

ArubaOS 6.1



Release Notes

Copyright

© 2011 Aruba Networks, Inc. Aruba Networks trademarks include  Airwave, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

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 | 7 |
| | Chapter Overview | 7 |
| | Release Mapping | 7 |
| | Supported Browsers..... | 8 |
| | Contacting Support | 8 |
| Chapter 2 | What's New in this Release | 9 |
| | Upgrading the New Software Image Scheme | 9 |
| | AP-130 Series Wireless Access Point | 10 |
| | Suite-B Encryption | 10 |
| | Support for Suite-B Cryptographic Algorithms..... | 10 |
| | Suite-B Cryptography for 802.11i | 11 |
| | Support for TLS 1.2..... | 11 |
| | Using CLI to Enable TLS 1.2 | 11 |
| | ECDSA Certificate Support..... | 11 |
| | IPv6..... | 11 |
| | IPv6 Support for Controller and AP | 11 |
| | IPv6 Extension Header (EH) Filtering | 12 |
| | Captive Portal over IPv6 | 12 |
| | Spectrum Analysis using Hybrid APs | 12 |
| | Hybrid AP Channel Changes | 12 |
| | Platform | 13 |
| | Virtual Router Redundancy Protocol (VRRP) Preempt Delay | 13 |
| | SNMP Traps for AP Management in Redundant Controller Deployments ... | 13 |
| | Network Time Protocol Authentication | 13 |
| | Configuring NTP | 13 |
| | DHCP Relay Information Option 82 | 14 |
| | Enhancements in VLAN Derivation | 14 |
| | QBSS (QoS Enhanced Basic Service Set) Load IE (Information Element).... | 14 |
| | Security..... | 14 |
| | Improvements to “Prohibit IP Spoofing” Feature..... | 14 |
| | RADIUS Interim Accounting..... | 15 |
| | RADIUS Server Source Interface Selection | 15 |
| | In the WebUI..... | 15 |
| | In the CLI | 15 |
| | Controller Authentication using Certificates | 15 |
| | CHAP Authentication Support over PPPoE | 16 |
| | VPN Support for Suite-B Algorithms..... | 16 |
| | VPN Support for IKEv2..... | 16 |
| | Smart Card clients using IKEv2 | 17 |
| | Site-to-Site VPNs | 17 |
| | Default IKE policies..... | 18 |
| | Block Traffic Between Clients On the Same Virtual AP | 18 |
| | Device Fingerprinting | 19 |
| | Walled Garden Access..... | 19 |
| | Certificate Revocation..... | 20 |
| | About OCSP and CRL | 20 |
| | How Aruba Networks Uses OCSP and CRL | 20 |

| | | |
|------------------|---|-----------|
| | Certificate Groups | 20 |
| | Voice | 20 |
| | Remote Node | 20 |
| | Wireless | 21 |
| | Updates to ArubaOS 6.1 Factory Default Image | 21 |
| | High-Throughput with TKIP and WEP | 21 |
| | Wireless Intrusion Prevention (WIP) | 21 |
| | Wi-Fi Multi-media Admission Control Improvements | 21 |
| | AP Upgrades to IKEv2 | 21 |
| | Seamless Failover from Backup Link to Primary Link on Remote AP (RAP) | 22 |
| | Dashboard Monitoring | 22 |
| | Licensing Change History | 22 |
| | ArubaOS 6.1 | 22 |
| | ACR Interaction | 23 |
| Chapter 3 | Fixed Issues | 25 |
| Chapter 4 | Known Issues | 31 |
| Chapter 5 | Upgrade Procedures | 43 |
| | Important Points to Remember | 43 |
| | Technical Upgrading Best Practices | 44 |
| | WIP Configuration Changes in Version 6.0 | 44 |
| | WIP Predefined Profiles | 44 |
| | Wireless Containment Parameter | 45 |
| | Signature Matching profile Default Instance | 45 |
| | WIP Logging Changes | 45 |
| | Basic Upgrade Sequence | 45 |
| | Managing Flash Memory | 46 |
| | Before you upgrade | 46 |
| | Backing up Critical Data | 46 |
| | Backup and Restore Compact Flash in the WebUI | 47 |
| | Backup and Restore Compact Flash in the CLI | 47 |
| | Licensing Change History and Mapping | 47 |
| | ArubaOS 6.1 | 47 |
| | ACR Interaction | 48 |
| | ArubaOS 6.0 | 48 |
| | ArubaOS 5.0 | 48 |
| | ArubaOS 3.4.1 | 48 |
| | ArubaOS 3.4.0 | 48 |
| | ArubaOS Legacy and End-of-Life | 48 |
| | Upgrading from 5.0.x to 6.1 | 49 |
| | Upgrading from 3.3.x or 3.4.x to 6.1 | 49 |
| | Caveats | 50 |
| | Load New Licenses | 50 |
| | Save your Configuration | 50 |
| | Saving the Configuration in the WebUI | 50 |
| | Saving the Configuration in the CLI | 50 |
| | Install ArubaOS 6.1 | 50 |
| | Minimum Installation Requirements | 50 |
| | Install ArubaOS 6.1 in the WebUI | 51 |
| | Install ArubaOS 6.1 in the CLI | 51 |
| | Upgrading from RN-3.x.x to 6.1 | 53 |
| | Caveat | 53 |

| | |
|---|----|
| Upgrading in a Multi-Controller Network..... | 53 |
| Pre-shared Key for Inter-Controller Communication | 53 |
| Downgrading after an Upgrade | 54 |
| Downgrading in the WebUI..... | 54 |
| Downgrading in the CLI..... | 55 |
| Controller Migration | 56 |
| Single Controller Environment | 56 |
| Multiple Master Controller Environment | 56 |
| Master/Local Controller Environment | 56 |
| Before You Start..... | 56 |
| Basic Migration Steps | 57 |
| Before You Call Technical Support | 57 |

ArubaOS 6.1 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 6.1 User Guide*, *ArubaOS 6.1 CLI Reference Guide*, and *ArubaOS 6.1 MIB Reference Guide*.



See the “Upgrade Procedures” on page 43 for instructions on how to upgrade your controller to this release.

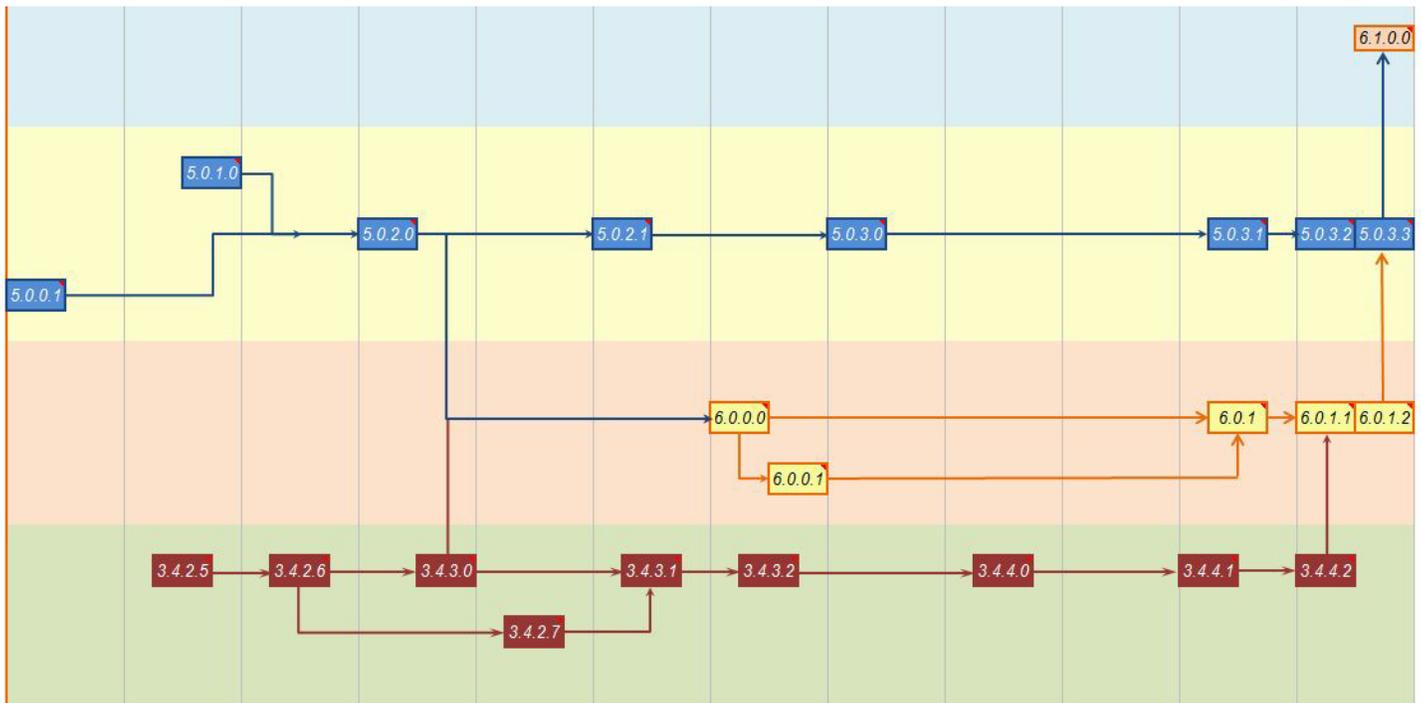
Chapter Overview

- Chapter 2, “What’s New in this Release” on page 9 describes the new features introduced in this release.
- Chapter 3, “Fixed Issues” on page 25 describes the issues that have been fixed in this release.
- Chapter 4, “Known Issues” on page 31 provides descriptions and workarounds for outstanding issues in ArubaOS 6.0.
- Chapter 5, “Upgrade Procedures” on page 43 cover the procedures for upgrading your controller from any release of ArubaOS to ArubaOS 6.0.

Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 6.1.

Figure 1 ArubaOS Releases and Code Stream Integration



Supported Browsers

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

- Microsoft Internet Explorer 8.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Mozilla Firefox 3.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.x on MacOS

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 |

The ArubaOS 6.1 release includes the following new features:

Upgrading the New Software Image Scheme



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



Upgrading from ArubaOS 3.3.x, 3.4x, 5.0.x or 6.0.x to ArubaOS 6.1 requires an “upgrade hop”. That is, *you must first upgrade to ArubaOS 6.0.1*. Then upgrade from ArubaOS 6.0.1 to ArubaOS 6.1. Carefully follow the upgrade steps in chapter “[Upgrade Procedures](#)” on page 43.



When upgrading the controller, the following is required:

- Confirm (`show memory`) that there is at least 40 MB of free memory available. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up upgrade immediately.
- Confirm (`show storage`) that there is at least 85 MB of /flash available.
- If less flash space is available run the `dir` command to list all files. Delete all unnecessary files including crash files, logs.tar file or a previous failed download image. To insure that all temporary (crash) files are removed perform a `tar crash` and then remove the `crash.tar` file from the controller.

[Table 1](#) provides a brief overview of the steps required to upgrade to ArubaOS 6.1. For more detailed information and procedures on upgrading, see “[Upgrade Procedures](#)” on page 43.

Table 1 ArubaOS 6.1 Upgrade Path Overview

| Version | Step 1 | Step 2 |
|----------|---|----------------|
| 3.3.x | Upgrade to 6.0.1 | Upgrade to 6.1 |
| 3.4.x | Upgrade to 6.0.1 | Upgrade to 6.1 |
| 5.0.x | Upgrade to 6.0.1 | Upgrade to 6.1 |
| 6.0 | Upgrade to 6.0.1 | Upgrade to 6.1 |
| RN_3.1.x | Upgrade to Latest RN version, then upgrade to 6.0.1 | Upgrade to 6.1 |

AP-130 Series Wireless Access Point

ArubaOS 6.1 introduces support for the Aruba AP-130 Series. The Aruba AP-130 series of wireless access points support the IEEE 802.11n standard for high-performance WLAN. These access points use MIMO (Multiple-in, Multiple-out) technology and support existing 802.11a/b/g/n wireless services. The AP-130 series access points work only in conjunction with an Aruba Controller.

Suite-B Encryption

This section describes features related to Suite-B encryption.

Support for Suite-B Cryptographic Algorithms

Suite-B cryptographic algorithms, as defined in RFC 4869, are highly secure algorithms used by ArubaOS to create IKE policies and IPsec tunnels. Aruba controllers running ArubaOS 6.1 support Suite-B encryption with the Advanced Cryptography (ACR) license. [Table 2](#) describes the Suite-B algorithms supported by ArubaOS IKE Policies and IPsec tunnels.

Table 2 Suite-B Algorithms Supported by the ACR License

| IKE Policies | Suite-B for IPsec tunnels |
|---|---|
| hash: SHA-256-128, SHA-384-192 | Encryption: AES-128-GCM, AES-256-GCM |
| Diffie-Hellman (DH) Groups : ECP-256, ECP-384 | Perfect Forward Secrecy (PFS): ECP-256, ECP-384 |
| Pseudo-Random Function (PRF) : HMAC_SHA_256, HMAC_SHA_384 | |
| Suite-B certificates: ECDSA-256, ECDSA-384 | |



NOTE

IKE Suite-B AES-128-GCM and AES-256-GCM encryption is supported by the Aruba hardware. IKE Suite-B Diffie-Hellman and Certificate-based signature operations and hash, PFS, and PRF algorithm functions are performed by the ArubaOS software.

It is important to note that not all controllers support the ACR license. The table below describes the controller support for Suite-B encryption in ArubaOS.

Table 3 Controller and Licensing Requirements

| Controller | Serial Number Prefix | ACR License Support |
|-------------|------------------------------|---------------------|
| Aruba 600 | All serial numbers supported | Yes |
| 3000 Series | BG | Yes |
| 3000 Series | AK | Yes |
| 3000 Series | A | No |
| M3 card | FC | Yes |
| M3 card | F | No |

To determine if your controller supports the ACR license, navigate to the **Monitoring>Controller>Inventory** page in the WebUI and note the prefix before the system serial number.

Suite-B Cryptography for 802.11i

ArubaOS has introduced a number of cryptographic algorithm/protocol and key size improvements to support 802.11i. Note that 802.11i Suite-B support is provided only for Virtual APs in tunnel forwarding mode. APs running ArubaOS 6.1 can advertise support for Suite-B by including Suite-B compliant cipher suites and AKM suites in their beacons and probe responses.

Support for TLS 1.2

The AAA FastConnect authentication mechanism has been enhanced to support TLS protocol version 1.2. This support allows you to use the Suite B cryptographic algorithms. By default the TLS 1.2 protocol is disabled. Use the `aaa authentication dot1x new-eap-termination` command to enable TLS 1.2 support.

Using CLI to Enable TLS 1.2

```
aaa authentication dot1x default-eap-termination
  enforce-suite-b-128
  enforce-suite-b-192
```

Where, the `enforce-suite-b-128` option enables 128-bit security level and the `enforce-suite-b-192` enables the 192-bit security level.

- To view the EAP termination debug counters use the `show datapath debug eap counters` command.
- To clear the EAP termination counters use the `clear datapath eap counters` command.

ECDSA Certificate Support

This release of ArubaOS provides Elliptic Curve Digital Signature Algorithm (ECDSA) certificate support for EAP-TLS v1.2 (AAA FastConnect), IKE server, and Site to site VPN.

You can now use the `crypto pki csr ec` command to generate the Certificate Signature Request (CSR) for ECDSA. The `show crypto pki csr` command allows you to view the generated CSR and the public key.

IPv6

This section describes features related to IPv6.

IPv6 Support for Controller and AP

This release of ArubaOS provides IPv6 support for controller and access points. You can now configure the master controller with an IPv6 address to manage the controllers and APs. Both IPv4 and IPv6 APs can terminate on the IPv6 controller. You can provision an IPv6 AP in the network only if the controller interface is configured with an IPv6 address. An IPv6 AP can serve both IPv4 and IPv6 clients.

You can perform the following IPv6 operations on the controller:

- Configure IPv6 interface address
- Configure IPv6 static neighbor
- Configure IPv6 default gateway and static IPv6 routes
- Manage the controller IP address
- Debug IPv6 controller
- Provision IPv6 AP

For more information on IPv6 operations, see *ArubaOS 6.1 User Guide*.

You can also view the IPv6 statistics on the controller using the following commands:

- `show datapath ip-reassembly ipv6`: View the IPv6 contents of the IP Reassembly statistics table.
- `show datapath route ipv6`: View datapath IPv6 routing table.
- `show datapath route-cache ipv6`: View datapath IPv6 route cache.
- `show datapath tunnel ipv6`: View the tcp tunnel table filtered on IPv6 entries.
- `show datapath user ipv6`: View datapath IPv6 user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users and maximum link length.

Additionally, you can view the IPv6 AP information on the controller using the following show commands:

- `show ap database`
- `show ap active`
- `show user`
- `show ap details`
- `show ap debug`

IPv6 Extension Header (EH) Filtering

ArubaOS firewall is enhanced to process the IPv6 Extension Header (EH) to enable IPv6 packet filtering. You can now filter the incoming IPv6 packets based on the EH type. To edit the packet filter options in the default EH, use the `netexthdr` command. By default, the default EH alias permits all EH types.

Captive Portal over IPv6

IPv6 is now enabled on the captive portal for user authentication on the Aruba controller. For user authentication use the internal captive portal that is initiated from the controller. A new parameter `captive` has been added to the IPv6 captive portal session ACL. The `netdestination` command is enhanced to automatically generate the controller alias required for IPv6 controllers.

The output of the following commands has been enhanced to support captive portal over IPv6:

- `ip access-list session captiveportal6`
- `show netdestination ipv6`
- `ip cp-redirect-address`

Spectrum Analysis using Hybrid APs

APs enabled with the spectrum analysis software module are able to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources. A radio on an AP-130 Series AP can be configured as a *hybrid* AP, allowing it to serve clients as an access point while it scans and analyzes spectrum analysis data for a single radio channel. You can record data for both hybrid APs and spectrum monitors, save that data, and then play it back for later analysis.

Hybrid AP Channel Changes

By default, a AP-130 Series hybrid AP only monitors the channel specified in its 802.11a or 802.11g radio profile for spectrum interference. If you want to change the channel monitored by a hybrid AP, you must edit the channel setting in those profiles. There are, however, other ArubaOS features that may automatically change the channels on hybrid APs. APs using Dynamic Frequency Selection (DFS) perform off-channel scanning to detect the presence of satellite and radar transmissions, and switch to a different channel if it detects that satellite or radar transmissions are present. APs using the Adaptive Radio

Response (ARM) feature constantly monitor the network and automatically select the best channel and transmission power settings for that AP.

If a hybrid AP is using ARM or DFS, that hybrid AP may automatically move to a different channel in response to changes in the network environment. If a hybrid AP changes channels while it is connected to a spectrum analysis client, the hybrid AP will update the graphs in the spectrum dashboard to start displaying spectrum data for the new channel, and will send a log message to the a spectrum analysis log.

Platform

This section describes platform related features.

Virtual Router Redundancy Protocol (VRRP) Preempt Delay

This release of ArubaOS introduces a preemption delay timer to prevent unnecessary transitions of VRRP state to master during network issues. The timer is triggered when the VRRP state moves out of backup or init state to become a master. When the timer is triggered, it delays the router for a specified period of time before taking over the master router. In the mean time, if there is an advertisement from another VRRP master (existing master), the router stops the timer and does not transition to master.

The new `vrrp preempt delay` option CLI command allows you to specify a VRRP delay for up to 60 seconds before it becomes the Master. Or, you can use the WebUI to set the delay value.

SNMP Traps for AP Management in Redundant Controller Deployments

A new trap, `wlsxNAPMasterStatusChange`, has been added. It is generated by the active master controller whenever any AP on that controller or one of the local controllers associated with that controller changes status. This trap has three OIDs.

The new trap includes the AP's wired MAC address, the IP address of the controller to which the AP is currently registered (or was most recently registered), and a status indication, which is represented by one of the following numerals:

- up: **1**
- down: **2**
- moved: **3**

To view information for this trap, access the command-line interface of the master controller and issue the command **show snmp trap-queue command**.

Example output for this trap is displayed as follows:

```
2010-12-13 02:14:50 Access point 00:0b:86:64:3b:a0 (LMS 10.3.6.51) status 1
```

Network Time Protocol Authentication

The Network Time Protocol (NTP) Authentication feature adds security to an NTP client by authenticating the server before synchronizing the local clock. NTP authentication works by using a symmetric key which is configured by the user. The secret key is shared by both the Aruba controller and an external NTP server and this helps identify secure servers from fraudulent servers.

Configuring NTP

Use the CLI to configure the NTP feature.

In the CLI

This example enables NTP authentication, add keys into the database, and specifies a subset of key which are trusted.

```
(host) (config) #ntp authenticate
(host) (config) #ntp authentication-key <key-id> md5 <key-secret>
(host) (config) #ntp trusted-key <key-id>
(host) (config) #ntp <server IP> iburst key <key-id>
```

DHCP Relay Information Option 82

DHCP Relay Information Option 82 is supported in this release. This option allows a DHCP Relay agent to insert circuit specific information into a request that is being forwarded to a DHCP server.

The controller, when acting as a DHCP relay agent, needs the ability to insert information about the AP and SSID through which a client is connecting into the DHCP request. Many service providers use this mechanism already to make access control decisions. Users have the option to include only the mac or mac and essid.

You can configure this feature using the CLI command `interface vlan <vlan-id> option-82`, or using the WebUI.

Enhancements in VLAN Derivation

Usually the client data is assigned the VLAN Id based on the virtual AP (VAP) of the client. The administrator can now associate a VLAN Id to a client data based on the authentication credentials in a bridge mode. The output of the `show datapath vlan ap-name <ap-name>` command has been enhanced to display the user mappings of VLAN and ports.

QBSS (QoS Enhanced Basic Service Set) Load IE (Information Element)

This release of ArubaOS includes the QBSS (QoS enhanced Basic Service Set) load element as part of the beacon frames generated by the QoS enhanced Access Points (QAP). You can enable the AP to advertize the QBSS load element. The element includes the following parameters that provide information on the traffic situation:

- Station count: The total number of stations associated to the QBSS.
- Channel utilization: The percentage of time (normalized to 255) the channel is sensed to be busy. The access point uses either the physical or the virtual carrier sense mechanism to sense a busy channel.
- Available admission capacity: The remaining amount of medium time (measured as number of 32us/s) available for a station via explicit admission control.

The QAP uses these parameters to decide whether to accept an admission control request. A wireless station uses these parameters to choose the appropriate access points.

You can use the `qbss-load-enable option` CLI command or the WebUI to enable QBSS Load Element.

Security

This section describes security features.

Improvements to “Prohibit IP Spoofing” Feature

ArubaOS can be configured to detect IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent. Previous versions of ArubaOS checked only the source IP and the source MAC address in the frame. Starting with ArubaOS 6.1, this feature also checks the destination IP and the destination MAC address in the frame.

This feature is enabled using the CLI command **firewall prohibit-ip-spoofing**.

RADIUS Interim Accounting

In previous versions of ArubaOS, the RADIUS accounting feature sent only Start and Stop messages to the RADIUS accounting server. Starting with ArubaOS 6.1, the RADIUS interim accounting feature allows the controller to send Interim-Update messages with current user statistics to the server at regular intervals. The default interval, and the lowest supported interval, is 10 minutes.

Interim radius accounting messages are disabled by default. To enable interim radius accounting messages, access the command-line interface in config mode, and issue the following command:

```
(host) (config) #aaa profile <profile> radius-interim-accounting
```

RADIUS Server Source Interface Selection

This feature allows you to use source IP addresses to differentiate RADIUS requests. This is useful if a customer site is already using source IP addresses before the introduction on Aruba devices. This feature is configured within the AAA server group. The CLI command `source-interface vlan <vlan number>` has been added under the existing `aaa authentication-server radius <name>` command. This new command permits the user to associate a VLAN interface with the RADIUS server and allows the group-specific source interface to override global configuration.

In the WebUI

1. Navigate to the **Configuration > Security > Authentication > Servers** page.
2. Select **Radius Server** to display the Radius Server List.
3. To configure a RADIUS server, enter the name for the server and click **Add**.
4. Select the name to configure server parameters.
5. In the **Source Interface** field, enter a VLAN number ID.

This allows you to use source IP addresses to differentiate RADIUS requests. It associates a VLAN interface with the RADIUS server to allow the server-specific source interface to override the global configuration.

- If you associate a Source Interface (by entering a VLAN number) with a configured server, then the source IP address of the packet will be that interface's IP address.
 - If you do not associate the Source Interface with a configured server (leave the field blank), the IP address of the global Source Interface will be used.
6. Select the **Mode** check box to activate the authentication server.
 7. Click **Apply** to apply the configuration.

In the CLI

```
(host) (config)# aaa authentication-server radius myserver  
(host) (RADIUS Server "myserver") #source-interface vlan 8
```

Controller Authentication using Certificates

Starting with ArubaOS 6.1, you can use either a preshared key or certificate to secure communication between a master and local controller. Earlier versions of ArubaOS supported pre-shared key authentication only.



If your master and local controllers use a pre-shared key for authentication, they will create the IPsec tunnel using IKEv1. If your master and local controllers use certificates for authentication, the IPsec tunnel will be created using IKEv2.

If your network includes multiple master controllers each with their own hierarchy of APs and local controllers, you can allow APs from one hierarchy to failover to any other hierarchy by defining a *cluster* of

master controllers. Each cluster will have one master controller as its cluster root, and all other master controllers as cluster members.

To create a controller cluster, you must first define the root master controller, then choose a method to secure communications between the cluster root and cluster members. Starting with ArubaOS 6.1, you can use certificates or an IPsec key to authenticate cluster members. Previous versions of ArubaOS required an IPsec key for communications between the cluster root and cluster members, and did not support certificate authentication.



You must use the command-line interface to configure certificate authentication for cluster members. The WebUI supports cluster authentication using IPsec keys only.

CHAP Authentication Support over PPPoE

Previously ArubaOS supported only the password authentication protocol (PAP) for authenticating the point-to-point protocol over ethernet (PPPoE) clients running on a remote AP (RAP).

The RAPs can now establish a PPPoE session with a PPPoE server at the ISP side and get authenticated using the challenge handshake authentication protocol (CHAP). The PPPoE client running on the RAP is capable of handling the CHAP authentication requests from the PPPoE server.

- To configure CHAP using the WebUI, navigate to the **Configuration > Wireless > AP Installation > Provisioning page** and enter the **CHAP Secret** in the text box under **Authentication Method**.
- To configure CHAP using the CLI, use the `configure terminal provision-ap pppoe-chap-secret <KEY>` command.

VPN Support for Suite-B Algorithms

The following VPN clients support Suite-B algorithms when establishing an L2TP/IPsec VPN.

Table 4 Client Support for Suite-B

| Client Operating System | Supported Suite-B IKE Authentication | Supported Suite-B IPsec Encryption |
|--|---|--|
| <ul style="list-style-type: none">• Windows 7• Windows Vista• Windows XP• Aruba VIA | <ul style="list-style-type: none">• IKEv1 Clients using ECDSA Certificates• IKEv1/IKEv2 Clients using ECDSA Certificates with L2TP/PPP/EAP-TLS certificate user-authentication | <ul style="list-style-type: none">• AES-128-GCM,• AES-256-GCM |

The Suite-B algorithms described in [Table 2](#) are also supported by Site-to-Site VPNs between Aruba controllers, or between an Aruba controller and a server running Windows 2008, Windows 7, Windows Vista, or StrongSwan 4.3.

In order to use Suite-B algorithms with IKEv2, you must install the ACR license on your controller and modify the default IKEv2 dynamic map to use Suite-B. Use the following commands to modify the default IKEv2 dynamic map using the command-line interface:

```
(config) #crypto dynamic-map default-ikev2-dynamicmap <priority>
(config-dynamic-map)# set transform-set default-gcm128 default-gcm256 default-1st-ikev2-transform default-3rd-ikev2-transform
```

VPN Support for IKEv2

Remote access VPNs allow hosts (for example, telecommuters or traveling employees) to connect to private networks (for example, a corporate network) over the Internet. Controllers running ArubaOS version 6.1 and later support both IKEv1 and the newer IKEv2 protocol to establish IPsec tunnels. IKEv2 is

simpler, faster, and a more reliable protocol than IKEv1, though both IKEv1 and IKEv2 support the same suite-B cryptographic algorithms.

ArubaOS does not support separate pre-shared keys for both directions of an exchange; the same pre-shared key must be used by both peers. ArubaOS does not support mixed authentication with both pre-shared keys and certificates; each authentication exchange requires a single authentication type. (For example, if a client authenticates with a pre-shared key, the controller must also authenticate with a pre-shared key.) ArubaOS does not support IKEv2 mobility (MOBIKE), Authentication Headers (AH) or IP Payload Compression Protocol (IPComp).

Not all clients support the both the IKEv1 and IKEv2 protocols. Only the clients in [Table 5](#) support IKEv2 with the following authentication types:

Table 5 VPN Clients Supporting IKEv2

| Windows 7 Client | StrongSwan 4.3 Client | Aruba VIA Client |
|---|---|---|
| <ul style="list-style-type: none"> Machine authentication with Certificates User-name password authentication using EAP-MSCHAPv2 or PEAP-MSCHAPv2 User smart-card authentication with EAP-TLS / IKEv2 EAP-TLS with IKEv2 using factory-installed certificates <p>NOTE: Windows 7 clients using IKEv2 do not support pre-shared key authentication.</p> | <ul style="list-style-type: none"> Machine authentication with Certificates User-name password authentication using EAP-MSCHAPv2. Suite-B cryptographic algorithms | <ul style="list-style-type: none"> Machine authentication with Certificates User-name password authentication using EAP-MSCHAPv2 EAP-TLS using Microsoft cert repository <p>NOTE: VIA clients using IKEv2 do not support pre-shared key authentication.</p> |

Smart Card clients using IKEv2

A smart card contains a digital certificate which allows user-level authentication without the user entering a username and password. Microsoft clients running Windows 7 (or later versions) support both IKEv1 and IKEv2. Microsoft clients using IKEv2 support machine authentication using RSA certificates (but not ECDSA certificates or pre-shared keys) and smart card user-level authentication with EAP-TLS over IKEv2.



Windows 7 clients without smart cards also support user password authentication using EAP-MSCHAPv2 or PEAP-MSCHAPv2.

Site-to-Site VPNs

Site-to-site VPN allows sites at different physical locations to securely communicate with each other over a Layer-3 network such as the Internet. You can use Aruba controllers instead of VPN concentrators to connect the sites. Or, you can use a VPN concentrator at one site and a controller at the other site.

The Aruba controller now supports the following new IKE SA authentication methods for site-to-site VPNs:

- Suite-B cryptographic algorithms
- Digital certificates: You can configure a RSA or ECDSA server certificate and a CA certificate for each site-to-site VPN IPsec map configuration. If you are using certificate-based authentication, the peer must be identified by its certificate subject-name distinguished name (for deployments using IKEv2) or by the peer's IP address (for IKEv1).



Certificate-based authentication is only supported for site-to-site VPN between two controllers with static IP addresses.

Controllers can use IKEv1 or IKEv2 to establish a site-to-site VPN between another Aruba controller or between that controller and third-party device. Note, however, that only Aruba controllers and devices running Windows 2008 Server or StrongSwan 4.3 support IKEv2 authentication.

Devices running Windows 2008 server can use Suite-B cryptographic algorithms and IKEv1 to support authentication using RSA or ECDSA. Strongswan 4.3 devices can use IKEv2 to support authentication using RSA or ECDSA certificates, Suite-B cryptographic algorithms, and pre-shared keys.

Default IKE policies

ArubaOS now includes the following default IKEv2 and Suite-B policies. These policies are predefined and cannot be edited.

Table 6 Default IKE Policy Settings

| Policy Name | Policy Number | IKE Version | Encryption Algorithm | Hash Algorithm | Auth Method | PRF Method | Diffie-Hellman Group |
|--|---------------|-------------|----------------------|----------------|---------------------|---------------|----------------------------|
| Default RAP IKEv2 RSA protection suite | 1004 | IKEv2 | AES-CBC-256 | SHA 160 | RSA Signature | hmac-sha1 | 2 (1024 bit) |
| Default IKEv2 RSA protection suite | 1006 | IKEv2 | AES-CBC-128 | SHA 96 | RSA Signature | hmac-sha1 | 2 (1024 bit) |
| Default IKEv2 PSK protection suite | 10007 | IKEv2 | AES-CBC-128 | SHA 96 | Pre-shared key | hmac-sha1 | 2 (1024 bit) |
| Default Suite-B 128bit ECDSA protection suite | 10008 | IKEv2 | AES-GCM-128 | SHA 256-128 | ECDSA-256 Signature | hmac-sha2-256 | Random ECP Group (256 bit) |
| Default Suite-B 256 bit ECDSA protection suite | 10009 | IKEv2 | AES-GCM-256 | SHA 384-192 | ECDSA-384 Signature | hmac-sha2-384 | Random ECP Group (384 bit) |
| Default Suite-B 128bit IKEv1 ECDSA protection suite | 10010 | IKEv1 | AES-GCM-128 | SHA 256-128 | ECDSA-256 Signature | hmac-sha2-256 | Random ECP Group (256 bit) |
| Default Suite-B 256 bit IKEv1 ECDSA protection suite | 10011 | IKEv1 | AES-GCM-256 | SHA 256-128 | ECDSA-256 Signature | hmac-sha2-256 | Random ECP Group (256 bit) |

Block Traffic Between Clients On the Same Virtual AP

Each virtual AP profile configuration now includes the ability to block traffic between clients using that virtual AP.

The global firewall also includes an option to deny all inter-user traffic, regardless of virtual AP used by those clients. If this global setting is enabled, all inter-user traffic will be denied, regardless of the settings configured in the virtual AP profiles. If the setting to deny inter-user traffic is disabled globally but is enabled on an individual virtual AP, only the traffic between un-trusted users and the clients on that one virtual AP will be blocked.

To use the WebUI to block traffic between users on a specific virtual AP:

1. Navigate to the **Configuration>Advanced Services>All Profiles** page and expand the **Wireless LAN** menu.
2. Expand the **Virtual AP profile** menu and select the Virtual AP Profile for which you want to block inter-user traffic.
3. Click the **Deny Inter User Traffic** checkbox.
4. Click **Apply Changes** to save your settings.

Device Fingerprinting

The device fingerprinting feature allows you to assign a user role or VLAN to a specific device type by identifying a DHCP option and signature for that device. If you create a rule for a user-derived rule with the **DHCP-Option** rule type, the first two characters in the **Value** field must represent the hexadecimal value of the DHCP option that this rule should match, while the rest of the characters in the **Value** field indicate the DHCP signature the rule should match.

The following table describes some of the DHCP options that are useful for assigning a user role or VLAN.

Table 7 DHCP Option values

| DHCP Option | Description | Hexadecimal Equivalent |
|-------------|-------------------------|------------------------|
| 12 | Host name | 0C |
| 55 | Parameter Request List | 37 |
| 60 | Vendor Class Identifier | 3C |
| 81 | Client FQDN | 51 |

The device fingerprinting features in ArubaOS can also automatically identify different client device types and operating systems by parsing the User-Agent strings in the client's HTTP packets. If you enable **Device Type Classification** in an AP's AAA profile, the controller will parse user-agent strings and attempt to identify the type of device connecting to the AP. When the device type classification is enabled, the Global client table shown in the **Monitoring>Network > All WLAN Clients** window shows each client's device type, if that client device can be identified.

Walled Garden Access



The Walled Garden feature is used with the PEFNG or PEFV licenses.

On the Internet, a walled garden typically controls a guest's access to web content and services. The walled garden directs the guest's navigation within particular areas to allow access to a selection of websites or prevent access to other websites.

Walled garden access is useful for when an external or internal captive portals are used. A common example could be a hotel environment where unauthenticated clients are allowed to navigate to the hotel's designated login page and all its contents.

Guests not signing up for Internet service (non paying) can view "allowed" websites (typically hotel property websites). The website names must be DNS-based (not IP address based) and support the option to define wildcards. This works for client devices with or without HTTP proxy settings.

When the guest attempts to navigate to other websites not configured in the white list walled garden profile, the guest is redirected back to the login page. In addition, the black listed walled garden profile is configured to explicitly block navigation to websites from unauthenticated guests.

You can configure a walled garden using both WebUI and CLI commands and is described in the *Captive Portal* chapter.

Certificate Revocation

The Certificate Revocation feature enables the ArubaOS controller to perform real-time certificate revocation checks using the Online Certificate Status Protocol (OCSP) or traditional certificate validation using the Certificate Revocation List (CRL) client.

About OCSP and CRL

OCSP (RFC 2560) is a standard protocol that consists of an OCSP client and an OCSP responder. This protocol determines revocation status of a given digital public-key certificate without having to download the entire CRL.

CRL is the traditional method of checking certificate validity. A CRL provides a list of certificate serial numbers that have been revoked or are no longer valid. CRLs let the verifier check the revocation status of the presented certificate while verifying it. CRLs are limited to 512 entries.

How Aruba Networks Uses OCSP and CRL

The ArubaOS controller can act as an OCSP client and issues OCSP queries to remote OCSP responders located on the intranet or Internet. As many applications in ArubaOS (such as IKE), use digital certificates, a protocol such as OCSP needs to be implemented for revocation.

An entity that relies on the content of a certificate (a relying party) needs to do the checking before accepting the certificate as being valid. One check verifies that the certificate has not been revoked. The OCSP client retrieves certificate revocation status from an OCSP responder. The responder may be the CA that has issued the certificate in question or it may be some other designated entity which provides the service on behalf of the CA. A *revocation checkpoint* is a logical profile that is tied to each CA certificate that the controller has (trusted or intermediate). Also, the user can specify revocation preferences within each profile.

The OCSP request is not signed by the Aruba OCSP client at this time. However, the OCSP response is always signed by the responder. The responder may refuse to serve the unsigned request depending on the configuration.

Certificate Groups

This feature allows you to select multiple server certificates for terminating clients. The new CLI command **crypto-local isakmp certificate-group** allows you to define a new certificate group that groups one server certificate with one CA certificate. You define a list of CA certificates using the existing `crypto-local isakmp ca-cert` command and then define each group using the `crypto-local isakmp certificate-group` command.

Voice

Remote Node

Configuring a local controller as a remote node master is considered beta quality in this release. Aruba recommends using a master as a remote node master.

Wireless

This section describes wireless features.

Updates to ArubaOS 6.1 Factory Default Image

The factory default setting of the ArubaOS 6.1 image will not have the default *aruba-ap* SSID associated to the default virtual AP. Since there are no virtual APs associated to an AP group, APs terminating on the controller will remain in inactive state.

High-Throughput with TKIP and WEP

The Wi-Fi Alliance has published a security road map that requires vendors to phase out support for legacy and unsecure encryption methods. Although the Wi-Fi Alliance has backed off on a mandatory date for enforcement, Aruba is implementing the first required change in this release in anticipation of the requirement becoming mandatory in the near future.

Specifically, stations are not allowed to use HT with TKIP standalone encryption, although TKIP can be provided in mixed-mode BSSIDs that support HT. Therefore, the **allow-weak-encryption** parameter, in the **ht-ssid-profile** command, is being deprecated. HT is also disabled on a BSSID if the encryption mode is standalone TKIP or WEP.

Wireless Intrusion Prevention (WIP)

- Power Save DoS in 802.11 Networks—Detection of the Meiners Power Save DoS attack, including event notification to the user.
- Known SSIDs Configuration Enhancement — For attack detections, an internally generated list of valid SSIDs is used in addition to the user configured list of Valid and Protected SSIDs.
- Collect wired and gateway MAC addresses at the controller—This information is used by Aruba APs to classify rogue APs, and is especially valuable when classifying rogues on subnets where Aruba APs can not be deployed.



The collect wired and gateway MAC addresses feature is intended for deployments with a single master or local controller in each geographical location, and where controllers are not Layer 2 connected to other controllers. If two Layer 2 connected controllers are geographically close, enabling this feature can result in false positives: one controller could mark APs belonging to the other controller as suspected rogue when this feature is enabled.

- Behavior change of SSID Misconfiguration detection — The feature detects misconfiguration of valid third party APs only and no longer checks valid Aruba APs. This eliminates false alarms for valid Aruba APs, while still fulfilling the intent of the feature.

Wi-Fi Multi-media Admission Control Improvements

ArubaOS 6.1 includes a new command to send DELTS for a live traffic stream, even if the client is not a voice client.

```
voice test force_send_delts sta <sta-mac> tid <tid_number>
```

where **<sta-mac>** is the MAC address of the client station to which the DELTS are sent, and **<tid_number>** The traffic stream ID. The valid range for this parameter is 0 to 7. If the traffic stream ID is not specified and there are multiple live traffic streams, multiple DELTS will be sent out to the station.

AP Upgrades to IKEv2

IKEv2 is the newest version of the IKE protocol used to establish IPsec tunnels, and is a simpler and more reliable protocol than IKEv1. When a controller upgrades to ArubaOS 6.1, any campus APs and remote APs

with RSA factory certificates will use IKEv1 to connect to the controller and upgrade their images. Once upgraded, these APs will then will use IKEv2 to create an IPsec tunnel to the controller.

APs with IKEv1 certificates only will be allowed to upgrade to an ArubaOS 6.1 image, but will not be allowed to receive its configuration or support clients. APs connecting to the controller using a pre-shared key will continue to create IPsec tunnels using IKEv1



If the controller is downgraded to an earlier release, an AP running ArubaOS 6.1 will try 30 times to create an IPsec tunnel using IKEv2. If there is no response from the controller, it will switch to IKEv1. If an AP running ArubaOS 6.1 reverts to IKEv1, either because the controller was unreachable or because it reverted to an earlier release, the AP will switch back to IKEv2 if it reconnects to a controller running ArubaOS 6.1.

Seamless Failover from Backup Link to Primary Link on Remote AP (RAP)

RAPs can now failover from a backup link to a primary link without much disruption to traffic. Also the failover is performed only if the controller is reachable via the primary link.

Dashboard Monitoring

The ArubaOS dashboard monitoring functionality provides enhanced visibility into your wireless network performance and usage within a controller. This allows you to easily locate and diagnose WLAN issues in the controller.

The dashboard monitoring is available via the WebUI. To monitor and troubleshoot RF issues in the WLAN, click the **Dashboard** tab. The following pages in the **Dashboard** page allows you to view various performance and usage information:

- Performance
- Usage
- Security
- Potential Issues
- WLANs
- Access Points
- Clients

Additionally, you can view the context sensitive help for each field in the **Dashboard** UI by doing a right click on the field.

Licensing Change History

License consolidation, renaming, and new licenses are introduced over time. The following changes and/or consolidation were made to ArubaOS licensing.

ArubaOS 6.1

- The VIA feature now requires a PEFV license (Policy Enforcement Firewall Virtual Private Network).
- Advanced Cryptography (ACR) is introduced—the ACR license is required for the Suite B Cryptography in IPsec and 802.11 modes. License enforcement behavior controls the total number of concurrent connections (IPsec or 802.11) using Suite B Cryptography. Bundled with this license are the xSec license features.

ACR Interaction

- On a platform that supports 2048 IPsec tunnels, the maximum number of Suite B IPsec tunnels supported is 2048, even if a larger capacity license is installed.
- The ACR license is cumulative. If you want to support 2048 Suite B connections, install two ACR licenses (LIC-ACR-1024).
- An evaluation ACR license is available (EVL-ACR-1024). You can install the ACR evaluation license with a higher capacity than the platform maximum.
- On a platform that supports 2048 IPsec tunnels, with a LIC-ACR-512 installed, only 512 IPsec tunnels can be terminated using Suite B encryption. An additional 1536 IPsec tunnels, using non-Suite B modes (e.g. AES-CBC), can still be supported.
- On a platform with LIC-ACR-512 installed, a mixture of IPsec and 802.11i Suite B connections can be supported. The combined number of these sessions may not exceed 512.
- A single client using both 802.11i Suite B and IPsec Suite B simultaneously will consume two ACR licenses.

This release contains all fixes up to and including those in ArubaOS 5.0.3.3. The following issues and limitations have been fixed in the ArubaOS 6.1 release:

Table 1 *Fixed Issues in ArubaOS 6.1*

| Bug ID | Description |
|-----------------|--|
| 31074 | The SNMP fault list now correctly clears RADIUS servers from the fault list when the server comes back into service. |
| 31783 | RAPs are able to establish IPSec connections when up to 64 character isakmp key. |
| 32807 | The controller now correctly blocks H.323 calls when the H.323 Call Capacity is reached. When the call is blocked, the blocked client is automatically deauthenticated. |
| 35928 | All APs that terminate on the same controller are correctly identified as a valid AP not an interfering AP. |
| 36123 | XML query with usernames now works correctly. |
| 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. |
| 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. |
| 40032 | The AP-105 no longer constantly detects spurious radar when operating DFS channels (52, 56, 60, and 64). |
| 41299, 45362 | An IP pool leak that was preventing users from connecting using L2TP VPN has been fixed. |
| 41363 | APs come up successfully if their AP Group Name contains a + symbol. |
| 42333, 42332 | wlanAPSysLocation has been added to AP table, which gives the value of the syslocation provisioning parameter for the AP. |
| 42717 | RAP fail-over to the backup cellular link in a case where ethernet link is NOT down, but some intermediate (between RAP and controller) connectivity is broken now work correctly. |
| 43026 | The font size of the guest provisioning printout will be the size that is configured. |
| 43215, 43915 | Clients correctly receive a DHCP ACK no 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. |
| 43300 | The issue with the pause in traffic during the Chariot throughput test has been fixed. |
| 43802, 44696 | A datapath timeout that occurred when pkt-trace global was enabled has been fixed. |
| 43855 | When a certificate on a local controller expires, it can no longer be overwritten and deleted to make room for a new certificate. |

Table 1 *Fixed Issues in ArubaOS 6.1 (Continued)*

| Bug ID | Description |
|---|--|
| 43948, 41351, 45266, 45689, 45002, 46391, 47928, 46486 | An AP reboot issue caused when the AP runs out of memory has been fixed. |
| 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. |
| 44504 | The command <code>show user location</code> now provides the correct information. |
| 44794 | An issue which many bridge mode users were listed with a 0.0.0.0 IP address and many users could be seen in the datapath user table but not in the user-table has been fixed. |
| 44846 | An issue in which APs bootstrap during a write mem on the master controller has been fixed. |
| 45009 | A connectivity issue caused by abnormally large <code>Available TX Buffers</code> counts 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. |
| 45126 | When a RAP is in always or backup mode, the radio LED will light up to indicate that AP is up. |
| 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. |
| 45383, 42958 | The RAP-5 no longer crashes with the message "PPP: Termination Request Received" when using a 3G modem. |
| 45384, 46355 | AMSDU is now disabled by default with a knob in the firewall command in the CLI. |
| 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. |
| 45606 | The Handoff Assist log message has been enhanced to show the actual low RSSI of the client. |
| 45643 | An AP-85 mesh point crashed caused when the AP attempts to process large frames has been fixed. |
| 45669, 46617 | AP coverage is now shown correctly on the RF Plan heatmap. |
| 45694 | The controller is now able to respond to ARP requests from a client when the ARP request is coming from a port-channel. |
| 45858 | The option <code>Include Technical Support Information</code> is not selected by default when logs are downloaded. |

Table 1 *Fixed Issues in ArubaOS 6.1 (Continued)*

| Bug ID | Description |
|---|--|
| 45866, 44712, 50392, 44934 | A datapath timeout issue causing the M3 controller to continuously reboot after upgrading has been fixed. |
| 45943 | In the WebUI, you can create an SNMP password with any number of characters instead of 5 or more characters. |
| 46027 | ArubaOS now ignores transient timeouts as long as subsequent LDAP requests are seeing responses back from the LDAP server. |
| 46095 | Unexpected controller behavior in the Mobile IP module caused by a race condition has been fixed. |
| 46204 | The controller's buffer size has been increased for EAPOL packets to help prevent authmgr crashes. |
| 46251 | Wireless clients no longer incorrect get a role from the wired aaa profile after an auth restart. |
| 46321 | Users are able to establish passive FTP connections. |
| 46340 | 46340 ZTE modem ttyUSB no longer changes between cold and warm boot. |
| 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. |
| 46701 | A RAP-5 crash that happens when the RAP is connected to an EVDO device has been fixed. |
| 46747 | A Mesh portal and point crash due to an assertion in ieee80211_decap() has been fixed. |
| 46761, 51443 | An SNMP walk issue that breaks at wlsxVoiceAPBssidInfoGroup has been fixed. |
| 46839 | An AP-125 crash in skb_over_panic has been fixed. |
| 47032, 49982, 50528, 51329, 52043 | The DNSmasq process on 600 Series controllers has been improved to allow a DNS query of a domain name longer than 51 characters. |
| 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. |
| 47074 | Users no longer lose IP connectivity when using split-tunnel mobility solution. |
| 47219, 47402 | The controller no longer stops forwarding traffic to clients connected via PPTP. |
| 47313 | A controller reboot caused by udbserver module crash has been fixed. |
| 47553 | A controller STM crash caused by a control process exception has been fixed. |
| 47614 | You can now successfully delete session ACLs from a policy when using the WebUI. |

Table 1 *Fixed Issues in ArubaOS 6.1 (Continued)*

| Bug ID | Description |
|---------------------|--|
| 48040 | Legacy AP with aggressive scanning settings now scan as expected. |
| 48107, 48802, 38376 | An issue in which the error log displays the message <code>SNMP agent timed out when sending a request to application WMS for object (object id)</code> and reports the controller as down when it is not has been fixed. |
| 48242 | When a TACACS accounting message fails, the SNMP trap returned by the controller under User Authentication Failed displays the user and MAC address instead of zeros. |
| 48243 | TACACS failed/success management authentication log messages now include the user name for the failed request. |
| 48244 | The controller now sends SNMP traps for failed TACACS management authentication. |
| 48459 | APs are no longer slowly running out of memory (memory leak). |
| 48537, 50123 | Authentication issues, accompanied by RADIUS timeout stats increasing, when static-wep and VLAN derivation are enabled has been fixed. |
| 48623 | The log message 301257 has been reclassified from INFO to DEBUG and the host IP information has been added. |
| 48660 | An error log message has been added to report if ArubaOS failed to decode mppe key attributes. |
| 48758 | Clients are now able to reconnect after being removed from the blacklist table and if the Max Auth failure value is set to 0, clients are not blacklisted. Additionally, the blacklist time can be set to values less than 3600. |
| 48838 | The Clear Session on Role Update firewall now works correctly in the case of a RADIUS disconnect event. |
| 49038 | An auth crash caused by a memory leak due to LDAP authentication timeouts has been fixed. |
| 49271 | You can now successfully delete a Captive Portal profile and user role without needing to restart the auth and httpd processes. |
| 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. |
| 49576 | When a server certificate is installed, controller now correctly responds to DNS query with the IP address specified by <code>ip cp-redirect-address</code> configuration. |
| 49825 | The formatting for the command <code>show phonehome stats</code> has been improved. |
| 49985 | When using Safari, the configuration fields are now correctly displayed when configuring ports under Configuration > Network > Ports > Port in the WebUI. |
| 50027, 50026 | A controller ISAKMPD module crash caused by a low memory state has been fixed. |
| 50313 | In the WebUI, the client activity graph for wired clients on a campus AP now correctly displays information. |
| 50578 | An AP STM memory leak initiated by a controller deauth has been fixed. |

Table 1 *Fixed Issues in ArubaOS 6.1 (Continued)*

| Bug ID | Description |
|-----------------|---|
| 51258 | An httpd module crash that prevents the WLAN wizard from working in any browser has been fixed. |
| 49184 | Upgrading by FTP using the WebUI now works correctly. |
| 48867, 48996 | Users now correctly move to the server role with user derivation rule <code>vlan equals bssid</code> and server derivation <code>role equals Server-Name</code> with dot1x termination. |
| 48325 | RAPs over PPPoE no longer crash when the ap-group has split-VAP and a bridge mode wired-AP. |
| 48190 | The Upload from local file option for upgrade now works when used through the WebUI. |

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

Table 1 *Known Issues and Limitations*

| Bug ID | Description |
|-----------------|---|
| | Configuring a local controller as a remote node master is considered beta quality in this release. Aruba recommends using a master as a remote node master. |
| 35734 | Role derivation does not happen correctly when machine authentication is successful but dot1x authentication fails. Instead of being placed in the default user role, the user is placed in the logon role. Workaround: None. |
| 43599 | In the WebUI under Access Control > Security > Access Control > Firewall Policies , the policy usage numbers shown are incorrect. The ACLs listed are shown as in-use when they are not being used. Workaround: None. Use the CLI command <code>show ip access-list</code> to view the correct information in the CLI. |
| 44254, 40208 | When a VIA user connects to a controller two user entries are shown on the User Table and two VPN user licenses are consumed. Workaround: None. This is expected behavior. |
| 45313 | The name Mocana appears in controller security logs while IKEv2 tunnel is being brought up. Workaround: None. This is expected behavior. |
| 45462, 45459 | The CLI hangs while using include with <code>show datapath</code> command for a non-existent address. Workaround: None. However, this issues can be avoided by not using IPv6 addresses that begin with zero. |
| 46443 | Do not enable Firewall TCP enforcement when IP mobility is enabled. Workaround: None. |
| 50396 | Deny Inter User Bridge does not block IPv6 traffic between untrusted clients on the same VLAN. Workaround: None. |
| 50474 | The Guest Provisioning Page becomes frozen for 3 to 4 minutes when a CSV file containing more than 250 user entries is imported. Workaround: None. This can be avoided by importing files with less than 250 user entries. |
| 50627 | A change-of-authorization (from RFC-3576) server does not update the role correctly for split-tunnel clients. Workaround: None. |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|-----------------|---|
| 50648 | <p>The maximum number of IPv6 sessions is approximately 420,000. Any sessions beyond that show packet loss and the number of allocation failure counter increases under <code>show datapath session ipv6 counters</code>.</p> <p>Workaround: None.</p> |
| 50730 | <p>The command <code>show ap database</code> applies the “D” flag (Dirty or no config) to active APs.</p> <p>Workaround: None.</p> |
| 50776 | <p>User entries for active clients associated to an AP in bridge or tunnel mode with WPA2-AES opmode are not retained in the user table.</p> <p>Workaround: None.</p> |
| 50779 | <p>Clients connected on bridge-VAP of mesh-AP are missing from <code>user</code> and <code>datapath session ap-name</code> tables.</p> <p>Workaround: None.</p> |
| 50785 | <p>Multicast key rotation does not work with dot1x clients on bridge mode.</p> <p>Workaround: None.</p> |
| 50787 | <p>Clients are pushed to the wrong vlan of UDR even though SDR and VSA is configured with opmode WPA2-AES and multicast key rotation.</p> <p>Workaround: None.</p> |
| 50850 | <p>Role derivation is not happening correctly with client machine authentication and user-dot1x auth for bridge users. The user is placed in machine authentication role even after successful Machine-auth and user-dot1x authentication.</p> <p>Workaround: None.</p> |
| 50852 | <p>The global user table does not contain any entries for bridge users.</p> <p>Workaround: None.</p> |
| 50899, 51065 | <p>Skinny packets are dropped after a Cisco client roams from one bridge mode VAP to another.</p> <p>Workaround: None.</p> |
| 51290 | <p>In a Spectrum enabled deployment, when a spectrum sensor detects a microwave, the microwave device’s duty cycle will always be displayed as 50 instead of the correct value.</p> <p>Workaround: None.</p> |
| 51361 | <p>CAC resources are not released when the “H” CAC Flag is set and the call is aborted after both clients on the call move out of wifi coverage and then reassociate to the same AP. This occurs even when calls are terminated on the client side.</p> <p>Workaround: None.</p> |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|--------|--|
| 51423 | <p>Setup IPSEC SA -- DONE messages are printed during deletion of ipsec sa when RAP goes down.</p> <p>Workaround: None.</p> |
| 51426 | <p>The DHCP-option introduced in User Derivation Rules for MDAC does not get hit if the client is deauthenticated from the controller end. For example, If an admin deauths the client using the command <code>aaa user delete</code>, the client, which can reauthenticate again, is placed in wrong User-Role after reconnecting.</p> <p>Workaround: If you enable <code>dhcp-enforce</code> option in the AAA profile, the client should be placed in the correct user role upon reconnecting.</p> |
| 51450 | <p>When configured as an Air Monitor, the internal AP on the Aruba 651 does not detect interfering or rogue APs.</p> <p>Workaround: When enabled as an AP, the 651's internal AP detects interfering or rogue APs.</p> |
| 51457 | <p>In a remote-node deployment, the current DNS proxy implementation allows guest user to do lookup on corporate network.</p> <p>Workaround: None.</p> |
| 51458 | <p>False restore does not upload the server certificate when one is present and the error log says certificate is not valid.</p> <p>Workaround: Ensure that the validity period and the controller time are compatible.</p> |
| 51592 | <p>The following CLI commands have no help text:</p> <ul style="list-style-type: none">• <code>source-interface</code>• <code>show ap global</code>• <code>show global-user-table list sort</code>• <code>show memory ap stm</code> <p>Workaround: None. Refer to the <i>ArubaOS 6.1 Command Line Reference Guide</i> for more information about these commands.</p> |
| 51604 | <p>The GCM flag is not shown in the output of the command <code>show datapath tunnel</code>.</p> <p>Workaround: None.</p> |
| 51625 | <p>The IP address for internal GRE tunnel interface on a remote-node controller is not changed after the DHCP pool is changed.</p> <p>Workaround: You must reboot the remote-node controller to the new IP address on the internal GRE tunnel if the DHCP pool is changed.</p> |
| 51650 | <p>When the command <code>apboot all global</code> is executed, any local 651 controllers will be rebooted.</p> <p>Workaround: None.</p> |
| 51691 | <p>DHCP Fingerprinting & Captive Portal cannot be used together.</p> <p>Workaround: None.</p> |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|--------|---|
| 51703 | <p>If an AP is provisioned with fqdn of a master controller and cannot resolve the master's name to IP address because of a wrong dns server or the dns server does not respond, the AP times out and reboots. However, the reboot reason is incorrectly listed as "Could not get a valid ip address for the AP" although the AP does have an IP address.</p> <p>Workaround: None.</p> |
| 51749 | <p>Ping does not work from a WMM client to a non-WMM client.</p> <p>Workaround: None.</p> |
| 51769 | <p>A duplicate remote-node dhcp pool entries added to the mysql database on RNC when it is setup.</p> <p>Workaround: None.</p> |
| 51794 | <p>When mobility is enabled, DHCP packets from wired clients connected on split tunnel ports of RAP are dropped. This does not happen when the client is connected to the RAP for the first but only occurs when the client is unplugged or ages out and attempts to reconnect.</p> <p>Workaround: None. However, the user will eventually come up after some time.</p> |
| 51831 | <p>On a 3200 or 600 Series controller, if the memory is too low during an upgrade a few processes such as cfgm and httpd will be restarted during the upgrade process.</p> <p>Workaround: None.</p> |
| 51872 | <p>When a remote-node is provisioned with uplink receiving IP address from DHCP, if no IP address is obtained, the fpapps will leak memory. Fpapps will become excessively large on memory which will result in a cfgm crash. Eventually, nanny will reboot the machine due to low on free memory.</p> <p>Workaround: None.</p> |
| 51875 | <p>The value of wlsxTrapAPBSSID in wlsxUserEntryAttributesChanged trap is always 0.</p> <p>Workaround: None.</p> |
| 51942 | <p>When media classification feature is enabled in decrypt tunnel (dtunnel) mode for SIPS or TCP 5061 for OCS clients, datapath is unable to set proper TOS for classified voice and video traffic.</p> <p>Workaround: This issue can be avoided by converting the dtunnel mode to tunnel mode and then switching back to dtunnel mode.</p> |
| 51951 | <p>RADIUS authentication for controller mgmt user fails after upgrade.</p> <p>Workaround: Toggle mgmt user authentication on master controller at aaa authentication mgmt.</p> |
| 52107 | <p>After upgrading to 6.1, the default MAC-AUTH Server-group may not appear. If the respective AAA profile is configured for MAC-AUTH, it will fail after the upgrade.</p> <p>Workaround: None.</p> |
| 52190 | <p>A link-local address is not added to the route-cache when configured.</p> <p>Workaround: To add a link-local address, create a new link-local address to overwrite the original.</p> |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|--------|--|
| 52216 | In the WebUI, the Monitoring tab displays the incorrect number of IPv4 clients. Workaround: None. The number of IPv4 clients can be viewed in the CLI. |
| 52361 | Enabling phonehome in the CLI will result in the a <code>command execution failed</code> message, even when it is successful. Workaround: Enable phone via the WebUI. |
| 52414 | The Spectrum feature does not work on IPv6 APs. The APs will remain in AP mode instead of changing to hybrid mode when Spectrum is enabled. Workaround: None. |
| 48533 | WebUI authentication using a certificate succeeds even when a client uses a certificate with a different serial number than is configured. Workaround: Clear your web browser's cache to prevent this. |
| 49914 | A RAP will fail with the error message <code>Setting up DHCP failed</code> if the uplink IP address range changes. Workaround: None. The RAP must be rebooted. |
| 50143 | A RAP is unable to setup EVDO successfully after a failover from a PPPoE link. Workaround: None. |
| 48182 | A remote node will fail to come up even when it has a valid profile associated. The remote node successfully creates an IPSec tunnel but the configuration push fails. Workaround: Remove the whitelist entry associated to the remote node and add it again. |
| 33678 | User statistics are not sent in RADIUS accounting packets for split-tunnel users. Workaround: None |
| 35647 | For wired clients, the authmgr periodically returns an error indicating that the maximum number of retries were attempted and the client is being deauthed. However, the client is not deauthed and connectivity is not affected. Workaround: None. |
| 50220 | SCCP 7921 phones using the G.729 codec for calls result in a high number of down stream delays when compared to the delays from RTCP based calls. Workaround: None. |
| 34635 | If you create a time range policy and apply it to the <code>deny time range</code> in virtual AP with forward mode set to split-tunnel or bridge, the clients are able to connect during the deny time range. Workaround: None. However, if the forward mode is set to tunnel, the client cannot connect as expected. |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|-----------------|--|
| 50315 | For calls from Ascom H323 client to Ascom SIP client, RTP analysis is not performed for the H323 client. But when H323 client receives a call from another SIP or H323 client, RTP analysis is performed. Workaround: None. |
| 32641 | For SSVPN Dynamic Addressed Pairs, IKE SAs are broken when there are multiple maps with the same peer IP and different local-fqdn value. Workaround: Do not have multiple maps with the same peer IP and different local-fqdn value. |
| 38433, 41930 | VIA disconnects when ISAKMP rekey occurs. Workaround: None. However, you can adjust the rekey lifetime using the following commands: For IKE and IPSec: <pre>crypto dynamic-map <name> <priority> set security-association lifetime seconds <seconds></pre> For ISAKMP: <pre>crypto isakmp policy <priority> lifetime <seconds></pre> |
| 48893 | In the WebUI, you cannot edit firewall policy if the policy name has a special character in it. Workaround: You can edit policies with a special character in the name using the CLI. |
| 50307 | An execution of the <code>no mgmt-user</code> command on a remote-node master does not push the configuration change to the remote-node. Workaround: You can recreate the remote-node profile and assign it to the remote-node or you can login to the remote-node and remove the <code>mgmt-user</code> from there. |
| 32665 | The <code>show user</code> command shows the wrong slot/port when a tunneled wired user moves from one tunnel port to another. Workaround: You must use execute the <code>aaa user delete</code> command to update the information. |
| 31098 | The command <code>show auth-tracebuf</code> does not show any information related to RADIUS transactions Workaround: None. |
| 44975 | Currently, APs with no radios count against the AP count for the WIP license despite not implementing any WIP features. Workaround: None. |
| 47868, 47882 | In IPv6, the Name option under <code>netdestination6</code> alias option is not available. Workaround: Complete this configuration using the IP address with the <code>host/network</code> options under the <code>netdestination6</code> alias. |
| 49956 | When a fan fails, a syslog message is not generated. However, SNMP traps are sent properly. Workaround: None. |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|--------|--|
| 39790 | When global user table query output is displayed, users from the internal user table are incorrectly displayed as well. Workaround: None. |
| 33578 | Incorrect information is displayed when the global user table is queried on a local controller. Workaround: None. However, you can execute the <code>show switches</code> or <code>show roleinfo</code> commands to get the same information. |
| 45688 | In a remote-node setup, spanning tree is globally disabled after executing a <code>write erase all</code> . Workaround: Have the spanning-tree command pushed from the profile. |
| 45935 | APs continue to use the IP address they received from DHCP even after the lease has expired in the case of renewal failures. Workaround: None. |
| 47055 | The controller is not proxying the DNS requests OCS clients to the OCS server. Workaround: Manually configure the OCS server address in the OCS tools options. |
| 47893 | ArubaOS does not display DHCP pool usage, specifically the blocks IP addresses currently in use and what is available. Workaround: None. |
| 47988 | If a local controller is a remote-node master and if any remote-nodes have APs terminating on them, the command <code>show ap database</code> on the master or local does not display any information about those APs. Such APs come up with default profiles and unprovisioned; these APs cannot be provisioned. Workaround: This behavior is not currently supported. |
| 37322 | When you export <code>local-userdb</code> , it exports the <code>local-userdb-ap</code> entries also. But when you use <code>local-userdb del-all</code> command it does not delete <code>local-userdb-ap</code> entries. Workaround: None. |
| 38049 | SSL fallback will not work when the controller IP is a DST-NAT address because the controller is not responding to the first IKE packet it receives. Workaround: None. |
| 50047 | Transform ID in <code>ike.pcap</code> should shows incorrect information. It displays Transform ID as UNKNOWN-ESP-TRAN-TYPE instead of the actual transform type. Workaround: None. |
| 44096 | When you try to configure captive-portal profile with a group-name of more than 63 characters you get the following error message: <code>Group name too long. Max allowed length = 63</code> Workaround: None. |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|--------------|--|
| 39542 | <p>If a Cluster-member needs to talk to a cluster-Root across the Internet, the Switch-IP of the Cluster-member be Routable. This is because IKE uses the Switch-IP to initiate IKE SA on the Cluster-member.</p> <p>Workaround: Set the Switch-IP to the IP of a routable VLAN on the master or place a router in front of the Cluster-member.</p> |
| 44171 | <p>The Captive Portal welcome page is shown after authentication even when option enable welcome page option is disabled. This happens when welcome page is configured as some external website.</p> <p>Workaround: None.</p> |
| 45571 | <p>Captive Portal does not work when local controller's loopback IP Address establishes IPSec tunnel with master Controller's vlan ip address instead of Master Controller's loopback IP Address.</p> <p>Workaround: The local controller should establish an IPSec tunnel with the master controller's loopback IP Address.</p> |
| 45386 | <p>Mac clients can not complete IPSec with controller. However, a Windows client can establish IPsec with the controller.</p> <p>Workaround: None.</p> |
| 44152 | <p>It is possible to upload captive portal certificates with an invalid Common Name. When a captive portal user in the initial role tries to access the internet, they will not be able to get to the login page. This only applies to internal captive portal.</p> <p>Workaround: None.</p> |
| 44164 | <p>After captive portal authentication, when user clicks logout button, <code>show user</code> still displays username.</p> <p>Workaround: None.</p> |
| 39730 | <p>With CPsec enables, users cannot use telnet to APs from the LMS controller.</p> <p>Workaround: None.</p> |
| 41134 | <p>When special characters are used as a part of the mobility domain description, the description is not displayed correctly in the WebUI.</p> <p>Workaround: None.</p> |
| 36632, 45416 | <p>ROLE / VLAN Derivation from VSA fails if both MAC Auth and dot1x auth are using same external server.</p> <p>Workaround: None.</p> |
| 50310 | <p>Fingerprinting/UDR does not work for RAP bridge users.</p> <p>Workaround: None.</p> |
| 38772 | <p>Stateful NTLM does not recognize and NTLM logoff and there is no role change.</p> <p>Workaround: None.</p> |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---------------------------|--|
| 43431 | <p>Client blacklisting on 802.1x auth failure does not work if the max-authentication-failures value is set to 2 or greater. However, it will work if the value is set to 1.</p> <p>Workaround: None.</p> |
| 31382, 32466, 44654 | <p>A global authentication profile for wired authentication must be specified for the controller before wired 802.1x authentication on wired port on the RAP is active.</p> <p>Workaround: To configure wired authentication on the controller, make the following configuration change:</p> <pre>config terminal aaa authentication wired profile <name of AAA profile></pre> <p>The AAA profile specified above must support 802.1x authentication.</p> |
| 48996 | <p>The Aruba 600 Series controller configured as a local controller or a remote node is not supported in this release.</p> <p>Workaround: None. However, the Aruba 600 Series controller as a standalone controller is supported.</p> |
| 48220 | <p>EAP-TLS fails when new-eap-termination is enabled.</p> <p>Workaround: None.</p> |
| 49244 | <p>EAP-TLS is not working. The client becomes stuck when the request for authentication is sent.</p> <p>Workaround: None.</p> |
| 49305 | <p>The Aruba 651 does not work in this build and will appear as Inactive in the CLI.</p> <p>Workaround: None.</p> |
| 45460 | <p>If a controller with the maximum amount of AP licenses and more APs than licenses loses connection to some of those APs, the now-freed licenses do not change over to previously inactive, unlicensed APs. Those APs will remain unlicensed and inactive.</p> <p>Workaround: None.</p> |
| 48325 | <p>RAPs over PPPoE crash when the ap-group has split-VAP and a bridge mode wired-AP.</p> <p>Workaround: None.</p> |
| 49282 | <p>A master-local setup and site-to-site VPN configured on the same controller with the site-to-site Peer-IP the same as the Master IP is not supported. This configuration will cause the Isakmpd to operate at 100% and make recovery impossible.</p> <p>Workaround: None.</p> |
| 48077 | <p>MAC address limiting does not work for untrusted port/trusted port with 802.1x authentication.</p> <p>Workaround: None.</p> |
| 36188, 49314 | <p>The AP Wizard in the WebUI becomes stuck for 3 to 4 minutes if the RAP Whitelist contains more than 4000 entries.</p> <p>Workaround: None.</p> |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|--------|---|
| 46332 | The SNMP variable USB Status for RAPs shows 3G mode as active even when the RAP is active only via Ethernet. Workaround: None. |
| 49347 | In a Bridge/Split mobility environment, when a wireless client roams from one AP to another AP, all current sessions will be moved successfully but the second AP will crash shortly after. Workaround: None. |
| 48190 | The upload local file option does not work in the WebUI. Workaround: Use the CLI to upload a local file instead. |
| 47719 | Site-to-site IPsec tunnels (IKEv1 with Suite-B) between an Aruba controller and a Windows device cannot be established in transport mode. Workaround: None. |
| 40759 | Site-to-site VPN with certificates does not work with Dynamic IP. Workaround: None. Currently, you must use a static IP. |
| 47720 | The command <code>show crypto isakmp sa</code> does not use the e-flag when ECDSA certificates are used for authentication. Workaround: None. |
| 45717 | Although two IPv6 nodes are assigned the same link-local address and Duplicate Address Detection works correctly, traffic still flows between them. Workaround: None. |
| 45806 | The ICMPv6 Time Exceeded message is not sent back to the client when the Hop Limit reaches zero (0). Instead, the message ICMPv6 Route Unreachable is returned. Workaround: None. |
| 47667 | Shutting down a port-channel, using the shutdown CLI command, with an IPv6 address configured on it displays an error in the error log. Workaround: None. Although the error is displayed, functionality is not affected and the port-channel is successfully shut down. |
| 47774 | OCSP requests are not being sent when the certificate revocation is rootCA instead of sub-sub-CA, which is the issuer of the certificate. Additionally, the status returned by the OCSP client process to IKE is <code>cert is revoked</code> . Workaround: None. |
| 47697 | When certificate chains in PFX format are loaded, they are not chained correctly by the certmgr during the conversion to PEM. When this happens, IKE fails when these certificate chains are used. Workaround: You must manually chain the certificates. |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|-----------------|--|
| 47674 | <p>The revocation status of each certificate in the certificate chain is not checked against the configured OCSP responder. Instead, the revocation check is only done for the certificate and none in the chain. Even if one certificate is in the chain is revoked, authentication still passes.</p> <p>Workaround: None.</p> |
| 45623 | <p>IPsec SA Rekey Number is displayed as zero (0) instead of reflecting the number of times IPsec SA was rekeyed under IKE_SA.</p> <p>Workaround: None.</p> |
| 47821 | <p>The OCSP revocation check is not performed and the status of the certificate is returned as revoked when the revocation check point is set to intermediate CA.</p> <p>Workaround: None.</p> |
| 47284 | <p>The command <code>show crypto ipsec sa</code> shows a different start-times when executed multiple times.</p> <p>Workaround: None.</p> |
| 47355 | <p>Options for configuring certificate based master-local, master redundancy, and cluster authentication, such as factory certificates or custom-certificates are not available in the WebUI.</p> <p>Workaround: You must use the CLI to configure this type of authentication.</p> |
| 46225 | <p>RAPs and CAPs do not rebootstrap immediately upon receiving an ICMP port unreachable message (<code>asap_gre_err: Received ICMP (DEST_UNREACH, PROT_UNREACH)</code>) from the controller. Instead the AP will become stuck in the same state for approximately ten (10) minutes.</p> <p>Workaround: None.</p> |
| 47204 | <p>RADIUS Interim Accounting updates are sent with an extra delay depending on the frequency configured. For example:</p> <ul style="list-style-type: none">If Interim stats frequency = 60 seconds, the delay is ~4 seconds.If Interim stats frequency = 120 seconds, the delay is ~8 seconds.If Interim stats frequency = 180 seconds, the delay is ~10 seconds. <p>Workaround: None.</p> |
| 47156 | <p>RADIUS Interim Accounting updates are shown as active in the authtrace-buf even after the interim accounting has been disabled. However, no actual updates are sent to the accounting server.</p> <p>Workaround: Executing the command <code>aaa user delete <client></code> will correct this.</p> |
| 47278 | <p>IPsec map names containing spaces are not saved after the controller is rebooted.</p> <p>Workaround: None.</p> |
| 46924, 47104 | <p>The Aruba 651 cannot be used in a Master-Local set up on this version of ArubaOS. Doing so will cause the device to become unresponsive and requires a hard reboot.</p> <p>Workaround: None.</p> |

Table 1 *Known Issues and Limitations (Continued)*

| Bug ID | Description |
|-----------------|--|
| 47866, 47879 | During initial bring up, the Aruba 651 returns a large number of errors and becomes unresponsive. Workaround: None. |
| 47538 | During image upgrade and reload of the Aruba 600 Series, some times the controller hangs after the step <code>Reading configuration from default.cfg</code> . Workaround: None. |

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



CAUTION

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

Topics in this chapter include:

- “Important Points to Remember” on page 43
- “Technical Upgrading Best Practices” on page 44
- “WIP Configuration Changes in Version 6.0” on page 44
- “Basic Upgrade Sequence” on page 45
- “Managing Flash Memory” on page 46
- “Before you upgrade” on page 46
- “Licensing Change History and Mapping” on page 47
- “Upgrading from 5.0.x to 6.1” on page 49
- “Upgrading from 3.3.x or 3.4.x to 6.1” on page 49
- “Upgrading from RN-3.x.x to 6.1” on page 53
- “Upgrading in a Multi-Controller Network” on page 53
- “Downgrading after an Upgrade” on page 54
- “Controller Migration” on page 56
- “Before You Call Technical Support” on page 57



NOTE

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 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.

WIP Configuration Changes in Version 6.0

New configuration parameters were added in ArubaOS 6.0. When you upgrade from an ArubaOS version prior to 6.0 to ArubaOS 6.1, 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 versions prior to 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 were deprecated in ArubaOS 6.0. 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 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 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



CAUTION

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

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 6.1

- The VIA feature now requires a PEFV license (Policy Enforcement Firewall Virtual Private Network).
- The Walled Garden feature requires the PEFNG or PEFV license.
- Advanced Cryptography License (ACR) is introduced—the ACR license is required for the Suite B Cryptography in IPsec and 802.11 modes. License enforcement behavior controls the total number of concurrent connections (IPsec or 802.11) using Suite B Cryptography.

ACR Interaction

- On a platform that supports 2048 IPsec tunnels, the maximum number of Suite B IPsec tunnels supported is 2048, even if a larger capacity license is installed.
- An evaluation ACR license is available (EVL-ACR-8192). You can install the ACR evaluation license with a higher capacity than the platform maximum.
- On a platform that supports 2048 IPsec tunnels, with a LIC-ACR-512 installed, only 512 IPsec tunnels can be terminated using Suite B encryption. An additional 1536 IPsec tunnels, using non-Suite B modes (e.g. AES-CBC), can still be supported.
- On a platform with LIC-ACR-512 installed, a mixture of IPsec and 802.11i Suite B connections can be supported. The combined number of these sessions may not exceed 512.
- A single client using both 802.11i Suite B and IPsec Suite B simultaneously will consume two ACR licenses.

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

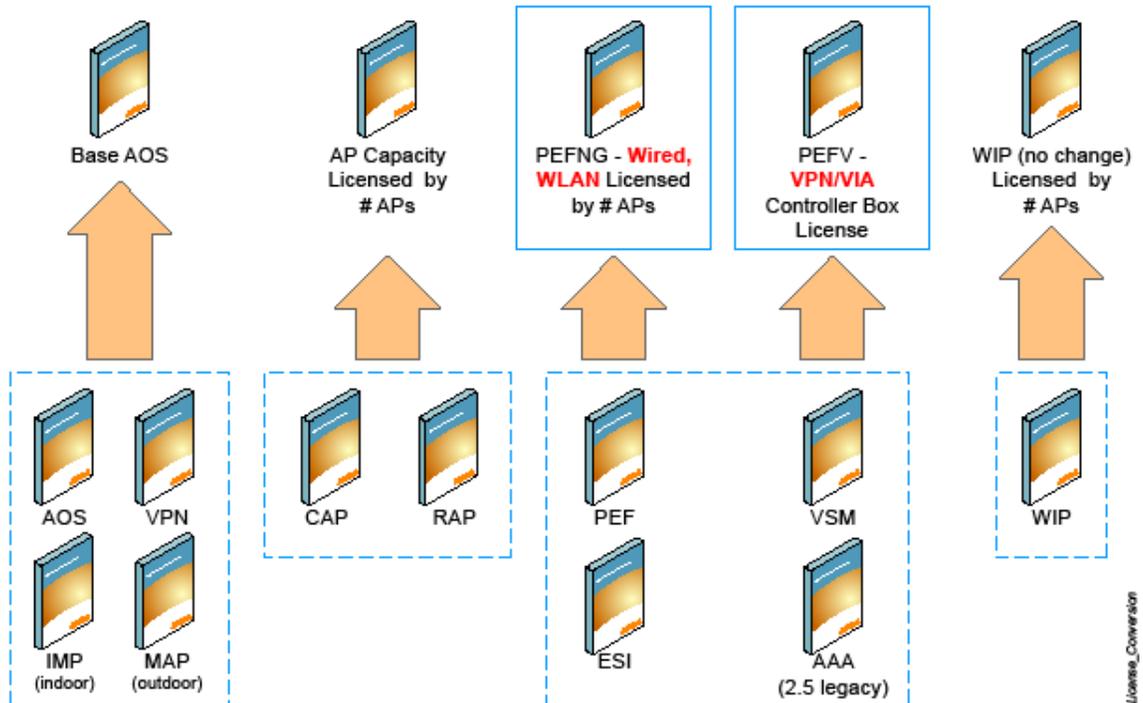
ArubaOS Legacy and End-of-Life

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



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 6.1

The procedure to upgrade from 5.0.x to 6.1 is nearly identical to the procedure to upgrade from 3.4.x to 6.1, with a single change. If you are upgrading from 5.0.x to 6.1, 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 6.1.

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 6.1 User Guide*.



When upgrading from ArubaOS 5.0.x to ArubaOS 6.1.x, control plane security configurations will be maintained.

Upgrading from 3.3.x or 3.4.x to 6.1



Upgrading from ArubaOS 3.3.x or 3.4.x to ArubaOS 6.1 requires an “upgrade hop”. That is, you must first upgrade from ArubaOS 3.3.x or ArubaOS 3.4.x to ArubaOS 6.0.1. Then upgrade from ArubaOS 6.0.1 to ArubaOS 6.1



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.

Read all the following information before you upgrade to ArubaOS 6.1.

- “Caveats” on page 50

- “Load New Licenses” on page 50.
- “Save your Configuration” on page 50.
- “Install ArubaOS 6.1” on page 50

Caveats

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

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

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

Load New Licenses

Before you upgrade to ArubaOS 6.1, assess your software license requirements and load any new or expanded licenses you require prior to upgrading to ArubaOS 6.1.

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.



If you need to downgrade to ArubaOS 3.4.x, the previous licenses will be restored. However, once you upgrade again to ArubaOS 6.1 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 46). 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 6.1

If you are upgrading from a release older than ArubaOS 6.0.1, you must first upgrade to the most recent version of ArubaOS 6.0.1 and then upgrade to ArubaOS 6.1

Minimum Installation Requirements



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



When upgrading the software in a multi-controller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence. (See “Upgrading in a Multi-Controller Network” on page 53.)



When upgrading the controller, the following is required:

- Confirm (`show memory`) that there is at least 40 MB of free memory available. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up upgrade immediately.
 - Confirm (`show storage`) that there is at least 85 MB of /flash available.
 - If less flash space is available run the `dir` command to list all files. Delete all unnecessary files including crash files, logs.tar file or a previous failed download image. To ensure that all temporary (crash) files are removed perform a `tar crash` and then remove the `crash.tar` file from the controller.
-

Install ArubaOS 6.1 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. Make sure the controller you want to upgrade is currently running ArubaOS 6.0.1. If not, you must upgrade to ArubaOS 6.0.1 first.
2. Download the latest ArubaOS 6.1 software image from the Aruba Customer Support website.
3. Upload the new software image to a PC or workstation on your network.
4. Log in to the WebUI from the PC or workstation.
5. 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.
6. Make sure you upgrade the partition that is currently running ArubaOS 6.0.1. To see the current boot partition, navigate to the **Maintenance > Controller > Boot Parameters** page.
7. Select **Yes** for Reboot Controller After Upgrade.
8. Click **Upgrade**.
9. 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).
10. 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 6.1 in the CLI

Follow these steps to upgrade a controller to ArubaOS version 6.1 using the CLI.

1. Make sure your controller is currently running ArubaOS 6.0.1.
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. Make sure to load the new software onto the partition that is currently running ArubaOS 6.0.1. Use the following command to check the partitions:

```
#show image version
-----
Partition           : 0:0 (/dev/hda1) **Default boot**
Software Version    : ArubaOS 6.0.1 (Digitally Signed - Production Build)
Build number        : 20219
Label               : 20219
Built on            : 2011-02-11 20:51:46 PST
-----
Partition           : 0:1 (/dev/hda2)
/dev/hda2: Image not present
```

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

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 0
or
(host) # copy tftp: <tftphost> <image filename> system: partition 0
```



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 6.1.0.0 (Digitally Signed - Production Build)
Build number        : 28106
Label               : 28106
Built on            : Wed Mar 09 09:11:59 PST 2011
-----
Partition           : 0:1 (/dev/hda2)
/dev/hda2: Image not present
```

6. Reboot the controller:

```
(host) # reload
```

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

```
(host) #show version
Aruba Operating System Software.
ArubaOS (MODEL: 3200-US), Version 6.1.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-03-09 at 09:11:59 PDT 6.1.0.0 (Digitally Signed - Production Build)
...
```

Upgrading from RN-3.x.x to 6.1

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 6.1.



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 or 3.4.x to 6.1”](#) on page 49 to complete your last “upgrade hop”.

Caveat

Should you need to downgrade from ArubaOS 6.1, you can only downgrade to version RN-3.1.4 or higher.

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 46.



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

To upgrade an existing multi-controller system to ArubaOS 6.1:

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 a, the upgrade script encrypts the internal database. Any new entries that were created in ArubaOS 6.1 will be lost after downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).

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

```
#show image version
-----
Partition           : 0:0 (/dev/hda1)
Software Version    : ArubaOS 3.4.1.2 (Digitally Signed - Production Build)
Build number        : 20219
Label               : 20219
Built on            : 2010-12-11 20:51:46 PST
-----
Partition           : 0:1 (/dev/hda2) **Default boot**
Software Version    : ArubaOS 6.1.0.0 (Digitally Signed - Production Build)
Build number        : 28106
Label               : 28106
Built on            : 2011-03-09 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, 3000 Series, 600 Series
- PPC Controllers—200, 800, 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 and verify that your new controller supports the ArubaOS version you are migrating to.

Migration instructions include:

- [“Single Controller Environment” on page 56](#)
- [“Multiple Master Controller Environment” on page 56](#)
- [“Master/Local Controller Environment” on page 56](#)

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 accessible 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.

