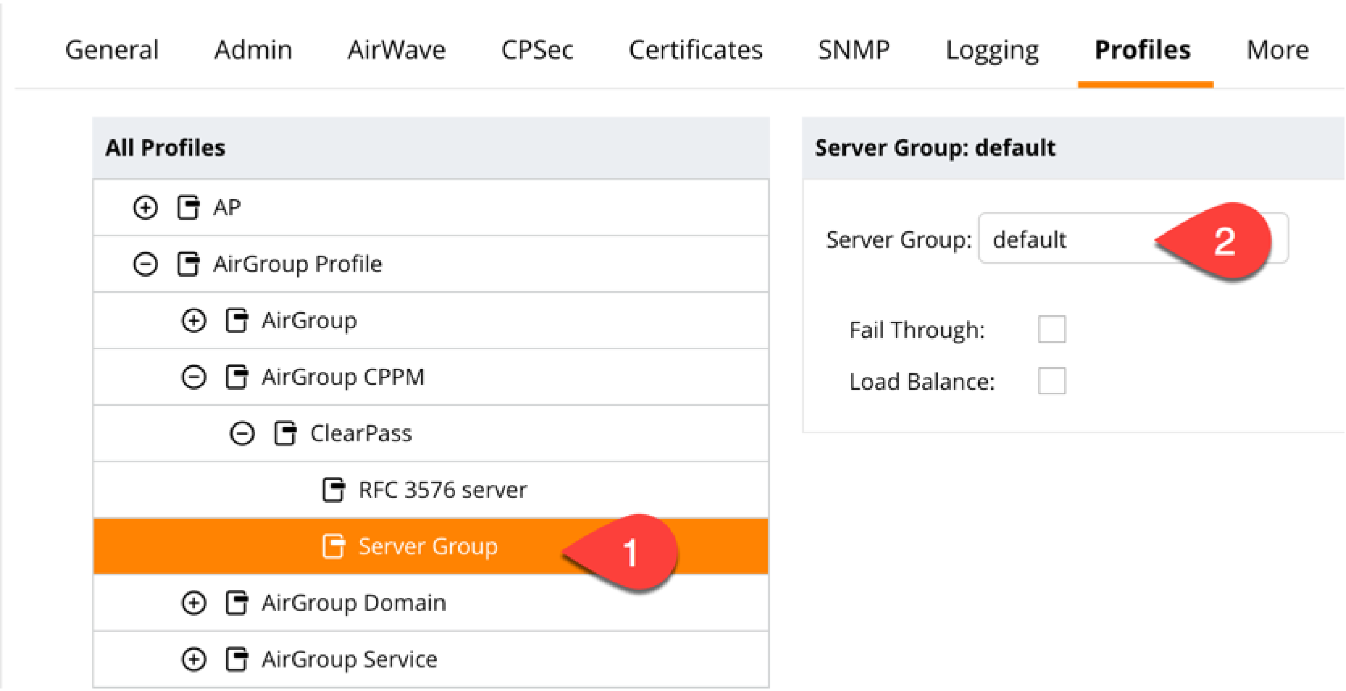
Configuring the AirGroup CPPM Profile

We will start with the RFC 3576 Server then move to the Server Group

1. Click on the **profile name** you created (in this example **ClearPass**)
    - We will leave the default options
2. Click on **RFC 3576 server**
3. Click on the blue **plus** (+) sign
4. A popup box will appear with a drop down to choose the **RFC 3576 server** (in this example there is only one)
5. Click **OK**
6. Then click on **Submit**



7. Click on **Server Group**
8. Click on the **dropdown selector** with will have default listed



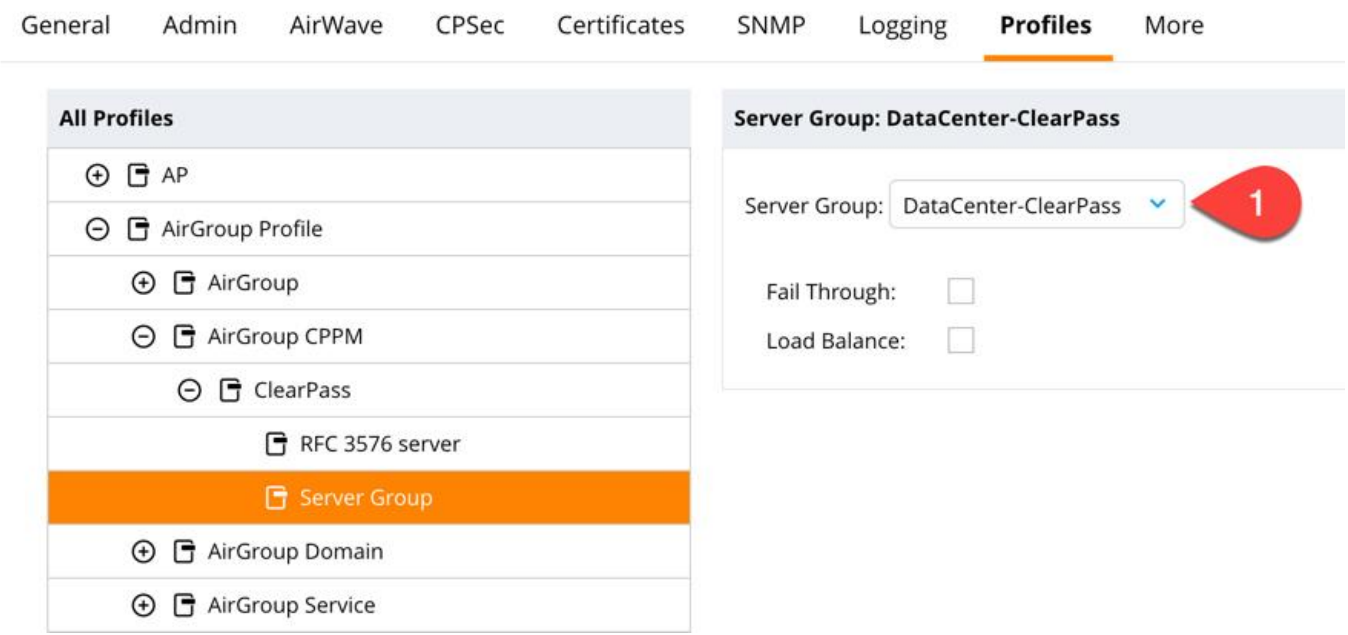
Server Group: default

Server Group: default

Fail Through: □

Load Balance: □

9. Select the **Server Group** which you defined. In this example, it is **DataCenter-ClearPass**.
10. Click **Submit**



Server Group: DataCenter-ClearPass

Server Group: DataCenter-ClearPass

Fail Through: □

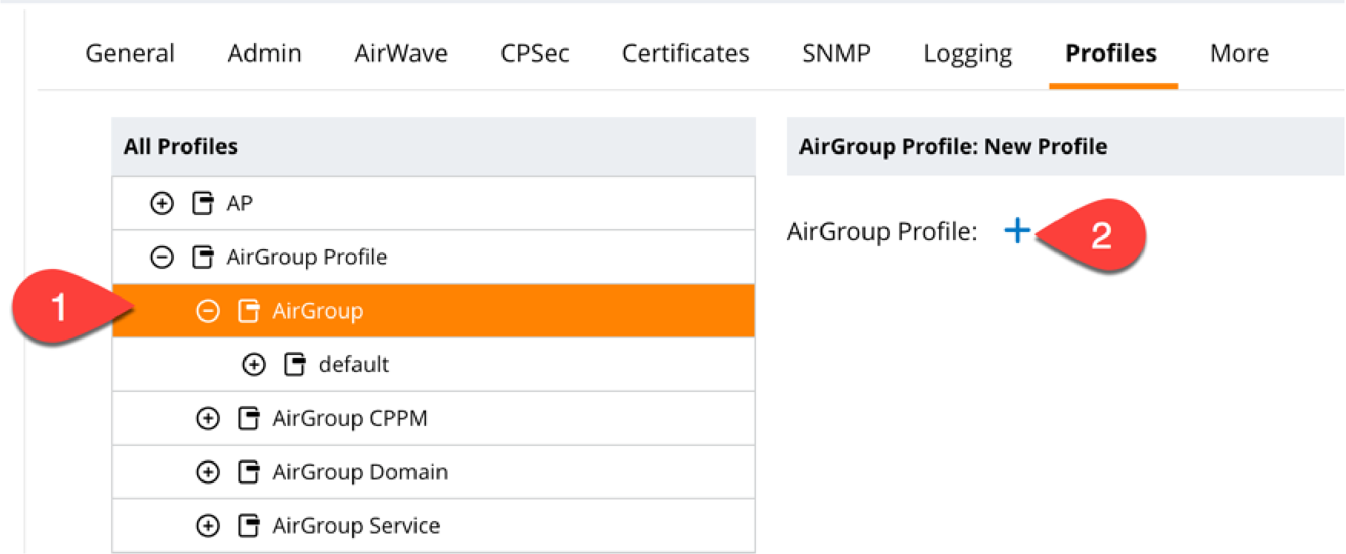
Load Balance: □

This completes the ClearPass profile

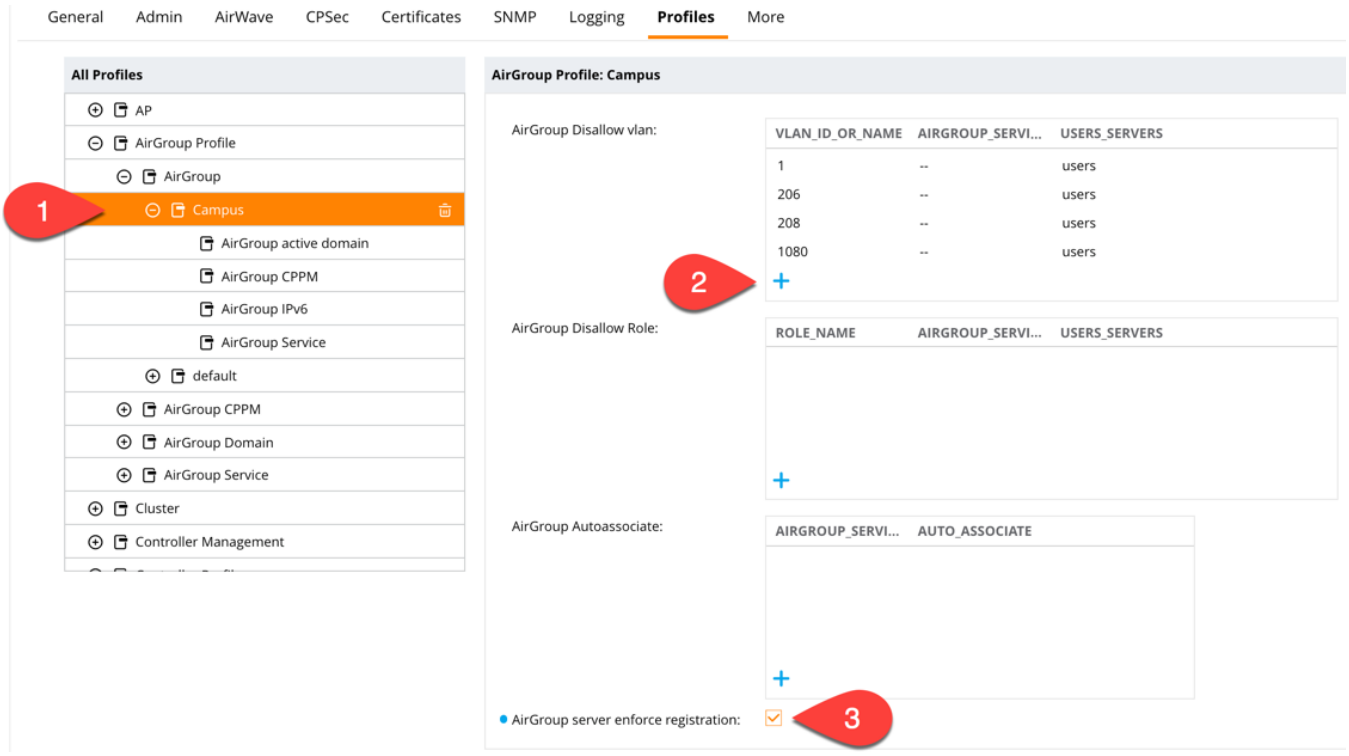
The AirGroup Service Profile

Defining the AirGroup Profile

1. Click on **AirGroup**
2. Click on the blue **plus** (+) sign next to AirGroup Profile:



1. The AirGroup Profile: **New Profile** window will appear.
2. In the **Profile name**: box use a descriptive profile name, in this example **Campus** was used.
3. In the **AirGroup Disallow VLAN** box**.** This is where you can exclude VLAN's you **do NOT want to participate in AirGroup**. In this example VLAN 1, 206 (MM VLAN), 208 (VMC VLAN) 1080 (AP management VLAN) will be excluded. These VLANs must be added one at a time.
4. If you want AirGroup to disallow a role click the blue **plus** (+) sign next to **AirGroup Disallow Role**.
5. **AirGroup Autoassociate**: in this example it will be left blank. Here you can create Autoassociate groupings.
6. Click the box for **AirGroup Server Enforce Registration**, enabling this will require device owners to register their AirGroup servers with ClearPass.
7. Click on **Submit**.



AirGroup Profile: Campus

AirGroup Disallow vlan:

VLAN_ID_OR_NAME	AIRGROUP_SERVI...	USERS_SERVERS
1	--	users
206	--	users
208	--	users
1080	--	users

AirGroup Disallow Role:

ROLE_NAME	AIRGROUP_SERVI...	USERS_SERVERS

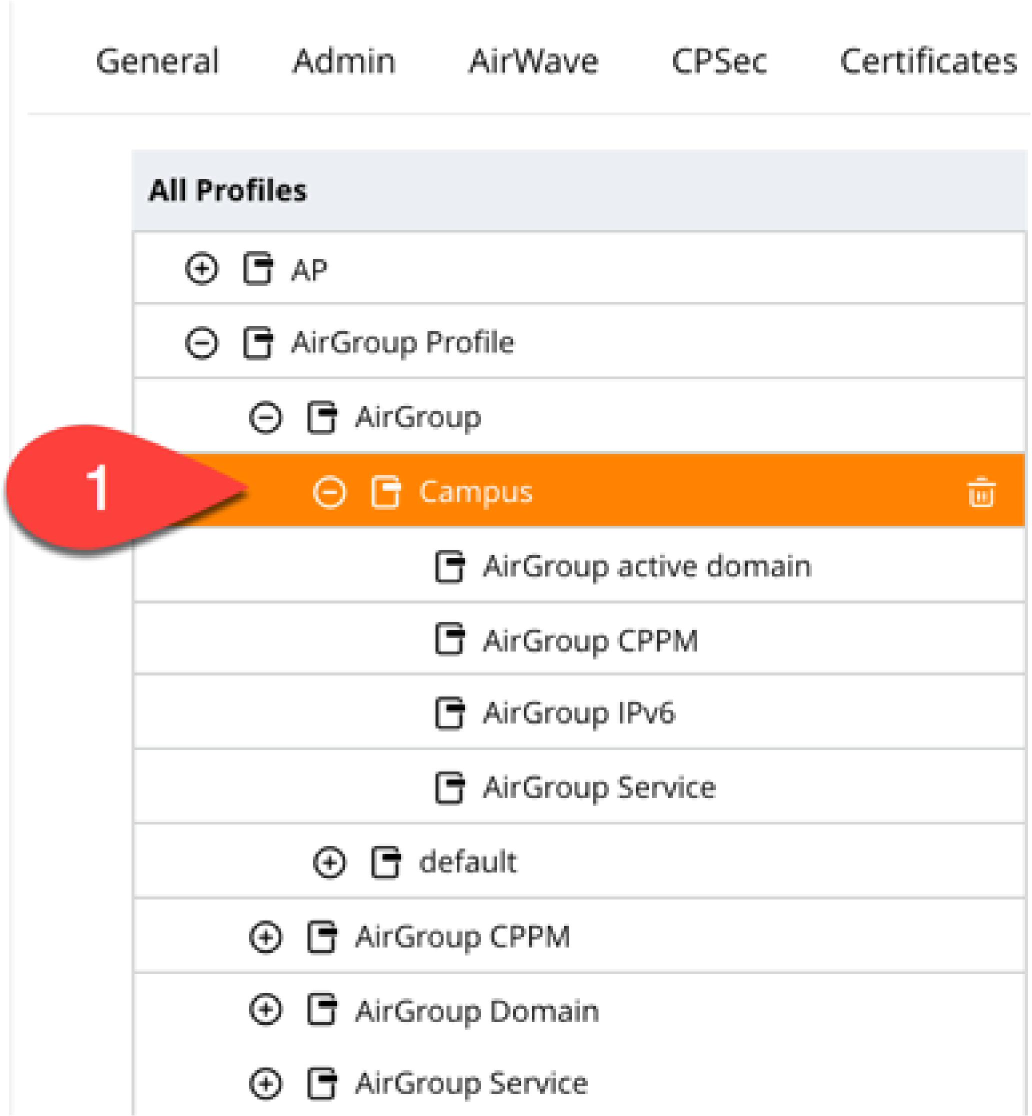
AirGroup Autoassociate:

AIRGROUP_SERVI...	AUTO_ASSOCIATE

AirGroup server enforce registration: ☑

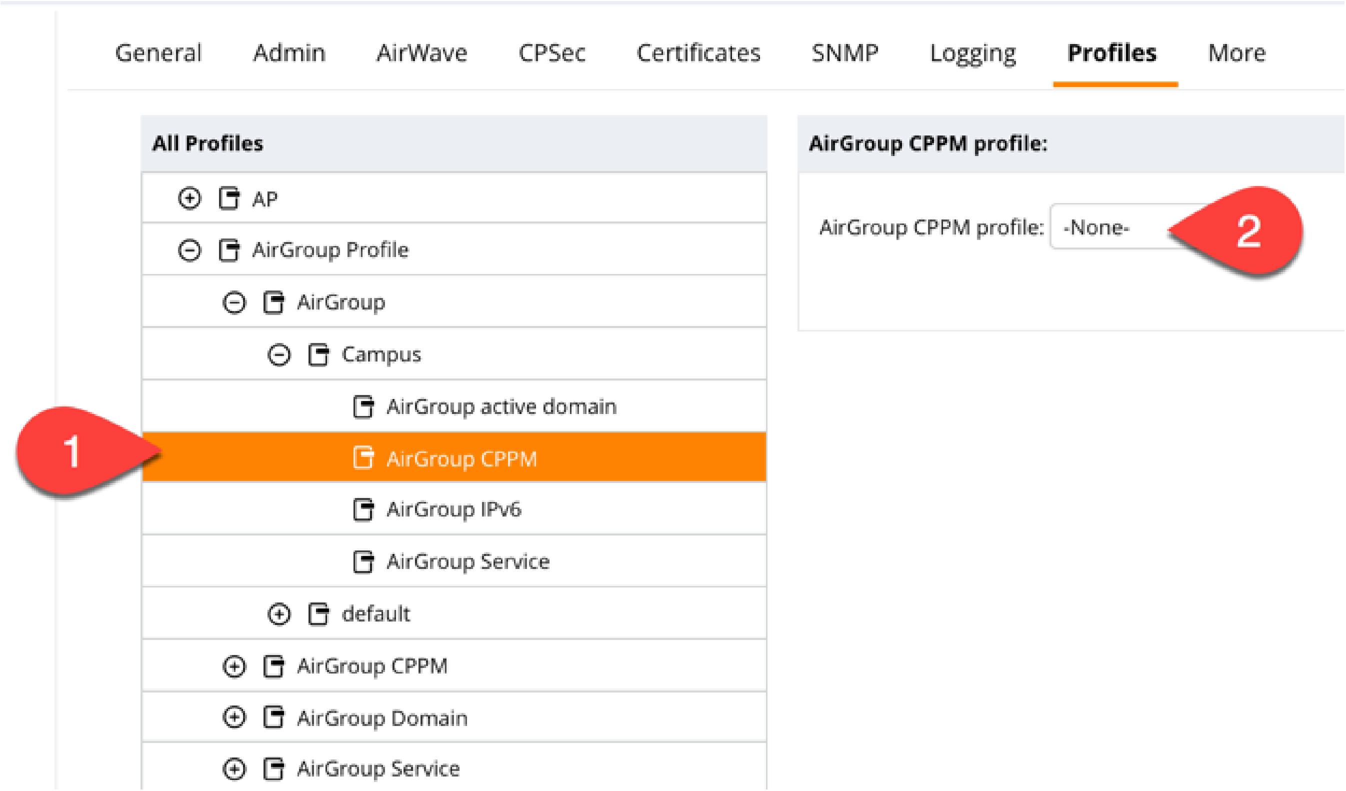
Configuring the AirGroup Profile

1. Click on the profile you created in the list (Campus in this example)



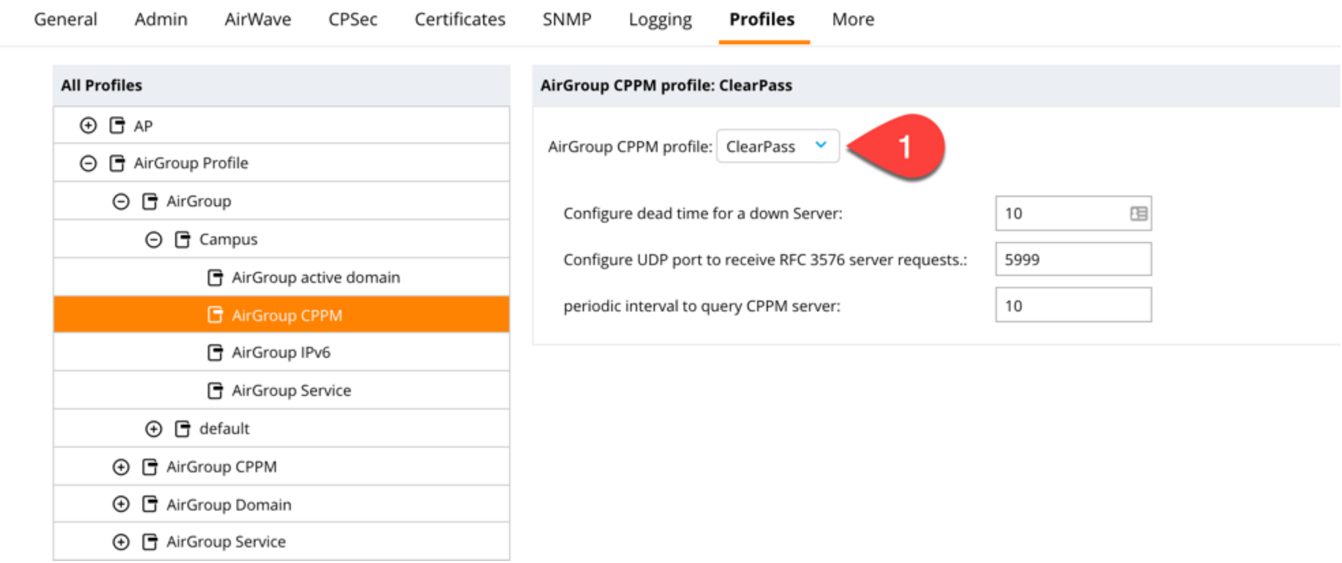
We will define the AirGroup service to use the previous AirGroup profiles which were created.

2. Click on **AirGroup CPPM** under the defined **AirGroup Profile**
3. We will see the **AirGroup CPPM** profile: is set to **None**



AirGroup CPPM profile: -None-

4. Click the drop-down box and chose the profile you created earlier (in this example, **ClearPass**)



AirGroup CPPM profile: ClearPass

Configure dead time for a down Server: 10

Configure UDP port to receive RFC 3576 server requests.: 5999

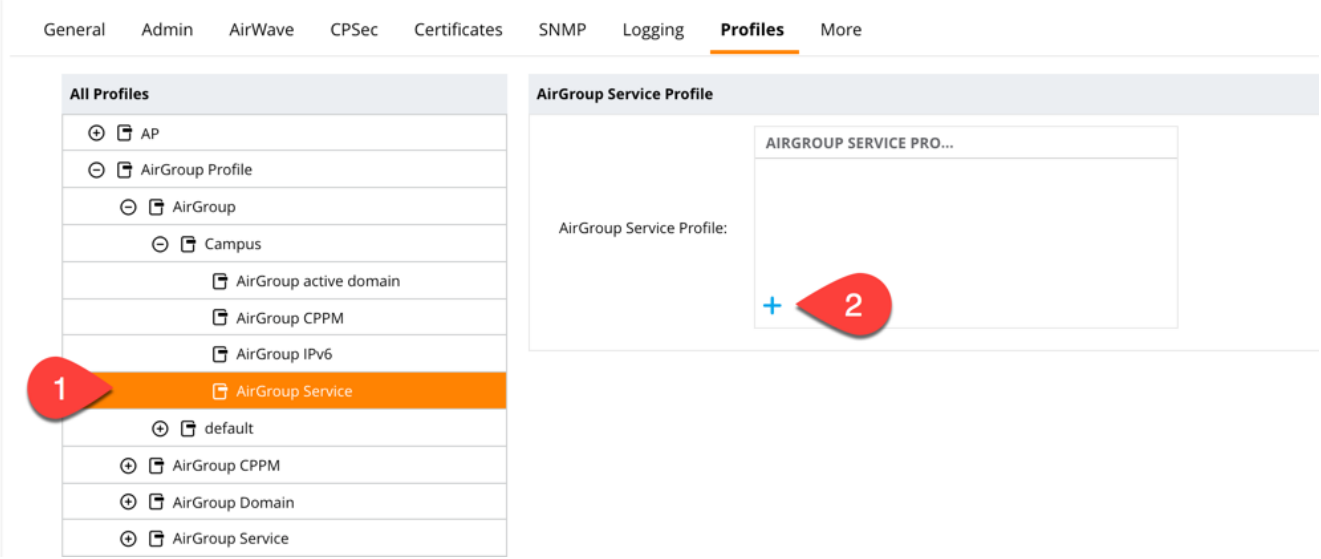
periodic interval to query CPPM server: 10

5. Click on **Submit**

Defining AirGroup Services

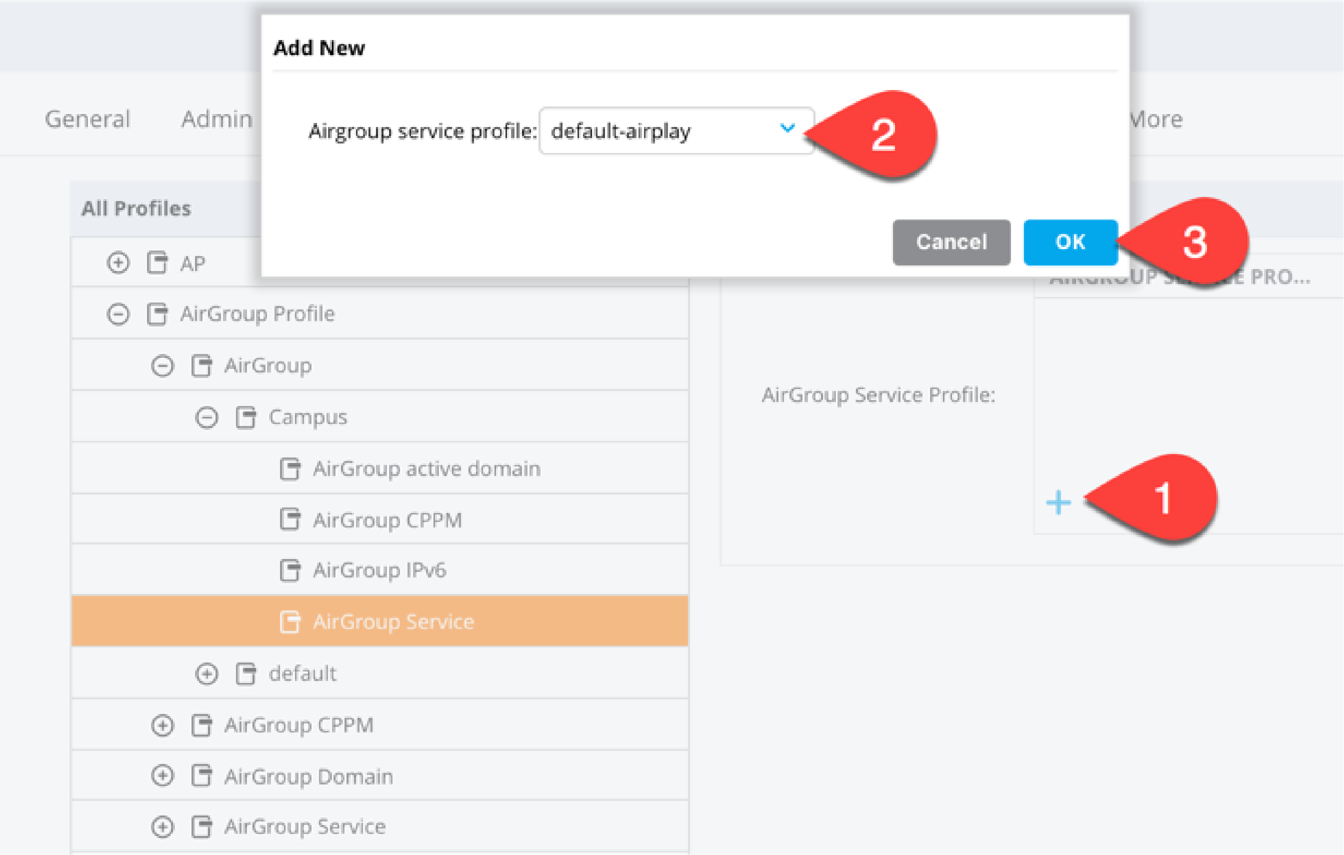
Within the AirGroup Service will permit the services to permit. In the AirPlay/Amazon TV/Chromecast will be allowed.

1. Click on AirGroup Service
2. Click the + in the AirGroup Service Profile:



With the drop-down box we will choose the services we are after. In this example we will repeat this step to get all the services we want.

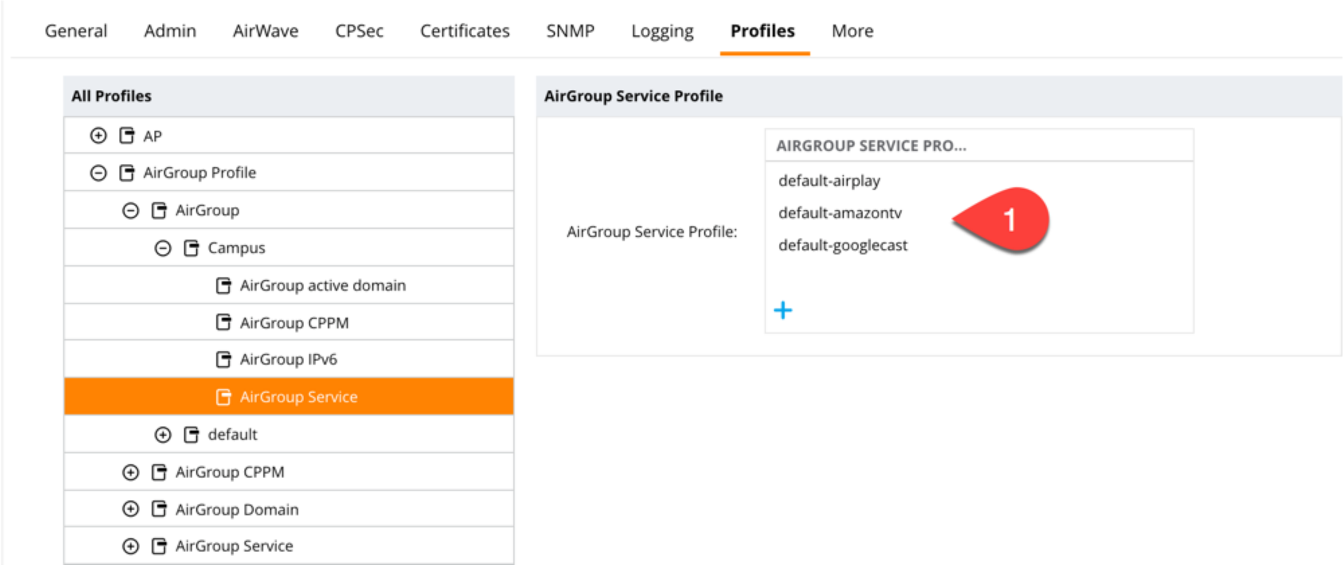
3. click the blue **plus** (+) sign
4. Choose **default-airplay** in the drop-down box
5. Click **OK**



Add New

Airgroup service profile: default-airplay

Repeat the steps above for **default-amazontv** and **default-googlecast** until we have all three services listed in the profile box.



General | Admin | AirWave | CPSec | Certificates | SNMP | Logging | Profiles | More

All Profiles
- AP
- AirGroup Profile
  - AirGroup
    - Campus
      - AirGroup active domain
      - AirGroup CPPM
      - AirGroup IPv6
      - AirGroup Service
    - default
  - AirGroup CPPM
  - AirGroup Domain
  - AirGroup Service

AirGroup Service Profile

AirGroup Service Profile:

AIRGROUP SERVICE PRO...
default-airplay
default-amazontv
default-googlecast

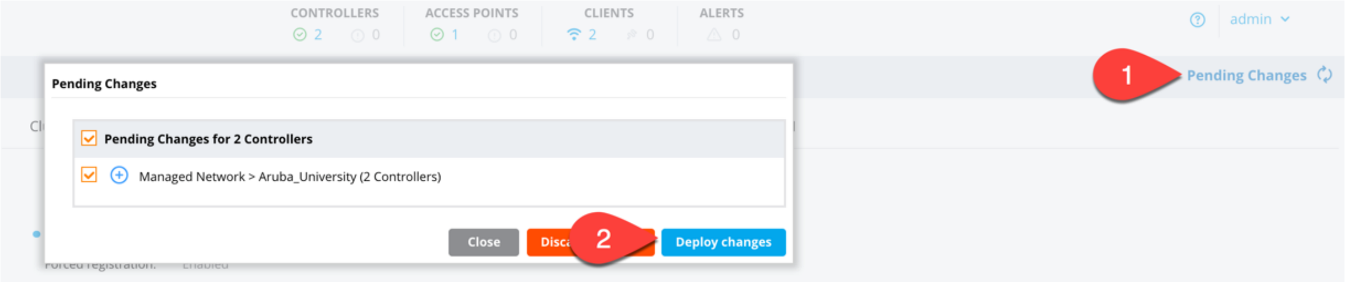
6. Click **Submit**

Please feel free to make adjustments as needed for your environment.

Applying the AirGroup Profile Changes

In the next steps we will be pushing the configuration out to the devices in the network. The devices or Mobility Master will then synchronize the configuration of the profile changes which were just completed.

1. Click on **pending changes**
2. Click on **Deploy Changes**

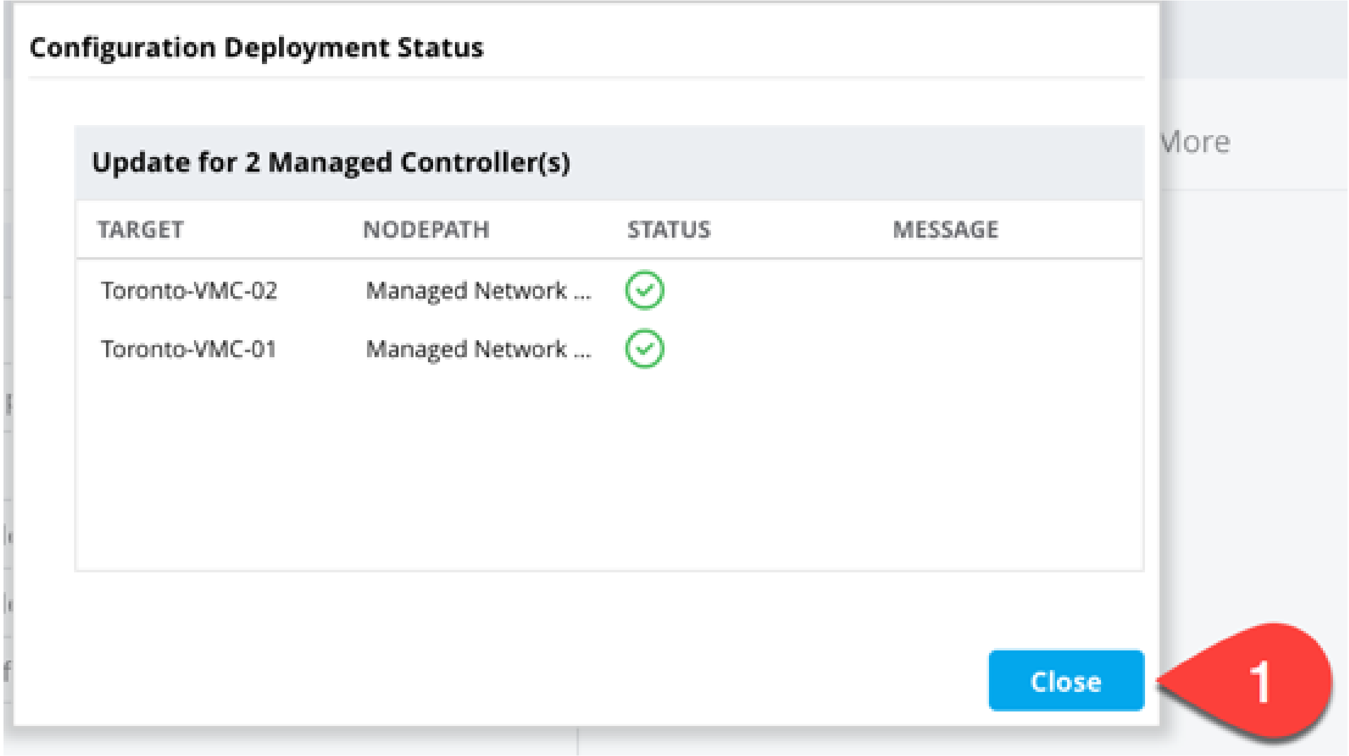


Pending Changes

☑ Pending Changes for 2 Controllers

☑ Managed Network > Aruba_University (2 Controllers)

3. A popup box will appear with the status of the configuration deployment click on Close



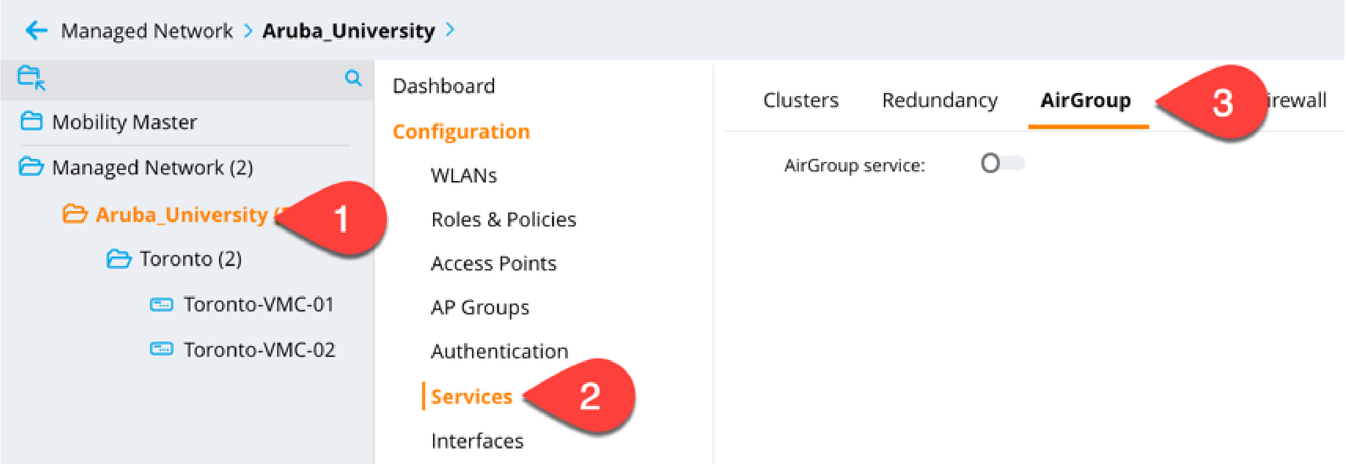
Configuration Deployment Status

Update for 2 Managed Controller(s)

TARGET	NODEPATH	STATUS	MESSAGE
Toronto-VMC-02	Managed Network ...	✓	
Toronto-VMC-01	Managed Network ...	✓	

Enabling the AirGroup Service

1. Click on the **Managed Network** then the Group (in this example **Aruba_University**)
2. Click on **Services**
3. Then on the **AirGroup TAB**



4. Click on the **slider icon** next to **AirGroup Service**
5. Define the AirGroup mode as either **Centralized** or **Distributed**

In this example Centralized was chosen as this environment is on a high speed network. If Mobility Controllers were located remote sites, we would use Distributed mode.

6. Then for the AirGroup Profile, click **the drop down** and choose the **profile** defined earlier. In in this example it's **Campus**
7. Click on **Submit**
8. Click on **Pending Changes**
9. Chen click on **Deploy Changes**
10. Click on **Close**

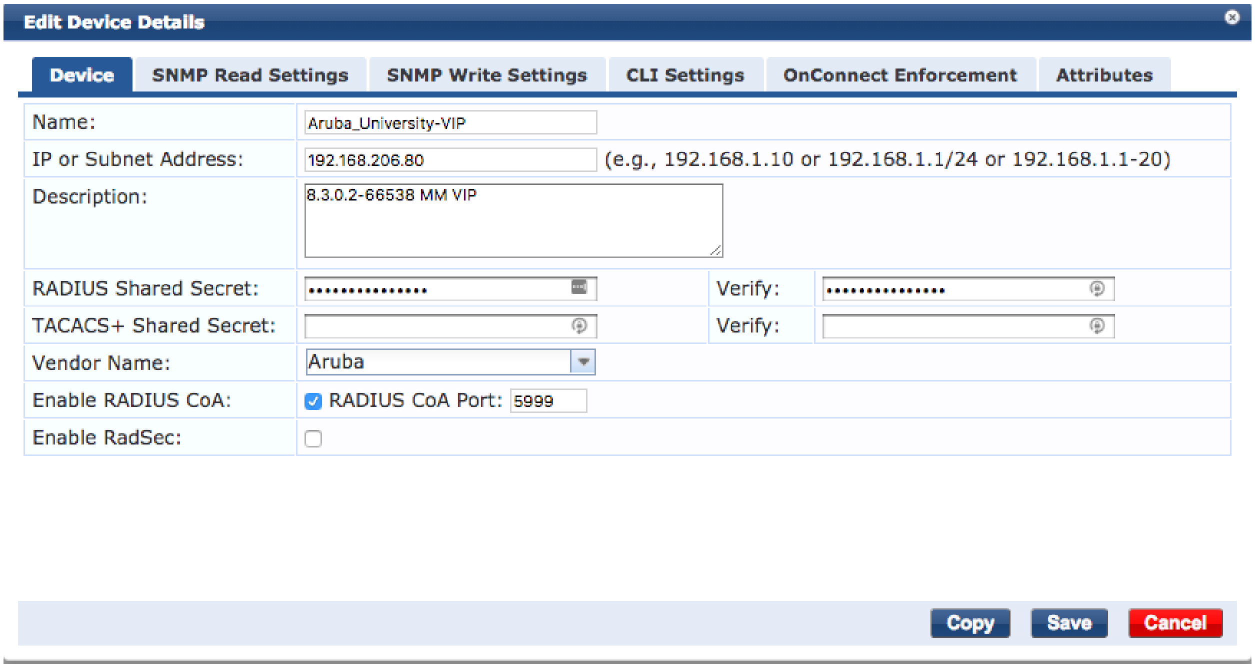
Now the AirGroup service has deployed at Managed Network <group> or /md/group in this example it's Managed Network Aruba_University (/md/Aruba_University)

Basic ClearPass Configuration

Adding Network Devices

During these steps, we will add the Mobility Master and Mobility Controllers to the network device list within ClearPass:

1. Log into ClearPass Policy Manager (https://<servername/ip>/tips).
2. Add the Mobility Master (MM) and Mobility Controllers (MC) to **Network Devices**.
   a. This is required due to authentication requests can come from the MM or the MC's
3. **Configuration -> Network -> Devices -> Add**

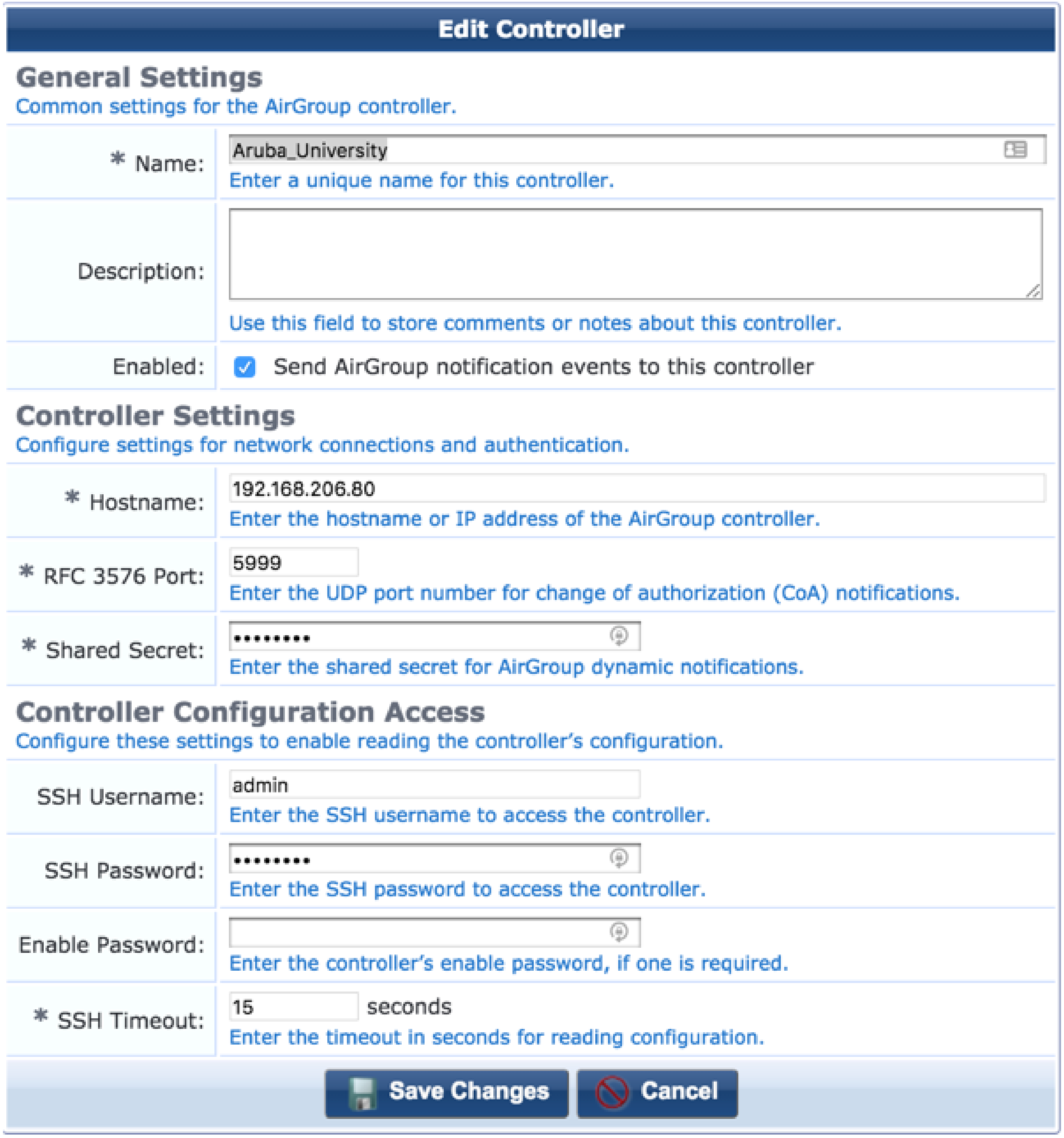


Name:	Aruba_University-VIP		
IP or Subnet Address:	192.168.206.80 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)		
Description:	8.3.0.2-66538 MM VIP		
RADIUS Shared Secret:	•••••••••••••••	Verify:	•••••••••••••••
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Aruba		
Enable RADIUS CoA:	☑ RADIUS CoA Port: 5999		
Enable RadSec:	□		

Defining Mobility Master in ClearPass Guest

Login to ClearPass Guest and add the MM or Instant Virtual Controller to the AirGroup Controller list

1. **Login** to ClearPass Guest (https://<servername/ip>/guest
2. **Administration -> AirGroup Services -> Controllers**
3. Click on **Create AirGroup controller** in the upper right
4. Complete the details for your **MM** or Controller (standalone/MCM)
5. Click on **Save Changes**



Edit Controller

General Settings
Common settings for the AirGroup controller.

* Name: Aruba_University
Enter a unique name for this controller.

Description:
Use this field to store comments or notes about this controller.

Enabled: ☑ Send AirGroup notification events to this controller

Controller Settings
Configure settings for network connections and authentication.

* Hostname: 192.168.206.80
Enter the hostname or IP address of the AirGroup controller.

* RFC 3576 Port: 5999
Enter the UDP port number for change of authorization (CoA) notifications.

* Shared Secret: ••••••••
Enter the shared secret for AirGroup dynamic notifications.

Controller Configuration Access
Configure these settings to enable reading the controller's configuration.

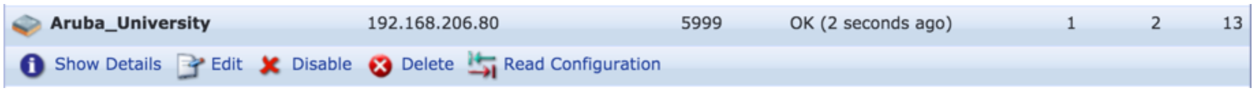
SSH Username: admin
Enter the SSH username to access the controller.

SSH Password: ••••••••
Enter the SSH password to access the controller.

Enable Password:
Enter the controller's enable password, if one is required.

* SSH Timeout: 15 seconds
Enter the timeout in seconds for reading configuration.

6. Click on **Read Configuration**



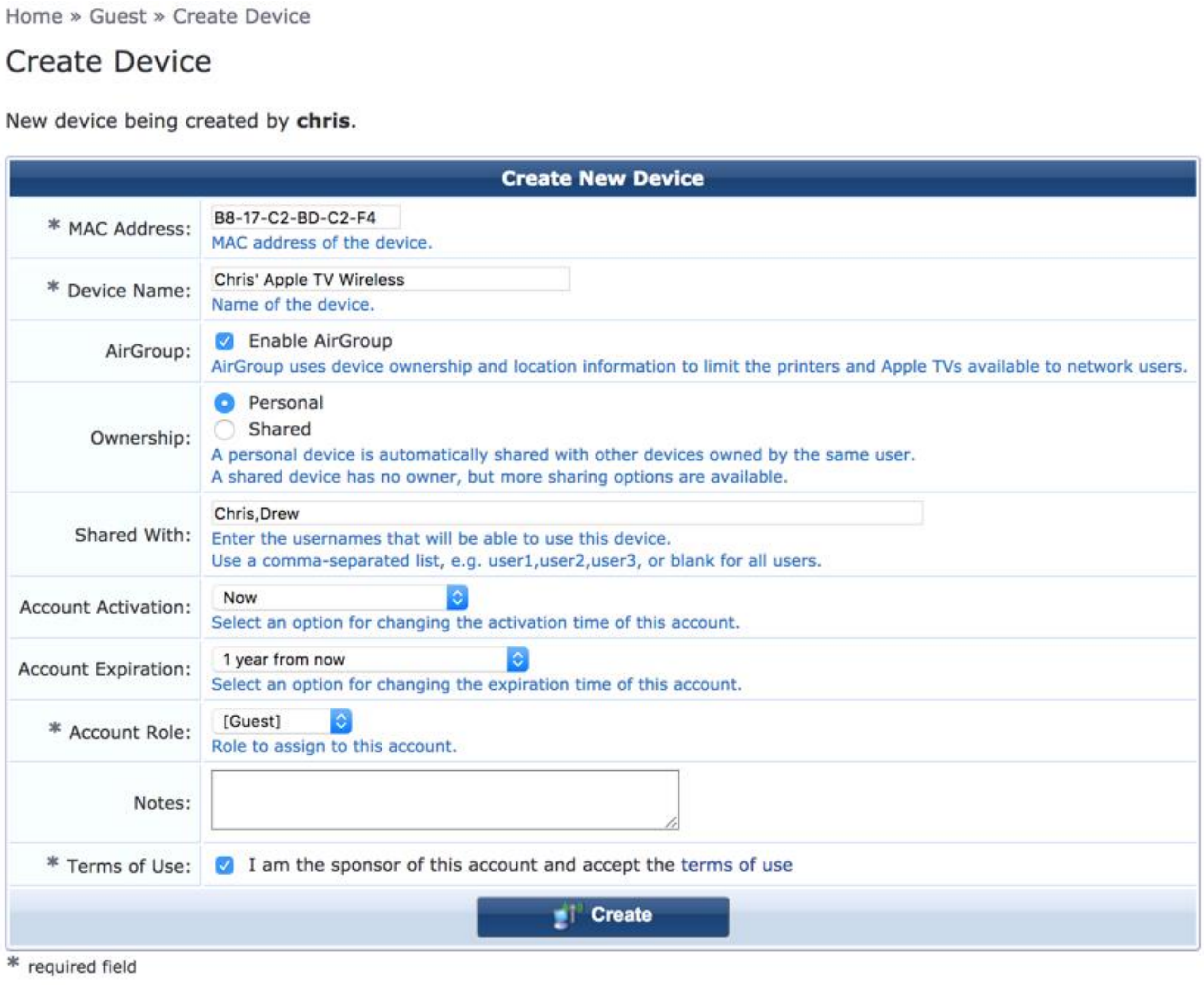
Aruba_University	192.168.206.80	5999	OK (2 seconds ago)	1	2	13

NOTE

In this example the ClearPass Guest Endpoints Database being used for device authentication.

Adding AirGroup Servers on ClearPass Guest

1. Click on **Create Device**
2. Add the **device MAC** Address with – format
3. Give the **device a name** (Chris' ATV in my example)
4. Click the **Enable AirGroup box**
5. In this example **Personal** was used
6. Complete the Shared with list (**user names**, **MAC address**, etc)
7. In this example the defaults were used
8. Click **Create**



Home » Guest » Create Device

Create Device

New device being created by **chris**.

Create New Device

* MAC Address:	B8-17-C2-BD-C2-F4 MAC address of the device.
* Device Name:	Chris' Apple TV Wireless Name of the device.
AirGroup:	☑ Enable AirGroup AirGroup uses device ownership and location information to limit the printers and Apple TVs available to network users.
Ownership:	● Personal ○ Shared A personal device is automatically shared with other devices owned by the same user. A shared device has no owner, but more sharing options are available.
Shared With:	Chris,Drew Enter the usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.
Account Activation:	Now Select an option for changing the activation time of this account.
Account Expiration:	1 year from now Select an option for changing the expiration time of this account.
* Account Role:	[Guest] Role to assign to this account.
Notes:	
* Terms of Use:	☑ I am the sponsor of this account and accept the terms of use

* required field

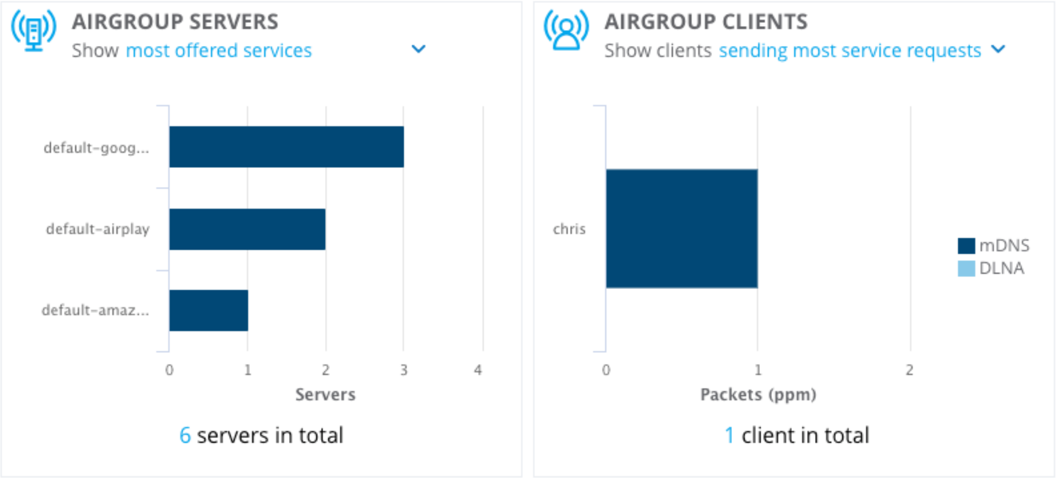
NOTE

At present AirGroup ClearPass Entries are not shown in the AOS GUI. In this example we will use the CLI to verify the AirGroup ClearPass entries

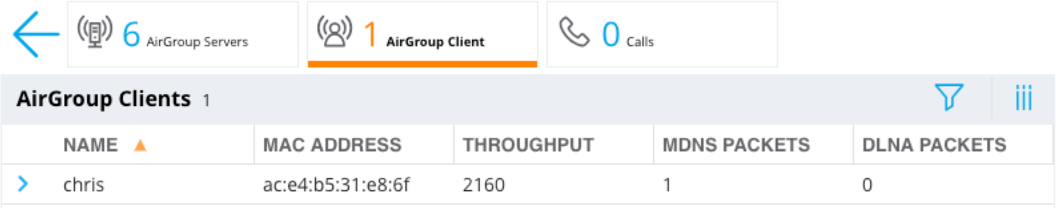
Verifying AirGroup Services (WebUI)

Mobility Master-

1. **Logon** to the **GUI of MM or Controller**
2. **Navigate to Dashboard -> Services**



3. Click on (AirGroup Client Icon) next to **Airgroup Clients**

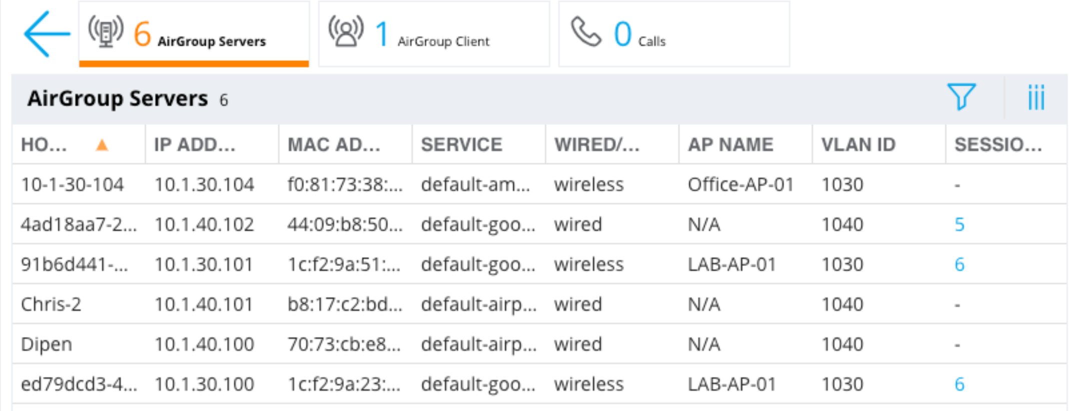


AirGroup Clients 1

	NAME ▲	MAC ADDRESS	THROUGHPUT	MDNS PACKETS	DLNA PACKETS
›	chris	ac:e4:b5:31:e8:6f	2160	1	0

Here, you can see the throughput along with the number of MDNS/DLNA packets.

4. Click on icon next to AirGroup Servers (AirGroup Server Icon)

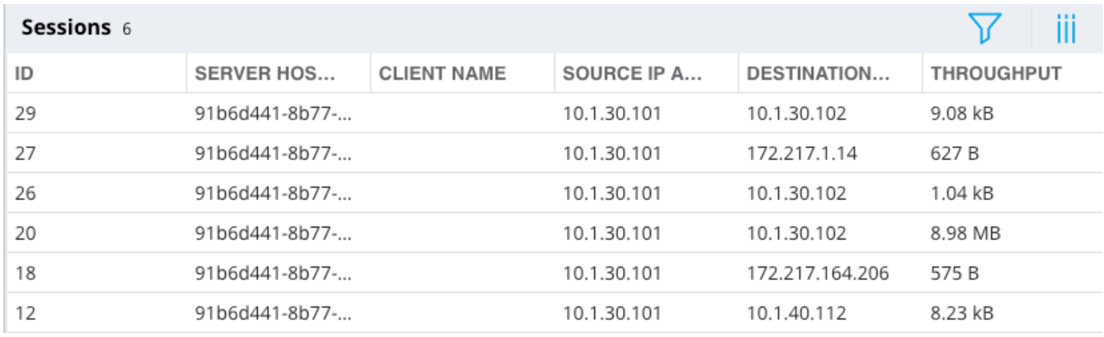


AirGroup Servers 6

HO... ▲	IP ADD...	MAC AD...	SERVICE	WIRED/...	AP NAME	VLAN ID	SESSIO...
10-1-30-104	10.1.30.104	f0:81:73:38:...	default-am...	wireless	Office-AP-01	1030	-
4ad18aa7-2...	10.1.40.102	44:09:b8:50...	default-goo...	wired	N/A	1040	5
91b6d441-...	10.1.30.101	1c:f2:9a:51:...	default-goo...	wireless	LAB-AP-01	1030	6
Chris-2	10.1.40.101	b8:17:c2:bd...	default-airp...	wired	N/A	1040	-
Dipen	10.1.40.100	70:73:cb:e8...	default-airp...	wired	N/A	1040	-
ed79dcd3-4...	10.1.30.100	1c:f2:9a:23:...	default-goo...	wireless	LAB-AP-01	1030	6

You can see the list of AirGroup services (default-google/default-amazon/default-airplay), the connection method (wireless/wired), access point (LAB-AP-01) and the VLAN the server is assigned to.

If you click on the number under the **Sessions** column, you can see the list of sessions for that AirGroup Server.



Sessions 6

ID	SERVER HOS...	CLIENT NAME	SOURCE IP A...	DESTINATION...	THROUGHPUT
29	91b6d441-8b77-...		10.1.30.101	10.1.30.102	9.08 kB
27	91b6d441-8b77-...		10.1.30.101	172.217.1.14	627 B
26	91b6d441-8b77-...		10.1.30.101	10.1.30.102	1.04 kB
20	91b6d441-8b77-...		10.1.30.101	10.1.30.102	8.98 MB
18	91b6d441-8b77-...		10.1.30.101	172.217.164.206	575 B
12	91b6d441-8b77-...		10.1.30.101	10.1.40.112	8.23 kB

Verifying AirGroup Services (CLI)

Mobility Master-

1. **Logon** to the **cli of MM or Controller**
2. **Cd /md/your group** (in this example **cd /md/TME**)
3. Type in **show airgroup status**

```
(8.4-MM-01) [TME] #show airgroup status


Showing AirGroup info from /md/TME


AirGroup Information

--------------------

Feature            Status

-------            ------

AirGroup mode        Centralised

AirGroup Profile     67334

CPPM Profile         WHI01-ClearPass

Active domain        N/A


MDNS               Enabled

DLNA               Disabled

Enforce Registration  Enabled

IPV6               Disabled


AirGroup Service Information

----------------------------

Service            Status

-------            ------

default-airplay     Enabled

default-googlecast  Enabled

default-amazontv    Enabled
```

4. Type in **show airgroupservice**

```
(8.4-MM-01) [TME] #show airgroupservice


Showing AirGroup info from /md/TME


AirGroupService Table

---------------------

Service            status   service ID       Auto-Associate  Description

-------            ------   ----------       --------------  -----------

default-airplay    Enabled  _airplay._tcp                    AirPlay

                            _appletv-v2._tcp

                            _raop._tcp

default-googlecast  Enabled  _googlecast._tcp                GoogleCast supported by Chromecast etc.

                            _googlezone._tcp

default-amazontv   Enabled  _amzn-wplay._tcp                 Amazon fire tv
```

5. Type in show airgroup users

```
(8.4-MM-01) [Whitby] #show airgroup users


Showing AirGroup users under /md/TME/Whitby


AirGroup Users

--------------

MAC                IP           Type  Host Name  VLAN  Wired/Wireless  Role           Group  Username  AP-Name

---                --           ----  ---------  ----  --------------  ----           -----  --------  -------

AC:E4:B5:31:E8:6F  10.1.20.100  mDNS             1020  wireless        authenticated         chris     LAB-AP-01

Num Users: 1.
```

6. Type in **show airgroup servers**

```
(8.4-MM-01) [Whitby] #show airgroup servers


Showing AirGroup servers under /md/TME/Whitby


AirGroup Servers

----------------

MAC          IP       Type  Host Name                    Service        VLAN  Wired/Wireless  Role         Group  Username     AP-Name

---          --       ----  ---------                    -------        ----  --------------  ----         -----  --------     -------

44:09:B8:50:CB:7E  10.1.40.102  mDNS  4ad18aa7-215c-39f7-e45c-5051db41f511  default-googlecast  1040  wired       CTRLROLE-3019-
2       4409b850cb7e  N/A

B8:17:C2:BD:C2:F5  10.1.40.101  mDNS  Chris-2                    default-airplay    1040  wired       CTRLROLE-3019-2      b817c2bdc2f5
N/A

F0:81:73:38:E4:66  10.1.30.104  mDNS  10-1-30-104                    default-amazontv   1030  wireless     authenticated
Office-AP-01

1C:F2:9A:23:2F:2F  10.1.30.100  mDNS  ed79dcd3-4e75-db44-6fd3-29dfa07da594  default-googlecast  1030  wireless     authenticated
LAB-AP-01

1C:F2:9A:51:8A:D2  10.1.30.101  mDNS  91b6d441-8b77-d7e2-988b-bc6e8470c0ad  default-googlecast  1030  wireless     authenticated
LAB-AP-01

70:73:CB:E8:70:36  10.1.40.100  mDNS  Dipen                    default-airplay    1040  wired       CTRLROLE-3019-2      7073cbe87036
N/A

Num Servers: 6.
```

7. Type **show airgroup cppm server-group (if configured)**

```
(8.4-MM-01) [TME] #show airgroup cppm server-group


Showing AirGroup info from /md/TME


AirGroup AAA Server Group

-------------------------

Name          Inservice  trim-FQDN  match-FQDN

----          ---------  ---------  ----------

WHI01-ClearPass  Yes       No
```

8. Type show airgroup cppm entries (if configured)

```
(8.4-MM-01) [Whitby] #show airgroup cppm entries

ClearPass Guest Device Registration Information
-----------------------------------------------
Device           device-owner  shared location-id AP-name  shared location-id AP-FQLN  shared location-id AP-group  shared user-list
shared group-list  shared role-list  CPPM-Req  CPPM-Resp
------           ------------  -------------------------  -------------------------  ---------------------------  ----------------  -----------------  ----------------  --------  -------
--
B8:17:C2:BD:C2:F5  chris                                                       Chris                              1      1
F0:81:73:38:E4:66  Farley                                                      farley                             1      1
                                                                  00714730107d
                                                                  Sati
                                                                  Chris
1C:F2:9A:23:2F:2F  admin                                                        Chris                             1      1
                                                                  Marius
                                                                  Sati
70:73:CB:E8:70:36  dipen                                                       Dipen                              1      1
                                                                  Chris
Num CPPM Entries:4
```

AirGroup with Dynamic Segmentation

Dynamic Segmentation is an umbrella group of technologies such as User-Based Tunneling, Port-Based Tunneling and Downloadable User Roles) used by switches running ArubaOS-Switch to tunnel users or ports from the switch to the Aruba Mobility Controller. This technology allows wired users to leverage the same role(s) as wireless users.

AirGroup with Dynamic Segmentation is supported with release ArubaOS release 8.4.0.0 and AurbaOS-Switch code 16.07 or greater.

ArubaOS-Switch key components:

Tunneled-node-server – Tunneled-node-server configuration context (used to establish the tunnel from the ArubaOS-S switch to the Mobility Controller(s)

Controller-ip - is the ip address of the primary mobility controller

Backup-controller-ip (optional)- This is the ip of the redundant mobility controller if utilizing clustering

Mode Role Based – Here we define if we are going to utilize User Based Tunneling (UBT) 1.0 or 2.0

- When reserved VLAN (xx.16.08.xxxx) - option is utilized this tells the switch to utilize UBT 2.0 options.
- The reserved VLAN does NOT need to exist on the switch, and is locally significant.

Enable – this will enable tunneled-node-server

You then need to configure the ArubaOS-Switch ports for tunneling

ArubaOS-Switch configuration for User Based Tunneling 1.0

Example:

```
ArubaOS-Switch(config)#Tunneled-node-server

ArubaOS-Switch(tunneled-node-server)#controller-ip 192.168.208.51

ArubaOS-Switch(tunneled-node-server)#mode role-based

ArubaOS-Switch(tunneled-node-server)#enable

ArubaOS-Switch(tunneled-node-server)#exit
```

ArubaOS-Switch configuration for User Based Tunneling 2.0

Example:

```
ArubaOS-Switch(config)# Tunneled-node-server

ArubaOS-Switch(tunneled-node-server)#controller-ip 192.168.208.51

ArubaOS-Switch(tunneled-node-server)#mode role-based reserved vlan 1000

ArubaOS-Switch(tunneled-node-server)#enable

ArubaOS-Switch(tunneled-node-server)#exit
```

Verification of VLAN status on the ArubaOS using UBT 2.0 we will see the reserved VLAN which gets created automatically:

```
ArubaOS-Switch#show vlan

Status and Counters - VLAN Information


 Maximum VLANs to support : 256

 Primary VLAN : DEFAULT_VLAN

 Management VLAN :


 VLAN ID Name                         | Status     Voice Jumbo

 ------- -------------------------------- + ---------- ----- -----

 1       DEFAULT_VLAN                  | Port-based No    No

 34      Management                    | Port-based No    No

 999     DEAD                          | Port-based No    No

 1000    TUNNELED_NODE_SERVER_RESERVED    | Port-based No    No
```

Example Scenarios for Autoassociate with AP-name

Below are some example scenarios where Autoassociate is used with AP-names.

Scenario 1

- Enforce registration enabled
- Autoassociate ap-name
- Registered device without any AirGroup enablement |policy
- Apple TV registered on CPPM without any sharing attributes.

Result: In this scenario, a user connected to an RF neighbor AP of the server's AP will be able to discover the server.

Also, a user connected to a non-RF neighbor AP of the server's AP will NOT be able to discover the server.

Scenario 2

- Enforce registration enabled
- Autoassociate ap-name
- Device not registered at all in ClearPass.

Result: The user connected to an RF neighbor AP of the server's AP will be able to discover the server.

Scenario 3

- Enforce registration enabled
- Autoassociate ap-name
- Registered device with AirGroup enabled and policy set to personal with no user specified

If an Apple TV is registered as personal with owner as "Holland" and iPad is connected with 802.1X username Bob:

Result: Bob's iPad connected to RF neighbor of the server will NOT see Holland's Apple TV

If the Apple TV is registered as personal with owner as "Holland" and iPad is connected with 802.1X username Holland

Result: Holland's iPad connected to RF neighbor AP of the Apple TV's AP will be able to discover Holland's Apple TV.

Also, Holland's iPad connected to a non-RF neighbor of the server's AP will be able to discover the Holland's Apple TV because Holland is the owner of the device.

So regardless of RF neighborhood, if a device is registered with a personal policy, the device will be shown to that particular user.

Scenario 4

- Enforce registration enabled
- Autoassociate ap-name
- Registered device with AirGroup enabled and policy set to personal with two other users specified (as good as adding no policies)

If an Apple TV is registered to Holland and shared with Bob, and an iPad is connected with 802.1X username as Bob:

Result: Bob’s iPad will be able to see Holland’s Apple TV if the iPad and Apple TV are connected to APs which are RF neighbors of each other.

Result_1: Bob’s iPad will NOT be able to see Holland’s Apple TV if the iPad and Apple TV are connected to APs which are NOT RF neighbors of each other.

Scenario 5

- Enforce registration enabled
- Autoassociate ap-name
- Registered device with AirGroup enabled and policy set to share with zero ap-groups specified

Apple TV registered by admin on ClearPass with zero AP-groups configured.

Result: In this scenario, a user connected to a RF neighbor AP of server’s AP will be able to discover the server.

A user connected to a non-RF neighbor AP of the server’s AP will NOT be able to discover the server.

Scenario 6

- Enforce registration enabled
- Autoassociate ap-name
- Registered device with AirGroup enabled and policy set to share with two ap-groups specified

Apple TV registered by admin on CPPM shared with ap-groups ‘Library’ and ‘Main building’ configured.

Result: In this scenario, all the users connected to Library and Main building will be able to see the server irrespective of their RF location.

If an iPad is connected to any ap-group other than "Library and Main building", it will not be able to see the server irrespective of their RF location.

DLNA Devices Tested

The following DLNA devices have been tested.

Device	Service	Inter-VLAN support	Apps Tested	Notes
Chromecast	DIAL	Yes	Chrome Browser YouTube RealPlayer Cloud Google Play Movies PostTV	
Fire TV	DIAL	Yes	YouTube Allcast	YouTube and Allcast applications should be installed on the Fire TV as well to make it work
ROKU	DIAL	Yes	YouTube	Add the channels from the channel store suitable for the particular app
Samsung Smart TV	Media Renderer	Yes	Bubble UPnP	
XBOX	Media Renderer	No	Windows Play To	
Samsung phones/Tabs	Media Server	No	Native music player and video player applications	
Windows Media Server	Media Server	No	MediaConnect, Native music player & video player in Samsung Tab	
PS3	--	Yes	Native applications	PS3 sends out M-Search queries for Media Server; Does not advertise any service.
iOmega Storage Device	Media Server	Yes	Bubble UPnP	

Minix	Media Renderer	Yes	Bubble UPnP	

Devices Tested for Default Services

Services	Devices and Applications Supported
default-airplay	Apple TV, iPhone, MacBook, iPad, Extron, AirParrot, Netflix, Prime, YouTube, TED, native AirPlay in Apple devices
default-airprint	MDNS enabled printers
default-amazontv	Amazon Fire TV, Prime, YouTube
default-dial	Google Chromecast, Amazon Fire TV and Roku
default-dlna-media	Windows laptops, native Android, media servers
default-dlna-print	Printers which support DLNA
default-googlecast	Google Chromecast, Netflix, Prime, YouTube
default-itunes	Apple devices
default-remotemgmt	Apple devices for Remote Desktop
default-sharing	MacBooks for accessing file servers (not tested)

Bug List

Below is a list of bugs that have been identified and fixed that are related to AirGroup. Not every install will hit these bugs as there are several factors involved if a deployment is susceptible to a bug. If you are having issues with AirGroup it is recommended to open a TAC case and evaluate the list below of known bugs. It is recommended to run the latest version of code possible to address known bugs. TAC and your account team can help evaluate issues and what version of code to upgrade to.

Bug ID	Summary	Minimum Fixed Version
AOS-196325	MM rebooted due to Multiple UCM Module crash	FCS8.5.0.0.patch.07
AOS-195546	Ensure delay delete logic do not add duplicate entries	FCS8.5.0.0.patch.07

AOS-200535	IPv6: MDNS process crashed on multiple 7240XM MDs	Not yet in patch FCS8.5.0.7 - Available in FCS 8.5
AOS-199715	No limit on ip address list for airgroup client cause memory consumption to go high	Not yet in patch FCS8.5.0.7 - Available in FCS 8.5
AOS-196231	Airgroup clients are not able to discover all the servers with Auto Associate AP name	FCS8.5.0.0.patch.07
AOS-195271	amon_serv_fw PROCESS_NOT_RESPONDING_CRITICAL state post upgrading to 8.5.0.3.	FCS8.5.0.0.patch.07
AOS-194813	process "mdns" crash in active VMM running 8.3.0.8 due to memory leak	FCS8.5.0.0.patch.07
AOS-192814	AP information on AG sever does not change after moving Clients to Different role/AP	Not yet in patch FCS8.5.0.7 - Available in FCS 8.5
AOS-191549	Unable see Apple TVs in AOS in 8.4.0.3	Not yet in patch FCS8.5.0.7 - Available in FCS 8.5
AOS-188697	mdns crash observed on MM controller while reload with build 8.6.0.0-mm-dev_70959	FCS8.5.0.0.patch.07