HPE Aruba Networking Central On-Premises

3.0.3.3

Release Notes

Copyright Information

© Copyright 2026 Hewlett Packard Enterprise Development LP.

Open Source Code

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://my-enterpriselicense.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 3

About this Guide 1

Related Documents 1

Conventions 1

Contacting Support 3

3.0.3.3 What's New 4

Resolved Issues 5

System Management Resolved Issues 5

Network Management Resolved Issues 5

Known Issues 8

System Management Known Issues 8

Network Management Known Issues 9

API Change Log in 3.0.3.x Release 12

New MRT APIs 12

New Configuration APIs 13

Modified APIs 14

Deprecated APIs 21

Chapter 1

About this Guide

This release notes describes the new features supported by HPE Aruba Networking Central On-Premises for the release and lists the known and resolved issues.

Related Documents

- HPE Aruba Networking Central On-Premises Installation and Setup Guide
- HPE Aruba Networking Central On-Premises Non-Appliance Installation and Setup Guide
- HPE Aruba Networking Central On-Premises User Guide
- HPE GreenLake Account Home User Guide

Conventions

The following conventions are used throughout this guide to emphasize important concepts:

Table 1: Typographical Conventions

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
System items	This fixed-width font depicts the following: ■ Sample screen output ■ System prompts ■ Keys that are pressed
Bold	■ Text typed into a GUI element ■ GUI elements that are clicked or selected

The following informational icons are used throughout this guide:

Note:
Indicates helpful suggestions, pertinent information, and important things to remember.

Caution:
Indicates a risk of damage to your hardware or loss of data.

Warning:
Indicates a risk of personal injury or death.

Contacting Support

Table 1: Contact Information

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

Chapter 2

3.0.3.3 What's New

This release does not include any new features or enhancements.

Chapter 3

Resolved Issues

The following sections provide a comprehensive list of resolved issues for 3.0.3.3 release:

- Network Management Resolved Issues

System Management Resolved Issues

Network Management Resolved Issues

Table 1: Network Management Resolved Issues

Issue ID	Description
CNX-260948	After upgrading HPE Aruba Networking Central On-Premises to version 3.0.3.2, audit logs were not generated or displayed in the **Audit Trail** table. The fix ensures that audit logs are generated correctly and displayed as expected on the **Menu** > **Audit Trail** page.
CNX-259561 CNX-252775	On AOS-CX 6000 stack switches, when a port profile with **Port Authentication** enabled (referencing an AAA profile) was applied to switch stack interface, the configuration was pushed successfully. However, after updating the same port profile to disable **Port Authentication**, HPE Aruba Networking Central On-Premises reported a successful configuration push and the audit trail confirmed the update, but the port authentication configuration remained on the switch stack interface. Other configuration changes in the updated port profile were applied correctly. This issue occurred because the translator did not generate the required delete CLI commands for port authentication, and interface updates were not triggered when the port profile content changed. The fix ensures that configuration change to Port Authentication is correctly applied to the interface port profile.

Table 1: Network Management Resolved Issues

Issue ID	Description
CNX-257888	On switch stacks, after applying an interface port profile and successfully pushing the configuration, the access VLAN was updated incorrectly. The switch did not use the VLAN specified in the **Native VLAN** field of the port profile and instead applied an incorrect VLAN value. The fix ensures that the access VLAN is updated correctly based on the configured Native VLAN setting in the port profile.
CNX-256401	On CX 6300 switch stacks, when a port profile containing Power over Ethernet (PoE) settings was applied to interfaces on stack member switches using the REST API, HPE Aruba Networking Central On-Premises reported that the configuration push was successful and the stack remained synchronized. However, the port profile configuration was not applied correctly to interfaces on stack members, causing the ports to retain their default settings. In some cases, audit trail entries were generated against different device identifiers within the stack, resulting in inconsistent configuration application across stack members.
CNX-256512	When converting standalone AOS-CX switches into a VSF stack, the stack creation process could fail with an error indicating that the switch was already associated with a VSF profile, even though the switches had previously been onboarded as standalone devices. This issue occurred because stack name information was not preserved during certain VSF stack formation workflows, causing stack creation validation to fail incorrectly. The fix ensures that VSF stack formation workflows process configuration data correctly and that standalone switches can be converted to VSF stacks without encountering erroneous profile association errors.
CNX-257952 CNX-252775	On AOS-CX 8100 switch stacks, port profile configuration pushes could fail even though the configuration changes were recorded in the audit trail. The configuration was not applied to the target interface, and the audit trail reported that the configuration was eliminated because the setting was not supported on the device. The fix ensures that port profile configurations are processed correctly and applied successfully to the target interfaces.

Table 1: Network Management Resolved Issues

Issue ID	Description
CNX-260548 CNX-254841	The HPE Aruba Networking Central On-Premises cluster failed to load and displayed the error message, **We are not able to process your request**. The fix ensures that the cluster loads successfully and operates as expected.
CNX-241952	After upgrading HPE Aruba Networking Central On-Premises to version 3.0.3.2, deleting a preconfigured OSPF profile created at the device scope as a local profile failed and displayed a misleading error message. The fix ensures that OSPF profiles can now be deleted successfully.
CNX-252775 CNX-260756	After updating HPE Aruba Networking Central On-Premises to version 3.0.3.2, which included a renewed internal proxy certificate, and restarting the cluster, configuration updates were not synchronized to managed devices. As a result, configuration changes, such as VLAN description updates on AOS-CX 6000 switches or system name updates on access points, were not applied. The fix ensures that configuration changes are processed correctly and successfully synchronized to managed devices.

Known Issues

The following sections provide a comprehensive list of known issues for 3.0.3.3 release:

- System Management Known Issues
- Network Management Known Issues

System Management Known Issues

Table 1: System Management Known Issues

Issue ID	Description
CNX-211280	Cluster setup fails with an NTP error stating **Cluster Onboard Stage - This stage bootstraps data to consul and value, has failed**. The issue occurs when invalid NTP server details were entered initially, even after the details were corrected later. **Workaround:** Contact the HPE Aruba Networking support team.
CNX-235850	Kingston USB drive is not detected on the HPE DL360 Gen10 server.
CNX-237437	In an **Air Gap** setup, the Web UI Interface is the recommended method for downloading and upgrading the new release build. It provides a more reliable option compared to the copadmin CLI menu.
CNX-242947	After a firmware upgrade, the device configuration may go out of sync, causing a full configuration push. During this process, the device temporarily loses connectivity, which can cause the configuration push to fail and result in an automatic rollback. Once the device reconnects to HPE Aruba Networking Central On-Premises, the configuration is reimported. However, the Trust Anchor (TA) profile is not applied during this step beca=use reverse translation is not supported on Greenfield devices. **Workaround**: After the device reconnects to HPE Aruba Networking Central On-Premises, manually push the TA root certificate from HPE Aruba Networking Central On-Premises.
CNX-245860	Adding a node after auto download fails because of an image synchronization failure on the new nodes.

Table 1: System Management Known Issues

Issue ID	Description
	Workaround: Perform the **Add Node** operation before the auto download process or after the upgrade operation is complete.
CNX-245881	In FIPS mode, USB-based ISO installation is not supported.
CNX-251591	During the HPE Aruba Networking Central On-Premises 3.0.30 installation, the following error message is displayed **CNX on-prem CREATE CLUSTER Stage - This stage creates a Kubernetes cluster of given nodes, has failed**. This issue occurs when the Virtual NIC is not reachable. **Workaround:** Perform the following steps on all nodes: 1. Login to iLO server as an Administrator (for password contact the HPE Aruba Networking support team). 2. Navigate to **Information** > **Diagnostics** > **Reset iLO**. 3. Perform a factory reset on the node from which the setup cluster was initiated.
CNX-253090	On the **Alerts** page, when the **Defer**, **Clear**, or **Set Priority** operation is performed on an active alert, the **Status** in the **Alert Details** pop-up remains stuck in the **In Progress** state and does not complete successfully.
CNX-253899	When an upgrade is initiated on the disaster recovery (DR) cluster, the **Data-Sync** alert is not generated in the **System Alerts** page.

Network Management Known Issues

Table 2: Network Management Known Issues

Issue ID	Description
CNX-84012	In AP **System** profile, the **Static Channel** drop-down list for the Non-Preferred Scan Channels (PSC) **6 GHz** radio band fails to display dynamic options based on the selected county code.
CNX-191954	AIOps is generating false VLAN Mismatch alerts for LAG and VSX interfaces, even when VLANs are configured and allowed on both switches.”
CNX-199108	Creating OSPF profiles over NBAPI with a **no-advertise-range** leaf specified throws an exception: **HPE_GL_ERROR_INTERNAL_SERVER_ERROR**.

Table 2: Network Management Known Issues

Issue ID	Description
CNX-210318	The Firmware Status column displays **Live upgrade scheduled** incorrectly for an AP even after the upgrade is completed and in certain cases even after the firmware policy is deleted. This issue occurs in the **Devices** table under **Firmware Management** page. It happens because an outdated status is sent after the upgrade and it remains in the database.
CNX-228888	A Net Destination UI for IPv6 automatically deletes both colons (::) when trying to delete a single colon.
CNX-230196	When a VLAN is used as an access VLAN on an interface, the system prevents its deletion and displays an error: **Validation Failure: VLAN '<ID>' cannot be deleted because it is referenced by Interface Ethernet '<Interface>' in the hierarchy**. However, if the VLAN is configured as a trunk VLAN with native VLAN as 1, the deletion succeeds silently, and the interface is configured to trunk all, with no warning or error messages. After deletion, the UI continues to display the deleted VLAN under the VLAN column, resulting in stale information.
CNX-233454	The device enters a conflict state during Capability and Capacity (CNC) validation for DNS and NTP. This issue occurs because the UI fails to validate device capability limits, allowing configurations to be pushed beyond the supported limits.
CNX-233604	Rogue devices on the Floorplan manager WebWebUI overlap due to having the same location. If a rogue device's location cannot be ascertained by location services, the location is assumed to be the same as the associated AP.
CNX-235803	The number of sites displayed on the expanded **Sites** card does not match the count shown on the **Sites** tab under the **Configuration** menu.
CNX-245410	In the **Alerts** table, the displayed list of alerts may not match the actual alert count. Alerts generated successfully are intermittently missing from the Web UI, and are not consistently visible in either the **Active** or **Cleared** tabs.
CNX-245410	In the **Alerts** table, the displayed list of alerts may not match the actual alert count. Alerts generated successfully are intermittently missing from the Web UI, and are not consistently visible in either the **Active** or **Cleared** tabs.

Table 2: Network Management Known Issues

Issue ID	Description
AOS-277233	Re-onboarding access points to HPE Aruba Networking Cen-tral On-Premises using Zero Touch Provisioning (ZTP) fails for access points that were previously onboarded manually and upgraded to AOS 10.8.0.2. The issue occurs because during device detection in HPE Aruba Networking Central On-Premises, a timing issue in the state machine prevents the Device Registration Token (DRT) check status from being updated when the AP attempts Activate provisioning or DRT validation. As a result, the AP is unable to log in to HPE Aruba Networking Central On-Premises. Although two DNS servers are configured, logs indicate that the activate domain (device.arubanetworks.com) cannot be resolved. **Workaround**: Configure a DNS entry for device.arubanetworks.com and map it to a dummy IP address or the HPE Aruba Networking Central On-Premises VIP address. This allows the DRT validation process to complete successfully and enables the AP to connect to HPE Aruba Networking Central On-Premises.
CNX-254712	The creation of a VSF stack may fail because the VSF auto-stack configuration is not pushed to the switches. This issue affects HPE Aruba Networking Central On-Premises clusters that were initially deployed using releases prior to 3.0.2.0 and do not contain the required database schema updates.

API Change Log in 3.0.3.x Release

Note:
All alpha (**v1alpha1**, and **v1alpha2**) MRT APIs are marked as deprecated. You must use the corresponding **v1** APIs.

This topic lists the APIs updated in this release.

- New MRT APIs
- New Configuration APIs
- Modified APIs
- Deprecated APIs

New MRT APIs

Table 1: New MRT APIs

Method	Path	Description
Services > **Location**		
GET	/network-services/v1/asset-tags/{asset-tag-id}/image	This API is used to fetch the asset tag image that was uploaded for the specified Asset id
Services > **Location**		
GET	/network-services/v1/asset-tags/{asset-tag-id}/image	This API is used to fetch the asset tag image that was uploaded for the specified Asset id
PUT	/network-services/v1alpha1/asset-tags/{asset-tag-id}/image	This API is used to update the asset tag image for the specified Asset ID.
DELETE	/network-services/v1alpha1/asset-tags/{asset-tag-id}/image	This API is used to delete an asset tag image for the specified Asset ID.

Table 1: New MRT APIs

Method	Path	Description
Notifications > **Insights**		
GET	/network-notifications/v1/insights-schema	This API is used to fetch the JSON schema definition for one or all available insights and the count of Insights available. If **insight-id** is provided, the API returns only the schema for that specific insight. If **insight-id** is is not entered, then the API returns schemas for all available insights as a JSON string.

New Configuration APIs

Table 2: New Configuration APIs

Method	Path	Description
Application Experience > **DAP**		
GET	/network-config/v1/dap	This API is used to fetch the list of configured Dynamic Application Prioritization (DAP) global profiles. DAP is an application-aware QoS feature that dynamically optimizes traffic handling based on individual application requirements. Unlike traditional QoS methods that treat all traffic within a classification equally, Dynamic Application Prioritization adjusts network behavior per application. It automatically tunes advanced RF parameters, such as uplink scheduling, to meet the SLA (Service Level Agreement).
GET, POST, PATCH, or DELETE	/network-config/v1/dap/{name}	These APIs are used to fetch, create, or update the parameters related to a specific Application Prioritization (DAP) global profile.
Application Experience > **DAP SLA**		

Table 2: New Configuration APIs

Method	Path	Description
GET	/network-config/v1/dap-sla	This API is used to fetch the list of configured Dynamic Application Prioritization (DAP) SLA profiles. SLA profile allows you to configure some SLA parameters such as latency, and jitter, based on which some specific applications can be optimized. A total of 32 the SLA profile numbers can be configured.
GET, POST, PATCH, or DELETE	/network-config/v1/dap-sla/{name}	These APIs are used to fetch, create, or update the parameters related to a specific Dynamic Application Prioritization (DAP) SLA profile.
Application Experience > **DAP Application**		
GET	/network-config/v1/dap-application	This API is used to fetch the list of configured Dynamic Application Prioritization (DAP) application profile. One DAP SLA profile must be configured under the DAP application profile to indicate how to optimize this application.
GET, POST, PATCH, or DELETE	/network-config/v1/dap-application/{name}	These APIs are used to fetch, create, or update the parameters related to a specific DAP application profile.

Modified APIs

- MRT APIs
- Configuration APIs

MRT APIs

Table 3: Modified MRT APIs

Method	Description
Monitoring > **Access Points**	
GET /network-monitoring/v1/aps	This API is enhanced to include the following parameters in the response body: ■ uptime ■ wlan_count

Table 3: Modified MRT APIs

Method	Description
	■ subnet_mask ■ mesh_role
GET /network-monitoring/v1/aps/{serial-number}	This API is enhanced to include the following parameters in the response body: ■ radio_type ■ subnet_mask ■ mesh_role ■ current_uplink_inuse ■ client_count
GET /network-monitoring/v1/aps/{serial-number}/tunnels GET /network-monitoring/v1/aps/{serial-number}/tunnels/{tunnel-id	These APIs are enhanced to include the **crypto_type** parameter in the response body.
GET /network-monitoring/v1/top-aps-by-wireless-usage GET /network-monitoring/v1/top-aps-by-wired-usage GET /network-monitoring/v1/top-aps-by-usage GET /network-monitoring/v1/aps/{serial-number}/throughput-trends GET /network-monitoring/v1/aps/{serial-number}/cpu-utilization-trends GET /network-monitoring/v1/aps/{serial-number}/memory-utilization-trends GET /network-monitoring/v1/aps/{serial-number}/power-consumption-trends GET /network-monitoring/v1/radios/{radio-number}/throughput-trends	The trend and statistics APIs are updated with the following enhancements: ■ The **sitename** parameter is added to the filter. ■ Based on the start and end timestamp range specified in the request body, the **samplingIntervalInMinutes** value is automatically set as follows: • 5 minutes — when the timestamp range is up to 1 day • 180 minutes (3 hours) — when the timestamp range is more than 1 day

Table 3: Modified MRT APIs

Method	Description
GET /network-monitoring/v1/radios/{radio-number}/channel-utilization-trends	
GET /network-monitoring/v1/radios/{radio-number}/channel-quality-trends	
GET /network-monitoring/v1/aps/{serial-number}/radios/{radio-number}/noise-floor-trends	
GET /network-monitoring/v1/aps/{serial-number}/radios/{radio-number}/frames-trends	
GET /network-monitoring/v1/aps/{serial-number}/ports/{port-index}/throughput-trends	
GET /network-monitoring/v1/aps/{serial-number}/ports/{port-index}/frames-trends	
GET /network-monitoring/v1/aps/{serial-number}/ports/{port-index}/crc-trends	
GET /network-monitoring/v1/aps/{serial-number}/ports/{port-index}/collisions-trends	
GET /network-monitoring/v1/aps/{serial-number}/tunnels/{tunnel-id}/throughput-trends	
GET /network-monitoring/v1/aps/{serial-number}/tunnels/{tunnel-id}/packet-loss-trends	
GET /network-monitoring/v1/aps/{serial-number}/tunnels/{tunnel-id}/mos-trends	
GET /network-monitoring/v1/aps/{serial-number}/tunnels/{tunnel-id}/jitter-trends	
GET /network-monitoring/v1/aps/{serial-number}/tunnels/{tunnel-id}/latency-trend	

Table 3: Modified MRT APIs

Method	Description
GET /network-monitoring/v1/aps/{serial-number}/wlans/{wlan-name}/throughput-trends GET /network-monitoring/v1/wlans/{wlan-name}/throughput-trends	
Notifications > **Insights**	
GET /network-notifications/v1/insights	The following are the enhancements to the source recommendations API: ■ The **id** parameter is updated to **insight-id**. To get the **insight-id** execute the GET /network-notifications/v1/insights API without entering any insight-id or site-id. This will fetch the list of source recommendations at a global level. ■ Pagination functionality is added for the source recommendations API. Pagination parameters includes limit, offset and sort. ■ The **message** field in the response body is removed.
Monitoring > **Client Onboarding**	
GET /network-monitoring/v1/client-onboarding-score	These APIs are enhanced with the following update: ■ The **type** parameter is changed to **stage**. ■ The **ID** parameter is updated to **version**. ■ The view-type parameter is added that supports the following

Table 3: Modified MRT APIs

Method	Description
	• DEFAULT • BY_CLIENT • BY_ATTEMPTS
GET /network-monitoring/v1/client-onboarding-stage/export	These APIs are enhanced with the following update: ■ The **type** parameter is changed to **stage**. ■ The **ID** parameter is updated to **version**. ■ The **view-type** parameter is added.
GET /network-monitoring/v1/client-onboarding-stage/reasons	These APIs are enhanced with the following update: ■ The **type** parameter is changed to **stage**. ■ The **ID** parameter is updated to **version**. ■ The **view-type** parameter is added. ■ The count parameter is added. It displays the top grouped counts for onboarding by stage and status. The count displays, **topclients**, **topaccessdevices**, **band**, **topwlans**, **topreasons**, and **topservers**.
GET /network-monitoring/v1/client-onboarding-stage/count	These APIs are enhanced with the following update: ■ The **type** parameter is changed to **stage**. ■ The **ID** parameter is updated to **version**. ■ The **view-type** parameter is added.

Configuration APIs

Table 4: Modified Configuration APIs

Method	Description
Gateway Clustering Orchestration > **Gw Cluster Intent**	The APIs under **GW Cluster Intent** are updated to support the following parameters: ■ The **device-type** parameter is added to the request body. This parameter supports **BRANCH_GW**, **MOBILITY_GW**, and **VPNC**. If the **device-type** parameter is not specified MOBILITY_GW is set as a default value. ■ The **default-gateway-mode** parameter is added to the request body to Enable or disable one-to-one-redundancy mode for auto cluster profiles. When this parameter is enabled, only two gateways are allowed in the cluster profile: one gateway is assigned the leader role, while the other remains in standby mode. ■ The uplink-tracking parameter is used to enable or disable uplink tracking for auto cluster profiles. This is applicable only for **BRANCH_GW** device-type with default-gateway-mode enabled. ■ The uplink-sharing parameter is used to enable or disable uplink sharing for auto cluster profiles. This is applicable only for **BRANCH_GW** device-type with default-gateway-mode enabled.

Table 4: Modified Configuration APIs

Method	Description
	■ The coa-vrrp supports only **VLAN** for **BRANCH_GW** device-type. ■ The coa-enable parameter refers to Change of Authorization (CoA). If coa-vrrp is not defined and coa-enable is set to true, for BRANCH_ GW device-type the system automatically selects the coa-vrrp value from the controller IP VLAN if available. For other device-type you must configure the coa-vrrp parameters.
Miscellaneous > **Overlay Wlan**	The APIs under Overlay WLAN are updated to support configuration of site-specific clusters terminating on BGWs. The **gw-cluster-list** parameter now includes support for **SITE_CLUSTER_BGW**.
System > **System Info** The **hostname-alias** parameter is removed from the APIs listed under **System Info**.	
[POST} network-config/v1alpha1/system-info	Previously, the **hostname** parameter value could either be user-defined or you could assigned the **hostname-alias** value. The **host-name-alias** value was derived from the **ALIAS_HOSTNAME** parameter configured through the Alias API call. Now, the **host-name-alias** parameter has been removed, and users must explicitly define the **host-name** parameter value.
Named Object > **Alias** The **ALIAS_HOSTNAME** is removed from the APIs listed under **Alias**	

Deprecated APIs

Table 5: Deprecated APIs

Deprecated API	Alternate APIs
All alpha **MRT APIs** (**v1alpha1**, and **v1alpha2**) are marked as deprecated. You must use the corresponding **v1** APIs.	