ArubaOS 6.1.3.6-AirGroup

ARUBA networks

Release Notes

Copyright

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

ARUBA®
networks

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1

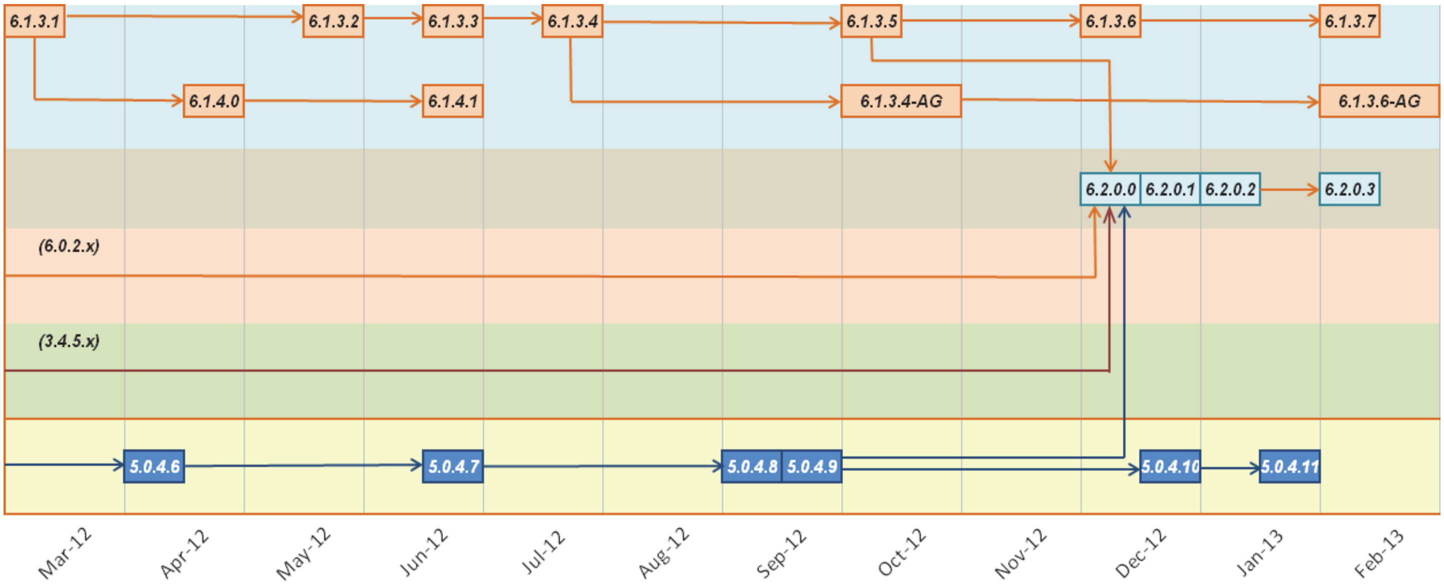
Release Overview

ArubaOS 6.1.3.6-AirGroup is a technology release that introduces multi-controller AirGroup support, master-local controller configuration synchronization, and a few more AirGroup feature. If you do not need the feature introduced in this release, Aruba recommends using the most recent mainline ArubaOS GA release instead. Security fixes and stability fixes deemed critical by Aruba will be applied to subsequent patches of this technology release until the AirGroup feature merges into the next major GA release. Minor issues or those requiring significant engineering changes will not be included in technology release patches. For more information, refer to the End-of-Life policy at http://www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/.

Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 6.1.3.6-AirGroup. To upgrade to ArubaOS 6.1.3.6-AirGroup, follow the procedures mentioned in Chapter 5, “Upgrade Procedures” on page 21.

Figure 1 *ArubaOS Releases and Code Stream Integration*



Contacting Support

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephones	arubanetworks.com/support-services/aruba-support-program/contact-support/
Software Licensing Site	licensing.arubanetworks.com/login.php
End of Support information	www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/
Wireless Security Incident Response Team (WSIRT)	arubanetworks.com/support/wsirt.php
Support Email Addresses	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Chapter 2

What's New in this Release

This chapter provides a brief summary of the new features included in this version of ArubaOS, as well as new resolved issues and known issues identified in this release. Topics in this chapter include:

- "Multi-Controller AirGroup Cluster" on page 7
- "Master-Local Controller Synchronization" on page 7
- "Enhancement" on page 7
- "New Resolved Issues" on page 8
- "New Known Issues" on page 8
- "Issues Under Investigation" on page 9

NOTE

AirGroup support on 600 Series controllers in ArubaOS 6.1.3.6-AirGroup is restricted to Proof Of Concept (POC) and demo deployments. Production deployments are not recommended due to system resource constraints.

Multi-Controller AirGroup Cluster

ArubaOS 6.1.3.6-AirGroup supports multiple mobility controllers running AirGroup to form a cluster. This feature enables an iPad user on one controller to discover an Apple TV available on another controller, if both the controllers are part of the same cluster. For more information, see the *ArubaOS 6.1.3.6-AirGroup Deployment Guide*.

Master-Local Controller Synchronization

Staring from ArubaOS 6.1.3.6-AirGroup, administrators can configure AirGroup from the master controller to ease deployment. The master controller then synchronizes the AirGroup configuration elements with all the local controllers it manages. For more information, see the *ArubaOS 6.1.3.6-AirGroup Deployment Guide*.

Enhancement

The following enhancement is introduced in ArubaOS 6.1.3.6-AirGroup:

Pre-configured AirGroup Services

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

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

For more information, see the *ArubaOS 6.1.3.6-AirGroup Deployment Guide*.

New Resolved Issues

The following issues are resolved in ArubaOS 6.1.3.6-AirGroup.

Table 1 *Resolved Issues in ArubaOS 6.1.3.6-AirGroup*

Bug ID	Description
69771	**Symptom**: AirGroup related configurations were not pushed from master to local controller. Starting from ArubaOS 6.1.3.6-AirGroup, the master controller synchronizes the AirGroup configuration elements with all the local controllers it manages. For more information, see "Master-Local Controller Synchronization" on page 7. **Scenario**: Configuring AirGroup in master controller This limitation was there in all controllers running ArubaOS 6.1.3.4-AirGroup.
73870	**Symptom**: Apple TVs upgraded to software version 5.1 no longer responded to mDNS queries from a controller with a source IP address of 169.254.53.53. Starting from ArubaOS 6.1.3.6-AirGroup, any mDNS packet originating from an AirGroup controller has the source IP as the VRRP or the controller IP address. **Scenario**: This issue was observed in both overlay and integrated AirGroup deployment models running ArubaOS 6.1.3.4-AirGroup that did not have an IP address configured on the VLAN interfaces to which Apple TVs were connected.
73729	**Symptom**: If an AP associated to the AirGroup controller stopped responding, it never got aged out from the AirGroup AP table displayed in the output of the **show airgroup ap** command. This issue is fixed in ArubaOS 6.1.3.6-AirGroup. **Scenario**: This issue occurs because the internal controller module that manages AP and user association does not send a message to the mDNS process indicating that an AP has gone down. This issue was observed in all controllers and AP hardware models running ArubaOS 6.1.3.4-AirGroup in an integrated deployment model.
76605, 76191, 78159, 79569	**Symptom**: mDNS process crashed on the controller. An internal code change in the mDNS process fixed this issue in ArubaOS 6.1.3.6-AirGroup. **Scenario**: This issue happened during MAC authentication of a user device by ClearPass Policy Manager. This issue was observed in controllers running ArubaOS 6.1.3.4-AirGroup.
77821, 77877	**Symptom**: mDNS process crashed on the master controller. This issue is fixed by making changes to the way mDNS process initializes the memory manager. **Scenario**: It was randomly observed that the mDNS process did not appear at initialization.This issue was a rare condition in controllers running ArubaOS 6.1.3.4-AirGroup.

New Known Issues

The following issues are identified in ArubaOS 6.1.3.6-AirGroup.

Table 2 *Known Issues in ArubaOS 6.1.3.6-AirGroup*

Bug ID	Description
69192	**Symptom**: Adding a new VLAN to a port does not cause AirGroup servers to be proactively discovered. **Scenario**: This issue occurs when the controller tries to generate an mDNS query to discover the network when a new VLAN is created. These queries cannot be sent because a new VLAN does not have any ports mapped to it, and additional query packets are not sent out when ports are subsequently mapped to the existing VLAN. **Workaround**: Assign an IP address to the VLAN interface.

Table 2 *Known Issues in ArubaOS 6.1.3.6-AirGroup*

Bug ID	Description
79464	**Symptom**: Saving the configuration immediately after deleting AirGroup domains one at a time from the master controller does not delete the domains from the local controller. **Scenario**: This issue is observed when the administrator deletes one domain at a time and issues the **write memory** command immediately after each deletion. The configuration change does not synchronize with the local controller. **Workaround**: After deleting all the domains from the master controller, issue the **write memory** command once.

Issues Under Investigation

In a rare case, the following issues are observed in ArubaOS 6.1.3.6-AirGroup. These issues are under investigation.

Table 3 *Issues Under Investigation*

Bug ID	Description
79845	**Symptom**: A rare case of an unexpected kernel panic crash has been observed in 3200 controller running ArubaOS 6.1.3.6-AirGroup.
80009	**Symptom**: A crash of the user authentication process has been observed in the controller when a Remote AP stalled during an upgrade.

Chapter 3

Issues Fixed in Previous Releases

This chapter describes fixed issues in previous versions of ArubaOS.

Resolved Issues in ArubaOS 6.1.3.4-AirGroup

The following issues were resolved in ArubaOS 6.1.3.4-AirGroup.

Table 4 *Resolved Issues in ArubaOS 6.1.3.4-AirGroup*

Bug ID	Description
66798	An issue has been resolved where a controller upgraded to 6.1.3.0 experienced slower-than-expected throughput when bandwidth contracts were enabled. This issue was triggered by a small queue size for lower contract rates in ArubaOS 6.1.3.0, and was resolved by increasing the queue size in ArubaOS 6.1.3.4-AirGroup so throughput is no longer negatively impacted.
73664	An issue was resolved when wired users connected to a controller acting as a multiplexer client failed to establish a 802.1X authentication upon moving from one port of the controller to another. This issue occurred when a controller was deployed as a multiplexer server (running ArubaOS 6.1.3.2/6.1.3.3/6.1.3.4), and another controller was used as a multiplexer client.
73343	Support for band-3 channels (100 - 140) has been added for AP-60, AP-61, AP-70, and AP-85 for Saudi Arabia.

Chapter 4

Known Issues Identified in Previous Releases

This chapter describes known issues and limitations identified in previous versions of ArubaOS.

Access Points

Table 1 *Access Point Known Issues and Limitations*

Bug ID	Description
56678	The Goodput (bps) values displayed on the **Dashboard > Access Points** and **Dashboard > Clients** pages in the WebUI appear lower than the expected value. As a workaround, view the usage data on the **Dashboard > Usage** page.
64248	If you use the *Iperf* network testing tool to measure throughput, the Last_ACK_SNR value may drop from 45 dB (idle) to 20 dB. When the client is idle or not running Iperf, the two SNR values are very similar. There is no applicable workaround, as this is an observation while testing throughput using Iperf.
62672, 63154, 61669	A 651 controller may reboot if its internal AP (radio) is configured in Air Monitor mode (am-mode). This can occur if memory becomes full by air monitoring statistics or excessive monitoring events for a number of days. As a workaround, reconfigure the internal AP (radio) in Access Point mode (ap-mode). Alternatively, you may disable the radio if not needed.
61938	In rare situations, a remote AP may fail to renew its IP address through DHCP after rebootstrapping. A remote AP stuck in this state will reboot after it exceeds its IPsec retry limit. The remote AP will recover from this state after rebooting.

57624	An AP-105 might not come up when connected to a Cisco PoE switch (WS-C6509-E:WS-X6148A-GE-45AF), even if the maximum amount of power is allocated to the port to which the AP is connected. The following error messages were returned when a the CLI command `shutdown` or `no shutdown` was executed on the port to which the AP was connected:
	`%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet9/48 (not half duplex), with SEP001BD5E87C32 Port 1 (half duplex).`
	`%C6K_POWER-SP-1-PD_HW_FAULTY: The device connected to port 3/2 has a hardware problem. Power is turned off on the port.`
	`%C6K_POWER-SP-1-PD_HW_FAULTY: The device connected to port 3/2 has a hardware problem. Power is turned off on the port.`

59177, 60722, 61100, 57925, 60846, 64517, 66118, 66128, 66185, 66659, 64526, 61539, 61196, 67435, 67670 67671, 67673, 67871, 67872, 67977, 63460, 65049, 62111, 66409, 66136, 58011, 64524, 64517	A 651 controller might crash and unexpectedly reboot when the internal AP is enabled. As a workaround, disable the radio on the internal AP on a 651 controller.

Air Management - IDS

Table 2 *Air Management - IDS Known Issues and Limitations*

Bug ID	Description
65946	The tables in the **Monitoring > Network > All Access Points** page of the WebUI and in the output of the `show wms ap list` command in the CLI show an incorrect number of users.

ARM

Table 3 *ARM Known Issues and Limitations*

Bug ID	Description
62878	If band steering is enabled, errors in the voice-aware band steering feature can cause active 802.11a/g capable voice clients to be disassociated from an AP if those clients roam to a new 802.11g radio.
56760	Per-SSID bandwidth contracts are not completely compatible with UDP traffic and Virtual APs in decrypt-tunnel mode. For example: ● The actual bandwidth allocation is around 25% off compared to the configured bandwidth allocation. With tunnel mode, the error rate is only 5-10%. ● The maximum UDP throughput for a single client is only 155 Mbps, which is about 30 Mbps lower than the throughput in tunnel mode.

Authentication

Table 4 *Authentication Known Issues and Limitations*

Bug ID	Description
56130	When a user switches between a wireless and wired connection, that user may get assigned a logon role instead of the correct MAC authenticated role.
56236	A replay counter mismatch may be observed during the 4-way handshake in WPA2-AES mode with Cisco 7921 and 7925 handsets. This usually happens after the clients recover from power save mode. This mismatch will not be seen on the next attempt.
61935	A DHCP fingerprinting user-derived rule with a **set-vlan** action does not work with 802.1X authentication. This type of rule does work on an open system network.

IPv6

Table 5 *IPv6 Issues and Limitations*

Bug ID	Description
57059	When maximum number of IPv6 L3 interfaces exceeds the supported platform limit, it affects the routing on controller. Do not exceed the maximum number of IPv6 L3 interfaces.

Management

Table 6 *Management Issues and Limitations*

Bug ID	Description
61423	Stale entries in the user table may not age out even after the client disconnects from the network. As a workaround, use the command `aaa user delete` to clear any stale entries.
63800	Valid APs might be incorrectly and randomly classified as unknown on local controller in a multi-controller environment. As a workaround, manually reclassify those AP as valid.
62852, 64110	A controller may reboot due to a a restart of the internal wireless management system process. This does not have any operational impact on clients. As a workaround, delete WMS entries from the controller database and restore the wms-backup.db database. For assistance in restoring the database, contact your Aruba support representative.

Mesh

Table 7 *Mesh Issues and Limitations*

Bug ID	Description
56642	An AP-135 configured as a mesh point fails to upgrade if its mesh link to a mesh portal with two spatial streams (AP-105, series, AP-120 Series, and AP-175) uses high-throughput mode. As a workaround, do not enable high-throughput on an mesh portal with two spatial streams or change the default supported-MCS from 0-23 to 0-15.

Mobility

Table 8 *Mobility Issues and Limitations*

Bug ID	Description
62988	Wireless clients might incorrectly be assigned to the wrong VLAN when VLAN mobility is enabled. As a workaround, set firewall bandwidth contract to Default.
63163	Mobility-enabled datapath bridge entries may be deleted for untrusted users. Mobility deletes and adds the datapath bridge entries for clients even when there is active traffic. This issue only occurs when Mobility is enabled.
63164	The mobile IP module might crash if there are several hundred mobile clients in addition to another 1000+ users, and all are roaming between L2 networks.

OCSP/CRL

Table 9 *OCSP/CRL Known Issues and Limitations*

Bug ID	Description
55419	The internal controller process that handles certificates becomes busy when a large number of OCSP requests hit the certificate manager while the OCSP server is unreachable. This issue will appear whenever there is misconfiguration or outage between the controller and the OCSP responder.

Platform/Datapath

Table 10 *Platform/Datapath Known Issues and Limitations*

Bug ID	Description
56242	The VPN Site-to-Site IPsec tunnel is unstable when a high rate of traffic is generated. This is caused by a miscalculation of the IPsec tunnel's idle timeout that triggers the Dead Peer Detection (DPD) exchange. As a workaround, disable the DPD on both controllers to prevent the tunnel from failing.
63140	A controller may experience a datapath timeout if 2,000 users are created from an untrusted port with upstream and downstream per-user bandwidth contracts.
62838	If an AP comes up on an untrusted port where the first port rule is *allow all*, that AP's sessions may be denied.
62238	In a network where the user VLANs extend from the controller to an uplink Cisco switch, applications may try to reach users connected behind a remote AP. The Cisco environment has the ARP Ageout and the Cam table ageout set to 4 hours. This causes any traffic for a user who has aged out to get flooded to all users in that VLAN.
63359, 62551	The kernel module crashed on the standby controller while running ArubaOS 6.1.2.5. Aruba support has not been able to reproduce this issue.
58487	In some cases, APs with control plane security enabled might take a long time (more than 30 minutes) to come up. This is caused by the control plane security SA setup timing out because the AP does not receive the fourth IKE packet from the controller.
65984	High core utilization on a 6000 controller running ArubaOS 6.1.3.1 causes APs associated to that controller to reboot. **Workaround:** Issue the **firewall deny-inter-user-bridging** CLI command to help suppress the high core utilization.

Port Channel

Table 11 *Port Channel Known Issues and Limitations*

Bug ID	Description
62936	If the native VLAN of a trunk LACP port channel is configured as an untrusted port, LACP member ports may stop responding after upgrading the controller to ArubaOS 6.1.3 or later.

PPTP

Table 12 *PPTP Known Issues and Limitations*

Bug ID	Description
55177	A Mac PPTP client connecting to an M3 as a PPTP server might disconnect if the client is idle for 10 minutes.

Remote Access Point

Table 13 *Remote Access Point Known Issues and Limitations*

Bug ID	Description
61428	In some cases, if an authentication process restart on controllers that have ACLs configured with large number of ACEs could cause APs to reboot. As a workaround, reboot the controller.
63073	Saving a backup of a virtual AP on a remote AP to flash memory may fail if the virtual AP has large ACLs with 500 ACE entries. As a workaround, reduce the number of ACE entries on the ACLs before saving the backup.
51546	If a Remote AP uses a Sierra modem 312 for a 3G uplink, 3G to wired failover may leave the USB uplink in hung state. Rebooting the remote AP will make it recover from this state.

Role/VLAN Derivation

Table 14 *Role/VLAN Derivation Issues and Limitations*

Bug ID	Description
51691, 56746	When using DHCP user derivation rules and captive portal authentication, the client is assigned to the wrong role after a DHCP-Renew. All controllers running version ArubaOS 6.1.0.0 are affected. DHCP user derivation rules and captive portal cannot be used together.

Security

Table 15 *Security Known Issues and Limitations*

Bug ID	Description
47868	You cannot configure an alias for an IPV6 netdestination using the `netdestination6` CLI command.
55913	After issuing the `aaa user delete all` command, users might be incorrectly placed in the logon role.

61690	In an ACL with the following lines:
	`ip access-list session good`
	`any any any deny blacklist log`
	The ACL has enabled the blacklist option, and the valid client is falling into the MAC auth default role. The non-valid client is being denied but not blacklisted.

62437	The AAA state for the an AP does not get cleared after the AP completes 802.1x authentication. The IP address from the AP's first assigned VLAN stays associated to the AP's MAC address, even after the AP moves to a different VLAN. As a workaround, manually change the AAA state of the AP and reboot the controller.
55898	The command `show user` does not display the correct information for captive portal users when those users are connected through an L3 gateway.
56503	The username shown in the user table is the client's dot1x username instead of the captive portal username when the client disconnects and then reassociates.

Table 15 *Security Known Issues and Limitations (Continued)*

Bug ID	Description
57500	Custom captive portal login pages do not work when guest logon is enabled. The guest logon field is not displayed on the custom login page. This issue does not occur with the default Aruba login page. As a workaround, use the default captive portal page or use user logon.
62099	When connecting a client to an untrusted wired port, user entries appear in the `show user-table` output and are not aged out. To avoid stale user entries from consuming user licenses on the controller, use the `aaa user delete` command to delete unwanted user names.

SNMP

Table 16 *SNMP Issues and Limitations*

Bug ID	Description
66990, 59292	When using HP OpenView MIB version 9.10+, you may see errors while importing the MIB. This may occur if you are using a newer MIB browser. As a workaround: Select the MIBs that have errors and change: TEXTUAL-CONVENTION to: TEXTUAL-CONVENTION FROM SNMPv2-TC **NOTE:** Make sure you do not have a comma ',' at the end when updating this entry.

Startup Wizard

Table 17 *Startup Wizard Issues and Limitations*

Bug ID	Description
66893	The campus WLAN wizard displays an error when deleting a WLAN using the **Exit Now** link in Step 1 after modifying the WLAN authentication type and internal/guest mode multiple times. As a workaround, delete the WLAN using the WebUI or CLI.

Syslog

Table 18 *Syslog Known Issues and Limitations*

Bug ID	Description
62916	Access Points may send debug log messages to the Syslog server, even if debug log messages are disabled.

Voice

Table 19 *Voice Known Issues and Limitations*

Bug ID	Description
65546	Classified media sessions from Lync clients might not be fast aged after call termination.

Table 19 *Voice Known Issues and Limitations (Continued)*

Bug ID	Description
56506	SIP ALG might generate an additional CDR with invalid data when DELTS is received while terminating the call. Additionally, an invalid entry is added to the voice call quality table.This is a CLI issue and does not impact functionality.
55058	CLI output might not show the Lync clients getting tagged with the high priority ToS value. This is a CLI display issue and doesn't affect Lync functionality. This issue has been seen with Lync clients taking part in conference calls, but does not occur with peer-to-peer calls.

WebUI

Table 20 *WebUI Known Issues and Limitations*

Bug ID	Description
55040	On the WebUI, the U600 modem in the 4G option is missing from the **Wireless > AP Installation > Provisioning Profile,** preventing you from creating a provisioning profile for the U600 in 4G. Perform one of the following as a workaround: ● Create a provisioning profile with 4G parameters (i.e., usb_type = "beeceem-wimax") from the command line and apply that profile to the ap-group. ● Choose the correct device type in the USB settings of the AP Installation page through the WebUI
66516	When APs are distributed in multiple pages in the WebUI in the **Configuration** > **WIRELESS** > **AP Installation** > **Provisioning** tab, the UI sorts only the APs in the current page and not the entire list.

Issues Under Investigation

The following issues have been reported in ArubaOS 6.1.3.6-AirGroup but not confirmed. The issues have not been able to be reproduced and the root cause has not been isolated. They are included here because they have been reported to Aruba and are being investigated. In the tables below, similar issues have been grouped together.

OSPF

Table 21 *OSPF Observed Issues*

Bug ID	Description
62839	The OSPF process on the controller may not function correctly when OSPF routing, OSPF neighbors, and a DHCP helper IP address are configured, causing the controller to reboot.

Platform/Datapath

Table 22 *Platform/Datapath Observed Issues*

Bug ID	Description
65690, 65632	An internal controller process malfunction, leading to a controller reboot, has been observed.

WebUI

Table 23 *WebUI Observed Issues*

Bug ID	Description
66521	The WebUI includes two **Apply** buttons in the **Configuration** > **Security** > **Authentication** > **Internal DB** page. The **Apply** button at the bottom of the page does not add the user but does apply any user list changes that already exist. Click the **Apply** button at the top to add a new user. After the screen refreshes, click the **Apply** button at the bottom to apply any user list changes.

Chapter 5

Upgrade Procedures

This chapter details software upgrade procedures. Aruba best practices recommend that you schedule a maintenance window when upgrading your controllers.

CAUTION

Read all the information in this chapter before upgrading your controller.

Topics in this chapter include:

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions listed below. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network during the upgrade, such as configuration changes, hardware upgrades, or changes to the rest of the network. This simplifies troubleshooting.
- Know your network. Please verify the state of your network by answering the following questions.
  - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > Network All Access Points** section of the WebUI, or by issuing the **show ap active** and **show ap database** CLI commands.
  - How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
  - What version of ArubaOS is currently on the controller?
  - Are all controllers in a master-local cluster running the same version of code?
  - Which services are used on the controllers (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the controller. FTP is faster then TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.

- Before you upgrade to ArubaOS 6.1.3.6-AirGroup, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the user guide.

Memory Requirements

All Aruba controllers store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the controller. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, Aruba recommends the following compact memory best practices:

- Issue the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI, or at least 60 MB of free memory available for an upgrade using the WebUI. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up, upgrade immediately.
- Issue the **show storage** command to confirm that there is at least 60 MB of flash available for an upgrade using the CLI, or at least 75 MB of flash available for an upgrade using the WebUI.

CAUTION

In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before rebooting.

If the output of the **show storage** command indicates that insufficient flash space is available, you must free up additional memory. Any controller logs. crash data or and flash backups should be copied to a location off the controller, then deleted from the controller to free up flash space. You can delete the following files from the controller to free memory before upgrading:

- **Crash Data:** Issue the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in "Backing up Critical Data" on page 22 to copy the **crash.tar** file to an external server, then issue the command **tar clean crash** to delete the file from the controller.
- **Flash Backups:** Use the procedures described in "Backing up Critical Data" on page 22 to backup the flash directory to a file named **flash.tar.gz**, then issue the command **tar clean flash** to delete the file from the controller.
- **Log files:** Issue the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in "Backing up Critical Data" on page 22 to copy the **logs.tar** file to an external server, then issue the command **tar clean logs** to delete the file from the controller.

Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Custom captive portal pages
- x.509 certificates
- Controller Logs

Backup and Restore Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the controller:

1. Click on the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to back up the contents of the compact flash file system to the flashbackup.tar.gz file.
5. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Backup and Restore Compact Flash in the CLI

The following steps describe the back up and restore procedure for the entire compact flash file system using the controller's command line:

1. Enter **enable** mode in the CLI on the controller, and enter the following command:

   ```
   (host) # write memory
   ```
2. Use the **backup** command to back up the contents of the Compact Flash file system to the flashbackup.tar.gz file.

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
3. Use the **copy** command to transfer the backup flash file to an external server:

   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
   <remote directory>
   ```

   You can later transfer the backup flash file from the external server to the Compact Flash file system with the copy command:

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   ```
4. Use the **restore** command to untar and extract the *flashbackup.tar.gz* file to the compact flash file system:

   ```
   (host) # restore flash
   ```

Upgrading in a Multi-Controller Network

In a multi-controller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in "Backing up Critical Data" on page 22.

NOTE

For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant (VRRP) environments, the controllers should be the same model.

To upgrade an existing multi-controller system to ArubaOS 6.1.3.6-AirGroup:

1. Load the software image onto all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded with the same software image and reloaded simultaneously, use the following guidelines:
   a. Remove the link between the master and local mobility controllers.
   b. Upgrade the software image, then reload the master and local controllers one by one.
   c. Verify that the master and all local controllers are upgraded properly.
   d. Connect the link between the master and local controllers.

Upgrading to 6.1.x

CAUTION

ArubaOS 6.x is supported only on the newer MIPS controllers (M3, 3000 Series and 600 Series). Legacy PPC controllers (200, 800, 2400, SC1 and SC2) are *not* supported. DO NOT upgrade to 6.x if your deployments contain a mix of MIPS and PPC controllers in a master-local setup.

When upgrading the software in a multi-controller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence.(See "Upgrading in a Multi-Controller Network" on page 23.)

Caveats

Before upgrading to any version of ArubaOS 6.1, take note of these known upgrade caveats.

- Control plane security is disabled when you upgrade from 3.4.x to 6.0.1 (control plane security is disabled in 6.0.1) and then to 6.1.
- If you want to downgrade to a prior version, and your current ArubaOS 6.1 configuration has control plane security enabled, disable control plane security before you downgrade.

  For more information on configuring control plane security and auto-certificate provisioning, refer to the *ArubaOS 6.1 User Guide*.

Install using the WebUI

CAUTION

Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI. For details, see "Memory Requirements" on page 22

Upgrading From an Older version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. **If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.1.3.6-AirGroup.**

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS RN-3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
- For ArubaOS versions 6.0.0.0 or 6.0.0.1, download the latest version of ArubaOS 6.0.1.x.

Follow step 2–step 11 of the procedure described in "Upgrading From a Recent version of ArubaOS" on page 25 to install the interim version of ArubaOS, then repeat step 1–step 11 of the procedure to download and install ArubaOS 6.1.3.6-AirGroup.

Upgrading From a Recent version of ArubaOS

The following steps describe the procedure to upgrade from one of the following recent versions of ArubaOS:

- 6.0.1.x or later
- 5.0.3.1 or later (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review "Upgrading With RAP-5 and RAP-5WN APs" on page 25 before proceeding further.)
- 3.4.4.1 or later

Install the ArubaOS software image from a PC or workstation using the Web User Interface (WebUI) on the controller. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Download ArubaOS 6.1.3.6-AirGroup from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Log in to the ArubaOS WebUI from the PC or workstation.
4. Navigate to the **Maintenance > Controller > Image Management** page. Select the **Upload Local File** option, then click **Browse** to navigate to the saved image file on your PC or workstation.
5. Select the downloaded image file.
6. In the **partition to upgrade** field, select the non-boot partition.
7. In the **Reboot Controller After Upgrade** option field, best practices is to select **Yes** to automatically reboot after upgrading. If you do not want the controller to reboot immediately, select **No**. Note however, that the upgrade will not take effect until you reboot the controller.
8. In Save **Current Configuration Before Reboot** field, select **Yes**.
9. Click **Upgrade**.
10. When the software image is uploaded to the controller, a popup window displays the message **Changes were written to flash successfully**.Click **OK**. If you chose to automatically reboot the controller in step 7, he reboot process starts automatically within a few seconds (unless you cancel it).
11. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade.

Once your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in into the WebUI to verify all your controllers are up after the reboot.
2. Navigate to **Monitoring > Network Summary** to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you would expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See "Backing up Critical Data" on page 22 for information on creating a backup.

Upgrading With RAP-5 and RAP-5WN APs

If you have completed the first upgrade hop to the latest version of ArubaOS 5.0.4.x and your WLAN includes RAP-5/RAP-5WN APs, do not proceed until you complete the following process. Once complete, proceed to step 5 on page 25. Note that this procedure can only be completed using the controller's command line interface.

1. Check the provisioning image version on your RAP-5/RAP-5WN Access Points by executing the **show ap image version** command.

2. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses.
3. For each of the RAP-5/RAP-5WN APs noted in the step 2, upgrade the provisioning image on the backup flash partition by executing the following command:

   ```
   apflash ap-name <Name_of_RAP> backup-partition
   ```

   The RAP-5/RAP-5WN reboots to complete the provisioning image upgrade.
4. When all the RAP-5/RAP-5WN APs with a 3.3.2.x-based RN provisioning image have successfully upgraded, verify the provisioning image by executing the following command:

   ```
   show ap image version
   ```

   The flash (Provisioning/Backup) image version string should now show a version that does not contain the letters “rn”, for example, 5.0.4.8.

If you omit the above process or fail to complete the flash (Provisioning/Backup) image upgrade to 5.0.4.x and the RAP-5/RAP-5WN was reset to factory defaults, the RAP will not be able to connect to a controller running ArubaOS 6.1.3.6-AirGroup and upgrade its production software image.

Install using the CLI

CAUTION

Confirm that there is at least 40 MB of free memory and at least 60 MB of flash available for an upgrade using the CLI. For details, see “Memory Requirements” on page 22

Upgrading From an Older version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your **controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.1.3.6-AirGroup.**

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS RN-3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
- For ArubaOS versions 6.0.0.0 or 6.0.0.1, download the latest version of ArubaOS 6.0.1.x.

Follow step 2 –step 7 of the procedure described in “Upgrading From a Recent version of ArubaOS” on page 26 to install the interim version of ArubaOS, then repeat step 1–step 7 of the procedure to download and install ArubaOS 6.1.3.6-AirGroup.

Upgrading From a Recent version of ArubaOS

The following steps describe the procedure to upgrade from one of the following recent versions of ArubaOS:

- 6.0.1.x or later
- 5.0.3.1 or later. (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review “Upgrading With RAP-5 and RAP-5WN APs” on page 25 before proceeding further.)
- 3.4.4.1 or later

To install the ArubaOS software image from a PC or workstation using the Command-Line Interface (CLI) on the controller:

1. Download ArubaOS 6.1.3.6-AirGroup from the customer support site.

2. Open a Secure Shell session (SSH) on your master (and local) controller(s).
   Execute the **ping** command to verify the network connection from the target controller to the FTP/TFTP server:

   ```
   (hostname)# ping <ftphost>
   ```

   or

   ```
   (hostname)# ping <tftphost>
   ```

3. Use the **show image version** command to check the ArubaOS images loaded on the controller's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

   ```
   (hostname) #show image version
   ----------------------------------
   Partition               : 0:0 (/dev/ha1)
   Software Version        : ArubaOS 6.1.1.0 (Digitally Signed - Production Build)
   Build number            : 28288
   Label                   : 28288
   Built on                : Thu Apr 21 12:09:15 PDT 2012
   ----------------------------------
   Partition               : 0:1 (/dev/ha1)**Default boot**
   Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
   Build number            : 33796
   Label                   : 33796
   Built on                : Fri May 25 10:04:28 PDT 2012
   ```

4. Use the **copy** command to load the new image onto the non-boot partition:

   ```
   (hostname)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition
   <0|1>
   ```

   or

   ```
   (hostname)# copy tftp: <tftphost> <image filename> system: partition <0|1>
   ```

5. Execute the **show image version** command to verify the new image is loaded:

   ```
   (hostname)# show image version


   ----------------------------------
   Partition               : 0:1 (/dev/ha1) **Default boot**
   Software Version        : ArubaOS 6.1.3.6-AirGroup (Digitally Signed - Production
   Build)
   Build number            : 39381
   Label                   : 39381
   Built on                : Fri Feb 22 00:03:14 PDT 2013
   ----------------------------------
   Partition               : 0:1 (/dev/ha1)
   Software Version        : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
   Build number            : 33796
   Label                   : 33796
   Built on                : Fri May 25 10:04:28 PDT 2012
   ```

6. Reboot the controller:

   ```
   (hostname)# reload
   ```

7. Execute the **show version** command to verify the upgrade is complete.

```
(hostname)# show version
```

Once your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in into the command-line interface to verify all your controllers are up after the reboot.
2. Issue the command **show ap active** to determine if your APs are up and ready to accept clients.
3. Issue the command **show ap database** to verify that the number of access points and clients are what you would expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See "Backing up Critical Data" on page 22 for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of ArubaOS.

WARNING

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.1.3.6-AirGroup are lost after the downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).

CAUTION

If you do not downgrade to a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.1.3.6-AirGroup to 5.0.3.2, changes made to WIPS in 6.x prevents the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with ids-transitional while older IDS profiles do not include transitional. If you think you have encountered this issue, use the `show profile-errors` and `show ap-group commands` to view the IDS profile associated with AP Group.

CAUTION

When reverting the controller software, whenever possible use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Before you Begin

Before you reboot the controller with the pre-upgrade software version, you must perform the following steps:

1. Back up your controller. For details, see "Backing up Critical Data" on page 22.
2. Verify that control plane security is disabled.
3. Set the controller to boot with the previously-saved pre-6.1 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

   When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message displays if system boot parameters are set for incompatible image and configuration files.

5. After downgrading the software on the controller:
   - Restore pre-6.1 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.1.3.6-AirGroup flash backup file.
   - You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.1.3.6-AirGroup, the changes do not appear in RF Plan in the downgraded ArubaOS version.
   - If you installed any certificates while running ArubaOS 6.1.3.6-AirGroup, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading using the WebUI

The following sections describe how to use the WebUI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
   a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
   b. For **Destination Selection**, enter a filename (other than default.cfg) for Flash File System.
2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the Configuration File menu.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition):
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading using the CLI

The following sections describe how to use the CLI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
or
(host) # copy tftp: <tftphost> <image filename> system: partition 1
```

2. Set the controller to boot with your pre-upgrade configuration file.

```
# boot config-file <backup configuration filename>
```

3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

In the following example, partition 0, the backup system partition, contains the backup release 6.1.3.2. Partition 1, the default boot partition, contains the ArubaOS 6.1.3.6-AirGroup image:

```
#show image version
----------------------------------
Partition                : 0:1 (/dev/ha1)
Software Version         : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
Build number             : 33796
Label                    : 33796
Built on                 : Fri May 25 10:04:28 PDT 2012
----------------------------------
Partition                : 0:1 (/dev/hda2) **Default boot**
Software Version         : ArubaOS 6.1.3.6-AirGroup (Digitally Signed - Production
Build)
Build number             : 39381
Label                    : 39381
Built on                 : Fri Feb 22 00:03:14 PDT 2013
```

4. Set the backup system partition as the new boot partition:

```
# boot system partition 0
```

5. Reboot the controller:

```
# reload
```

6. When the boot process is complete, verify that the controller is using the correct software:

```
# show image version
```

Before You Call Technical Support

Before you place a call to Technical Support, please follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba controller with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the controller at the time of the problem. Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture logs from the controller.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Aruba controller) or any recent changes to your controller and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred.If the problem is reproducible, list the exact steps taken to recreate the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the controller site access information, if possible.