ArubaOS 6.0

Release Note

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Contents

Chapter 1 Release Overview 5

Chapter Overview 5
Supported Browsers 5
Release Mapping 5
Contacting Support 6

Chapter 2 What's New in this Release 7

Control Plane Security Enabled by Default 7
WIP (Wireless Intrusion Prevention) 7
    WIP Licensing Exceptions 8
Spectrum Analysis 8
OSPF 8
PVST+ 9
Remote Node Controllers 9
Band Steering 9
    Steering Modes 10
Guest Provisioning 10
    Importing Bulk Guest Entries 10
    Email Confirmation in Guest Provisioning 10
TACACS+ Enhancements 10
Multiple Wired Uplink Enhancements 11
Multicast Optimization 11
"Enable" Mode Bypass 11
Extended Authentication Using XML API 11
Content Security Services for VIA 11
Broadcast and Multicast Optimization 11
Wi-Fi Edge Detection and Handover for Voice Clients 11
IPv6 Enhancements 12
Enhanced 911 Support 12
Real Time Call Quality Analysis 12
SIP Session Timer 12
Voice and Video Traffic Awareness for Encrypted Signaling Protocols 12
Advanced Voice Troubleshooting 12
Single Heartbeat Per AP 13
Incremental Configuration Synchronization 13
Description for Home Agent Table Entry 13
PhoneHome Automatic Reporting 13
Exception List for Broadcast/Multicast Traffic 13
Manual Blacklisting 13
Show Switches Command Enhancements 14
Define a RADIUS Server using an FQDN 14
Campus AP Wired Port Bridging 14

Tagged VLANs Can Be Used As AP Uplink VLANs 14
Per-Vlan Wired AAA Profiles 14
Multimode Wired Authentication 14
Sample Configuration 14
User Derivation Rules Description Parameter 15
New MIBs and Traps 15

Chapter 3 Fixed Issues 17

Chapter 4 Known Issues and Limitations 21

Chapter 5 Upgrade Procedures 25

Important Points to Remember 25
Technical Upgrading Best Practices 26
WIP Configuration Upgrade 26
WIP Predefined Profiles 27
WIP Configuration Knobs 27
Basic Upgrade Sequence 27
Managing Flash Memory 28
Before you upgrade 28
Backing up Critical Data 28
Backup and Restore Compact Flash on the WebUI 28
Backup and Restore Compact Flash on the CLI 29
Licensing Change History and Mapping 29
Upgrading from 3.4.x to 6.0 31
Caveats 31
Load New Licenses 31
Save your Configuration 31
Install ArubaOS 6.0 32
Upgrading from 3.3.x to 6.0 33
Upgrading on the WebUI 33
Upgrading on the CLI 34
Upgrading from 2.5.x to 3.3.x to 6.0. 34
Upgrading from RN-3.x.x to 6.0 35
Caveat 35
Upgrading in a Multi-Controller Network 35
Pre-shared Key for Inter-Controller Communication 35
Downgrading after an Upgrade 36
Controller Migration 38
Single Controller Environment 38
Multiple Master Controller Environment 38
Master/Local Controller Environment 38
Before You Start 39
Basic Migration Steps 39
Before You Call Technical Support 39

Chapter 1

Release Overview

ArubaOS 6.0 is a major software release that introduces new features and fixes to many previously outstanding issues. For details on all of the features described in the following sections, see the *ArubaOS 6.0 User Guide*, *ArubaOS 6.0 CLI Reference Guide*, and *ArubaOS 6.0 MIB Reference Guide*.

NOTE

See the "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 17 describes the issues that have been fixed in this release.
- Chapter 4, "Known Issues and Limitations" on page 21 provides descriptions and workarounds for outstanding issues in ArubaOS 6.0.
- Chapter 5, "Upgrade Procedures" on page 25 cover the procedures for upgrading your controller from any release of ArubaOS to ArubaOS 6.0.

Supported Browsers

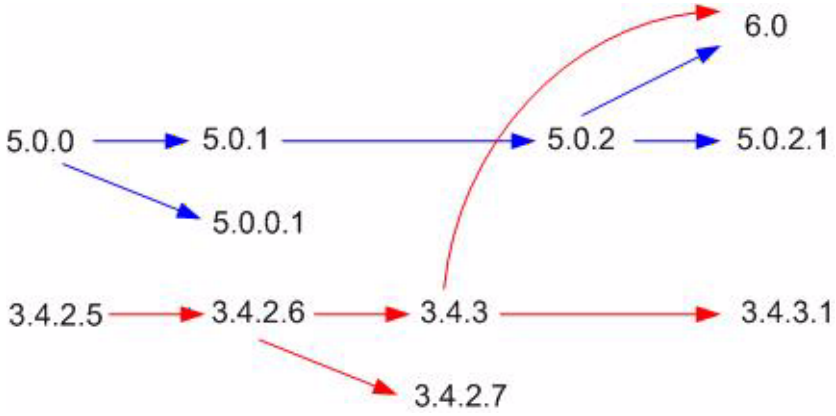
Beginning with ArubaOS 6.0, the following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer on
- Mozilla Firefox on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari on MacOS

Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 6.0.

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

Chapter 2

What's New in this Release

This chapter provides a brief summary of the new features included in this release of ArubaOS. For more information about each feature, refer to the *ArubaOS 6.0 User Guide* or *Command Line Reference*.

Control Plane Security Enabled by Default

When you initially deploy a controller running ArubaOS 6.0 or later, you create your initial control plane security configuration using the setup wizard. This wizard enables control plane security by default unless you specifically choose to disable this feature.

Controllers using control plane security only send certificates to APs that you have identified as valid APs on the network. If you want closer control over each AP that gets certified, you can do one of two things:

- Manually add individual campus APs to the secure network by adding each AP's information to the campus AP whitelist when you first run the initial setup wizard.
- Configure automatic certificate provisioning (in the initial setup wizard) to send certificates from the controller to each campus AP, or to all campus APs within a specific range of IP addresses. Do this if you are confident that all campus APs currently on your network are valid APs.

The default automatic certificate provisioning setting requires that you manually enter each AP's information into the campus AP whitelist. If you change the default automatic certificate provisioning values to let the controller send certificates to all APs on the network, that setting ensures that all valid APs will receive a certificate. That setting also increases the chance that a rogue or unwanted AP will be certified.

If you configure the controller to send certificates to only those APs within a range of IP addresses, there is a smaller chance that a rogue AP will get a certificate. However, any valid AP with an IP address outside the specified address range will not be given a certificate and will not be able to communicate with the controller (except to obtain a certificate). Consider both options carefully before you complete the control plane security portion of the initial setup wizard. If your controller has a publicly accessible interface, you should identify the campus APs on the network by IP address range. This prevents the controller from sending certificates to external or rogue campus APs that may attempt to access your controller through that publicly accessible interface.

If your APs do not come up after enabling control plane security, the APs may not have been validated by the controller. Refer to the Control Plane Security chapter of the ArubaOS 6.0 User Guide for troubleshooting tips.

WIP (Wireless Intrusion Prevention)

The ArubaOS WIP features and configurations offer a wide selection of intrusion detection and protection features that protect the network against wireless threats. Like most other security-related features of the Aruba network, WIP configuration is done on the master controller in the network.

To use most WIP features, you must install a Wireless Intrusion Prevention (RFprotect) license on all controllers in your network. If you install an RFprotect license on a master controller only, an AP or AM terminated on a local controller will not provide the WIP features. WIP features include:

- Reusable Wizard (**Wizards ->Configure WIP**)
- Monitoring Dashboard (**Monitoring -> Security Summary**)

- Rogue AP Detection
- Intrusion Detection
- Intrusion Protection
- WLAN Management System
- Client Blacklisting

WIP Licensing Exceptions

These features do not require an RFprotect license:

- Rogue AP classification techniques other than AP classification rules
- Rogue containment
- Wired containment
- Wireless containment without Tarpit


NOTE

The RFprotect license was formerly named the WIP license. For important upgrade license information, refer to Chapter 5, “Upgrade Procedures” .

Spectrum Analysis

The Spectrum Analysis software modules on AP models AP-105, the AP-120 Series and the AP-90 Series are able to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources. Each spectrum monitor, or SM, will scan and analyze the spectrum band used by the SM's radio (2.4Ghz or 5Ghz). The spectrum analysis feature also allows you to record spectrum monitor data over a defined time period, save that data, and then play it back for later analysis. An analysis of the results can then be used to quickly isolate issues with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel.

A spectrum analysis client can simultaneously access data from up to four individual spectrum monitor radios. Each spectrum monitor radio, however, can only be connected to a single client WebUI, and a controller can support up to 22 connections between a spectrum analysis client and a spectrum monitor. Individual campus APs or groups of campus APs can be converted to dedicated spectrum monitors via the dot11a and dot11g radio profiles of that AP or AP group, or through a special spectrum override profile. The spectrum analysis feature requires the RF Protect license. APs cannot be converted to spectrum monitors without this license installed on the controller.

For details on this feature, refer to http://www.arubanetworks.com/products/spectrum-analyzer.php

OSPF

OSPFv2 (Open Shortest Path First) is a dynamic Interior Gateway routing Protocol (IGP) based on IETF RFC 2328. The premise of OSPF is that the shortest or fastest routing path is used. Aruba’s implementation of OSPFv2 allows Aruba controllers to deploy effectively in a Layer 3 topology. New in this version is:

- All area types are supported
- Multiple configured areas are supported
- An Aruba controller can act as ABR (Area border router)

PVST+

PVST+ (Per-VLAN Spanning Tree plus) protocol allows for load balancing of VLANs across multiple ports resulting in optimal network resource usage. Inclusion of PVST+ ensures controller interoperability with other standard spanning tree protocols.

Remote Node Controllers

The Remote Node Controllers feature is Beta-quality only for this release. Please note the following limitations regarding this feature:
- Custom captive portal pages and certificates cannot be synced centrally.
- CPSec is not supported in remote node controller deployments.
- VRRP redundancy across remote nodes is not supported

A remote node, or RN, is an easy-to-provision controller that can get its local and global configuration and license limits from a central controller called a remote node manager. You define configuration settings for each remote node via an remote-node profile on the remote node manager, which can be either a local controller or a master controller.

Each remote-node configuration profile defines values for VLANs, VLAN interfaces, GRE tunnels, and management users for one or more RNs. Each profile can also include values for RN DHCP pools, which define the VLAN and the range of IP addresses be allocated for each RN. IP addresses in an RN configuration profile can also be defined dynamically, meaning that IP addresses in the remote-node profile do not need to be predefined, and can be automatically derived when each RN is provisioned. After the RN is provisioned and active on the network, management users can edit the RN's configuration via the RN configuration profile on the remote master.

If the remote node fails to setup IPSec connection to remote node manager after it has been initially provisioned, a debug management user will be activated, which can be used to login to the remote node to debug connectivity failure. This account will only be available if the Remote node config sync to remote node master has not happened. The debug management console can be accessed using remotenodesupport as the username and Base MAC address of the remote node (in all CAPS) as the password.

Only M3, 3000 Series and 600 Series series controllers can be configured as remote nodes.

Band Steering

ARM's band steering feature encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4GHz band for single band clients like VoIP phones.

Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5GHz band than on the 2.4GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40MHz or 20MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.

The band steering feature supports both campus APs and remote APs that have a virtual AP profile set to tunnel, split-tunnel or bridge forwarding mode. Note, however, that if a campus or remote AP has virtual AP profiles configured in bridge or split-tunnel forwarding mode *but no virtual AP in tunnel mode*, those APs

will gather information about 5G-capable clients independently and will not exchange this information with other APs that also have bridge or split-tunnel virtual APs only.


NOTE

The Band Steering feature may not work correctly unless you enable the "Local Probe Response" parameter in the Wireless LAN SSID profile for the SSID that requires band steering. You can enable the local probe response parameter using the CLI command **wlan ssid-profile <profile> local-probe-response**, or via the WebUI by navigating to **Configuration>All Profiles**, expanding the **Wireless LAN** and **SSID Profile** menus, then selecting the **SSID profile** and checking the **Local Probe Response** checkbox in the **SSID Profile Details** window.

Steering Modes

Band steering supports the following three different band steering modes.

- **Force-5GHz**: When the AP is configured in **force-5GHz** band steering mode, the AP will not respond to 2.4 Ghz probe requests from a client if all the following conditions are met:
  - The client has already probed the AP on the 5Ghz band and therefore is known to be capable of sending probes on the 5Ghz band.
  - The client is not currently associated on the 2.4Ghz radio of this AP
- **Prefer-5GHz** (Default): If you configure the AP to use **prefer-5GHz** band steering mode, the AP will not respond to 2.4 Ghz probe requests from a client if all the following conditions are met:
  - The client has already probed the AP on the 5Ghz band and therefore is known to be capable of sending probes on the 5Ghz band.
  - The client is not currently associated on the 2.4Ghz radio to this AP.
  - The client has sent less than 8 probes requests/auth in the last 10 seconds
- **Balance-bands**: In this band steering mode, the AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has more channels than the 2.4 Ghz band, and that the 5Ghz channels operate in 40MHz while the 2.4Ghz band operates in 20MHz.


NOTE

The band steering feature in ArubaOS versions 5.0 does not support multiple bandsteering modes. The band-steering feature in these versions of ArubaOS functions the same way as the default **prefer-5GHz** steering mode available in ArubaOS 6.0 and later.

Guest Provisioning

Importing Bulk Guest Entries

The Guest Provisioning user can now import multiple guest entries into the database from a CSV file. In previous releases, guest entries had to be entered manually one by one. This is useful and more efficient if you want to enter multiple guest entries at once.

Email Confirmation in Guest Provisioning

The Guest Provisioning user can send out Email from the Guest Provisioning Page to either the guest or the sponsor. When an email is sent from the Details pop-up window, a pop-up message confirming that the email was successfully sent displays.

TACACS+ Enhancements

TACACS+ now supports an optional authorization session for admin users.

Multiple Wired Uplink Enhancements

This feature lets Aruba controllers support multiple wired uplink interfaces. You can assign up to four VLAN interfaces, in the WebUI or CLI, to operate in active-standby topology. An active-standby topology provides redundancy so that when an active interface fails, the user traffic can failover to the standby interface. When you enable the DHCP or PPoE client on the controller for a VLAN, the controller can obtain a dynamic IP address for a VLAN.

Multicast Optimization

A new parameter (shape-mcast) was added to the **firewall** CLI command. This parameter enables multicast optimization which provides excellent streaming quality regardless of the number of VLANs or IP IGMP groups that are used.

"Enable" Mode Bypass

The bypass enable feature lets you bypass the enable mode prompt and go directly to the privileged commands (config mode) after logging into the controller. This is useful if you want to avoid having to change the enable password for your company policy.

Extended Authentication Using XML API

You can now use ArubaOS XML API interface to perform extended or customized authentication on users or clients connecting to the network. This interface provides a seamless and transparent mechanism to authenticate users. You can now add, delete, authenticate, query, and blacklist a client.

See the Extended Authentication Using ArubaOS XML API chapter in the ArubaOS User Guide.

Content Security Services for VIA

You can now enable and configure the content security services to verify traffic to external (non-corporate) resources from a VIA connection. The content security services should be enabled and configured in the VIA connection profile. You can configure CSS using the WebUI and the CLI.


NOTE

VIA is supported only on the M3, 3000 and 600 Series series controllers.

Broadcast and Multicast Optimization

You can now effectively prevent flooding of BCMC traffic on all VLAN member ports using the **`bcmc-optimization`** parameter under the `interface vlan` command. This parameter ensures controlled flooding without compromising client connectivity. By default this option is disabled. You must enable this parameter for the controlled flooding of BCMC traffic.

Wi-Fi Edge Detection and Handover for Voice Clients

Voice clients in an Aruba infrastructure can be switched to cellular network when the infrastructure determines that the clients might leave the active Wi-Fi coverage area or roam to an area with poor Wi-Fi coverage. The infrastructure monitors the *Beacon Reports* received from the clients to determine the roaming pattern. If the roaming pattern suggests that the client is moving away from the active coverage area (based on the RSSI threshold value), the infrastructure initiates the handover process.

You can use the `handover-trigger` command to enable this feature and the `handover-threshold` command to configure the RSSI threshold level for initiating the handover process. These commands are available in the `wlan dot11k-profile`.

IPv6 Enhancements

This release of ArubaOS introduces significant changes to IPv6 users:

- IPv4 and IPv6 details of a client or user is now available in a single user table.
- You can now use the IPv4 configuration commands with the `ipv6` keyword to issue IPv6 specific commands.
- IPv6 users can now inherit IPv4 roles.
- You must now enable IPv6 and IPv6 firewall before using any of the IPv6 features.

Enhanced 911 Support

This release of ArubaOS provides seamless support for emergency calls in an Aruba network by interoperating with the RedSky emergency call server. The controller interoperates with the RedSky call handling system by registering the call server as an SNMP host on the controller. The controller tracks the location of the voice clients and notifies the emergency call server using SNMP traps. The notification process ensures that the emergency call server is notified whenever a voice client is identified or the location of the client is updated.

Real Time Call Quality Analysis

You can now view the voice call quality parameters such as jitter, delay, packet loss, and call quality score (R-value) computed directly from the RTP media stream. Additionally, the controller saves the periodic samples of the quality parameters for detailed analysis of the results. You can enable this feature using the `voice real-time-config` command and view the analysis reports using the `show voice real-time-analysis` command.

SIP Session Timer

This release of ArubaOS introduces SIP session timer in the SIP ALG. This support defines a keepalive mechanism for the SIP sessions using the periodic session refresh requests from the user agents. The session timer configuration options are added to the `voice sip` command.

- `session-timer` —Used to enable the session-timer on the SIP ALG
- `session-expiry` —Used to set the timeout value of the session timer.

Voice and Video Traffic Awareness for Encrypted Signaling Protocols

You can now enable the controller to identify the voice or video sessions established using a secure signaling protocol by deep inspection of the traffic. The controller can now provide QoS for the voice or video sessions established even over the secure layers such as TLS or IP Sec.

Advanced Voice Troubleshooting

ArubaOS enables you to debug voice issues more efficiently and quickly by providing detailed information about the voice calls, voice client status, and Call Detail Records (CDR). You can now easily obtain the

advanced troubleshooting information such as time of failure of the call, status of the client during the call failure, signal strength of the call, AP handoff information, and signaling message issues using the following commands:

- `show voice client-status ip <ip address>` —Used to view the details of a voice client based on the client's IP address.
- `show voice call-cdr cid <CDR Id>` —Used to view the details of a call based on the CDR Id.
- `voice logging` —Used to enable voice logging on a specific client.
- `show voice trace` —Used to view the detailed voice trace information.
- `show voice configurations` —Used to view the voice related configurations on the controller.

Single Heartbeat Per AP

Now, a single heartbeat per AP is sent and received by the AP regardless of the number of virtual APs or wired APs on the APs. Using this new heartbeat mechanism the control plane traffic load on the controller is signifcantly reduced.

Incremental Configuration Synchronization

You can now send the incremental updates to the local during master and local configuration synchronization.You can use the **cfgm set sync-type <snapshot>** command to enable incremental configuration synchronization.

Description for Home Agent Table Entry

You can now add a description for a HAT entry. This description can be a maximum of 30 characters (including spaces).

PhoneHome Automatic Reporting

The automatic reporting feature, also known as PhoneHome, allows a controller to securely contact Aruba support servers over the Internet to report events such as hardware failures, software malfunctions, and other critical events. When the PhoneHome automatic reporting feature is enabled, the controller sends Aruba support weekly reports about the controller's configuration, licenses, software and hardware versions, and any software malfunctions via a secure email. Aruba processes these reports and sends any necessary warnings or updates back to you in an email message so that you can take any necessary actions.

In the event that you need to contact Aruba support with a question about your controller, you can use this feature to generate and immediately send a status report, so that Aruba support can diagnose the issue with the most current controller data.

Exception List for Broadcast/Multicast Traffic

Bandwidth contracts on a VLAN can limit broadcast and multicast traffic. ArubaOS version 6.0 and later includes an internal exception list to allow broadcast and multicast traffic using the VRRP, LACP, OSPF, PVST and STP protocols. To remove per-vlan bandwidth contract limits on an additional broadcast or multicast protocol, add the MAC address for that broadcast/multicast protocol to the Vlan Bandwidth Contracts MAC Exception List. This feature supports up to 64 MAC address entries.

Manual Blacklisting

Starting with ArubaOS 6.0, you have the option to manually clear all entries in the client blacklist, rather than removing each entry individually.

Show Switches Command Enhancements

The output of the **show switches** command now displays the build number for ArubaOS version 6.0 or later.

Define a RADIUS Server using an FQDN

You can now define a RADIUS server using either the servers IP address, or the server's Fully Qualified Domain Name (FQDN). This feature also allows you to configure how often the controller should generate a DNS request to cache the IP address for a RADIUS server identified via its FQDN.

Campus AP Wired Port Bridging

The wired port profile of a campus AP can be configured in bridge forwarding mode. In previous releases of ArubaOS, this feature was available for remote APs only.

Tagged VLANs Can Be Used As AP Uplink VLANs

The provisioning profile of a remote AP or campus AP can define an uplink VLAN for that AP. If you configure an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature. Note that if an AP is provisioned with an uplink VLAN, it must be connected to a trunk mode port or the AP's frames will be dropped.

Per-Vlan Wired AAA Profiles

ArubaOS 6.0 allows you to assign an AAA profile to a VLAN to enable role-based access for wired clients connected to an untrusted VLAN or port on the controller. This parameter applies to wired clients only. Note that this profile will only take effect if the VLAN and/or the port on the controller is untrusted. If both the port and the VLAN are trusted, no AAA profile is assigned.

Multimode Wired Authentication

This feature allows the user (Guest User or Employee User) to be able to plug into any port in an Aruba Controller and be placed in the right vlan and right role based on the authentication scheme used.

User (Employee or Guest) initially obtains a short lease from controller acting as DHCP server. When the user (Guest) does captive portal authentication, user falls into guest role (captive portal authenticated role) and obtains a new lease configured as multimode-auth-lease. If user (an Employee) does dot1x authentication, he is moved to different vlan and is assigned dot1x authenticated role.

For this feature to work, it is mandatory that controller is configured as DHCP server with short lease for initial vlan for wired users.

Multimode auth lease con be configure on per vlan basis. The new cli introduced to configure the same is `multimode-auth lease-time <lease time>`

Sample Configuration

```
(Aruba3600) #configure t
Enter Configuration commands, one per line. End with CNTL/Z
(Aruba3600) (config) #interface vlan 6
(Aruba3600) (config-subif)#multimode-auth lease-time ?
<value>                 lease time in minutes <5 - 3600>
```

User Derivation Rules Description Parameter

A new option in the `aaa derivation-rules user` CLI command allows you to add a description of a user-derivation rule. This lets the users know why a specific rule was added.

New MIBs and Traps

- New and replacement WLSX trap objects and WLSX trap definitions have been added. Several traps have been deprecated and replaced with equivalent traps.
- New 802.11 MIB counters were added to the WlanAPChStatsEntry in the WLSX-WLAN-MIB.adm
- A new object, “wlanAPSysLocation” has been added to the aruba-wlan.my MIB file

Table 1 *Fixed Issues for ArubaOS 6.0*

Bug ID	Descriptions
22560	Air monitors (AMs) and APs now correctly propagate their wired-MAC table to neighboring APs.
25265	The validuser ACL now accepts IPv6 rules.
27201	A validation check has been added to the WebUI for summer time zones. If the time offset is not provided, an error message is displayed in the alert dialog.
27674	A issue that resulted in a CPU spike when a netdestination is added to the configuration has been fixed.
30536	Support for interface ipv6 access-group has been added; so now users need to explicitly permit ipv6 traffic by defining a rule otherwise an implicit "deny all" will be a hit.
30554	New IPv6 user no longer triggers the authmgr to clean up any IPv4 users of the same client MAC when `aaa user fast-age` is enabled.
30558	User roles and association correctly changes when IPv6 users move from virtual AP (VAP) to VAP.
30684	Clients are now assigned an IP and the the correct role when the IPv6 firewall is enabled.
31745	The syslog now displays the username, user MAC address, and user IP address on a single line.
34716	The CLI command `show user_session_count` has been deprecated.
34745	If a controller uses a TACACS server for management authentication, the debug log messages do not erroneously display failed or successful management logins for RADIUS servers.
35208	The Firefox browser no longer displays SSL errors when loading the captive portal feature.
35305	SIP packets are no longer prevented from reaching the application-level gateway (ALG) when the **disable scanning** option is enabled for SIP access-control lists.
35361	Users can no longer add new firewall rules to an access control list when that list has reached its maximum number of access control entries.
35549	The output of the CLI command `show audit trail` shows data for user login sessions initiated using the WebUI.
35596	VLAN derivation rules for user vlan assignments properly support string attributes.
36099	The controller no longer erroneously uses a multicast Source MAC address during part of the EAP authentication process.
36140	The controller no longer stops responding or reboots due to memory issues.
36560	SAPM will not try to generate a config message for an AP that has been marked for full reconfiguration. Until ArubaOS ready to do the configuration, the AP's config may be in an inconsistent state.

Table 1 *Fixed Issues for ArubaOS 6.0*

Bug ID	Descriptions
36590	The datapath command no longer assumes the “established” option when the “mirror” flag is set for an ACL rule.
36707	When the system time is changed, the timestamp in logs also change. If any system time change involves a time zone, the change takes effect after the AP reboots.
36821	MIPT-C can now make a call immediately after MIPT-A releases the call.
36848	The client is now able to pass traffic on an encrypted ssid.
36935	For Voice CAC, call status is no longer reset on client roam during active session with tspec-enforcement enabled.
37844	The controller no longer fails while it is being upgraded to the non-boot partition.
38185	When master-redundancy is used, 'masterip 0.0.0.0' no longer causes issues in configuration and has been fixed.
39108	The syslog message, “Unable to open system file /dev/max6640” does not appear for any specific clients on the system.
39405	Log messages have been fixed to correctly display speed information for 10G ports on the Aruba 6000 series controllers.
39700	Issues with poor roaming performance by OCS clients have been fixed.
39275	Useres are now prevented from adding new rules when system does not have enough aces to support the rule.
40235	APs that are up but have not downloaded configuration are now displayed with the `Dirty / No Config` flag.
40831	Issue with the controller crashing due to datapath exception have been fixed.
41243	After upgrading from 3.x.x.x to 6.0 guest provisioning users were unable to see the users created by them in the old version. This has now been fixed.
41469	You can now specify non-contiguous ports to create netservice in the WebUI.
41639	Issue with spectrum monitor frequently unsubscribing has been fixed.
41727	The issue with TCP connections not being closed after role change has been fixed.
41735	You can now specify a different filename while transferring a file from the controller using FTP.
41946	The **Guest Provisioning** page in the WebUI does not appear blank when navigated through the **Configuration - > Management** page.
42067	The issue with controller crashing while downloading configuration has been fixed.
42168	The issue with the WebUI not maintaining the status of the radio buttons for **Spanning Tree** has been fixed.
42261	The issue with the file transmission over poor links has been fixed.
42384	You can now delete an IPv6 user using the `aaa ipv6 user delete <user-name>` command.

Table 1 *Fixed Issues for ArubaOS 6.0*

Bug ID	Descriptions
42760	Wireless users can now authentication with **Request must contain the Message Authenticator attribute** enabled on the Microsoft IAS 2003 Radius server.
42771	The Tx and Rx databytes now support 64 bits on all platforms.
43051	The **Module Authentication is busy** error message while adding ACLs has been fixed.
43264	The WebUI will now accept only ASCII type characters in the username and password fields.
43341	When the external name server is not configured the controller does not act as a DNS proxy but responds with its own IP address to the queries.
42194, 42213, 42568	The device correlator now works correctly; new entries are no longer created for device that have already been detected.
42139	After Captive Portak authentication, wireless IPv6 users now change into their correct roles.
42820	ArubaOS now drops all Broadcast source dataframes, with broadcast/unicast DST/BSSIDs, since they can be used for Denial of Service (DoS) attacks.
43426	When adding an AP to Spectrum-Override profile, no spaces can be added to the end of the AP's name. If a space is added at the beginning or end of the name, the WebUI will show that it is an invalid AP name..
40521	APs in spectrum monitor mode now correctly detect interference from inverter microwaves.
41237	The WebUI will no longer time out and stop responding while a spectrum monitor is streaming the data to a spectrum analysis client.
43306	The **Monitoring > Network > Security Summary** tab now correctly displays the scroll bars when viewed using Internet Explorer 7.
42810	APs in spectrum monitor mode now correctly detect interference from standard microwave ovens.
42602	The output of the `show ap debug radio-stats` command may incorrectly show an increasing number of failed beacons even though there is no such traffic.
40889, 41804	The Intrusion Detection section of the WIP wizard now correctly displays pop-up warnings.
43224	When a user selects a specific file size to be recorded, the recording will stop and saved file will be the selected size.
43386	The issue with the monitoring page not showing the correct information under Guest WLAN has been fixed.
43584	The issue with full name of the guest not visible while creating a user with the guest provisioning access has been fixed.
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.
43706	The output of the `show ap tech-support` command now displays all the additional commands.
43741	The `Acct-Multi-Session-Id` identifier has been added in all the accounting start and stop messages.

Table 1 *Fixed Issues for ArubaOS 6.0*

Bug ID	Descriptions
43766	The issue with `calling-station-id` and `called-station-id` not sent while authenticating using Captive Portal and selecting MSCHAP option has been resolved.
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.
43938	The issue with the SSH server getting disconnected after three failed login attempts 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.

Chapter 4

Known Issues and Limitations

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

Table 1 *Known Issues for ArubaOS 6.0*

Bug ID	Descriptions
	Do not use the `mgmt-server type amp` command. This command is not supported in ArubaOS 6.0. If you execute this command, your controller will experience a memory leak in the STM process and the controller's performance will become sluggish, eventually causing it to reboot. **Workaround:** None.
41521	APs in spectrum monitor mode cannot detect the Jabra GN9120 2.4 GHz wireless headset. **Workaround:** None.
41522	APs in spectrum monitor mode cannot detect the Uniden DMX776 2.4 GHz DSS cordless phone. **Workaround:** None.
43440	The Spectrum UI does not work with Adobe Flash 10.1. **Workaround:** Downgrade Flash Player to 10.0.x. For details on downgrading to Adobe Flash 10, see the Spectrum Analysis chapter of this ArubaOS 6.0 User Guide.
38150	APs stop responding to clients after CPsec is enabled. **Workaround:** Reboot all APs after CPSec is enabled. The APs will begin repsonding to clients after the reboot.
43248	If you minimize and maximize the browser window while you create a spectrum analysis recording, that recording may show incorrect data when you play it back. **Workaround:** Do not change the browser window size while creating a spectrum analysis recording.
40577, 41836, 41456	When a guest-provisioning user is logged in to the WebUI, the logout link says Logout Admin instead of the username of the logged in guest-provisioning user. **Workaround:** None.
41092	In both the WebUI and the CLI, attempting to add a guest users whose name (full name, not username) contains a "%" will cause the fpcli (in the CLI) and arci-cli-helper (in the WebUI) to crash and display the following error message: `Error: Failed to read socket: Success`. **Workaround:** Do not create a guest guest whose full name contains a "%."
41898	Role derivation from UDR does not happen with a per-vlan-aa profile. **Workaround:** Associate a dummy aaa profile to `aaa authentication wired`, where the same UDR is referenced. Role derivation will happen correctly when this dummy aaa profile is referenced.

Table 1 *Known Issues for ArubaOS 6.0*

Bug ID	Descriptions
42832	Executing the command show ap database on a remote master does not show the APs terminating on that controller even if that device is a local controller. **Workaround:** None.
43920	From the WebUI, commands are executed twice when the AAA profile is modified from the **AP Group Page** on a remote AP (RAP). **Workaround:** The commands being executed twice is not harmful to your configuration. However, if you want to avoid this, the CLIs can be modified from the **All Profiles Page**.
43963	If you access the spectrum analysis dashboard using the Safari 5.0 browser, clicking the backspace button may return you to the previous browser screen. **Workaround:** None. Avoid using the backspace button when changing dashboard view names or chart options.
43945	The controller should not send EAP-request ID for multimode authenticated user when dhcp lease expires. **Workaround:** None.
43937	EAP request ID is not sent by the controller in response to eapol start from the client after executing the `aaa user delete all` command. **Workaround:** None.
44568	DHCP offer from a guest vlan should is incorrectly sent in response to DHCP discover for 802.1x users. **Workaround:** None.
44106	Any users with the a quotation mark (“) in their email address will not be successfully imported from a CSV file. **Workaround:** None. Do not import users with an email address containing a quotation mark.

44496	The New, Import, Delete, Print, and Edit buttons on the top right of the GPP page appear as hyperlinks instead of buttons.
	Workaround:
	To make the buttons appear normally, use the following style in your upload policy text.
	`a:link, span.MsoHyperlink`
	`{color:blue;`
	`text-decoration:none;}`

44499	GPP users are unable to to modify the Account End Time during policy text import if the following policy text is included:
	`p {mso-margin-top-alt:auto;`
	`margin-right:0in;`
	`mso-margin-bottom-alt:auto;`
	`margin-left:0in;`
	`mso-pagination:widow-orphan;`
	`font-size:12.0pt;`
	`font-family:"Times New Roman";`
	`mso-fareast-font-family:"Times New Roman";}`
	Workaround:
	Do not include the above policy text.

Table 1 *Known Issues for ArubaOS 6.0*

Bug ID	Descriptions
44645	Load balancing is not working consistently. Occasionally, the load balancing flag is not being set properly. **Workaround:** None
44758	Campus APs provisioned in PPPoE mode do not work. The PPPoE connection with the PPPoE server will break right after a successful connection is established. **Workaound:** None.
45033	A remote node controller master will not come up if the controller-ip is set as loopback. The controller becomes stuck at the “Update in progress” state and the error log shows that the remote-node-profile did not pass validation because “Vlan interface not configured for the controller-ip vlan.” And, therefore, the configuration is not pushed to the remote node. **Workaround:** None.
45092	In the remote-node-master (RNM), you need to specify the remote-node-localip for authenticating each of the remote-node on the IPSec connection. This is a different behavior than the case of master-local IPSec connection. **Workaround:** Aruba recommends putting 0.0.0.0 (which means any IP) in the RNM, where you might want to be very specific on the allowed IP lists.
45245	The Aruba 651 occasionally encounters a watchdog timeout when no traffic is passing through the device and the AP is configured as a mesh point. **Workaround:** None.
45351	The wlsxUserEntryAttributesChanged trap does not work for wired, open clients. **Workaround:** None.
45463	Changing the forwarding mode from bridge to split-tunnel and vice-versa on an existing virtual AP does not work. **Workaround:** To ensure that the forwading mode changes take effect, you must manually reboot the AP. This can be done through the CLI be executing one of the following commands: • `apboot ap-name <ap-name>` • `apboot ip-addr <ip-address>` • `apboot wired-mac <mac-address>`
45464	After a split user roams to RAP from another RAP, it is placed in the wired-ap bridge role rather than its previous actual split user role. Since the traffic is handled differently because of the changed role, the split user’s data sessions breaks after the roaming to new RAP. **Workaround:** None.
45465	Connecting RAPs through the secure jack ENET ports on RAP-5 has become a use-case as part of split user mobility. As these RAPs are the wired bridge users on the RAP-5, these are maintained in controller user table as well. But, these wired bridge user's status is not accurate or consistent on the controller. **Workaround:** Track these wired bridge user RAPs through `show datapath user ap-name RAP-5`.

Table 1 *Known Issues for ArubaOS 6.0*

Bug ID	Descriptions
45553, 45735	FTP sessions break when a split-user roams from one RAP to another RAP. After the client roams to the second RAP, the ftp datapath sessions become marked as local (inidcating local traffic) while, on the controller, these sessions remain marked as RAP1 (indicating the previous RAP's tunnel). Therefore, the FTP sessions does not continue when the client roams to the second RAP. **Workaround:** None.
45607	AAA user derivation rules are activating for visitor users on FA when the client re-associate on FA. Initially when the clients roam to FA, they get the correct role that redirects all traffic from the visitor to the HA. But when a client re-associates, it's role on FA gets updated to the one configured in the derivation rules. As a result the visitor traffic are no longer redirected to HA. **Workaround:** The only way to avoid this issue is to not use user derivation rules.

Chapter 5

Upgrade Procedures

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
- "Technical Upgrading Best Practices" on page 26
- "WIP Configuration Upgrade" on page 26
- "Basic Upgrade Sequence" on page 27
- "Managing Flash Memory" on page 28
- "Before you upgrade" on page 28
- "Licensing Change History and Mapping" on page 29
- "Upgrading from 3.4.x to 6.0" on page 31
- "Upgrading from 3.3.x to 6.0" on page 34
- "Upgrading from 2.5.x to 3.3.x to 6.0." on page 35
- "Upgrading from RN-3.x.x to 6.0" on page 35
- "Upgrading in a Multi-Controller Network" on page 35
- "Downgrading after an Upgrade" on page 36
- "Controller Migration" on page 38
- "Before You Call Technical Support" on page 39

All version 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, show image version,** or the **show switches** 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 then TFTP and also offers more resilience over slower links.

If you must use TFTP, ensure that your TFTP servers can send more then 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.

WIP Configuration Upgrade

New configuration parameters that are added in ArubaOS 6.0 do not require any special handling during upgrade; when you upgrade to ArubaOS 6.0, new parameters will automatically be added to their respective profiles and given their default value.

If the default value of an existing parameter changed in ArubaOS 6.0, profiles using the default value will automatically be changed to use the new default value. If your configuration uses a non-default value prior to upgrade, the value will not be modified during the upgrade process. The following default values were changed:

Detect AP Impersonation—changed from **True** to **False**

Detect Adhoc Network— changed from **True** to **False**

Detect Wireless Bridge—changed from **True** to **False**

Detect 40MHz Intol—changed from **True** to **False**

Detect Active Greenfield mode—changed from **True** to **False**

WIP Predefined Profiles

Except for predefined profiles IDS Rate Thresholds and IDS Signature, all IDS predefined profiles have been deprecated. Mapping the deprecated profiles are handled as follows:

- If a predefined profile is referenced by default from another profile, the reference will point to the new default instance of the profile

- If a predefined profile is referenced explicitly (that is, you changed from the default value so that it points to a predefined profile), after the upgrade the reference will point to a profile which is an editable clone of the predefined profile. That profile is named similarly to the predefined profile, except the word “transitional” is inserted after “ids-“

Wireless Containment Parameter

The wireless-containment parameter in the ids-general-profile went from an enabled/disabled knob to an enumeration (none, deauth-only, tarpit-non-valid-sta, tartip-all-sta).

- If the parameter was set to *enabled* (its default value), the upgrade will render the value as *deauth-only* (the new default value)
- If the parameter was set to *disabled*, the upgrade will render the value as *none*

Signature Matching profile Default Instance

The default instance of the signature matching profile in ArubaOS contain references to 2 predefined signatures: Deauth-Broadcast and Disassoc-Broadcast (a new signature in 6.0). The default instance of this profile was empty prior to 6.0.

- If the profile was empty, the upgrade will render the profile with both predefined signatures.
- If the profile was not empty, the upgrade will add references to the 2 predefined signatures, if they are not already there.

WIP Logging Changes

In ArubaOS 6.0, all WIP logs related to intrusion detection and protection are in the ‘security’ logging category. Previously, most WIP logs were generated under the Wireless Logging category. Many of the logs that were previously generated at the Error level have been moved to the Warning level. In the security logging category, two new subcategories are added:

- The ‘ids’ subcategory contains ‘correlated’ WIP logs.
- The ‘ids-ap’ subcategory contains WIP logs generated by the APs (uncorrelated).

Both of these new WIP logging subcategories: ‘ids’ and ‘ids-ap’ are enabled at the Warning level by the upgrade. However, by default, AP logging of WIP events is disabled and correlation of WIP logs is enabled.

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 expected.
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 or VisualRF 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 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. 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 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. 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
   ```

Licensing Change History and Mapping

License consolidation and even renaming of licenses occur over time. The following changes and/or consolidations were made to the ArubaOS licensing.

ArubaOS 6.0

- WIP license is changed to RFprotect and includes the WIP and Spectrum Analysis features.

ArubaOS 5.0

Figure 1 is an up-to-date illustration of the consolidated licenses effective with this release.

- 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

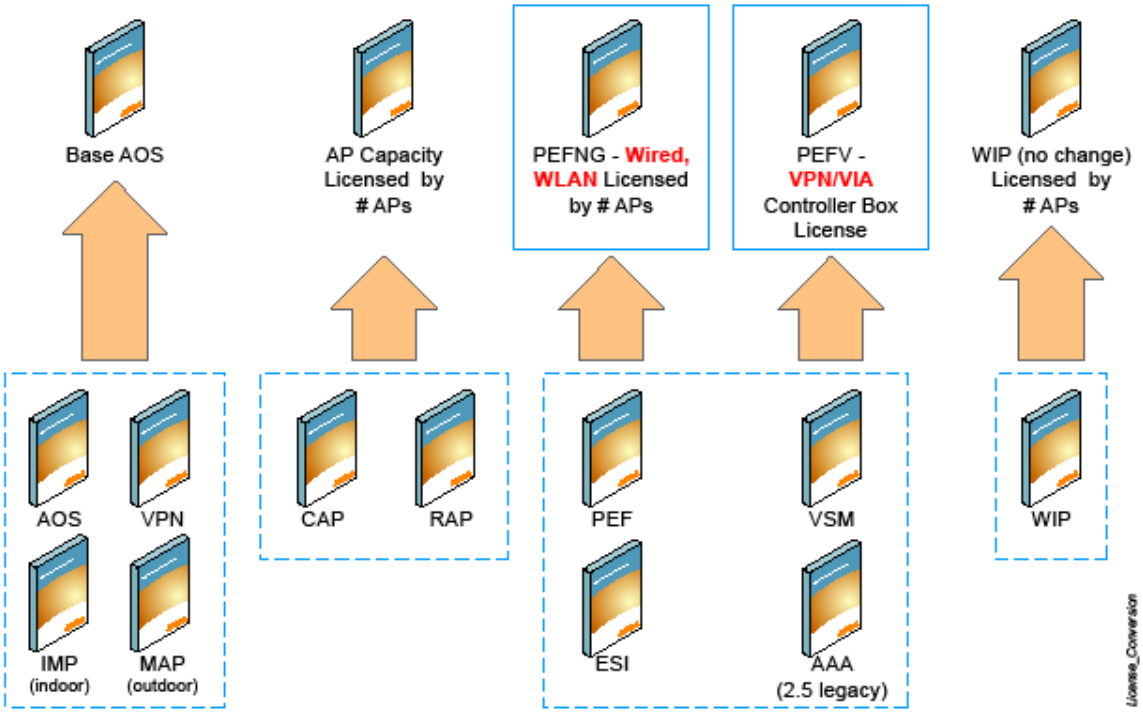
ArubaOS Legacy and End-of-Life

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

NOTE

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

Figure 1 *Licensing Consolidation ArubaOS 5.0*



Upgrading from 5.0.x to 6.0

The procedure to upgrade from 5.0.x to 6.0 is nearly identical to the procedure to upgrade from 3.4.x to 6.0, with a single change. If you are upgrading from 5.0.x to 6.0, your control plane security settings will be retained during the upgrade. If you had enabled the control plane security feature in ArubaOS 5.0, the feature will still be enabled after you upgrade to ArubaOS 6.0.

If you have occasion to downgrade to ArubaOS 5.0, you will not need to disable control plane security. If, however, you downgrade to ArubaOS 3.4.x or earlier versions, you must disable control plane security

before you downgrade. For more information on configuring control plane security and auto-certificate provisioning, refer to the *ArubaOS 6.0 User Guide*.

NOTE

When upgrading from ArubaOS 5.0.x to ArubaOS 6.0,x, control plane security configurations will be maintained.

Upgrading from 3.4.x to 6.0

Read all the following information before you upgrade to ArubaOS 6.0 . If you are upgrading from a version earlier than 3.4.x, see "Upgrading from 3.3.x to 6.0" on page 34 or "Upgrading from 2.5.x to 3.3.x to 6.0." on page 35.

- "Caveats" on page 31
- "Load New Licenses" on page 31.
- "Save your Configuration" on page 31.
- "Install ArubaOS 6.0" on page 32

Caveats

Before upgrading to ArubaOS 6.0 take note of these known upgrade caveats.

- When you upgrade to ArubaOS 6.0, the control plane security feature will be disabled by default. You can enable this feature at any time after the upgrade.
- If you have occasion to downgrade to a prior version, and your current ArubaOS 6.0 configuration has control plane security enabled, you must disable control plane security before you downgrade.

  For more information on configuring control plane security and auto-certificate provisioning, refer to the *ArubaOS 6.0 User Guide*.

Load New Licenses

Before you upgrade to ArubaOS 6.0, assess your software license requirements and load any new or expanded licenses you require prior to upgrading to ArubaOS 6.0.

Software licenses in ArubaOS 5.0 were consolidated and in some instances license names and modules were renamed to more accurately represent the modules supported by the licenses (see Figure 1).

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

NOTE

If you need to downgrade to ArubaOS 3.4.x, the previous licenses will be restored. However, once you upgrade again to ArubaOS 6.0 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 28). Saving your configuration saves the **admin** and **enable** passwords in the proper format.

Saving the Configuration in the WebUI

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

Saving the Configuration in the CLI

Enter the following command in enable or config mode:

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

Install ArubaOS 6.0

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 35.)

Install ArubaOS 6.0 in 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 6.0 in 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 3.4.1.23 (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 6.0.0.0 (Digitally Signed - Production Build)
Build number            : 23711
Label                   : 23711
Built on                : Wed July 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 6.0.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2010, Aruba Networks, Inc.
Compiled on 2010-04-25 at 15:18:56 PDT 6.0.0.0 (Digitally Signed - Production Build)
...
```

Upgrading from 3.3.x to 6.0

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 in 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 in 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 6.0.

Upgrading from ArubaOS 2.5.x to ArubaOS 6.0 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 6.0.

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 6.0" on page 34 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 6.0

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 6.0.

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 6.0" on page 34 to complete your last "upgrade hop".

Caveat

Should you need to downgrade from ArubaOS 6.0., 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 28.

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 6.0:

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 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 a, the upgrade script encrypts the internal database. Any new entries that were created in ArubaOS 6.0 will be lost after downgrade (this warning does not apply to upgrades from 3.4.x to 6.0),

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

1. Verify that Control Plane Security (CPSec) is disabled.
2. Set the controller to boot with the previously-saved pre-6.0 configuration file.
3. 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 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 pre-6.0 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.0 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 6.0 , the changes will not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.0 , 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 in 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 in 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 6.0 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 6.0.0.0 (Digitally Signed - Production Build)
Build number            : 23711
Label                   : 23711
Built on                : 2010-07-25 01:59:13 PDT
```

NOTE

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

NOTE

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 and verify that your new controller supports the ArubaOS version you are migrating to.

Migration instructions include:

- "Single Controller Environment" on page 38
- "Multiple Master Controller Environment" on page 39
- "Master/Local Controller Environment" on page 39

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. Ensure that the ArubaOS version on the newer controllers match the ArubaOS version on the rest of the controllers in your network.
2. Backup the old controller data and move the backup files to a safe place that is easily accesible through FTP/TFTP.
3. Physically swap the hardware (for example, mounting, cabling, power).
4. Initialize the new controller with the correct license.
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.