Aruba Central On-Premises 2.5.8.0

Release Notes

a Hewlett Packard
Enterprise company

Copyright Information

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America.

Contents

Revision History

The following table provides the revision history of this document.

Table 1: *Revision History*

Revision Number	Description
Revision 01	Initial release.

Release Overview

Aruba Central On-Premises is a deployment of Aruba Central in your datacenter.

The maximum number of nodes supported is seven, and a seven-node instance of Aruba Central supports up to 25, 000 devices. Supported devices include switches, controllers, Instant APs, and Campus APs.

Aruba Central On-Premises require specific hardware for installation. Refer to the Installation guide for information on how to get started. Alternately, if you are migrating from AirWave, refer to the migration guide.

Additional Information

- Verifying Configuration Before Upgrade
- Switching to 10 Gigabit Ethernet Interface

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	networkingsupport.hpe.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

Chapter 2

New Features and Enhancements

The following features and enhancements are introduced in this release.

What's New

Important Notes

- Upgrade instruction for the 1GbE switch interface users:
  - 1 GbE interface—For users who are still on the 1 Gigabit Ethernet (GbE) switch interface, it is mandatory to first upgrade to Aruba Central On-Premises 2.5.6.7 version before switching to the 10 GbE interface. For information on switching to 10 GbE interface, see Switching to 10 Gigabit Ethernet Interface.

NOTE

10 GbE interface—Users who have already switched from 1 GbE to 10 GbE can directly upgrade to the Aruba Central On-Premises 2.5.7.0 version.

- For new Aruba Central On-Premises deployments, it is a prerequisite to use 10 GbE interface for optimum performance.
- Hazelcast license expires on **December 28, 2023**. Post the expiry, Aruba Central On-Premises may encounter functionality outages. Therefore, it is mandatory to update the license for all Aruba Central On-Premises clusters. To update the license, upgrade the clusters to Aruba Central On-Premises 2.5.7.3 or higher version.
- For offline upgrade from Aruba Central On-Premises 2.5.7.6, use the *apps_pkg* file. Do not use the *upgrade_pkg* file because it contains only the difference docker image layers.
- During upgrade workflow Aruba Central On-Premises servers reboot, if the uptime reaches 30 days for any one of the node or all the nodes in the cluster.
- The nodes of an Aruba Central On-Premises cluster must be deployed in the same data center and same VLAN subnet. It is a prerequisite to get 10 Gbps throughput for intra-cluster communication.
- High Availability (HA) with n-1 Aruba Central On-Premises is supported in multi-node COP cluster, where 'n' denotes the number of nodes in the cluster. In the event of a single node failure in a multi-node cluster, COP cluster functions in High availability mode. Once the COP cluster enters the HA mode, Aruba Central On-Premises user interface might not be accessible as it takes approximately 30 minutes for the system to get stabilized after any one of the cluster node goes down.

NOTE

It is recommended to bring up the down nodes to join back to the COP cluster. This ensures that Aruba Central On-Premises runs with all the nodes up.

- All nodes on Aruba Central On-Premises require minimum 512 GB RAM.
- Admins must prepare all the Aruba Central On-Premises nodes to upgrade with HPE release Service Pack. This Service Pack fixes any kind of known vulnerabilities and provides security updates for the

drivers along with additional features. It is recommended by HPE to keep ILO to the latest Service Pack as it improves reliability and performance of the servers.

NOTE

Customers must sign-in to HPE Networking Support Portal to access this Support Advisory.

- You must upgrade Aruba Central On-Premises within 90 days, for any major release such as Aruba Central On-Premises 2.5.7 to Aruba Central On-Premises 2.5.8.

New Features

The following sections provide an overview of the new features that are added to Aruba Central On-Premises in this release.

11-Node Scale

Starting Aruba Central On-Premises 2.5.8.0, users can implement clusters up to 11 nodes.

Advanced License for AOS-CX Switch Features

Some of the AOS-CX switch features require Aruba Central On-Premises Advanced licenses. A notification message is displayed indicating that a valid advanced license is required for the Fabric Overlay, Network Underlay workflows, and for AOS-CX Advanced Feature Pack using MultiEdit. You can acknowledge the message by clicking the close button. The notification message is user-specific. Once the message is closed, it will not be displayed for the same user, but the message will be displayed for other users. Also, the message acknowledgment needs to be done independently for each feature. The notification message will re-appear after 90 days and the user will have to acknowledge it every 90 days. For more information, refer to the *AOS-CX switches Feature Pack Ordering Guide* and EULA.

Aruba Central On-Premises APIs

Listed below are the APIs introduced in this release.

API Category	New APIs
Monitoring > Switch	■ [GET] /monitoring/v1/cx_switches/{serial}/neighbors ■ [GET] /monitoring/v1/cx_switch_stacks/{stack_id}/neighbors

Aruba Central NetConductor

The following are the new Aruba Central NetConductor features added in this release:

- **Configuration for System VLAN-Client-Presence for Fabric Wizard**—Aruba Central NetConductor now supports a toggle for VLAN Client Presence Detect to disable the VNI mapped VLANs if there are no authenticated clients on the VLAN, or if the VLAN has no statically configured ports and those ports are up.
- **Muti-Fabric EVPN Overview**—Aruba Central NetConductor now supports Muti-Fabric EVPN deployment provides end-to-end segmentation across SD-WAN Fabric by carrying the VRF and Role information natively in the data-plane.

- **RIB-to-FIB Optimization Knob for Fabric Wizard**—Aruba Central NetConductor now supports FIB Optimization to optimize unused host routes.
- **Support for Extended Edge Fabric Persona and Fabric Designs**—Aruba Central NetConductor now supports extended edge fabric persona and provides two types of Fabric Design options Routed-Access and Scaled-Access Design.
- **VSX Support for Campus Access Aggregation in Network Wizard**—Aruba Central NetConductor now supports a checkbox to specify the VSX pair in the Access-Aggregration when configuring a a Campus (3 tier L3 access) Underlay Network.
- Aruba Central On-Premises now provides a re-sync button to resolve configuration conflicts within existing overlay fabrics. This button is only available when a configuration conflicts exists.
- Aruba Central On-Premises now supports Layer 2 overlay segments for the default gateways.

Authentication

- The **Smart Card** authentication method is introduced for **RADIUS** and **RadSec** servers.
- The **Local Authentication** and **Sessions** tabs are introduced under **Authentication** to manage password reset policy and session configuration.

IPv6 Support

Starting from this release, users can onboard, monitor their devices and upgrade the AOS-CX firmware over IPv6 or dual stack networks.

Packet Capture Support for AOS-CX Switches

The packet capture feature is now supported on AOS-CX switches.

Support for HPE Networking Comware Switches

Aruba Central On-Premises now supports adding and monitoring HPE Networking Comware switches, in addition to its existing support for Cisco 9200 and 9300 switches under third-party devices. You can also create and schedule reports, as well as configure alerts for these devices.

Offline Upgrade through User Interface

Along with Command Line Interface (CLI), Aruba Central On-Premises now enables offline upgrade though **Versions** page on the user interface.

NOTE

- For non FIPS users, you must first enable Airgap mode through Command Line Interface (CLI) to perform offline upgrade through **Versions** page on the user interface.
- For FIPS-enabled users, Airgap is enabled by default and you can perform offline upgrade through **Versions** page on the user interface directly.

Enhancements

The following sections provide an overview of the enhancements introduced in Aruba Central On-Premises in this release.

Alert for Backup\Restore

The **COP Backup\Restore Operation Status** alert is added under the **Central System** category. It generates an alert if any backup or restore operation failure is detected.

Automatic Recovery

Aruba Central On-Premises has introduced the **Auto Recovery** tab under **System Management**. This feature allows you to recover critical resources in an event of network interface failure. The option to set up time for node reboot operation is also provided in this tab.

Controller Dashboard

The **WAN** tab is added to the controller dashboard for monitoring purpose. It displays the **Port Status** and **WAN Interfaces** information.

Controller Replacement

The **Controller Details** page is enabled to perform the replacement operation. Use **Replace Device** under the **Actions** drop-down list for replacing a controller.

Datacenter Redundancy

The feature and functionality of Datacenter Redundancy is extended to support Instant Access Points and AOS-CX switches running 10.12.1000 or later firmware versions.

Enhancements to Template Group Configurations

Starting from this release, when firmware compliance is set for a template group, then the template configuration push will be blocked on all non-compliant devices. The configurations will be pushed to these devices only when a compliant build firmware is downloaded and when the devices are rebooted.

AOS-CX Switch Alerts

- **Switch Uplink Port Usage**—Generates an alert when the total uplink port usage of a switch at a site exceeds the configured value within the specified duration.
- **Switch Routing Neighbor Status Change**—Generates an alert when the current status of the BGP neighbor changes from up (established) to down.
- **Switch NAE Agent Status**—Generates an alert when an NAE agent hits a condition that requires to be reported. This alert is disabled by default. This alert is supported only on AOS-CX switches running 10.13.1000 or later versions. This alert is generated only for the following NAE agent scripts:
  - routing_health_monitor
  - EVPN_VXLAN
  - Client Services
  - VSF_agent
  - VSX
  - default_agent

Monitoring CPU Utilization in AOS-CX Switches

Starting from this release, the AOS-CX switches calculate their own average CPU utilization for every five minutes. This feature is supported only on switches running AOS-CX 10.12.xx or later versions.

AOS-CX Switch Events

Support for the AOS-CX switch events in the following categories are now available in Aruba Central On-Premises:

- Services
- Routing
- Interface
- Hardware
- Overlays

In the AOS-CX Switch Software Documentation portal, navigate to a switch model and click the View software feature and user guides (HTML) link. Click Software Release Version listed next to the Event Log Message Reference Guide to view the events for the software release version selected.

Remote Console Support for IAPs and Controllers

Aruba Central On-Premises now allows remote console support for IAPs and controllers, in addition to its existing support for switches. This feature enables in-depth diagnostics and troubleshooting of device-related issues through a secure SSH connection.

Retiring an Offline AP

Aruba Central On-Premises now allows you to retire an offline access point (AP) from the device inventory.

SNMP Trap Notifications for System Alerts

Aruba Central On-Premises now allows you to configure SNMP trap email notifications for **Central System** alerts.

Aruba Central On-Premises Service Pack Package

Aruba Central On-Premises now supports `2024.04.00.00` service pack version. On checking ILO service pack version through Command Line Interface, it now displays RAID value, ILO timestamp, ROM and NIC details.

List of Devices Supported for Cable Test

Support for Cable test feature is now available in Aruba Central On-Premises for the following switches:

- AOS-S switches: 16.05.000 or higher
- AOS-CX switches: 10.11.1000 or higher
  - AOS-CX 4100 Switches
  - AOS-CX 6000 Switches
  - AOS-CX 6100 Switches
  - AOS-CX 6200 Switches
  - AOS-CX 6300 Switches
  - AOS-CX 6400 Switches
  - AOS-CX 8360 Switches
  - AOS-CX 8360V2 Switches
  - AOS-CX 6400V2 Switches

- AOS-CX switches: 11.1000 or higher
    - AOS-CX 6200V2 Switches

Troubleshooting Tests for Campus AP

Aruba Central On-Premises now enables you to perform Ping, Traceroute, HTTP, HTTPS, and TCP tests for Campus AP, with IPV6 support for each test.

Unified Communications Reports

Aruba Central On-Premises supports Unified Communications reports. Unified Communications reports may be created or scheduled from the **Analyze > Reports > Applications > UCC** page.

Unified Communications Support for Zoom

Aruba Central On-Premises supports Zoom as an Unified Communications application. Identification, prioritization and visibility is provided for Zoom audio calls. Zoom media traffic is tagged with the applicable and configured WMM/DSCP priority. Visibility of the Zoom audio sessions is available in the Unified Communications list and summary views and CDR.

Aruba Central On-Premises APIs

Listed below are the APIs enhanced in this release.

API Category	Modified APIs
Configuration > AP Configuration	▪ [GET]/configuration/v1/ap_cli/{group_name_or_guid_or_serial_number} ▪ [POST]/configuration/v1/ap_cli/{group_name_or_guid_or_serial_number}

Listed below are the APIs removed in this release.

API Category	Removed APIs
Monitoring > VPN	▪ [GET] /monitoring/v1/vpn/usage ▪ [GET] /monitoring/v2/vpn/usage
Monitoring > AP	▪ [GET] /monitoring/v1/aps ▪ [GET] /monitoring/v2/aps/{serial}/rf_summary ▪ [GET] /monitoring/v1/aps/bandwidth_usage ▪ [GET] /monitoring/v2/aps/bandwidth_usage ▪ [GET] /monitoring/v1/aps/{serial}/neighbouring_clients ▪ [GET] /monitoring/v1/bssids ▪ [GET] /monitoring/v1/aps/bandwidth_usage/topn
Monitoring > Network	▪ [GET] /monitoring/v1/networks ▪ [GET] /monitoring/v1/networks/{network_name} ▪ [GET] /monitoring/v1/networks/bandwidth_usage

New Hardware Platforms

The following are the newly supported hardware platforms in Aruba Central On-Premises 2.5.8 release.

Access Points

- AP-605H
- AP-675
- AP-677
- AP-679

Third-Party Devices

- HPE Networking Comware Switch Series 5140 EI
- HPE Networking Comware Switch Series 5140 HI
- HPE Networking Comware Switch Series 5520 HI
- HPE Networking Comware Switch Series 5600 HI
- HPE Networking Comware Switch Series 7500X

Resolved Issues in Aruba Central On-Premises 2.5.8.0

The following table describes the resolved issues identified in this Aruba Central On-Premises release:

Table 3: *Resolved Issues*

ID	Description
CN-134904	Core update reachability was required during the last stage of the acp-upgrade. The fix ensures there is no core update dependency during the upgrade.
CN-233662	**Issue**: Installation of Aruba Central On-Premises 2.5.7.0 failed intermittently. This issue occurred because the PgBouncer was not connecting to the server.
CN-238624	Default certificates were inaccessible on the WebUI and API gateways. This issue occurred because the strict check option was enabled after uploading the certificates to the server. The fix ensures that the certificates are accessible and strict check option is disabled in the default mode.
CN-241587	**Issue**: Wall layers were misaligned in the WebUI after importing the Floor Plan using DWG files. The fix ensures that the wall layers are aligned correctly in the WebUI when importing DWG files.
CN-241640	**Issue**: Under **Alerts & Events** > **Events** tab, the **AP Reboot** and **AP Crash** event types displayed an incorrect MAC address. The fix ensures that the correct MAC address is displayed for both the **AP Reboot** and **AP Crash** event types.
CN-246226	**Issue**: The upgrade from Aruba Central On-Premises 2.5.7.x to later versions failed because the proxy configuration was not copied to newly added nodes in the cluster. The fix ensures that the proxy configuration is copied to newly added nodes and upgrade to Aruba Central On-Premises 2.5.8 works as expected
CN-250110	**Issue**: The CSV file downloaded from the **Manage > Devices > Access Points** tab incorrectly displayed the name of the **Controller AP Group** header as **AP Group**. The fix ensures that the CSV file displays the correct header names when users import data from the AP list table.
CN-251015	The sites were not displayed in the **Global** > **Overview** > **Network Health** page. The fix ensures that the sites data is displayed in the **Network Health** page.
CN-252033	A mismatch in the bandwidth data was observed in the **Top APs By Usage** and **Throughput** graphs in the Aruba Central On-Premises UI. The fix ensures that bandwidth data is similar in both the **Top APs By Usage** and **Throughput** graphs.

ID	Description
CN-263315	**Issue**: Incremental backup schedule configured on DR-enabled clusters failed in the new primary. This issue occurred because of the switchover of primary to secondary after the auto failover. The fix ensures that the backup and restore operation works as expected.
GLCP-193492	**Issue**: The SAML SSO configuration failed and **Bad Request** error was encountered only in airgap instances. This issue was seen in the **Claim a Domain** window after specifying the organization domain name because GET request failed. The fix ensures that SAML SSO configuration works as expected.

Known Issues in Aruba Central On-Premises 2.5.8.0

Limitations

Third-Party Device Reports

The **Client Usage** report in the **Analyze** > **Reports** page generates an empty document for third-party devices. This is because wired clients are not supported for third-party devices.

Modifying Multi-Fabric Network

Modifying a multi-fabric network could be disruptive on a live network. The network takes up to 3 minutes to converge, and hence, it is recommended to add or edit configurations during the maintenance window.

Upgrade Failing on Secondary Server of a DR Cluster

If upgrade is initiated when NTP is out-of-sync on the secondary server of a DR-enabled cluster, it sometimes fails due to traffic restrictions on the secondary server. NTP re-synchronization and new NTP server configuration also may not work. If this situation is encountered, contact the Aruba Technical Support through https://www.arubanetworks.com/support-services/contact-support/ for NTP synchronization.

Upgrade Failing at Readiness Check Stage

If the upgrade operation fails at pre-health check, download the upgrade pod logs to view the error details or the logs generated on the **Audit Trail** page. Troubleshoot the errors and re-run the upgrade health check.

Known Issues

The following table describes known issues identified in this Aruba Central On-Premises release.

Table 4: *Known Issues*

ID	Description
CN-230197	**Issue**: The Cassandra database restore operation does not complete and displays the status as **In Progress**. This issue occurs because SSTableLoader is not loading the data. **Workaround**: None.
CN-250119	**Issue**: Validation of FIPS cluster replace operation fails with non FIPS node, and non FIPS cluster replace operation fails with FIPS node. **Workaround**: While performing Add or Replace operation in a FIPS cluster, you must use only FIPS enabled nodes whereas, in a non FIPS cluster, you must use only non FIPS enabled nodes.
CN-235628	**Issue**: Users are unable to view the **Devices** > **Controllers** page and an error message, **504 Gateway Time-out** is displayed.

ID	Description
	Workaround: None.
CN-237833	**Issue**: The data is incorrectly displayed for the **Top IAP Clusters by Clients** on the **Global** > **Summary** page. **Workaround**: None.
CN-238456	**Issue**: The value for **Top APs By Usage** does not populate sometimes on the **Overview** > **Summary** page. **Workaround**: None.
CN-241604	**Issue**: The alerts are not generated for Aruba Central On-Premises connected clients per VC and client per AP. **Workaround**: None.
CN-252017	**Issue**: Network Link Aggregation (LAG) gets disabled when a node in the cluster is reset. Replacing the node does not restore LAG setting. **Workaround**: None
CN-265116	**Issue**:The **WAN Interfaces** table for WAN controllers in Aruba Central On-Premises under **Manage** > **WAN** > **Summary** page does not display **Performance MOS** for a time range filter of 3 hours. **Workaround**:None.
CN-265588	**Issue**: Adding a new node under **System Management** > **Performance** > **Appliance Resources** table fails on a 3-node setup when LAG is enabled on either one of the nodes. **Workaround**: Disable the LAG and then add the node. After the add node operation is successful, enable the LAG.
CN-265113	**Issue**: In a Datacenter Redundancy (DR) enabled cluster setup, with primary and secondary clusters forming the peer, the template group (TG) configuration push takes more than 10 minutes after the second auto failover. **Workaround**: None.
CN-266181	**Issue**: In some APs, the decimal part of Tx power is seen in the **VRF Floor Plan** page but **AP Monitoring** page shows only the whole number. **Workaround**: None.

Chapter 5
Aruba Central On-Premises Upgrade

Aruba Central On-Premises strongly recommends that you upgrade your On-premise version to the next available major version for a smooth and hassle free operation of your account. Upgrade watcher checks for any major versions release and notifies you for its availability on your next Aruba Central On-Premises account login. The upgrade workflow differs based on the regular-Online, occasional-online user accounts, and offline users.

NOTE

- The Upgrade operation can only be done by the user with admin rights.
- To upgrade to Aruba Central On-Premises 2.5.7, it is mandatory for the Aruba Central On-Premises setup to be connected to the network through 10 Gig interfaces. For any assistance, contact Aruba TAC (Technical Assistance Center) team.

Important Points

- 10 GbE interface: Users who have already switched from 1 GbE to 10 GbE can directly upgrade to the Aruba Central On-Premises 2.5.7 version.
- 1 GbE interface: Users who are still on the 1 GbE switch interface must first upgrade to Aruba Central On-Premises 2.5.6.7 before switching to 10 GbE interface. This is mandatory.

This section includes the following topics:

- Online Upgrade Through the Versions Page
- Version
- Offline Upgrade Through Command Line Interface
- Handling Upgrade for Datacenter Redundancy

Version

The **Version** tab displays the installed version, available version for upgrade, upgrade status, and you can also generate logs related to events that occurred during an upgrade.

Viewing Installed and Available Version Information

To view the Aruba Central On-Premises versions, complete the following steps:

1. In the **Aruba Central On-Premises** app, set the filter to **Global**.
2. Under **Maintain**, click **System Management**.
3. Click the **Version** tab.

The **Version** pane displays the following information:

- The **Installed Version** displays the currently installed version in the Aruba Central On-Premises server.

- The **Available Version** displays the version that is currently available and the user can upgrade to this version.

Upgrading Aruba Central On-Premises

> CAUTION
>
> You must take backup before upgrading. If a hardware failure is encountered for any reason, only then the restore operation must be performed. After the installation and resolving the hardware issue, restore the backup.

To upgrade Aruba Central On-Premises to the latest version, complete the following steps:

1. In the **Aruba Central On-Premises** app, set the filter to **Global**.
2. Under **Maintain**, click **System Management**.
3. Click the **Version** tab.
4. In the **Upgrade** pane, click **Upgrade Now** to upgrade to the latest version of Aruba Central On-Premises.

The **Upgrade** pane also displays the following information:

- **Status**— Displays the overall status of the upgrade.
- **File Transfer**—Displays the status of the file transfer.
- **Extract**—Displays the status of the file extraction.
- **Upgrade**—Displays the status of the upgrade.

Generating Logs

Aruba Central On-Premises allows you to view and download logs related to the events that occurred during the upgrade process. To generate the logs for the events, click **Generate Logs** in the **Logs** pane. Once generated, the logs can be viewed in the Logs table.

The **Logs** table displays the following information and also allows you to download or delete logs:

- **File**— Displays the generated file name.
- **Created**— Displays the date and time of the log creation.
- **Status**— Displays the status of the generated logs.
- **Action**— Allows you to do the following actions:
  - **Download**— Select the file and click the ⤓ icon to download the generated file.
  - **Delete**— Select the file that you want to delete and click the delete icon. In the **Confirm Action** pop-up window, click **Yes**.

Offline Upgrade

This section describes the upgrade workflow and the requirements for offline Aruba Central On-Premises user accounts. This scenario is applicable for users who have enabled Airgap mode through Command Line Interface (CLI) to enable offline upgrade. For FIPS-enabled users, Airgap is enabled by default. All the account GUI functionality is allowed and the user has to upgrade to the major available version within the prescribed period and time range (49 days - 55 days).

Users get a notification on the Aruba Central On-Premises user interface or an email is sent notifying for an upgrade.

NOTE

- For offline mode, upgrade notification is shown on the user interface only when users manually uploads the update checker file or the upgrade package.
- For offline upgrade from Aruba Central On-Premises 2.5.7.6 onwards, use `apps_pkg` file. Do not use the `upgrade_pkg` file because it contains only the difference docker image layers.

For more information, see the following sections:

- Offline Upgrade Through Command Line Interface
- Offline Upgrade Through User Interface

Offline Upgrade Through Command Line Interface

To update Aruba Central On-Premises on offline mode through CLI, complete the following steps:

Step 1: Enabling and Disabling Airgap via CLI

Step 2: Uploading the Watcher File

Step 3: Uploading Signature Files and Upgrade Packages

Step 4: Selecting the Uploaded Files

Step 5: Verification and Extraction of the Files

Step 6: Triggering Aruba Central On-Premises Upgrade

Step 7: Retry Upgrade

Step 1: Enabling and Disabling Airgap via CLI

Airgap can be enabled and disabled through CLI option **4** System Configuration commands. Under option **4**, you must use option **7**, (**4-7**) for Airgap.

System Configuration Commands

Enter command option **4** from the main menu to view all the System Configuration commands.

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advanced
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
====================================
0. exit

Enter option [ 0 - 11 ]: 4
```

The supported System Configuration commands are displayed. These commands are used to configure system parameters like network setup, cluster setup, timezone setup. enable airgap mode, and also, upgrade the setup or perform a complete factory reset.

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Airgap
8. Disaster Recovery
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 8 ]:
```

Airgap

Enter command option **7** from the System Configuration menu to enable or disable Airgap mode for upgrade. Enabling Airgap allows you to upgrade the Aruba Central On-Premises setup offline without any internet access.

```
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Airgap
8. Disaster Recovery
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 8 ]: 7
```

```
1. Enable Airgap
2. Disable Airgap
3. Status
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]:
```

- **Enable Airgap**—Enter command option **1** from the Airgap menu to enable the same.

  ```
  Enter option [ 0 - 3 ]:  1
  Changing of Airgap mode requires restart of services and is recommended ONLY in
  maintenance window.Do you want to continue?(Y/N):
  ```

- **Disable Airgap**—Enter command option **2** from the Airgap menu to disable the same.

```
Enter option [ 0 - 3 ]:  2
Airgap is already disabled.
Press [Enter] key to continue...
```

- **Status**—Enter command option **3** from the Airgap menu to see the status.

```
Enter option [ 0 - 3 ]:  3
Airgap is already disabled.
Press [Enter] key to continue...
```

NOTE

In a FIPS-enabled Aruba Central On-Premises setup, Airgap is enabled by default, and users cannot disable this feature.

Step 2: Uploading the Watcher File

Upgrading the Watcher file is mandatory for every Aruba Central On-Premises release. The Aruba Central On-Premises watcher file is uploaded on the HPE Networking Support Portal site in every 30 days. The purpose of the Watcher file is to check regarding availability of any new release. Users receive a notification/ prompt in every 49 days in order to upload the Watcher file to verify if there is any new Aruba Central On-Premises release available. The snooze period to upload the Watcher file is 6 days. If a user, doesn't upload the watcher file within the snooze period, the Aruba Central On-Premises user interface (UI) is completely blocked and cannot be accessed.

For any minor Aruba Central On-Premises release there is no time restriction to do the upgrade.

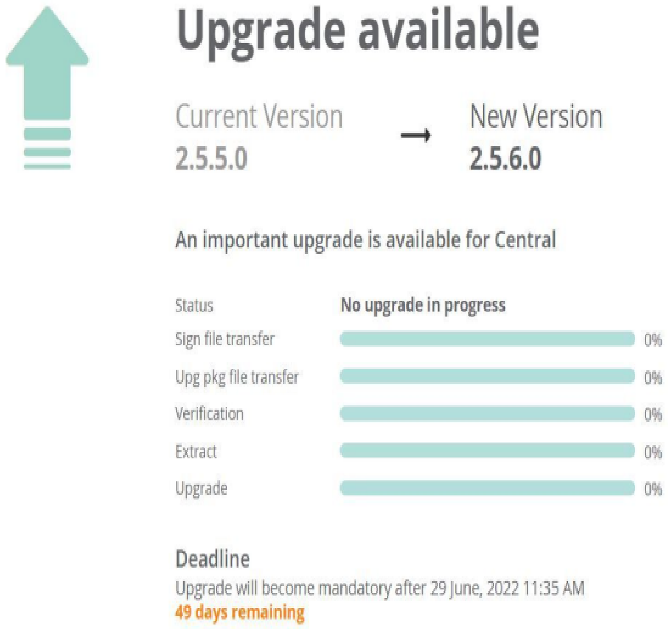
Upgrade Status

Based on the account login period, one of the following pages is displayed:

1. **Upgrade Available**—This window is displayed when you log in to your Aruba Central On-Premises account within the deadline of the version upgrade (55 days from the date of version release). The upgrade available window provides the following information:
   - **Current version**—Current running version.
   - **New versions**—Next major available version.
   - **Status**—Provides the status and progress bar for the file transfer, verification, extract, and upgrade.
   - **Deadline**—Displays the number of days remaining for upgrade. The number of days varies depending on the version available date and the day of login. For example, if the version was available on 8th of December and the user logs in on 10th of December, the remaining days gets changed to 53 days within which the account needs to be upgraded.
   - **Remind in x days**—Allows you to snooze the notification for some days. Notification can be snoozed for 7 days (55-20 remaining days), 5 days (20-10 remaining days), 3 days (10-5 remaining days), 2 days(5-3 remaining days), and 1 (for the rest remaining days). On snoozing the notification, you can use the account normally and the next notification comes after the set dates.

   The following example image displays the **Upgrade available** window.

Figure 1 *Upgrade Available*



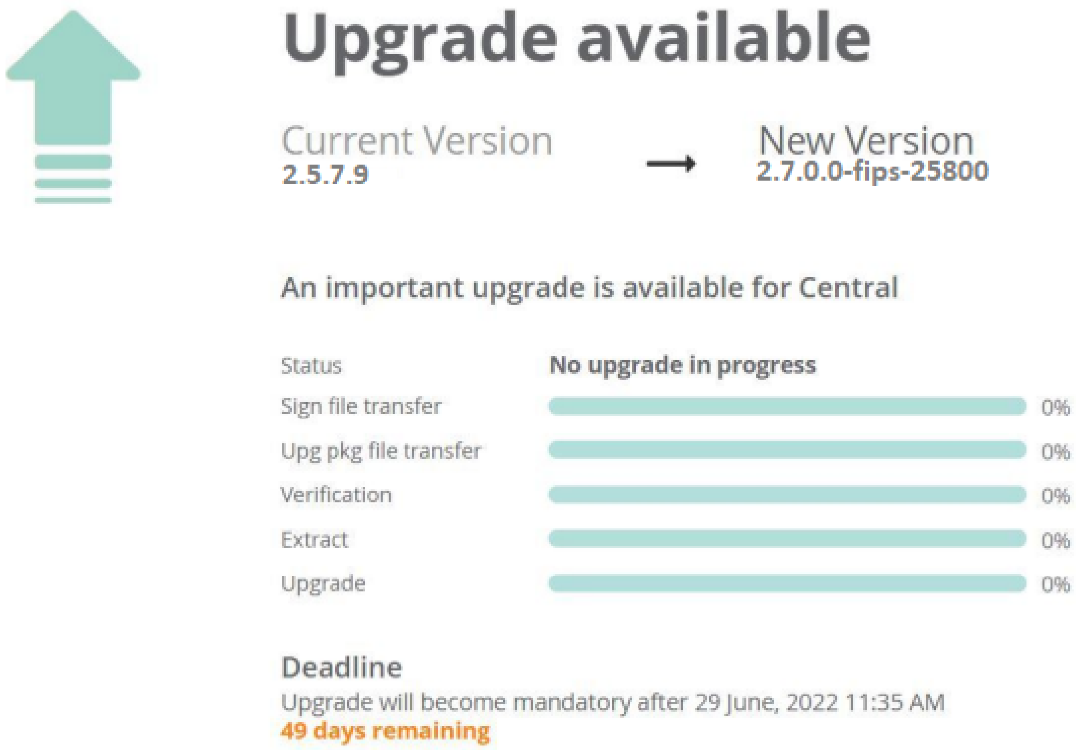
Upgrade available

Current Version
2.5.5.0
→
New Version
2.5.6.0

An important upgrade is available for Central

Status	No upgrade in progress
Sign file transfer	0%
Upg pkg file transfer	0%
Verification	0%
Extract	0%
Upgrade	0%

Deadline
Upgrade will become mandatory after 29 June, 2022 11:35 AM
49 days remaining



Upgrade available

Current Version
2.5.7.9
→
New Version
2.7.0.0-fips-25800

An important upgrade is available for Central

Status	No upgrade in progress
Sign file transfer	0%
Upg pkg file transfer	0%
Verification	0%
Extract	0%
Upgrade	0%

Deadline
Upgrade will become mandatory after 29 June, 2022 11:35 AM
49 days remaining

2. **Upgrade Check Required**—This window is displayed when you log in to your Aruba Central On-Premises account after the deadline is missed. This window indicates that you have missed the upgrade check deadline and an immediate upgrade check is required. All the account GUI functionality is blocked till the upgrade availability is checked with the latest version of the update checker file. To check, follow the steps mentioned on the screen, and upload the update checker file. The upgrade check required window provides the following information:

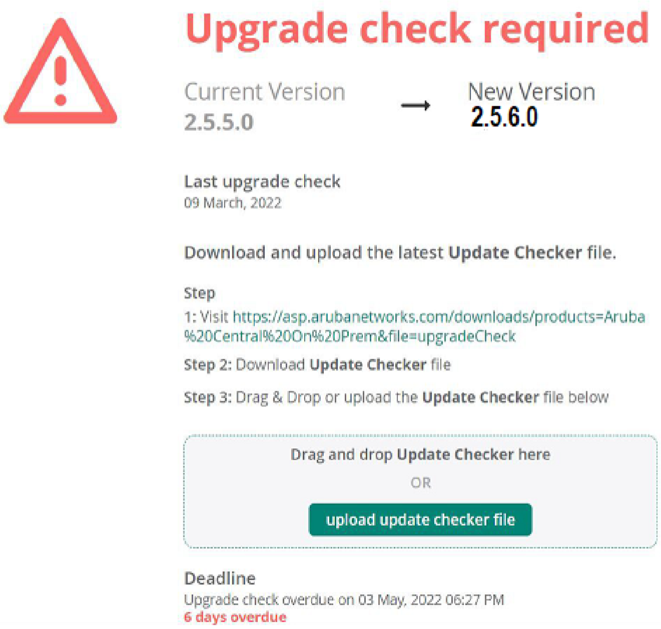
- **Current Version**—Current running version.
- **New Version**—Next major available version.
- **Last Upgrade Check**—Displays the date of last upgrade check.
- **Deadline**—Displays the remaining days for mandatory upgrade check.
- **Upgrade Check Steps**—Displays the steps to update the check file.

To check the available version once notified, you can either drag and drop the update checker file from your local browser, or you can click the **upload update checker file**. Once the upgrade check is successful, you can use the account normally and the next notification comes after the set dates.

Once the upgrade check is successful, the account comes to its normal functionality.

The following example image displays the **Upgrade check required** window.

Figure 2 *Upgrade Check Required*



Upgrade check required

Current Version
2.5.5.0 → New Version
2.5.6.0

Last upgrade check
09 March, 2022

Download and upload the latest **Update Checker** file.

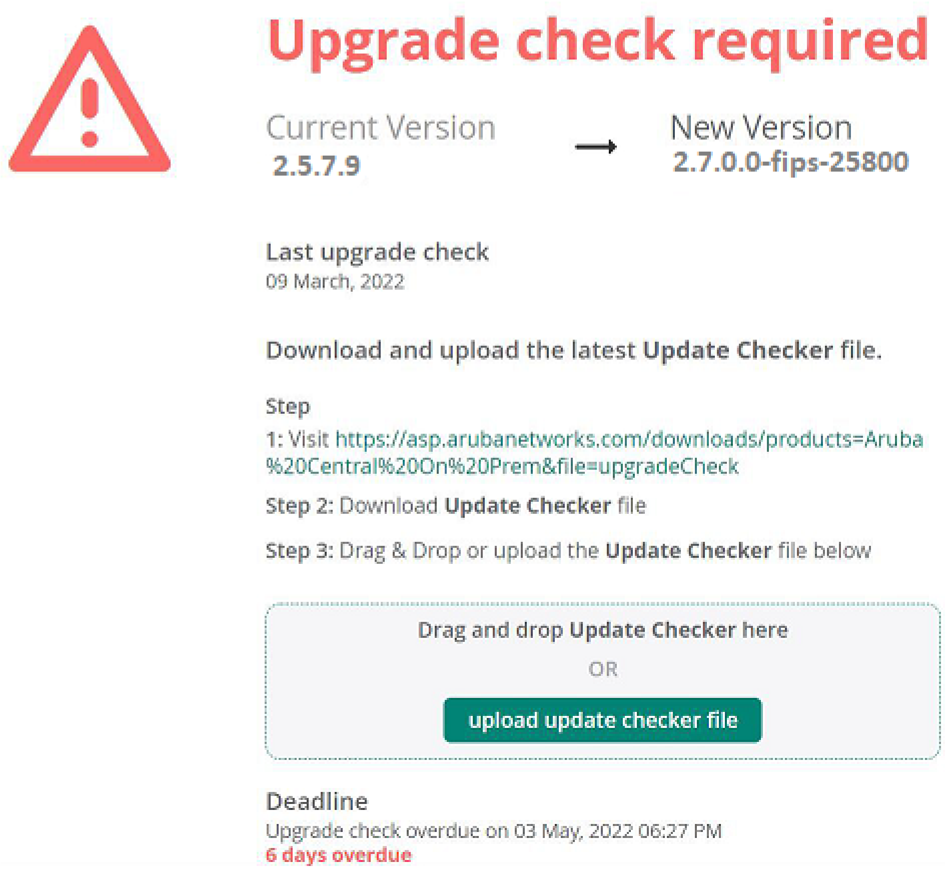
Step
1: Visit https://asp.arubanetworks.com/downloads/products=Aruba%20Central%20On%20Prem&file=upgradeCheck

Step 2: Download **Update Checker** file

Step 3: Drag & Drop or upload the **Update Checker** file below

Drag and drop **Update Checker** here
OR
upload update checker file

Deadline
Upgrade check overdue on 03 May, 2022 06:27 PM
6 days overdue



Upgrade check required

Current Version 2.5.7.9 → New Version 2.7.0.0-fips-25800

Last upgrade check
09 March, 2022

Download and upload the latest **Update Checker** file.

Step
1: Visit https://asp.arubanetworks.com/downloads/products=Aruba%20Central%20On%20Prem&file=upgradeCheck

Step 2: Download **Update Checker** file

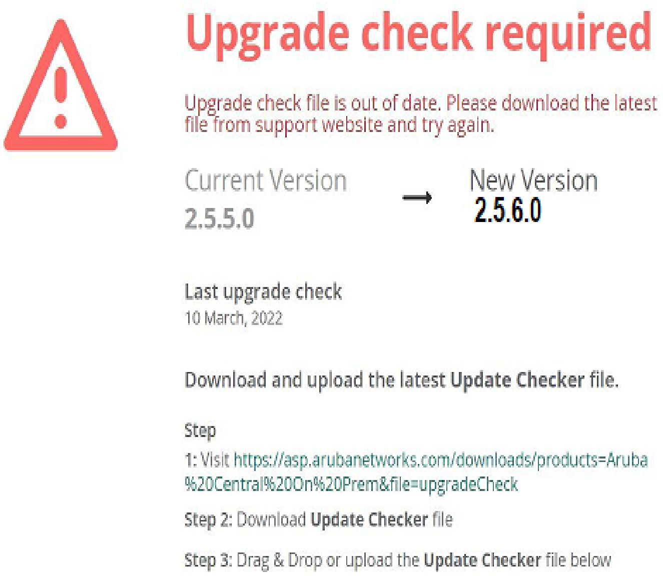
Step 3: Drag & Drop or upload the **Update Checker** file below

Drag and drop **Update Checker** here
OR
upload update checker file

Deadline
Upgrade check overdue on 03 May, 2022 06:27 PM
6 days overdue

3. **Upgrade Check Failed**—This window is displayed when the user logs into Aruba Central On-Premises within the above mentioned periods. The upgrade check can fail because of the following reasons:
   - User uploaded an old version of upgrade file as compared to the latest available file

Figure 3 *Upgrade Version Check Required*



Upgrade check required

Upgrade check file is out of date. Please download the latest file from support website and try again.

Current Version 2.5.5.0 → New Version 2.5.6.0

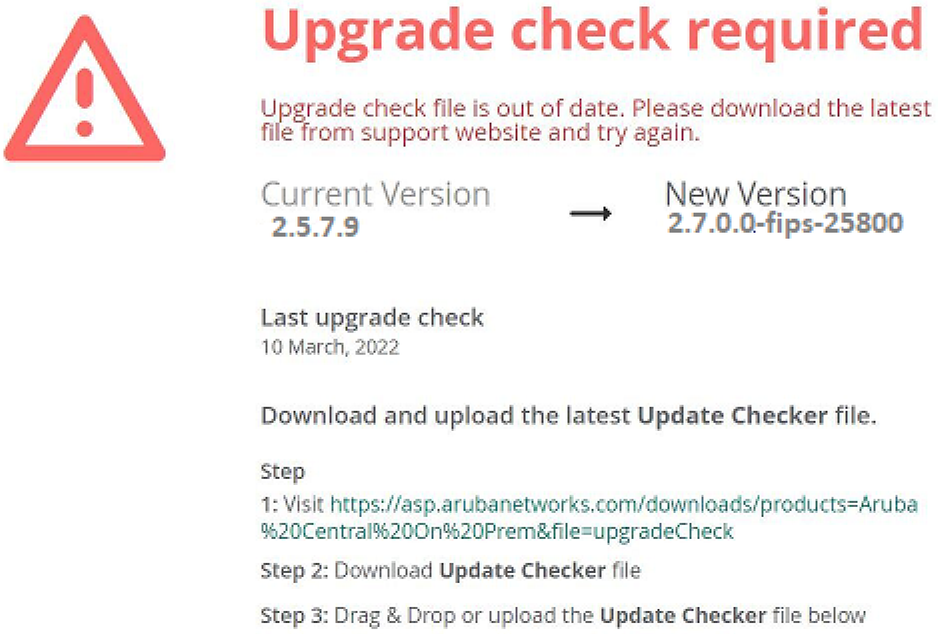
Last upgrade check
10 March, 2022

Download and upload the latest **Update Checker** file.

Step
1: Visit https://asp.arubanetworks.com/downloads/products=Aruba%20Central%20On%20Prem&file=upgradeCheck

Step 2: Download **Update Checker** file

Step 3: Drag & Drop or upload the **Update Checker** file below



Upgrade check required

Upgrade check file is out of date. Please download the latest file from support website and try again.

Current Version 2.5.7.9 → New Version 2.7.0.0-fips-25800

Last upgrade check
10 March, 2022

Download and upload the latest **Update Checker** file.

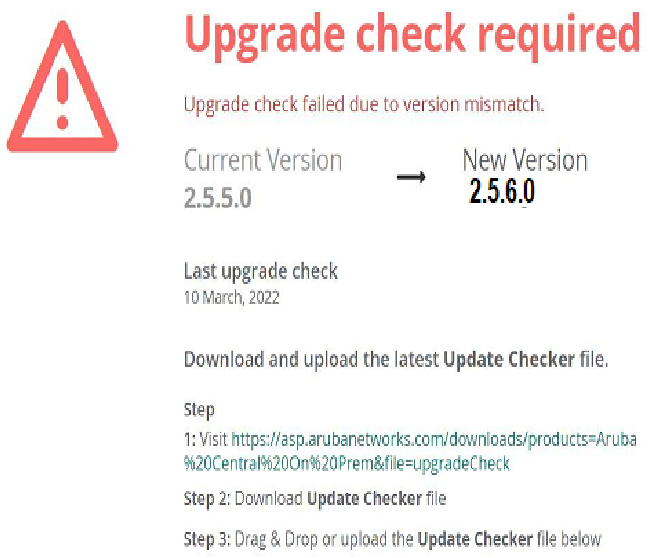
Step
1: Visit https://asp.arubanetworks.com/downloads/products=Aruba%20Central%20On%20Prem&file=upgradeCheck

Step 2: Download **Update Checker** file

Step 3: Drag & Drop or upload the **Update Checker** file below

- User uploaded a lower version of upgrade check file as compared to the running version

Figure 4 *Upgrade Version Mismatch*



Upgrade check required

Upgrade check failed due to version mismatch.

Current Version 2.5.5.0 → New Version 2.5.6.0

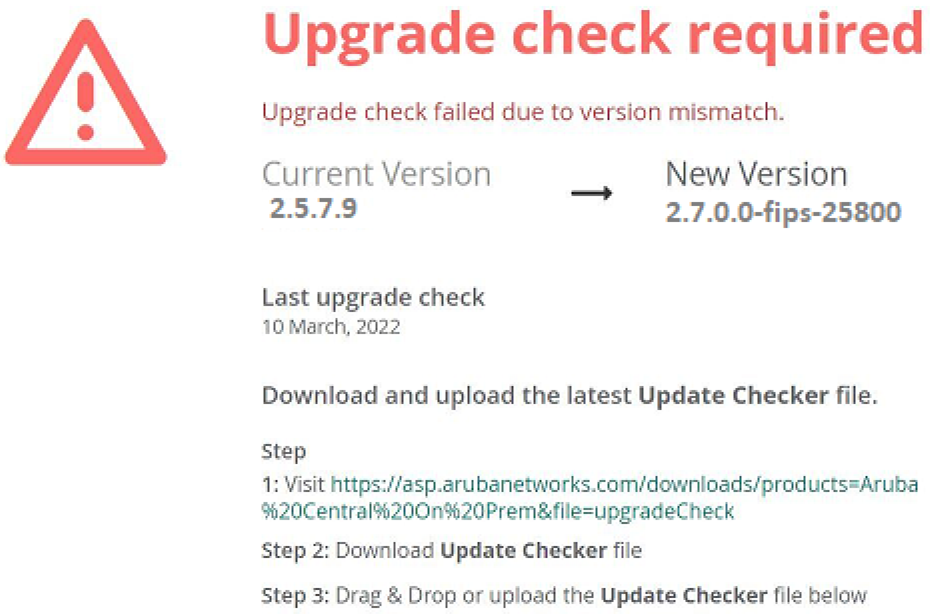
Last upgrade check
10 March, 2022

Download and upload the latest **Update Checker** file.

Step
1: Visit https://asp.arubanetworks.com/downloads/products=Aruba%20Central%20On%20Prem&file=upgradeCheck

Step 2: Download **Update Checker** file

Step 3: Drag & Drop or upload the **Update Checker** file below



Upgrade check required

Upgrade check failed due to version mismatch.

Current Version 2.5.7.9 → New Version 2.7.0.0-fips-25800

Last upgrade check
10 March, 2022

Download and upload the latest **Update Checker** file.

Step
1: Visit https://asp.arubanetworks.com/downloads/products=Aruba%20Central%20On%20Prem&file=upgradeCheck

Step 2: Download **Update Checker** file

Step 3: Drag & Drop or upload the **Update Checker** file below

Step 3: Uploading Signature Files and Upgrade Packages

After every Aruba Central On-Premises release, upgrade packages are uploaded to HPE Networking Support Portal site. You should download it to your local file server and from there you can upload it to the COP server using CLI option.

System Configuration Commands

The System Configuration commands are used to configure system parameters like network setup, cluster setup, timezone setup and also, upgrade the setup or perform a complete factory reset.

Enter command option **4** from the main menu to view all the system configuration commands supported.

```
Enter option [ 0 - 11 ]: 4
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Airgap
8. Disaster Recovery
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 8 ]:
```

Upgrade

Enter command option **4-1** from the System Configuration commands menu to upgrade the system for either an online user or an offline user.

```
Enter option [ 0 - 8 ]: 1
1. Upload Package
2. Upgrade Status
3. Proceed With Upgrade
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]:
```

- **Upload Package**

  Enter command option **4-1-1** from the Upgrade commands menu to view the options for uploading and selecting upgrade packages. The upgrade package includes the signature file and the installation file.

  ```
  Enter option [ 0 - 3 ]: 1
  1. Select Signature and Installation File
  2. Upload Signature and Installation via SCP
  3. Upload Signature and Installation via SFTP
  =====================================
  b. back
  m. main menu
  0. exit
  Enter option [0 - 3]:
  ```

- **Upload Signature File and Installation File via SCP**

  Enter command option **4-1-1-2** from the Upload Package commands menu to upload the signature file and installation file through Secure Copy Protocol (SCP).

NOTE

For offline upgrade from Aruba Central On-Premises 2.5.7.6 onwards, use `apps_pkg` file instead of `upgrade_pkg` file. If you are on any older release than 2.5.7.6, you must continue using `apps_upgrade_pkg` file only.

Uploading the Signature File

```
Enter option [ 0 - 3 ]: 2
This will scp a sign file from the remote server to COP server
Enter remote hostname and path (username@hostname:<filepath>):
admin@10.xx.xx.xx:/build/2.5.7/454-20240206/apps_pkg
-2.5.7-454-prod.sign
Copying admin@10.xx.xx.xx:/build/2.5.7/454-20240206/apps_pkg_
-2.5.7-454-prod.sign COP server
admin@10.xx.xx.xx's password:
apps_pkg_-2.5.7-454-prod.sign

Press [Enter] key to continue...
```

After uploading the Signature file, press **Enter** and upload the Installation file.

Uploading the Installation File

```
Enter option [ 0 - 3 ]: 2
This will scp a sign file from the remote server to COP server
Enter remote hostname and path (username@hostname:<filepath>):
admin@10.xx.xx.xx:/build/2.5.7/454-24567891/apps_pkg
-2.5.7-454-prod.tar.gz
Copying admin@10.xx.xx.xx:/build/2.5.7/454-24567891/apps_pkg_
-2.5.7-454-prod.tar.gz to COP server

admin@10.xx.xx.xx's password:
apps_pkg-2.5.7-454-prod.tar.gz
Press [Enter] key to continue...
```

- **Upload Signature File and Installation File via SFTP**

  Enter command option **4-1-1-3** from the Upload Package commands menu to upload the signature file and installation file through Secure File Transfer Protocol (SFTP).

NOTE

For offline upgrade from Aruba Central On-Premises 2.5.7.6 onwards, use `apps_pkg` file instead of `upgrade_pkg` file. If you are on any older release than 2.5.7.6, you must continue using `apps_upgrade_pkg` file only.

Uploading the Signature File

```
Enter option [ 0 - 3 ]: 3
This will scp a sign file from the remote server to COP server
Enter remote hostname and path (username@hostname:<filepath>):
admin@10.xx.xx.xx:/build/2.5.7/454-20240206/apps_pkg
-2.5.7-454-prod.sign
Copying admin@10.xx.xx.xx:/build/2.5.7/454-20240206/apps_pkg_
-2.5.7-454-prod.sign to COP server
administrator@10.xx.xx.xx's password:
apps_pkg-2.5.7-454-prod.sign
```

```
Press [Enter] key to continue...
```

After uploading the Signature file, press **Enter** and upload the Installation file.

Uploading the Installation File

```
Enter option [ 0 - 3 ]: 3
This will scp a sign file from the remote server to COP server
Enter remote hostname and path (username@hostname:<filepath>):
admin@10.xx.xx.xx:/build/2.5.7/454-24567891/apps_pkg
-2.5.7-454-prod.tar.gz
Copying admin@10.xx.xx.xx:/build/2.5.7/454-24567891/apps_pkg_
-2.5.7-454-prod.tar.gz to COP server
administrator@10.xx.xx.xx's password:
apps_pkg-2.5.7-454-prod.tar.gz

Press [Enter] key to continue...
```

Step 4: Selecting the Uploaded Files

After uploading the upgrade packages to Aruba Central On-Premises server, you must select the signature and installation files to initiate the offline upgrade.

Select Signature and Installation File

Enter command option **4-1-1-1** from the Upload Package commands menu to select the files.

```
Enter option [ 0 - 3 ]: 1

1. apps_pkg-2.5.7-369-dev_from_10.0.0-GA02.sign

Choose a signature file [1 - 1]: 1

Selected file is :: apps_pkg-2.5.7-369-dev_from_10.0.0-GA02.sign
1. apps_pkg-2.5.7-369-dev_from_10.0.0-GA02.tar.gz

Choose an installation file [1 - 1]:
1 Selected file is :: apps_pkg-2.5.7-369-dev_from_10.0.0-GA02.tar.gz

============Verification in progress===========
Press [Enter] key to continue...
```

NOTE

For offline upgrade from Aruba Central On-Premises 2.5.7.6 onwards, use `apps_pkg` file instead of `upgrade_pkg` file. If you are on any older release than 2.5.7.6, you must continue using `apps_upgrade_pkg` file only.

Step 5: Verification and Extraction of the Files

After selecting the uploaded files, validation of the files begin and after the validation is successful, file extraction is started. After the extraction is complete, you can manually trigger the upgrade through either CLI or UI.

Upgrade Status

After selecting the file, to confirm regarding the extraction process you can monitor the status in the UI as well in the CLI. For more information on selecting files, see Step 4: Selecting the Uploaded Files.

To monitor the status through CLI, enter command option **4-1-2** from the Upgrade commands menu.

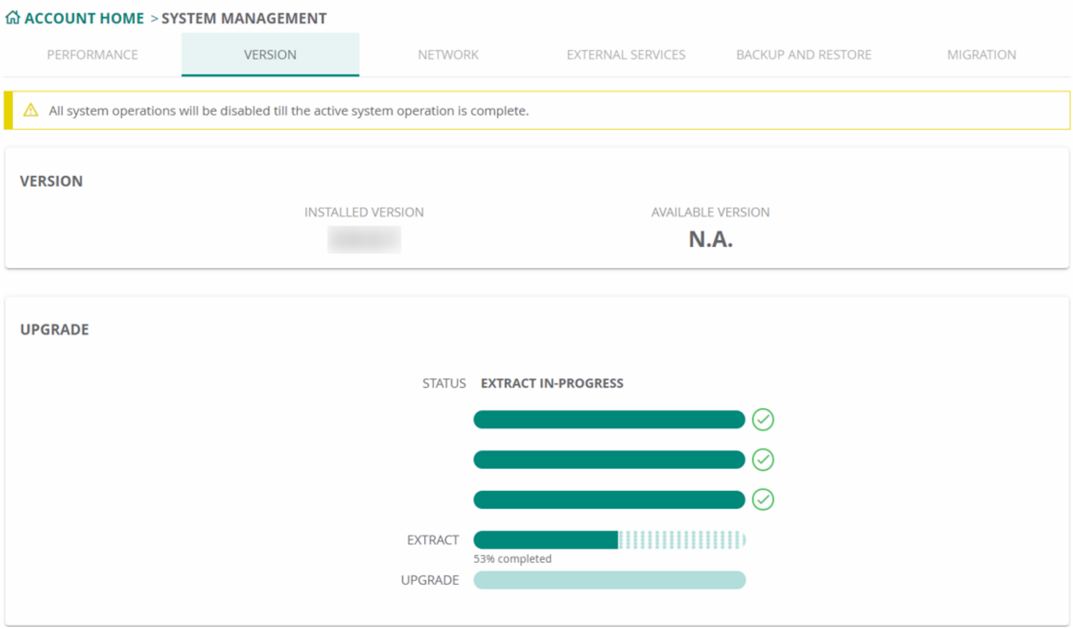
```
Enter option [ 0 - 3 ]: 2
COP Server Status
--------------------------------------------------------------------------------
Current Version                             : 2.5.7.0
Latest Version                              : 2.5.7.0
Online Customer                             : false
Upgrade Status                              : EXTRACT_IN_PROGRESS
Upgrade Available                           : true
Sign File Transfer Completion Percentage    : 100
Upg Pkg File Transfer Completion Percentage : 100
Pkg Sign Validate Completion Percentage     : 100
Extract Completion Percentage               : 100
Upgrade Stage Completion Percentage         : 0
--------------------------------------------------------------------------------

                                                                        -
Last Sign File Transfer Status              : SUCCESS
Last Sign File Transfer Message             :
Last Sign File Transfer Time                : 2023-07-26 06:10:50
Last Upg Pkg File Transfer Status           : SUCCESS
Last Upg Pkg File Transfer Message          :
Last Upg pkg File Transfer Time             : 2023-07-26 06:10:54
Last Pkg Sign Validate Status               : SUCCESS
Last Pkg Sign Validate Message              :
Last Pkg Sign Validate Time                 : 2023-07-26 06:21:05
Last Extract Status                         : SUCCESS
Last Extract Message                        :
Last Extract  Time                          : 2023-07-26 11:14:34
Last Upgrade Status                         : SUCCESS
Last Upgrade Message                        :
Last Upgrade Time                           : 2023-07-21 09:58:55
--------------------------------------------------------------------------------


Press [Enter] key to continue
```

To monitor the status through GUI, navigate to **System Management** > **Versions** page.

Figure 5 *Upgrade Status through Versions tab*



ACCOUNT HOME > SYSTEM MANAGEMENT

All system operations will be disabled till the active system operation is complete.

VERSION

INSTALLED VERSION [redacted]

AVAILABLE VERSION N.A.

UPGRADE

STATUS EXTRACT IN-PROGRESS

EXTRACT 53% completed

UPGRADE

Step 6: Triggering Aruba Central On-Premises Upgrade

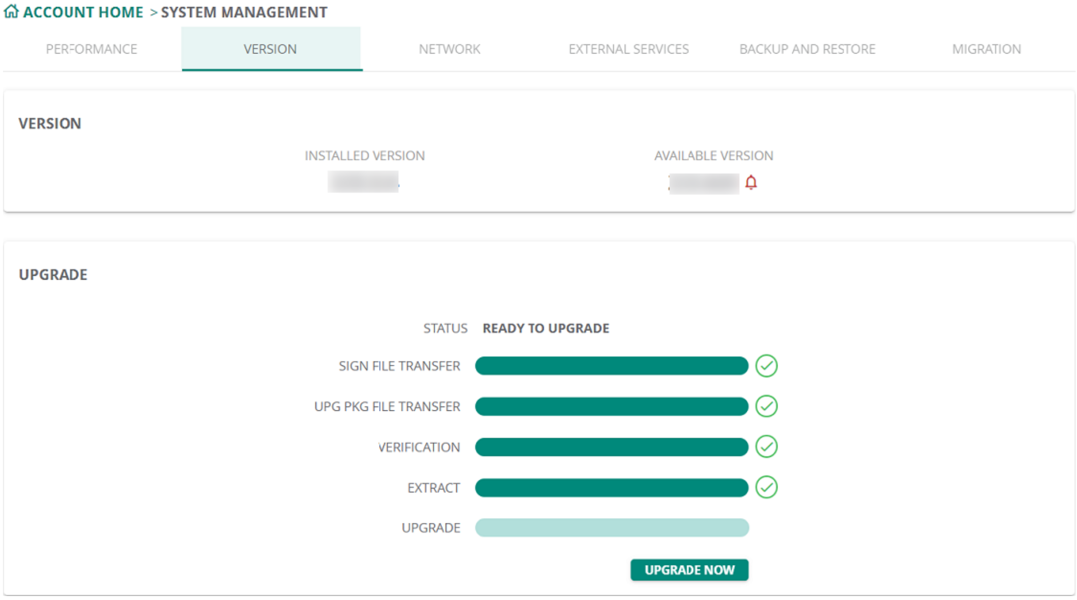
Once extraction is completed, upgrade status will change to **UPGRADE_NOT_STARTED**. You can trigger the update through CLI or GUI.

For CLI, enter option **4-1-3 Proceed With Upgrade** :

```
Enter option [ 0 - 3 ]: 3
Please confirm to start the upgrade to 2.5.7.0 version (Y/N):
```

To proceed upgrade through GUI, click the **Upgrade Now** button displayed on the **System Management** > **Versions** page after verification and extraction of the files.

Figure 6 *Upgrade Status*



VERSION

INSTALLED VERSION [redacted]

AVAILABLE VERSION [redacted]

UPGRADE

STATUS READY TO UPGRADE

SIGN FILE TRANSFER ✓

UPG PKG FILE TRANSFER ✓

VERIFICATION ✓

EXTRACT ✓

UPGRADE

Step 7: Retry Upgrade

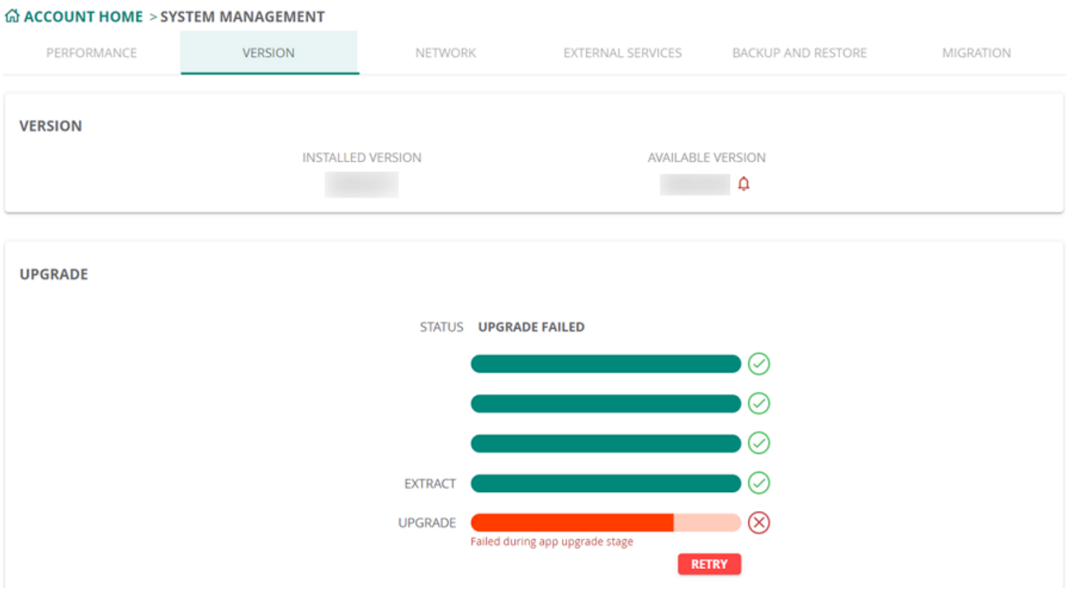
In case the upgrade fails, you can perform a retry through the CLI or GUI.

- To retry upgrade through CLI you have to use the same option **4-1-3 Proceed with Upgrade** again.

```
1. Upload Package
2. Upgrade Status
3. Proceed With Upgrade
====================================
b. back
m. main menu
0. exit
Enter option [ 0 - 3 ]: 3
Previous Upgrade was failed. Do you want to retry(Y/N):
```

- To retry upgrade through GUI, click the **Retry** button on the **System Management** > **Versions** page.

Figure 7 *Retry Upgrade*



STATUS UPGRADE FAILED

Failed during app upgrade stage

Offline Upgrade Through User Interface

Aruba Central On-Premises can be upgraded offline to the next version from user interface through the **Versions** page under **Maintain** > **System Management**.

NOTE

- For non FIPS users, you must first enable Airgap mode through Command Line Interface (CLI) to perform offline upgrade through **Versions** page on the user interface.
- For FIPS-enabled users, Airgap is enabled by default and you can perform offline upgrade through Versions page on the user interface directly.

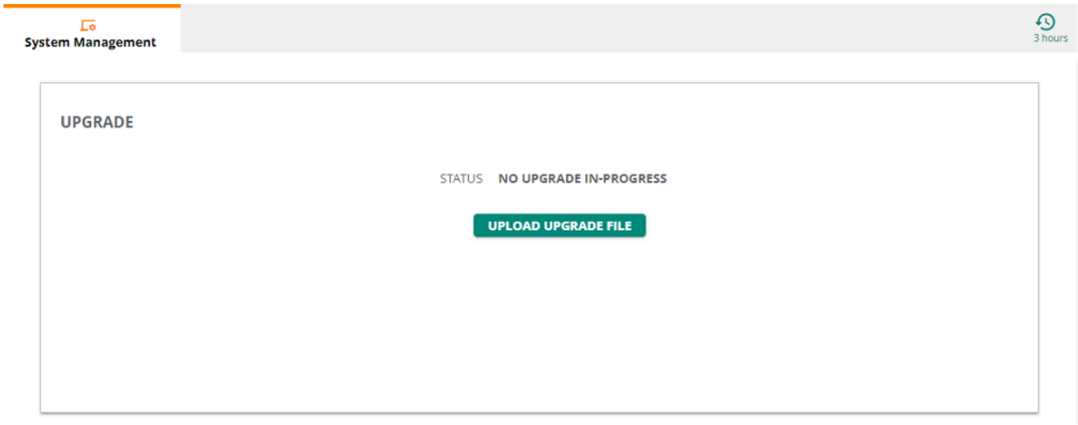
Prerequisite

You must download the Upload Package to your local system from the asp site before starting the upgrade.

Initial Stage Upgrade Watcher Workflow

This window is displayed when you log in to your Aruba Central On-Premises account within the deadline of the version upgrade (50 days from the date of version release). Based on the watcher file, the following page is displayed:

Figure 8 *Initial Upgrade*

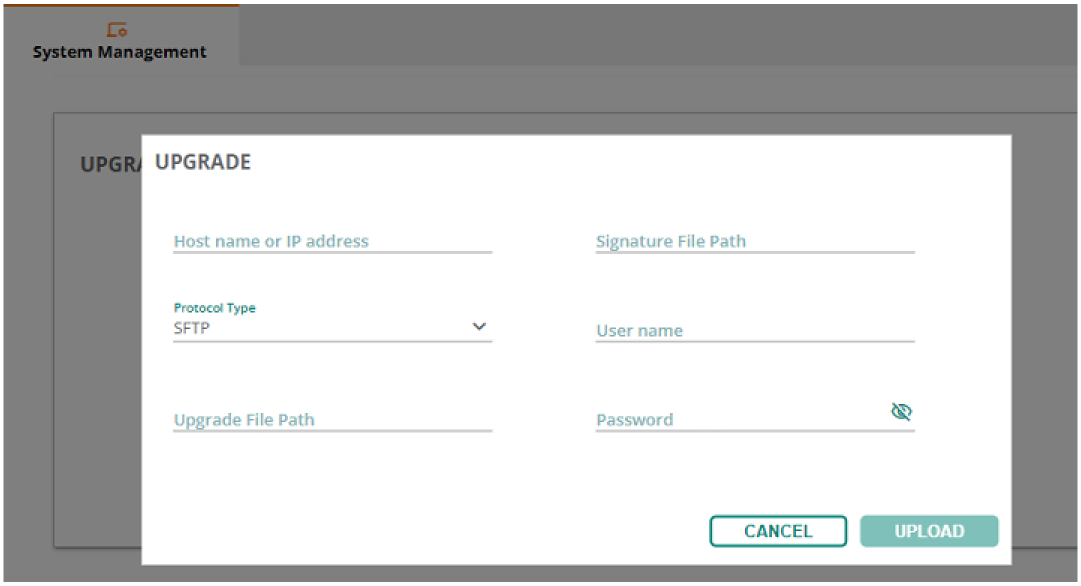


- **Upgrade**
  - **Status**—Provides the status of the upgrade.
  - **Upload Upgrade File**—Clicking this navigates you to the **Upgrade dialog** box where you can provide the following information to start upgrade process:
    1. Enter the **Host name / IP address**.
    2. Select the **Protocol Type** from the drop-down list, **SFTP** (Secure File Transfer Protocol) or **SCP** (Secure Copy Protocol).
    3. Copy and paste the file path for upgrade and signature file.

NOTE

For offline upgrade from Aruba Central On-Premises 2.5.7.6 onwards, use `apps_pkg` file instead of `upgrade_pkg` file. If you are on any older release than 2.5.7.6, you must continue using `apps_upgrade_pkg` file only.

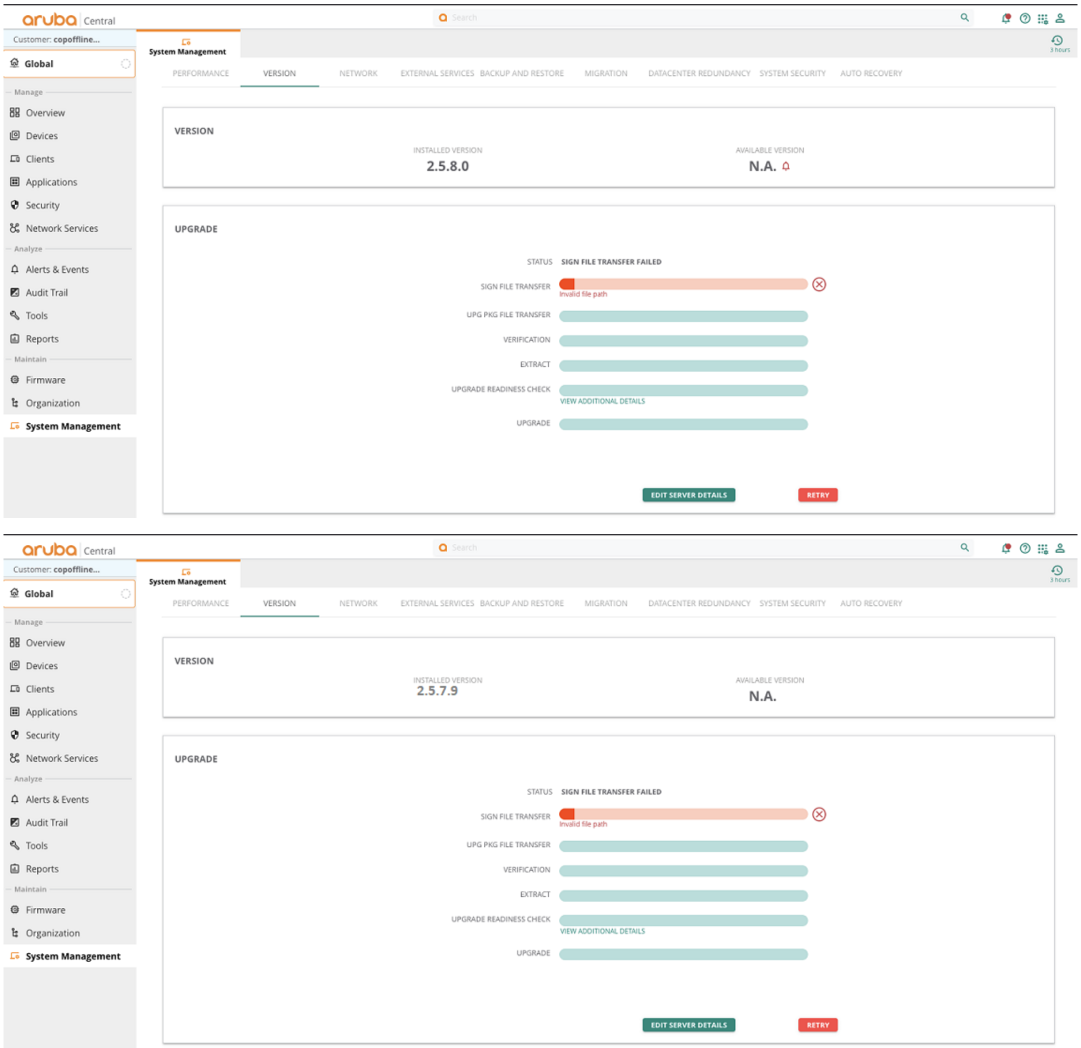
4. Enter the username and password and click **Upload**.



If there any error in the details provided on the **Upgrade** dialog box, **Retry** and **Edit Server Details** options are displayed so that you can restart the upload again by editing the details correctly. If the

Upgrade fails after multiple retries, contact Aruba Central support representative. The following page is displayed:

Figure 9 *Failed Upload*



VERSION

INSTALLED VERSION 2.5.8.0

AVAILABLE VERSION N.A.

UPGRADE

STATUS SIGN FILE TRANSFER FAILED

SIGN FILE TRANSFER – Invalid file path

UPG PKG FILE TRANSFER

VERIFICATION

EXTRACT

UPGRADE READINESS CHECK – VIEW ADDITIONAL DETAILS

UPGRADE

VERSION

INSTALLED VERSION 2.5.7.9

AVAILABLE VERSION N.A.

UPGRADE

STATUS SIGN FILE TRANSFER FAILED

SIGN FILE TRANSFER – Invalid file path

UPG PKG FILE TRANSFER

VERIFICATION

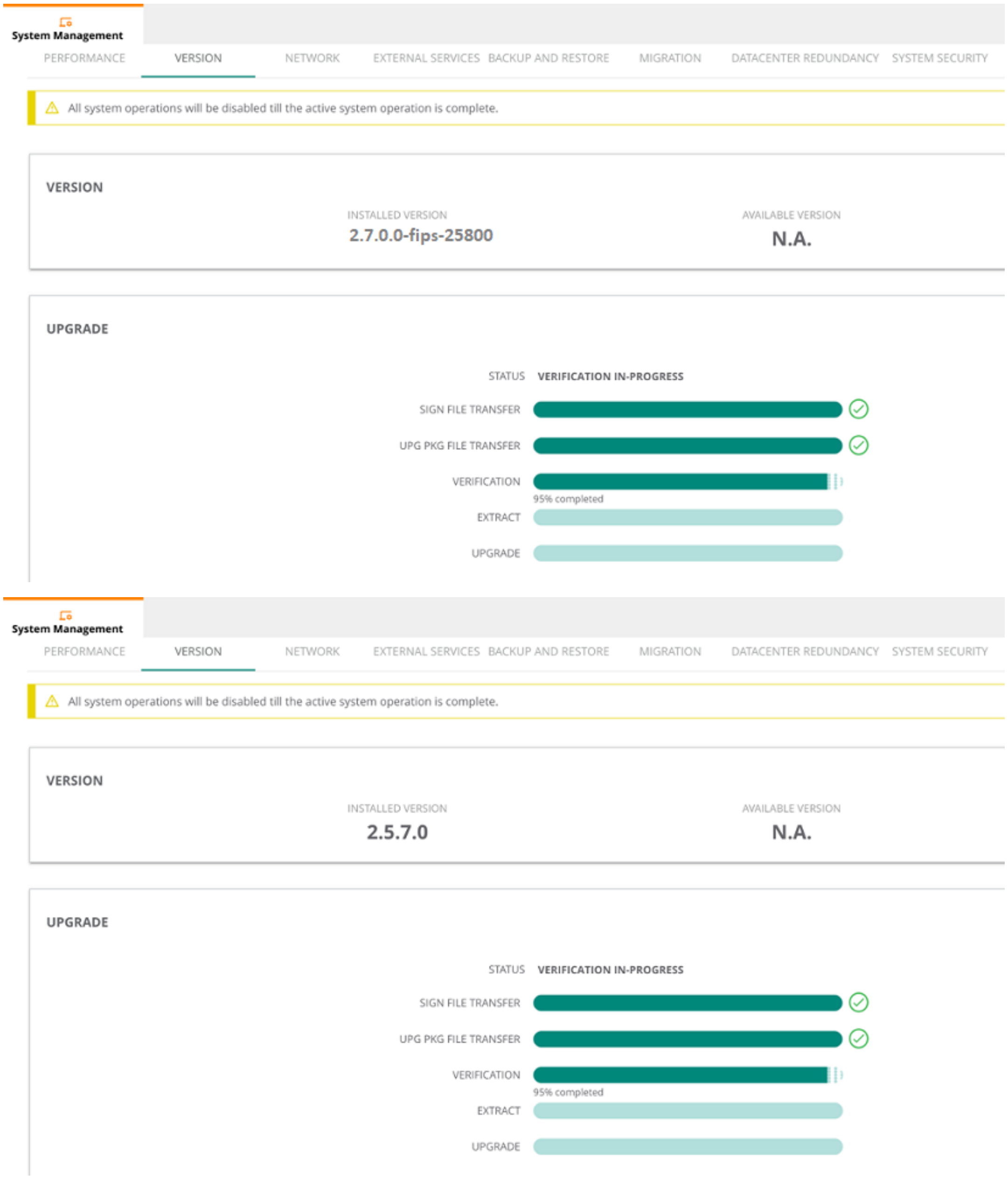
EXTRACT

UPGRADE READINESS CHECK – VIEW ADDITIONAL DETAILS

UPGRADE

If the upload is successful and there is no error in the details provided, the following page is displayed:

Figure 10 *Successful File Upload*



System Management

PERFORMANCE | VERSION | NETWORK | EXTERNAL SERVICES | BACKUP AND RESTORE | MIGRATION | DATACENTER REDUNDANCY | SYSTEM SECURITY

⚠ All system operations will be disabled till the active system operation is complete.

VERSION

INSTALLED VERSION 2.7.0.0-fips-25800

AVAILABLE VERSION N.A.

UPGRADE

STATUS VERIFICATION IN-PROGRESS

SIGN FILE TRANSFER ✓

UPG PKG FILE TRANSFER ✓

VERIFICATION

95% completed

EXTRACT

UPGRADE

System Management

PERFORMANCE | VERSION | NETWORK | EXTERNAL SERVICES | BACKUP AND RESTORE | MIGRATION | DATACENTER REDUNDANCY | SYSTEM SECURITY

⚠ All system operations will be disabled till the active system operation is complete.

VERSION

INSTALLED VERSION 2.5.7.0

AVAILABLE VERSION N.A.

UPGRADE

STATUS VERIFICATION IN-PROGRESS

SIGN FILE TRANSFER ✓

UPG PKG FILE TRANSFER ✓

VERIFICATION

95% completed

EXTRACT

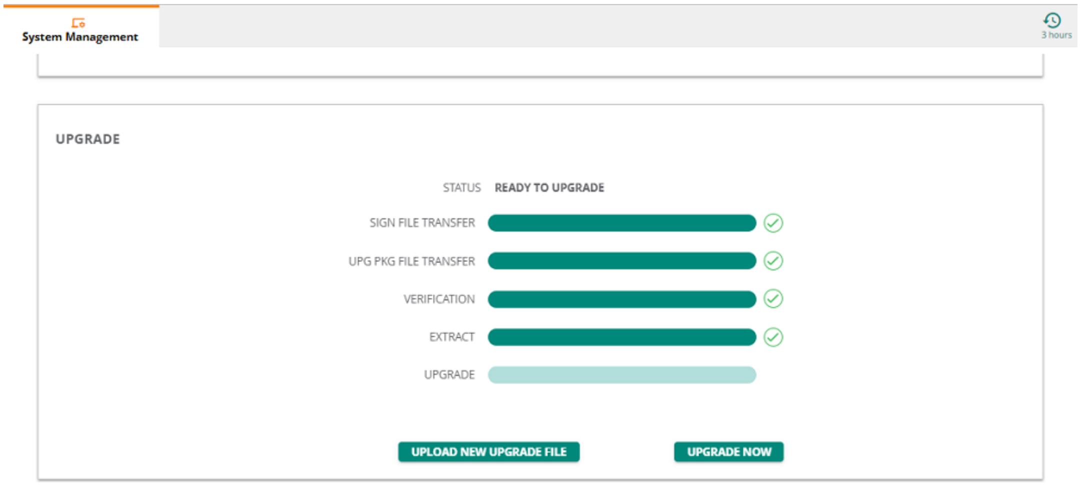
UPGRADE

- **Version**
  - **Installed Version** —The version of the Aruba Central On-Premises currently installed.
  - **Available Version**—Since the installed version is latest, the available version is displayed is NA.
- **Upgrade**
  - **Status**—Provides the status and progress bar for file transfer, verification, extract, and upgrade.

Upgrade Watcher Workflow

Once the file upload is complete, you can now start the upgrade process to upgrade your Aruba Central On-Premises account to the latest version. The following page is displayed:

Figure 11 *Upgrade*



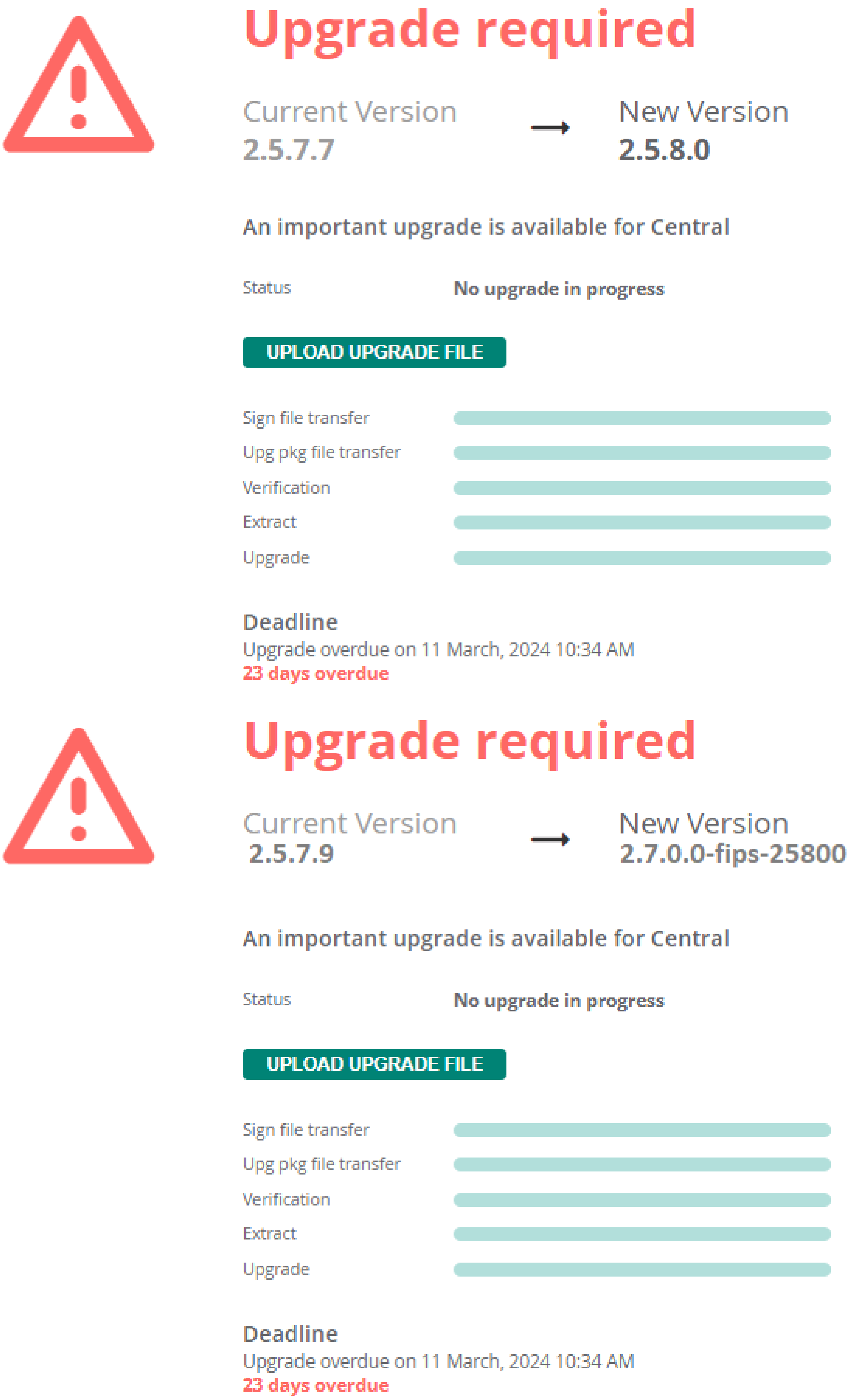
STATUS READY TO UPGRADE

Click the **Upgrade Now** option to start the upgrade. In case you want to upload a new upgrade file, you can click **Upload New Upgrade File** option, to upload the upgrade package file. It also displays the status and progress bar for file transfer, verification, extract, and upgrade.

Upgrade Required (Force Upgrade) after Watcher File Upload

This window is displayed when you log in to your Aruba Central On-Premises account after the deadline is missed. This window indicates that you have missed the upgrade deadline and an immediate upgrade is required. All the account GUI functionality is blocked till the Aruba Central On-Premises is upgraded to the latest version. To start updating, you must first upload the upgrade. Click **Upload Upgrade File** to initiate the upgrade and enter all the required details on the Upgrade dialog box. For more information, see Upload Upgrade File—Clicking this navigates you to the Upgrade dialog box where you can provide the following information to start upgrade process:

Figure 12 *Upgrade Required*



Upgrade required

Current Version 2.5.7.7 → New Version 2.5.8.0

An important upgrade is available for Central

Status: No upgrade in progress

Deadline

Upgrade overdue on 11 March, 2024 10:34 AM

23 days overdue

Upgrade required

Current Version 2.5.7.9 → New Version 2.7.0.0-fips-25800

An important upgrade is available for Central

Status: No upgrade in progress

Deadline

Upgrade overdue on 11 March, 2024 10:34 AM

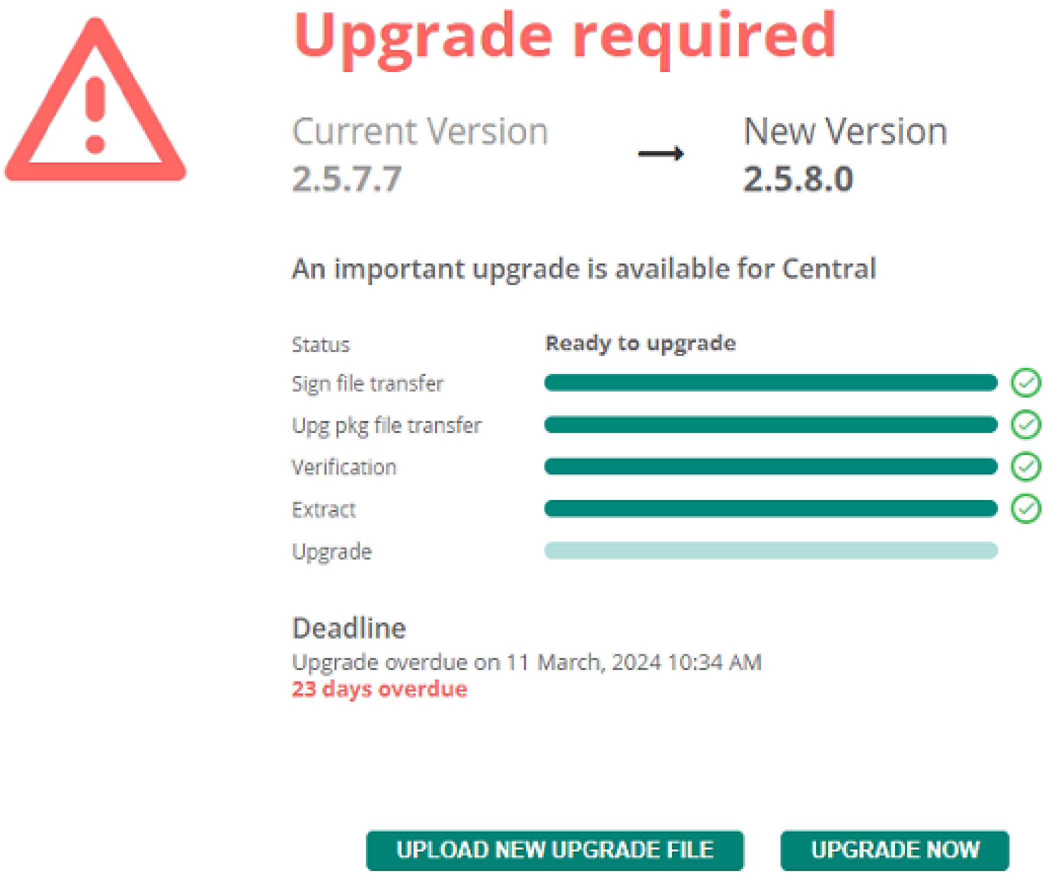
23 days overdue

- **Current Version**—Current running version.
- **New Version**—Next major available version.

- **Status**—Provides the status and progress bar for file transfer, verification, extract, and upgrade.
- **Upload Upgrade File**—Enables to upload the upgrade package files.
- **Deadline**—Displays the number of overdue days post deadline.

Once the watcher file is extracted, the following page is displayed:

Figure 13 *Upgrade after Watcher File Extraction*



Upgrade required

Current Version 2.5.7.7 → New Version 2.5.8.0

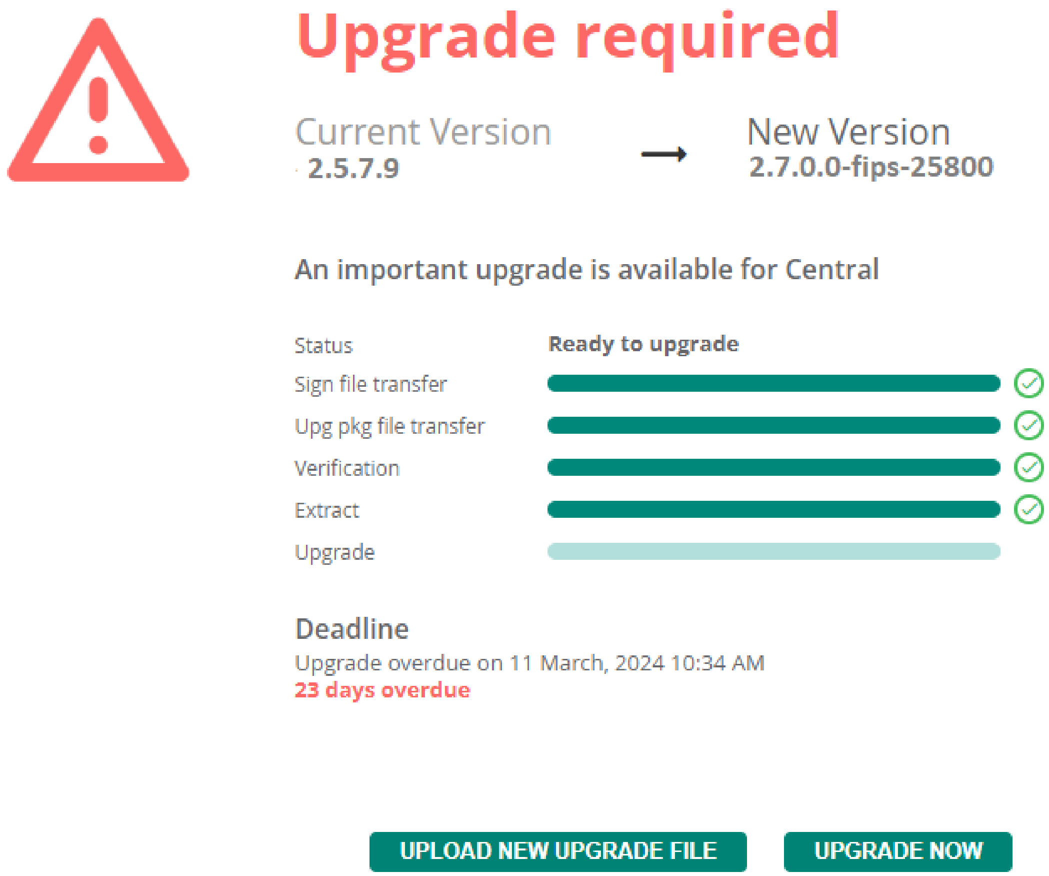
An important upgrade is available for Central

Status	Ready to upgrade	
Sign file transfer		✓
Upg pkg file transfer		✓
Verification		✓
Extract		✓
Upgrade		

Deadline

Upgrade overdue on 11 March, 2024 10:34 AM

23 days overdue



Upgrade required

Current Version
2.5.7.9
→
New Version
2.7.0.0-fips-25800

An important upgrade is available for Central

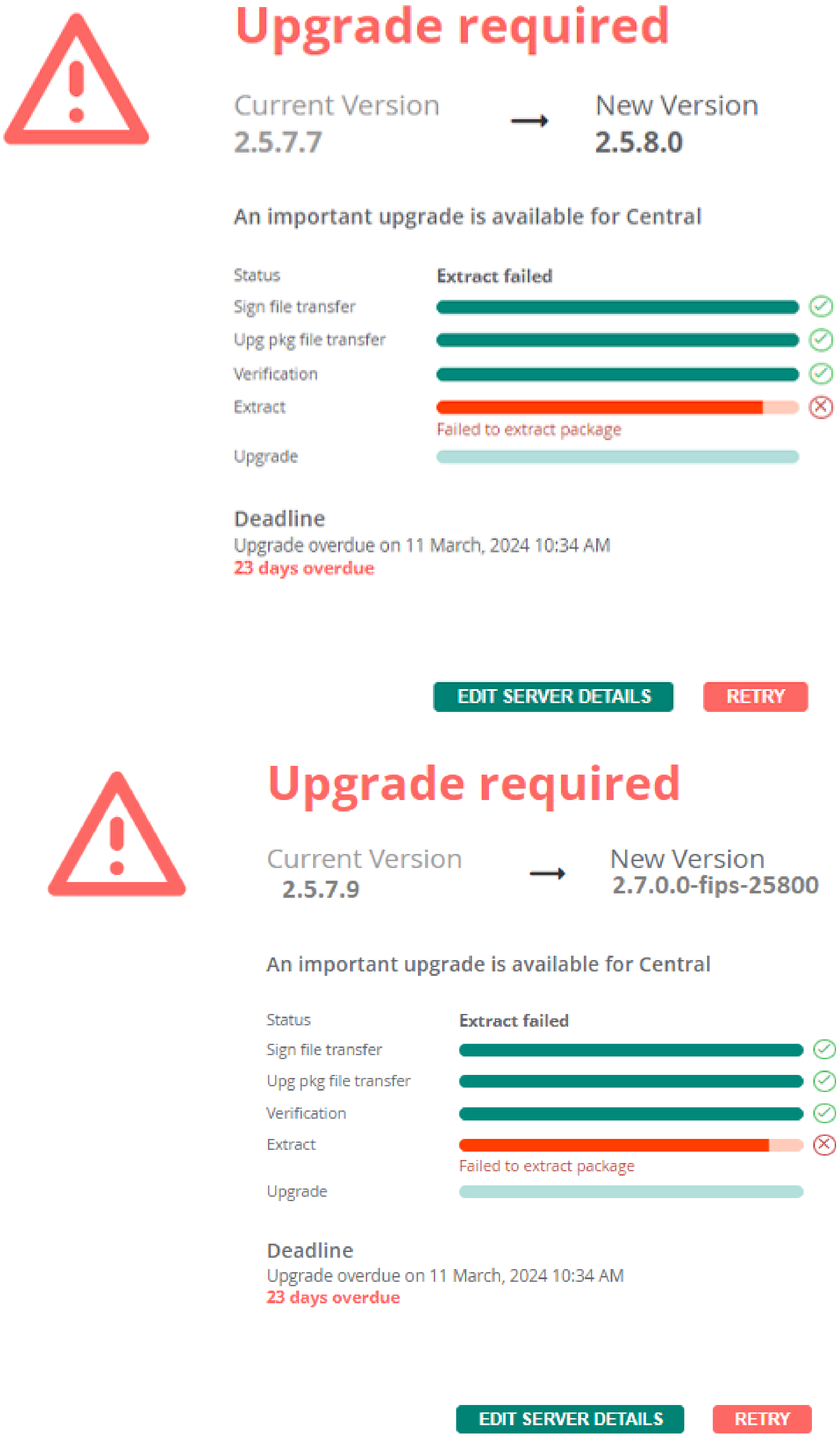
Status	Ready to upgrade
Sign file transfer	✓
Upg pkg file transfer	✓
Verification	✓
Extract	✓
Upgrade	

Deadline
Upgrade overdue on 11 March, 2024 10:34 AM
23 days overdue

- **Current Version**—Current running version.
- **New Version**—Next major available version.
- **Status**—Provides the status and progress bar for file transfer, verification, extract, and upgrade.
- **Deadline**—Displays the number of overdue days post deadline.
- **Upload New Upgrade File**—Enables to upload the upgrade package files.
- **Upgrade Now**—Allows you to initiate the upgrade process.

If there any error in the details provided on the **Upgrade** dialog box, **Retry** and **Edit Server Details** options are displayed so that you can restart the upload again by editing the details correctly. If the Upgrade fails after multiple retries, contact Aruba Central support representative. The following page is displayed:

Figure 14 *Upgrade Failed*



Upgrade required

Current Version 2.5.7.7 → New Version 2.5.8.0

An important upgrade is available for Central

Status: Extract failed

Sign file transfer ✓

Upg pkg file transfer ✓

Verification ✓

Extract ⊗

Failed to extract package

Upgrade

Deadline

Upgrade overdue on 11 March, 2024 10:34 AM

23 days overdue

Upgrade required

Current Version 2.5.7.9 → New Version 2.7.0.0-fips-25800

An important upgrade is available for Central

Status: Extract failed

Sign file transfer ✓

Upg pkg file transfer ✓

Verification ✓

Extract ⊗

Failed to extract package

Upgrade

Deadline

Upgrade overdue on 11 March, 2024 10:34 AM

23 days overdue

Online Upgrade Through the Versions Page

Aruba Central On-Premises can be upgraded online to next version from **Versions** page on the user interface.

Upgrade Watcher Workflow for Regular-Online User

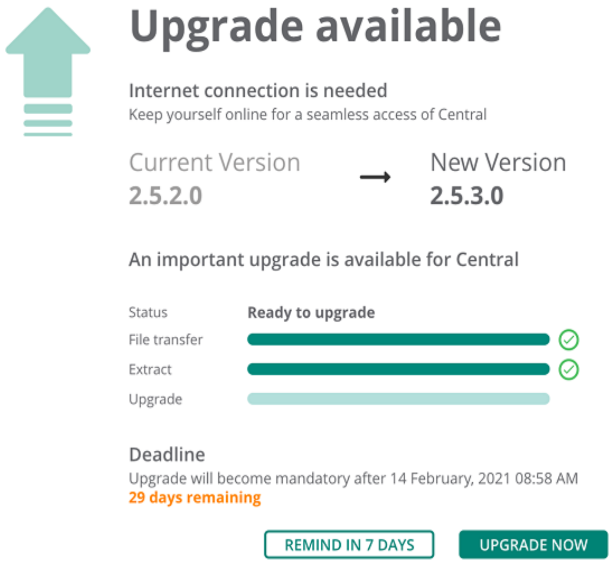
This section describes the upgrade workflow and the requirements for the regular-online Aruba Central On-Premises user accounts. Based on the version availability, upon logging onto your Aruba Central On-Premises account, one of the following pages is displayed:

1. **Upgrade Available**—This window is displayed when you log in to your Aruba Central On-Premises account within the deadline of the version upgrade (50 days from the date of version release). The upgrade available window provides the following information:
    - **Internet Connection is needed**—Informs the connectivity requirement for the process.
    - **Current version**—Current running version.
    - **New versions**—Next major available version.
    - **Status**—Provides the status and progress bar for file transfer, extract, and upgrade.
    - **Deadline**—Displays the number of days remaining for upgrade. The number of days varies depending on the version available date and the day of login. For example, if the version was available on 10th of December and the user logs in on 12th of December, the remaining days gets changed to 47 days within which the account needs to be upgraded.
    - **Upgrade Now**—Allows you to initiate the upgrade process.
    - **Go to Versions**—This tab is displayed if any one of the extraction stage is interrupted, in progress or failed. Clicking on the **Go to version** navigates to **System Management > Version** tab with version upgrade in process.
    - **Remind in x days**—Allows you to snooze the notification for some days. Notification can be snoozed for 7 days (50-20 remaining days), 5 days (20-10 remaining days), 3 days (10-5 remaining days), 2 days(5-3 remaining days), and 1 (for the rest remaining days). On snoozing the notification, you can use the account normally and the next notification comes after the set dates.

    To upgrade the version once notified, click **Upgrade Now** to initiate the upgrade process. You can also navigate to **System Management > Version** tab to initiate the upgrade. For more information on how to navigate to version tab, see Version.

    The following example image displays the **Upgrade available** window.

Figure 15 *Upgrade Available*



Upgrade available

Internet connection is needed

Keep yourself online for a seamless access of Central

Current Version 2.5.2.0 → New Version 2.5.3.0

An important upgrade is available for Central

Status: Ready to upgrade

Deadline

Upgrade will become mandatory after 14 February, 2021 08:58 AM

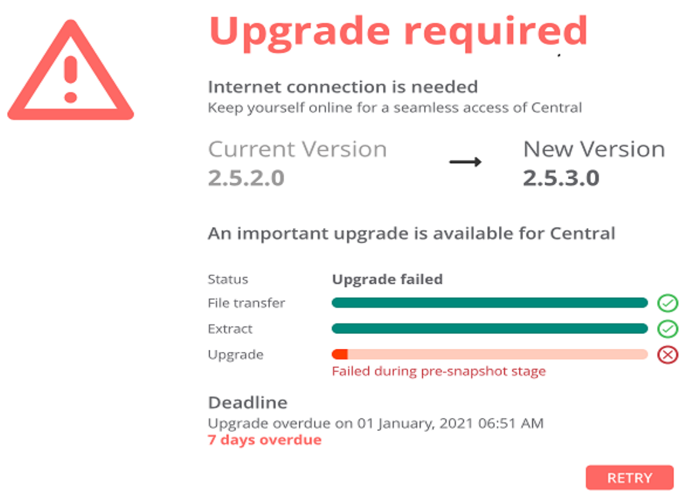
29 days remaining

2. **Upgrade Required**—This window is displayed when you log in to your Aruba Central On-Premises account after the deadline is missed. This window indicates that you have missed the upgrade deadline and an immediate upgrade is required. All the account GUI functionality is blocked till the Aruba Central On-Premises is upgraded to the latest version. To upgrade, click **Upgrade Now** to initiate the upgrade. The upgrade required window provides the following information:
   - **Internet Connection is needed**—Informs the connectivity requirement for the process.
   - **Current version**—Current running version.
   - **New versions**—Next major available version.
   - **Status**—Provides the status and progress bar for file transfer, extract, and upgrade.
   - **Deadline**—Displays the number of overdue days post deadline.
   - **Upgrade Now**—Allows you to initiate the upgrade process.
   - **Retry**—This tab is displayed only when any one of the upgrade stage fails. Click **Retry** to retry the upgrade process. If the Upgrade fails after multiple retries, contact Aruba Central support representative.

   Once the upgrade is successful, the account comes to its normal functionality.

   The following example image displays the **Upgrade required** window with retry option.

Figure 16 *Upgrade Required*



Upgrade required

Internet connection is needed

Keep yourself online for a seamless access of Central

Current Version → New Version

2.5.2.0 → 2.5.3.0

An important upgrade is available for Central

Status: Upgrade failed

File transfer ✓

Extract ✓

Upgrade ⊗

Failed during pre-snapshot stage

Deadline

Upgrade overdue on 01 January, 2021 06:51 AM

7 days overdue

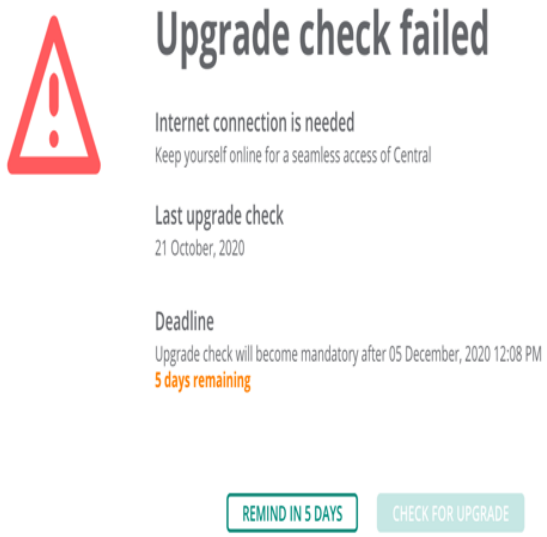
Upgrade Watcher Workflow for Occasional-Online User

This section describes the upgrade workflow and the requirements for the occasional-online Aruba Central On-Premises user accounts. This scenario is based on the users that logs into Aruba Central On-Premises after 49 days or a maximum of 55 days from the date of connectivity loss. All the account GUI functionality is allowed and the user has to upgrade to the major available version within the prescribed period. Based on the account login period, one of the following pages is displayed:

1. **Upgrade Check Failed-**—This window is displayed when the user logs into Aruba Central On-Premises within the above mentioned periods. The upgrade check failed window provides the following information:
   - **Internet Connection is needed**—Informs the connectivity requirement for the process.
   - **Last Upgrade Check**—Displays the date of last upgrade check.
   - **Deadline**—Displays the remaining days for mandatory upgrade check.
   - **Check for Upgrade**—Once connected, it check for the status and redirects you to the Upgrade available/ Upgrade required page.
   - **Remind in x days**—Allows you to snooze the notification. Snoozing can be done for 5 days (on 49th day) and 1 day for the remaining.

   The following example image displays the **Upgrade check failed** window.

Figure 17 *Upgrade Check Failed*



Upgrade check failed

Internet connection is needed

Keep yourself online for a seamless access of Central

Last upgrade check

21 October, 2020

Deadline

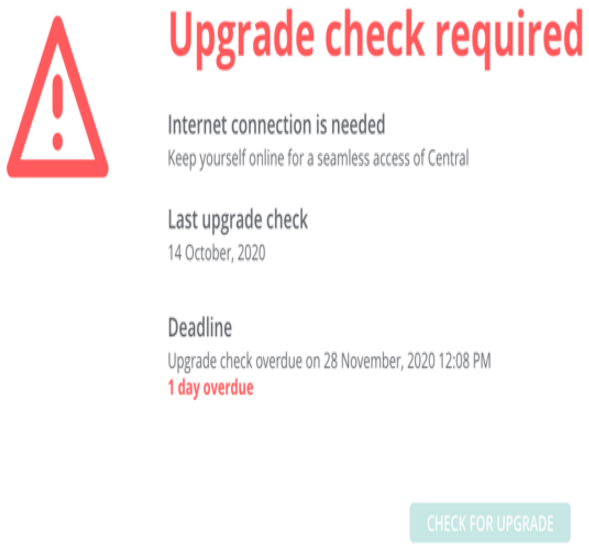
Upgrade check will become mandatory after 05 December, 2020 12:08 PM

5 days remaining

2. **Upgrade Check Required**—This window is displayed when the user logs into Aruba Central On-Premises account after 55 days from the day of connectivity loss. In this scenario, the user account is blocked and an immediate upgrade check is required. The upgrade check required window displays the following information:
   - **Internet Connection is needed**—Informs the connectivity requirement for the process.
   - **Last Upgrade Check**—Displays the date of last upgrade check.
   - **Deadline**—Displays the remaining days for mandatory upgrade check.
   - **Check for Upgrade**—Once connected, it check for the status and redirects you to the Upgrade available/ Upgrade required page.

   The following example image displays the **Upgrade check required** window.

Figure 18 *Upgrade Check Required*



Upgrade check required

Internet connection is needed

Keep yourself online for a seamless access of Central

Last upgrade check

14 October, 2020

Deadline

Upgrade check overdue on 28 November, 2020 12:08 PM

1 day overdue

NOTE

In a FIPS-enabled Aruba Central On-Premises setup, the users are notified of any available version upgrade by e-mail or by the TAC team. Aruba Central On-Premises does not provide notification for any available version upgrade through the WebUI."

Verifying Configuration Before Upgrade

Aruba recommends to perform the pre-upgrade health check for validating the Aruba Central On-Premises cluster configuration. This operation is required to avoid issues that may be encountered and halt the upgrade. You must first ensure that the cluster complies with the requirements and verify the stability before an upgrade.

If any check fails, rectify it and then proceed to upgrade. Otherwise, upgrade will fail. Contact Aruba Support for any assistance or check details in the *deployment-tools-pre-upgrade-health-check* pod and **Audit Trial** logs.

The following checks must be performed:

- Ensure that all mandatory CNAMEs are resolvable. If CNAMEs are not resolved, the *CNAME_UNRESOLVABLE* error is encountered. Aruba Central On-Premises WebUI will list the CNAMEs that are not resolvable.
- Ensure that the health status of infra services is in **Good** state on all nodes of the cluster. Otherwise, the upgrade fails with the *Pre Upgrade Health Check Failed* error. For details regarding this error, see the IVT logs. Download the logs by clicking **Generate Logs** under **System Management** > **Version** > **Logs**.
- Ensure all nodes in the cluster run 512 GB RAM. Otherwise, the upgrade fails with the *Pre Upgrade Health Check Failed* error. For details regarding this error, check logs in the **Audit Trail** page.
- Ensure all nodes in the cluster have 10 GbE interface bandwidth. Otherwise, the upgrade fails with the *Pre Upgrade Health Check Failed* error. For details regarding this error, check logs in the **Audit**

Trail page.

- Ensure all nodes in the cluster have DNS server configuration that resolves both internal and external URLs (core update and Quay). Otherwise, the upgrade fails with the *Pre Upgrade Health Check Failed* error. For details regarding this error, check logs in the **Audit Trail** page.
- Ensure all nodes in the cluster have 3.4 TB disk space. Otherwise, the upgrade fails with the *Pre Upgrade Health Check Failed* error. For details regarding this error, check logs in the **Audit Trail** page.
- Ensure that if any recent replace node operation is done, is successful. Otherwise, the upgrade fails with the *Pre Upgrade Health Check Failed* error. For details regarding this error, check logs in the **Audit Trail** page.

Chapter 6
Switching to 10 Gigabit Ethernet Interface

You must use Command Line Interface (CLI) from the ILO console to run the Switch Network Interface command.

NOTE

- For users who are still on the 1 Gigabit Ethernet (GbE) switch interface, it is mandatory to first upgrade to Aruba Central On-Premises 2.5.6.7 version before switching to the 10 GbE interface.
- Ensure to run the commands for all the nodes in the cluster.

To switch to 10 GbE interface, complete the following steps:

1. From a secure shell (SSH) client, open an SSH connection.
2. Login as **copadmin**.
3. When prompted, enter the **copadmin** password.

   A list of commands is displayed.

```
1. System
2. File Operations
3. Show
4. System Configuration
5. Advancedswitch
6. Security
7. Support
8. Temporary Root Shell
9. Authentication
10. Certificate configuration
11. Search commands
====================================
0. exit

Enter option [ 0 - 11 ]:
```

4. Enter command option **4** from the Show commands menu to view the system configuration settings.

```
Enter option [ 0 - 11 ]: 4
1. Upgrade
2. Network Setup
3. Proxy Setup
4. Setup Timezone
5. Setup NTP
6. Node Setup
7. Airgap
8. Disaster Recovery
```

```
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 7 ]:
```

5. Enter command option **2** from the System Configuration commands menu to view the network setup settings.

```
Enter option [ 0 - 8 ]: 2
1. Permanent (Network settings)
2. Temporary (Network settings)
3. Switch Network Interface
====================================
b. back
m. main menu
0. exit

Enter option [ 0 - 3 ]:
```

6. Enter command option **3** from the Network Setup commands menu to switch to 10 GbE network interface.

7. Enter the 10 Gigabit Ethernet interface details.

   In the following example, a new network interface ("ens1f1") is entered for 10 GbE.

```
Enter option [ 0 - 3 ]: 3

The network interface currently configured is: eno1
Please capture and note down current network configurations for interface,
IP Address, Subnet mask and Gateway before
proceeding further.

Current Network Settings
--------------------------
Current Interface          : eno1
IP Address                 : 10.22.154.83
Subnet Mask                : 255.255.255.0
Gateway                    : 10.22.154.3
DNS                        : 10.20.50.10
Secondary DNS              : 10.20.50.15
FQDN                       : cop-upgrade-node3.arubathena.com

Enter new interface name: ens1f1
Configuring the ens1f0 network interface
Interface is up...moving on

Network Settings Being Applied
-------------------------------
Network Interface          : ens1f1
IP Address                 : 10.22.154.83
Subnet Mask                : 255.255.255.0
Gateway                    : 10.22.154.3
DNS                        : 10.20.50.10
Secondary DNS              : 10.20.50.15
```

```
FQDN                       : cop-upgrade-node3.arubathena.com

Network settings exist: will be reset to a new value
9f83d89df0f5
Kubernetes is up...moving on
deployment.apps/coredns scaled
deployment.apps/coredns scaled
1
OK
pod "platform-config-platform-uwsgi-deployment-86dc68d4d6" deleted
updating cache, please wait
Interface is updated to ens1f1

Press [Enter] key to continue...
```

NOTE

- You cannot switch interface from Aruba Central On-Premises CLI to a port slower than 10 Gbps.
- If all nodes are not connected to interfaces with same speed, any addition or replacement of nodes might fail.

Chapter 7
Migrating the AirWave Server

Important Information for Migration

The following are the requirements and guidelines for the migration process:

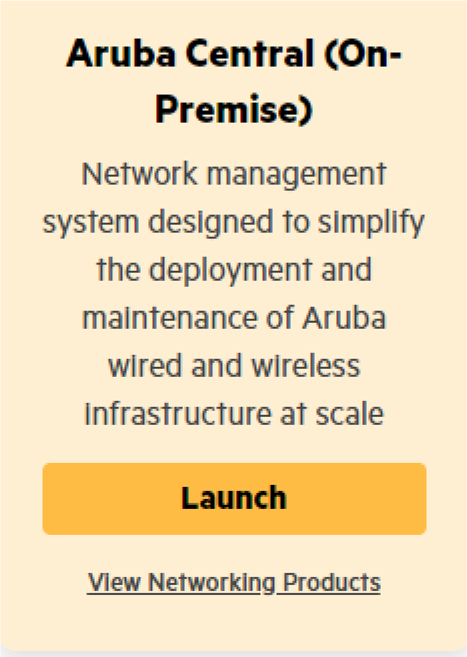
- The AirWave system must be running a minimum AirWave version of 8.2.8.2 for the migration to proceed. If the AirWave system is running an earlier version, refer to the AirWave documentation to upgrade the version to 8.2.8.2 or later versions.
- Only those APs, controllers, and switches that are supported in Aruba Central On-Premises are migrated. For information on supported hardware, see *Supported Devices* section.
- As part of migration, Visual RF and the device inventory for CAPs, IAPs, controllers, and Aruba/HPE switches are migrated.
- For controllers, the device credentials for SNMP and HTTPS profiles are mapped.
- Migration of multiple AirWave systems to a single Aruba Central On-Premises server is supported. That is, you can migrate multiple AirWave systems to Aruba Central On-Premises by adding the IP addresses or **AMP Hostnames** of each AirWave system individually.
- All the historical data including data related to reports, monitoring, and stats are not migrated from Airwave to Aruba Central On-Premises during the migration process.
- Templates are not migrated from Airwave to Aruba Central On-Premises during the migration process. You must manually create a new template in Aruba Central On-Premises based on the requirement.
- All data related to VisualRF is migrated from Airwave to Aruba Central On-Premises during the migration process.

Accessing Aruba Central On-Premises

The Dashboard gives you access to the feature application card, Aruba Central On-Premises added to your account. After launching the application, you can interact and use it through HPE GreenLake.

To launch the Aruba Central On-Premises app, perform the following steps.

1. From the HPE GreenLake home page, Aruba Central On-Premises is available on the Dashboard.
2. Click Launch on the Aruba Central On-Premises tile to launch the application.



Aruba Central (On-Premise)

Network management system designed to simplify the deployment and maintenance of Aruba wired and wireless infrastructure at scale

Logging Aruba Central On-Premises

To log out of Aruba Central On-Premises, complete the following steps:

1. On the Aruba Central On-Premises WebUI, click the user icon (👤) in the header pane.
2. Click **Logout**.

Accessing the Migration Page

To access the **Migration** page, complete the following steps:

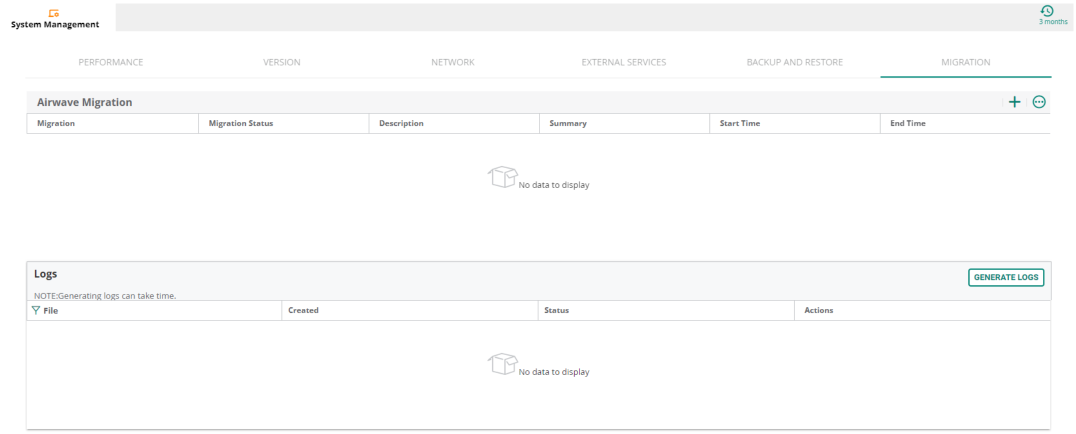
1. In the **Aruba Central On-Premises** app, set the filter to **Global**.
2. Under **Maintain**, click **System Management**.
3. Click the **Migration** tab.

   The **Migration** page is displayed.
4. Click the **Migration** tab at the top right corner of the table to add a new migration task.

   For more information, see Performing the Migration on page 55.

The following image displays the **Migration** page.

Figure 19 *Viewing the Migration Page*



The following table provides **Airwave Migration** parameter details.

Table 5: *Migration Parameters*

Name	Description
Migration	FQDN or IP address of the AMP server.
Migration Status	Indicates the current status of the migration. For example, Migration Success, Waiting to start migration, or Migration Failed.
Description	Provides a description of the current status of migration.
Summary	Provides a summary of the migration. Following are some of the messages displayed: ▪ Number of devices existing on Aruba Central On-Premises ▪ Number of devices on AirWave 8.x ▪ Number of devices to migrate ▪ Number of devices successfully migrated ▪ Number of devices failed to migrate
Start Time	Displays the start time of the migration.
End Time	Displays the end time of the migration.

Migration Status

In the **Airwave Migration** table, the **Status** column displays the following list of migration status:

- Waiting to start migration
- Migration Stopped
- Migration Started
- AW8.X generating migration dump
- AW8.X migration dump is ready
- COP migration is in progress
- Migration Success
- Migration Failed

Migration Descriptions

In the **Airwave Migration** table, the **Description** column displays the following list of migration status:

- Migration of AMP not started
- Starting migration of AMP to COP
- Connecting to AMP
- Could not establish connection to AMP
- Could not prepare backup on AMP
- Waiting for AMP backup to be prepared
- AMP backup not prepared after 2 hours, please check AMP logs
- AMP backup is ready for download from AMP
- AMP backup is being downloaded to COP
- AMP backup download failed
- AMP backup downloaded successfully
- Restoring AMP backup in COP
- AMP version not supported for migration
- Migrating devices to COP Migrating profiles to COP
- Checking for VRF data to migrate VRF migration in progress
- Migration of VRF data failed VRF
- Migration did not complete after 4 hours, please check the VRF logs
- Migration of AMP completed successfully, VRF data not found
- Migration was terminated abruptly, please retry migration
- Migration of AMP completed successfully
- Exception occurred during migration, please check the logs
- Another system operation is active, retry after sometime

NOTE

During the migration process, a new AMP back up is created in AirWave and transferred to the Aruba Central On-Premises. The scheduled nightly backup is independent of the backup operation performed as a part of the migration process.

Performing the Migration

For performing the migration, you need to add the AirWave server that is running the older software version to Aruba Central.

Aruba Central On-Premises supports both offline and online migration.

Online Migration

Aruba Central On-Premises establishes a connection with AirWave to perform an online migration of the onboarded devices and VisualRF data from AirWave to Aruba Central On-Premises.

To perform an online migration, complete the following steps with active internet connection:

1. In the **Aruba Central On-Premises** app, set the filter to **Global**.
2. Under **Maintain**, click **System Management**.
3. Click the **Migration** tab.

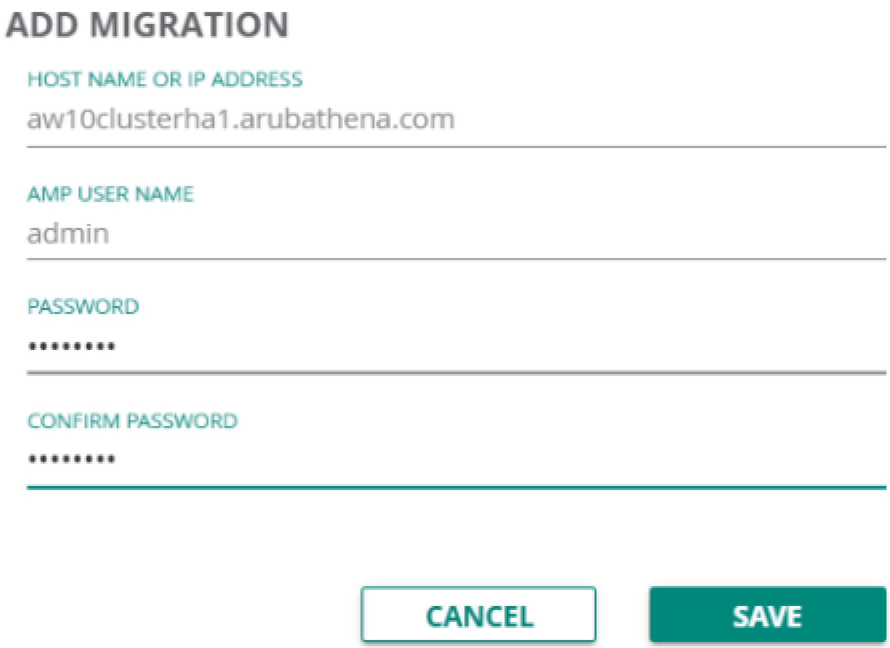
   The **Migration** page is displayed.

4. Click + in the **Airwave Migration** table.

   The **Add Migration** window is displayed.
5. In the **Add Migration** window, select the **Online Migration** option.
6. Enter the following details:
   - **Hostname or IP Address**—Enter the IP address of the AirWave Management Platform (AMP).
   - **AMP User name**—During the migration process, a new AMP back up is created in AirWave and transferred to the Aruba Central On-Premises. The scheduled nightly backup is independent of the backup operation performed as a part of the migration process.
   - **Password**—Enter the password associated with the administrative account.
   - **Confirm password**—Re-enter the password.
7. Click **Save** to start the migration process.

The following image displays the online migration of the AirWave server using the hostname of the AMP server.

Figure 20 *Online Migration using Hostname*



ADD MIGRATION

HOST NAME OR IP ADDRESS
aw10clusterha1.arubathena.com

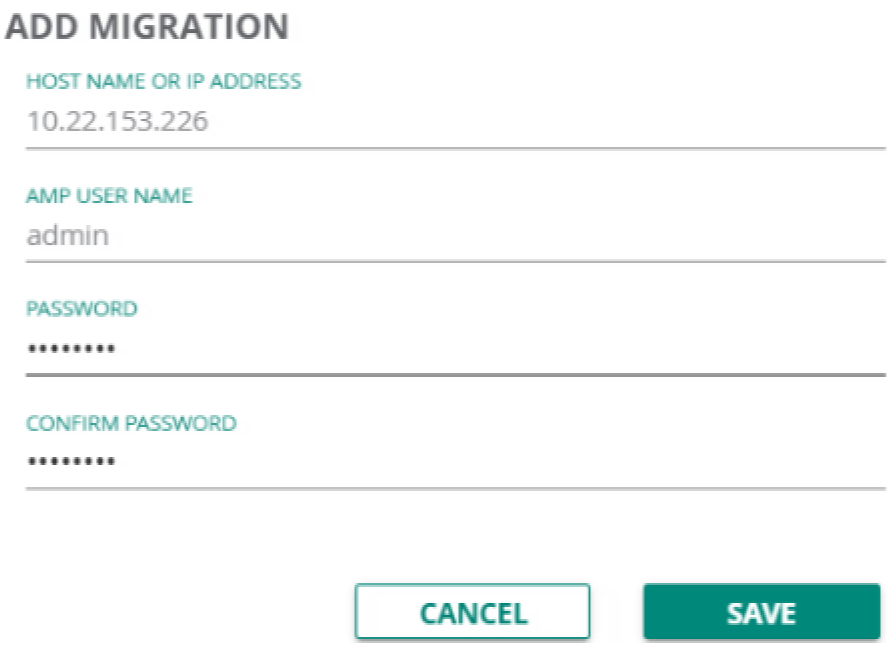
AMP USER NAME
admin

PASSWORD
••••••••

CONFIRM PASSWORD
••••••••

The following image displays the online migration of the AirWave server using the IP address of the AMP server.

Figure 21 *Online Migration using IP Address*



ADD MIGRATION

HOST NAME OR IP ADDRESS
10.22.153.226

AMP USER NAME
admin

PASSWORD
••••••••

CONFIRM PASSWORD
••••••••

NOTE

- You can add multiple IP addresses to migrate from multiple AirWave servers to one Aruba Central On-Premises server. In this case, each AMP will be migrated sequentially.
- You can not delete an AMP when the migration is in-progress.
- In the **Airwave Migration** table, the ✎ , ⏻ , and, 🗑 icons allow you to edit, restart, and delete the migration.
- All system operations are disabled until the active system operation is complete. The migration, backup and restore, high availability processes, and the upgrade operations are the system operations in Aruba Central On-Premises

Offline Migration

Aruba Central On-Premises performs an offline migration of the onboarded devices and VisualRF data from AirWave to Aruba Central On-Premises by uploading the backup file that was earlier downloaded from AirWave.

Offline Migration is also called as the Inplace Migration. The user need not have the AirWave server up and running for an offline migration. Offline migration is required when the user wants to deploy Aruba Central On-Premises on the same AirWave server. The advantage of an offline migration is that the user can onboard all the devices to Aruba Central On-Premises from AirWave in a single operation.

In offline migration, the Aruba Central On-Premises is installed on the servers where the AMP is operational.

NOTE

The minimum supported version for the migration is AirWave 8.2.8.2.

To perform an offline migration, complete the following steps:

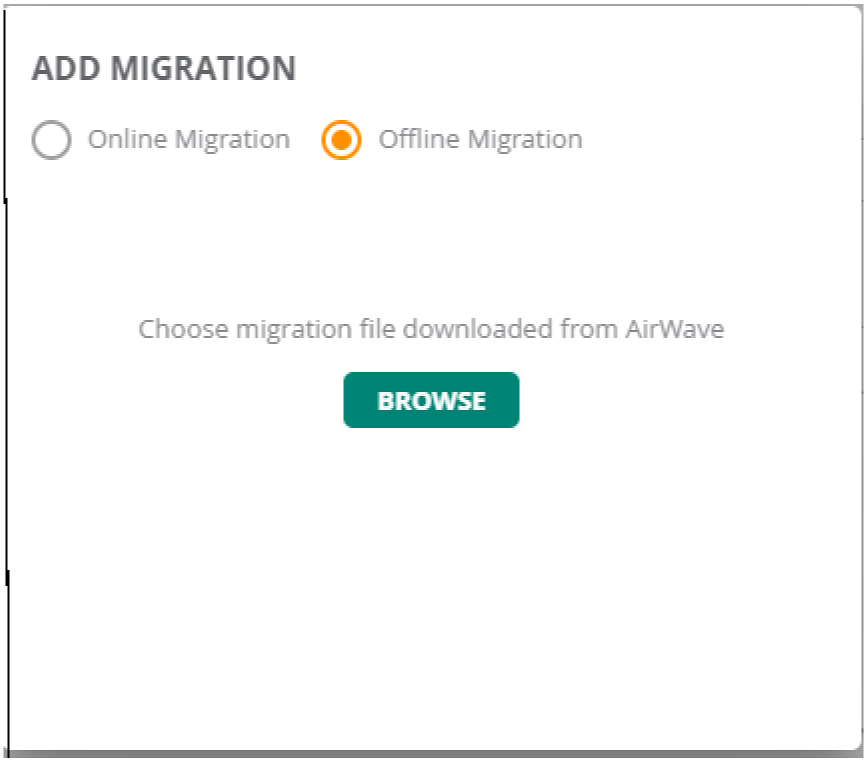
1. In the **Aruba Central On-Premises** app, set the filter to **Global**.
2. Under **Maintain**, click **System Management**.
3. Click the **Migration** tab.

   The **Migration** page is displayed.
4. Click + in the **Airwave Migration** table.

   The **Add Migration** window is displayed.
5. In the **Add Migration** window, select the **Offline Migration** option.
6. Browse to the location to choose the migration file that was downloaded from AirWave.
7. Click **Save** to start the migration process.

The following images displays the offline migration of the AirWave server.

Figure 22 *Offline Migration*



ADD MIGRATION

○ Online Migration ● Offline Migration

Choose migration file downloaded from AirWave

NOTE

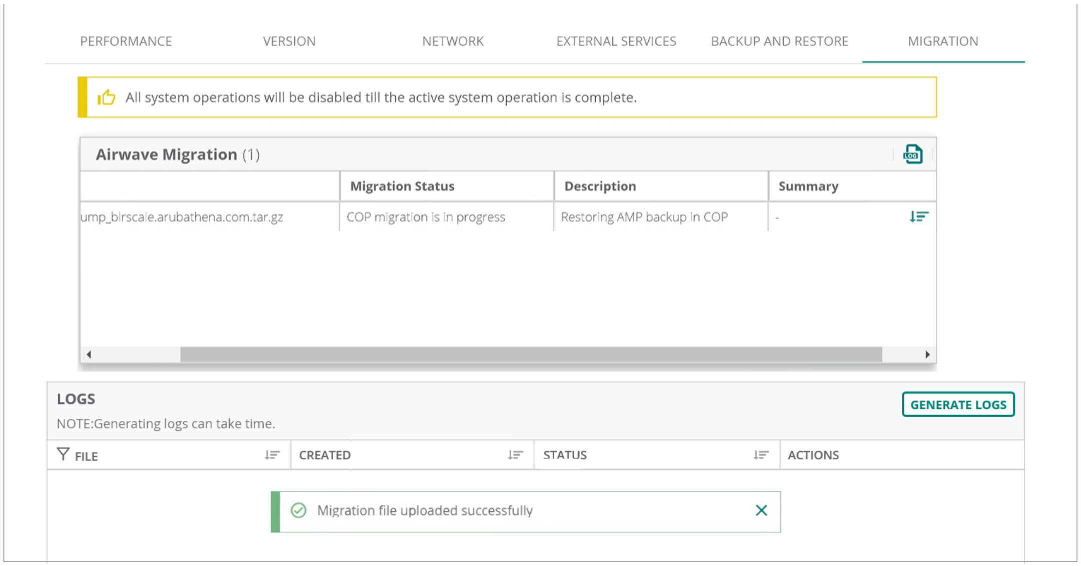
- In the **Airwave Migration** table, the 🗑 icon allows you to delete the migration.
- You must not refresh the page when the upload is in-progress.

Validating the Migration Process

After you click **Save** on the migration window, the migration process starts. If multiple AMPs are added, each AMP will be migrated sequentially.

The following image displays the offline migration main components of the **Migration** page.

Figure 23 *Screen Capture of Offline Migration*



All system operations will be disabled till the active system operation is complete.

Airwave Migration (1)

	Migration Status	Description	Summary
ump_birscale.arubathena.com.tar.gz	COP migration is in progress	Restoring AMP backup in COP	-

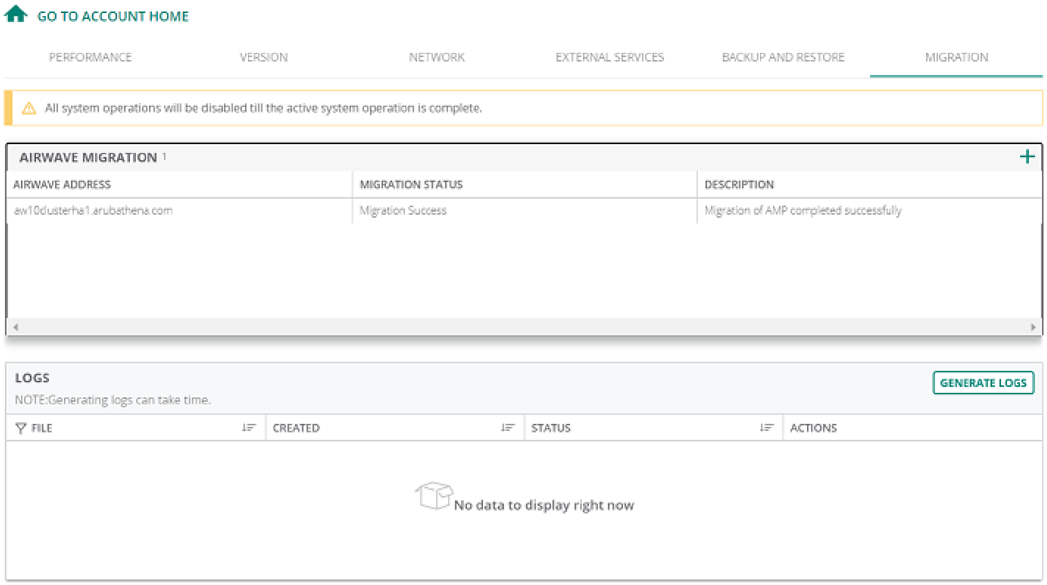
LOGS

NOTE:Generating logs can take time.

FILE	CREATED	STATUS	ACTIONS

Migration file uploaded successfully

Figure 24 *Screen Capture of a successful Migration*



All system operations will be disabled till the active system operation is complete.

AIRWAVE MIGRATION 1

AIRWAVE ADDRESS	MIGRATION STATUS	DESCRIPTION
aw10clusterha1.arubathena.com	Migration Success	Migration of AMP completed successfully

LOGS

NOTE:Generating logs can take time.

FILE	CREATED	STATUS	ACTIONS

No data to display right now

NOTE

- During the migration process, a fresh AMP back up is created in AirWave 8.x and transferred to Aruba Central On-Premises. The scheduled nightly backup is not performed as a part of the migration process.
- The default time out period for the backup process during the migration is **120 minutes**.

Logs

The **Logs** table displays all the logs related to the migrations that are either complete or failed.

You can generate the log files in one of the following ways:

- In the **System Management** > **Migration** > **Logs** table, click **Generate Logs** to create the log files.
- In the **System Management** > **Performance** > **Service Monitoring** table, select the deployment service and click the icon.

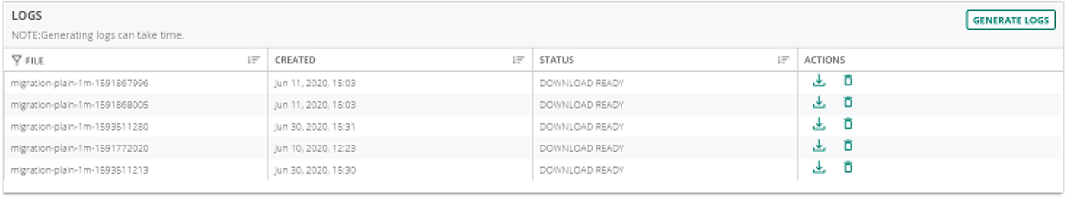
The log files that are generated contains the cumulative data of all the AMP migrations.

NOTE

- You can view the device migration POD logs from the Aruba Central On-Premises backend or from the Aruba Central On-Premises UI.
- The VisualRF migration POD logs are available in one of the Aruba Central On-Premises cluster node and can be viewed in the **/var/log/visualrf** path.

The following image displays the **Logs** table.

Figure 25 *Log Files*



LOGS

NOTE:Generating logs can take time.

FILE	CREATED	STATUS	ACTIONS
migration-plain-1m-1591867996	Jun 11, 2020, 15:03	DOWNLOAD READY	
migration-plain-1m-1591868005	Jun 11, 2020, 15:03	DOWNLOAD READY	
migration-plain-1m-1593511280	Jun 30, 2020, 15:31	DOWNLOAD READY	
migration-plain-1m-1591772020	Jun 10, 2020, 12:23	DOWNLOAD READY	
migration-plain-1m-1593511213	Jun 30, 2020, 15:30	DOWNLOAD READY	

The following table provides the **Logs** information.

Table 6: *Logs Table*

Name	Description
File	Name of the log file.
Created	The date and time when the log file is created.
Status	Indicates the status of the logs that are generated. The status indicated is **Download Ready**, **In Progress**, **Successful**, or **Failed.**
Action	Enables you to perform the following actions: - Click the icon to download the log files. The files are then saved to the local drive as a TAR file. - Click the icon to delete the log files.