


# ArubaOS 7.4.0.1



Release Notes

## Copyright Information

© 2014 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. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site

[http://www.arubanetworks.com/open\\_source](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.

---

<b>Contents</b>	<b>3</b>
<b>Release Overview</b>	<b>7</b>
Supported Browsers	7
Related Documents	7
Contacting Support	7
<b>What's New in this Release</b>	<b>9</b>
New Features and Enhancements	9
Layer 2 and Layer 3 Features	9
Route Monitoring	9
IGMPv3 Snooping	9
Support for Static Address Resolution Protocol	9
Security Enhancements	9
Enhancements to web-server Command	9
Session ACLs on RVI	10
Deny Inter-User Traffic	10
Enhancements to Netdestination Alias	10
Branch Features	10
Support for IP NAT Outside	10
Support for Dynamic Domain Name Server Client	10
Support for Myonlineportal.net	11
Aruba VPN Tunnel	11
Distributed, L3 DHCP Scopes	11
NAT Pools	11
VPN Survivability	11
Default Route to VPN	11
Multiple Default Gateway Support	12

---

Access Point Integration Features .....	12
Configurable Rogue AP Containment .....	12
Dynamic Port Reconfiguration .....	12
Platform Features .....	12
Resolved Issues .....	13
AirWave/Activate .....	13
Base OS Security .....	13
Configuration .....	14
DPA .....	14
IPSec .....	14
Layer 2 Forwarding .....	15
Multicast .....	15
RADIUS .....	15
Routing .....	16
Stacking .....	16
Switch-Datapath .....	17
Switch-Platform .....	17
WebUI .....	17
Known Issues and Limitations .....	18
Base OS Security .....	18
Central .....	19
Configuration .....	19
DHCP .....	20
DHCP Snooping .....	20
Data Path Agent (DPA) .....	20
Dynamic ARP Inspection (DAI) .....	20
Generic Routing Encapsulation (GRE) .....	21
Interface .....	21
IPsec .....	21

---

IPv6 .....	22
Layer 2 Forwarding .....	22
Multicast .....	22
OSPF .....	23
Port-Channel .....	23
QoS .....	23
Routing .....	24
Security .....	25
SNMP .....	26
Stacking .....	26
STP .....	26
Switch-Datapath .....	27
Switch-Platform .....	27
WebUI .....	29
Issues Under Investigation .....	29
Layer 2 Forwarding .....	29
Stacking .....	29
System .....	29
<b>Upgrade Procedures .....</b>	<b>31</b>
Important Points to Remember .....	31
Installing the FIPS Version of ArubaOS 7.4.0.1 .....	31
Before Installing FIPS Software .....	31
Before You Upgrade .....	31
Save Your Configuration .....	32
Saving the Configuration in the WebUI .....	32
Saving the Configuration in the CLI .....	32
Upgrading to ArubaOS 7.4.0.1 .....	32
Upgrading from the WebUI .....	32
Upgrading from the Command Line Interface .....	33

---

Upgrading from your USB using the LCD .....	33
Downgrading after an Upgrade .....	34
Before You Call Your Support Provider .....	35

ArubaOS 7.4.0.1 is a patch release that introduces new features, fixes to issues identified in the previous ArubaOS releases, and outstanding known issues and limitations in the current release. For details on all the features supported on Mobility Access Switch, see the [Related Documents](#) section.

This release note contains the following chapters:

- [What's New in this Release on page 9](#) describes the new features, fixes, known issues, and enhancements introduced in this release.
- [Upgrade Procedures on page 31](#) covers the procedures for upgrading a Mobility Access Switch to ArubaOS 7.4.0.1.

## Supported Browsers

The following browsers are officially supported for use with the ArubaOS 7.4.0.1 WebUI:

- Microsoft Internet Explorer 9.x and 10.x on Windows XP, Windows Vista, Windows 7, and Windows 8
- Mozilla Firefox 17 or higher on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.1.7 or higher on MacOS

## Related Documents

The following documents are part of the complete documentation suite for the Aruba Mobility Access Switch:

- *ArubaOS 7.4 User Guide*
- *ArubaOS 7.4 Command Line Reference Guide*
- *ArubaOS 7.4 Quick Start Guide*
- *Aruba S3500 Series Mobility Access Switch Installation Guide*
- *Aruba S2500 Series Mobility Access Switch Installation Guide*
- *Aruba S1500 Series Mobility Access Switch Installation Guide*

## Contacting Support

**Table 1:** *Contact Information*

Website Support	
Main Site	<a href="http://arubanetworks.com">arubanetworks.com</a>
Support Site	<a href="http://support.arubanetworks.com">support.arubanetworks.com</a>
Airheads Social Forums and Knowledge Base	<a href="http://community.arubanetworks.com">community.arubanetworks.com</a>
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200

Website Support	
International Telephone	<a href="http://www.arubanetworks.com/support-services/support-program/contact-support">http://www.arubanetworks.com/support-services/support-program/contact-support</a>
Software Licensing Site	<a href="https://licensing.arubanetworks.com/">https://licensing.arubanetworks.com/</a>
End of Support Information	<a href="http://www.arubanetworks.com/support-services/end-of-life-products/">http://www.arubanetworks.com/support-services/end-of-life-products/</a>
Security Incident Response Team (SIRT)	<a href="http://www.arubanetworks.com/support-services/security-bulletins/">http://www.arubanetworks.com/support-services/security-bulletins/</a>
<b>Support Email Addresses</b>	
Americas, EMEA, and APAC	<a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a>
Security Incident Response Team (SIRT)	<a href="mailto:sirt@arubanetworks.com">sirt@arubanetworks.com</a>



## New Features and Enhancements

New features in the following categories are introduced in ArubaOS 7.4:

- [Layer 2 and Layer 3 Features on page 9](#)
- [Security Enhancements on page 9](#)
- [Branch Features on page 10](#)
- [Access Point Integration Features on page 12](#)
- [Platform Features on page 12](#)

### Layer 2 and Layer 3 Features

This release of ArubaOS provides support for the following Layer 2 and Layer 3 features:

#### Route Monitoring

Starting from ArubaOS 7.4, Mobility Access Switch provides support for Route Monitoring. Route Monitoring enables the Mobility Access Switch to monitor the L3 uplink status using ping probe. Ping probe destined to a server IP address is sent on the uplink interface which is under monitoring. Based on the status of ping reply, probe status of the interface is updated to up or down. When the probe status of the interface is down, the Mobility Access Switch removes the interface host and network routes from the routing table. When the probe status of the interface is up, interface host and network routes are added back.



---

By default Route Monitoring is disabled on the Mobility Access Switch.

---

For more information on configuring Route Monitoring, see *ArubaOS 7.4 User Guide*.

#### IGMPv3 Snooping

The Mobility Access Switch provides support for IGMPv3 snooping starting from ArubaOS 7.4. IGMPv3 Snooping is used to snoop the membership reports that have group records of different types. These group records specify the source specific Multicast (SSM) traffic for a particular group.

IGMP Snooping is configured as a profile under vlan-profile and is attached to a VLAN. By default, v3 snooping is disabled and v2 snooping is enabled in an igmp-snooping profile. A new configuration command is introduced to enable v3 snooping explicitly.

For more information on IGMPv3 Snooping, see *ArubaOS 7.4 User Guide*.

#### Support for Static Address Resolution Protocol

Starting from ArubaOS 7.4, you can add a static Address Resolution Protocol entry on the Mobility Access Switch. You can configure a static ARP entry using the CLI. For more information, see *ArubaOS 7.4 User Guide*.

### Security Enhancements

This release of ArubaOS provides support for the following Security Enhancements:

#### Enhancements to web-server Command

As part of [CVE-2014-3566](#) security vulnerabilities and exposures, **SSLv3** transport layer security is disabled from ArubaOS 7.4.0.1.



Clients exclusively using SSLv3 will fail to access Captive Portal or Mobility Access Switch WebUI. It is recommended to use TLSv1, TLSv1.1, or TLSv1.2 transport layer security.

To address this, the following changes are introduced under the **web-server ssl-protocol** command.

Parameter	Description	Range	Default
ssl-protocol tls tls1 tls1.1 tls1.2	Specifies the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol version used for securing communication with the web server: <ul style="list-style-type: none"><li>• TLS v1</li><li>• TLS v1.1</li><li>• TLS v1.2</li></ul>	—	tls1 tls1.1 tls1.2

### Session ACLs on RVI

Starting from ArubaOS 7.4, you can apply session ACLs on a routed VLAN interface (RVI) of the Mobility Access Switch. For more information on configuring session ACLs on RVI, see *ArubaOS 7.4 User Guide*.

### Deny Inter-User Traffic

Starting from ArubaOS 7.4, Mobility Access Switch provides support for Deny Inter-user Traffic. Deny Inter-user Traffic feature enables Mobility Access Switches to block the communication between users with the same role. For example, an organization can block communication between any two guest users. If the role has voip-profile configured, then the traffic across the VoIP users is also denied.



The inter-user traffic denial happens only within an ArubaStack and does not span across multiple Mobility Access Switches or ArubaStack.

By default this feature is disabled. You can configure Deny Inter-user Traffic for a maximum of seven user-roles (including CPPM downloaded roles) on a per user-role basis. For more information on configuring Deny Inter-User Traffic, see *ArubaOS 7.4 User Guide*.

### Enhancements to Netdestination Alias

Starting from ArubaOS 7.4, a new netdestination alias, **localip** is introduced in the Mobility Access Switch. This is a system-defined alias which can be used as a destination alias for all the local IP addresses defined in the Mobility Access Switch.

### Branch Features

This release of ArubaOS provides support for the following portfolio integration features:

#### Support for IP NAT Outside

Starting from ArubaOS 7.4, Mobility Access Switch provides support for IP NAT outside on egress VLAN interface. The IP NAT outside feature changes the source IP of all the egressing packets to the IP of the egress VLAN interface. You can configure IP NAT outside using the CLI. For more information on configuring IP NAT Outside, see *ArubaOS 7.4 User Guide*.

#### Support for Dynamic Domain Name Server Client

Starting from ArubaOS 7.4, Mobility Access Switch provides support for Dynamic DNS Client. The Dynamic DNS Client enables a Mobility Access Switch to update its DHCP assigned IP address with a Dynamic DNS service provider. This helps to keep the remote devices reachable without tracking their IP address. For more information on DDNS configuration, see *ArubaOS 7.4 User Guide*.

## Support for Myonlineportal.net

Starting from ArubaOS 7.4.0.1, Mobility Access Switch extends support for the **myonlineportal.net** dynamic DNS server in addition to the other servers supported in ArubaOS 7.4.

## Aruba VPN Tunnel

The Mobility Access Switch at the branch acts as the VPN endpoint and the controller at the datacenter acts as the VPN concentrator. When a Mobility Access Switch is set up for VPN, it forms an IPsec tunnel to the controller to secure sensitive corporate data. IPsec authentication and authorization between the controller and the Mobility Access Switches is based on the RAP whitelist configured on the controller.



---

You can configure an Aruba VPN tunnel either manually or through Zero Touch Provisioning (ZTP).

---

For more information on ZTP VPN and manual configuration of Aruba VPN Tunnel, see *ArubaOS 7.4 User Guide*.

## Distributed, L3 DHCP Scopes

Starting from ArubaOS 7.4, Mobility Access Switch allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically. This release of Mobility Access Switch provides support for Distributed, L3 DHCP scope.

In Distributed L3 mode, DHCP server resides in the local branch on the Mobility Access Switch and each branch location is assigned a dedicated subnet. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server is configured with a unique subnet.

For more information on configuring Distributed L3, DHCP Scope, see *ArubaOS 7.4 User Guide*.

## NAT Pools

Starting from ArubaOS 7.4, Mobility Access Switch provides support for NAT pools to protect private IPs of trusted servers behind the switch. It also gives the flexibility to support source NAT and dual NAT without using the switch IP. NAT actions can be performed only on packets processed by software. Support for applying session ACLs on RVI enables software processing of the packets that require a NAT action.

For more information on configuring NAT pools, see *ArubaOS 7.4 User Guide*.

## VPN Survivability

The Mobility Access Switch provides support for a standby VPN uplink when the primary VPN uplink interface goes down. Whenever the primary uplink is detected to be down, the standby uplink is used to establish VPN.

For more information on configuring VPN Survivability, see *ArubaOS 7.4 User Guide*.

## Default Route to VPN

Starting from ArubaOS 7.4, a crypto map matching all destinations can be used for customer applications that require all client generated traffic (Internet and Corporate bound) to be sent over a VPN tunnel. A branch office Mobility Access Switch has VPN tunnel which terminates on a Firewall. Any client non-corporate traffic from Mobility Access Switch is forwarded to the firewall through the VPN tunnel. This requires a default gateway route on Mobility Access Switch pointing to a VPN tunnel.

For more information Default Route to VPN, see *ArubaOS 7.4 User Guide*.

## Multiple Default Gateway Support

Default gateway is the route configured on the Mobility Access Switch to reach the upstream network. Starting from ArubaOS 7.4, Mobility Access Switch allows you to configure multiple default gateways using the metric option introduced in the CLI. Gateway with lower metric takes precedence when more than one gateways exist to a given upstream network. The second gateway with higher metric takes over when the first route is down.

For more information on multiple Default gateway support, see *ArubaOS 7.4 User Guide*

## Access Point Integration Features

This release of ArubaOS provides support for the following portfolio integration features:

### Configurable Rogue AP Containment

Starting from ArubaOS 7.4, the Mobility Access Switch allows you to configure the rogue AP containment using the CLI. This was enabled by default and was not configurable in ArubaOS 7.3.x versions.

You can now enable or disable rogue AP containment and configure the action to be taken on the list of MAC addresses received from IAP that are detected as rogue. The default action is to shut down the access port and PoE on which it is detected and to discard the MAC address of the rogue AP and blacklist it if detected on a trunk port.

This feature is enabled by default. For more information on configuring Rogue AP Containment, see *ArubaOS 7.4 User Guide*.

### Dynamic Port Reconfiguration

Starting from ArubaOS 7.4, Mobility Access Switch dynamically configures an interface based on the type of device connected to it. It uses LLDP to detect the type of device connected to an interface and applies a device-group configuration (a set of predefined configuration) on the interface based on the device-type.



---

In this release, the Mobility Access Switch provides support only for the device-type and Aruba APs that support Aruba's proprietary LLDP TLVAP device-group.

---

This feature is disabled by default. For more information on reconfiguring ports dynamically, see *ArubaOS 7.4 User Guide*.

## Platform Features

This release of ArubaOS provides support for the following platform feature enhancements:

- DAC support on S1500 (GE Only)
- 10GBASE-ER SFP+
  - 40km over SMF
- 10GBASE-ZR SFP+
  - 80km over SMF

## Resolved Issues

This section lists the issues that are resolved until ArubaOS 7.4.0.1:

### AirWave/Activate

**Table 2:** *Fixed AirWave/Activate Issues*

Bug ID	Description	Fixed in
108372	<b>Symptom:</b> The AirWave details obtained through DHCP options (60 and 43) were not retained by a Mobility Access Switch after a reload. <b>Scenario:</b> This issue was observed in Mobility Access Switches running ArubaOS 7.3 or later versions when in factory default settings.	7.4.0.1

### Base OS Security

**Table 3:** *Fixed Base OS Security Issues*

Bug ID	Description	Fixed in
105743	<b>Symptom:</b> A Mobility Access Switch crashed and rebooted due to a synchronization issue with the AAA user table. <b>Scenario:</b> This issue was not limited to any specific Mobility Access Switch model or release version.	7.4.0.1
105890	<b>Symptom:</b> The administrators were unable to login to the Mobility Access Switch using the console for a brief period. The logs indicated that the kernel killed an internal process with the following out of memory message:  <b>nanny[1345]: &lt;303093&gt; &lt;ERRS&gt;   nanny   Out Of Memory handler killed process /mswitch/bin/aaa_proxy:1380 due to low memory. Set 1</b> <b>Scenario:</b> This issue was not limited to any specific Mobility Access Switch model or release version.	7.4.0.1
107099	<b>Symptom:</b> The log operator applied on an ACL was not effective when the ACL was applied to a Routed VLAN interface. <b>Scenario:</b> This issue was not limited to any specific Mobility Access Switch model or release version.	7.4.0.1
85582	<b>Symptom:</b> Quate CMS cross site scripting (XSS) vulnerabilities were noticed in the system. This issue is resolved by upgrading OpenSSL and Apache HTTP. <b>Scenario:</b> This issue was not limited to any specific Mobility Access Switch model or release version.	7.4

## Configuration

**Table 4:** *Fixed Configuration Issues*

Bug ID	Description	Fixed in
106082	<b>Symptom:</b> The CLI did not process a command that exceeded 252 characters. This issue is fixed by increasing the maximum command-line character limit to 512. <b>Scenario:</b> This issue was not limited to any specific Mobility Access Switch model or release version.	7.4.0.1
93768	<b>Symptom:</b> Multiple mirroring profiles creation was not allowed. This issue is resolved by allowing creation of multiple mirroring profiles. However, at a given time, only one mirroring profile can be applied to different interfaces. <b>Scenario:</b> This issue was not limited to a specific Mobility Access Switch model or release version.	7.4
94375	<b>Symptom:</b> Authenticated clients were unable to pass traffic causing a network outage. This issue is resolved by clearing the user table. <b>Scenario:</b> This issue was observed when MAC address of the uplink interface was learnt on untrusted interface. This issue was observed on Mobility Access Switches running ArubaOS 7.3.2.1	7.4

## DPA

**Table 5:** *Fixed Data Path Agent Issues*

Bug ID	Description	Fixed in
99566	<b>Symptom:</b> The DPA process crashed on the Mobility Access Switch. <b>Scenario:</b> This issue occurred when a user pressed the MODE button on the front panel of the Mobility Access Switch during the boot process. This issue was observed in S1500-12P model running ArubaOS 7.3.0.1 or earlier versions.	7.4

## IPSec

**Table 6:** *Fixed IPSec Issues*

Bug ID	Description	Fixed in
85235	<b>Symptom:</b> Traffic outage occurred when re-keying of the VPN tunnel failed. This issue is resolved by enabling the NAT-T option in configuration because traffic is across WAN. <b>Scenario:</b> This issue was observed in a WAN deployment where VPN tunnel was established and re-keying of the tunnel was set to be executed every hour. However, VPN tunnel failed to re-key after every 6 to 8 hours causing traffic outage. But at the next re-key interval (after one hour), the re-keying was successful and allowed traffic.	7.4

## Layer 2 Forwarding

**Table 7:** *Fixed Layer 2 Forwarding Issues*

Bug ID	Description	Fixed in
107450	<b>Symptom:</b> The process handling layer 2 functions crashed when the Mobility Access Switch received LLDP BPDUs with System Description exceeding 256 bytes. <b>Scenario:</b> This issue was observed in Mobility Access Switches running ArubaOS 7.4.	7.4.0.1

## Multicast

**Table 8:** *Fixed Multicast Issues*

Bug ID	Description	Fixed in
93220	<b>Symptom:</b> Domain login takes unusually long time when the traffic goes through tunnel node. This issue was resolved by changing the configuration to use TCP instead of UDP so that the server does not expect packets in sequence. <b>Scenario:</b> This issue was observed when the kerb client was connected to tunneled node port, and the client sent packets exceeding tunnel MTU. This issue was not limited to any specific Mobility Access Switch model or release version.	7.4

## RADIUS

**Table 9:** *Fixed RADIUS Issues*

Bug ID	Description	Fixed in
107183	<b>Symptom:</b> The following debug message was incorrectly reported in the error logs of the Mobility Access Switch as the accounting messages were incorrectly sent for the unauthenticated users: <b>An internal system error has occurred at file rc_acct.c print</b> <b>Scenario:</b> This issue was observed in Mobility Access Switches running ArubaOS 7.3.2.1 or later versions when interim accounting was enabled in the AAA profile.	7.4.0.1

## Routing

**Table 10:** *Fixed Routing Issues*

Bug ID	Description	Fixed in
109727	<p><b>Symptom:</b> A Mobility Access Switch failed to respond to ARP requests for an IP used in a NAT pool even though <b>session-processing</b> was enabled on the uplink VLAN.</p> <p><b>Scenario:</b> This issue was observed when a session ACL was applied on a VLAN that had a source NAT configured from a NAT pool. This issue was limited to Mobility Access Switches running ArubaOS 7.4.</p>	7.4.0.1
109920	<p><b>Symptom:</b> The following error message was displayed on a Mobility Access Switch when executing any layer 3 command in the CLI: <b>Module Layer3 Manager is busy. Please try later</b> The message logs indicated that the module handling the layer 3 functions had crashed.</p> <p><b>Scenario:</b> The crash occurred when a default OSPF route or a router IP that conflicted with the tunnel destination IP was advertised through GRE over VPN tunnel. This issue was observed in Mobility Access Switches running ArubaOS 7.3 or later versions.</p>	7.4.0.1

## Stacking

**Table 11:** *Fixed Stacking Issues*

Bug ID	Description	Fixed in
94551	<p><b>Symptom:</b> The output of <b>show stacking members</b> command displayed more than 8 members with valid member IDs even though Mobility Access Switch supports only up to 8 members in an ArubaStack. This issue is resolved by ensuring that a maximum of 8 members are only allowed in an ArubaStack.</p> <p><b>Scenario:</b> This issue was observed when more than 8 members were added to the ArubaStack. This issue was not specific to any Mobility Access Switch model or release version.</p>	7.4
95855	<p><b>Symptom:</b> The Primary member of a 5 member ArubaStack rebooted due to memory leak.</p> <p><b>Scenario:</b> The issue occurred when LLDP was enabled in the ArubaStack. This issue was limited to ArubaStack with S3500 Mobility Access Switches running ArubaOS 7.3.0 or later.</p>	7.4
103518	<p><b>Symptom:</b> The Mobility Access Switch displayed the <b>Module Layer 2 manager is busy</b> error message on issuing any CLI command.</p> <p><b>Scenario:</b> This issue occurred during a system switchover or Layer 2 Module (L2M) process restart. This issue was observed in Mobility Access Switches running ArubaOS 7.3.2.2 or earlier versions.</p>	7.4



## Switch-Datapath

**Table 12:** *Fixed Switch-Datapath Issues*

Bug ID	Description	Fixed in
97002	<b>Symptom:</b> The Mobility Access Switch dropped packets when the traffic rate was high on the egress port due to insufficient port buffer. <b>Scenario:</b> The issue was not limited to any specific Mobility Access Switch model or release version.	7.4

## Switch-Platform

**Table 13:** *Fixed Switch-Platform Issues*

Bug ID	Description	Fixed in
98030	<b>Symptom:</b> A stack member stopped responding and rebooted. <b>Scenario:</b> The log files for the event suggested multiple link flaps. Due to this, the Chassis Manager (CM) process missed keep-alives and removed the stack member from the ArubaStack. This issue was observed in Mobility Access Switches running ArubaOS 7.2.2.2. <b>NOTE:</b> This issue was caused due to a cabling problem at the customer site.	N/A
89131 95757 104999	<b>Symptom:</b> Crash file was unavailable for a crash due to kernel panic. This issue is resolved by adding the watchdog and Non Maskable Interrupt (NMI) support. <b>Scenario:</b> This issue occurred because of synchronization problems in the panic routine. This issue was not limited to a specific Mobility Access Switch model or release version	7.4
99562	<b>Symptom:</b> The Mobility Access Switch stopped detecting SFP/SFP+ transceivers when they were plugged out and inserted back in, or replaced. <b>Scenario:</b> This issue was observed in Mobility Access Switches running ArubaOS 7.3.1.0 or earlier versions.	7.4

## WebUI

**Table 14:** *Fixed WebUI Issues*

Bug ID	Description	Fixed in
105975	<b>Symptom:</b> <b>Copy Backup</b> option in WebUI did not redirect to the <b>Copy files</b> page after upgrading the Mobility Access Switch from ArubaOS 7.2 to 7.3.2.2. <b>Scenario:</b> This issue occurred when ArubaOS was upgraded to 7.3 or later versions on the Mobility Access Switches.	7.4.0.1
104261	<b>Symptom:</b> The <b>Allowed VLAN</b> field under the <b>Configuration &gt; Ports &gt; Switching</b> tab was inaccessible through the WebUI of the Mobility Access Switch. <b>Scenario:</b> This issue occurred when the Mobility Access Switch was upgraded from ArubaOS 7.3.1.0 to ArubaOS 7.3.2.0. This issue was observed in Mobility Access Switches running ArubaOS 7.3.2.0 or later versions.	7.4

## Known Issues and Limitations

The following are known issues and limitations observed in ArubaOS 7.4.0.1. Bug IDs and applicable workarounds are included.

### Base OS Security

**Table 15:** *Known Base OS Security Issues and Limitations*

Bug ID	Description
74264	<p><b>Symptom:</b> A combination of CPPM and Windows Radius server for fail-through is not supported.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model or release version.</p> <p><b>Workaround:</b> Use either CPPM servers as Primary and Backup or Windows Radius as Primary and Backup. Do not combine them.</p>
87971	<p><b>Symptom:</b> The Mobility Access Switch IP is programmed as the loopback IP automatically when there is no <b>ip-cp redirect address</b> configured. If <b>ip-cp redirect address</b> is configured and saved in the config, either system switchover or reload is invoked. After switchover or reload the configured <b>ip-cp redirect address</b> is lost. The IP address displays all 0s.</p> <p><b>Scenario:</b> This issue occurs only when the <b>ip cp-redirect-address&lt;ip-addr&gt;</b> command is configured on Mobility Access Switches running ArubaOS 7.3.</p> <p><b>Workaround:</b> If the <b>ip-cp redirect address</b> command is explicitly configured and it is lost after reload or switchover, configure the <b>ip cp-redirect-address&lt;ip-addr&gt;</b> command once again and save it.</p>
90067	<p><b>Symptom:</b> A ClearPass Policy Manager (CPPM) <b>Downloadable Role</b> may not be properly assigned to a Mobility Access Switch user if it is not correctly configured in CPPM.</p> <p><b>Scenario:</b> This issue occurs when the Mobility Access Switch is still processing the invalid <b>Downloadable Role</b> and an administrator has already modified the <b>Downloadable Role</b> in CPPM. This issue occurs on Mobility Access Switches running ArubaOS 7.3.</p> <p><b>Workaround:</b> Ensure that the role definition syntax is correct in CPPM. This can be verified by testing the configuration on a test switch before configuring the role details in CPPM. If that is not possible and a <b>Downloadable Role</b> has been incorrectly defined, wait for the Mobility Access Switch to complete processing the invalid role (~3 minutes), delete the user(s) assigned to that role, update the role definition in CPPM and re-trigger authentication.</p>
100904	<p><b>Symptom:</b> When a client successfully authenticated by MAC and/or dot1x authentication fails reauthentication, it remains in the authenticated VLAN even after it moves back to the previous role.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model or release version.</p> <p><b>Workaround:</b> Delete the failed user entry manually.</p>
101489	<p><b>Symptom:</b> When an authenticated client fails reauthentication after an EAP-start, it remains in the previously authenticated role and VLAN.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model or release version.</p> <p><b>Workaround:</b> Delete the failed user entry manually.</p>

## Central

**Table 16:** *Known Central Issues and Limitations*

Bug ID	Description
102328	<p><b>Symptom:</b> When the Mobility Access Switch is in managed mode, the configuration received or sent from Aruba Central are not processed and applied properly, if the size of running-config file exceeds 150KB.</p> <p><b>Scenario:</b> This issue occurs when the Mobility Access Switch has a large number of profile configuration defined and managed by Aruba Central. This issue is observed on a standalone Mobility Access Switch running ArubaOS 7.3.2 or later versions.</p> <p><b>Workaround:</b> None.</p>
104181	<p><b>Symptom:</b> Users are unable to configure the Mobility Access Switch from the console for 5 to 10 mins after it loses connection from Aruba Central.</p> <p><b>Scenario:</b> This issue occurs when the Mobility Access Switch in Managed mode abruptly disconnects from Aruba Central. This issue is observed on a standalone Mobility Access Switch running ArubaOS 7.3.2.2 or later versions.</p> <p><b>Workaround:</b> None.</p>

## Configuration

**Table 17:** *Known Configuration Issues and Limitations*

Bug ID	Description
55306	<p><b>Symptom:</b> User is unable to delete the characters using the backspace key when the admin username is as long as the maximum characters.</p> <p><b>Scenario:</b> This issue is observed when the admin username reaches the maximum limit (32 characters). This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> Press enter key and type the username again.</p>
99871	<p><b>Symptom:</b> Sometimes, the user prompt does not appear on the Mobility Access Switch console after a reload.</p> <p><b>Scenario:</b> This issue is observed only when a Mobility Access Switch running ArubaOS 7.4 is reloaded.</p> <p><b>Workaround:</b> Press any key to proceed with the login.</p>
101284	<p><b>Symptom:</b> The local IP address of the NTP servers are displayed as 0.0.0.0 when executing the <b>show ntp servers</b> command after rebooting the Mobility Access Switch. This occurs because the NTPD is not refreshed with the switch IP address.</p> <p><b>Scenario:</b> This issue is observed only when a Mobility Access Switch running ArubaOS 7.3 or later version is rebooted.</p> <p><b>Workaround:</b> Remove and reconfigure the NTP servers.</p>
101943	<p><b>Symptom:</b> Users cannot configure the banner MOTD text using the <b>banner motd</b> command in the same line.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model or release version.</p> <p><b>Workaround:</b> Enter the banner text to be configured with a delimiter in a new line after the <b>banner motd</b> keyword.</p>

## DHCP

**Table 18:** *Known DHCP Issues and Limitations*

Bug ID	Description
104220	<b>Symptom:</b> The Mobility Access Switch leases out an IP address which is used by another client. <b>Scenario:</b> This issue is observed when the DHCP server pool on the Mobility Access Switch has only one IP address to offer. This issue is not limited to any specific Mobility Access Switch model or release version. <b>Workaround:</b> None.

## DHCP Snooping

**Table 19:** *Known DHCP Snooping Issues and Limitations*

Bug ID	Description
87131	<b>Symptom:</b> When a line card member of an ArubaStack is individually rebooted, the DHCP Snooping bindings for that particular member switch are lost. <b>Scenario:</b> Reloading a line card does not trigger repopulating the DHCP Snooping database. However, the DHCP Snooping database repopulates in case of a stack or box reload. This issue occurs on Mobility Access Switches running ArubaOS 7.3. <b>Workaround:</b> None.

## Data Path Agent (DPA)

**Table 20:** *Known DPA Issues and Limitations*

Bug ID	Description
98845	<b>Symptom:</b> The DPA process crashes on the Mobility Access Switch. <b>Scenario:</b> This issue is observed when the DPA process waits for an acknowledgment from the SOS process and times out. This issue is observed in Mobility Access Switches running ArubaOS 7.3.0.1 or later versions. <b>Workaround:</b> None.

## Dynamic ARP Inspection (DAI)

**Table 21:** *Known DAI Issues and Limitations*

Bug ID	Description
91146	<b>Symptom:</b> An ACL matching on ARP traffic for specific source and destination pairs may not always be enforced. <b>Scenario:</b> This issue is observed only when Dynamic ARP Inspection (DAI) is enabled on the Mobility Access Switch and is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> Disable DAI when using ACLs matching on ARP for specific source and destination pairs.

## Generic Routing Encapsulation (GRE)

**Table 22:** *Known GRE Issues and Limitations*

Bug ID	Description
87459 88968	<b>Symptom:</b> L3 GRE tunnel interfaces toggles between up and down states. <b>Scenario:</b> This issue occurs when the L3 GRE tunnel forwarding rate exceeds 40 Kilo packets per second (Kpps). This issue occurs in Mobility Access Switches running ArubaOS 7.3. <b>Workaround:</b> None.

## Interface

**Table 23:** *Known Interface Issues and Limitations*

Bug ID	Description
85529	<b>Symptom:</b> Issuing <b>show port stats</b> command displays increasing <b>InputErrorBytes</b> count when connected to Aruba AP-135 but does not appear to have any connectivity issues. <b>Scenario:</b> The errors are due to Maximum Transmission Unit (MTU) probe packets sent by the AP-135. This issue is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> The errors do not impact the performance of the Mobility Access Switch or the AP-135. Ignore the errors.

## IPsec

**Table 24:** *Known IPsec Issues and Limitations*

Bug ID	Description
73261	<b>Symptom:</b> Site-to-site IPsec VPN with transport-mode is not functioning correctly. <b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model or release version. <b>Workaround:</b> None.
94073	<b>Symptom:</b> The IKE gets deleted when the Mobility Access Switch is used as a NAT box. <b>Scenario:</b> This issue is observed when the <b>session-idle-timeout</b> value was less than the DPD timer value. This issue is not limited to any specific Mobility Access Switch model or release version. <b>Workaround:</b> Use the <b>crypto-local isakmp dpd idle-timeout &lt;idle_sec&gt;</b> command to reduce the DPD time to a value lower than the <b>session-idle-timeout</b> value configured under the <b>firewall</b> command.
103560	<b>Symptom:</b> The <b>crypto isakmp pre-shared key</b> does not accept special characters to establish an IKE session. <b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model or release version. <b>Workaround:</b> None.

## IPv6

**Table 25:** *Known IPv6 Issues and Limitations*

Bug ID	Description
57529	<p><b>Symptom:</b> Copy on IPv6 address does not work as this command is not recognized for IPv6. As a result, the scp/ftp/tftp copy over IPv6 address will not work.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> Use an IPv4 address instead of an IPv6 or use the WebUI and try the local file management.</p>

## Layer 2 Forwarding

**Table 26:** *Known Layer 2 Forwarding Issues and Limitations*

Bug ID	Description
68312	<p><b>Symptom:</b> DHCP Offer/ACK messages are not discarded when using DHCP Trust .</p> <p><b>Scenario:</b> This issue is observed when <b>no trust DHCP</b> is enabled in a port- security profile and a MAC ACL with a <b>permit any any rule</b> is applied to an interface. This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> Use a stateless ACL instead of a MAC ACL.</p>
73285	<p><b>Symptom:</b> The Mobility Access Switch does not register a GVRP VLAN on the STP blocked ports.</p> <p><b>Scenario:</b> This issue occurs when there is a change in the STP topology and the blocked ports become forward. The ports first register the VLAN and then the data traffic flow continues. Under these conditions, there is a long delay in resuming the traffic.</p> <p><b>Workaround:</b> None.</p>
109561	<p><b>Symptom:</b> A disruption in the network traffic is sometimes observed in an ArubaStack. Users may also see the following error message when executing any layer 2 CLI command:</p> <p><b>Module Layer 2 manager is busy</b></p> <p><b>Scenario:</b> This issue occurs if a stack member disconnects and re-joins the ArubaStack when spanning tree is enabled. This issue is observed in an ArubaStack running ArubaOS 7.3.x or later versions.</p> <p><b>Workaround:</b> None.</p>

## Multicast

**Table 27:** *Known Multicast Issues and Limitations*

Bug ID	Description
63951	<p><b>Symptom:</b> As IPv6 on untrusted port is not supported in this release, Multicast Listener Discovery (MLD) snooping on untrusted port is ignored. Hence, MLD snooping membership table cannot be formed.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> None.</p>
65314	<p><b>Symptom:</b> The Mobility Access Switch does not send query when there is a change in the Spanning Tree Protocol (STP) topology. This delays the formation of the MLD snooping membership table.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> None.</p>
77185	<p><b>Symptom:</b> IGMP Snooping entries are removed in 12 seconds before expiry of the age-out timer.</p>

**Table 27:** *Known Multicast Issues and Limitations*

Bug ID	Description
	<p><b>Scenario:</b> This issue is observed when mutlicast stream is sent over 40Kpps on a L2 GRE tunnel. This issue is not limited to any specific Mobility Access Switch version.</p> <p><b>Workaround:</b> Send multicast stream less than 40 Kpps over a L2 GRE tunnel.</p>

## OSPF

**Table 28:** *Known OSPF Issues and Limitations*

Bug ID	Description
59609	<p><b>Symptom:</b> Layer 3 Manager utilizes more memory and throws an error message during the removal of large number of OSPF routes.</p> <p><b>Scenario:</b> This issue is observed in S3500 running Aruba 7.2.0.0.</p> <p><b>Workaround:</b> None.</p>
59738	<p><b>Symptom:</b> Loss of traffic is observed on some advertised OSPF routes.</p> <p><b>Scenario:</b> This issue is observed when it reaches the route capacity limitation (1500). This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> None.</p>

## Port-Channel

**Table 29:** *Known Port-Channel Issues and Limitations*

Bug ID	Description
104770	<p><b>Symptom:</b> Connectivity to devices across port channel results in extended request time out when the member port status is changed.</p> <p><b>Scenario:</b> This issue is observed under the following configuration setup:</p> <ul style="list-style-type: none"> <li>On Mobility Access Switch, configure port channel in LACP mode.</li> <li>On Cisco switch, configure port channel.</li> <li>Configure the link between the two devices as a trunk link.</li> </ul> <p>This issue is observed in S2500 running ArubaOS 7.3.2.1.</p> <p><b>Workaround:</b> None.</p>

## QoS

**Table 30:** *Known QoS Issues and Limitations*

Bug ID	Description
79774	<p><b>Symptom:</b> The Mobility Access Switch does not apply QoS remarking or prioritization for traffic in an L2 GRE tunnel.</p> <p><b>Scenario:</b> A QoS profile configured on the interface of the Mobility Access Switch does not prioritize traffic in an L2-GRE tunnel traversing through the same interface. This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> None.</p>

## Routing

**Table 31:** *Known Routing Issues and Limitations*

Bug ID	Description
84327	<p><b>Symptom:</b> Traffic continues to be routed even though the ingress Routed Virtual Interface (RVI) is administratively shutdown.</p> <p><b>Scenario:</b> If any Layer 3 unicast traffic is received destined to an RVI that is in an administratively down state, the RVI will route the unicast traffic towards destination even though it is shutdown. This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> None.</p>
74123	<p><b>Symptom:</b> With Source NAT enabled, no matter what MTU value is assigned to the RVI, packets up to 1784 bytes will be source NAT'ed. Packets larger than this are dropped on the ingress RVI because fragmentation is not supported. Additionally, no matter what MTU is configured, packets leaving the egress RVI are not fragmented.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model or release version.</p> <p><b>Workaround:</b> None.</p>
103209	<p><b>Symptom:</b> The routing table sometimes contains routes for the reserved multicast IP addresses of IGMPv3.</p> <p><b>Scenario:</b> This issue is observed when L3 GRE tunnel is configured with OSPF routing protocol. This issue is limited to Mobility Access Switches running ArubaOS 7.4</p> <p><b>Workaround:</b> None.</p>
105540	<p><b>Symptom:</b> The peer IP route configured in the crypto map points to the default gateway even though a static route is configured for the peer IP.</p> <p><b>Scenario:</b> This issue is limited to Mobility Access Switches running ArubaOS 7.4</p> <p><b>Workaround:</b> Configure a higher metric on the VLAN interface through which the peer IP is reachable.</p>
105550	<p><b>Symptom:</b> Sometimes, the connected routes on a VLAN interface may not appear in the routing table after a switchover.</p> <p><b>Scenario:</b> This issue is observed when the VLAN interface with a dynamic IP address is configured on a port channel. This issue is observed on Mobility Access Switches running ArubaOS 7.4.</p> <p><b>Workaround:</b> None.</p>
110596	<p><b>Symptom:</b> The following error message appears when executing the command, <b>clear ip ospf process</b> on the Mobility Access Switch:</p> <p><b>Module Layer 3 Manager is busy. Please try later</b></p> <p><b>Scenario:</b> The issue occurs if the command is executed when a default OSPF route or a router IP that conflicts with the tunnel destination IP is advertised through GRE over VPN tunnel. This issue is observed in Mobility Access Switches running ArubaOS 7.3 or later versions.</p> <p><b>Workaround:</b> None.</p>



## Security

**Table 32:** *Known Security Issues and Limitations*

Bug ID	Description
64356	<p><b>Symptom:</b> Router Advertisement (RA) messages are not dropped on untrusted interfaces.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> None.</p>
67157	<p><b>Symptom:</b> If a phone connected to a Mobility Access Switch port using 802.1X MD5 authentication experiences an Extensible Authentication Protocol (EAP) transaction failure, the Mobility Access Switch sends an EAP-Fail packet every 5 seconds after the failure until the phone restarts 802.1X authentication.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> None.</p>
67159	<p><b>Symptom:</b> If a phone connected to a Mobility Access Switch port using 802.1X authentication and the AAA profile bound to the interface has a user-derivation rule associated with it, the phone may exchange multiple EAP transactions with the Mobility Access Switch, but may not be able to complete the 802.1X authentication.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> Remove the <b>user-derivation-rule</b> from the AAA profile.</p>
82617	<p><b>Symptom:</b> When Captive Portal authentication is provided by ClearPass Guest, instead of assigning a <b>Downloadable Role</b> with Captive Portal redirect, the user gets the default Captive Portal user role defined in the Captive Portal settings.</p> <p><b>Scenario:</b> The issue was observed when the user table has two L3 entries for a same MAC. This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> Delete both the stale and valid user entry and perform Captive Portal authentication again.</p>
84802	<p><b>Symptom:</b> A Cisco® IP phone that is assigned a user-role via a device-type User Derivation Rule (UDR) and also 802.1X authenticated (UDR user-role overrides 802.1X user-role), shows the authentication type as <b>Web</b> as opposed to <b>802.1X-Wired</b> after a switchover of the primary and secondary ArubaStack members.</p> <p><b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> The <b>show user ip &lt;A.B.C.D&gt;</b> command incorrectly displays <b>Web</b> under the <b>Auth</b> column for a Cisco IP phone connected to the Mobility Access Switch. However, the switch assigns the correct role to the Cisco IP phone.</p>
85674	<p><b>Symptom:</b> For some IP phones, the <b>show station-table</b> command entry displays the MAC or 802.1X default authentication role of the AAA profile. However, the <b>show user-table</b> command entry displays the initial role of the AAA profile.</p> <p><b>Scenario:</b> This issue occurs when an IP phone connected to one of the ports of the Mobility Access Switch, gets an IP address before an L2 authentication completes. This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> None.</p>
85682	<p><b>Symptom:</b> When 802.1X authentication is configured with Extensible Authentication Protocol (EAP) termination, even if the user gets black-listed it is still able to re-attempt authentication prior to the black-list timer expiring.</p> <p><b>Scenario:</b> This issue is observed when 802.1X authentication with EAP termination type is set to <b>eap-tls</b> and <b>inner-eap-type</b> is set to EAP-General Token Type (GTC). This issue is not limited to any specific Mobility Access Switch model.</p> <p><b>Workaround:</b> None.</p>

## SNMP

**Table 33:** *Known SNMP Issues and Limitations*

Bug ID	Description
82812	<b>Symptom:</b> SNMP may not respond temporarily due to a process crash. <b>Scenario:</b> This issue is observed while issuing an SNMP GetNext on the ipNetToMediaTable. This issue occurs in Mobility Access Switch running 7.2.0.0 or later and not limited to any specific model. <b>Workaround:</b> None.

## Stacking

**Table 34:** *Known Stacking Issues and Limitations*

Bug ID	Description
92339	<b>Symptom:</b> Multicast packets in an S1500 ArubaStack are rate limited to 40kpps when IGMP-snooping is enabled on a Rendezvous Point interface. <b>Scenario:</b> This issue is limited to S1500 ArubaStack where PIM-Sparse Mode and IGMP-Snooping are enabled on the ArubaStack and affects clients that are not on the same member as that of the interface connecting to the Rendezvous Point. <b>Workaround:</b> None.

## STP

**Table 35:** *Known STP Issues and Limitations*

Bug ID	Description
57519	<b>Symptom:</b> With Spanning Tree loopguard enabled, an interface will enter LOOP_Inc state if that interface is not receiving any more BPDU. <b>Scenario:</b> When the situation happens, restart L2M daemon (such as doing stacking primary failover) may mistakenly bring the interface back to DES/FWD state. <b>Workaround:</b> Check your network when an interface enters LOOP_Inc state. Resolve your network problem before doing stacking primary failover or L2M restart. <b>NOTE:</b> A typical problem that causes an interface not to receive BPDU happens on the fiber connection in which TX is successful but RX fails.
91798	<b>Symptom:</b> After multiple recoveries on a BPDU guard enabled interface, BPDU guard may take a long time to trigger the shutdown operation on the interface. <b>Scenario:</b> This issue is observed when a Mobility Access Switch or a connected downstream hub/switch is looped upon itself and if BPDU guard is enabled on the connected interfaces. This issue is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> None.
92327	<b>Symptom:</b> In an MSTP topology, the interfaces of the Mobility Access Switches may go into an STP boundary state if the STP mode is manipulated. <b>Scenario:</b> This issue is observed if the STP Mode is manually changed from MSTP to PVST and then changed back to MSTP in any one of the Mobility Access Switches connected in a spanning tree environment. This issue is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> Remove the MSTP instance from VLAN mapping and add it back.

## Switch-Datapath

**Table 36:** *Known Switch-Datapath Issues and Limitations*

Bug ID	Description
58584	<b>Symptom:</b> When an AP is connected to a Mobility Access Switch through a mid-span PoE injector, auto negotiation might fail. <b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> Force link speed on the ports.

## Switch-Platform

**Table 37:** *Known Switch-Platform Issues and Limitations*

Bug ID	Description
52196	<b>Symptom:</b> Press 'q' to abort does not work after issuing the <b>ping interval &lt;delay_pkts&gt; &lt;host&gt;</b> command. <b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> None.
65618	<b>Symptom:</b> The Mobility Access Switch does not synchronize with a Network Time Protocol (NTP) server. <b>Scenario:</b> This issue is observed when a NTP server entry is configured prior to configuring or changing the IP address of the egress Routed Virtual Interface (RVI) which is used to contact said NTP server. This issue is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> First configure the IP address the RVI and then configure the NTP server address.
65807	<b>Symptom:</b> When you create an <b>eth</b> ACL with <b>permit any</b> , apply the ACL to a user-role, and send IPv6 traffic to untrusted port, the Mobility Access Switch did not create an L2 user nor forward the IPv6 traffic. ArubaOS 7.3 does not support IPv6 on untrusted port. <b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> None.
68091	<b>Symptom:</b> An interface is operationally down. <b>Scenario:</b> This issue occurs when an Ethernet OAM failure may still transmit data and other control packets. <b>Workaround:</b> Enable STP on the interface or configure the link as a port-channel member.
86723	<b>Symptom:</b> Copying files from any source to an external USB flash drive or the local flash drive using the CLI does not show the transfer progress and there is no option to abort the transfer. <b>Scenario:</b> This issue is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> None.
86853	<b>Symptom:</b> Copying a raw image from a USB connected to the primary stack member copies the image only on primary and not all stack members. <b>Scenario:</b> This issue occurs on Mobility Access Switches running ArubaOS 7.3. <b>Workaround:</b> None.
86857	<b>Symptom:</b> Users cannot exit from Quick-Setup in the CLI using CTRL+C. <b>Scenario:</b> This issue is observed in an ArubaStack when the console port is redirected from a secondary or line card member. This issue is not limited to any specific Mobility Access Switch model. <b>Workaround:</b> Connect the console port to the primary member of the ArubaStack if using Quick-Setup.
90167	<b>Symptom:</b> AP-220 Series and AP-130 Series may not get powered up when connected to a Mobility Access Switch.

**Table 37:** *Known Switch-Platform Issues and Limitations*

Bug ID	Description
	<p><b>Scenario:</b> This issue is observed when both ethernet ports of the access point are connected to the PoE ports of the same Mobility Access Switch. This issue is limited to PoE models of Mobility Access Switch.</p> <p><b>Workaround:</b> Remove the <b>poe-profile</b> (i.e. disable PoE) from one of the two ports of the Mobility Access Switch that are connected to the access point.</p>
90231	<p><b>Symptom:</b> Cisco IP phones utilizing pre-standard PoE (also known as legacy power) may lose power after being operational for a long time.</p> <p><b>Scenario:</b> This issue is limited to PoE models of the Mobility Access Switch.</p> <p><b>Workaround:</b> Disconnect the phone for a few minutes and reconnect it.</p>
99827	<p><b>Symptom:</b> Sometimes, the following I2C error messages are observed in the output of <b>show log system</b> command due to an internal processor issue:</p> <ul style="list-style-type: none"> <li>• <b>Mar 4 08:22:17 KERNEL: 2:i2c_xls_wait_for_idle: i2c line is busy (status: 0003)</b></li> <li>• <b>Mar 4 08:22:17 KERNEL: 2:Unable to select i2c mux channel 6</b></li> <li>• <b>Mar 4 08:22:17 KERNEL: 2:Hard reset to i2c mux on bus 0 address 0x70</b></li> <li>• <b>Mar 4 08:22:17 KERNEL: 2:Unable to access hw sensor on bus 9 address 0x2d</b></li> </ul> <p><b>Scenario:</b> This issue is very rarely observed and is not limited to any specific Mobility Access Switch model or release version.</p> <p><b>Workaround:</b> Reload the box.</p>
103600	<p><b>Symptom:</b> Uplink port status LED remains in <b>On</b> state even after the link is locally shutdown with 1G SFP.</p> <p><b>Scenario:</b> This issue is observed only when a 7205 Mobility Controller is connected to the uplink port of the Mobility Access Switch.</p> <p><b>Workaround:</b> None.</p>
103713	<p><b>Symptom:</b> Kernel panic is observed in the tar logs of one of the members of the ArubaStack.</p> <p><b>Scenario:</b> This issue is observed when an IGMPv2 client joins and disconnects from a group where IGMPv3 is enabled. This issue is limited to ArubaStack running ArubaOS 7.4.</p> <p><b>Workaround:</b> None.</p>
103793	<p><b>Symptom:</b> All APs associated to a Mobility Access Switch goes down, and the system status LED on the Mobility Access Switch turns blinking amber indicating a major alarm.</p> <p><b>Scenario:</b> This issue is observed during lightening, thunder storm, or if another PSE is providing inline power to the Mobility Access Switch. This issue is observed in S2500 and S1500-24/48P Mobility Access Switches running ArubaOS 7.2.2 or earlier versions.</p> <p><b>Workaround:</b> Upgrade the Mobility Access Switch to ArubaOS 7.3.2.1 to benefit from many PoE features introduced in this release version.</p>
105354	<p><b>Symptom:</b> A Mobility Access Switch stops responding and reboots. The log files for the event listed the reason as <b>Hard Watchdog Reset</b>.</p> <p><b>Scenario:</b> This issue is observed in S3500 running ArubaOS 7.3.1.0.</p> <p><b>Workaround:</b> None.</p>

## WebUI

**Table 38:** *Known WebUI Issues and Limitations*

Bug ID	Description
106087	<b>Symptom:</b> Copying an image using TFTP from the WebUI does not upgrade the image on an ArubaStack. <b>Scenario:</b> This issue occurs only when the TFTP copy is tried from the WebUI for an ArubaStack running ArubaOS 7.3.x or later versions. <b>Workaround:</b> Copy the image using the <b>copy tftp</b> command in the CLI.
107809	<b>Symptom:</b> The following error message appears when downloading logs from the Mobility Access Switch using the WebUI: <b>can't query: TimeoutError: DOM Exception 23</b> <b>Scenario:</b> This issue occurs only when Safari is used as the browser for the WebUI. This issue is limited to Mobility Access Switches running ArubaOS 7.4 or later versions. <b>Workaround:</b> Use browsers such as Google Chrome or Mozilla Firefox to access the WebUI.

## Issues Under Investigation

The following are the issues observed in ArubaOS 7.4.0.1 and are under investigation. The associated Bug IDs are included.

### Layer 2 Forwarding

**Table 39:** *Layer 2 Forwarding Issues Under Investigation*

Bug ID	Description
110300	<b>Symptom:</b> Mobility Access Switches connected with certain Aruba Access Points lose connectivity to the controller when ArubaOS is upgraded on the controller. The message logs indicate that the process handling layer 2 functions has crashed.

### Stacking

**Table 40:** *Stacking Issues Under Investigation*

Bug ID	Description
99121	<b>Symptom:</b> Error octets are seen in Received Statistics (Rx counters) on the stack ports of S2500 and S3500 Mobility Access Switches.

### System

**Table 41:** *System Issues Under Investigation*

Bug ID	Description
102268	<b>Symptom:</b> The uplink on an S3500 Mobility Access Switch running ArubaOS 7.3.1 is occasionally not responding.



This chapter details the Mobility Access Switch software upgrade procedures. To optimize your upgrade experience and ensure a successful upgrade, read all the information in this chapter before upgrading and follow all the procedures carefully.

Topics in this chapter include:

- [Important Points to Remember on page 31](#)
- [Installing the FIPS Version of ArubaOS 7.4.0.1 on page 31](#)
- [Before You Upgrade on page 31](#)
- [Save Your Configuration on page 32](#)
- [Upgrading to ArubaOS 7.4.0.1 on page 32](#)
- [Downgrading after an Upgrade on page 34](#)
- [Before You Call Your Support Provider on page 35](#)

## Important Points to Remember

You should create a permanent list of the following information for future use:

- Best practice is to upgrade during a maintenance window. This will limit the troubleshooting variables.
- 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).
- Always upgrade the non-boot partition first. If something happens during upgrade, you can switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- If you have removed the default stacking interfaces (ports 0/1/2 and 0/1/3) from 7.0.x but plan to use them for stacking purposes after upgrading to ArubaOS 7.3, you must reconfigure them for stacking.

## Installing the FIPS Version of ArubaOS 7.4.0.1

Download the FIPS version of the software from <https://support.arubanetworks.com>.

### Before Installing FIPS Software

Before you install a FIPS version of software on a Mobility Access Switch that is currently running a non-FIPS version of the software, you must reset the configuration to the factory default or you will not be able to login to the CLI or WebUI. Do this by running the **write erase** command just prior to rebooting the Mobility Access Switch. This is the only supported method of moving from non-FIPS software to FIPS software.

## Before You Upgrade

Run the following checklist before installing a new image on the Mobility Access Switch:

- Ensure that you have at least 60 MB of free flash space (**show storage** command).
- Run the tar crash command to ensure that there are no “process died” files clogging up memory and FTP/TFTP the files to another storage device. To clean up any crash core file, use the tar clean crash command.
- Remove all unnecessary saved files from flash (**delete filename** command).

## Save Your Configuration

Before upgrading, save your configuration and back up your Mobility Access Switch data files. Saving your configuration will retain 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 either the enable or configuration mode:

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

## Upgrading to ArubaOS 7.4.0.1

Read all the following information before you upgrade. Download the latest software image from the Aruba Customer Support web site.

There are three ways to upgrade your software image:

- [Upgrading from the WebUI on page 32](#)
- [Upgrading from the Command Line Interface on page 33](#)
- [Upgrading from your USB using the LCD on page 33](#)



If you are upgrading from 7.0.x to 7.3 and are going to create a stack, each Mobility Access Switch in the stack must be upgraded to ArubaOS 7.3 before forming the stack.

### Upgrading from the WebUI

The following steps describe how to install the Aruba software image from a PC or workstation using the WebUI on the Mobility Access Switch. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Upload the new software image to a PC or workstation on your network.
2. Log in to the WebUI from the PC or workstation.
3. Navigate to the **Maintenance > Image Management** page. Select the **Upgrade using local file** option, then click **Browse** to navigate to the image file on your PC or workstation.
4. Determine which partition will be used to hold the new software image. Best practice is to load the new image onto the non-boot partition. To see the current boot partition, navigate to the **Maintenance > Boot Parameters** page.
5. Select **Yes** in the **Reboot after upgrade** field to reboot after upgrade.
6. Click **Upgrade Image**. The image, once copied to the ArubaStack primary, will be pushed down to every stack member.
7. When the software image is uploaded to the Mobility Access Switch, a popup appears. Click **OK** to reload the entire stack. The boot process starts automatically within a few seconds.
8. When the boot process is complete, log in to the WebUI and navigate to the **Monitoring > Summary** page to verify the upgraded code version.
9. Select the **Configuration** tab.
10. Click **Save Configuration** at the top of the screen to save the new configuration file header.



## Upgrading from the Command Line Interface

The following steps describe how to install the ArubaOS software image using the CLI on the Mobility Access Switch. You need a FTP/TFTP server reachable from the Mobility Access Switch you are upgrading.

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

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



---

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

---

3. Determine which partition to load the new software image. Best practices is to load the new image onto the backup partition (the non-boot partition). To view the partitions, use the show image version command.
4. Use the copy command to load the new image onto the Mobility Access Switch. The image, once copied to the stack Primary, will be pushed down to every stack member:

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

or

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



---

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

---

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

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

6. Reload the entire stack:

```
(host) # reload
```

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

```
(host) #show version member all
```

8. Execute the **write memory** command to save the new configuration file header.

## Upgrading from your USB using the LCD



If you are upgrading from ArubaOS 7.0.2.0 to ArubaOS 7.1.0.0 or greater, you cannot upgrade from an external USB device using the LCD screen. Use either the WebUI or the CLI to complete your upgrade.

The Mobility Access Switch is equipped with an LCD panel that displays a variety of information about the status of the Mobility Access Switch and provides a menu that allows you to do basic operations such as initial setup and reboot. The LCD panel displays two lines of text.

Use the upper right **Menu** button to navigate through LCD functions and the lower right **Enter** button to select (or enter) an LCD function. The active line, in the LCD panel, is indicated by an arrow.

Use a USB device to transfer the upgrade image:

1. Create a folder named **arubaimage** on your USB device.
2. Using your laptop, copy the new image from the support site to your USB device's folder **arubaimage**.



---

You must download the new image to the **arubaimage** folder or the image will not properly upload to the Mobility Access Switch.

---

3. Insert your USB device into the rear USB port (next to the console port) of your Mobility Access Switch.

4. Press the **Menu** button until you reach the **Maintenance** function.
5. Press the **Enter** button to enter the maintenance function.
6. Press the **Enter** button at **Upgrade Image** function.
7. Press the **Menu** button to locate the partition you want to upgrade.

```
partition 0
partition 1
```

Then press the **Enter** button to select the partition to upgrade.




---

Always upgrade the non-boot partition first. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.

---

8. Press the Enter button again to confirm the partition you are upgrading (or press the Menu button to exit).

```
y: Enter button
n: Menu button
```

9. The LCD displays an a upgrade in process acknowledgement:

```
Upgrading...
```

When the upgrade is complete, the LCD displays the message:

```
Reload to boot from new image
```




---

When loading a software image, the specified partition automatically becomes active (default boot partition) the next time the Mobility Access Switch is rebooted. There is no need to manually select the partition.

---

10. From the command line, execute **show image version member all** to view the partitions:

11. Issue the following command to reload the stack:

```
(host) # reload
```

12. Execute the **show version member all** command to verify if the reload and upgrade is complete.

```
(host) #show version member all
```

13. Execute the **write memory** command to save the new configuration file header.

After completing the upgrade, your system will create a configuration file called **default.cfg.<timestamp>**. This file is your configuration at the time of upgrade. Another file called **default.cfg** is created, which is your configuration post-upgrade.

## Downgrading after an Upgrade

If necessary, you can roll-back to the previous version of ArubaOS on your Mobility Access Switch using the procedure given below.

Note the following points before downgrading ArubaOS:

- Save your configuration file before and after completing your downgrade
- MSTP will be disabled upon downgrading.

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

1. Set the Mobility Access Switch to boot with the previously-saved configuration file. By default, ArubaOS creates a file called **original.cfg** upon upgrade. This file can be used instead of a previously-saved configuration file in case you did not save your configuration before upgrade.
2. Use the **dir** command to confirm your saved configuration files or **original.cfg**.

```
(host) #dir
-rw-r--r-- 1 root root 3710 Nov 7 14:35 default.cfg
-rw-r--r-- 2 root root 3658 Nov 7 14:35 default.cfg.2011-11-07_1
-rw-r--r-- 2 root root 3658 Nov 7 14:35 original.cfg
```

3. Use the boot **config-file <filename>** command to select the configuration file you will boot from after downgrading.  

```
(host)#boot config-file original.cfg
```
4. Confirm that you have selected the correct file using the **show boot** command.  

```
(host)#show boot
Config File: original.cfg
Boot Partition: PARTITION 0
```
5. Set the Mobility Access Switch to boot from the system partition that contains the previously running image.
6. Execute the **write memory** command after the downgrade to save your configuration

## Before You Call Your Support Provider

Before you place a call to Technical Support, follow the steps listed below:

1. Provide a detailed network topology (including all the devices in the network between the user and the Mobility Access Switch with IP addresses and Interface numbers if possible).
2. Provide the Mobility Access Switch logs and output of the **show tech-support** command.
3. Provide the syslog file of the Mobility Access Switch at the time of the problem.  
Best practices strongly recommends that you consider adding a syslog server if you do not already have one to capture from the Mobility Access Switch.
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 Mobility Access Switch) or any recent changes to your Mobility Access Switch 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 the Mobility Access Switch site access information, if possible.

