

This document describes resolved issues, new and changed features, and known issues in AirWave 8.0.11 and previous releases. The release notes include the following sections:

- ["What's New in This Release" on page 1](#)
- ["Changes" on page 22](#)
- ["The Support Download Page" on page 27](#)
- ["Supported Infrastructure Devices" on page 27](#)
- ["Fixed Issues" on page 28](#)
- ["Known Issues" on page 56](#)

What's New in This Release

The following enhancements have been added in AirWave 8.0.11:

- ["IAP-324 and IAP-325 Support" on page 2](#)

The following issues have been resolved in AirWave 8.0.10.1:

- ["Issues Fixed in AirWave 8.0.10.1" on page 29](#)

The following issues have been resolved in AirWave 8.0.10:

- ["Issues Fixed in AirWave 8.0.10" on page 30](#)

The following enhancements have been added in AirWave 8.0.10:

- ["Third-Party Device Support in AirWave 8.0.10" on page 3](#)
- ["Aruba Instant Configuration Enhancements" on page 3](#)
- ["Instant 4.2.1 Feature Support" on page 3](#)
- ["Firmware Upgrade Failure Timeout " on page 4](#)

The following enhancements have been added in AirWave 8.0.9.2:

- ["AP-324 and AP-325 Support" on page 4](#)

The following enhancements have been added in AirWave 8.0.9.1:

- ["CentOS Update" on page 4](#)

The following enhancements have been added in AirWave 8.0.9:

- ["Firmware Distribution Over HTTP" on page 4](#)
- ["Aruba Instant 4.2" on page 5](#)
- ["Aruba Instant 4.1.2.0" on page 6](#)
- ["Instant Whitelist Database Enhancements" on page 6](#)
- ["Brocade Network Advisor Support " on page 7](#)
- ["Third-Party Device Support in 8.0.9" on page 7](#)

The following enhancements have been added in AirWave 8.0.8.1:

- ["Licensing Enhancements" on page 7](#)

The following enhancements have been added in AirWave 8.0.8:

- ["Aruba Mobility Access Switch Enhancements in ArubaOS 7.3. or Earlier" on page 8](#)

- "Aruba Mobility Access Switch Enhancements in ArubaOS 7.3.1.0 or Later" on page 8
- "Aruba Mobility Access Switch Enhancements in ArubaOS 7.3.2.0 or Later" on page 9
- "Aruba Mobility Access Switch Enhancements in ArubaOS 7.4.0.0 or Later" on page 9
- "Juniper Device Monitoring Enhancements" on page 11
- "RF Health Report Enhancements " on page 15
- "VisualRF Enhancements in HTML5" on page 19

The following enhancements have been added in AirWave 8.0.7:

- "New Supported Devices" on page 22
- "VisualRF Support for Third-Party Devices " on page 12
- "Instant Improvements " on page 15
- "RF Health Report Enhancements " on page 15
- "HTTP Request Retry Attempts" on page 16
- "MIB Improvements" on page 16

The following enhancements have been added in AirWave 8.0.6:

- "Third-Party Device Support " on page 12
- "UCC Dashboard Improvements " on page 15
- "New Configuration API " on page 15

The following enhancements have been added in AirWave 8.0.5:

- "Instant Improvements " on page 15
- "Mobility Access Switch Support Enhancements" on page 16

The following enhancements have been added in AirWave 8.0.4:

- "Instant Improvements " on page 15
- "Bulk Editing of the Switching File " on page 16
- "Site to Site IKE " on page 17
- "API for Streaming Raw Records " on page 17

The following enhancements were added in AirWave 8.0.x releases prior to AirWave 8.0.4.

- "Usage Column in AP Table " on page 17
- "Support for SCP for Aruba Firmware Upgrades " on page 17
- "Creating Custom Filtered Views " on page 17
- "VisualRF Support for Third-Party Devices " on page 12
- "AppRF Enhancements" on page 19
- "UCC Visibility" on page 20
- "Additive Licensing" on page 21
- "Client Health Graph" on page 21

IAP-324 and IAP-325 Support

Beginning with AirWave 8.0.11, AirWave supports the IAP-324 and IAP-325 access points.

Third-Party Device Support in AirWave 8.0.10

Cisco

Support for stacking of the Cisco 3650.

HP

Added support for the following HP devices:

- MSM-775 controller
- HP425 AP
- HP560 AP
- HP-350 AP
- HP-355 AP
- HP-365 AP
- HP-385 AP
- 1910, 1920, and 1950 series Comware switches

Aruba Instant Configuration Enhancements

AirWave 8.0.10 introduces the following Instant configuration enhancements:

- In order to reduce confusion when using the Instant GUI configuration, AirWave now makes it clear whether the user is making changes at the group level or virtual controller level. When a specific virtual controller is selected, on the **AirWave** link is highlighted and the remaining links are greyed out. If the user clicks on one of the grayed-out links, AirWave will prompt the to continuing working at the virtual-controller level or not. If the user clicks **OK**, the grayed-out links become highlighted. If the user clicks **Cancel**, the user is moved to the group level to continue configuration.
- Uplink configuration is now supported at the group level.
- Configuration template for thin IAPs. Prior to 8.0.10, template configuration for Instant only applied to virtual controllers. To create a thin IAP virtual controller template, navigate to **Group > Template** and use the **Aruba Instant Thin AP (Any Model)** option.
- AirWave now calculates the uptime of a device based on the actual uptime of the device, not just the time that the device is connected to the AMP.
- Existing clients with an unknown device type are now automatically updated when AirWave's OUI table is updated.
- The **Overrides** tab in the IGC has been update. Overrides are now displayed as a list of CLI commands that from the group configuration per virtual controller. Additionally, a **Remove All Overrides** button has been added at the virtual controller level to remove all overrides configured on the specified virtual controller.
- The IGC supports uplink configuration at the group and virtual controller levels.

Instant 4.2.1 Feature Support

AirWave 8.0.10 introduces support for the following Instant 4.2.1 features in IGC. For more information about each of these features, see the *Aruba Instant 6.4.3.4-4.2.1.0 User Guide*.

- **Dynamic Proxy for RADIUS and TACACS:** IGC now supports dynamic proxy for RADIUS and TACACS. To enable this feature in IGC, navigate to **System > General > Dynamic Proxy** and check the **RADIUS** and/or **TACACS** check boxes and click **OK**.
- **Deauth of Inactive Clients:** Instant can now be configured to deauth clients when they become inactive. To configure this feature in IGC, navigate to **Networks > General > Show Advanced Options >**

Miscellaneous and select **Enabled** from the **Deauth inactive clients** drop-down menu. This feature is disabled by default.

- **Time Based Services:** You can configure time range profiles using the IAP UI and CLI. These Time Range Profiles can be enabled on an IAP to allow or deny access to an SSID only during a specific period of time. You can create different types of time profiles, namely:
 - **Periodic:** The SSIDs and user roles will be provided access to the websites periodically within the specified time range. The user needs to select the **Period type** (day/weekday/weekend/daily) and the time range (**Start Time** and **End Time**) to create the periodic profile.
 - **Absolute:** The SSIDs and user roles will be provided access to the websites only during the specified date and time duration.
- **XML-API Server Configuration Enhancement:** You can now configure up to 8 XML API server entries on IAP. You can also create XML API requests with appropriate authentication commands.
- **DHCP Enforcement:** You can now block traffic for IAP clients that do not obtain IP address from DHCP by selecting **Enable** under **Networks > General > Enforce DHCP** in the IGC.
- **Very High Throughput Configuration:** You can now enable or disable Very High Throughput (VHT) function on devices that support VHT. VHT is enabled by default on 802.11ac series IAPs. However, you can disable VHT if you want the 802.11ac IAPs to function as 802.11n IAPs. You can configure VHT on SSID or a 5 GHz radio profile. If you enable or disable VHT on an SSID, the configuration is applicable only to the clients connecting through that SSID. To disable or enable VHT on all SSIDs, configure VHT on the 5 GHz radio profile.
- **Minimum RSSI:** You can now configure the minimum Received Signal Strength indicator (RSSI) for probe and auth requests. The minimum can be specified between 0 and 100 dB.
- **Deny Inter User Bridging:** you can disable bridging traffic between two clients connected to the same AP on the same VLAN if you have security and traffic management policies defined in upstream devices.
- **Cellular SIM PIN Locking:** IAPs support SIM PIN lock function for 3G/4G modems that support the SIM locking feature to prevent fraudulent use. The IAP can now lock and unlock the SIM PIN using the **pin-enable** and **pin-puk** parameters in the **per-ap-settings** of the Instant configuration template.
- **Ethernet Type for L2 ACL:** Ethernet is now a configureable value in L2 ACLs and traffic can now be filtered based on the Ethernet field in the frame header.

Firmware Upgrade Failure Timeout

Beginning with AirWave 8.0.10, you can configure the amount of time AirWave continues to retry a firmware upgrade after a failure. The timeout limit range is from five minutes to 60 minutes. To configure this option, navigate to **AMP Setup > General > Firmware Upgrade/Reboot Options**.

AP-324 and AP-325 Support

Beginning with AirWave 8.0.9.2, AirWave supports the AP-324 and AP-325 access points.

CentOS Update

Beginning with AirWave 8.0.9.1, the AirWave software installation package is bundled with CentOS 6.6.

Firmware Distribution Over HTTP

Beginning with AirWave 8.0.9, firmware distribution over HTTP is disabled by default. To enable this feature, navigate to **AMP Setup > General > Firmware Upgrade/Reboot Options** and select the **Yes** radio button for the **Enable firmware distribution via http** option.

This change impacts upgrades from Instant 4.0 and lower. Enable this feature before upgrading from Instant 4.0 or lower.

Aruba Instant 4.2

AirWave 8.0.9 introduces support for Instant 6.4.3.x-4.2.0.0, also known as Instant 4.2. The following enhancements have been added to support Instant 4.2:

- **Support for Multiple XML API Server Configuration:** Users can now configure up to four XML API server entries on an IAP. These server entries can be edited or deleted if required. To configure this feature for a virtual controller or group of virtual controllers, navigate to **Instant Config > Services > Network Integration**.
- **Prevent Inter-user Bridging:** If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same AP on the same VLAN. When inter-user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision. To find this option in the IGC, navigate to **Networks > New Network > General > Show advanced options > Deny inter user bridging**.
- **RadSec Certificate Support:** You can now upload RadSec and RadSec CA certificates to the IAP. These certificates are used for client authentication when RADIUS communication over TLS is enabled. To access this feature, navigate to **Instant Config > Security > Authentication Servers > New** or **Edit**.
- **Dell Service Tag for IAPs:** The **APs/Devices > Monitor** tab displays the Dell Service tag for Dell Networking W-Series IAPs running Instant 4.2.



This feature is not supported by some earlier W-Series IAP models, including the IAP-92, IAP-93, IAP-104, IAP-105, IAP-114, IAP-115, IAP-134, IAP-135, RAP-155, RAP-155P, IAP-175, RAP-3WN and RAP-3WNP.

- **Inactivity Timeout:** This feature allows you to specify a session timeout interval in seconds, minutes or hours. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. You can specify a value within the range of 60-86400 seconds (24 hours) for a client session. The default value is 1000 seconds. To access this feature, navigate to **Instant Config > Networks**, then selected **Wired** for **Type** and click **Show advanced options**.
- **Creating Custom Error Page for Web Access Blocked by AppRF Policies:** You can create a list of URLs to redirect users to when they access blocked websites. You can define an access rule to use these redirect URLs and assign the rule to a user role in the WLAN network. To find this option in IGC, navigate to **Security > Custom Blocked Page URL > New**.
- **Voice Traffic Prioritization:** In the 6.4.3.x-4.2 release, IAPs comply with Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification to ensure interoperability and high performance between Spectralink 84-Series, 87-Series, and 8020/8030 Wireless Telephones and WLAN infrastructure products. You can configure the following parameters in a WLAN SSID profile for voice traffic and Spectralink Voice Prioritization:
 - **Traffic Specification (TSPEC)**—Prioritizes time-sensitive traffic such as voice traffic initiated by the client.
 - **TSPEC Bandwidth**—Reserves bandwidth for voice traffic.
 - **Spectralink Voice Protocol (SVP)**—Prioritizes voice traffic for SVP handsets.To find these options in IGC, navigate to **Networks > New Network > General > Show advanced options > WMM**.
- **Captive Portal Server Offload:** This feature enables the external captive portal to reduce the load on the Portal server. This load on the external captive portal server by ensuring that the non-browser client applications are not unnecessarily redirected to the external portal server. To find this option in IGC, navigate to **Security > External Captive Portal > New**.
- **Configurable Transmission Power Limits for Radio Profiles:** The **Customize ARM power range** option is added to the radio profile configuration window to allow administrators to set transmit power limits for a specific radio band. To find this option in the IGC, navigate to **RF > Radio**.

- **Accounting Server Configuration in Wired Profiles:** You can now configure accounting servers for a wired network profile. You can either use the same server for authentication and accounting, or configure a separate accounting server. To enable accounting for wired profile users, configure an accounting server and set an accounting interval. To find this option in the IGC, navigate to **Networks > New Network > Security** and select the authentication server from the drop-down menu.
- **DNS IP Configuration for Virtual Controller:** You can explicitly configure the DNS IP address for Virtual Controllers. IAPs can obtain their DNS IP addresses from per AP configuration (**ip-address** command), from the DHCP server, or from the Virtual Controller DNS IP address configuration. The Virtual Controller DNS IP address is only used for APs and does not apply to the clients connected to the APs. To find this option in the IGC, navigate to **System > General** and then select a virtual controller. Then change the **Virtual Controller network settings** drop-down menu to **Custom** and complete your configuration.
- **Configuring Multiple Exclusion Ranges of IP Subnets:** IAPs now allow you to configure multiple exclusion ranges of IP subnets in a local, L2 DHCP profile. Based on the size of the subnet and the configured exclusion range, the IP addresses before and after the defined range are excluded. To find this option in the IGC, navigate to **DHCP Server > New** and enter the IP Range in the **IP Address Range** fields.
- **Configurable USB Port Status:** IAPs now allow you to set the USB port status to **enabled** or **disabled** based on your uplink preferences. If you do not want to use cellular uplink or 3G/4G USB modems in your current network, set the USB status to disabled. By default, the USB port status is enabled. To find this option in the IGC, navigate to **Access Points**, select an AP from the list, and then click **Uplink**.

Instant 6.4.3.x-4.2 does not support the IAP-92 and IAP-93.

For more information about the features and enhancements in Instant 4.2, refer to the following documents:

- *Aruba Instant 6.4.3.x-4.2 User Guide*
- *Aruba Instant 6.4.3.x-4.2 Quick Start Guide*
- *Aruba Instant 6.4.3.x-4.2 Release Notes*

Aruba Instant 4.1.2.0

AirWave 8.0.9 introduces support for Instant 6.4.2.3-4.1.2.0.

Instant Whitelist Database Enhancements

The Instant whitelist database is a list of the Instant APs that are allowed to access the AMP server after completing pre-shared key or certificate authentication. AirWave 8.0.9 allows network administrators to download Instant AP data from their Aruba Activate account directly into the Instant AP whitelist database.

To import Instant AP data from Activate to the AMP server:

1. Navigate to **AMP Setup > General > Automatic Authorization**.
2. In the **Authorize Aruba Instant APs connecting to AirWave** section, click **Whitelist**.
3. Next, navigate to Click **Import Instant AP Whitelist from Activate**. The **Activate Settings** page opens.
4. Configure the Activate settings to allow AirWave to access Instant AP data on the Activate server.

AirWave imports Instant AP data over a secure (HTTPS) connection. After AirWave receives the data from Activate, a status message appears at the top of the **Activate Settings** window in AirWave, describing the number of Instant APs added to or updated in the whitelist database, and the number of Instant APs removed from the whitelist database.



For more information on configuring the Instant AP whitelist, refer to the *Aruba Instant in AirWave Deployment Guide*.

Brocade Network Advisor Support

In AirWave 8.0.9, AirWave supports Brocade Network Advisor. Once integrated, a link to the Network Advisor is listed on the **Switch Monitoring** page in the **Device Info** section.

To integrate Brocade Network Advisor with AirWave:

1. Log in to AirWave.
2. Navigate to **AMP Setup > External Server**.
3. Enter the IP Address or Hostname of the Brocade Network Advisor.
4. Click **Save**.

Third-Party Device Support in 8.0.9

AirWave 8.0.9 introduces monitoring support for the following devices:

HP

- MSM417
- MSM425
- MSM525
- MSM527
- MSM560
- 830 Unified Wired-WLAN Switch
- 850 Unified Wired-WLAN Switch
- 870 Unified Wired-WLAN Switch
- 7500 Switch Series
- 10500 Switch Series



AirWave supports these devices for monitoring only, not configuration. These devices are also not currently supported by VisualRF.

Cisco

The Cisco 3850/3650 acting as a switch.

Licensing Enhancements

AirWave 8.0.9 introduces the following licensing enhancements:

License Expiration Email Notifications

For licenses with an expiration date, the administrator can configure email messages to notify specified parties of when a license is set to expire. AirWave sends an expiration notification email six months, three months, one month, and one week prior to expiration. Additionally, the email lists time remain for each expiring license installed on the AMP. This feature is disabled by default.

To configure Expiry Notifications:

1. Navigate to **Home > License > Expiry Notification Settings**.
2. Check the **Receive Email Notifications** check box to enable.
3. Insert any number of email addresses separated by spaces, commas, or semicolons.
4. Click **Save**.

New Single Device License

AirWave 8.0.9 introduces support for the LIC-AW license SKU. This new license represents a single device monitored by AirWave.

Subscription License

AirWave 8.0.9 introduces support for three new subscription-based license SKUs. These licenses are available in one, three, and five year subscriptions.

The new SKUs are:

- SUB1-AW-K12: One-year license
- SUB3-AW-K12: Three-year license
- SUB5-AW-K12: Five-year license

Aruba Mobility Access Switch Enhancements in ArubaOS 7.3. or Earlier

AirWave 8.0.8 introduces the following enhancements to support for Aruba MAS devices:

Bulk Override

Destination Prefix, **Destination Prefix Mask**, and **Next-Hop Address** are now support bulk override for Aruba MAS devices running version 7.3 or earlier. These are modified under **Groups > Switch Config > Layer 3 Features > IP** in the AMP.

Aruba Mobility Access Switch Enhancements in ArubaOS 7.3.1.0 or Later

AirWave 8.0.8 introduces the following enhancements to support for Aruba MAS devices running ArubaOS 7.3.1.0 or later:

802.1x Authentication Profile

Deny DHCP support in the **802.1x Authentication Profile** for devices running version 7.3.1.0 or later. To configure Deny DHCP:

1. Navigate to **Groups > Switch Config > Security & Authentication > 802.1x**.
2. Click **Add**.
3. Select **Yes** to enable or **No** to disable deny DHCP.

Deny DHCP is disabled by default.

Delay EAP Success support in the **802.1x Authentication Profile** for devices running version 7.3.1.0 or later. To configure Delay EAP Success:

1. Navigate to **Groups > Switch Config > Security & Authentication > 802.1x**.
2. Click **Add**.
3. Select **Yes** to enable or **No** to disable delay EAP success.

This feature is disabled by default.

Web SSH Management Profile

Enable or disable Webserver in the **Web SSH Management** profile for devices running 7.3.1.0 or later. To enable or disable Webserver:

1. Navigate to **Groups > Switch Config > System Features > Web Server**.
2. Click **Yes** to enable or **No** to disable Webserver in the **Enable Webserver** field.
3. Click Save to complete the configuration. This feature is enabled by default.

Enable or disable Captive Portal Ports in the **Web SSH Management Profile** for devices running 7.3.1.0 or later. To enable or disable Captive Portal Ports:

1. Navigate to **Groups > Switch Config > System Features > Web Server**.
2. Click **Yes** to enable or **No** to disable Captive Portal Ports in the **Enable Captive Portal Ports (8080/8081)** field.
3. Click **Save** to complete the configuration. This feature is enabled by default.

Aruba Mobility Access Switch Enhancements in ArubaOS 7.3.2.0 or Later

AirWave 8.0.8 introduces the following enhancements to support for Aruba MAS devices running ArubaOS 7.3.2.0 or later:

Aruba Central

Aruba Central support for Aruba MAS Devices running version 7.3.2.0 and later. To enable Aruba Central Configuration in AirWave:

1. Navigate to **Groups > Switch Config > System Features > General Config > Aruba Central Configuration**.
2. Select **Yes** to enable or **No** to disable.
3. Click **Save**. This feature is enabled by default.

BPDU Filtering Support

BPDU filtering support in the **Rapid-PVST+ Port Profile** for devices running version 7.3.2.0 or later. To configure BPDU filtering in the AMP:

1. Navigate to **Groups > Switch Config > Layer 2 Features > STP > Rapid-PVST+ > Interface Config**.
2. Click **Add**.
3. Select **default** or **unconditional** from the drop-down menu next to the **BPDU Filter** option.
4. Click **Add** to complete the configuration.

BPDU filtering support in the **MSTP Port Profile** for devices running version 7.3.2.0 or later. To configure BPDU filtering in the AMP:

1. Navigate to **Groups > Switch Config > Layer 2 Features > STP > MSTP > Interface Config**.
2. Click **Add**.
3. Select **default** or **unconditional** from the drop-down menu next to the **BPDU Filter** option.
4. Click **Add** to complete the configuration.

Storm Control Bandwidth Range

The storm control bandwidth range has been increased to 1-100. The default value is still 50. This feature is modified in the AMP under **Groups > Switch Config > Layer 2 Features > Switchport**.

Aruba Mobility Access Switch Enhancements in ArubaOS 7.4.0.0 or Later

AirWave 8.0.8 introduces the following enhancements to support for Aruba MAS devices ArubaOS 7.4.0.0 or later:

Aruba-VPN Pools Profile

Aruba-VPN Pools profile configuration support for devices running version 7.4.0.0 or later. To add a new Aruba-VPN Pool profile:

1. Navigate to **Groups > Switch Config > System Features > DHCP > Aruba-VPN Pools**.
2. Click **Add**.

3. Fill in the fields to complete the configuration.

Deny Inter User Traffic in a User Role

Deny Inter User Traffic support in a **User Role** for devices running version 7.4.0.0 or later. To configure Deny Inter User Traffic:

1. Navigate to **Groups > Switch Config > Security & Authentication > User Roles**.
2. Click **Add** to create new role or selecting an existing role to edit.
3. Select **Yes** to enable or **No** to disable deny inter user traffic in the **Deny Inter User Traffic** field.

Deny Inter User Traffic is disabled by default.

Device-Group Profile

Device-Group profile configuration support for devices running version 7.4.0.0 or later. To add a Device-Group profile:

1. Navigate to **Groups > Switch Config > Interfaces > Device-Group**.
2. Fill in the fields to complete the configuration.

Dynamic DNS Client Profile

Dynamic DNS Client profile configuration support for devices running version 7.4.0.0 or later. To configure a Dynamic DNS Client profile:

1. Navigate to **Groups > Switch Config > Layer 3 Features > Dynamic DNS Client**.
2. Click **Add**.
3. Populate the fields relevant to your configuration.
4. Click **Add** to complete the configuration.

IGMPv3 Snooping

Support for **IGMPv3 Snooping** configuration on devices running version 7.4.0.0 or later. To enable configure **IGMPv3 Snooping** in the AMP:

1. Navigate to **Groups > Switch Config > Multicast Features > IGMP Snooping (v1/v2)**
2. Click **Add** or select an existing IGMP snooping profile.
3. For both **IGMPv3 Snooping** and **IGMPv3 Snooping Proxy**, select **Yes** to enable or **No** to disable in the appropriate field.

This feature is disabled by default.

Invert and Range Options

The **Invert** and **Range** options under **Groups > Switch Config > Security & Authentication > Network Aliases > Destination** have been removed.

NAT Pool

NAT Pool configuration support for devices running version 7.4.0.0 or later. To configure a NAT Pool profile in the AMP:

1. Navigate to **Groups > Switch Config > Security & Authentication > NAT Pools**
2. Click **Add**.
3. Configure the NAT Pool completing the UI fields.
4. Click **Add** to complete the configuration.

Probe Profile

The **Probe** profile for L3 interface monitoring configuration support for devices running version 7.4.0.0 or later. To add a new Routed VLAN Interface profile:

1. Navigate to **Groups > Switch Config > Layer 3 Features > Probe**.
2. Click **Add**.
3. Fill in the fields to complete the configuration.

Rogue Containment Profile

Rogue AP Containment profile configuration support for devices running version 7.4.0.0 or later. To add a new Rogue AP Containment profile:

1. Navigate to **Groups > Switch Config > System Features > Rogue AP Containment**.
2. Complete the configuration.
3. Click **Save**.

Route Metrics

Support for route metrics for DHCP Client-enabled L3 Interfaces on devices running version 7.4.0.0 or later. To configure **Interface Metrics**:

1. Navigate to **Groups > Switch Config > Interfaces > Routed VLAN Interfaces**.
2. Enter value between 0 and 65535 in the **Interface Metric** field.
3. Click **Add** to complete the configuration.

By default, the value is set to 0.

Route VLAN Interfaces Profile

Routed VLAN Interface profile configuration support for devices running version 7.4.0.0 or later. To add a new Routed VLAN Interface profile:

1. navigate to **Groups > Switch Config > Interfaces > Routed VLAN Interfaces**.
2. Click **Add**.
3. Fill in the fields to complete the configuration.

Standby Interface VLAN

Standby Interface VLAN configuration support on devices running version 7.4.00 or later. To configure a **Standby VLAN Interface** in the AMP:

1. Navigate to **Groups > Switch Config > Security & Authentication > Virtual Private Networking > IPSEC > IPSEC MAP**.
2. Click **Add** or select an existing IPSEC Map.
3. Select an interface VLAN from the drop-down menu next to **Standby Interface VLAN** or click the **plus (+)** symbol to configure a new one.
4. Click **Add** to complete the configuration.

Juniper Device Monitoring Enhancements

AirWave 8.0.8 introduces the following for Juniper devices:

- A tab on the AMP Setup page has been renamed from **Third Party Integration** to **Juniper**. A link to Network Director appears on the **Switch Monitoring** page: [Link to Juniper Network Director](#).
- dot11 counters on the Juniper WLAN

- The collection of CPU and memory information from Juniper switches. This information is displayed on the monitoring page of the switch and can be included in reports and triggers.

In AirWave 8.0.7, AirWave supports Juniper Network Director (ND) 2.0. Once integrated, a link to the ND is listed on the **Switch Monitoring** page in the **Device Info** section. Clicking the link redirects the user to the ND UI, where they are prompted for ND login credentials. Users are redirected to the URL

https://<nd>/mode=Monitor&deviceip=<x.x.x.x>.



Currently, AMP does not have visibility into devices managed in ND. ND will display an error if a device with IP address is not found.

To integrate ND with AirWave:

1. Login to the AMP.
2. Navigate to **AMP Setup > External Server**.
3. Enter the IP Address or Hostname of the ND.
4. Click **Save**.

VisualRF Support for Third-Party Devices

Beginning in AirWave 8.0.7, the following third-party devices are supported in VisualRF:

- Cisco Controllers: 3650, 3850, and 8510
- Cisco Access Points: 1700, 2700, and 702W
- Juniper Controllers: WLC100, WLC2, WLC2800, WLC8, WLC800, WLC880, and WLCJUNOSV

Third-Party Device Support

AirWave 8.0.6 introduces support for the following third-party devices.

Brocade

The Brocade ICX6610-48 switch is now supported in VisualRF. AirWave supports Brocade switches operating as standalone and stacked switches.

Table 1: *Supported Firmware for switches*

| Firmware Version | Model Type |
|------------------------------|------------|
| 08.0.20T211 and 08.0.30aT213 | ICX6610-48 |

Cisco

The following Cisco products are supported for monitoring, configuration, and software upgrades.

Table 2: *Supported Firmware for controllers*

| Firmware Version | Model Type |
|---|--|
| 03.06.01E, 03.03.05SE, 03.06.01E, 03.07.00E | <ul style="list-style-type: none"> • 3650 • 3850 |
| 7.4.121.0, 7.6.130.0, 8.0.100.0, 8.0.110.0 | 8510 |
| 10.2.111.0 (IOS: 15.3(3)JN3) | 2700 |

Table 3: *Supported Firmware for APs*

| Firmware Version | Model Type |
|------------------------------|--|
| 10.2.111.0 (IOS: 15.3(3)JN3) | <ul style="list-style-type: none">• 1700• 2700• 702W |

Dell Networking

The following Dell Networking products are supported for monitoring using AirWave.

Table 4: *Supported Firmware for switches*

| Firmware Version | Model Type |
|------------------|--|
| 8.3.2.0 | <ul style="list-style-type: none">• E150• E300• E600• E610• E1200• E1200i |
| 8.4.2.9 | <ul style="list-style-type: none">• C300• C150 |
| 8.4.2.6 | <ul style="list-style-type: none">• S25n• S25pac• S25pdc• S25v• S50• S50nac• S50ndc• S50e• S50v• S2410cp• S2410p |

Juniper

The following Juniper products are supported for controller and AP discovery and monitoring.

Table 5: *Supported Firmware for APs*

| Firmware Version | Model Type |
|------------------|--|
| 9.1.0.6.0 | <ul style="list-style-type: none">• WLA321• WLA322• WLA522• WLA532• WLA632 |

Table 6: Supported Firmware for controllers

| Firmware Version | Model Type |
|------------------|---|
| 9.1.0.6.0 | <ul style="list-style-type: none">• WLC100• WLC2• WLC2800• WLC8• WLC800• WLC880• WLC JunosV |

Meru

The following Meru controllers and APs are now supported in VisualRF.

Table 7: Supported Firmware for APs

| Firmware Version | Model Type |
|------------------|---|
| 6.1.1-25 | <ul style="list-style-type: none">• AP302• AP320i• AP332i• AP433i• AP433is• AP822e• AP822i• AP832e• AP832i• RS4000 |

Table 8: Supported Firmware for controllers

| Firmware Version | Model Type |
|------------------|--|
| 6.1.1-25 | <ul style="list-style-type: none">• MC1550• MC3200• MC4200 |



VisualRF support for the for the AP433i, AP433e, AP433is, AP822i, and AP822e is not included in AirWave 8.0.6

Motorola

The following Motorola autonomous APs are now supported in VisualRF.

Table 9: Supported Firmware for APs

| Firmware Version | Model Type |
|------------------|---|
| 5.4.2.0-30R | <ul style="list-style-type: none">• AP621• AP622• AP6521• AP6522• AP6532• AP7161 |

Table 10: *Supported Firmware for controllers*

| Firmware Version | Model Type |
|------------------|------------|
| 5.4.2.0-30R | RFS4000 |

UCC Dashboard Improvements

Starting with AirWave 8.0.6, on the UCC dashboard, The MOS (Mean Opinion Score) is now visible in the Call details, Client Details and Client dialog page. The MOS is updated after a call has ended.

New Configuration API

A new configuration API has been added in AirWave 8.0.6 that changes customer variables, Instant VC variables, and configuration push.

Instant Improvements

AirWave 8.0.7 added the following:

- The IGC CLI model now initializes when the AMP starts for the first time. If the IGC engine is not currently running, it may be disabled. You can enable it on the Groups Basic page. The engine may take a few minutes to start after it is enabled.
- After an IAP receives configuration information from AirWave, the Virtual Controller now enters a confirmation message in the AMP Device Events log. The message displayed reads: "Configuration is successfully synchronized from management server."
- AirWave now supports bulk configuration of thin AP radio roles and ARM mode.
- Support has been added for batch collection of debug data from AMP to IAP groups.

AirWave 8.0.5 added the following:

- IAP certificate authentication performance has been improved.

AirWave 8.0.4 added the following:

- Instant 4.1.1 CLI in template mode.
- Instant 4.1 and Instant 4.1.1 GUI Config (IGC)

RF Health Report Enhancements



Starting in AirWave 8.0.8, the folder, client, and radio statistics in the RF Health Report are unchecked and disabled by default. Additionally, upon upgrade to AirWave 8.0.8, these options will become unchecked and disabled in any previously configured RF Health Report definitions.

In AirWave 8.0.7, a number of enhancements have been added to the RF Health Report. A report can now be summarized by:

- Top Folders By Worst Client and Radio Statistics Combined 2.4 GHz and 5 GHz
- Client and Radio Statistics by Folder - Combined 2.4 GHz and 5 GHz
- Top Folders By Worst Client and Radio Statistics 2.4 GHz
- Client and Radio Statistics by Folder - 2.4 GHz
- Top Folders By Worst Client and Radio Statistics 5 GHz
- Client and Radio Statistics by Folder - 5 GHz

The statistics displayed can be Client Health, Client SNR, Radio Noise, Radio Utilization, or Radio Interference. The thresholds for the statistics are defined in the corresponding fields below. These thresholds are defined by a specified percentage (0-100%) or dBm (-110-0 dBm) for Radio Noise Threshold.

To enable these:

1. Login to the AMP
2. Navigate to **Reports > Definitions**.
3. Select **Daily RF Health Report**.
4. Check any options under **Summarize report by**.
5. Select the statistics to be displayed from the **Top Folder Sorting Column** drop-down menu.
6. Define any thresholds appropriate to your report.
7. Click **Save and Run** or **Save**.

HTTP Request Retry Attempts

In AirWave 8.0.7, you can configure the number of HTTP request retry attempts. Also, more log information regarding **amp_events** about an HTTP retry has been added.

MIB Improvements

In AirWave 8.0.7, two new enhanced traps have been added: **apUp** and **apDown**. These traps now allow the AP MAC address and the AP name to be added. They support rogue containment so there is no mismatch in the AP list when the AP is in **monitor_only** mode and the IGC is enabled.

Because the error is not set in the configuration response from the AP when the IGC is enabled, the error is displayed by the IGC instead.

Mobility Access Switch Support Enhancements

In AirWave 8.0.5, The drop-down list of Show commands on the switch monitoring page are now categorized. The commands are grouped as follows:

- Switch Details
- ArubaStack
- LLDP/CDP
- Power over Ethernet
- Layer 1 / Layer 2
- Layer 3
- Tunneling (IPSEC/GRE)
- Authentication & 802.1x Troubleshooting
- User Details

Support for parsing the bandwidth values for wired clients connected to an Aruba Mobility Access Switch has been added. Now AMP shows the data usage for wired clients connected to the switch.

Bulk Editing of the Switching File

Starting in AirWave 8.0.4, the VLAN bulk edit allows you to update the following switching configuration options at the same time:

- access-vlan
- native-vlan
- trunk allowed vlan <list>

Site to Site IKE

AirWave 8.0.4 introduces a Site to Site IKE configuration page under **Controller Config > Advanced Services > VPN Services > IKE > Site to Site IKE** as shown in [Figure 1](#). This page allows you to configure Site to Site IKE on a controller. Refer to the Virtual Private Networks chapter in the *ArubaOS User Guide* for more information about IKE.

Figure 1: Site to Site IKE

Configure DPD: Yes No

Permit Invalid Certificates: Yes No

Disable Aggressive Mode: Yes No

XAuth: Yes No

CA-Certificate for VPN Clients: Certificate Name, type uniqueness conflicts between "Aruba Config" and "Controller Override" may result in pushing unintended certificate to the controller.

Server-Certificate for VPN Clients: Certificate Name, type uniqueness conflicts between "Aruba Config" and "Controller Override" may result in pushing unintended certificate to the controller.

Configure IKE Certificate-Group for VPN Clients: Yes No

Site to Site IKE Shared Secrets

New Site to Site IKE Shared Secret

API for Streaming Raw Records

An API, which streams raw records for reports in CSV format, is available in AirWave 8.0.4. This API is a beta version only. To try this API, please contact your support person for details.

Usage Column in AP Table

In AirWave 8.0.2, a usage column, which can be filtered and sorted, has been added to the AP table.

Support for SCP for Aruba Firmware Upgrades

In AirWave 8.0.2, SCP is now supported for uploading a firmware file to a controller when performing a firmware upgrade. An option has been added to select SCP when uploading a firmware file to the AMP.

Creating Custom Filtered Views

In AirWave 8.0.2, the custom filtered views feature supports up to 20 data columns. The columns in these customizable tables resize automatically to fit their contents, but if the table still does not fit within the browser page, a scroll bar appears below the table, allowing you to scroll and view the additional columns. The columns in the default view for each of the following pages are defined in AirWave and cannot be modified. However, you can now create a new view in each of these pages that returns custom information based on the filter parameters and data columns you selected when creating that new view.

- **APs/Devices > List**
- **APs/Devices > Up**
- **APs/Devices > Down**
- **APs/Devices > Mismatched**

- **Groups > Monitor**
- **Clients> Connected**
- **Clients> All**
- **RAPIDS > List**

Figure 2: Default View of Devices

The screenshot shows a web interface for managing devices. At the top, there is a dropdown menu set to 'Default View: Devices' and three icons: a plus sign, a notepad with a pencil, and a minus sign. Below this, it says 'Total Row Count: 3' and 'Modify Devices'. There are several control elements: 'Change device Group/Folder' with a dropdown arrow, 'Group: Choose Group' with a dropdown arrow, 'Folder: Choose Folder' with a dropdown arrow, and two buttons labeled 'Move' and 'Apply All'. The main part of the interface is a table with the following columns: Device, Status, Configuration, Controller, Folder, Group, Clients, Usage, IP Address, and Type. The table contains three rows of data:





| Device | Status | Configuration | Controller | Folder | Group | Clients | Usage | IP Address | Type |
|------------|--------|---------------|------------|--------|-------|---------|-------|-------------|------------------|
| CN18DWY09T | Up | Good | MSM720 | HP | HP | 0 | 0 bps | 10.51.1.2 | HP ProCurve M... |
| MSM720 | Up | Good | - | HP | HP | 0 | 0 bps | 10.51.3.104 | HP ProCurve M... |
| SG102LBW12 | Up | Good | - | HP | HP | 0 | 0 bps | 10.51.3.103 | HP ProCurve M... |

To create a new filtered view, navigate to any page that contains a default view list, such as **APs/Devices > List**.

1. Click the icon. The **Filtered View** page opens.
2. Enter the name of the new view.
3. (Optional) AMP administrators can select the **Is Global** check box to give all users access to the filtered view. Administrators are able to edit any global view they can see in the filtered view drop-down list.
4. Click **Add Filter**. A new list of parameters is added to the **Filter** field.
5. Scroll the list of parameters and select a **Device** or **Radio** parameter. If required, enter search parameters such as "=" to refine the filter parameters.
6. (Optional) To create a filtered view with multiple filter parameters, click **Add Filter** again and define any additional filter parameters. For example, to create a view that displays APs with more than zero clients but less than five clients, you would need to create one filter with the parameters **Clients > 0**, and a second filter with the parameters **Clients < 5**.
7. Drag and drop data columns from the **Available Columns** list to the **Current Columns** list to the columns display in the view. You can reorder the columns in the **Current Columns** list by dragging and dropping a data column to a different place in the list.
8. Click **OK**. The name of the new view is added to the view list.
9. Click the name of the new view. A new page displays the results of the new view, based on the configured filters.

You can edit a custom filtered view at any time, by selecting the view in the view list, then selecting the icon and modifying filter parameters and column displays.

Table 11: Filter icons

| Icon | Description |
|---|---|
|  | Click this icon to create a custom filtered view. |
|  | Click this icon to edit an existing custom filtered view. |
|  | Click this icon to clone a custom filtered view. |
|  | Click this icon to delete a custom filtered view. |

VisualRF Enhancements in HTML5

This section describes the new features associated with the HTML5-based UI for VisualRF.

Copy a Floor in the Same Building

In AirWave 8.0.8, the Floor plan **Duplicate** option lets you copy a floor in a building when you want to create a duplicate floor in the same building.

Floor Upload Wizard

Starting in AirWave 8.0.0, the **Floor Upload Wizard** allows you define the parameters required to complete a new floor plan. The wizard has three pages:

- **Scale** - This page allows you define the lengths and width of the new floor plan.
- **Region** - This page provides drawing tools you use to define the floor plan boundary and planning region(s).
- **Access Points** - This page gives you the option to plan an AP deployment, or to add APs that are already deployed.

Navigation Improvements

Starting in AirWave 8.0.0:

- You can select between the **Map** and **List** views from the **VisualRF** page. The **Map** view shows the geographic location of each campus. The **List** view is a sortable table that lists the names of building and campuses in the network, the number of floors in each building and the name of each floor. You can click any of the links in the table to view that campus, building or floor plan in VisualRF.
- When you select a campus in VisualRF and drill down to view buildings and floor plans within that campus, the VisualRF page displays your path in a breadcrumbs format, such as **Campus One > Building One > Floor 2**. Click a link in the breadcrumb list to view the selected campus or building.
- The **Network** page now displays **Properties**, **View**, and **Edit** menu links in the Map view. In the List view, the menu links appear after you select a campus name from the list. These links display information for the selected network, campus, building or floor level.
- A new drop-down menu in VisualRF lists all campuses in the network. To access this menu, click the arrow to the left of the **Network** label on the **VisualRF** page. Select a campus name, then expand the list to access a building or floor in the campus.
- The VisualRF **Overlays** menu contains three new overlays:
 - AppRF: Identifies clients who are contributing to the usage of one or more selected applications.
 - Channel: Identifies the overlapping and specific regions for selected channels on a floor plan.
 - UCC: Displays the call quality of Unified Communication and Collaboration (UCC) calls.
- The new HTML5 UI replaces the Flash UI as the default view.



The HTML5-based UI does not support wired overlays or wired devices. The **VisualRF Plan** was not migrated to HTML5. To administer wired overlays and devices, go to **VisualRF > Setup** and click **No** in the **Enable HTML5-based UI** field.

AppRF Enhancements

This section describes enhancements to the AppRF visibility features introduced in AirWave 8.0.0.

AppRF Overlay

The AppRF overlay identifies clients who are using one or more selected applications, such as YouTube or Facebook. The overlay uses colors to show usage thresholds. To see the usage, mouse over the client icon. The threshold colors for the following usage categories are preset and cannot be edited:

- Green: Client has used between 0 and 20 MB in the past two hours.

- Yellow: Client has used between 20 MB and 1 GB in the past two hours.
- Red: Client has used more than 1 GB in the past two hours.

AppRF Reports

The AppRF reports show the top client destinations and applications for all groups and folders. The available options for this report are:

- Top Applications Summary
- Top Destination Summary
- Top ten Applications By Device Types
- Top ten Applications By User Roles
- Top ten Applications By SSIDs
- Top three Applications For Top Ten Users
- User Detail

Note that the **User Detail** report is available only to users configured in the report definition.

UCC Visibility

AirWave 8.0.0 introduces an aggregated view of the UCC calls made in the network. The administrator can see a top level view of the call quality assessment, and further drill down into a specific view based on the analysis required.

Home>UCC charts

The **Home>UCC** page provides the four charts described below.

- **Call Quality:** This set of graphs show the quality of calls on the network over the selected time period. The **Trend** chart shows the number of calls with good, fair, or poor client health over the selected time period. The **Distribution** graph shows the relative proportions of calls with each quality type, and the APs chart shows information about APs that supported poor quality calls. You can also hover your mouse over the **Trend** or **Distribution** charts to view details about the highlighted section of that chart.
- **Quality Correlation:** These graphs display the correlation between the VoIP call quality and the VoIP client health of every UCC call. The **Trend** chart shows the number of calls with good, fair, or poor client health over the selected time period, while the **Scatterplot** chart shows the call quality and client health of each individual call.
- **Call Volume:** The Call Volume **Trend** graph displays the number of calls by UCC application type, for example, SIP, Lync, SCCP, H.323, NOE, SVP, VOCERA, or FaceTime. The Call Volume **APs** graph shows the names of the APs that supported these calls.
- **Devices:** These graphs display information about the calls made by different device types, such as Windows 7, Mac OS X, iPhone, or Android devices. The Devices **Trend** and **Distribution** graphs show the numbers of calls by each platform type, while the **Quality** graph shows the numbers of calls at each quality level made by each device type.

AMON provides data to populate the charts. The UCC feature also provides a Lync overlay that shows a historic view of calls, and a Lync Mobility trail to track historic call sessions.

Figure 3: UCC Dashboard Example



Call Details and Diagnostics

You can mouse over any of these UCC charts to view details about that chart, or drill down to a detailed view to display more specific information based on call quality and client metrics. To display an aggregated list of UCC call data metrics, click any of the following hyperlinks on the **Home > UCC** page:

- Call Details
- Call Volume Details
- Device Details

Click on any call on the Quality Correlations **Scatterplot** graph to open the **Clients >Diagnostics** page. This page provides an overview of a WLAN user's general status and connectivity on the network

UCC Overlay

VisualRF includes a new UCC Overlay that displays information about UCC calls. You can configure this overlay to display calls that match any of the following values:

- Protocol: **Lync** or **All**
- Type: **Voice**, **Video**, or **All**
- Quality: **All**, **Good**, or **Unknown**

Additive Licensing

AirWave 8.0.0 introduces support for multiple licenses on one system. This enhancement allows you to install a new license for additional APs without modifying existing AP licenses.

Client Health Graph

Starting with AirWave 8.0.0, the **Home** and **Folder** pages include a new graph that provides client health information. The graph shows the percentage of clients with good, fair, and poor health. To view the new graph from the **Home** page, select **Client Health** from the **Clients** menu.

The client health metric displayed in these charts is the efficiency at which that AP transmits downstream traffic to a particular client. This value is determined by comparing the amount of time the AP spends transmitting call data to a client to the amount of time that would be required under ideal conditions, that is, at the maximum Rx rate supported by client, with no data retries.

New Supported Devices

- Aruba Access Points
 - AP-103/AP-103H and IAP-103
 - AP-114/AP-115 and IAP-114/IAP-115
 - AP-204/AP-205 and IAP-204/IAP-205
 - AP-205H (starting in AirWave 8.0.7) and IAP-205H (starting in AirWave 8.0.9)
 - AP-214/AP-215 and IAP-214/IAP-215
 - AP-228 (starting in AirWave 8.0.7) and IAP-228 (starting in AirWave 8.0.9)
 - AP-274/AP-275 and IAP-274/IAP-275
 - AP-277 (starting in AirWave 8.0.7) and IAP-277 (starting in AirWave 8.0.9)
 - AP-324/AP-325 starting in AirWave 8.0.9.2
- Multi-Vendor Devices
 - Cisco 5760 wireless LAN controller*
 - Cisco 3700 and 1550 access points
 - Motorola Wing5 RFS controllers and 6532, 6522 and 6521 APs**
 - Brocade ICX switches*

* Monitoring only; configuration within AirWave not supported

** These AP and controller models may require adjustments to the AirWave SNMP timeouts to compensate for known SNMP issues on these devices.

Changes

Changes to AMP were made to the following general categories:

- ["Audit Page Enhancements "](#) on page 22
- ["License Limit Alert"](#) on page 23
- ["Automatic IGC Policy Upgrade "](#) on page 23
- ["IGC Policy Copy "](#) on page 23
- ["Introduced in AirWave 8.0.5:"](#) on page 23
- ["VisualRF Improvements"](#) on page 23
- ["List Changes"](#) on page 24
- ["Configurable Tables"](#) on page 24
- ["Enhanced Export Report Option"](#) on page 25
- ["Controller Backups and Restoration"](#) on page 25
- ["System Resources Trigger"](#) on page 25
- ["LDAP Enhancements"](#) on page 25
- ["Redis Statistics"](#) on page 26
- ["Match Events Table Improvement"](#) on page 26
- ["Local Controller Configuration"](#) on page 26
- ["Other Categories"](#) on page 26

Audit Page Enhancements

Starting with AirWave 8.0.6, the **Audit** page is divided into multiple subsections, improving the time it takes that page to load.

The **Audit** page appears when you select a device from the **Devices** list on the **AP/Devices > List** page. Each section of this page sends requests separately and loads as soon as a response is received. This eliminates a dependency on the other sections and reduces bottlenecks in data loading. Additionally, if there is a delay in response, a loading message is now displayed while the data is sent.

License Limit Alert

Introduced in AirWave 8.0.6, in addition to displaying the number of days remaining on a license, the **Home > Licenses** page now displays a warning message when usage levels for a license exceeds 90%. If your AirWave deployment includes temporary or evaluation licenses, the **License** page shows the **License Usage: xx%** warning next to the **Days Remaining: xx** message.

Automatic IGC Policy Upgrade

Introduced in AirWave 8.0.6, if all IAPs in a group upgrade to a new software version, the IGC now migrates the group policy to the new version if the new version of software is higher than the current one.

IGC Policy Copy

Introduced in AirWave 8.0.6, the IGC is now notified to copy the group policy from the original group to the new group when you duplicate a group using the IGC.

Instant Improvements

Introduced in AirWave 8.0.6:

- AirWave 8.0.6 introduces support for destination IP and reverse DNS lookup for IAP AppRF data.
- Beginning with AirWave 8.0.6, Instant thin AP batch configuration supports DNS and swarm mode configuration.

Introduced in AirWave 8.0.5:

- The IAP reboots automatically when you change the IP address of the IAP.
- In the IGC, the multi-edit save function now saves a change but does not apply it until you click the **Apply** button.
- In the IGC, you can view and edit the **Longitude**, **Latitude**, **Altitude**, and **Notes** configuration values of a VC or an AP. For a VC, view or edit these values from the **AirWave > AirWave Settings** pages of the IGC. To view or edit values for an AP associated with a VC, select that device from the **Access Points** page of the IGC, then select **AirWave Settings**.
- A new configuration option has been added that allows you to perform bulk template modifications on virtual controller timezones .
 1. From the **Groups > List** page, select a group of Instant devices and click **Modify Devices**.
 2. Click the **Change device Group/Folder** drop-down list and select **Aruba Instant virtual controller variables**.
 3. Select one or more VCs and click **Update**. If the selected devices are *not* managed using the IGC, the **Groups > Monitor** page opens, allowing you to modify the **Clock_timezone** field.
- IAP certificate authentication performance has been improved.

VisualRF Improvements

The following VisualRF Enhancements were introduced in AirWave 8.0.4 to improve performance:

- Background loading of AP and client discovery data in the UI. This causes the floor plan and AP heatmaps to appear immediately while client, rogues, association line data loads in the background.

- Background fetching of AP bandwidth, uptime, AP Radio Channel Utilization and Client health data when user clicks on AP or client to view properties. AirWave will now only fetch the data when a particular AP is clicked on instead of fetching the data for all APs when the floorplan loads.
- Optimize fetching of data from internal caches.
- Reduce startup time by not fetching ap_detail values from AirWave during startup. Viewing of client and rogue data on floor plan is delayed until the next controller SNMP poll cycle period.
- Read-only users can now use location history.
- The loading icon now appears when a floor plan is opened in any view.
- The channel utilization overlay now loads properly in 8.0.4.
- When using VisualRF in Mozilla Firefox, devices do not stick to the cursor when moving them around the floor plan.

List Changes

The lock icon in the configuration column of an AP/Devices List has been reimplemented in AirWave 8.0.4. The lock icon indicates that the device in that row is in **Monitor only** mode.

For a new Instant device in the **APs/Devices > New** page, the admin user can mouse over the value under the **Type** column to verify the device's Shared Secret with the AMP server.

The **Manage** (wrench) icon has been removed in AirWave 8.0.4, however the same functionality has been maintained. If you mouse over an device's line in a list, a popup menu appears, allowing you to select options such as **Manage**, **Audit**, **Monitor**, and **Compliance**. Clicking any of the links takes you to the corresponding page in the UI; additionally, clicking on the device link takes you to the monitor page.

Figure 4: Device Drop Down Menu

| Device ▲ | Status ▼ |
|-------------------|----------|
| 00:0b:86:f0:33:20 | Up |
| 00:1a:1e:c0:1a:dc | Up |
| 00:1a:1e:c0:55:3a | Up |
| 00:24:6c:c7:f8:1c | Up |
| 00:24:6c:c8:de:8a | Up |
| 6c:f3:7f:ca:84:f0 | Up |

Manage

Audit

Monitor

Compliance

Configurable Tables

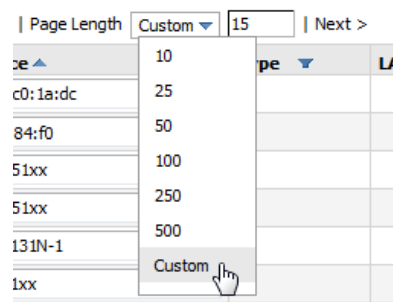
By default, the tables on the pages listed show 25 rows of information. AirWave 8.0.2 allows you to change this value and display a different number of table rows on each page. Click the **Page Length** drop-down menu above the table and select any of the predefined page lengths, or select **Custom** and enter a value in the **Page Length** field to create a new custom page length. You can force all lists to take on a change made to the **Default Number of Records per List** setting on the **User Info** page by clicking the **Reset** button directly below it.

- **APs/Devices > List**
- **APs/Devices > Up**
- **APs/Devices > Down**
- **APs/Devices > Mismatched**
- **Groups > Monitor**
- **Clients > Connected**
- **Clients > All**
- **RAPIDS > List**



Although this feature allows you to configure a page length of up to 2000 table entries, longer page lengths require more time to load the page in the Web browser. Best practices are to limit the page display to display 500 or fewer entries.

Figure 5: Defining a Custom Page Length



Enhanced Export Report Option

Introduced in AirWave 8.0.0, a new **Export Report** option allows you to use SCP or FTP protocols to transfer a report to an external server. To export a report, the report must be in the .csv or .pdf format. The export parameters are set in the **Export Options** field on the **Reports Definitions** page. Click **Yes** in the **Export Report** field to open the **Export Options** pane, which allows you to define settings for external server.

Controller Backups and Restoration

Starting in AirWave 8.0.0, you can create a backup on demand by creating and collecting a flash backup from the Controller. Daily backups are also created. At a minimum, there are four backup files:

- Two daily backups
- One backup from last week
- One backup from last month

The backup saved from a firmware upgrade is automatic and requires no manual intervention. All backups can be saved or restored and are displayed on the **Audit** page. You can only perform a backup on a device if the firmware version of the device and the backup image are identical. After you click Restore, the device on which the restoration is being performed automatically switches from monitor mode to maintenance mode. After you restore a backup image to a device, you must restart AMP.

System Resources Trigger

Starting in AirWave 8.0.0, system resources usage values are now available as Trigger types. To create a **System Resources** trigger,

1. go to **System > Triggers** and click **Add**.
2. In the **Type** drop down list, select **AMP Health>System Resources**.
3. The available matching conditions for this trigger are **CPU Utilization Percentage**, **Disk I/O Utilization Percentage**, and **Memory Utilization Percentage**. You must configure at least one matching condition before you can save the new trigger.
4. Click **Add** to save your trigger.

LDAP Enhancements

Starting in AirWave 8.0.0, AirWave includes an option to define an LDAP rule that assigns an AMP user role. The configurable parameters for this LDAP rule are **Position**, **Role Attribute**, **Operation**, **Value** and **AMPRole**. If you create multiple LDAP rules, rules are processed in order based on the rule position value, so the position you

assign to the LDAP rule represents the order in which the LDAP rule is applied to determine the AMP role. LDAP rules can only be configured and applied after LDAP authentication is enabled. The LDAP rules are similar to the rules used by the controller to derive the AMP role.

Redis Statistics

Starting in AirWave 8.0.0, the **System>Performance** page includes three **Redis Statistics** charts: **Redis Activity**, **Redis Used Memory**, and **Redis Keyspace**. Use these charts under the supervision of Aruba support to troubleshoot Redis activity and keys.

Match Events Table Improvement

Starting in AirWave 8.0.0, the **Match Events** table in the **Clients>Diagnostics** page now includes dBm information in the **From AP Signal** and **To AP Signal** columns. The far right column of the table now uses a green check mark to indicate successful events.

Local Controller Configuration

In AirWave 8.0.0, an enhancement was added to the local controller configuration feature allows you to configure additional settings and perform a bulk edit on those controller settings during local configuration. Local configuration is disabled by default and can be enabled or disabled under **Groups > Basic**.

You can change the following variables using the bulk edit feature:

- VLAN ID
- Interface VLAN
 - ID
 - IP
 - Netmask
 - Secondary IP
 - Secondary Netmask
- Interface Loopback IP
- Interface - Group Gigabit Ethernet
- Site-to-site VPN
 - IKE shared secret,
 - IP Netmask
- Site-to-site (IPSEC Map)
 - Source Network Address
 - Source Netmask
 - Local FQDN ID
 - Peer Gateway IP Address
- DHCP Server (DHCP scopes)
 - Server Pool IP Address
 - Server Pool Mask
 - Default Router Address
- IP-Profile - Default Gateway

Other Categories

- Starting in AirWave 8.0.6, a tooltip displays in the AMP UI when your mouse hovers over any cluster in the list and not just the selected cluster.

- Starting in AirWave 8.0.6, an in-progress status displays in the AMP UI anytime a change is being applied.
- Starting in AirWave 8.0.0 the **RAPIDS** Rules feature now includes a new Channel rule. The Channel rule allows you to search for devices and classify whether the devices are or are not on a specific channel. The specific channel to search for is set when configuring the rule. The rule is configured on the **RAPIDS > Rules** page.
- Starting in AirWave 8.0.0, the **Client Session Summary** box at the end of the **Client Session Report** page now includes information about total traffic in and out, average traffic in and out per session, and average traffic in and out per client. Traffic statistics are presented in MB.

The Support Download Page

The table below describes the different packages/files that you might see on the Support site when you download AirWave.

Table 12: *Download page file descriptions*

| File name | Description |
|--------------------------|---|
| Install iso | Standalone installation media including CentOS operating system. This can fit on a CD/DVD, or it can be mounted as a virtual disk for installation. |
| Install tar file | Used for installation on a customer-installed CentOS or RHEL server. |
| Upgrade package tar file | Used for AirWave upgrades. Note that updates are only supported from up to two versions prior. Contact support if you are upgrading from three versions prior or more (for example, from 7.4 to 7.7). |
| Virtual appliance ova | VMware OVA template for AirWave deployment on VMware ESXi infrastructure. |

Supported Infrastructure Devices

AirWave provides a range of features to manage network infrastructure devices from Aruba Networks and other vendors. This document describes the supported product families, software versions, and feature set for Aruba products. For a list of supported products from other vendors, see the *AirWave 8.0 Supported Infrastructure Devices* document, which can be found at support.arubanetworks.com.

ArubaOS

AirWave supports all controllers and most access points that are running ArubaOS 6.4.x and all prior versions, and that have not reached the End of Support milestone. The AP-80M series of access points is not supported by AirWave. Refer to <http://www.arubanetworks.com/support-services/end-of-life-products> for the complete list of end-of-life products.

FIPS

Aruba Controllers running ArubaOS 6.0.x through 6.4.x FIPS and all prior versions that have not reached the End of Support milestone are supported by this version of AirWave, including the management of global configuration profiles and software upgrades.

Instant

Aruba Instant access points running Instant software versions 6.4.3.x-4.2 and prior are also supported, including the management of configuration settings and software upgrades. The following table shows when each new version of Instant was initially supported in AirWave.

Table 13: Instant Support in AirWave

| Instant Version | Support For Template Configuration | Support for IGC Configuration |
|-----------------|------------------------------------|-------------------------------|
| Instant 4.2 | AirWave 8.0.9 | AirWave 8.0.9 |
| Instant 4.1.1 | AirWave 8.0.4 | AirWave 8.0.4 |
| Instant 4.1 | AirWave 8.0 | AirWave 8.0.4 |
| Instant 4.0 | AirWave 8.0 and AirWave 7.7.10 | AirWave 7.7.8 |
| Instant 3.4 | AirWave 7.7.3 | AirWave 7.7.8 |
| Instant 3.3 | AirWave 7.6.4 | AirWave 7.7.8 |
| Instant 3.2 | AirWave 7.6.1 | AirWave 7.7.5 |
| Instant 3.1 | AirWave 7.5.6 | N/A |
| Instant 3.0 | AirWave 7.5 | N/A |

AirMesh

Aruba AirMesh outdoor products running MeshOS 4.2 are supported for monitoring and for software upgrades.

Aruba Mobility Controller 651

Aruba Mobility Controller 651 running 6.2.0 and prior versions are supported.

Aruba Mobility Access Switches

The Aruba series of Mobility Access Switches (S3500, S2500, and S1500) are supported for profile configuration, monitoring, and software upgrades.

In addition to the port statistics supported for most Ethernet switches with the supported firmware described below, AirWave also tracks the activity of authenticated wired clients on Aruba switches.

Table 14: Aruba MAS Supported Firmware and Devices

| Firmware Version | Switch Type |
|-------------------------------------|---------------------------------|
| Validated up to 7.3.2.0 and 7.4.0.0 | Standalone and stacked switches |

Fixed Issues

This table lists the fixed issues in AirWave 8.0.11.

Table 15: Issues Fixed in AirWave 8.0.11

| ID | Description |
|--------------------|---|
| DE21373 | An issue is resolved where the daily RF Health report could only display a maximum count of 200 under the MAC/PHY Errors field for devices using either the 5 GHz or 2.4 GHz radios. The MAC/PHY Errors fields in this report have been replaced with the MAC Errors (%) and PHY Errors (%) fields. The MAC Errors (%) field represents the maximum percentage of MAC errors out of the total errors reported for a given period, and PHY Errors (%) represents the maximum percentage of PHY errors out of the total errors reported for a given period. |
| DE22284 | Line breaks have been restored in email alerts from AirWave, allowing Microsoft Outlook to display the proper paragraph alignment in email alert messages. |
| DE23543 DE24065 | An issue is resolved that prevented data from being populated in the graphs on the APs/Devices > Monitor > Radio Statistics page. Internal improvements ensure that the graphs are properly displaying data from a valid source. |
| DE23767 | Users creating new time-based services using the Groups > Instant Config > System > Time Based Services page no longer encounter a "Policy Change Failed" error message. |
| DE23788 | The HTML link to the Supported Infrastructure Devices document on the Home > Documentation page no longer sources content from a location that does not exist. This resolves an issue in AirWave 8.0.10, where clicking this link displayed output with missing content. |
| DE23803 | The Clients > Client Details page and APs/Devices > Monitoring page now correctly display client data sent from controllers running any version of ArubaOS. This resolves an issue where AirWave failed to correctly parse AMON messages from a controller running ArubaOS 6.4.2.9. |
| DE24004 | When the AirWave server is upgraded to AirWave 8.0.10, the Action drop-down list under Instant Config > Security > Roles now displays the options for Source-NAT and Destination-NAT for all IAPs. Previously, the AirWave server only displayed these options for IAPs with firmware versions lower than 6.4.3.4-4.2.1.0. |
| DE24042 | An AirWave server configured as a master console no longer reverts back to a regular AirWave server after the master console license expires. Starting with AirWave 8.0.11, when the master console license expires, the device enters a 90-day grace period. During this grace period users may continue using the master console and failover servers without any changes in functionality or visibility. |
| DE24385 | The nightly VisualRF backup period has been extended to one hour, allowing the backup process to reach completion before timing out. The backup process previously timed out before all VisualRF sites could be incorporated, producing backup files with missing data. |
| DE24387 | AirWave now validates the IP address or FQDN of a primary or secondary Network Time Protocol (NTP) server configured on AMP Setup > Network > Network Time (NTP) , to ensure that the NTP is configured with valid network addresses. |

This table lists the fixed issues in AirWave 8.0.10.1.

Table 16: Issues Fixed in AirWave 8.0.10.1

| ID | Description |
|---------|--|
| DE23915 | An issue is resolved where an upgrade to AirWave 8.0.10 incorrectly triggered an error which stated that the GNU Transport Layer Security Library (GNUTls) package was already installed. Improvements to the internal upgrade processes resolve this issue in AirWave 8.0.10.1. |
| DE23810 | Improvements in AirWave 8.0.10.1 refined the logic for internal checks for database table size. If you see the AirWave error message " <i>Database tables need vacuuming before you can proceed with upgrade</i> " prior to an upgrade, contact support for further assistance. |

This table lists the fixed issues in AirWave 8.0.10.

Table 17: Issues Fixed in AirWave 8.0.10

| ID | Description |
|--------------------|---|
| DE20082 | Adding a single device from thousands on the New Devices list now takes less than one second. |
| DE20179 | Mismatches are cleared for the IKE Server Certificate and CA Certificate when Site to Site IKE settings are being imported to AirWave. |
| DE21161 | SHA Authentication Protocol and AES Privacy Protocol options can be selected for HP ProCurve switches under Device Setup > Communication and Device Setup > Add . |
| DE21215 | Rogue device alerts are not triggered for devices outside of the folder configured in the trigger definition. This applies only to rogue devices that do not have a last discovery event in the database. |
| DE21720 | Access to the /api/ap_bssid_list.json and /api/ap_bssid_list.xml API queries has been updated to allow read-only users or greater. |
| DE21750 | The funnel mechanism used to classify rules under RAPIDS > List has been updated to display all rule names consistently when the Classifying Rule is set to All . |
| DE21821 | Polling enhancements have been enabled for thin AP clients and thin AP rogues on the MSM controller to prevent clients from being reported with unknown SSIDs when they are in a transition state and do not have a valid vsc_index. A check has also been added to the AMP server to verify whether a client has a valid vsc_index. Clients without a valid vsc_index are ignored by AirWave. |
| DE21972 | The RAPIDS rogue signal calculation has been fixed to ensure all rogue signal strengths are calculated and classified correctly. High-threat rogues no longer display unusually low signal strengths, which previously caused AirWave to classify these potential threats incorrectly and delete them from RAPIDS, where only the highest threats are retained. |
| DE22144 | Upgrade triggers are now enforced in all IAP firmware upgrades. Each IAP is upgraded successfully, and no upgrade job is deleted when the IAP reboots. AirWave no longer triggers the Needs Firmware Upgrade alert or restarts the upgrade process once the IAP has already been upgraded. |
| DE22163 DE22763 | The Channel Utilization widget calculates and displays the correct max channel usage by storing tx_time and rx_time as percentages and determining the time at which tx_time + rx_time is the greatest. Max channel usage was previously calculated using greatest tx_time + greatest rx_time. |
| DE22259 | A duplicate vpn hold time command has been removed from the IGC CLI command file. The IGC page no longer crashes or requires constant rebooting when IAPs are deployed in place of existing APs. The IGC page can now load successfully when an IAP configuration is pushed to the deployment. |
| DE22279 | When the Aruba Controller Role is set to root from the AMP Setup > Roles page, AirWave is now directed to the VPN IP address of a virtual controller instead of the "real" IP address of the virtual controller when a user clicks on the VPN IP address hyperlink found on the controller's Monitor page |
| DE22319 | Channel Utilization calculations have been fixed to ensure that both AirWave and the IAP display the same data. |
| DE22340 | When a global group template is modified on the primary AMP of the Master Console, the SSID display updates successfully, and the Master Console no longer crashes due to a timezone and HTTP timeout error. |
| DE22342 | <p>A new change owner command has been added to the following folders/files so the VisualRF file permissions no longer change when a user attempts to add a new floorplan to the VisualRF server, as this previously caused floorplan uploads to fail:</p> <ul style="list-style-type: none"> ● The /var/airwave/temp folder ● AirWave VisualRF directories ● set_visualrf_file_perms |
| DE22345 | After a new virtual controller is created from an IAP factory reset, the AMP whitelist is re-imported to authorize and map dynamic AP variables to the new controller, which requires the dynamic variables for successful configuration. |

Table 17: Issues Fixed in AirWave 8.0.10 (Continued)

| ID | Description |
|---------|--|
| DE22413 | The send_interferes_to_vrf command is now enabled on the seas_config table, allowing VisualRF to receive information on interfering devices and display those devices on the VisualRF floorplans. |
| DE22419 | Variables can now be referenced twice on a single line of the controller configuration template. |
| DE22466 | The New AP Monitor page of the AMP server no longer displays an error message indicating that the "AP is not associated to Virtual Controller" when a new AP is provisioned and successfully replaces an AP that goes down in a cluster. |
| DE22468 | When an IAP is added to an AMP server and assigned the static AirWave IP address through the IGC, the shared ams-key for the server can be configured on the IAP under the Admin tab of the Groups > Instant Config > System page. The IAP can now authenticate and connect to the AMP server using the shared key. |
| DE22474 | The AirWave server now discovers HP 560 APs under the correct device type. |
| DE22481 | The IAP CPU Utilization graph no longer displays sudden, unwarranted drops in CPU usage, with the added support for IAP 4.2.1 in the IGC 4.2.0 UI. If an IAP client's IP address is 0.0.0.0, the radio mode must be set to the actual radio mode manually, as the reported radio mode may be incorrect and produce inaccurate data. The batch command and run-command APIs have also been updated with new parameters and improved security features. |
| DE22523 | WMS offload messages are now sent to the PAPI daemon using RabbitMQ, preventing the airbus from stalling while sending large messages (1MB or larger). |
| DE22543 | AP transmit power levels are now updated and synchronized automatically in the VisualRF without requiring users to execute the poll_aps_now.xml command. As long as the synchronization timer is set (2mins/5mins/15mins), VisualRF no longer fails to display the updated power levels periodically. The new Refresh button also allows users to view the most recently updated power levels. |
| DE22547 | Load time for the Client Monitoring page has been improved. |
| DE22563 | Cisco WLC 5760 controllers that are configured successfully and respond to queries no longer appear as 'down' on the AMP server . The AMP server is also able to retrieve firmware information from the WLC controller through the constants.pm file without encountering the "error: fetching existing configuration" message. |
| DE22599 | The RabbitMQ snoop for VisualRF no longer fails and displays an error message when a user executes the rabbitmq_snoop command to view the data sent to the VisualRF bus. |
| DE22600 | The VisualRF channel overlay now displays the name of each AP instead of the AP ID, even if the APs are on different floors. APs that are in a planned state appear as PlannedAp:<last four digits of AP ID> since they do not have a name or MAC address. |
| DE22636 | The Instant Config > AirWave > Config Archive page now updates and displays the archived configuration properly when a user selects a specific archived config, such as Show Delta or Show Audit . |
| DE22664 | After a configuration is pushed to an AP group, the server no longer deadlocks when the template changes are being saved and applied. |
| DE22671 | Upstream device information is now available on the IAP Monitoring page. |
| DE22674 | Users can now select and delete one or more firmware jobs from the WebUI without deleting every job posted on the page. |
| DE22729 | Users are now able to push configurations to the Aruba S1500 and S2500 switches successfully without encountering mismatches in the configuration output. |

Table 17: Issues Fixed in AirWave 8.0.10 (Continued)

| ID | Description |
|---------|--|
| DE22767 | <p>The AirWave Groups page and VisualRF now display the same AP and client counts through the following enhancements:</p> <ul style="list-style-type: none"> ● Updated RabbitMQ snoop message ● Fixed database flush command ● New debug message to debug client count issues |
| DE22818 | <p>AP and client database tables no longer overload on data and cause the AMP server to slow down due to a database cleanup failure during the nightly maintenance.</p> |
| DE22879 | <p>The IGC encryption option is now set correctly so it does not get disabled automatically after the IGC security configuration is saved under IGC > Networks > Security.</p> |
| DE22892 | <p>The RF Health Report no longer causes out-of-memory issues due to the accumulation of data in stashed arrays, in which data is continuously pushed on top of itself until memory runs out. AirWave now processes data in a stream-like fashion, removing data at the same rate that it is read. Speed has also been optimized in bottlenecks to help improve the flow of data.</p> |
| DE22901 | <p>AirWave performs a safe eval on individual rogue AP classifications to prevent the database cleanup from failing during the nightly maintenance.</p> |
| DE23046 | <p>Whenever a walls.xml file is overwritten due to a clean shutdown or a wall retrieval error in the database, multiple backup copies of the file are saved in the system.</p> |
| DE23193 | <p>When a new VM server is installed on an AirWave deployment, to which IAP devices have successfully connected, the AMP IGC no longer executes duplicate pppoe-username and pppoe-passwd commands for adding and removing the PPPoE username and password under pppoe-uplink-profile. The virtual controller retrieves and displays the proper configuration parameters from the IAP under System > Uplink and contains a VC configuration override link.</p> |
| DE23273 | <p>When a device attempts to connect to a virtual controller, it is automatically added to an appropriate group, which contains a desired configuration that is pushed to all new devices joining the group. If auto-configuration is enabled for a virtual controller, the IGC compares the desired configuration, which is set in the IGC, with the actual IAP configuration to locate mismatches and deltas. The user can automatically or manually handle mismatches and push the delta configurations from the IGC to the IAP.</p> <p>If auto-configuration is disabled for the virtual controller, mismatches and delta configurations can only be handled and pushed to the IAP manually.</p> |
| DE23327 | <p>A umask is explicitly set at the start of the AirWave installation process to ensure proper permissions are granted for installed AMP files, allowing AirWave to install successfully on Redhat 6.7.</p> |
| DE23330 | <p>The schema migration has been updated, and the report cleanup code has been removed so AirWave no longer removes files from the graphs directory and produces empty Network Usage reports after upgrading the Master Console to AirWave 8.0.9.1.</p> |
| DE23518 | <p>The Master Console's Device Inventory report has been fixed to display data even if the Devices widget or 'Include details about every device' option is not selected.</p> |
| DE23532 | <p>Master Console reports are no longer exported for each managed AMP due to multiple FTP/SCPs. The Master Console now exports only one report when the option to export the MC report is set.</p> |

There are no new fixed issues in AirWave 8.0.9.1.

This table lists the fixed issues in AirWave 8.0.9.

Table 18: Issues Fixed in AirWave 8.0.9

| ID | Description |
|--------------------|--|
| DE18515 | Rogue devices manually set as valid are no longer incorrectly reclassified as unclassified by AirWave. This improvement resolves an issue where different rogue devices with the same source IP address were treated as duplicate devices. |
| DE20233 | Cloning a group in AirWave no longer triggers an error which can cause the UI to stop responding. |
| DE20516 | AirWave correctly follows configured folder hierarchy restrictions for RADIUS client authentication failure alerts. This resolves an issue where RADIUS authentication alerts appeared in an incorrect folder. |
| DE20920 | Using the Master Controller IP Address/DNS field under the Configuration > Wireless > AP Installation > Provisioning on the controller to provision an AP no longer causes a configuration mismatch. |
| DE21162 DE21777 | Using the crop option on a .jpg or .png image in the HTML5 version of VisualRF no longer results in a stretched and zoomed image. The crop option now behaves correctly in Flash and HTML5 versions of VisualRF. |
| DE21470 | Filtered data from Syslog messages or SNMP trap reports can now be successfully exported to a CSV file. AirWave no longer exports the entire report when a filter is applied. |
| DE21494 | The RF Performance tab now includes an IAP client health graph. This information was previously only available in the Clients > Diagnostics page. |
| DE21683 | RAPIDS now supports rogue device information in Aruba Instant deployments. AirWave can display information about wireless and wired rogues seen by Instant APs running Instant 4.2. |
| DE21694 | An issue is resolved where a device misconfigured with incorrect SSH credentials could cause errors in the AirWave authentication processes, delaying or preventing the configuration verification of other devices. |
| DE21698 | In the IAP configuration template, custom variables for wlan access-rule and wlan ssid-profile settings that contain spaces are now successfully pushed to the virtual controller. |
| DE21723 | AirWave now correctly handles description information in user derivation rules sent to a controller. This resolves an issue where the inverted commas could be absent from the rule description in the command, causing the command to fail due to a syntax error. |
| DE21730 | AirWave now correctly generates disk usage alerts when disk usage for the AMP server has met or surpassed a defined threshold and the Alert Notification setting Suppress Until acknowledged is set to No . |
| DE21837 | AirWave allows you to correctly remove an old WLAN authentication server from the IGC after adding a new one. This resolved an issue where AirWave could retain the old authentication server and attempt to push both to the IAPs. |
| DE21838 | Beginning with AirWave 8.0.9, firmware distribution over HTTP is disabled by default. To enable this feature, navigate to AMP Setup > General > Firmware Upgrade/Reboot Options and select the Yes radio button for the Enable firmware distribution via http option. This change impacts upgrades from Instant 4.0 and lower. Enable this feature before upgrading from Instant 4.0 or lower. |
| DE21856 | Valid access points marked as neighbors, are no longer incorrectly classified as rogues after upgrading AirWave. The Wireline Aruba Instant Data discovery method for IAPs was removed to prevent this. |
| DE21861 | A nightly maintenance failure due to "unsuccessful jobs: clean_database" has been resolved by moving the operation from the server's RAM to the disk. |

Table 18: Issues Fixed in AirWave 8.0.9 (Continued)

| ID | Description |
|---------|---|
| DE21868 | If the IGC receives only virtual controller configuration information from an IAP but no IAP information, it no longer removes the IAP from its database. The IGC now tries to retrieve the IAP information again when it gets incomplete information. |
| DE21880 | An issue is resolved where adding or removing a URL in the Security > Custom Blocked Page URL page of the IGC caused mismatches in the Instant devices using that configuration. |
| DE21962 | When managing the IAPs with AirWave, the option to deauthenticate a client from AirWave behaves as expected. This resolves an issue where the Deauthenticate Client option on the Clients > Client Detail page appeared to be disabled. |
| DE21964 | When an IAP's configuration is reverted, AirWave now generates an entry in the event and AP logs. This change provides an alert for administrators in cases where a network error occurs while AirWave pushes a configuration update to a virtual controller and the push is unsuccessful. |
| DE21999 | The IGC no longer rejects IP addresses containing 255. The acceptable IP range is now 0.0.0.0 to 255.255.255.255. |
| DE22042 | An issue is resolved where a failure in database migration upon upgrade caused the AirWave UI to stop responding. |
| DE22059 | The IGC correctly saves a configured DHCP Scope and accepts a DHCP Scope imported to AirWave from an IAP. The error message "Policy Change Failed - cannot set no command on multi-allowed command-set, Comparer handles this" is no longer returned when saving a DHCP Scope in IGC. |
| DE22060 | When an Instant AP creates a GRE tunnel to a controller, the VPN session appears as a user in the VPN sessions table, where the user is mapped to the folder ID of the Instant AP. An issue is resolved where the folder ID for this user would not update when the Instant AP was moved to another folder, preventing the network administrator from deleting the folder that previously contained the Instant AP. |
| DE22128 | <p>AirWave displays more accurate AP metrics on the APs/Devices > Monitor > Radio Statistics page due to an improved handling of missing AP data from the controller. In previous releases, missing AP SSID values could cause AirWave to return null values for the following AP metrics:</p> <ul style="list-style-type: none"> ● Radio Errors ● Radio Power ● Usage ● Clients |
| DE22144 | An issue is resolved where a reboot command sent to Instant APs that recently attempted a firmware upgrade caused some of those devices to attempt another firmware upgrade, greatly increasing the amount of time elapsed until those devices appeared in AirWave. |
| US13499 | <p>If the Network Interface Vendor field in the Clients > Client Details page or the By WLAN Vendor graph on the Clients > Overview page displays a large number of unknown vendors, this issue can be resolved by manually running a script to update the AirWave OUI database.</p> <ol style="list-style-type: none"> 1. Access the command-line interface of the AirWave server or appliance using a secure shell (SSH) connection. 2. Log into the device as a root user. 3. Issue the command <code>/usr/local/airwave/bin/update_client_vendor.pl</code> to run the embedded OUI update script. |

This table lists the fixed issues in AirWave 8.0.8.1

Table 19: Issues Fixed in AirWave 8.0.8.1

| ID | Description |
|---------|---|
| DE21669 | The error message "Nightly maintenance failed because of unsuccessful jobs: clean_database" no longer appears on the AirWave UI homepage when the AMP attempts to rebuild the AP Aruba Role table during nightly maintenance. This error only affected users that had deleted an Aruba AP. |
| DE21687 | The error message "Nightly maintenance failed because of unsuccessful jobs: unknown" no longer appears on the AirWave UI homepage while nightly maintenance is running. This message displayed because AirWave attempted to parse the empty error file before maintenance was complete. |
| DE21707 | Generating an RF Health Report using the folder options under Reports > Definitions > Report Restrictions > Summarize report by no longer returns the error message "The server encountered an error while performing your request". |
| DE21715 | Signal and Signal-to-Noise Ratio (SNR) values shown across different tables in the AirWave UI, as well as neighbor client locations in VisualRF, are now correct. Starting in ArubaOS 6.4.2.5, ArubaOS changed the way it communicated Signal and SNR values. This caused incorrect Signal and SNR-related information to display in AirWave. |

This table lists the fixed issues in AirWave 8.0.8

Table 20: Issues Fixed in AirWave 8.0.8

| ID | Description |
|---------|---|
| US13278 | Tzdata on AirWave was updated to tzdata-2015b-1 to account for the 2015 leap second. |
| DE17243 | The Target column in the VisualRF Audit log now updates correctly when a building is deleted. |
| DE18839 | AirWave no longer misclassifies a CPPM device type as an access point when a trigger is set up. The device type ClearPass Policy Manager was added as a trigger condition. The device type in the Device Setup page changed from Aruba ClearPass Policy Manager to ClearPass Policy Manager . |
| DE18679 | In VisualRF, the x and y coordinates now adjust to the correct size when a client is moved within a floor plan boundary. |
| DE19572 | The proper heatmap now generates correctly when a planned AP is moved. |
| DE19913 | The Device Setup > Certificates page now more quickly; the database query for the tables of certificates was optimized. |
| DE19947 | The IAP now connects successfully to AirWave when any port is changed. |
| DE20489 | Heatmaps now display properly for the Cisco 3700I LWAPP when it is connected to a Cisco 5760 running at 5 GHZ. |
| DE20493 | The AMP now correctly displays the SSID for Juniper and Trapeze APs on the APs/Devices > Monitor page. |
| DE20770 | The Rogue Overview and Rogue > List pages now load properly for users. This transaction caused deadlocks in the database. |
| DE20894 | The VisualRF ListView page no longer loads slowly. The page load performance time has been improved. |
| DE20895 | Depending on the IAP configuration, more messages were received from the AP than required and this caused performance issues. VisualRF can now clobber the incoming messages. To clobber the messages, add svg.clobber.aps=true in the /usr/local/airwave/lib/java/svg property file. |

Table 20: Issues Fixed in AirWave 8.0.8 (Continued)

| ID | Description |
|--------------------|--|
| DE20951 | AirWave no longer crashes unexpectedly due a memory fragmentation. Two non-GUI settings were added to control when ALC daemons terminate. By default the ALC now recycles after completing 60K payloads or after growing past 4G in memory. |
| DE20963 | Local firmware versions are now listed in the Group > Group name >Firmware drop-down menu in the Desired Version pane. |
| DE21010 | The VisualRF Deployed Devices pop-up displays APs without a delay. Previously, when navigating to a floor in VisualRF, clicking Edit and then Add Deploy Devices caused the pop-up to load quickly but it took several minutes to display all the APs. |
| DE21022 | An extra slash in the XML file has been removed and no longer adversely affects the floor mapping. |
| DE21023 | VisualRF now accepts negative integers as floor numbers. |
| DE21038 | The AMP now passes the band value in XML. This allows the AMP to calculate the channel overlay in VisualRF more efficiently. |
| DE21065 | All relevant commands are executed successfully when pushing an AirWave template, which contains wired-port profiles, from AirWave to the IAP. |
| DE21073 | The AMP now considers the build numbers of ArubaOS when upgrading a controller. This allows the AMP to accept a new build of the currently installed version of ArubaOS as an upgrade. |
| DE21078 | AMP no longer sequentially scans the aggregate session table for each dimension when running nightly maintenance. This change reduces the time required for AMP to complete clean_database.pl. |
| DE21082 | The Juniper ND Hostname/IP Address field on AMP Setup > Third Party Integration is now blank instead of displaying 0.0.0.0 after a fresh AMP installation or upgrade. |
| DE21098 | The split-tunnel option now works properly when adding a centralized DHCP scope on the Groups > Instant config > DHCP server page. |
| DE21134 DE21119 | When IAPs are added to an IGC group, the IAPs all sync properly now after the devices are upgraded to the group enforced firmware. |
| DE21121 | This release of AirWave introduces a security fix for CVE-2014-8159. |
| DE21131 | Exporting AP run commands from the IAP > Monitor page now runs without returning the Request URI is too long error. |
| DE21137 | An IGC bootstrap error no longer incorrectly appears in igc.log when attempting to view the IGC GUI when the IGC is disabled. |
| DE21156 | Editing and deleting of the Aruba controller time-range ACL profiles is now supported in AirWave. |
| DE21170 | The IGC now generates the correct order of commands for the WLAN profile. The IGC now pushes the auth-server command before pushing the auth- survivability command. |
| DE21196 | The IGC now sorts the commands no wlan ssid-profile and no wlan access-rule correctly when using the del ssid profile command to delete the SSID profile on the IGC Network page. |
| DE21213 | VisualRF now supports the configuration of floor numbers with decimals up to one digit in HTML5. |
| DE21214 | The AMP no longer attempts to push any system default ACLs, the RAP Whitelist, or user roles to Aruba controllers. Since ArubaOS 6.3, the Aruba controller has treated system default ACLs, the RAP Whitelist, and user roles as part of the global configuration. When AMP tried pushing those values to the controller, it resulted in an error and no other configuration changes were pushed. Additionally, opcode has been deleted from the policy rule any any svc-kerberos redirect opcode 51 queue low position 1 since it does not exist on the controller. The policy rule now reads as any any svc-kerberos redirect 51 queue low position 1 |

Table 20: Issues Fixed in AirWave 8.0.8 (Continued)

| ID | Description |
|---------|--|
| DE21231 | Executing the command show ap monitor arp-cache from the IAP > Monitor page no longer returns an AP Monitor ARP Cache error. |
| DE21239 | After Client Session reports are run, AirWave now deletes unneeded temporary databases entries. |
| DE21244 | This releases provides to the performance of the Groups > Lists page. |
| DE21247 | The MAC ID now displays on the Controller Monitoring page for the Cisco 5760. |
| DE21252 | The IGC configuration performance time has improved. |
| DE21256 | When a planned AP is added and automatched to a deployed AP using MAC addresses, heatmaps correctly appear in VisualRF. When automatching, AMP now checks whether a radio configuration already exists for a particular ID and only attempts to add the new one after removing the old. |
| DE21261 | The VisualRF audit log is now less verbose and easier to read. VisualRF server log events are now recorded in /var/log/visualrf/visualrf_server_audit.log and only user events are logged in /var/log/visualrf/visualrf_audit.log . |
| DE21298 | Improvements to the performance of the RAPIDS > Overview page were made. |
| DE21302 | In VisualRF, the buttons Delete Planned and Delete Deployed and related warning pop-up text now include the word all . The buttons now say Delete All Deployed Devices and Delete All Planned Devices . Additionally, if a single AP is selected, the Delete All options are hidden and only the Actions sub-menu is visible. |
| DE21307 | The Apply All button now works properly after adding a new route and saving the changes. Previously, this button was grayed out. |
| DE21309 | The IGC configured Network page now displays properly. Previously the default configuration Network page displayed when trying to view a network configuration. |
| DE21311 | Catalog errors preventing heatmaps from appearing for some APs in VisualRF are resolved. |
| DE21358 | In the IGC, the LED display option in General tab now works properly. |
| DE21632 | The internal Captive Portal page under Instant Config now works properly and can be edited. |
| DE21364 | Changing the order of authentication servers on the Security tab now works properly on the IGC. |
| DE21376 | Changing a wired profile on a network port now displays properly on the IGC. |
| DE21382 | The average RRD values are now calculated correctly. |
| DE21386 | In the IGC, enabling and disabling the Security Firewall setting options display correctly after saving and applying changes. |
| DE21388 | On the AP List page, an IGC IAP's configuration state is now displayed accurately instead of only displayed Verifying after upgrading AirWave. |
| DE21399 | Dragging APs when adding planned APs now works correctly in Firefox. |
| DE21457 | When creating a DHCP Scope, the AMP automatically creates invalid DHCP Scope entry (CL2) with undefined type and VLAN. This entry can now be edited. |
| DE21462 | IAP cluster SSIDs are now displayed correctly on the Groups > List page. |
| DE21471 | Clicking the magnifying glass icon in the Add Deployed Devices list now filters the list as expected. |

Table 20: Issues Fixed in AirWave 8.0.8 (Continued)

| ID | Description |
|---------|---|
| DE21511 | Users are now able to adjust the Environment Factor , by using the environment slider, when uploading a new floor plan. Additionally, similar capabilities are available through the Region Properties tab. Upon adding a planning region to a floor, users can click the properties tab and use the Coverage Calculator window to estimate the number of planned APs in a given region. |
| DE21520 | AirWave now sets the HttpOnly flag in cookies to safeguard against cross-site scripting attacks. |
| DE21561 | The AP Group page time to load performance has improved. |

This table lists the fixed issues in AirWave 8.0.7.1

Table 21: Issues Fixed in AirWave 8.0.7.1

| ID | Description |
|---------|--|
| DE21201 | This release of AirWave includes updated openssl packages to resolve the affected vulnerabilities described by Red Hat Security Advisory RHSA-2015:0715-1. |

This table lists the fixed issues in AirWave 8.0.7

Table 22: Issues Fixed in AirWave 8.0.7

| ID | Description |
|---------|--|
| DE18310 | The config_verifier log no longer displays incorrect warnings saying that device mismatch has occurred on the Audit tab. |
| DE18556 | In VisualRF, the View in Google Earth link now works properly. |
| DE19018 | An issue is resolved where AirWave was not pushing rogue AP reclassification commands to an IAP |
| DE19822 | The Instant configuration page now loads properly. |
| DE19841 | In VisualRF, SVG files is now scale correctly when cropped thus allowing floor plans to be uploaded accurately. |
| DE19898 | SSIDs in the Radio list now show what is being broadcast at that moment. |
| DE20139 | VisualRF walls now appear in the proper place after upgrading from AirWave 7.7.11 to AirWave 8.0.4.1. |
| DE20152 | APs listed from the Controller Monitor page or the group/folder view, now show the down radio indicator. The AP list view also shows if the radio is enabled or disabled. |
| DE20164 | An issue is resolved where floor plans in a .dwg format could not be uploaded using the Firefox web browser. |
| DE20239 | The Device UP and DOWN alerts are no longer getting auto acknowledgments and now work properly. |
| DE20269 | IAP no longer shows as being mismatched when there are no mismatches in the IGC. |
| DE20302 | In VisualRF, the error message, "The file you are trying to upload might be corrupted. Please check the file and try again" inaccurately displayed. This no longer occurs. |
| DE20347 | In Visual RF, a campus relationship can be dropped from a building when the strongest permission is set to admin and when the object has no parents. |
| DE20357 | The Policy Version for Specific IAP Groups running the IGC now maps properly on Firefox. |
| DE20874 | When updating the Syslocation setting for each virtual controller, the IGC no longer indicates the virtual controller as down in AirWave, even though it is up and running. |

Table 22: Issues Fixed in AirWave 8.0.7 (Continued)

| ID | Description |
|---------|---|
| DE20889 | Configurations with a capital letter in the Community string can be pushed to the Mobility Access Switch using Activate. |
| DE20895 | VisualRF no longer times out and now works properly. |
| DE20903 | A crash no longer occurs when logging into amp_events . |
| DE20922 | Defining the stationary device in Visual RF HTML now works properly. |
| DE20424 | Polling now works correctly for the Motorola RSF4000. |
| DE20949 | List View transactions no longer slow down the AirWave UI process. D |
| DE20479 | This release of AirWave introduces a security fix for CVE-2015-1390. |
| DE20489 | Heatmaps are now correctly displayed in VisualRF for Cisco 3600 LWAPPs terminating on a Cisco 5760. |
| DE20536 | This release of AirWave introduces a security fix for CVE-2015-1391. |
| DE20537 | Closed a cross-site scripting (XSS) GET request vulnerability. |
| DE20546 | Captive Portal logos are now successfully pushed using the IGC. |
| DE20559 | A configuration from a controller that gets its licenses from a centralized licensing server can be correctly imported into AirWave. |
| DE20571 | AMP now reports AP uptime of APs connected to a Cisco 5760. |
| DE20587 | The AirWave UI no longer becomes unresponsive due to a database deadlock issue. |
| DE20596 | When the IGC is enabled, clicking on the Username and Password fields on Configuration > Security > Users for Internal Server no longer returns an Invalid warning. |
| DE20626 | A crash no longer occurs when navigating to the Audit page when you select a Aruba Controller or the Manage page for an AP. |
| DE20633 | Floorplans are no longer incorrectly deleted when tasks for polling sites are removed. |
| DE20643 | Aruba AP-214 and AP-215 Radio MAC addresses are populated from the AP device configuration. |
| DE20658 | The following OUIs have been added to the AirWave database: 10:08:B1 (HonHaiPr), 38:B1:DB (HonHaiPr), 34:E6:D7 (Dell), AC:87:A3 (Apple) 90:FD:61 (Apple), F4-4E-05 (Cisco), and FC-5B-39 (Cisco). |
| DE20715 | Upper case letters are allowed in the URL field for configuring External Captive Portal in the IGC. |
| DE20770 | To prevent the RAPIDS > Overview/List Page from becoming inaccessible, AirWave now deletes old discovery events for each discovery agent except the most recent. |
| DE20805 | The links for Rogues and Suspected Rogues under the RAPIDS classifications list on the RAPIDS > Overview page have been re-added. The RAPIDS Classification list, which is located on the RAPIDS > Overview page, was not displaying the Rogues and Suspected Rogues links. These links now display properly. |
| DE20935 | The IGC UI now displays the correct value for LDAP server and matches the value in the IAP UI. |
| DE20943 | This release of AirWave introduces a security fix for CVE-2015-2201. |
| DE21024 | The User Inventory report now generates more quickly with improved performance. |
| DE21041 | This release of AirWave introduces a security fix for CVE-2015-2202. |

This table lists the fixed issues in AirWave 8.0.6.3

Table 23: *Issues Fixed in AirWave 8.0.6.3*

| ID | Description |
|---------|--|
| DE20803 | This release of AirWave introduces a glibc security update (RHSA-2015:0092-1). See CVE-2015-0235 for more information. |

This table lists the fixed issues in AirWave 8.0.6.2

Table 24: *Issues Fixed in AirWave 8.0.6.2*

| ID | Description |
|---------|---|
| DE20587 | AirWave UI access now works properly. Previously, access failed when AirWave ran out of database connections. |
| DE20617 | VisualRF no longer loses memory due to a leak in AbstractTransactionAwareService . The number of threads that a service can use is limited to 12. |
| DE20633 | Floor plans now display properly in AirWave 8.0.x. A new separate file for auditing deleted items called visualrf_audit_del.log was added. This audit captures deleted campus, building, site, and AP information. |

This table lists the fixed issues in AirWave 8.0.6.1

Table 25: *Issues Fixed in AirWave 8.0.6.1*

| ID | Description |
|---------|--|
| DE20568 | On VisualRF, the client and rogue location on the floor maps now works properly for all devices. |

This table lists the fixed issues in AirWave 8.0.6

Table 26: *Fixed Issues in AirWave 8.0.6*

| ID | Description |
|---------|--|
| DE16753 | In the IGC, the uplink priority list now works properly no longer generates an error index when eth1-4 were enabled . |
| DE18442 | In VisualRF, the Edit tab removed all objects of different types. Now the Action menu has been deprecated with functionality was moved to the Dynamic Popup menu and the Action section. |
| DE18601 | In VisualRF, all columns in the UI are properly aligned. |
| DE18917 | In the IGC, Need seven minutes to change group basic's setting when group already has 2000 devices. |
| DE19124 | In VisualRF, the client health model now automatically updates when a new client health value is added. |
| DE19197 | DWF files are now uploaded correctly to VisualRF in the HTML5 mode. |
| DE19416 | Newly added APs now display a heatmap properly on VisualRF. |
| DE19451 | Console refresh issues regarding the list view have been fixed and now works properly. |
| DE19621 | Stale PEF entries are now deleted from all pef_dim_tables during nightly maintenance. |
| DE19638 | AP Audit issues that occurred when the IGC was enabled have been fixed. |

Table 26: Fixed Issues in AirWave 8.0.6 (Continued)

| ID | Description |
|---------|--|
| DE19641 | In the IGC 8.0, issues with the error log in <code>async_logger_client</code> have been fixed. |
| DE19690 | The IGC external-captive-portal is now deleted if referenced by SSID. |
| DE19711 | Monitor lock issues have been resolved and it now works properly in IAP when the IGC is enabled. |
| DE19712 | In the IGC, Ethernet 0 now supports wired-instant profile. |
| DE19719 | During Audit and Import, mismatch sequences no longer appear. |
| DE19744 | Multi-byte username and SSID issues no longer cause AppRF to crash. |
| DE19745 | The IAP IP address now updates correctly after it is changed in the IGC. |
| DE19746 | The AirWave server now cleans up the RRD files based on the historical retention setting properly. |
| DE19767 | AirWave now shows the IP of the APs associated to the Cisco WLC 5760 on the AP Monitor page. |
| DE19779 | VisualRF performance improvements now prevent VisualRF from crashing during the startup inventory service check. |
| DE19812 | Cluster AP name changes now work properly and appear in the IGC. |
| DE19821 | In the IGC, the DHCP command now works properly. |
| DE19847 | When a VC is deleted from the AirWave cluster it no longer displays as being down. |
| DE19858 | A new field in the Group > Basic page was added that allows you to ignore the folder changes of the device. This applies only for Aruba switches provisioned through Activate, DHCP or the switch CLI. |
| DE19859 | The MAS ZTP VPN tunnel, changing the SNMP community in the Group configuration now works properly with no errors occurring in the syslog or traps. |
| DE19876 | In the IGC, a new validation value for disallow role number has been added on the Service page. |
| DE19902 | In the IGC the number of the users for an internal server now shows the correct value, and the Wi-Fi setting for uplink can now be deleted. |
| DE19903 | In the IGC, all separate accounting server issues work properly for version Instant 4.1.1. |
| DE19904 | The AMP whitelist Edit box IP list works properly now. |
| DE19905 | In the IGC, the no accounting-server command now works properly when editing the account server option. |
| DE19906 | In the IGC, when switching the accounting mode, the Apply button now works properly. |
| DE19907 | In the IGC, when switching the accounting mode, the command no accounting-server now works properly. |
| DE19908 | In the IGC, issues for separate accounting servers for version Instant 4.1.1 now perform correctly. |
| DE19909 | In the IGC, the Facebook setting now works properly in the WLAN security page. |
| DE19912 | In the IGC, the Wi-Fi setting on the System > Uplink page now shows the correct value when you delete those uplink values. |
| DE19917 | VisualRF performance works properly now. |
| DE19945 | In the IGC, support is now available for a new channel for the 802.11ac radio. |
| DE19959 | Viewing a certificate now works properly. |

Table 26: Fixed Issues in AirWave 8.0.6 (Continued)

| ID | Description |
|---------|---|
| DE19960 | The IAP no longer fails to log into AirWave in cert mode. |
| DE19964 | <p>The default values for the rf-arm-profile and HTSSID profiles have changed.</p> <p>In the ARM Profile, the default values for Client Match Load Balancing and Client Threshold is now 30 and Client Match Sticky Client Check SNR (dB) is 18 starting with AOS 6.3.1.7.</p> <p>In the HTSSID profile, the max number of MSDUs in an A-MSDU on Background AC, Max number of MSDUs in an A-MSDU on Best-effort AC, Max number of MSDUs in an A-MSDU on Video AC. All the three field defaults are now 2 instead of 3 in AOS 6.3.1.7 and later.</p> |
| DE19972 | IAP now supports chained server certificate upload instead of single server certificate upload. |
| DE19973 | In the IGC, the uplink priority list works properly and no longer generates an error index when Ethernet 1-4 were enabled for uplink. |
| DE19974 | When guest security is selected, AirWavenow supports a Facebook secret command. |
| DE19979 | The AirWave UI now performs properly and no longer crashes after a reboot. |
| DE19983 | In the IGC, all server drop-down lists now work properly. |
| DE19984 | In the IGC, the Uplink tab on System and Settings page is now hidden if it is in Group mode. |
| DE19993 | The VC no longer stays in a verifying state when a new IAP cannot be created. |
| DE19995 | In VisualRF, auth in iconainer.find(id) is no longer commented out. AP Group/Folder drop-down lets read-write users add new APs to floorplans. |
| DE19998 | Adding an AP to VisualRF no longer sets the Notes column value to null. |
| DE20011 | Deleting all licenses and then re-adding them no longer creates duplicate daily or weekly report definitions. |
| DE20013 | A license now saves unassigned user role information properly and no longer crashes. |
| DE20017 | VisualRF works properly when floorplans are imported. |
| DE20025 | The kernel security update (RHSA-2014:1392-2) has been applied. |
| DE20030 | In VisualRF, heat maps are now updated when moving APs. |
| DE20032 | The AirWave UI now displays the proper AirWave release. |
| DE20033 | AirWave now queries information from the AP_detail.xml file correctly. |
| DE20034 | In the IGC, an issue is resolved where SSIDs could not be created if there were spaces in the SSID name, for example, "public - mobile". |
| DE20036 | In the IGC, the second authentication server now performs properly when you create an SSID with a wireless or wired guest. |
| DE20044 | In VisualRF, only the error code and message appear, and not the entire HTTP response, when the VisualRF backup fails. |
| DE20056 | In the IGC, the message "Processing" appears on the cluster list when a VC is verifying or applying a configuration. |
| DE20057 | In the IGC, the authentication server 1 no longer shows the selected value of authentication server 2 of the wired employee profile. |
| DE20070 | The AMP Whitelist page now displays all information properly. |

Table 26: Fixed Issues in AirWave 8.0.6 (Continued)

| ID | Description |
|---------|--|
| DE20071 | The Duration column now shows the correct value on client lists. |
| DE20085 | The Licenses table displays changed information more quickly now. |
| DE20103 | The report definitions now load properly and efficiently after upgrading. |
| DE20105 | In the IGC, the syslocation now performs properly regarding multi-edit. |
| DE20106 | In the IGC, the VC and IAP monitor page now properly shows the note message. |
| DE20107 | In the IGC, the VC status now works properly when a note message is modified. |
| DE20110 | AMP charts now correctly display Chinese characters. |
| DE20115 | This release of AirWave includes a Wget security update for RHSA-2014:1764-1. |
| DE20117 | After OVA deployment, AMP restarts daemons to prevent the AMP from becoming stuck. |
| DE20125 | The IGC now correctly handles a change in Virtual Controller uplink. Re-adding the Virtual Controller after an uplink change is no longer required. |
| DE20127 | When an Ethernet port network assignment is changed from one network to another, the deselected network is made available for use by other Ethernet ports and appears in the Network Assignments drop-down menu for each port. |
| DE20128 | In the IGC, the configuration for enforce uplink value is correctly pushed to devices. |
| DE20129 | The IGC is now able to successfully push commands from the uplink page. |
| DE20140 | AirWave now successfully pushes the no accounting-server command when a profile is edited. |
| DE20141 | AirWave pushes commands to the virtual controller in the correct order when editing the auth server configuration. |
| DE20143 | When viewing the Internal User Number, the actual internal user value is now displayed. |
| DE20153 | WCS files are now imported correctly into VisualRF using Safari, Firefox, or Chrome. |
| DE20158 | Weekly reports no longer timeout during execution and no longer return empty Client and Usage graphs. |
| DE20165 | The IGC now ignores any IAP Facebook commands since they may be different for each Virtual Controller and are not configurable. |
| DE20166 | Deleting an access rule from the IGC no longer causes a mismatch. |
| DE20169 | The IGC no longer allows the following characters to be used: % and &. |
| DE20171 | After deleting all APs from AirWave, all APs can be re-added successfully. This resolves an issue where only a subset of detected APs were added. |
| DE20188 | The Master Console Overview, Usage, and Clients graphs now only return data from the last complete update, preventing incomplete data being displayed. |
| DE20189 | Quotation marks no longer erroneously appear around input text in the Internal Captive Portal configuration tab when the text is retrieved from the database. |
| DE20190 | Editing an existing inbound firewall rule no longer causes the rule to appear on two lines. |
| DE20191 | Changes made when editing an existing External Captive Portal are now saved correctly. |
| DE20192 | A reboot log for resolve duplicate VC keys and per-ap-settings commands has been added. |

Table 26: Fixed Issues in AirWave 8.0.6 (Continued)

| ID | Description |
|---------|---|
| DE20193 | RADIUS Authentication configuration no longer incorrectly changes to Authentication Text after creating an External Captive Portal with RADIUS Authentication. |
| DE20194 | The IGC now allows the change IP address retrieval method from manual to DHCP on the Access Point > General page and does not return any errors. |
| DE20197 | Deleting the Services > Network Integration configuration from the IGC no longer causes a mismatch. |
| DE20201 | GlusterFS RPMs have been removed from AirWave. |
| DE20208 | The Discard Pending Changes dialog no longer appears when moving from System > Admin in the IGC when no changes were made. |
| DE20215 | Information displayed by AirWave is consistent with the information displayed on the Audit tab; AirWave does not show a Virtual Controller mismatch when one does not actually exist. Additionally, a new indicator has been added that displays "Verifying" while AMP is waiting for Instant running config. |
| DE20217 | Logged-in users are no longer able to see any file viewable by Apache. |
| DE20229 | Improvements in AMP's handling of state messages to prevent an internal server error in amp_events. |
| DE20235 | SSID bandwidth tracking for SSIDs with Chinese characters on IAPs no longer fails. |
| DE20244 | New uplink priority items configured in the IGC now appear as expected. |
| DE20245 | This release of AirWave includes a kernel security update for RHSA-2014:1843-1. |
| DE20258 | In the IGC, subnet addresses in ACL rules are now truncated according to netmask to prevent a mismatch for too long access rules. |
| DE20259 | Editing an AppRF rule to add an option for Application Throttling and remove another rule now works as expected. It no longer deletes the old item without removing the new one. |
| DE20260 | The value for the set-role-machine-auth , set-role-mac-auth , and set-role-pre-auth are no longer incorrectly set to False when they are already false. |
| DE20261 | In the IGC, creating a WLAN profile with the WMM option configured no longer results in policy change failure. |
| DE20262 | Deleting a WMM option from the Networks > General page in the IGC no longer returns a Policy Change Failed error message. |
| DE20278 | On the IGC system page, the value for the auto join option is now correctly reflects the configuration. |
| DE20280 | The IGC now sends the correct commands for the Disable SSID on uplink failure option. |
| DE20281 | In the IGC, the creation of centralized and local DHCP scopes now works as expected. |
| DE20282 | The maximum length of an SSID name in the IGC increased to 32 from 31 to reflect the Instant software. |
| DE20291 | Safe Migration of the failover AMP license has been enhanced to prevent license failure on the second make. |
| DE20295 | Airtime and air radio options can now be saved in the WLAN profile in the IGC. |
| DE20296 | SSID limits configured in the IGC are now correctly enforced. |
| DE20297 | The IGC now accurately displays the Instant configuration and matches the corresponding Instant UI. |
| DE20298 | LDAP servers no longer appear in the Authentication Server drop-down menu when termination is disabled. |

Table 26: Fixed Issues in AirWave 8.0.6 (Continued)

| ID | Description |
|---------|--|
| DE20306 | VisualRF performance has been improved by resolving a number of database issues causing campus and building floorplans to load slowly. |
| DE20313 | The IGC no longer adds quotation marks around existing welcome text or policy text when opening the dialog to edit the text. |
| DE20316 | The release introduces performance improvements of the new device page in the IGC. |
| DE20323 | The IGC now correctly saves the values for access rule, for to particular server, except to a particular server, and to domain name instead of displaying 0.0.0.0. |
| DE20324 | The IGC wired security page now supports the IAP Facebook commands. |
| DE20325 | In the IGC, an error message is now displayed when more than one port is configured as an uplink-enable port. |
| DE20326 | The maximum length of a hostname in the IGC increased to 32 from 31 to reflect the Aruba Instant software. |
| DE20334 | The IGC wired network wizard page now blocks the creation of duplicate network names. |
| DE20335 | In the IGC, when an internal server is selected as the auth server, authentication survivability is disabled and cannot be changed. |
| DE20336 | The IGC uplink item priority index now performs as expected. |
| DE20343 | The AMP now displays a configuration error when the IGC has a configuration error instead of displaying a mismatch. |
| DE20344 | The config process error status reporting from AMP database has been improved to prevent inaccurate reporting of Virtual Controller status. |
| DE20345 | Editing access rules in the IGC no longer returns an error when done correctly. |
| DE20359 | When AP license limit is reached, AMP now displays an error messaging informing the user that no additional APs can be added. |
| DE20360 | The restore option on the Audit page now works as expected and no longer requires the user to manually refresh the browser. |
| DE20367 | On the Network page in the IGC, a validation has been added when deleting a wired or wireless profile to prevent a mismatch. |
| DE20369 | Using multi-edit for syslocation in the IGC now allows spaces in the parameter string. |
| DE20370 | In the IGC, the TACACS Accounting checkbox now appears a TACACS server is chosen as the auth server. |
| DE20371 | The auth server can now be edited successfully from the System > Admin page in the IGC. |
| DE20381 | On the L3 Mobility tab in the IGC, the IP address will automatically update to match the subnet when the subnet is modified. |
| DE20382 | The IGC now correctly pushes SNMPv3 configuration to devices |
| DE20386 | Zero (0) can now be typed into the Port field in the SNMP Trap Receivers dialog box in the IGC. |
| DE20387 | In the IGC, on the WLAN General page, the Disable SSID on uplink failure checkbox is now unchecked by default. |
| DE20390 | After configuring and applying L2 DHCP server setting in the IGC, the Option Type configuration is saved correctly. |

Table 26: Fixed Issues in AirWave 8.0.6 (Continued)

| ID | Description |
|---------|--|
| DE20391 | In the IGC, the domain name is no longer saved as false when the Domain Name field is left empty on the Access Point page. |
| DE20392 | The Centralized DHCP Scopes configuration dialog in the IGC now displays correctly in Mozilla Firefox. |
| DE20393 | The DLNA Media and DLNA Print checkboxes on the Service > Airgroup page in the IGC remain checked when changes are saved. |
| DE20394 | The IGC now allows the use of spaces in non-Virtual Controller AP names. |
| DE20395 | SNMPv3 Users are correctly deleted from the System-Monitor page in the IGC; they no longer exist after applying the changes to delete them. |
| DE20396 | The IGC now requires at least eight characters in the password fields on SNMPv3 page from Instant 4.1.1. |
| DE20397 | The OK button on the VPN Tunnel profile configuration page now works correctly. |
| DE20398 | An 802.11ac new channel option at customize valid channel was added to the RF page in the IGC. |
| DE20399 | The IAP configuration no longer disappears, resulting in an IGC mismatch when the Restore Default Value option is used on the RF Radio page. |

This table lists the fixed issues in AirWave 8.0.5

Table 27: Fixed Issues in AirWave 8.0.5

| ID | Description |
|---------|--|
| DE16614 | When the "Prefer AMON vs SNMP Polling" option is enabled, the number of clients reported in AirWave now matches the number of clients that are reported on the controller. |
| DE16649 | Unaudited stacked MAS member switches no longer appear on the APs/Devices > Mismatch page. |
| DE18556 | Viewing an outdoor AP location in Google Earth now works properly. |
| DE18915 | The Modify Devices Apply All option now works with remote users. |
| DE18937 | VisualRF no longer displays campuses and the location of APs in folders outside of the user's access level. |
| DE19072 | The VisualRF > List page now appears properly and no longer displays the zoom bar. |
| DE19101 | The VisualRF Campus view background can be set to None from a custom background image. |
| DE19299 | AirWave refreshes the FQDNs of APs when an entry is not available in the dns_result table periodically. |
| DE19444 | Pagination now works for the bulk override feature. Accepted parameters include: <ul style="list-style-type: none"> start_row: this number is the first row of the table. Default is 0. page_length: this number indicates how many records to send in API response. has_next: this indicates if the table has more records in next page. |
| DE19445 | The AirWave Audit page performance issues have been fixed. |
| DE19503 | An HTTP response splitting vulnerability in the network management framework on the remote web server has been resolved. |
| DE19544 | The headers in a CSV file from a connected client list are now in English. |
| DE19547 | An Aruba S1500-24 Mobility Access Switch can be successfully upgraded and rebooted from AirWave. |
| DE19590 | Down devices in the Monitor page no longer show the uptime. |

Table 27: Fixed Issues in AirWave 8.0.5 (Continued)

| ID | Description |
|--------------------|---|
| DE19622 | Setting a table's custom page length to something other than a number no longer causes AirWave to crash. |
| DE19626 | The AppRF > Destinations > Summary total destinations count now works properly. Previously the summary total displayed the page length number instead of the number of entries in the Destination list. |
| DE19652 | An explanation now displays if a license is not verified during migration. |
| DE19667 | The Client Detail page performance has been improve by optimizing the query for rogue client historical data. |
| DE19674 | A name displays with a link to down devices with AP IDs. |
| DE19678 | AirWave includes security fixes for Red Hat Enterprise Security Advisory RHSA-2014:1167-1, which resolves vulnerabilities that could allow users to gain additional system privileges, , leak memory to the user space, or cause the system to stop responding. |
| DE19680 | UCC calls now display on the Client Detail page. |
| DE19698 | The Whitelist populates variables to virtual controller. |
| DE19704 | An IAP can be verified and configured now as long as the firmware is upgraded successfully. |
| DE19705 | To improve the loading time of the AppRF tab, missing indicies have been restored to the start and stop columns on aggregate. |
| DE19706 | JSON encoding has been enhanced to prevent AMON data loss and Papi/AMON graph spikes. |
| DE19707 | The error messages displayed on the licensing tab now accurately reflect the error instead of displaying inaccurate information. |
| DE19718 | Show commands can now be executed when logged in with view-only credentials. |
| DE19721 | A timeout was added back to the last_process mmap to help prevent the UI from becoming inaccessible. |
| DE19722 | IAP cert auth performance has been improved. |
| DE19730 | The IGC displays the slave IAP IP address on the access point page. |
| DE19737 | The VisualRF backup script no longer stops the current running VisualRF process. |
| DE19740 | The visualrf_backup.pl no longer fails. |
| DE19742 | AMP no longer inverts the Radio Mode for 2.4 GHz and 5.0 GHz. The correct information is displayed for the appropriate radio. |
| DE19743 DE19138 | The HTML5 UI now matches the Flash UI in older versions of AirWave and correctly draws holes or gaps in the wireless coverage for heatmaps. |
| DE19749 | Acknowledge and Delete buttons are no longer displayed on the alert lists for read-only users. |
| DE19752 | The character length for airwave-ip and airwave-backup-ip is changed from 15 to 127 to allow for domain name, IP, and port. |
| DE19754 | OS details are now accurately displayed for iPhone 6 devices. |
| DE19757 | Role assignment rules can now be reordered in the IGC. |
| DE19762 | Template versions can now be updated when unsupported commands are shown. |

Table 27: Fixed Issues in AirWave 8.0.5 (Continued)

| ID | Description |
|---------|---|
| DE19781 | This version of AirWave includes a fix for the Bash Code Injection Vulnerability via specially crafted environment variables, which was announced publicly on September 24, 2014. See CVE-2014-6271 and CVE-2014-7169 for more information. |
| DE19782 | The attenuation grid is recalculated when the transmit power for planned APs is changed by the user. |
| DE19799 | The report process for IAP devices has been made more robust. |
| DE19800 | The config push result has been added to the IGC log file. |
| DE19813 | The Discard Pending Changes pop-up message no longer appears when navigating away from Network > Security if no changes are made. |
| DE19820 | On the DHCP server page, the domain name in the dialog is limited to 64 characters and in panel is limited to 32 characters. |
| DE19824 | This AirWave release includes a fix for the Authenticated Privilege Escalation Vulnerability. See CVE-2014-8368 for more information. |
| DE19842 | Client list views and client search have been optimized to reduce the loading time of client data. |
| DE19878 | VisualRF now works properly during startup, visualrf_bootstrap file deletion is not required. |
| DE19884 | Abbreviations for standard protocols are now used in AppRF in regards to Instant devices. |
| DE19885 | In the IGC System > Admin page, the cursor no longer jumps to the Password field when characters are entered in the Username field. |
| DE19897 | AMP now correctly interprets 2.4 GHz and 5.0 GHz IAP radio information, preventing VisualRF from displaying a wrong heatmap. |
| DE19922 | Auditing is still performed if AMP has the correct credentials to perform an audit but the encrypt disable command fails. |
| DE19931 | This release of AirWave eliminates exposure to the POODLE SSL vulnerability. See CVE-2014-3566 for more information. |
| DE19940 | This release of AirWave closes two OpenSSL vulnerabilities, an SRTP Memory Leak and a Session Ticket Memory Leak. See CVE-2014-3513 and CVE-2014-3567 for more information. |
| DE19965 | This version of AirWave includes an update to a Critical Java Security update (RHSA-2014:1657-01). |

This table lists the fixed issues in AirWave 8.0.4.1

Table 28: Fixed Issues in AirWave 8.0.4.1

| ID | Description |
|---------|---|
| DE19781 | This version of AirWave includes a fix for the Bash Code Injection Vulnerability via specially crafted environment variables, which was announced publicly on September 24, 2014. See CVE-2014-6271 and CVE-2014-7169 for more information. |

The table below lists fixed issues in AirWave 8.0.4.

Table 29: Issues Fixed in AirWave 8.0.4

| ID | Description |
|---------|--|
| DE18124 | An update to RPM Security (RHSA-2012:0451-3) has been added. |

Table 29: Issues Fixed in AirWave 8.0.4 (Continued)

| ID | Description |
|---------|--|
| DE18292 | Modifications made to the default profile of the Gigabit Ethernet Group are saved and pushed to devices as expected; AirWave no longer returns the error Invalid slot(ALL) for Interfaces. |
| DE18502 | Read-only users can now use location history. |
| DE18888 | AirWave can push passwords with special characters in the management user and enable passwords. |
| DE19049 | Creating and saving a custom report using the config detail widget, while not editing the email settings, no longer returns the error Cannot email configuration audit widget in CSV format." |
| DE19054 | Devices can now be filtered based on a single SSID and the output will contain all devices that are transmitting the selected SSID. This includes those devices that are transmitting multiple SSIDs. |
| DE19059 | When creating multiple profiles in AirWave in the Group Config UI, the newly created profiles are not incorrectly deleted if an error occurs when saving and applying the profiles. |
| DE19066 | When you select a Mobility Access Switch from the APs/Devices > List page, the Switch Role column now displays the switch's actual role (Primary, Secondary, etc.) instead of an integer value. |
| DE19068 | AirWaveno longer uses the same defaults for switches and controllers, which prevents a mismatch for Download Role from Clearpass under the AAA profile. |
| DE19091 | When a new interface is created in AMP, such as Interface Gigabitethernet 0/0/2, fields that use default named profiles are pre-populated by default. |
| DE19118 | The Overview > License page now displays the correct technical support email address. |
| DE19189 | List views stay on the same page and retain all configured filters after a console refresh. |
| DE19191 | Rogue client reports are generated and can be viewed properly. |
| DE19198 | The AMP no longer returns the Invalid XML data error message when running a Network Wide Usage and Network Client Session error reports. |
| DE19221 | A new menu for configuring Site-to-Site IKE on the controller has been added under Advanced Services > VPN Services > IKE > Site to Site IKE. |
| DE19234 | Configuring WPA-2 Personal key management on a new network no longer returns the error message wrong value: wpa-psk-kip,wpa-psk-aes. |
| DE19244 | An error message displays if "Prefer AMON to SNMP" is enabled and the audit is disabled or there are no credentials for the CLI. |
| DE19253 | Attempting to simultaneously edit and delete separate items on the Manual Blacklisting page and then applying those changes no longer returns an error message and incomplete changes. |
| DE19269 | If an SSH user attempts to use the encrypt disable command and does not have permission, the configuration fails and an error message displays. |
| DE19270 | On the Instant Config page, the VC Name and Organization fields now support spaces in the name. |
| DE19290 | On the IGC, the Auth server 1 and Auth server 2 fields under Admin now work properly. |

Table 29: Issues Fixed in AirWave 8.0.4 (Continued)

| ID | Description |
|---------|---|
| DE19305 | The IGC no longer generates a mismatch message when the Host IP is deleted from the manual GRE. |
| DE19371 | On the AirWave 8.0.4 Instant Config > Access Points page, users can set the AP radio modes separately. |
| DE19375 | AirWave no longer pushes existing port channels while it is creating new channels. |
| DE19383 | The loading icon now appears when a floor plan is opened in any view. |
| DE19395 | The channel utilization overlay now loads properly in AirWave 8.0.4. |
| DE19396 | AppRF supports up to a maximum of 39K clients. |
| DE19415 | Adding new devices to a group in IE 9 now works properly. |
| DE19440 | Deleting a VC from a group and then re-adding it to the same group no longer causes the VC to be duplicated. |
| DE19460 | Configuring ports when creating Access Rules using the IGC now works properly. |
| DE19468 | When using VisualRF in Mozilla Firefox, devices do not stick to the cursor when moving them around the floor plan. |
| DE19475 | Both AirWave 8.0.4 and Instant produce the same report regarding detection of rogues. |
| DE19476 | AMON process performance improvements were made to reduce the chances of a backlog in handling AMON messages and provide a more up-to-date view of the network. |
| DE19477 | The IGC System Location field now works in Instant 4.1 and greater. |
| DE19502 | The single poller now starts and works properly. |
| DE19532 | Dragging VisualRF icons now works properly. |
| DE19633 | Sorting by the Radio Antenna on AP lists now works properly. |

The table below lists issues fixed in AirWave 8.0.3.1

Table 30: Issues Fixed in AirWave 8.0.3.1

| ID | Description |
|---------|--|
| DE19149 | An additional internal issue was fixed in AirWave 8.0.3.1 so that VisualRF is now using the proper amount of CPU. |
| DE19295 | A VisualRF performance issue that was caused by an architectural change has been fixed. VisualRF performance now works properly. |
| DE19395 | VisualRF now loads properly when the Channel Utilization overlay is applied to a floor plan. |
| DE19423 | <p>The clean_database.pl maintenance script did not execute for users running 8.0.3. This problem has been resolved with AirWave 8.0.3.1. Users upgrading from 8.0.3 to this release may experience a longer than usual clean_database.pl run time initially to make up for it not being run since upgrading to 8.0.3.</p> <p>Users running AirWave 8.0.3 who do not want to upgrade to AirWave 8.0.3.1 can run this command to fix the issue:</p> <pre>mv /usr/local/airwave/bin/clean_database /usr/local/airwave/bin/clean_database.pl</pre> |

Table 30: Issues Fixed in AirWave 8.0.3.1 (Continued)

| ID | Description |
|---------|---|
| DE19475 | The issue, where only a reported classification of valid from a device is allowed to demote the threat level, has been fixed. |

The table below lists issues fixed in AirWave 8.0.3.

Table 31: Issues Fixed in AirWave 8.0.3

| ID | Description |
|---------|--|
| DE18908 | Floor Upload Wizard changes are now saved correctly after clicking Finish . |
| DE19141 | VisualRF is no longer using too much CPU. Previously it was using over 40% CPU. |
| DE19149 | The Floor plan page is no longer timing out after upgrading the server to AirWave 8.x. |
| DE19320 | The loading speed of floors in the Flash UI has been improved. |
| DE19358 | The loading speed of densely-populated floor plans has been improved. |

The table below lists issues fixed in AirWave 8.0.2.

Table 32: Issues Fixed in AirWave 8.0.2

| ID | Description |
|--------------------|--|
| DE17161 | AirWave includes includes security fixes for Red Hat Enterprise Security Advisory RHSA-2014:0917-1, which resolves vulnerabilities that could allow users to return unencrypted information to the server. |
| DE18122 | AirWave includes ca-certificates security update (RHSA-2013:1866-3). |
| DE18533 | The Uptime report, which was not 100% for IAPs, has been resolved. |
| DE18753 DE17510 | When sorting AppRF data by MAC address, the Home > AppRF > MAC address window filters out entries that do not have MAC address data. |
| DE18449 | HTTPD has been updated to resolve https://rh.redhat.com/errata/RHSA-2014-0370.html |
| DE18609 | In VisualRF, an issue is resolved where changing the band setting for channel bands displayed by the VisualRF overlay triggered an error that could cause the VisualRF UI to stop responding and display an "Unresponsive script" error. |
| DE18680 | In previous versions of AirWave, a file locking error could lead to concurrency issues with AirWave tools interacting with data stored in the AirWave database. This issue is resolved in AirWave 8.0.2. |
| DE18694 | The number of items viewable on a list is changeable and maximum value is capped at 2000. NOTE: The user info list settings only apply to the first time viewing the list. If the setting was ever changed manually, then changing user info setting will not have any effect. |
| DE18733 | A lock option has been added to the VisualRF floor plan to prevent accidental changes to the location of campuses, buildings, APs, etc. |
| DE18745 | When VisualRF requests information from the AMP, it logs in with a randomly generated username and password. An improvement in AirWave 8.0.2 prevents unnecessary external authentication requests for these internally generated usernames and passwords. |

Table 32: Issues Fixed in AirWave 8.0.2 (Continued)

| ID | Description |
|--------------------|---|
| DE18718 | 802.11ac is now bucketed by channel width (20/40/80/160). This appears corrected on the RF Performance page and lists. |
| DE18792 | This change corrects a VRRP shutdown processing issue. Additionally, ip access-group <name> session is correctly understood in interface vlan . |
| DE18853 DE17510 | When sorting AppRF data by MAC Address, data that does not include the MAC address is not returned. |
| DE18860 | When list view refreshed per the console refresh rate, the list view stays on the current page and retains all filters. |
| DE18904 | The Restore Backup function no longer fails between AMP and the controller. |
| DE18913 | On the Rapids setup page, a warning message appears anytime a user enables containment. |
| DE18954 | When selecting Show Label in Channel in VisualRF, the full ap name and 802.11 channels are displayed. |
| DE18968 DE18784 | The change helps prevent a database lock contention between multiple processes |
| DE18985 | The maximum viewable columns in list view is 20. Once you reach 20, the available options go grey and you cannot slide over any other column options. |
| DE18994 | Exported CSV files no longer displays device uptime in epoch format. Uptime is now displayed as days, hours, minutes. |
| DE18997 | LV pagination options are now available for 25,50,100,250,500, and Custom. |
| DE19143 | AirWave includes includes security fixes for Red Hat Enterprise Security Advisory RHSA-2014:0924-1, which resolves vulnerabilities that could allow users to gain additional system privileges, or cause the system to stop responding. |
| DE19149 | In VisualRF, the floor plan data is now working properly and is no longer timing out. |
| DE19174 | Recent IAP template changes, including several Instant and IAP changes, are now available in AirWave 8.0. |

The table below lists issues fixed in AirWave 8.0.1.

Table 33: Issues Fixed in AirWave 8.0.1

| ID | Description |
|---------|--|
| DE15596 | If you override the Routed Virtual Interface value an Aruba switch inherits from its group profile, and then move that device to another group, the routed virtual interface count in the AP/Devices > Manage page increases correctly. |
| DE15994 | Action icons in the UI display tooltips when you mouse over those icons. |
| DE17274 | AirWave includes security fixes for Red Hat Enterprise Security Advisory RHSA-2014:0475-1, which resolves vulnerabilities that could allow users to gain additional system privileges, or cause the system to stop responding. |
| DE17619 | The VPN session client graphs displayed on the Clients VPN Sessions page correctly show Usage as the default Y-axis value. Previously, this value was undefined until the Usage value was selected. |

Table 33: Issues Fixed in AirWave 8.0.1 (Continued)

| ID | Description |
|---------|---|
| DE17642 | In VisualRF, clicking on a campus or building link in the List view correctly displays the campus or building Map view, regardless of the browser used to access the AirWave UI. |
| DE17987 | The Clients > Diagnostic page for a wired client no longer displays data fields applicable to wireless clients only. |
| DE18117 | AirWave includes security fixes for Red Hat Enterprise Security Advisory RHSA-2014:0126-1, which resolves vulnerabilities that could allow a remote attacker to crash an OpenLDAP server. |
| DE18118 | AirWave includes security fixes for Red Hat Enterprise Security Advisory RHSA-2013:1409-1, which resolves extended Internet daemon (xinetd) package vulnerabilities that could allow users to gain additional system privileges. |
| DE18125 | AirWave includes security fixes for Red Hat Enterprise Security Advisory RHSA-2014:0043-1, which resolves vulnerabilities in the way Berkeley Internet Name Domain (BIND) handles queries for NSEC3-signed zones, |
| DE18169 | If you edit a Routed Virtual Interface profile to define an IP Netmask for multiple devices, the confirmation page now correctly shows the IP Netmask value is associated with the IP Netmask field. In previous releases, the confirmation page incorrectly showed the netmask value associated with the IP Address field, even though the netmask value was correctly defined in the profile. |
| DE18182 | When the Use Global Aruba Configuration setting is enabled in the AMP Setup > General page, changes to a Gigabit Ethernet interface port on the Device setup > Aruba Configuration > Local Config Network > Ports/interfaces page can now restrict the Gigabit Ethernet interface port setting to devices within a selected group or set of groups. |
| DE18371 | VisualRF correctly displays properties for APs with disabled radios. In previous versions of AirWave, an AP with a disabled radio incorrectly appeared as an AP with an error in VisualRF. |
| DE18378 | Association or neighbor lines in an HTML5 VisualRF floor plan correctly display settings for the connection PHY band (5 Ghz and/or 2.4 GHz). |
| DE18405 | VisualRF floor plans correctly show distances in metric units (rather than US [imperial] units), when the Use Metric Units setting is selected in the VisualRF > Setup page. |
| DE18410 | By default, VisualRF allocates 2,500 grid cells to each floor plan, and calculates grid cell size by dividing the square footage of the floor plan by 2,500. The grid cell size shown in the floor plan lists on the VisualRF > Floor Plans page now limits the cell size value to two decimal places. (for example, 1.85 ft.) |
| DE18413 | Users logging in to AirWave with read-only credentials are able to change the size of VisualRF icons. |
| DE18419 | A user logging in to AirWave with read-only credentials is no longer incorrectly logged out of AirWave when the user selects and drags a region point on a VisualRF floor plan. |
| DE18422 | VisualRF correctly prevents users from drawing walls outside the floorplan background when editing a floor plan. |
| DE18437 | AirWave includes security fixes for Red Hat Enterprise Security Advisory RHSA-2014-0513, which resolves a libxml2 vulnerability that could allow a remote attacker to launch a Denial of Service (DoS) attack on the system. |
| DE18489 | An issue has been resolved where resizing a VisualRF floorplan before adding planned APs prevented the floor from loading correctly. |

Table 33: Issues Fixed in AirWave 8.0.1 (Continued)

| ID | Description |
|---------|---|
| DE18490 | An issue is resolved where settings from an Instant Virtual Controller were not imported correctly, triggering a configuration mismatch error. AirWave now correctly stores the VLAN ID, netmask and gateway for a Virtual Controller. |
| DE18522 | The 802.11g Radio profile now appears in the list of controller profile settings that can be managed using the Aruba Controller override list in the APs/Devices > Manage Page . |
| DE18538 | In VisualRF, the grid size for an AutoCad floorplan can be configured correctly using either the flash UI or the default HTML5 UI, and the size of the floorplan no longer limits the available grid size settings. |
| DE18551 | Importing a configuration from a 7200 Series controller caused the AirWave UI to stop responding. This issue is resolved by changes that allow AirWave to ignore an unrecognized configuration setting imported from a controller running a newer version of ArubaOS not yet unsupported by that version of AirWave. |
| DE18558 | The information on the Home > UCC page correctly refreshes with the frequency defined in the Console Refresh Rate field in the Home > User page. |
| DE18578 | When AMP is installed on a virtual machine, the AMP monitoring process recognizes the correct number of CPU cores allocated in the VM. Previously, the monitoring process on an AMP installed on a VM did not get updated with this information, and would use the number of cores configured in the AMP Setup > General > Performance page. |
| DE18582 | An issue is resolved where importing a configuration from a master controller with a local controller did not correctly add the local controller's IPsec keys. |
| DE18588 | AirWave includes security fixes for OpenSSL Security Advisory CVE-2014-0224, which resolved vulnerabilities for a Man-in-the-middle (MITM) attacks that could allow an attacker to decrypt and modify traffic from the attacked client and server. |
| DE18594 | An issue is resolved where the AirWave UI would stop responding because longer data retention periods caused the cached data to reach the maximum cache size of 4 Gb. There is no longer a defined limitation on the cache size, which is now limited only by the size of the AirWave server. |
| DE18619 | The device uptime reported in the Device Info section of the APs/Devices > Monitor page displays accurate uptime values. |
| DE18621 | The VisualRF List View correctly refreshes the information on that page with the frequency defined in the Console Refresh Rate field in the Home > User page. |
| DE18628 | AirWave can import planned APs using the Ekahau format into VisualRF floor plans. |
| DE18650 | The Instant GUI Configuration (IGC) feature now supports configuration of the AirWave AMS-IP, AMS-backup-IP and Organization settings. |
| DE18675 | An issue is resolved where rogue APs did not correctly appear in Visual RF floor plans. |
| DE18710 | AirWave includes security fixes for Red Hat Enterprise Security Advisory RHSA-2014:0771-1, which resolves vulnerabilities that could allow local users to gain additional system privileges, or cause the system to stop responding and display an unresponsive script warning. |

The table below lists issues fixed in AirWave 8.0.0.

Table 34: Issues Fixed in AirWave 8.0.0

| ID | Description |
|---------|---|
| DE15403 | The default view for user graphs is now the <i>maximum</i> user count. In previous releases, user count graphs showed the <i>average</i> user count by default. |

Table 34: Issues Fixed in AirWave 8.0.0 (Continued)

| ID | Description |
|--------------------|--|
| DE15629 | The client diagnostics page no longer displays an unnecessary blue area in the match events popup window. |
| DE16457 | Time stamps on for traps on the System > Syslog & Traps page correctly coincide with the time stamp value on SNMP trap messages. |
| DE17077 | The SNMP Source column that appears in the Client lists has been renamed to Source , as this column can now show information for the following source types: <ul style="list-style-type: none"> ● SNMP Poll ● SNMP Trap ● AMON ● HTTPS |
| DE17731 | The User column in the in the Home > AppRF > Users table correctly resizes to display the entire User name. In previous releases, longer user names could be truncated. |
| DE17839 | Open menus close correctly when a user scrolls up and down a page in the AirWave UI using a mouse scroll wheel. |
| DE17939 | The AppRF graphs Trend for Top 3 Destinations and Trend for Top 3 Applications correctly show data for the selected time period, without any unexpected data gaps. |
| DE18022 | The Interface Gigabit Ethernet profile and Port Channel profiles used for Aruba device configuration includes fields for configuring a session ACL and a session VLAN ACL. |
| DE18078 | Changes to client diagnostic page thresholds are saved as expected. |
| DE18133 | The VisualRF Auto-match Planned Devices feature correctly displays the total number of floors for the view of all campuses. |
| DE18171 | AMP has an internal whitelist that allows administrators to use the UI to view the log files on the System>Status page. If a user attempts to access a file not on this list through the UI, AMP displays an 'Access Denied' error message. |
| DE18178 | An issue is resolved that prevented a VLAN without a description or AAA profile from being correctly pushed to a controller and created on the device. |
| DE18185 | If you use the controller UI to assign an IP address to a VLAN, and then delete that VLAN from the Device Setup > Aruba Configuration > Local Config > Network > VLANS > VLAN page of the AirWave UI, AirWave correctly deletes the IP address for the VLAN before it deletes the VLAN itself. In previous versions, the VLAN was deleted <i>before</i> its IP address, triggering a configuration mismatch error. |
| DE18188 | The DHCP Option 82 setting configurable in the Device Setup > Aruba Configuration > Local Config>Network>IP page of the AirWave UI is correctly applied to the controller configuration. |
| DE18275 | Resizing campus icons on the VisualRF>Network map no longer causes the campus icons to move to an incorrect location on the map. |
| DE18287 | Instant template configurations created and edited in AirWave support WPA2 passwords with an apostrophe (') or other special characters. |
| DE18367 DE18372 | When you configure a report definition to allow that report to be exported via FTP or SCP, the Reports >Definitions page displays a warning if the FTP or SCP settings are invalid. |

Table 34: *Issues Fixed in AirWave 8.0.0 (Continued)*

| ID | Description |
|---------|--|
| DE18424 | You can use VisualRF to create and export a bill of materials for a campus, building or floor by right-clicking on the icon for that location, and selecting Bill of Materials . Earlier versions of AirWave could incorrectly display an error message when a user attempted to create a bill of materials using the right-click menu. |
| DE18433 | VisualRF allows you to drag-and-drop an AP onto a floor plan using the Internet Explorer 11 browser. |
| DE18487 | VisualRF supports .svg files as floor plan background images. |

Known Issues

The table below lists known issues in AirWave 8.0.11.

Table 35: *Known Issues in AirWave 8.0.11*

| ID | Description |
|---------|--|
| DE19307 | The Home > UCC page did not correctly display call quality, device trend, call volume and call quality data for a group of over 9,100,000 calls generated by a UCC simulation script. The httpd log file displayed an out of memory error for the event. |
| DE21611 | AirWave may fail to send large report messages via email if the report is longer than 1000 lines. These longer reports may also not display correctly in the Reports > Details page of the AirWave WebUI. |
| DE21674 | An MDM server configured using AMP Setup > MDM Server cannot be accessed using the View Device in SOTI MobiControl link on the Clients > Client Details page if the device is managed using SOTI version 9.0 or higher. |
| DE22214 | Adding or deleting a group using the Group > List page does not trigger an entry in the event log files. When a group name is changed, however, the name change does trigger a log entry which shows the name of the user that updated the group. |
| DE23283 | The Clients and Usage graphs on the APs/Device > Monitor page may show some inconsistencies in the total numbers of clients and traffic for an IAP cluster with a VPN tunnel, if the virtual controller is itself a VPN client. This is because the "total clients" value displayed in the in the Clients graph does not include VPN clients, which appear as a separate "total VPN clients" value. |
| DE23419 | When you use the Instant GUI Config (IGC) wizard on the Groups > Instant Config page to create a new wired network, the New Rule portion of the Access configuration steps allow you to select the Disable Scanning option, even though that setting applies to wireless networks only, not wired networks. |

There are no new known issues in AirWave 8.0.10.1.

The table below lists known issues in AirWave 8.0.10.

Table 36: Known Issues in AirWave 8.0.10

| ID | Description |
|--------------------|--|
| DE23716 | <p>IGC migration removes a virtual controller's override settings after the IAP's firmware is upgraded and then migrating the IGC to the corresponding version. However, the overrides for the following components are not removed:</p> <ul style="list-style-type: none"> ● Uplink ● AirWave info (IP address, key, organization) ● System location ● Virtual controller IP address, netmask, gateway, VLAN, and name ● Per AP (thin AP) settings |
| N/A | <p>It is recommend that you do not enable the IGC > AirWave > AirWave Settings > Allow Configuration of AirWave Settings option in releases prior to 8.0.10 before migrating to 8.0.10. Enabling this option creates an ams-key mismatch after upgrading to 8.0.10 and it may cause IAPs disconnect from AirWave. This option is disabled by default in the IGC. After the midnight auto audit, the IGC retrieves and stores a device's ams-key after migration is complete.</p> |
| DE22425 | <p>AirWave does not create the default ACLs that a controller creates upon role creation. In ArubaOS 6.4.x, this creates a conflict that prevents AirWave from correctly pushing policy configuration to the controller. As a workaround, create new roles on the controller first and then import them to AirWave.</p> |
| DE23282 DE23670 | <p>AirWave sends incorrect trigger alerts for AP down events during the controller upgrade process. For example, AirWave might send AP down alerts when the AP is down for less than the time configured in the trigger. This issue is caused when AirWave picks up an old entry when the AP went down instead of the most recent down event. Since the time since the old entry meets the configured trigger time, an alert is sent.</p> |
| DE23289 | <p>When viewing VisualRF in the Microsoft Edge browser on a Windows 10 client, double clicking on a building or floor does not open the floor or map page.</p> |
| DE23697 | <p>If an invalid or unreachable IP address is configured on a virtual controller through the IGC, the IAP cluster managed by the misconfigured VC becomes completely unreachable. Additionally, attempting to change the VC IP address from the Instant UI does not work because the VC thinks it is being managed by AirWave.</p> |

There are no new known issues in AirWave 8.0.9.2.

The table below lists known issues in AirWave 8.0.9.1.

Table 37: Known Issues in AirWave 8.0.9.1

| ID | Description |
|--------|---|
| 123937 | <p>In ArubaOS 6.4.2.12, the PhyType message sent by the controller to AirWave for wireless clients does not include the proper encoding information. This causes AirWave to display 802.11g clients as 802.11b.</p> |

The table below lists known issues in AirWave 8.0.9

Table 38: *Known Issues in AirWave 8.0.9*

| ID | Description |
|---------|---|
| DE21393 | The AMP Setup > General page allows you to configure time periods for retaining historical data. If you run a report for a longer period of time than the configured data retention period (e.g., you want to view 30 days of data for IDS events, but AirWave is configured to retain only 14 days of IDS data) then the reports may show unexpected results due to the limited data available. AirWave does not display a warning message if an administrator runs a report for a longer amount of time than the data retention window. |
| DE22133 | In VisualRF, when you edit a floor plan to add a deployed device, the names of the folders in the Devices pane may appear as a question mark (?) instead of the correct folder name. This is only a display issue, as you can still drag and drop devices from these folders onto the floor plan. |
| DE22139 | In VisualRF, the auto-match feature matches a managed device to a planned device with the same name or MAC address. In AirWave 8.0.9, when you right-click a floor plan, campus or network icon and select the Auto-Match Planned Devices option, those devices may incorrectly appear as down, even if the managed device is correctly matched with the planned device, and is active on the network. |

The table below lists known issues in AirWave 8.0.8

Table 39: *Known Issues in AirWave 8.0.8*

| ID | Description |
|---------|---|
| DE21374 | AirWave does not allow you to Telnet to a switch from the AirWave server. The browser opens a pop-up to launch the Telnet application but no response is returned from the Telnet application. |
| DE21464 | In the IGC, the global DHCP Server scope cannot be deleted from the cluster. |
| DE21465 | The IGC continues pushing a configuration to IAPs after the configured Retry Limit is reached. This occurs when the configured value of Clients Per Branch , in the Branch Size tab under DHCP Servers > Distributed DHCP Scopes , is larger than the value calculated by AirWave. Because the configured number is out the required range, the configuration is not pushed to the IAPs and results in a mismatch. To work around this issue, configure a value smaller than the maximum value suggested in the UI. |
| DE21551 | VisualRF does not display all the folders when you add APs to floors. |
| DE21570 | When two IAPs are configured as a preferred master in the same cluster, the following occurs: <ol style="list-style-type: none"> 1. Each IAP becomes a virtual controller (VC). However, they do not form a cluster together and instead enter standalone mode. 2. Because they both become virtual controllers and were configured to be in the same cluster, they have the same VC key. 3. Each VC fluctuates between the up and down states because both VCs attempt to connect to AirWave with the same VC key. 4. AirWave detects this situation and, after for 10 minutes, resolves the conflict by making one VC key unique and rebooting both VCs. |
| DE21581 | VPN traffic statistics (VPN IN and VPN OUT) and VPN client statistics do not populate correctly in the Client graph on the Clients > VPN Sessions page. The VPN client count appears as zero. |

Table 39: *Known Issues in AirWave 8.0.8 (Continued)*

| ID | Description |
|---------|---|
| DE21607 | <p>When you use the IGC to add a new IAP, there may be a configuration mismatch because IAPs do not support the command no wlan captive-portal. Since AirWave does support that command, the resulting configuration mismatch cannot be resolved.</p> <p>To avoid this issue, on Groups > Instant Config > Security > Internal Captive Portal, set the Authenticated field to Enabled. Alternately, if a mismatch occurs, factory reset the IAP after the IAP is added to an existing IAP group.</p> |

The table below lists known issues in AirWave 8.0.7

Table 40: *Known Issues in AirWave 8.0.7*

| ID | Description |
|---------|---|
| DE20356 | Users are unable to change the Orientation, Gain, and Beamwidth values for IAPs in VisualRF. |
| DE20493 | The Radios table on the APs/Devices > Monitor page displays a blank SSID column for Juniper APs. This is due to a defect in the base code implementation for Trapeze from where the Juniper code is derived. |
| DE20541 | A CDP error appears for Motorola SNMP polling. When a Motorola controller is polled through SNMP, timeouts are seen while polling a few OIDs. The timeouts appear in the AirWave Events log. |
| DE20908 | Instant auth-fail SNMP traps send seven parameters, but AirWave does not currently support this. AirWave currently supports two parameters. |
| DE20922 | In VisualRF, the Defining Stationary Devices option does not work properly. In the VisualRF HTML5-based interface, the client changes when the client is placed in the floor plan as static. This option does work properly in the flash-based UI. |

The table below lists known issues in AirWave 8.0.6.3

Table 41: *Known Issues in AirWave 8.0.6.3*

| ID | Description |
|---------|--|
| DE20768 | The Download AirWave Management Client link on the Home > Documentation does not work correctly. Clicking the link does not start the file download and may cause the page to stop responding. To download the file, right-click on the link and select Save As to properly save the file. |

The table below lists known issues in AirWave 8.0.6.2

Table 42: *Known Issues in AirWave 8.0.6.2*

| ID | Description |
|---------|--|
| DE20751 | The List view in VisualRF has an extraneous lock icon to the right of the List link. This is a cosmetic defect and has no impact on VisualRF behavior. |
| DE20753 | Heatmaps in VisualRF and heatmaps in Bill of Material (BOM) reports do not match because BOM reports calculate heatmaps with a default signal cutoff of -85dBm. |
| DE20754 | Sensor maps are not shown in BOM reports for floors that have Air Monitors. |

The table below lists known issues in AirWave 8.0.5

Table 43: *Known Issues in AirWave 8.0.5*

| ID | Description |
|---------|---|
| DE15549 | The Total Disk Usage chart may not display the total number of disk mounts that have taken place. If more than eight disks have been mounted, AirWave only displays the first eight mounted disks. Once the limit on historical mount points is reached, subsequent mounts are not graphed, regardless of whether the previous mounts are connected. |
| DE19741 | Running nightly maintenance during midnight can cause AirWave to temporarily stop monitoring the network. Normal monitoring resumes once nightly maintenance completes. |

The table below lists known issues in AirWave 8.0.4

Table 44: *Known Issues in AirWave 8.0.4*

| ID | Description |
|---------|---|
| DE19369 | To enable Console Access, use the following procedure: From the AirWave UI, navigate to System > General . Click Console access: enable again, then select Save or Apply All . |
| DE19548 | The nightly backup log may have errors related to the VisualRF backup. Ignore these errors as they do not affect the overall AirWave nightly backup. |

The table below lists known issues in AirWave 8.0.3.1.

Table 45: *Known Issues in AirWave 8.0.3.1*

| ID | Description |
|---------|--|
| DE19491 | The VisualRF UI takes longer to load after the VisualRF engine has been restarted. |
| DE19490 | Floorplans with a high client density take a long time to load. |

There are no new known issues in AirWave 8.0.3.

The table below lists known issues in AirWave 8.0.2.

Table 46: *Known Issues in AirWave 8.0.2*

| ID | Description |
|---------|---|
| DE23819 | AppRF data from an IAP running Instant 4.2.1 does not appear on the AppRF chart on the Clients > Diagnostics page of the AirWave WebUI. |

The table below lists known issues in AirWave 8.0.0.

Table 47: *Known Issues In AirWave 8.0.0*

| ID | Description |
|---------|--|
| DE12398 | AMP servers using Security Technical Implementation Guide (STIG) management standards do not run the security-hardening script stig.pl upon each upgrade. |

Table 47: Known Issues In AirWave 8.0.0 (Continued)

| ID | Description |
|---------|---|
| DE12888 | SecureAMP has no menu item for setting the clock. A re-installation may be necessary if the clock is wrong, because login attempts are denied for significant clock deviations. |
| DE12919 | VMWare tools cannot be installed during the SecureAMP installation procedure, and must be pre-loaded before the installation. The tools should be pre-loaded, or loaded from the CLI menu. |
| DE13668 | In the legacy flash-based VisualRF UI, the QuickView Preferences>General , Preferences>APs and Preferences>Clients menus display configuration options that are no longer applicable to VisualRF. This is not a known issue for the default HTML5 VisualRF UI. |
| DE13678 | The overlay and display menus in the legacy flash-based VisualRF UI refers to "sensors", while the default HTML5 UI refers to these devices as "air monitors." |
| DE13683 | When you edit and save the Virtual Controller Variables - Default Values template, the Confirm Changes page shows the database changes, rather than the user-defined settings. |
| DE15112 | When you perform a search in AirWave, then resize the Search Results pop-up window, you have to scroll to see some of the buttons in this window. |
| DE15239 | If AirWave is not getting health data from Aruba controllers, the user diagnostic page shows an empty health graph. |
| DE15304 | On the Groups > Templates page, there is a note saying you can use templates to manage the configuration of devices. Although this list includes HP, only HP WesM devices support template configuration. |
| DE15512 | <p>When you perform a search in AirWave, pressing Enter and clicking the magnifying glass icon return different results.</p> <ul style="list-style-type: none"> ● Pressing Enter does a search based on what is specified on the AMP Setup > General page under the Search Method section. ● Clicking the magnifying glass always does a quick search. |
| DE15596 | If you import settings from an Aruba switch, then move that switch to a new group, the Aruba Overrides section of the APs/Devices>Manage page can show an incorrect number of Routed Virtual Interfaces. |
| DE15814 | When an inactive client expires, RRD files containing AMC Signal Data for that client are retained. |
| DE15921 | Links in the UI do not allow you to right-click the link and select the Open in new Tab or Open in New Window options. |
| DE16144 | Adding a user to the internal user database using the Instant GUI Config (IGC) feature incorrectly triggers a no user error for a configuration mismatch when you save and apply the change, even though the user is added correctly. |
| DE17613 | The AirWave UI does not fully support the Safari for Windows browser. (5.1.7 or earlier) |
| DE17665 | AirWave can allow more devices to be added than are supported by the current license count. Exceeding the device licensing limits can cause performance issues. |

Table 47: Known Issues In AirWave 8.0.0 (Continued)

| ID | Description |
|--------------------|---|
| DE17739 | Active APs making UCC calls can appear to be down when the device is polled using SNMP. This can cause AirWave to incorrectly report that a down AP is supporting an active UCC call. |
| DE17897 | AirWave uses outdated timezone data, which incorrectly calculates the date that daylight savings time in Brazil. AirWave can also encounter errors when it attempts to calculate reoccurring event times during the changeover period between standard time and daylight savings time in Brazil. |
| DE17960 DE17998 | <p>The table in the RAPIDS > List page cannot be sorted or filtered by the by the following data columns.</p> <ul style="list-style-type: none"> ● Name ● Detecting APs ● Channel ● Threat level ● Confidence |
| DE17971 | The Scatterplot UCC data chart supports a maximum of 1000 datapoints. |
| DE17998 | The device table on the RAPIDS > List page does not allow you to filter data by the Detecting APs, Channel, Threat level or Confidence table columns. |
| DE18051 | Reinstalling AirWave doesn't overwrite and clear all previous database entries. |
| DE18259 | In VisualRF, if the Draw Walls tool is selected, moving an AP to a new location on the floor plan will draw a wall between the previous location of the AP and its new location on the floor plan. |
| DE18920 | <p>With the parameter as "none" in the xml request (<a href="https://<your.airwave.server>/amp_stats.xml">https://<your.airwave.server>/amp_stats.xml), the following parameters are not listed in the xml response:</p> <ul style="list-style-type: none"> ● bandwidth_in ● bandwidth_out <p>To get all the attributes (including bandwidth details) in the amp_stats response, use the URL <a href="https://<your.airwave.server>/amp_stats.xml?include_bandwidth=1">https://<your.airwave.server>/amp_stats.xml?include_bandwidth=1.</p> |
| DE19266 | When enabling AMON, auditing should be set to daily and have been successful at least once to allow AirWave to calculate the proper BSSIDs per radio. If these BSSIDs do not exist, clients are dropped because they do not have any corresponding BSSIDs in the AirWave database. |
| US12233 | <p>Buildings cannot be moved to new campuses under the HTML5 version of AirWave 8.0.11. To work around this issue:</p> <ul style="list-style-type: none"> ● Disable the HTML5 user interface (revert back to flash). ● Restart the VisualRF engine and make the necessary changes. |