ArubaOS 8.0.0.0

aruba

a Hewlett Packard
Enterprise company

Release Notes

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at dl-gplquery@arubanetworks.com.

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 04	Updated the list of supported AP platforms for Clarity Synthetic.
Revision 03	Added 210 Series access points to list of supported AP platform.
Revision 02	Added note to backup ArubaOS 6.x configuration and rebuild configuration in ArubaOS 8.0 if upgrading from ArubaOS 6.x to ArubaOS 8.0.
Revision 01	Initial release.

ArubaOS 8.0.0.0 is a major release that includes new features and enhancements.

Throughout this document, branch controller and local controller are termed as managed device.

Use the following links navigate to the corresponding topics:

- New Features and Enhancements on page 8 describes the new features and enhancements introduced in this release of ArubaOS.
- Supported Hardware Platforms on page 26 describes the hardware platforms supported in this release of ArubaOS.
- Regulatory Updates on page 28 lists the regulatory updates in this release of ArubaOS.
- Known Issues on page 29 lists the issues identified in this release of ArubaOS.

Supported Browsers

The following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or later on Windows Vista, Windows 7, Windows 8, and Mac OS
- Apple Safari 5.1.7 or later on Mac OS

Related Documents

The following guides are part of the complete documentation for the Aruba user-centric network:

- *ArubaOS Release Notes*
- *ArubaOS Quick Start Guide*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- *ArubaOS 8.x Syslog Message guide*
- *ArubaMobility Master Licensing Guide*
- *Aruba Mobility Master Installation Guide*
- *Aruba VMC Installation Guide*
- *Aruba Wireless Access Point Installation Guide*

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	licensing.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

This chapter describes the features and/or enhancements introduced in ArubaOS 8.0.0.0 release.

Mobility Master Architecture

ArubaOS 8.0 is a brand new centralized, multi-tier architecture that provides a clear separation between management, control, and forwarding functions. Mobility Master takes the place of a master controller in the network hierarchy. A single Mobility Master or a cluster of Mobility Masters oversee controllers that are co-located (on-premise local controllers or off-campus branch office local controllers). Each Mobility Master cluster is referred to as a Mobility Master domain. All the controllers that connect to Mobility Master act as managed devices. In a large campus, there may be multiple Mobility Master domains.

The entire configuration for both the Mobility Master and managed devices is set up from a centralized point, thereby simplifying and streamlining the configuration process. Mobility Master consolidates all-master, single master-multiple local, and multiple master-local deployments into a single deployment model. In contrast, the ArubaOS 6.x and earlier release trains run on a flat configuration model containing global and local configurations. Global configurations are applied to the master controller and can only be propagated to each local controller through the master. The respective local configurations are applied directly to each master or local controller.

The goal of Mobility Master is to develop a platform that achieves the following:

- Reduces complexity of configuring and managing WLAN deployments.
- Hosts services that run with a central view of the network.
- Assimilates and provides access to the context and data available in the network infrastructure.
- Provides rich APIs that create an ecosystem to build custom applications (in-house/custom/third party), connecting the application intelligence with network intelligence.
- Is highly available and can scale elastically using VM and clustering techniques.

Platform and Server Specifications

Mobility Master runs on a virtual machine that is deployed through an OVF/OVA file. ArubaOS 8.0 only supports VMware ESXi Hypervisor.

The following items must be in place before Mobility Master can be deployed:

- vSphere Client 5.1 or 5.5 must be installed on a Windows machine.
- vSphere Hypervisor 5.1, 5.5, or 6.0 must be installed on the server.
- An OVF/OVA template must be accessible from the ESXi host.

Minimum server requirements include:

- Quad Core i5 1.9 GHz processor with hyper-threading
- 8GB RAM
- Two physical Network Interface Controller (NICs)
- Total CPU, memory, and network throughput utilization must be less than 80% of the host capacity

Minimum Virtual Machine Manager (VMM) requirements include:

- Three vCPUs
- 8GB memory
- 60GB disk space
- Four virtual NICs

Limitations

ArubaOS 8.0 includes the following limitations:

- Mobility Master only supports VMware ESXi Hypervisor.
- Certain VMware features, such as vMotion and DRS, are not supported.
- CPU oversubscription is not supported.
- A maximum of four network adapters are supported.
- Promiscuous mode must be enabled on the vSwitch to avoid address resolution protocol (ARP) issues.

Controllers may be upgraded from ArubaOS 6.x to ArubaOS 8.0, but non-disruptive seamless upgrade is not supported. The configuration from ArubaOS 6.x is not maintained after upgrading to ArubaOS 8.0 because the ArubaOS 8.0 configuration model is different from the ArubaOS 6.x configuration model. After upgrading to ArubaOS 8.0, a controller boots with default configuration. Hence, it is recommended to take a backup of the ArubaOS 6.x configuration as a reference to re-configure the controller in ArubaOS 8.0.

New Features

AirGroup

Define Number of Hops

To support location based sharing, AirGroup allows an administrator to define the number of hops or the neighborhood of access points an AirGroup server is shared with. An administrator can define the hop count as 1, 2, 3, or no neighborhood.

Disallowed Named VLANs

Named VLANs can be used to configure disallow VLAN policy for AirGroup devices.

Improved Scaling

AirGroup can scale to support up to 100,000 devices in which up to 17,000 servers can exist.

Disallowed VLANs

AirGroup extends support for disallowed VLAN policy for users in addition to servers.

Disallowed Role

AirGroup extends support for disallowed role policy for servers in addition to users.

AirGroup Dashboard

The **AirGroup** dashboard provides enhanced visibility into AirGroup, displaying the following information:

- Traffic trends
- Server distribution
- Server and user bandwidth

The combined view of all AirGroup devices and usage in the network is available under the **AirGroup** dashboard of Mobility Master.

AP-Platform

Novatel U620L Modem Support

ArubaOS 8.0 introduces the support of the Novatel U620L 4G LTE USB modem for Verizon's LTE service on the RAP-3WN, RAP-108, RAP-109, RAP-155P, AP-205H, 210 Series, 220 Series, and 320 Series access points.

Plug and Play 4G USB Modem

ArubaOS 8.0 supports the USB modem Plug and Play. The Mobility Master auto-configures the 4G USB modem as soon as the user plugs in the modem into an AP or a RAP. The following 4G USB modem supports Plug and Play:

- Netgear AirCard 340U (AT&T)
- Netgear AirCard 341U (Sprint)
- Franklin Wireless U770 (Sprint)
- Pantech UML290 (Verizon)
- Pantech UML295 (Verizon)
- Novatel MC551L (Verizon)

- Novatel U620L (Verizon)

AP Configuration

AP Health Checks

The AP Health check feature uses ping probes to check reachablility and latency levels for the connection between the AP and the managed device. The recorded latency information appears in the output of the **show ap ip health-check** command. If the managed device IP address becomes unreachable from the AP uplink, this feature records the time that the connection failed, and saves that information in a log file (tmp/ap_hcm_log) on the AP.

Support for Port Bounce for APs

Mobility Master provides support for the port bounce feature which enables a client to re-initiate a DHCP request when there is a VLAN change. This is achieved when a RADIUS server such as ClearPass Policy Manager sends Disconnect-Request with a Vendor Specific Attribute (VSA 40) to Mobility Master. Then, Mobility Master forwards the request to the device to trigger an interface shut down for a specified period. This allows the device to re-initiate a DHCP request for obtaining an IP address in the changed subnet.

AppRF 2.0

Defining Custom Applications and Application Categories

Creating custom application and application categories is supported on the Mobility Master. The custom application can be associated with custom application categories This will enable to customers to apply a policy for this category so that multiple applications associated with this category can receive the same policy.

Protocol Data Definition (PDD) based Application Signatures

With the new protocol signature set, the pdd based signature definitions could be leveraged for hit-less upgrade of the managed devices.

Centralized Image Upgrade

Centralized image upgrade allows an administrator to initiate and upgrade the images on Mobility Master and the managed devices in a unified way. Centralized image upgrade provides a detailed view of the image upgrade progress over the WebUI or the CLI. Centralized image upgrade affects only the managed devices that are active at the time of the upgrade. Centralized image upgrade uses the configuration hierarchy by taking implicit parameters from the Mobility Master or the managed devices form where the image upgrade is executed or where the affected managed device is located in the hierarchy.

Centralized Visibility Backend Support for WebUI

ArubaOS 8.0 uses a centralized, multi-tier architecture under a new UI that provides a clear separation between management, control, and forwarding functions. The entire configuration for both the Mobility Master and managed devices is set up from a centralized point, thereby simplifying and

streamlining the configuration process. Mobility Master consolidates all-master, single master-multiple local, and multiple master-local deployments into a single deployment model.

Controller Clustering

Cluster

Clustering is based on keeping client processing, that is, signaling and traffic, anchored to a managed device regardless of which AP the client roams to, as long as the AP is within the control scope of the cluster. Since, the client is fixed at a given managed device, a single Basic Service Set (BSS) on an AP can now have clients that are anchored at multiple managed devices.

- The cluster size can reach up to 12 managed devices to support very large campus deployments. It supports 7200 Series, 7000 Series, and VM platforms. Cluster supports all the cluster-related GSM channels on 7000 Series and VM platforms. Cluster setup supports RAPs and IPv6 clients.
- The client load is shared by all the managed devices and there is a larger roaming domain with smaller fault domain which helps with faster recovery.
- Enhanced Multicast Proxy feature is an integral part of the cluster setup.
- Session State Synchronization feature resolves all issues regarding seamless roaming, service availability, and high availability.
- Cluster supports redundancy for both APs and clients.
- An AP will be able to failover between clusters.
- **AP-Move** feature enables a user to move a specific AP to the target managed device from a specific managed device.

Cluster Dashboard

The **Cluster** dashboard provides a visual overview of each cluster deployed on the network, displaying the following information:

- Health information between cluster members
- Total AP load per Cluster (AAC)
- Total User load per Cluster (UAC)
- Connection time

The **Cluster** dashboard can only be accessed from the root (Managed Network) node of the Mobility Master hierarchy. This information is not displayed on any stand-alone controllers, managed devices, or other nodes in the hierarchy.

Configuration Enhancements

Configuration Auto-Rollback

Mobility Master supports an auto-rollback mechanism that reverts the managed device to the last known good configuration prior to any management connectivity loss. Mobility Master indicates if a device has recovered from a bad configuration through the **show switches** command output. The output for this command labels the **Configuration State** for the managed device as **CONFIG ROLLBACK** if the device has recovered

connectivity using the rollback configuration. When the user fixes the bad configuration on Mobility Master, the managed device recovers automatically, and the state changes to **UPDATE SUCCESSFUL**.

Bulk Edit

The bulk edit support feature enables you to do a bulk configuration in the Mobility Master.

Device Auto-Parking

By default, a device that is not mapped to any configuration node does not receive any configuration. Users can specify a default node to automatically push configurations to such devices using the **configuration device default-node** command.

Disaster Recovery

If auto-rollback from a bad configuration fails, and connectivity between the managed device and Mobility Master remains disrupted, users can enable **Disaster Recovery** mode on the managed device using the **disaster-recovery on** command. **Disaster Recovery** mode grants users access to the **/mm** node directly on a managed device, while blocking any further configuration syncs from Mobility Master. With full control of the **/mm** node, users can make local modifications on each managed device to restore connectivity to Mobility Master.

Controller-Platform

SDN Controller

The Software Defined Networking (SDN) Controller introduces an improved networking infrastructure to build, deliver, and manage features through the following enhancements:

- Separation of control-plane and data-plane functions
- Centralized manageability
- Dynamic programmability of network devices

The SDN Controller is comprised of the following modules:

- **Southbound Interface**: The Southbound Interface is a collection of drivers that handles communication to all data-plane elements (DPE) in the network.
- **Platform Services**: SDN Platform Services gather and build the information required for core controller functions, such as host discovery and routing.
- **Northbound API**: The Northbound API makes the information built from the SDN Controller available for applications through both synchronous (REST) and asynchronous (ZMQ) APIs.

OpenFlow Agent

OpenFlow agent runs on network devices such as Switches, Routers, Wireless Controllers and APs. This interacts with a centralized SDN Controller using the OpenFlow protocol. The OpenFlow agent translates OpenFlow commands into device specific actions.

For OpenFlow to be functional in a network, you must enable SDN Controller on the Mobility Master and OpenFlow agent on the required Managed devices. By default, OpenFlow is disabled on Mobility Master as well as the managed devices.

Database Migration to Postgres

The MySQL databases used in the ArubaOS 6.x and earlier release trains have been migrated to the Postgres database. The Postgres database, which is available in both hardware and x86-based platforms, maintains data and performs functions for the following applications/features:

- WLAN Management System (WMS)
- STM
- Auth
- AirGroup Manager
- License Manager
- IAP Manager
- Managed devices

The branch whitelist that is maintained in the MySQL database is translated to a managed device whitelist on Mobility Master, which corresponds with the devices that have been added to the configuration hierarchy.

Disable Console Access

A new command, **mgmt-user console-block**, is introduced to disable the console-login. The purpose of this command is to introduce an ability to lock down all console ports, for example, micro USB, mini USB on the managed device to enable high-level security. This also ensures that no Secure Shell (SSH) access is allowed at the remote branch office. The SSH is only allowed from the headquarters through the IPsec tunnel.

Remote Telnet or SSH Session from Mobility Master

Starting from ArubaOS 8.0, an administrator can initiate a remote telnet or SSH session from Mobility Master to a remote host. The host can be a managed device or a non-Aruba host.

Whitelist Management for APs and Managed Nodes

Zero touch provisioning (ZTP) automates the deployment of APs and managed devices plug-n-play. The managed device learns the local configuration, global configuration, and license limits from Mobility Master and provisions itself automatically. ZTP offers the following advantages over a standard configuration:

- simple deployment
- reduced operational cost

- limits to provisioning errors

Managed devices that are configured using ZTP automatically discover the Mobility Master, download the local configuration from that Mobility Master, and are provisioned with the corresponding device role and country code. After the managed device is provisioned, it can obtain its global configuration in one of two ways:

- The administrator enters the global configuration via the WebUI or CLI of the Mobility Master.
- The managed device retrieves its global configuration from the Mobility Master.

Seamless Logon

The Seamless Logon feature enables you to login from the Mobility Master to a managed device without entering a password. The user can remotely login from a centralized location (Mobility Master) to any managed device and execute the show and action commands.

PortFast Support for AP's Access Ethernet Port

In ArubaOS 8.0.0.0, the PortFast feature has been enhanced to reduce the time taken for wired clients connected to an AP to detect the link before data traffic is sent.

IPv6

IPsec IPv6

Starting from ArubaOS 8.0, IPsec support is enhanced to accommodate IPv6 which includes overlay networks across IPv4 and IPv6 IPsec Tunnels. IPsec is the base for security features like Site-to-Site VPNs, CPsec, RAP, and Master-Local deployments. The control plane handles the configuration of these features and translation to IPsec Security Association. The data plane handles encryption / decryption, encapsulation / decapsulation, tunneling, session setup, management, and routing of IPsec data.

In this release, IKEv2/IPsec support is extended to IPv6 for the following topologies:

- Mobility Master
- CPsec (Tunnel Mode only)
- RAP (Tunnel Mode only)
- Site-to-Site Crypto Map (Tunnel Mode only)

Prefix Delegation

Starting from ArubaOS 8.0, prefix delegation can be used to assign a network address prefix to a customer site, as defined in IPv6 prefix delegation protocol (RFC 3769). The hosts at the customer site use this prefix to derive a unique IPv6 address using RA and SLAAC. Prefix delegation client uses DHCPv6 IA_PD to request and assign prefixes.

Licensing Changes

ArubaOS 8.0 introduces new licenses, and deprecates previously supported licenses.

New Licenses

A license is required to install ArubaOS on a server VM, instead of an Aruba controller. There are three different license types that are used for VM installations only.

- **VM**: Required to install a managed node local controller (LC) on a VM.
- **VM-PEFV**: Required to apply firewall policies to clients using a VPN to connect to the VM controller.

Deprecated Licenses

The **xSec** license is deprecated in ArubaOS 8.0. In previous releases, one xSec license was required for each active client termination using Extreme Security (xSec), a secure tunneling network protocol implemented over the 802.1X protocol. ArubaOS 8.0 supports xSec features in the base operating system, without any additional license requirements.

License Support for Mobility Master

The procedure to generate a license for a 7000 Series controller uses the controller's serial number to create a license key can be used only by that device. When you obtain a VM license to install on a VM, you are provided with a unique serial number that must be added to the server when you configure the VM. A new CLI command, **show license passphrase**, is introduced in ArubaOS 8.0. Use the passphrase shown in the output of this command in conjunction with the VM serial number to generate unique license keys for a VM controller.

You must enable support for sharable ArubaOS licenses by enabling each licensing feature type via the Mobility Master command-line interface. Enabling a licensing feature in Mobility Master activates all licenses of that type in all licensing pools, allowing managed devices to use that licensing feature. Starting in ArubaOS 8.0, you add licenses to a managed node by adding the license to Mobility Master, and then associating that license to either a specific managed node, or a shared pool of licenses. Licenses cannot be added directly to a managed node.

If a controller had previously installed sharable licenses before it was added to Mobility Master as a managed node, those licenses are no longer usable on the managed node. Those license keys must be regenerated and assigned to a managed node or licensing pool using the Mobility Master WebUI.

Managed Devices

WAN Interface Bandwidth Priorities

ArubaOS supports minimum bandwidth guarantees per traffic class, and allows critical delay-sensitive applications like voice and video to use more bandwidth and/or be scheduled with higher priority. Each interface can be associated with a scheduler profile, that supports four queues with different priority levels. If you use session ACLs to define traffic policies on the managed node, you can use the scheduler profile to automatically associate these different priority levels assigned by these policies to a scheduler profile queue.

Uplink Load Balancing

A managed node supports multiple 3G cellular uplinks in addition to its standard wired ports, providing redundancy in the event of a connection failure. WAN traffic can be balanced across two or more active uplinks from a managed device to a VPN concentrator (VPNC). The uplink load balancing feature supports both active and standby uplinks, so the traffic load can be balanced across two wired uplinks, even while the backup cellular uplink remains idle.

Other Features

AP Termination on Mobility Master

Mobility Master cannot be used as an AP Master since APs are not allowed to terminate on the Mobility Master. If the AP manager on a Mobility Master receives an AP HELLO message, the message is dropped.

Loadable Service Module

The Loadable Service Module (LSM) provides an infrastructure that allows users to dynamically upgrade or downgrade individual service modules without requiring an entire system reboot. Services are delivered as individual service packages containing the version and instructions for loading and running the service. Service modules must be upgraded if there is a bug in the existing module or a newer version of the module has been released.

The following service modules are LSM-capable:

- AirGroup
- AppRF
- ARM
- AirMatch
- NBAPI
- UCM
- WebCC
- WMS

MultiZone

The MultiZone feature allows AP to terminate to multiple managed devices that reside in different zones. A zone is a collection of managed devices under a single administration domain.

Local Termination of the WMS Service

If a managed device is installed at a location with strict bandwidth limitations and in a network topology where the managed device is geographically away from another managed device terminating APs, WMS services can be configured to locally terminate on the managed device instead of

terminating on Mobility Master. Enable this feature with caution, as it may impact WMS device classification and IDS detection and protection on your network.

Customized Response

This feature allows you to add customized messages that will be displayed in the case of an authentication failure.

Support for Secondary Managed Device

The secondary managed device feature in ArubaOS 8.0.0.0 provides seamless connectivity by allowing an access point to terminate on a secondary managed device in the event of the primary managed device failing.

ARM Channel Planning Enhancements

Starting from ArubaOS 8.0.0.0, the following enhancements have been made to resolve issues that occur with the distributed channel/power algorithm that updates APs associated to a stand-alone controller:

- **Push random channel assignments to APs:** Random channels are pushed from the controllerStation Management and System AP Manager processes to APs that belong to a specific ap-group. This replaces the dynamic channel change solution in a high-density environment, thereby overcoming the issue with convergence.
- **Reduce interference channel change:** To reduce the number of interference channel changes and to configure the weight of interfering APs when calculating the interference index, the **interfering-ap-weight** parameter has been introduced in the **rf-arm-profile** command.

Protecting Against Adhoc Networks Using Valid SSID

Protection from adhoc networks using valid SSID involves containing the adhoc networks that use a valid or protected SSIDs so that clients cannot connect to it. This feature provides protection against WPA/WPA2/WEP/open adhoc networks.

Role-based Access and Authorization

Starting from ArubaOS 8.0, Mobility Master provides support for a new default role, **ap-provisioning**. Users assigned with this role have access only to AP provisioning commands.

Clarity Synthetic

Clarity Synthetic enables the controller to select and convert a supported access point to client mode based on the instruction from a Network Management System (NMS). The converted AP acts like a Wi-Fi client and starts synthetic data transaction within the network to monitor and detect the network health.

Clarity Synthetic provides support for the following AP platforms:

- 200 Series access points
- 210 Series access points
- 220 Series access points

Support for Self-Signed Certificate

Starting from ArubaOS 8.0, Mobility Master provides support for generating a new self signed certificate (**default-self-signed**) to demonstrate the authentication of the managed device for captive portal and WebUI management access while booting.

The **default-self-signed** certificate is the default certificate used by Mobility Master and managed devices.

RF Management

AirMatch RF Management

AirMatch is the next generation radio resource management service introduced in ArubaOS 8.0. AirMatch provides RF network resource allocation with unprecedented quality. It analyzes the past 24 hours of RF network statistics, and proactively optimizes the network for the next day. Any RF plan change is applied in the early morning to minimize client disruption and to maximize the user experience. AirMatch can react to detrimental RF events such as radar and high noise levels, to allow the network to manage sudden changes in the RF environment.

The AirMatch channel and EIRP optimization features deprecate the channel planning and EIRP optimization features in the legacy Adaptive Radio Management (ARM) feature. AirMatch is supported on Mobility Master only, while legacy ARM channel optimization and EIRP features continue to be supported by stand-alone controllers running ArubaOS 8.0.

AirMatch channel planning evens out channel distributions in any size of network, and in any subset of the contiguous network (as much as allowed by the network configuration, regulatory domain and AP hardware capability). AirMatch also minimizes channel coupling, where adjacent radios are assigned to the same channel. The computing power of Mobility Master impacts channel distribution calculations, so channel coupling may occasionally be allowed in complex networks to keep the computing time practical. The more powerful the processing power of the Mobility Master server, the less channel coupling will be allowed by AirMatch.

AirMatch EIRP planning automatically considers the local density of the network to manage the APs' coverage and modulation and coding scheme (MCS) operation, and optimizes EIRP changes across neighboring AP radios in order to offer users the best roaming experience.

AirMatch Vs. ARM Comparison

Table 3 describes some of the differences between the channel and EIRP optimization features supported by ArubaOS 8.0 AirMatch and ArubaOS 8.0 ARM.

Table 3: *AirMatch and ARM features in ArubaOS 8.0*

Features	AirMatch	ARM
Initial Release	ArubaOS 8.0	ArubaOS 2.x

Features	AirMatch	ARM
Supported Topology	Mobility Master / Managed device	Stand-alone controller
Run Period	24 hours	As little as 5 minutes
RF information used	Past 24 hours of RF data	Instantaneous snapshot of the RF environment
Deployment Time	5 AM (by default) , or any time necessary	Any time necessary
Computing Time	10 seconds to 1 hour, depending upon network size	Less than 1 second
Optimization Scope	The entire RF network	Each individual AP

AirMatch Database and RF Calculations

Each AP in a Mobility Master deployment measures its RF environment for a five minute period, every 30 minutes. The AP then sends the managed device AMON messages about the radio feasibility based on that AP's hardware capability, cell size, regulatory domain, and RF neighbors. The managed device forwards these messages to Mobility Master, and the Mobility Master adds this information to a database, computes an optimal solution, and deploys the latest RF plan by sending updated settings to the APs every 24 hours. By default, this configuration update is sent at 5 AM (as per the Mobility Master system clock), but time of this configuration update can be modified via the AirMatch profile.

The database for the AirMatch service is empty when Mobility Master first boots up. When Mobility Master first detects APs on the network, it enters its initial optimization phase, collects data from all the APs, and generates an incremental solution every 30 minutes, for next eight hours. When this initial eight-hour period has elapsed, the AirMatch service calculates a new RF configuration for these devices every 24 hours.

When a new AP is deployed on a network with an active Mobility Master during the initial 8-hour AirMatch optimization phase, that AP joins the network with its preassigned channel and transmission power values. The AirMatch service detects the newly deployed AP on the network, it restarts its RF computations, and sends an incremental RF configuration update to the new AP 30 minutes later. APs added to the network after the initial 8-hour optimization period will not receive an additional RF configuration update until the next scheduled update period.

Incremental Rules-Based Client Match Updates

The client match feature continually monitors a client's RF neighborhood to provide ongoing client bandsteering and load balancing, and enhanced AP reassignment for roaming mobile clients. ArubaOS 8.0 supports incremental updates to Client Match rules to support network devices running newer operating systems that may be incompatible with the existing Client Match client association rules. This feature allows the controller to use a newer set of client match rules without updating the entire operating system, reducing network downtime.

Unified Communication and Collaboration

UCC Application in ArubaOS 8.0

Starting from ArubaOS 8.0, UCM runs as a loadable service module on Mobility Master. UCC supports various applications like Apple FaceTime, Alcatel-Lucent New Office Environment (NOE), Microsoft® Lync/Skype for Business, Cisco Jabber, Cisco Skinny Call Control Protocol (SCCP), Spectralink Voice Priority (SVP), SIP, H.323, Vocera, and Wi-Fi Calling. UCC application on Mobility Master implements the VoIP Application Layer Gateway (ALG) to support both encrypted and non-encrypted VoIP protocols. UCC application uses the OpenFlow infrastructure to receive the signaling messages from the managed devices and also install and delete flows on the managed devices for calls made.

In addition, UCC is supported on a stand-alone controller.

UCC Features in Mobility Master

ArubaOS 8.0.0.0 introduces the following UCC features:

Cisco Jabber

Mobility Master provides QoS and visibility for voice, video calls, and desktop-sharing sessions made using an unencrypted version of the Cisco Jabber client. UCM can uniquely identify and prioritize Cisco jabber voice, video calls, and desktop-sharing sessions.

Multi-ALG Support

In ArubaOS 8.0.0.0, multiple applications running simultaneously on the same client device can be identified and prioritized. A maximum of 10 applications running simultaneously on client device is supported. The multi-ALG feature is enabled by default in Mobility Master.

Intelligent Call Handling

ArubaOS 8.0.0.0 replaces Call Admission Control with Intelligent Call Handling (ICH). ICH monitors the channel utilization of all radios of the APs on the managed device. If the channel utilization exceeds beyond a configurable threshold on a radio, new UCC calls are not prioritized. This is to ensure that existing calls on the radio are not penalized due to a new call when channel utilization is very high. ICH is enabled by default and applies to all ALGs supported by UCM.

RTP Analysis

Mobility Master performs RTP analysis for most VoIP ALG calls in both downstream (at AP) and upstream direction (at managed device) and captures the quality metrics. The downstream UCC score measures call quality between the AP and the wireless client in the downstream direction. The upstream UCC score measures call quality over the wired network between the AP and the managed device in the upstream direction. The quality metrics captured is applicable for all the active sessions belonging to the same or different ALG running on that client.

AppRF Integration with ALGs and User Role

The QOSMOS engine does not recognize many of the UCC applications. For the ones it recognizes, it does not maintain the state of the application. Due to this limitation, it cannot provide granular visibility into the UCC applications. To resolve this limitation, in ArubaOS 8.0, voice ALGs identify the

application type for supported UCC applications, so that the administrator can now use AppRF rules to deny, permit, apply QoS, or rate limit UCC application traffic.

In addition, the following features are introduced:

- Enables VoIP ALGs to run as a service on Mobility Master and managed devices need not run the same. This results in better scalability.
- Supports Loadable Service Module. UCM is a Loadable Service Module. ALGs are completely decoupled from the managed devices. This enables faster innovation of VoIP services such as introduction of new ALGs and enhancements to existing features as they will become independent of the ArubaOS release version.
- Provides a solution to the fanout problem in Lync/Skype for Business SDN API. In ArubaOS 6.x, Lyn/Skype for Business SDN Manager sent call information messages to every local controller in the network, regardless of whether the local controller is involved in the call or not. This additional processing is an unnecessary overhead on the local controller. In addition, the bandwidth utilization between the data center and remote location is not efficient. With the Mobility Master deployment, Lync/Skype for Business SDN Manager sends the call information messages to Mobility Master only.
- Provides aggregation of statistical information at a centralized entity.

UCC Changes in ArubaOS 8.0.0.0

The following is a list of UCC changes from ArubaOS 6.x to ArubaOS 8.0.0.0:

- In ArubaOS 6.x, VoIP ALGs run on the respective local controllers that parse the signaling messages, dynamically opens sessions in firewall, prioritizes traffic, and provide visibility. In ArubaOS 8.0.0.0, VoIP ALGs do not run from the managed devices. They run as an application on Mobility Master. In a stand-alone controller deployment, the VoIP ALGs run on the stand-alone controller itself.
- UCC running on Mobility Master uses OpenFlow infrastructure to receive signaling packets on Mobility Master, parse them, open sessions in the firewall, and prioritizes them.
- Visibility for all supported UCC applications are provided from the centralized Mobility Master dashboard.
- Unlike ArubaOS 6.X, where ALGs use Wi-Fi Multimedia-Differentiated Services Code Point (WMM-DSCP) mappings in the WLAN SSID profile to set the Type of Service (ToS) for Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP), Mobility Master has ALG-specific Quality of Service (QoS) configurations.

UCC Features Deprecated in ArubaOS 8.0.0.0

The following are the features deprecated in ArubaOS 8.0.0.0:

- Basic Service Set (BSS) transition and force BSS transition.
- Call count, bandwidth, and Traffic Specification (TSPEC)-based call admission control.
- Classify media action in ACL for media classification – Microsoft® Lync/Skype for Business calls will automatically get prioritized without the need for classify media ACLs.
- SIP session timer
- SIP dial plans
- WMM-DSCP override setting in the SSID profile

- Stateful ALG settings in global firewall options. These settings are now available in Mobility Master under the **Configuration > System > Profiles > All Profiles > UCC** profile.
- Lync/Skype for Business traffic control profile
- Web Server port configuration for Lync/Skype for Business SDN API. The Mobility Master uses 32000 as the default port now.
- The **Monitoring** tab in the WebUI.
- The **show voice** commands.
- **sip-authentication-role** parameter in AAA profile.
- **voice-aware** parameter in AAA authentication 802.1X profile.

WebUI

Configuration Hierarchy

Mobility Master contains a centralized, multi-tier architecture that provides a clear separation between management, control, and forwarding functions. The entire configuration for both the Mobility Master and managed devices is set up from a centralized point, simplifying and streamlining the configuration process. Mobility Master consolidates all-master, single master-multiple local, and multiple master-local deployments into a single deployment model.

The following enhancements have been introduced for the Mobility Master configuration model:

- Multi-tier configuration hierarchy
- Centralized configuration
- Centralized validation
- Efficient configuration distribution
- ZTP and branch support
- Multi-version support
- Recovery mechanisms for connectivity loss
- Centralized licensing
- New parser and CLI infrastructure
- Improved user interface
- Northbound APIs

Configuration User Interface

The Mobility Master user interface runs on a flat hierarchy profile design that provides ease-of-use through a simple navigation model. The Mobility Master UI contains the following enhancements:

- **Multi-Level Menu**: The Mobility Master menu is divided into Level-1 items and Level-2 items. Each Level-1 item can be expanded to display the corresponding Level-2 items. Each Level-2 item is further expanded to organize and group content on the work-screen.
- **Profile Configuration Interface**: The profile configuration model is based off a single-page, flat hierarchy architecture, in which only a portion of the page is updated based on the action performed. The left-navigation panel, headers, and footer remain constant throughout all changes and selections, while only the work-screen is updated based on the menu, tab, and profile selections.
- **Primary and Secondary Tables**: Mobility Master presents data and configuration information through primary and secondary tables. Primary tables display the main object of the page, while secondary tables provide more in-depth information on a specific primary table entry.
- **Pending Changes**: When a user saves or submits a configuration change, the configuration is pushed to the **Pending Changes** zone of Mobility Master. Modifications are not applied to the network until all pending changes are deployed.
- **Help Mode**: Users can enable help mode to view help information for configuration fields.
- **Hierarchy Management**: The Mobility Master UI allows users to create, modify, and delete all hierarchical nodes from a central location. When a node is selected from the network hierarchy, users are directed to the corresponding configuration profile. Any configuration changes made across the UI are executed and applied to the selected node.

Enhancements

Authentication

Support for IKE Fragmentation

ArubaOS 8.0 supports the functionality where non-Aruba devices can fragment the large IKE_AUTH packets using the standards described in the **RFC 7383 – Internet Key Exchange Protocol Version 2 (IKEv2) message fragmentation** when the Aruba device acts as a responder and not as an initiator.

IPv6

Radius Accounting for IPv6 Clients

Starting from ArubaOS 8.0, customers can monitor bandwidth usage by clients/hosts with IPv6 addresses, over RADIUS protocol. The **Framed-IPv6-Address** attribute is used in accounting start, stop, and interim packets. A host can have multiple IPv6 addresses and all of them are tracked to check the usage, for billing purpose.

Firewall

Routing Traffic through Web Proxy

When the Mobility Master needs to access data on the cloud or the internet, and if the internet bound traffic needs to pass through a proxy, execute the **web-proxy server** command. Once the command is executed the Mobility Master routes web (HTTP/HTTPS) traffic through the proxy server.

Redirect User Session

The **block-redirect-url** command has been introduced to redirect a user session to an URL when it encounters a WebCC deny policy.

Managed Node Health Checks

If the managed device health check feature is configured to use **UDP** probe mode, the WAN health checks can measure jitter on the connection to the remote host by sending and measuring packets at fixed intervals.

Unified Communication and Collaboration

Wi-Fi-Calling

Mobility Master provides QoS for voice calls made using Wi-Fi Calling. UCM in Mobility Master can identify and prioritize calls made using Wi-Fi Calling. UCM also provides visibility for all voice calls made using Wi-Fi Calling.

WAN Enhancements

Health Check

The WAN health check feature uses ping-probes to measure WAN availability and latency on selected uplinks. Based upon the results of this health-check information, the managed device can continue to use its primary uplink, or failover to a backup link. If the health check feature is configured to use **UDP** probe mode, the WAN health check feature can measure jitter on the connection to the remote host by sending and measuring packets at fixed intervals.

Cellular Handoff Assist

When both the Client Match and the cellular handoff assist features are enabled, the cellular handoff assist feature can help a dual-mode, 3G/4G-capable Wi-Fi device such as an iPhone, iPad or Android client at the end of a Wi-Fi network switch from Wi-Fi to an alternate 3G/4G radio that provides better network access. This feature is supported by iOS and Android devices only.

WebUI

Blocked Session

The **Blocked** tab in **Dashboard Monitoring > Traffic Analysis** page displays WebCC and AppRF sessions which are blocked by ACL through system logging. This tab is available when logged into the managed device.

Web-CC Database

The Web-CC database is downloaded to the Mobility Master and the managed devices access the Web-CC database from the Mobility Master.

This chapter describes the hardware platforms supported in ArubaOS 8.0.

Controller Platforms

The following table displays the controller platforms supported in ArubaOS 8.0.

Table 4: *Supported Controller Platforms in ArubaOS 8.0*

Controller Family	Controller Model
7000 Series	7005, 7008, 7010, 7024, 7030
7200 Series	7205, 7210, 7220, 7240, 7240XM

AP Platforms

The following table displays the AP platforms supported in ArubaOS 8.0.

Table 5: *Supported AP Platform in ArubaOS 8.0*

AP Family	AP Model
90 Series	AP-92, AP-93
—	AP-93H
—	AP-103, AP-103H
100 Series	AP-104, AP-105

AP Family	AP Model
110 Series	AP-114, AP-115
130 Series	AP-134, AP-135
200 Series	AP-204, AP-205
—	AP-205H
210 Series	AP-214, AP-215
220 Series	AP-224, AP-225
—	AP-228
270 Series	AP-274, AP-275, AP-277
320 Series	AP-324, AP-325
—	RAP-155, RAP-155P
RAP 100 Series	RAP-108, RAP-109
—	RAP-3WN, RAP-3WNP

This topic lists the Downloadable Regulatory Table (DRT) file version introduced in ArubaOS 8.0.0.0.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller Command Line Interface (CLI) and execute the **show ap allowed-channels country-code <country-code> ap-type <ap-model>** command.

For a complete list of countries certified with different AP models, refer to the DRT release notes at support.arubanetworks.com.

The following default DRT file version is part of ArubaOS 8.0.0.0:

- DRT-1.0_55489

This chapter describes the issues identified in ArubaOS 8.0.0.0.

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
119532	**Symptom:** The **Operational State** of a VLAN ID is shown as **N/A** in the WebUI although the operational status of the VLAN ID is up. **Scenario:** This issue is observed in a Mobility Master running ArubaOS 8.0. **Workaround:** Use the **show vlan status CLI** command.	WebUI	All platforms	ArubaOS 8.0
120199	**Symptom:** The user is unable to create the same management user for different nodes. **Scenario:** In a node hierarchy, when a management user is created for one node and again created for another node, the first entry is deleted. This issue is observed in a Mobility Master running ArubaOS 8.0. **Workaround:** None.	Authentication	All platforms	ArubaOS 8.0
120673	**Symptom:** After a masterip is configured on a managed device, the user is unable to remove the masterip configuration. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0. The masterip of a managed device cannot be removed, but only modified. Modifying the masterip erases the configuration on the managed device and the managed device reboots. After the managed device reboots and connects to a new Mobility Master, the configuration of the managed device is downloaded from the Mobility Master. In ArubaOS 8.0, factory reset the managed device to change its role. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.0
127454	**Symptom:** The **Per-VLAN AirGroup control** table in the WebUI does not show all entries.	AirGroup	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
	Scenario: This issue occurs when a set of VLANs are allowed/disallowed in AirGroup. This issue is observed in Mobility Master and stand-alone controllers running ArubaOS 8.0. **Workaround:** Manually make a whitelist db entry on the Mobility Master.			
127731	**Symptom:** Although Auto Cert Provisioning is enabled, AP does not come up in a Data zone device if there is no CPsec whitelist entry. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0. **Workaround:** Manually make a whitelist db entry on the Mobility Master.	AP-Platform	All platforms	ArubaOS 8.0
129826	**Symptom:** MultiZone AP on the Data Zone is unable to take the channel from Primary Zone. **Scenario:** This issue occurs when the wireless driver beacons on the channel that is provided in the Primary Zone. This issue is observed in managed devices running ArubaOS 8.0. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0
130055	**Symptom:** A user is unable to configure IP Mobile Active List Domain under in the mynode configuration node of the Mobility Master. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** The IP Mobile Active List Domain should be configured under the device configuration node.	Mobility	All platforms	ArubaOS 8.0
130088	**Symptom:** Existing VLANs are not displayed under **Virtual-AP** profile in the **Configuration > Controller > Profile** page of the WebUI. **Scenario:** This issue is observed in Mobility Master, managed devices, and stand-alone controllers running ArubaOS 8.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
130121	**Symptom:** In the **Configuration > Access Points > Whitelist** page of the WebUI, a user cannot filter the CPsec and RAP whitelist database entries based on the column names. **Scenario:** This issue is observed in the **Managed Network** node hierarchy in Mobility Master running ArubaOS 8.0. **Workaround:** Use the following CLI command with appropriate filters: `(host) [mynode] # show whitelist-db cpsec <filter>`	WebUI	All platforms	ArubaOS 8.0
130161	**Symptom:** Cluster specific logs are displayed in the AP console when the user tries to establish a tunnel with the stand-alone Data zone device. **Scenario:** This display issue is observed in managed devices running ArubaOS 8.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0
130735	**Symptom:** AP is **UP** in the Primary zone device with **Z** flag, if the Data zone and the Primary zone IPs are similar in the managed devices. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0. **Workaround:** Provide the appropriate configuration, as this is a misconfiguration issue.	AP-Platform	All platforms	ArubaOS 8.0
130741	**Symptom:** Chromecast applications do not work when AirGroup is enabled on a Mobility Master. **Scenario:** This issue occurs because of changes to how the Google cast supported applications query for Chromecast. This issue is observed in Mobility Master and stand-alone controllers running ArubaOS 8.0. **Workaround:** None.	AirGroup	All platforms	ArubaOS 8.0
131117	**Symptom:** Although the total number of nodes have reduced to 12, the status of the AP is still set to **L** flag. **Scenario:** This issue is observed in a MultiZone mode when the total number of nodes are greater than 12. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
131133	**Symptom:** When the primary Local Mobility Switch (LMS) is down, AP does not failover to the backup LMS. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0 only in MultiZone mode, with Backup LMS configured. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0
131390	**Symptom:** Client is deauthenticated due to inconsistency in the bucket map. **Scenario:** Load balancing algorithm is not functional when a Data zone with more than 12 zones is marked with an **L** flag and is disabled. This issue is observed in managed devices running ArubaOS 8.0. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0
132544	**Symptom:** Wi-Fi Calling ALG continues to prioritize an already ended Wi-Fi call. Due to this, the CDR record remains active even after a call has ended. **Scenario:** This issue is occasionally observed on Apple iPhones. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0
133304	**Symptom:** A user is unable to assign static IP to a RAP using the WebUI. **Scenario:** This issue occurs because the Sample CSV file that is used to upload in the WebUI does not support static IPs for RAP. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** Configure static IPs for RAPs individually using the following CLI command: `(host) [mynode] (config) #whitelist-db rap add mac-address <mac> ap-group <ap-group-name> ap-name <name> description <text> remote-ip <static-ip-address>`	WebUI	All platforms	ArubaOS 8.0
135939	**Symptom:** An option to create netdestination from the WebUI is not available. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0.	WebUI	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
	Workaround: Configure netdestination using the following CLI commands: **For IPv4—** `(host) [mynode] (config) #netdestination <name>` **For IPv6—** `(host) [mynode] (config) #netdestination6 <name>`			
137890	**Symptom:** The following unclear error message is displayed when trying to edit a local user database entry from the **Configuration > Authentication > Internal Server** page of the WebUI: **Invalid Input, input should be a time** **Scenario:** This issue occurs when the local user database entry has the expiration duration value as a number format in the **Time (mins)** field. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** Enter the time duration in **hh:mm** format.	WebUI	All platforms	ArubaOS 8.0
138254	**Symptom:** The client which is not involved in UAC failover gets deleted after the flapped uplink of this client's UAC is up. The log files for the event listed the reason as **observed ip_user delete** in Mobility Master. **Scenario:** This issue occurs when shut is performed on the standby-UAC, and the sta/user/mac user/ip user entries are activated on the standby-UAC because it looses connectivity with the active UAC. This issue is observed in a cluster setup in Mobility Master running ArubaOS 8.0. **Workaround:** The workaround is as follows: • Decrease the user idle timer to 30 secs in the cluster setup. • Once shut is performed, wait for at least a minute before performing no shut. This helps stabilizing the cluster environment.	Base OS Security	All platforms	ArubaOS 8.0
139098	**Symptom:** An SNMP-server trap configuration is not disabled when the **no snmp-server trap** command is executed. **Scenario:** This issue occurs because most snmp-server trap configurations are enabled by default but they do not contain any configuration. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	SNMP	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
139138	**Symptom:** When OpenFlow profile is configured on a stand-alone controller, no error is displayed. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0. **Workaround:** None.	SDN-Platform	All platforms	ArubaOS 8.0
139330	**Symptom:** Access points are operating in deleted channels. **Scenario:** This issue occurs when the commands for deleting the channels from the regulatory domain profile are working, however, these changes are not getting updated in the managed devices. This issue is observed in managed devices running ArubaOS 8.0. **Workaround:** Configure the profile first and then, remove unwanted channels after profile is pushed from the Mobility Master.	Configuration	All platforms	ArubaOS 8.0
139994	**Symptom:** On executing the **show ucc client-info** command, the **ap-name** field for a Remote AP is displayed as **NA**. **Scenario:** This issue is seen when a wired client is connected to a RAP in split-tunnel forwarding mode. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0
140664	**Symptom:** An AP crashes unexpectedly. **Scenario:** This issue occurs when control plane security is enabled. This issue is observed in AP-225 access points connected to a managed device running ArubaOS 8.0. **Workaround:** None.	AP-Wireless	All platforms	ArubaOS 8.0
140678	**Symptom:** The SNMP CLI commands are not case sensitive. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	SNMP	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
140686	**Symptom:** The CLI commands are case sensitive. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** The **disallow-role** and **disallow-vlan** CLI commands take role name and VLAN name. Ensure that they match the case mentioned in the configuration.	AirGroup	All platforms	ArubaOS 8.0
141640	**Symptom:**The WebUI navigation freezes when a user clicks on the **?** icon on the top right corner of the **Configuration** page in the WebUI. **Scenario:** By clicking on the **?** icon, some of the WebUI fields are supposed to turn green indicating that the mouseover help is enabled. However, there is no indication of enabling the help system because the help system is not completely integrated into the **Configuration** pages of the WebUI. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** Click on the **?** icon once again to unfreeze the WebUI navigation.	WebUI	All platforms	ArubaOS 8.0
141641	**Symptom:**The mouse over help system is not enabled upon clicking the **?** icon on top right corner of the **Configuration** pages in the WebUI. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0
141856	**Symptom:** The buddy list disappears from the messages application. **Scenario:** This issue occurs when AirGroup and chat service are enabled in Mobility Master running ArubaOS 8.0. **Workaround:** Disable AirGroup.	AirGroup	All platforms	ArubaOS 8.0
141859	**Symptom:** In a rare case, the managed device fails to program datapath for a few New Office Environment (NOE) clients. **Scenario:** When an NOE client initiates a call, the NOE ALG fails to prioritize the call and set the application ID. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
141986	**Symptom:** The banner text does not appear in the WebUI **Logon** page though it is visible in the Command Line Interface. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0
142041	**Symptom:** Data Zone on the Mobility Master displays standby IP for the MultiZone APs that are down. **Scenario:** This issue occurs when the Mobility Master does not remove the standby IP even after removing the MultiZone profile from the Primary Zone. This issue is observed in Mobility Master running ArubaOS 8.0 in a MultiZone topology. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0
142097	**Symptom:** User session terminates and the user is automatically logged out **Scenario:** This issue is observed when the user is on any page of Dashboard and when the WebUI remains idle for longer than the set Idle Timeout value. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0
142334	**Symptom:** The original Wi-Fi Multimedia (WMM) and Differentiated Services Code Point (DSCP) values are not displayed for remote Lync/Skype for Business calls. **Scenario:** This issue is observed when two Lync/Skype for Business clients connected to a RAP initiate a call in split-tunnel forwarding mode. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0
142463	**Symptom:** Clients are disconnected and reconnected randomly. **Scenario:** This issue is observed when the radio on the Data Zone Mobility Master is enabled or disabled resulting in resetting of the Basic Service Set (BSS). This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
142737	**Symptom:** Remote AP (RAP) fails to reestablish the tunnel in Ethernet uplink. **Scenario:** RAP establishes tunnel using cellular uplink (with USB modem) where cellular link has higher priority than Ethernet link. When the USB modem from RAP is physically plugged out, the RAP takes very long (5 to 30 mins or even more) to establish the tunnel on Ethernet uplink. The issue persists even with Mobility Master providing the public IP address or FQDN in the AP provisioning profile attached to the AP group. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	Remote Access Point	All platforms	ArubaOS 8.0
142771	**Symptom:** Mobility Master incorrectly tags a few calls as **ICH-deny** even when the channel utilization is lesser than the threshold limit. **Scenario:** This issue is intermittently observed in a cluster deployment. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0

142987	**Symptom:** The option to disable dynamic map is not available in the **IKEv1** or **IKEv2 IPSEC Dynamic Maps** section under the **Configuration > Services > VPN** page of the WebUI.
	Scenario: This issue is observed in Mobility Master running ArubaOS 8.0.
	Workaround: Use the following CLI command to disable dynamic map for IKEv1/IKEv2 policies:
	`(host) [mynode] (config) #crypto dynamic-map <dynamic-map-name> <dynamic-map-num>`
	`(host) [mynode] (config-submode)#disable`
		WebUI	All platforms	ArubaOS 8.0

143009	**Symptom:** In a stand-alone setup, the grace period for license expiry is not displayed for WebCC. **Scenario:** The status of WebCC is shown as **Active** even when the license is in grace period. This issue is observed in all platforms except the Mobility Master running ArubaOS 8.0. **Workaround:** None.	Licensing	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
143135	**Symptom: IP address** field fails to accept IPv6 address. **Invalid IPv4** error is displayed. **Scenario:** This issue is observed when IPv6 address is used to create tacacs server in **Authentication > authserver**. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** Configure from CLI.	WebUI	All platforms	ArubaOS 8.0
143138	**Symptom:** A client may drop a call when it roams to another managed device when both IP mobility and RTP analysis is enabled. **Scenario:** When RTP analysis is enabled, the roamed client's audio RTP traffic fails to get tunneled from foreign agent to home agent. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0
143161	**Symptom:** ACL whitelist fails to display all the default ACLs. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0
143244	**Symptom:** Zone statistics are not segregated in the CLI output for the command, **show ap debug radio-stats ap-name <ap-name> radio <radio name> advanced**. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0. **Workaround:** None.	Station Management	All platforms	ArubaOS 8.0
143276	**Symptom:** When OpenFlow version lower than 1.3 is detected, AirGroup IPv6 flows do not install for the remaining managed devices. **Scenario:** This issue occurs when an OpenFlow enabled managed device is configured with OpenFlow version lower than 1.3. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** Configure the Mobility Master and all managed devices to use OpenFlow version 1.3.	AirGroup	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
143316	**Symptom:** Whitelisting of sites fails to bypass Captive Portal authentication. **Scenario:** This issue occurs when Captive Portal profile is configured with whitelisted sites This issue is observed in VMC and ArubaOS 8.0. **Workaround:** None.	Base OS Security	VMC	ArubaOS 8.0
143439	**Symptom:** Once a session is classified as blocked, it is listed in the blocked session in the UI, even when there is no traffic. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0. **Workaround:** None.	Firewall	All platforms	ArubaOS 8.0
143604	**Symptom:** The managed device is blocked while initializing the CFGM process if the managed device is reloaded when the Mobility Master configuration is in progress. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0. **Workaround:** None.	Configuration	All platforms	ArubaOS 8.0
143813	**Symptom:** The **Trend** graph in the **Dashboard > UCC > Call Quality** page of the WebUI does not display any data. **Scenario:** This issue is seen even when there are active calls. This issue is observed in a stand-alone controller deployment. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0
143826	**Symptom:** In a cluster deployment, media classification fails to classify and prioritize Lync/Skype for Business calls. **Scenario:** This issue is observed if a managed device acts as the User Anchor Controller (UAC) for one user on the call and also as a standby UAC for the other user on the same call. **Workaround:** None.	UCC	All platforms	ArubaOS 8.0
143888	**Symptom:** Unable to configure MAC address for IPsec authentication while setting master IP deployment from managed device.	WebUI	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
	Scenario: This issue is observed in all groups and managed devices in Mobility Master running ArubaOS 8.0. **Workaround:** Configure from CLI using the following command: `(host)[md](config) #masterip 10.15.92.5 ipsec ****** peer-mac-1 00:0C:29:D4:FF:D4 interface vlan 92`			
144140	**Symptom:** Rebootstrap messages from the AP are printed on the Primary zone when the AP rebootstraps on the Data zone. **Scenario:** This issue is observed in managed devices running ArubaOS 8.0 in a MultiZone topology. **Workaround:** None.	AP-Platform	All platforms	ArubaOS 8.0
144517	**Symptom:** Device-level license usage is not displayed in WebUI. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	WebUI	All platforms	ArubaOS 8.0
144520	**Symptom:** A customer defined application name is not supported as **appname** in the **interface gigabitethernet <port> bandwidth-contract app <appname> <bwc>** and **route acl** CLI commands. Only standard application names are supported. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0
144602	**Symptom:** Unable to add Management-user, Certificate Management-user and local-user-guestdb users from WebUI in Edge browser. **Scenario:** This issue is observed because the + symbol is missing is these sections in WebUI when using the Edge browser. In general, Edge browser is partially supported in ArubaOS 8.0. **Workaround:** Use a different browser like IE 11, Chrome, and Firefox.	WebUI	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
144883	**Symptom:** The multicast traffic is not forwarded to a client. **Scenario:** This issue occurs when IGMP proxy is disabled and no multicast VLAN is configured. When the UAC is changed (AAC and UAC are different for the client) because of cluster client load balancing feature, multicast traffic is not forwarded to a client. This issue is observed in cluster topology in ArubaOS 8.0. **Workaround:** None.	Multicast	All platforms	ArubaOS 8.0
145042	**Symptom:** A customer defined application (custom-app) does not work. **Scenario:** This issue occurs in a Mobility Master with multiple managed devices that are part of a cluster. This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** None.	Controller-Datapath	All platforms	ArubaOS 8.0
145328	**Symptom:** The startup script does not migrate the **airgroupservice disable** command. **Scenario:** This issue is observed in Mobility Master running ArubaOS 8.0. **Workaround:** Migrate the **airgroupservice disable** command manually.	AirGroup	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
145330	**Symptom:** The startup script does not parse an airgroupservice name with more than one word. **Scenario:** This issue is observed when an airgroupservice name with more than a word is migrated. Only the first word in the airgroupservice name is migrated. **Workaround:** Migrate the service names with more than one word manually.	AirGroup	All platforms	ArubaOS 8.0
145331	**Symptom:** Managed Devices using the **ip nat outside** configuration with uplink VLAN losses connectivity to the Mobility Master. **Scenario:** This issue is observed when **ip nat outside** is not part of the **interface vlan** command and as a result the configuration related to **ip nat outside** is not collected by the **interface vlan** command. Listed below are some of the reasons due to which this issue is observed: • **show configuration committed** does not display this line of configuration even though it is configured and saved accurately in the memory under an interface VLAN. • If a managed device's initial configuration contains **ip nat outside** then this line of configuration is not part of device's complete configuration file downloaded from the Mobility Master to the managed device. • When **ip nat outside** is added to a configuration node on the Mobility Master, only the existing managed devices will receive this configuration; new devices added after this will not receive the complete configuration when it is downloaded from the Mobility Master. • If a managed device has received **ip nat outside** from a partial configuration update, the configuration will be lost next time the device receives a complete configuration synchronization from the Mobility Master. • For managed devices that has **ip nat outside** configured locally (with local overwrite), the configuration needs to be added again if the managed device is reloaded. **Workaround:** After each reload use local overwrite to directly commit the configuration on the managed device.	Configuration	All platforms	ArubaOS 8.0

Table 6: *Known Issues in 8.0.0.0*

Bug ID	Description	Component	Platform	Reported Version
145516	**Symptom:** A user cannot activate a VM controller with a license generated using the factory installed product serial number. **Scenario:** This issue occurs when a VM controller boots with a factory installed product serial number. This issue is observed in VM controllers running ArubaOS 8.0. **Workaround:** Enter a new product serial number and generate the passphrase and license from the new product serial number manually.	Controller-Paltform	VM controllers	ArubaOS 8.0

Maximum Number of NAT Pools

A controller supports a maximum of 60 NAT pools.