

ArubaOS 5.0.3.3



Release Note

Copyright

© 2011 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, Bluescanner, For Wireless That Works®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFprotect®, The All Wireless Workplace Is Now Open For Business, Green Island, and The Mobile Edge Company® are trademarks of Aruba Networks, Inc.

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. Any other trademarks appearing in this manual are the property of their respective companies.

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. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

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

Warranty

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

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



www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Chapter 1	Release Overview	5
	Chapter Overview	5
	Release Mapping	5
	Contacting Support	6
Chapter 2	What's New in this Release	7
	In Previous ArubaOS 5.0.3 Releases	7
	Voice Performance Enhancement	7
	Firewall Enforce TCP Sequence	7
Chapter 3	Fixed Issues	9
Chapter 4	Known Issues	19
Chapter 5	Upgrade Procedures	25
	Important Points to Remember	25
	Technical Upgrading Best Practices	26
	Basic Upgrade Sequence	26
	Managing Flash Memory	27
	Before you upgrade	27
	Backing up Critical Data	27
	Backup and Restore Compact Flash on the WebUI	27
	Backup and Restore Compact Flash on the CLI	28
	License Mapping	28
	Licensing Change History	28
	ArubaOS 5.0	28
	ArubaOS 3.4.1	28
	ArubaOS 3.4.0	28
	Upgrading from 3.4.x to 5.0	29
	Caveats	29
	Load New Licenses	30
	Save your Configuration	30
	Saving the Configuration on the WebUI	30
	Saving the Configuration on the CLI	30
	Install ArubaOS 5.0.3.3	30
	Install ArubaOS 5.0.3.3 on the WebUI	30
	Install ArubaOS 5.0.3.3 on the CLI	31
	Upgrading from 3.3.x to 5.0	32
	Upgrading on the WebUI	32
	Upgrading on the CLI	32
	Upgrading from 2.5.x to 3.3.x to 5.0.	33
	Upgrading from RN-3.x.x to 5.0	33
	Caveat	33
	Upgrading in a Multi-Controller Network	34
	Pre-shared Key for Inter-Controller Communication	34
	Downgrading after an Upgrade	34
	Downgrading on the WebUI	35

Downgrading on the CLI.....	36
Controller Migration.....	36
Single Controller Environment	37
Multiple Master Controller Environment	37
Master/Local Controller Environment	37
Before You Start.....	37
Basic Migration Steps.....	37
Before You Call Technical Support	38

ArubaOS 5.0.3.3 is a patch software release that introduces fixes to many previously outstanding issues. For details on all of the features described in the following sections, see the *ArubaOS 5.0 User Guide*, *ArubaOS 5.0 CLI Reference Guide*, and *ArubaOS 5.0 MIB Reference Guide*.



See the [Chapter 5, “Upgrade Procedures”](#) on page 25 for instructions on how to upgrade your controller to this release.

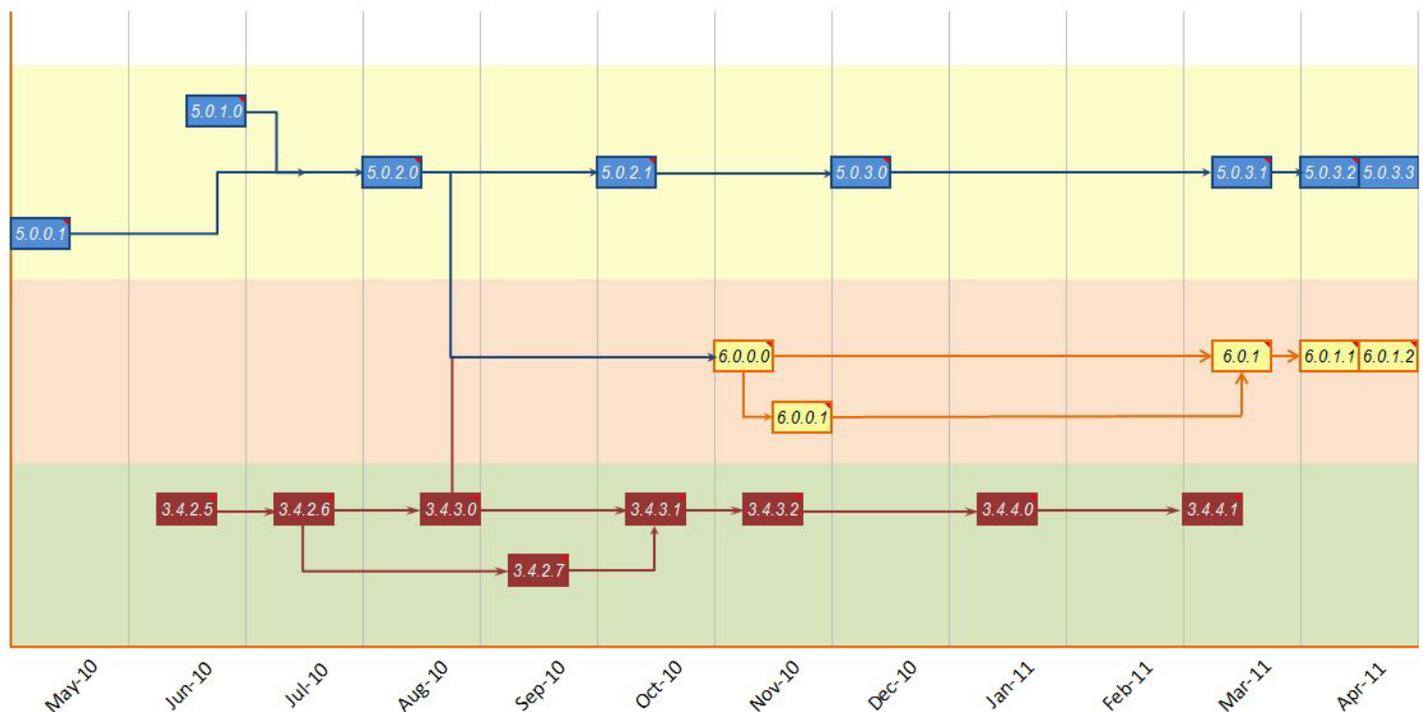
Chapter Overview

- [Chapter 2, “What’s New in this Release”](#) on page 7 describes the new features introduced in this release.
- [Chapter 3, “Fixed Issues”](#) on page 9 describes the issues that have been fixed in this release.
- [Chapter 4, “Known Issues”](#) on page 19 provides descriptions and workarounds for outstanding issues in ArubaOS 5.0.3.
- [Chapter 5, “Upgrade Procedures”](#) on page 25 cover the procedures for upgrading your controller from any release of ArubaOS to ArubaOS 5.0.3.

Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 5.0.3.1.

Figure 1 ArubaOS Release Mapping



Contacting Support

Table 1 *Web Sites and Emails*

Web Site	
• Main Site	http://www.arubanetworks.com
• Support Site	https://support.arubanetworks.com
• Software Licensing Site	https://licensing.arubanetworks.com/login.php
• Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
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

Table 2 *Contact Phone Numbers*

Telephone Numbers	
• Aruba Corporate	+1 (408) 227-4500
• FAX	+1 (408) 227-4550
Support	
United States	800-WI-FI-LAN (800-943-4526)
Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and the UK	+800-4WIFI-LAN (+800-49434-526)
All other countries	+1 (408) 754-1200

ArubaOS 5.0.3.3 is a patch release that addresses and provides solutions for a number of known issues. For more information about ArubaOS, refer to the *ArubaOS 5.0 User Guide* or *Command Line Reference*. See the “[Upgrade Procedures](#)” on page 25 for instructions on how to upgrade your controller to this release.

In Previous ArubaOS 5.0.3 Releases

Previous releases of ArubaOS 5.0.3 have introduced additional software enhancements for all Aruba controllers. This section describes those enhancements.

Voice Performance Enhancement

This release contains voice performance enhancements for SIP calls over 11n APs. To take advantage of this improvement, you must set the interference-immunity in the 11a and 11g radio profiles to Level-3. This can be done through the WebUI or the CLI.

Firewall Enforce TCP Sequence

A command has been added to the CLI that allows the user to enable enforcement of the packet sequence numbers of TCP traffic passing through the firewall.



Enabling this feature creates very strict TCP enforcement that, while helping protect your network from unwanted attacks, can make it difficult for genuine client traffic from connecting if the client's packets are out of sequence.

By default, this feature is disabled. To enable this feature, use the following CLI command:

```
firewall enforce-tcp-sequence
```

To disable this feature:

```
no firewall enforce-tcp-sequence
```


This release contains all fixes up to and including those in ArubaOS 5.0.3. The following issues and limitations have been fixed in the ArubaOS 5.0.3.3 release:

Table 4 Fixed in ArubaOS 5.0.3.3

Bug ID	Description
35596	VLAN derivation with <code>value-of</code> against a string attribute works correctly.
38793, 37387, 45049	An issue in which local-userdb entries became corrupted after a power failure has been fixed.
41043	In the WebUI, firewall policies are now displayed when editing user roles.
42452	The issue in which mesh points drop large multicast frames due to <code>rx_ccmreply</code> has been fixed.
43584	The full name of the guest is now correctly displayed when creating a new user with guest provisioning access.
43812	To prevent the <code>/tmp/deviceCertLib.log</code> file from growing indefinitely, the file is now broken up into two parts: Error and Debug. Additionally, the file size has been limited to 20 KB for all AP platforms and 200 KB for all controller platforms.
44126	Client devices equipped with an Intel 4965AGN NIC can now maintain a connection and pass traffic when connected to an AP-125 via an HT SSID.
45009	A connectivity issue caused by abnormally large <code>Available TX Buffers</code> counts has been fixed.
45643	An AP-85 mesh point crash caused when the AP attempts to process large frames has been fixed.
45829, 46344, 45668	Clients are now able to correctly authenticate while doing AAA Radius authentication.
45866, 44712, 50392, 44934	A datapath timeout issue causing the M3 controller to continuously reboot after upgrading has been fixed.
46340	ZTE modem <code>ttyUSB</code> no longer changes between cold and warm boot.
46701	A RAP-5 crash that happens when the RAP is connected to an EVDO device has been fixed.
46761, 51443	An SNMP walk issue that breaks at <code>wlsxVoiceAPBssidInfoGroup</code> has been fixed.
47048	Aruba-ESSID and Aruba-Location-ID are no longer missing from RADIUS requests sent to an external server when the client is authenticated by an XML-API command.
47219, 47402	The controller no longer stops forwarding traffic to clients connected via PPTP.
47313	A controller reboot caused by <code>udbserver</code> module crash has been fixed.

Table 4 Fixed in ArubaOS 5.0.3.3

Bug ID	Description
47890, 48314, 49921, 50349, 51860, 52146, 52192	A controller auth module crash has been fixed.
48413	An auth crash caused when the controller queries an LDAP server has been fixed.
48537, 50123	Authentication issues, accompanied by RADIUS timeout stats increasing, when static-wep and VLAN derivation are enabled has been fixed.
48625	When a user is added to the user-table, the controller updates that entry in the route-cache table and deletes any old entries.
48660	An error log message has been added to report if ArubaOS failed to decode mppe key attributes.
48873	APs no longer deauth all associated clients when an association flood is detected.
49321	The RADIUS attribute for Aruba-Location-Id is now correctly filled when the forwarding mode is split-tunnel.
49418, 38174	Disabling VRRP preemption now works correctly in a master-local setup.
49907	Multicast now works correctly when port channeling is enabled on the master controller.
49977, 50665	An isakmpd module crash caused by VRRP flaps has been fixed.
50578	An AP STM memory leak initiated by a controller death has been fixed.
50893, 51812, 52174, 51474, 52544	An issue in which APs are not coming up with the error message <code>PAPI_Send failed: No buffer space available</code> has been fixed.

Table 5 Fixed in ArubaOS 5.0.3.2

Bug ID	Description
51446, 51733	ArubaOS now provides full trust chain of its server certificate in TLS sessions.
N/A	This release contains fixes for issues found internally.

Table 6 Fixed in ArubaOS 5.0.3.1

Bug ID	Description
33079	SSH access does not incorrectly hang if the controller is unable to contact the DNS server.

Table 6 Fixed in ArubaOS 5.0.3.1

Bug ID	Description
37115	The time it takes for the controller to locate APs for the first time, or after the cache has expired, has been improved and no longer causes the WebUI to freeze for long periods of time.
40144	Dot1x authentication now works correctly when both user and machine authentication are enabled.
40315, 34967, 37402	An issue in which APs bootstrapped and failed to come back up after configuration change due to broken tunnels has been fixed.
40444	The default gateway can successfully be deleted using the WebUI.
41299, 45362	An IP pool leak that was preventing users from connecting using L2TP VPN has been fixed.
43215, 43915	Clients correctly receive a DHCP ACK not matter what broadcast flag bit is applied to the DHCP request. To allow this, shaping/policing for multicast and broadcast traffic on APs based on descriptor usage has been disabled.
43625	Broadcast packets were being flooded into bridge/split tunnels and consuming bandwidth. A fix has been added to drop non-EAPOL packets on bridge/split dot1x tunnel for wired and wireless traffic.
44846	An issue in which APs bootstrap during a write mem on the master controller has been fixed.
44984, 45155	An ACL mismatch between Auth and STM/SAPM that was preventing client devices from receiving an IP address from the DHCP server has been fixed.
45053, 46234, 39935, 45710, 45203	Improvements have been made to the stm module to prevent the controller and APs terminating on it from experiencing unintended reboots.
45117, 45116	AN STM crashed caused by an API signature mismatch has been fixed.
45128, 45896	The controller displays the correct user role in <code>show user-table</code> .
45174	In forward bridge mode, tunnels are not added to vlan-mcast table to prevent the flooding of any kind of packets (unicast, broadcast, multicast) on the base tunnel.
45202	The minimum frame size on encrypted channel has been reduced from 16 bytes to 8 bytes. This is to ensure that EAPOL-Start packets on encrypted channel are correctly decoded.
45270, 46442, 45744	Unexpected controller behavior due to a datapath exception has been fixed.
45325, 44379, 46315, 47913	This release contains voice performance enhancements for SIP calls over 11n APs. To take advantage of this improvement, you must set the interference-immunity in the 11a and 11g radio profiles to Level-3. This can be done through the WebUI or the CLI.
45383, 42958	The RAP-5 no longer crashes with the message "PPP: Termination Request Received" when using a 3G modem.

Table 6 Fixed in ArubaOS 5.0.3.1

Bug ID	Description
45505, 45618, 46068, 46536, 47884, 48878	Controller no longer reloads or fails to respond due to datapath timeouts.
45534	Clients that support PMK caching are now placed into the correct cached user role after a disconnect and reconnect. When connecting to the same BSSID, the cached user role information is used.
45631, 45066	After disabling SNMP server using the <code>no snmp-server</code> command, SNMP server can be re-enabled by executing the command <code>snmp-server</code> from the configure mode.
45777	There is no longer an ACL mismatch between the RAP datapath and controller when the ACL is applied to a user role.
45864	The command <code>show ap-global ace-table acl</code> now correctly displays all ACE entries no matter how many ACE entries the ACL has.
45871, 45924	Clients no longer incorrectly remain in the Failed machine auth role after user and machine authentication have succeeded.
45895	After a rebootstrap, RAPs come back up and now sync to the correct ACL.
45914, 45917	An STM crash, which occurs when executing the <code>show ap-global acl-table</code> command, causing the controller to become unusable has been fixed.
45932	RAP clients are placed in the correct role when moved from an LMS to the backup-LMS and back again. However, for this to take affect, the client must completely deauth and reassociate.
46001	An issue in which datapath utilization reaches 100% during peak traffic has been fixed.
46080, 46128, 46142	This release introduces the following improvements to the User table: <ul style="list-style-type: none"> • The User table shows correct client IP address even before the clients send an IP packet. • The User table displays the correct number of user entries. The User table displays the correct user ages.
46204	The controller's buffer size has been increased for EAPOL packets to help prevent authmgr crashes.
46237	The process to add and modify users and bridge mode has been improved, increasing AP stability.
46249	If an AP uplink's router port is shut down for extended period of time, the AP will automatically recreate an IPsec tunnel to the controller once the router port is reenabled.
46321	Users are able to establish passive FTP connections.
46348	Clients no longer experience a delay in switching to a VLAN specified by server derivation rule.
46483	Improvements to the Auth and STM modules prevent the controller from failing to respond due to IPIP loops.
46624	For APs using a bridge-mode SSID, VLANs in a virtual AP profile no longer appear in the Datapath VLAN Multicast Entries table, since the VLAN is only local to the bridge.
46963	Improvements to the Authmgr module increase controller stability.

Table 6 Fixed in ArubaOS 5.0.3.1

Bug ID	Description
47032, 49180	The DNSmasq process on 600 Series controllers has been improved to allow a DNS query of a domain name longer than 51 characters.
47069	Improvements to NAT discovery payload handing allow the controller to continue to respond properly even if the NAT discovery payload includes in an incorrect length.
47519	Captive Portal whitelists can be created or modified regardless of whether the PWA license is installed on the controller.
47850	In a RAP-5WN deployment, a Vonage phone adapter that plugs into a wired port in bridge mode is now able to obtain an IP address using DHCP.
47805	The internal database on a master controller can be used for 802.1x machine authentication.
48387	If a captive portal page requires a user to click an Accept button to agree to a user policy, the customer will not be redirected to the requested Web site until the Accept button is clicked.
46237	The process to add and modify users and bridge mode has been improved, increasing AP stability.
46249	If an AP uplink's router port is shut down for extended period of time, the AP will automatically recreate an IPsec tunnel to the controller once the router port is reenabled.

Table 7 Fixed in ArubaOS 5.0.3

Bug ID	Description
25362, 24401	Stale vpn user entries are no longer building up in the user table because their associated L2TP tunnels are now deleted when no longer in use.
28532	Previous parsing mechanism used space as delimiter, so if there is a space in cluster profile, it would pick the wrong values. The parsing mechanism has been changed to TLV blocks, which can handle any possible case.
34993	Internal database fields for both usernames and emails can be up to 128 characters.
37703, 46596	Clients can now successfully authenticate against configured 802.1x profiles and the associated auth module crash has been fixed.
38793, 37387	An issue in which local-userdb entries became corrupted after a power failure has been fixed.
38938	The errorlog no longer shows a missing VPN auth profile for every reboot of the controller when there is a RAP terminating on that controller.
38964, 42709, 42708, 42751	Session age now checks for reverse age against configured timeout to avoid pre-aging session to avoid spurious deletes.
39595, 41875	An issue in which APs rebootstrap when datapath SP becomes busy has been fixed.
40032	The AP-105 no longer constantly detects spurious radar when operating DFS channels (52, 56, 60, and 64).

Table 7 Fixed in ArubaOS 5.0.3

Bug ID	Description
40225, 40639, 45001, 37873, 41471	The Network Summary > APs Down page in the WebUI no longer returns a blank page. It now returns the same information as AP database table in the CLI.
40377	An snmpd process crash that occurs when deleting a version 3 trap host has been fixed.
40558	Username checking in single-session captive-portal is no longer case-sensitive.
40664	When DNS interception is disabled using the command <code>ip cp-redirect-address disable</code> it is now correctly disabled and remains that way after rebooting the controller.
40822	When using Internet Explorer 6.0, a Guest Provision Profile user is now able to add/delete new users with the browser freezing or displaying error messages.
41351	Bridge clients now correctly get an IP address when switching from a standard VAP to a backup VAP on the same Remote AP, when the RAP is coming through a DSL router or NAT device.
41353, 44508	When a netdestination invert rule is changed, the change is now correctly reflected in the ACL immediately.
41408	A controller cfg module crash caused by an older heartbeat message packet received by the master controller; a switch entry was created for the old message, however the magic cookie was not set causing the assert call to fail. This issue has been fixed.
41727	The issue with TCP connections not being closed after role change has been fixed.
41822, 44062	The phone number and IP address of an NOE phone are now correctly displayed in the output of the <code>show voice client-status</code> command.
41894	The command <code>show ap debug driver-log</code> shows the kernel log messages and the driver log as well. Once the driver log is retrieved from the driver, the second read does not retrieve any messages because all of the messages has already been consumed and there are no new messages in the driver log.
41935, 44103	The ARM algorithm now takes into account RF anomalies to prevent APs from continually moving to channels with high amounts of interference.
42010, 43743	Special characters can be used when creating a new dialer group profile or modifying an existing one.
42132	When <code>ip local-proxy-arp on interface vlan</code> is enabled, ARP for wireless clients are no longer broadcast to all APs that share the same user VLAN. Instead controller does proxy-arp for the wireless client.
42155	L3 GRE now works correctly when Keepalive is enabled.
42261	The issue with the file transmission over poor links has been fixed.
42333, 42332	wlanAPSysLocation has been added to AP table, which gives the value of the syslocation provisioning parameter for the AP.
42493	Aeroscout tags now correctly associate with Aruba APs.

Table 7 Fixed in ArubaOS 5.0.3

Bug ID	Description
42524	The Token Caching Function has been verified. The username is now concatenated with device MAC so same user on different devices will get different cached entries in local user db. This way, a same user using a 2nd device will always go to server the first time (since no hit in cache), and create a different cache entry for the 2nd device. From then on, each device will use its own cached entry without interfering with each other.
42670, 43267	Increased stability in the UAPSD (WMM-powersave) protocol prevents unintended lock-outs on Alcatel-Lucent Mobile IP Touch (MIPT) wireless telephones after Virtual Router Redundancy Protocol (VRRP) failover.
42676	On APs, the number of open file descriptors for each monitor process are now checked once per minute and reboot the device only if the a process has more than 75% of the maximum number (1024) of file descriptors open.
42771	The Tx and Rx databytes now support 64 bits on all platforms.
42841, 40322	The issue in which APs terminating on a controller rebootstrap whenever the master controller is rebooted has been fixed.
42862, 42865	The AP-120 Series and AP-105 are now supported in the Philippines (country code PH).
42882	Spectrum Load Balancing domain now correctly calculates domain neighborhoods and will not incorrectly load balance all APs.
43079	The AP-70 no longer crashes every few minutes when JP2 or JP3 country code is set, ARM scanning is enabled, and the AP's 11b/g radio is set to channel 14.
43178	When using a wildcard certificate for Captive Portal, the URL is redirected to captiveportal-login instead of the portal.
43237, 35686, 42096, 43303	Improvements have been made to the derivation logic to prevent clients from being incorrectly moved from role to role when roaming.
43264	The WebUI will now accept only ASCII type characters in the username and password fields.
43300	The issue with the pause in traffic during the Chariot throughput test has been fixed.
43401	The AP-90 Series AP now supports up to 16 BSSIDs.
43406	A controller reboot issue caused by a datapath module crash in a master-local setup with VRRP on both controllers has been fixed.
43454	The uploaded logo now displays correctly when user credentials are printed for a new guest provisioning user.
43503	Users can now successfully send email using guest-provisioning when using a gmail server as an SMTP server.
43663	The issue with derived VLAN not assigned when both the MAC authentication and the 802.1X authentication are enabled on a AAA profile has been fixed.
43820, 40689	Handoff assist now works because RSSI values are now reported correctly.
43834, 43840	The issue with an AP being inactive for 3-5 minutes after changing the LMS on the system profile to the local controllers IP has been resolved.

Table 7 Fixed in ArubaOS 5.0.3

Bug ID	Description
43901, 43887	Hardcoding the speed to 1000Mbps on an Aruba Aruba 3000 Series controller will not cause the link to go down.
43948, 41351, 45266	An AP reboot issue caused when the AP runs out of memory has been fixed.
43949	The issue with multiple entries in the user table for a single wireless client and the missing datapath route cache table entry of a client has been fixed.
43958	The issue with the fastethernet interface not coming up has been fixed.
43977	The issue with the local controller not accessible through the WebUI after upgrading to 3.4.2.5 has been resolved.
44111	An issue in which a large syslogd buffer overwrites the syslogd stack and then crashes the syslogd process has been fixed.
44183	Dot1x authentication requires all three attributes (Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-Id) in the server derivation rules for “automatic” VLAN derivation using Tunnel-Private-Group-Id.
44256	The issue with the traffic being blocked from the bridge user to the split user has been fixed.
44378	The issue with PPTP VPN connection between a client and a server has been fixed.
44384	The issue with the min-tx (Minimum transmit power) parameter of the Adaptive Radio Management (ARM) on the mesh point was not working has been fixed.
44492	In a master-local set up the client can now successfully send the traffic after roaming from local to master.
44605	Support for G-band, as well as additional channels for the A-band, has been added for the AP-124 and AP-125 for the country code AE (United Arab Emirates).
44619, 44493	Improvements to the CFGM module prevent the controller from occasionally failing to respond, and allow users to access the controller via the WebUI or command-line interfaces.
44968	The bootstrap timer no longer erroneously reports missed heartbeats, which can cause remote APs to unnecessarily reboot.
45053	Improvements to the stm module prevents the controller and APs terminating on that from performing unintended reboots.
45179	Wired/wireless clients that MAC authentication and get assigned to an initial role are correctly assigned to the VLAN mapped in the initial role.
45189	The output of the show inventory command issued for an M3 controller module in slot 1 of a mobility controller correctly displays data for that M3 module.
45384, 46355	AMSDU is now disabled by default with a knob in the firewall command in the CLI.
45606	The Handoff Assist log message has been enhanced to show the actual low RSSI of the client.
45680	UPS Delivery Information Acquisition Devices (DIADs) stay properly connected to an Remote AP in bridge mode.
45971	Controllers can include an AP group name (Aruba-AP-Group) in the list of RADIUS attributes sent in a RADIUS authentication request.

Table 7 *Fixed in ArubaOS 5.0.3*

Bug ID	Description
46163	Improvements to the controller kernel prevent APs from performing unintended reboots.
46421	Clients are no longer being incorrectly deauthenticated when admission control is mandatory for VO and VI.
46715, 44859	EAP termination on legacy controllers no longer intermittently stops working.

The following are known issues and limitations for this release of ArubaOS. Applicable bug IDs or workarounds are included:

Table 8 *Known Issues and Limitations*

Bug ID	Description
53041	<p>APs with a static IP running ArubaOS 5.0.0.0 and later begin the Aruba Discovery Protocol (ADP) while the uplink switch spanning tree is still learning. The ADP/DNS master discovery declare failure before the port switches to forwarding causing the AP to enter a reboot loop.</p> <p>Workaround: To allow the AP to complete master discovery, disable spanning-tree or enable portfast on the AP's uplink connected switch port.</p>
46443	<p>Do not enable Firewall TCP enforcement when IP mobility is enabled.</p> <p>Workaround: None.</p>
46854	<p>On Aruba 600 Series controllers, when firewall enforce-tcp-sequence is enabled, there is an up to 3 second delay when TCP connections are established.</p> <p>Workaround: None.</p>
43798	<p>When a DHCP helper IP is configured, it is internally maintained as 2 separate entries for the vlan. Now if you try to delete the helper IP or change it to another helper IP, one incarnation of the same old helper IP is retained. So DHCP requests from a client on the vlan, the request will still get relayed to the old helper IP.</p> <p>Workaround: If you want to change/delete the DHCP helper IP, first delete the helper IP, do a "write mem" and reboot the box. This will remove the helper IP completely from the vlan after the box boots up again. Now you can assign a new helper IP if required.</p>
44240	<p>In the Alcatel-Lucent version, under Startup Wizard > VLAN and IP Interface > VLAN, when the user attempts to select a VLAN from the drop-down menu, the user will receive a Java script error and be unable to configure a VLAN pool.</p> <p>Workaround: Configure VLANs through the CLI.</p>
40558	<p>Multiple logins can be allowed when single-session is enabled, if a RADIUS server allows case-insensitive usernames.</p> <p>Workaround: None.</p>
40800	<p>On some occasions, Remote AP stops responding to association messages for clients connecting to split-tunnel SSIDs when the AP is also advertising a backup/always mode bridge SSID.</p> <p>Workaround: None.</p>

Table 8 *Known Issues and Limitations*

Bug ID	Description
40835	<p>After a VIA session is timed out, VIA is unable to make a new connection and shows the VIA Peer not responding message. This could happen if you have configured more than 10 tunnel IP addresses in VIA connection profile. VIA supports only 10 user configurable tunnel addresses and one for internally assigned IP address.</p> <p>Workaround: On the controller update the VIA connection profile to have only 10 tunnel address. On the client do the following:</p> <ol style="list-style-type: none"> 1. Navigate to the Setting > Connection Profile and click the Clear Profile button. 2. In the Status tab, click the Download Profile button. Enter your domain credentials and the VIA controller IP address and download new profiles.
40995	<p>If the DNS IP address is not configured on the controller for VPN remote clients then the client fails to set the IP address on the Windows Vista and Windows 7 systems. To verify if it is related to DNS entry or not, start Wireshark on Virtual adapter and check the DHCP (bootp) protocol packets.</p> <p>Workaround:</p> <p>Using CLI :-</p> <pre>(host)(config)# vpdn group l2tp client configuration dns <dns-ip1> <dns-ip2> (host)(config)# Write mem</pre> <p>Using the WebUI :</p> <ol style="list-style-type: none"> 1. Navigate to Configuration > Advanced Services > VPN Services IPSEC and set the Primary DNS Server under L2TP and XAUTH Parameters. 2. save configuration.
42940	Symbol wireless barcode scanners may unexpectedly de-authenticate and disassociate from remote APs.
18286	<p>The current QBSS-alternative implementation in ArubaOS has the following limitations:</p> <ul style="list-style-type: none"> • Probe-response may not actually reflect the real status if local probe is enabled. • After cac-capacity is reached, if you disconnect and re-connect a phone again, the call may not go through for 10 seconds. • Even if you disable local probe, sometime phone roaming can fail in the following scenario: <ol style="list-style-type: none"> 1. Spectralink phone roams when the phone sees an AP with better RSSI(~10dB difference) 2. let us say the cac is configured to 10. There are 16 phones and 2 APs 3. 6 phones associated to AP2 and 10 phones associated to AP1. 4. 6 phones associated to AP1 moved to nearer to AP2 where RSSI of AP2 is 10dB better than RSSI of AP1. 5. Even if there is a retry or packet loss issue for the phones associated with APs, the 6 phones will try to move to AP2. 6. They send QBSS probs and AP will send out QBSS + responses to all 6 Phones. 7. Then the 6 Phones will try to associate to AP2 since all 6 got QBSS response. But only 4 phones will succeed and two will be rejected eventually. 8. This will cause some temporary call drops for the two rejected phones.
20441	After the STM module is respawned (i.e. after a crash), the <code>show voice</code> commands will not display any information because the memory that stores the data is cleared after STM restarts.
26699	Due to the use of different methods to setup an IPSec policy filter between the Aruba dialer and the Microsoft native dialer, the Aruba dialer will “break” the Microsoft native dialer for IPSec L2TP.
28608, 28939	The <code>show datapath</code> command does not return any output for RAPs connected to high latency 3G/EVDO links.
30592	Bulk RAP provisioning for multiple AP groups does not support triangulation.
31388	User role and VLAN derivation based on DHCP-option-77 is not supported on RAPs.
31601	When a user changes VLANs, the SSID user entry for both VLANs will be updated.

Table 8 *Known Issues and Limitations*

Bug ID	Description
32076	Unicast and multicast key rotation does not work for split-tunnel 802.1x authentication.
32320	Hitachi wireless IP 5000 phone with firmware version 2.5.2 LA1 cannot associate with an AP in WPA2-PSK-AES mode when the SSID has both WPA-PSK-TKIP and WPA2-PSK-AES enabled on it. This is because the STA is sending AES CCMP as the multicast cipher, instead of TKIP.
32503	NTP must be run on the controller before VRRP. If this is not done, the system clocks between controllers in a master-backup setup will not be synced correctly.
32619	Controllers can only export up to 100 VLAN subnets to neighbors.
32650	If the local-userdb-ap entry is deleted for a non-remote AP, the AP will reboot.
32896	An Air Monitor will not process Ethernet frames on the 'eth1' interface, except in cases where eth0 and eth1 are deployed in a standby configuration for an AP-70. In this scenario, if eth1 is active, the Air Monitor will receive the ethernet frames on this interface. This issue will affect rogue AP classification for devices on the eth1 interface.
33192	Aruba VIA does not support new pin and next pin mode for Radius authentication.
33541	For RAPs, the local debugging ping and traceroute tools will not work if the AP's IP address is not routable.
33829	In the WebUI, under Monitoring > Access Points > USB , the serial number will not be displayed.
34148	Double encryption does not work for tunnel SSIDs on AP-120 series and RAP-5s conneted to an M3 controller.
34202	All client associations will be cleared for an AP terminated to local controller when the master controller is rebooted.
34238	Load balancing over equally costed routes does not work.
34435	The RAP DHCP server feature does not work. Clients will not receive an IP address.
34635	"Deny time range" in virtual AP does not work in split-tunnel and Bridge mode.
35088	The ap-group provisioning profile will always take precedence over the ap-name provisioning profile.
35231, 30257	Max-retries cannot be configured in an SSID profile.
35463	The uplink connection to a RAP must be through ethernet port 0, otherwise the RAP will not come up.
35605	When RAP reboots after provisioning at home, if the wired port is in tunnel mode, local debugging page does not refresh as local debugging does not work on tunnel mode vap/port.
35674	Dynamic pullout or plug-in of an EVDO modem on a RAP does not work with Huawei E272
36117	RFProtect shielding fails if the SSID is using WEP authentication. It will work when the SSID is open or using WPA PSK.
36291	RAP-5 and RAP-5WN cannot be used as a mesh point.
36601	Mesh points are unable to get an IP address from a DHCP pool defined on the controller if the rf-band configured under dummy split VAP is not the same as the rf-band configured under the mesh cluster.

Table 8 *Known Issues and Limitations*

Bug ID	Description
36891	RAPs cannot be provisioned when using D-Link DIR-100 NAT device due to decryption failures.
36923	RAPs running ArubaOS 2.5 cannot upgrade directly to ArubaOS 5.0 because ArubaOS 2.5 does not support AES.
37304	There is a discrepancy in the way the CLI and WebUI display local-userdb users. The WebUI does not have following columns: Staus, Sponsor-Name and Grantor-Name but the specified tables are shown in CLI.
37443	Uplink Manager functionalities appear on non-600 series platforms but cannot be used.
37700	When a client's ethernet port is connected, the client fails wireless 802.1x authentication.
37774	CPSec CAP cannot TFTP core files to the configured dumpserver unless a route is added on the upstream router to point to the controller for AP subnets.
37776	If cookies are disabled in Microsoft Internet Explorer (IE) VIA profiles cannot be download. Workaround: Enable cookies in IE to download VIA profiles.
37858	A controller will not process OSPF LS Update packets if the packet is fragmented.
37905	MTU size is not displayed in an <code>ap bss-table</code> for RAP bridge port because there is no data-pkt tunnel between RAP and controller for bridge mode. Therefore, no MTU discovery happens
38015	Aruba VIA client does not automatically detect Aruba Captive Portal. Workaround: Launch Aruba VIA client after completing the authentication process using the Aruba Captive Portal.
38105	Aruba VIA client is not supported on 64-bit operating systems.
38398	Only one VAP can have band steering enabled per ap group. Enabling it on multiple VAPs will not give expected results for clients connecting to all VAPs having band steering enabled.
38403, 40238	The <code>master-ip</code> parameter has been removed from the command <code>ap system-profile</code> .
38571	Spectrum load balancing requires scanning to be enabled in the ARM profile.
38602	The <code>aaa</code> profile used for the <code>dummy-split-vap</code> should not have L2 authentication enabled.
38782	A <code>mgmt-user</code> with a username of <code>l</code> , <code>s</code> , or <code>w</code> cannot be created since they are the starting character of keywords under the <code>mgmt-user</code> command.
38850	A <code>mgmt-user</code> username cannot exceed more than 16 characters, however <code>local-userdb</code> username can exceed 16 characters.
39149	Voice ALGs are not supported in bridge mode.
39356	IPSec encryption is not available for d-tunnel wireless traffic on RAPs.
39364	Cluster-root cannot point to the VRRP IP address of cluster-member-ip.
39417	The limit for static routes is 128, not 256.
39614	RAP-2WG cannot be used as a remote mesh point since the RAP-2WG does not have an 802.11a radio and mesh points are configured over 'a' radio.

Table 8 *Known Issues and Limitations*

Bug ID	Description
39664	The rapconsole does not show the IP addresses of clients.
39666	When a split-tunneled wired client is disconnected from a RAP, the client is immediately removed from the user table.
39668	Saving the 3G/EVDO values for the provisioning at home feature can take up to 30 seconds. When the save is complete, the page will refresh automatically.
39849	Versions ArubaOS pre-3.4 do not support local-userdb export files generated by versions of ArubaOS 3.4 or newer.
39906	In ArubaOS 5.0, the <code>aaa authentication vpn default</code> cannot be modified without the PEFV license.
40076	Captive Portal is not supported in bridge mode.
40400	In Windows 7, connectivity to an internal resource/network fails after a suspend and restart activity. Workaround: Disconnect and reconnect Aruba VIA from the Status tab.
40611	ArubaOS only supports up to 4 aliases in a returned FQDN query.

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



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

Topics in this chapter include:

- “Important Points to Remember” on page 25
- “License Mapping” on page 28
- “Upgrading from 3.4.x to 5.0” on page 29
- “Upgrading from 3.3.x to 5.0” on page 32
- “Upgrading from 2.5.x to 3.3.x to 5.0.” on page 33
- “Upgrading from RN-3.x.x to 5.0” on page 33
- “Upgrading in a Multi-Controller Network” on page 34
- “Downgrading after an Upgrade” on page 34
- “Controller Migration” on page 36
- “Before You Call Technical Support” on page 38



All versions assume that you have upgraded to the most recent version as posted on the Aruba download site. For instance, 3.3.x assumes you have upgraded to the most recent version of 3.3.

Important Points to Remember

Upgrading your Aruba infrastructure can be confusing. To optimize your upgrade procedure, take the actions listed below to ensure your upgrade is successful. You should create a permanent list of this information for future use.

- Best practices recommends upgrading during a maintenance window. This will limit the troubleshooting variables.
- Verify your current ArubaOS version (execute the **show version** or the **show image version** command).
- Verify which services you are using for each controller (for example, Employee Wireless, Guest Access, Remote AP, Wireless Voice).
- Verify the exact number of access points (APs) you have assigned to each controller.
- List which method each AP uses to discover each controller (DNS, DHCP Option, broadcast), and verify that those methods are operating as expected.
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- List the devices in your infrastructure that are used to provide your wireless users with connectivity (Core switches, radius servers, DHCP servers, firewall, for example).

Technical Upgrading Best Practices

- Know your topology. The most important path is the connectivity between your APs and their controllers. Connectivity issues will interfere with a successful upgrade. You must have the ability to test and make connectivity changes (routing, switching, DHCP, authentication) to ensure your traffic path is functioning.
- Avoid combining a software upgrade with other upgrades; this will limit your troubleshooting variables.
- Avoid making configuration changes during your upgrade.
- Notify your community, well in advance, of your intention to upgrade.
- Verify that all of your controllers are running the same software version in a master-local relationship. The same software version assures consistent behavior in a multi-controller environment.
- Use FTP to upload software images to the controller. FTP is much faster than TFTP and also offers more resilience over slower links.



If you must use TFTP, ensure that your TFTP servers can send more than 30 MB of data.

- Always upgrade the non-boot partition first. If something happens during 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.

Basic Upgrade Sequence

Testing your clients and ensuring performance and connectivity is probably the most time-consuming part of the upgrade. Best practices recommends that you enlist users in different locations to assist with the validation before you begin the upgrade. The list below is an overview of the upgrade and validation procedures.



If you manage your controllers via the AirWave Wireless Management Suite, the AirWave upgrade process automates most of these steps.

1. Upload the same version of the new software image onto all controllers.
2. Reboot all controllers simultaneously.
3. Execute the **ping -t** command to verify all your controllers are up after the reboot.
4. Open a Secure Shell session (SSH) on your Master Controller.
5. Execute the **show ap database** command to determine if your APs are up and ready to accept clients.
6. Execute the **show ap active** to view the up and running APs.
7. Cycle between [step 5](#) and [step 6](#) until a sufficient amount of APs are confirmed up and running.

The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table <access point ip address>** command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.

8. Verify that the number of access points and clients are what you would expect.
9. Test a different type of client for each access method (802.1x, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.

Managing Flash Memory

All Aruba controllers store critical configuration data on an onboard compact flash memory module. To maintain the reliability of your WLAN network, Aruba recommends the following compact flash memory best practices:

- Do not exceed the size of the flash file system. For example, loading multiple large building JPEGs for RF Plan can consume flash space quickly.

Warning messages alert you that the file system is running out of space if there is a write attempt to flash and 5 Mbytes or less of space remains.

Other tasks which are sensitive to insufficient flash file system space include:

- DHCP lease and renew information is stored in flash. If the file system is full, DHCP addresses can not be distributed or renewed.
- If a controller encounters a problem and it needs to write a log file, it will not be able to do so if the file system is full and critical troubleshooting information will be lost



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.

Before you upgrade

You should ensure the following before installing a new image on the controller:

- Make sure you have at least 10 MB of free compact flash space (**show storage** command).
- Run the **tar crash** command to ensure there are no “process died” files clogging up memory and FTP/TFTP the files to another storage device.
- Remove all unnecessary saved files from flash (**delete filename** command).

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 facility. 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
- Customer captive portal pages
- Customer x.509 certificates

Backup and Restore Compact Flash on 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. Navigate to the **Maintenance > File > Backup Flash** page.
2. Click **Create Backup** to back up the contents of the Compact Flash file system to the file `flashbackup.tar.gz`.
3. 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 by navigating to the **Maintenance > File > Copy Files** page.

4. 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 on 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. Use the **backup** command to back up the contents of the Compact Flash file system to the file `flashbackup.tar.gz`:

```
(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.
```

2. 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
```

3. Use the **restore** command to untar and extract the `flashbackup.tar.gz` file to the Compact Flash file system:

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

License Mapping

License consolidation and even renaming of licenses occur over time. [Figure 2](#) is an up-to-date illustration of the consolidated licenses effective with this release.

Licensing Change History

The following changes and/or consolidations were made to the ArubaOS licensing.

ArubaOS 5.0

- MAP was merged into base ArubaOS
- VPN was merged into base ArubaOS
- RAP was merged into AP license
- PEF (user basis) was converted to PEFNG (AP basis) with ArubaOS 5.0

ArubaOS 3.4.1

- VOC was merged into PEF. This merge happened with ArubaOS 3.4.1
- IMP was merged into base ArubaOS

ArubaOS 3.4.0

- ESI was merged into PEF

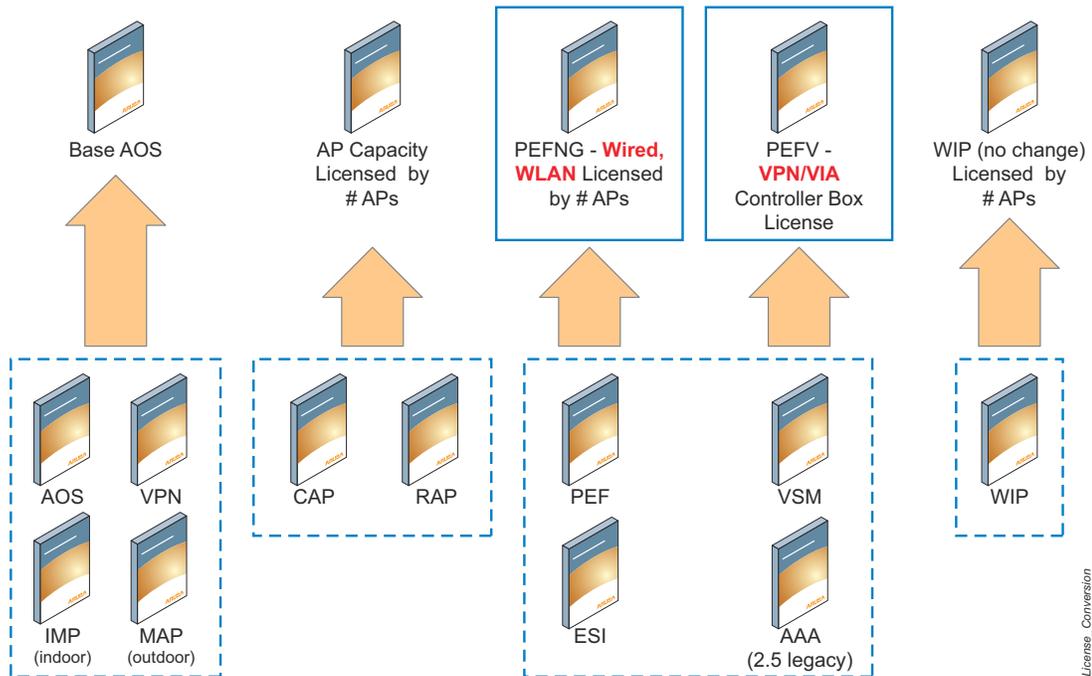
ArubaOS Legacy and End-of-Life

- AAA was merged into ESI with the release of ArubaOS 2.5.3.
- CIM is End-of-life



Releases older than ArubaOS 2.5.4 have been End-of-Lifed.

Figure 2 License Consolidation



Upgrading from 3.4.x to 5.0

Read all the following information before you upgrade to ArubaOS 5.0.3.3. If you are upgrading from a version earlier than 3.4.x, see “Upgrading from 3.3.x to 5.0” on page 32 or “Upgrading from 2.5.x to 3.3.x to 5.0.” on page 33.

- “Caveats” on page 29
- “Load New Licenses” on page 30.
- “Save your Configuration” on page 30.
- “Install ArubaOS 5.0.3.3” on page 30

Caveats

Before upgrading to ArubaOS 5.0 take note of these known upgrade caveats.

- If you have occasion to downgrade to a prior version, and your current ArubaOS 5.0 configuration has CPsec enabled, you must disable CPsec before you downgrade.

For more information on configuring control plane security and auto-certificate provisioning, refer to the *ArubaOS 5.0 User Guide*.

Load New Licenses

Before you upgrade to ArubaOS 5.0, assess your software license requirements and load any new or expanded licenses you require prior to upgrading to ArubaOS 5.0.

Software licenses in ArubaOS 5.0 are consolidated and in some instances license names and modules are renamed to more accurately represent the modules supported by the licenses (see [Figure 2](#)).

For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the user guide.



If you need to downgrade to ArubaOS 3.4.x, the previous licenses will be restored. However, once you upgrade again to ArubaOS 5.0 the licenses will no longer revert should you need to downgrade again.

Save your Configuration

Before upgrading, save your configuration and back up your controllers data files (see “[Managing Flash Memory](#)” on page 27). Saving your configuration saves the **admin** and **enable** passwords in the proper format.

Saving the Configuration on the WebUI

1. Click on the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the screen.

Saving the Configuration on the CLI

Enter the following command in enable or config mode:

```
(host) #write memory
```

Install ArubaOS 5.0.3.3

Download the latest software image from the Aruba Customer Support website.



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 34.)

Install ArubaOS 5.0.3.3 on the WebUI

The following steps describe how to 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. Upload the new software image to a PC or workstation on your network.
2. Log in to the WebUI from the PC or workstation.
3. Navigate to the **Maintenance > Controller > Image Management** page. Select the Upload Local File option, then click the **Browse** button to navigate to the image file on your PC or workstation.
4. Determine which memory partition will be used to hold the new software image. Best practices is to load the new image onto the backup partition. To see the current boot partition, navigate to the **Maintenance > Controller > Boot Parameters** page.
5. Select **Yes** for Reboot Controller After Upgrade.
6. Click **Upgrade**.
7. When the software image is uploaded to the controller, a popup appears. Click **OK** in the popup window. The boot process starts automatically within a few seconds (unless you cancel it).

8. When the boot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade, including country code. The Country field displays the country code configured on the controller.

Install ArubaOS 5.0.3.3 on the CLI

The following steps describe how to install the ArubaOS software image using the CLI on the controller. You need a FTP/TFTP server on the same network controller you are upgrading.

1. Upload the new software image to your FTP/TFTP server on your network.
2. Execute the ping command to verify the network connection from the target controller to the FTP/TFTP server:

```
(host) # ping <ftphost>
or
(host) # ping <tftphost>
```



A valid IP route must exist between the FTP/TFTP server and the controller. A placeholder file with the destination filename and proper write permissions must exist on the FTP/TFTP server prior to executing the **copy** command.

3. Determine which partition to load the new software image. Use the following command to check the partitions:

```
#show image version
-----
Partition           : 0:0 (/dev/hda1) **Default boot**
Software Version    : ArubaOS 3.3.1.23 (Digitally Signed - Production Build)
Build number        : 20219
Label               : 20219
Built on            : 2009-05-11 20:51:46 PST
-----
Partition           : 0:1 (/dev/hda2)
/dev/hda2: Image not present
```

Best practices is to load the new image onto the backup partition (the non-boot partition). In the above example, partition 0 is the boot partition. Partition 1 is empty (image not present) and can be used to load the new software.

4. Use the **copy** command to load the new image onto the controller:

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



When using the **copy** command to load a software image, the specified partition automatically becomes active (default boot partition) the next time the controller is rebooted. There is no need to manually select the partition.

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

```
(host) #show image version
-----
Partition           : 0:0 (/dev/hda1) **Default boot**
Software Version    : ArubaOS 4.3.0.0 (Digitally Signed - Production Build)
Build number        : 23623
Label               : 23623
Built on            : Wed Mar 10 09:11:59 PST 2009
-----
Partition           : 0:1 (/dev/hda2)
Software Version    : ArubaOS 5.0.0.0 (Digitally Signed - Production Build)
Build number        : 23711
Label               : 23711
Built on            : Wed Mar 24 09:11:59 PST 2010
```

6. Reboot the controller:

```
(host) # reload
```

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

```
(host) #show version
Aruba Operating System Software.
ArubaOS (MODEL: Aruba 3200-US), Version 5.0.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2010, Aruba Networks, Inc.
Compiled on 2010-04-25 at 15:18:56 PDT 5.0.0.0 (Digitally Signed - Production Build)
...
```

Upgrading from 3.3.x to 5.0

The following steps describe how to 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 FTP/TFTP server using the same WebUI page.

Upgrading on the WebUI

1. Upload the new software image to a PC or workstation on your network.
2. Log in to the WebUI from the PC or workstation.
3. Navigate to the **Maintenance > Controller > Image Management** page. Select the Upload Local File option, then click the **Browse** button to navigate to the image file on your PC or workstation.
4. Determine which memory partition will be used to hold the new software image. Best practices is to load the new image into the backup partition. To view the current boot partition, navigate to the **Maintenance > Controller > Boot Parameters** page.
5. Select **Yes** for Reboot Controller After Upgrade.
6. Click **Upgrade**.
7. When the software image is uploaded to the controller, a popup appears. Click **OK** in the popup window. The boot process starts automatically within a few seconds (unless you cancel it).
8. When the boot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade, including country code. The Country field displays the country code configured on the controller.

Upgrading on the CLI

The following steps describe how to install the ArubaOS software image using the CLI on the controller. You need a FTP/TFTP server on the same network controller you are upgrading.

1. Upload the new software image to your FTP/TFTP server on your network.
2. Execute the ping command to verify the network connection from the target controller to the FTP/TFTP server:

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

or

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



A valid IP route must exist between the FTP/TFTP server and the controller. A placeholder file with the destination filename and proper write permissions must exist on the FTP/TFTP server prior to executing the **copy** command.

3. Determine which partition to load the new software image. Best practices are to load the new image onto the backup partition (the non-boot partition). In the above example, partition 0 is the boot partition. Partition 1 is empty (image not present) and can be used to load the new software.

4. Use the **copy** command to load the new image onto the controller:

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



When using the **copy** command to load a software image, the specified partition automatically becomes active (default boot partition) the next time the controller is rebooted. There is no need to manually select the partition.

5. Verify that the new image is loaded:

```
(host) # show image version
```

6. Reboot the controller:

```
(host) # reload
```

7. When the boot process is complete, use the **show version** command to verify the upgrade.

Upgrading from 2.5.x to 3.3.x to 5.0.

Upgrading from ArubaOS 2.5.x to ArubaOS 5.0 requires an “upgrade hop”. That is, you must upgrade from ArubaOS 2.5.x to ArubaOS 3.3.x first and then from ArubaOS 3.3.x to ArubaOS 5.0.



Once you have completed the upgrade to the latest version of 3.3.x, then follow the steps in “[Upgrading from 3.3.x to 5.0](#)” on page 32 to complete your last “upgrade hop”.

To assist you with this migration, Aruba Networks, Inc. provides comprehensive web site with migration tools listed below.

<https://support.arubanetworks.com/MIGRATIONTOOL/tabid/85/Default.aspx>

The tools include:

- Migration Design Guide

<https://support.arubanetworks.com/UPGRADEGUIDE/tabid/88/Default.aspx>

- Video

<https://support.arubanetworks.com/UPGRADETUTORIAL/tabid/87/Default.aspx>

- Online Migration Tool

<https://support.arubanetworks.com/25to3xTool/tabid/84/Default.aspx>

Upgrading from RN-3.x.x to 5.0

If you are upgrading from a release older than RN-3.1.4, you must upgrade to the most recent RN build that is available on the support site. Once your RN release is current, you can upgrade to ArubaOS 5.0.



Once you have completed the upgrade to the latest version of RN-3.x.x, then follow the steps in “[Upgrading from 3.3.x to 5.0](#)” on page 32 to complete your last “upgrade hop”.

Caveat

Should you need to downgrade from ArubaOS 5.0., you can only downgrade to version RN-3.1.4.

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 27.



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 5.0:

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.

Pre-shared Key for Inter-Controller Communication

A pre-shared key (PSK) is used to create IPSec tunnels between a master and backup master controllers and between master and local controllers. These inter-controller IPSec tunnels carry management traffic such as mobility, configuration, and master-local information.



An inter-controller IPSec tunnel can be used to route data between networks attached to the controllers. To route traffic, configure a static route on each controller specifying the destination network and the name of the IPSec tunnel.

There is a default PSK to allow inter-controller communications, however, for security you need to configure a unique PSK for each controller pair. You can use either the WebUI or CLI to configure a 6-64 character PSK on master and local controllers.



Do not use the default global PSK on a master or standalone controller. If you have a multi-controller network then configure the local controllers to match the new IPSec PSK key on the master controller. Leaving the PSK set to the default value exposes the IPSec channel to serious risk, therefore you should always configure a unique PSK for each controller pair.

Downgrading after an Upgrade

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



If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. Any new entries that were created in ArubaOS 5.0.3.3 will be lost after downgrade (this warning does not apply to upgrades from 3.4.x to 5.0),

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

1. Verify that Disable Control Plane Security (CPSec) is disabled.
2. Set the controller to boot with the previously-saved pre-upgrade configuration file.



3. Set the controller to boot from the system partition that contains the pre-upgrade image file.

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 that will be used on the next controller reload. An error message displays if a system boot parameters are set for incompatible image and configuration files.

After downgrading the software on the controller:

- Restore your configuration from your pre-upgrade configuration back up stored on your flash file. Do not restore the flash file system from a ArubaOS 5.0.3.3 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 5.0.3.3, the changes will not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 5.0.3.3, you need to reinstall the certificates in the downgraded ArubaOS version.

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

Be sure to back up your controller before reverting the OS.



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.

Downgrading on the WebUI

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 on the CLI

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.

In the following example, partition 0, the backup system partition, contains the backup release 3.4.1.23. Partition 1, the default boot partition, contains the ArubaOS 5.0.3.3 image:

```
#show image version
-----
Partition           : 0:0 (/dev/hda1)
Software Version    : ArubaOS 3.4.1.23 (Digitally Signed - Production Build)
Build number        : 20219
Label               : 20219
Built on            : 2009-12-11 20:51:46 PST
-----
Partition           : 0:1 (/dev/hda2) **Default boot**
Software Version    : ArubaOS 5.0.0.0 (Digitally Signed - Production Build)
Build number        : 23711
Label               : 23711
Built on            : 2010-03-25 01:59:13 PDT
```



You cannot load a new image into the active system partition (the default boot).

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
```

Controller Migration

This section outlines the steps involved in migrating from an Aruba PPC controller environment to MIPS controller environment. These steps takes into consideration the common Aruba WLAN controller environment. You must have an operational PPC controller in the environment when migrating to a new controller. The controllers are classified as:

- MIPS Controllers—M3, Aruba 3000 Series, 600 Series
- PPC Controllers—Aruba 200, Aruba 800, Aruba 2400, 5000 and SC1/SC2



Use this procedure to upgrade from one Aruba controller model to another. Take care to ensure that the new controller has equal or greater capacity than the controller you are replacing.

Migration instructions include:

- [“Single Controller Environment” on page 37](#)
- [“Multiple Master Controller Environment” on page 37](#)
- [“Master/Local Controller Environment” on page 37](#)

Single Controller Environment

A single controller environment is one active controller, or one master controller that may have standby master controller that backs up the master controller.

- Replacing the standby controller—Does not require downtime
- Replacing the master controller—Requires downtime

Multiple Master Controller Environment

An all master environment is considered an extension of the single master controller. You can back up the master controllers with a standby controller. In an all master controller deployment, each master controller is migrated as if it were in a standalone single controller environment.

For every master-standby controller pair

- Replacing the standby controller—Does not require downtime
- Replacing the master controller—Requires downtime

Master/Local Controller Environment

In a master/local environment, replace the master controller first and then replace the local controllers.

- Replacing the local standbys (when present)
- Replacing local controllers—one controller at a time

Before You Start

You must have:

- Administrative access to the controller via the network
- Administrative access to the controller via the controller’s serial port
- Pre-configured FTP/TFTP server that can be reached from the controller
- Aruba serial cable
- The ArubaOS version (same as the rest of the network)

Basic Migration Steps

1. Upgrade your network to the newer image to ensure that the image on the newer controllers match the image on the rest of the controllers in your network.
2. Backup the controller data from the PPC controller.
3. Physically swap the hardware (for example, mounting, cabling, power).
4. Initialize the new controller.
5. Install the backed up data onto the new controller.
6. Test the new setup.

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 controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
3. 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 from the controller.
4. 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.
 - a brand new installation.
5. 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.
6. 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.
8. If the problem is reproducible, list the exact steps taken to recreate the problem.
9. Provide any wired or wireless sniffer traces taken during the time of the problem.
10. 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.
11. Provide the controller site access information, if possible.