HPE Aruba Networking Central On-Premises

3.0.3.0

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

3.0.3.0 What's New 4

Alerts 20

Insights 20

API Change Log in 3.0.3.0 Release 21

Resolved Issues 34

Known Issues 36

System Management Known Issues 36

Network Management Known Issues 38

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

3.0.3.0 What's New

This release includes the following new features and enhancements:

- Application Services
- Disaster Recovery
- Dynamic Application Prioritization
- Dual Stack Cluster Setup
- FIPS
- Switch Configuration
- Switch Alerts
- Enhancements to Aliases and Role-based Policies
- Enhancements to AP System Profile
- Enhancements to Application Visibility
- Enhancements to Backup and Restore
- Enhancements to Certificate Management
- Enhancements to Configuration Health
- Enhancements to Device Inventory
- Enhancements to Firewall Visibility
- Enhancements to Gateway Configuration
- Enhancements to Inventory and Subscriptions Card
- Enhancements to Network Overview—Cards Arrangement
- Enhancements to Subscription Keys
- Enhancements to Switch Configuration
- Enhancements to External Services
- Enhancements to Firmware Management

- Enhancements to Floorplan Manager
- Enhancements to Location Analytics
- Enhancements to Reports
- Enhancement to RF Profile
- Role-Based Access Control (RBAC)
- Enhancements to Troubleshooting Tools
- Enhancements to Unified Device List

Application Services

HPE Aruba Networking Central On-Premises supports Application Services, previously known as AirGroup. Application Services enables service discovery across modern enterprise wired and wireless networks. Using zero-configuration networking, it allows client devices to reliably discover and access network services, even in environments with multiple VLANs and wireless access constraints.

Dynamic Application Prioritization

A new Dynamic Application Prioritization (DAP) profile enhances performance for business-critical application or any applications performance by intelligently identifying applications, and dynamically prioritizing uplink and downlink traffic based on Service Level Agreement (SLA) metrics such as latency, jitter, and packet loss. It also enforces Quality of Service (QoS) policies through application tags, and delivers end-to-end visibility and detailed telemetry in HPE Aruba Networking Central On-Premises. It optimizes operational efficiency by correlating application performance with network behavior, ensuring superior end-user experience.

Disaster Recovery

A new Disaster Recovery capability is available for HPE Aruba Networking Central On-Premises, providing high availability through paired primary and secondary clusters across two data centers. The system supports automatic and manual failover to maintain service continuity during site or system outages, with devices reconnecting automatically to the active cluster. Administrators can monitor redundancy health, data synchronization status, and failover readiness through a dedicated Disaster Recovery interface, helping reduce downtime and ensure operational resilience.

Dual Stack Cluster Setup

HPE Aruba Networking Central On-Premises now supports dual-stack cluster setup, enabling both IPv4 and IPv6 communication within the cluster environment. . During installation, you can optionally enable dual-stack mode and configure IPv6 addressing for cluster nodes and services. For more information, see the Setting up the Permanent Network.

FIPS

A new appliance mode installation called Federal Information Processing Standards (FIPS) has been introduced for HPE Aruba Networking Central On-Premises. This specialized variant operates on FIPS-validated platform, ensuring compliance with the strict security requirements mandated by certification standards. However, when operating in this mode, disaster recovery (DR) and IPv6 features are not supported.

For more information, see FIPS—HPE Aruba Networking Central On-Premises.

Switch Configuration

The following new profiles are added for AOS-CX switch configuration:

- **HPE ANW Central**—The **HPE ANW Central** profile enables devices to securely connect to an HPE Aruba Networking Central On-Premises instance for centralized monitoring and configuration. These settings define how devices establish and maintain communication with Central, including primary and secondary server endpoints and the network context used for connectivity.
- **VSF Stack Builder**—The VSF Stack Builder profile allows administrators to streamline and standardize the configuration of multiple switch stacks by leveraging a common, reusable template. This template can be applied across both global and site scopes, reducing the manual effort required to create individual stack profiles when stacks share similar properties such as platform type, links, and SKUs.
- **Mulicast Global**—The **Multicast Global** profile enables centralized configuration of multicast behavior across fabrics through the UI.
- **Multicast Source Discovery Protocol (MSDP)**—Multicast Source Discovery Protocol (MSDP) is a mechanism that connects multiple Protocol Independent Multicast sparse mode (Multicast Source Discovery Protocol (MSDP)-SM) domains.

- **MDNS** —Multicast DNS (mDNS) helps users discover servers, such as printers and Apple TV, across VLANs. It uses a reflection mechanism to enable service discovery between VLANs.
- **Port Mirroring Profile**—The Port Mirroring profile enables a network administrator to replicate all traffic arriving at (ingress) and/or leaving (egress) selected system interfaces. The mirrored traffic is forwarded to a designated destination where it can be captured and analyzed for monitoring, security inspection, or troubleshooting purposes.
- **NAE Agent** and **NAE Script**—The Network Analytics Engine (NAE) provides a troubleshooting solution that helps monitor data from the switch database and automatically execute operations when certain conditions are met. NAE uses Python-based scripts to define monitored data, conditions, and automated actions. Validated scripts can be turned into NAE agents, with parameters set at creation.

Switch Alerts

Health support is added for the following alert:

- Radius Server Status

Enhancements to Aliases and Role-based Policies

- HPE Aruba Networking Central On-Premises now extends IPv6 support for **Network Destination** alias.
- HPE Aruba Networking Central On-Premises now supports configuration of rules for IPv6 address-family.
- HPE Aruba Networking Central On-Premises now extends support to the following aliases for Aruba gateways:
  - **IPv4 System VLAN**
  - **Auth Server Address**
  - **Auth Server Shared Secret**
  - **Gateway Switchport**

Enhancements to AP System Profile

The following enhancements are added to AP System Profile:

- The **Recovery SSID backoff timer** parameter is now available to set recovery SSID backoff timer duration.
- The **Preference of SAN over CN for Certificates** parameter is now available to use SAN as the primary validation field during certificate validation.

Enhancements to Application Visibility

- Applications from all sites are aggregated into one global list, wherever application visibility data exists. For more information, see Application Visibility Planet in Global List.
- GraphQL APIs and UI side-panel list now show switches in Switch Monitoring with a single Name column. That column displays the Hostname, a health icon to its left, and the switch status, either online or offline, with a health reason if available.
- In the **Application Visibility** site context, when a user selects a UCC-enabled application such as Microsoft Teams, the sidebar now displays key Unified Communications metrics for that application in the Call Session Summary Card. These include:
  - Total users
  - Total calls
  - Call Quality

  This feature gives users a quick, time-based overview of call activity directly within the Application Context view. To review more information about the Call Session Summary Card, see Viewing UCC Information in the Application Dashboard.
- Also, SaaS WAN information is now available from the Application Dashboard. SaaS WAN information helps administrators quickly determine whether degraded application experience is driven by WAN conditions rather than the application itself. For more details, see Viewing SaaS WAN Information in the Application Dashboard.
- **Application Visibility** now includes Quality of Experience (QoE) insights for websites, providing experience scores, QoE metrics, health trends, and experience counts. For more information, see Viewing Application Dashboard.

- Users can also access latency information from both the side panel on the application dashboard and the latency charts in the **Application Visibility** troubleshooting page. See Application Visibility Troubleshooting for further information. This ensures latency is visible anywhere users expect it when troubleshooting applications.

Enhancements to Backup and Restore

The **Hostname or IP address** parameter supports the IPv6 configuration for dual stack deployment of external services.

Enhancements to Certificate Management

Certificate Management now enforces strict cryptographic compliance for FIPS deployments. You must generate PEM or DER certificates and private keys using OpenSSL version 3.x to align with modern cryptographic standards and support FIPS approved algorithms. The system also disables PKCS12 certificate uploads to enforce security and compliance requirements.

Enhancements to Configuration Health

The status **Synced with Limitations** is renamed to **Synchronized**. The error categories **Validation Blocker** and **Validation Non Blocker** are renamed to **Invalid Configuration** and **Filtered Configuration**, respectively.

Enhancements to Device Inventory

- IPv4 and IPv6 addresses are listed in the device inventory if available. For more information, see Viewing the Device Inventory Table.
- EdgeConnect devices are listed in the device inventory. Filter for them using the **Gateway** filter. For more information, see Filtering Devices in the Device Inventory Table.
- The following filters are now available in the device inventory:
  - **Device Function Assignment** is a quick filter. Possible filter values are *Assigned* or *Unassigned*.
  - **Site** is a traditional filter that can be used to filter devices by site.

  For more information, see Filtering Devices in the Device Inventory Table.

Enhancements to Device Inventory

- IPv4 and IPv6 addresses are listed in the device inventory if available. For more information, see Viewing the Device Inventory Table.
- EdgeConnect devices are listed in the device inventory. Filter for them using the **Gateway** filter. For more information, see Filtering Devices in the Device Inventory Table.
- The following filters are now available in the device inventory:
  - **Device Function Assignment** is a quick filter. Possible filter values are *Assigned* or *Unassigned*.
  - **Site** is a traditional filter that can be used to filter devices by site.

  For more information, see Filtering Devices in the Device Inventory Table.

Enhancements to Firewall Visibility

- You can now view the top sessions activity for the blocked sessions in the **Summary** view of the **Sessions** dashboard.
- On-demand sessions support for AP.
- Support for **Security** dashboard in **Global** view.
- On-demand sessions support for client.
- The **Security** dashboard in **Global** view now provides an expanded view of **Top Sites By Blocked Sessions** and **Top Applications By Blocked Sessions** cards.
- HPE Aruba Networking Central On-Premises now supports **Security** dashboard in a client context. The **Security** dashboard in the **List** view provides a tabular representation of all the blocked session reported by clients. The **Security** dashboard in the **Summary** view provides graphical representation of all the blocked session reported by clients.
- HPE Aruba Networking Central On-Premises now supports **Security** dashboard in a device context. The **Security** dashboard in the **List** view provides a tabular representation of all the blocked session reported by devices. The **Security**

dashboard in the **Summary** view provides graphical representation of all the blocked session reported by devices.

Enhancements to Gateway Configuration

The following enhancements are added to gateway configuration:

- The **Certificate Usage** profile is now added for gateway configuration.
- The **Interface Profile** is now added for gateway configuration.
- **Scope Mapping Roles at Device Group**—In HPE Aruba Networking Central On-Premises, roles could only be mapped at **Global**, **Site Collections**, **Sites**, and **Devices** level. When you configured a WLAN, associated user roles were required to be mapped at the **Global** level only, even if the WLAN was scope mapped at a **Device Groups** level. This update now allows roles to be scoped at the **Device Groups** level that enhances scalability and optimizes resource efficiency. It is important to note that roles mapped to **Device Groups** derive policies from the **Global** level only. For more information, see WLAN Profile.
- **Gateway System Profile**—The following are the updates to the profile:
  - The **Deny Inter User Bridging** parameter is now added under the **Firewall Options**.
  - The **GPS** parameter is now removed from the profile.
  - The **FIPS Compliance** parameter is now added under **Security** section.
- **VLAN** Profile—The following parameters are now added under the **Gateway Layer 3 Parameters** section:
  - **Broadcast Multicast Optimizations**
  - **Suppress ARP**
  - **Local Proxy ARP**
  - **Client Mode***

Enhancements to Inventory and Subscriptions Card

The **Inventory and Subscriptions** card displays an overview of device distribution and subscription usage in your network. This feature helps you effectively monitor and manage your subscription usage.

Enhancements to External Services

The **Syslog** feature is now available to send messages to the syslog server in the Common Event Format (CEF) format.

The **SMTP** feature supports the IPv6 configuration for dual stack deployment of external services.

Enhancements to Network Overview—Cards Arrangement

The dashboard has a revised layout to support a bigger **Alerts** card. To achieve a unified grid structure, the layout was adjusted to allow mixed-dimension cards to integrate seamlessly. This rearrangement improves the spatial balance between cards, reduces visual crowding where the Alerts card resides, and enhances the overall readability of critical information.

Enhancements to Subscription Keys

Following are the enhancements to the **Subscription Keys** page:

- The **Subscriptions Keys** table now displays information regarding HPE order, purchase order, and reseller purchase order associated with the subscription keys.
- On the **Subscription Keys** page, when you click on the subscribed devices count, it redirects you to the **Device Inventory** page with the subscribed devices filtered out.

Enhancements to Switch Configuration

The following enhancements are made to the Switch Configuration:

- **Enhancements to Switch Interface Configuration and VLAN Profiles**

  When configuring **Switch Interface Configuration** and **VLAN** profiles, you can now enable MLD and configure advanced MLD parameters for ports, LAGs, and VLANs.

- **Enhancements to Port Profile**

  The following features can now be configured using Port Profiles on AOS-CX switches:

  - IP Source Lockdown
  - Flow Telemetry for Central

- **VSF Profile Support**

  The VSF profile is now supported on the AOS-CX 4100i and 6100 Switch Series. This support allows administrators to configure the Virtual Switching Framework (VSF) profile on these platforms starting with AOS-CX firmware version 10.16.1000 or later.

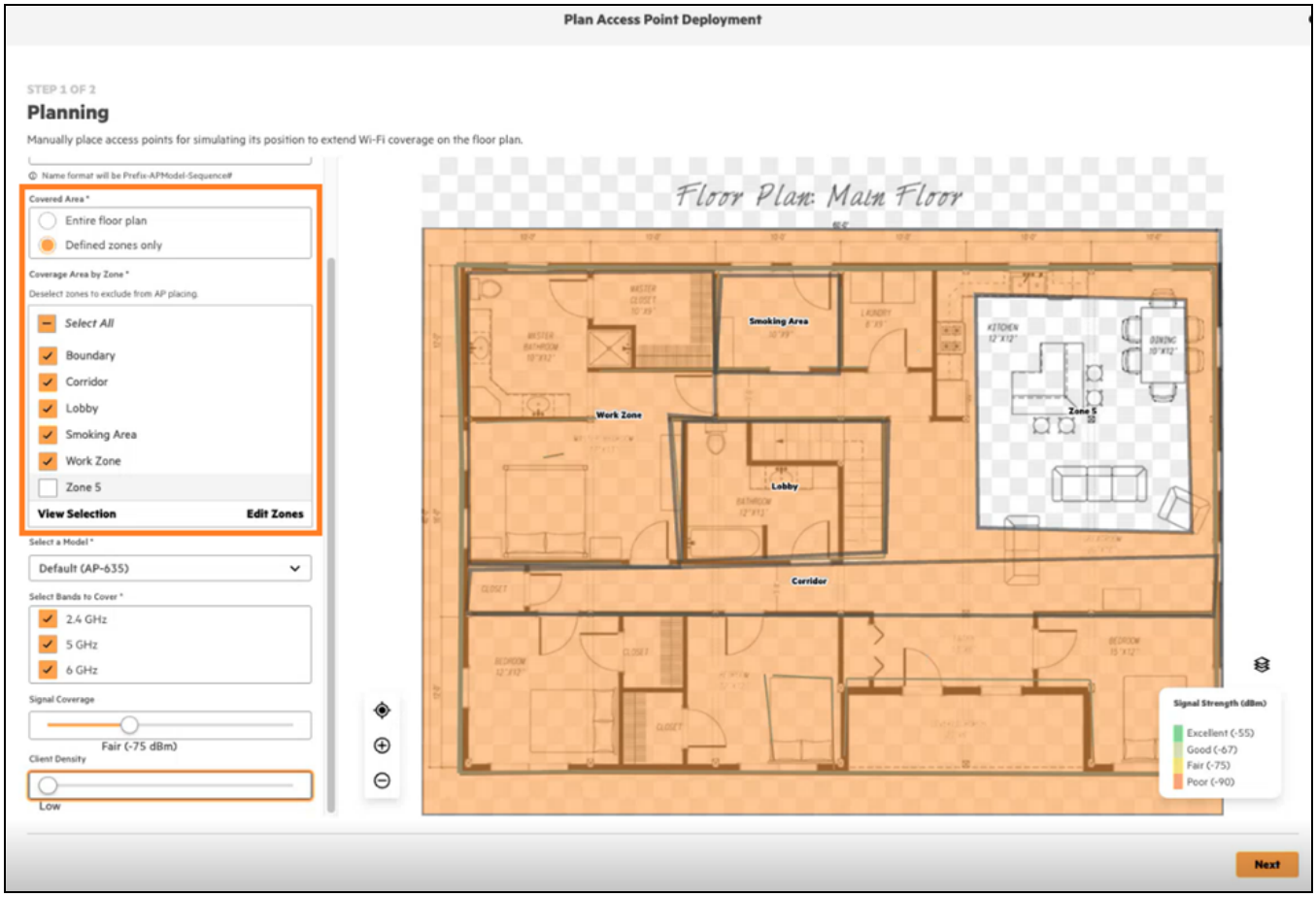
Enhancements to Firmware Management

The following enhancements are added to **Firmware Management**:

- The **Custom Build** field now enables you to provide the custom firmware version while creating and editing the firmware policies.
- The **Pause** and **Resume** feature now allows users to pause or resume the firmware policy.
- The following firmware statuses are now available:
  - Upgrade Scheduled
  - Upgrade Initiated
  - Upgrade Aborted
  - Upgrade Canceled
  - New Firmware Recommended
- The **Upgrade Successful** or **Upgrade Failed** status will automatically transition to either **New Firmware Recommended** or **–**.
- The **Download & Install Firmware Immediately** parameter is renamed to **Pre-download Firmware Image**. The **Pre-download Firmware Image** enables you to download the firmware image in advance before the scheduled upgrade time.
- The **Upgrade Non-Failsafe Modules** parameter is now available to perform upgrades to non-failsafe components on the AOS-CX switch during firmware upgrade.

Enhancements to Floorplan Manager

You can now deploy access points to specific zones within your floorplan. A new **Covered Area** option lets you select predefined zones for automatic AP placement, giving you greater control and flexibility. You can now deploy APs across the full floor-plan boundary or target only the zones you choose.



A new **Mini Map** view is added in the **Topology Link Node View**, to enable efficient and easy navigation of the actual topology. It is essentially a simplified visual representation of the entire network structure, displayed as a small inset or overview diagram. It helps users quickly understand the layout and connectivity of devices without displaying every detail.

Additionally, a new **Actions** drop-down list is available which you can use to expand and collapse the topology nodes at once.

For more information, see Topology Link Node View and Link Node Navigation.

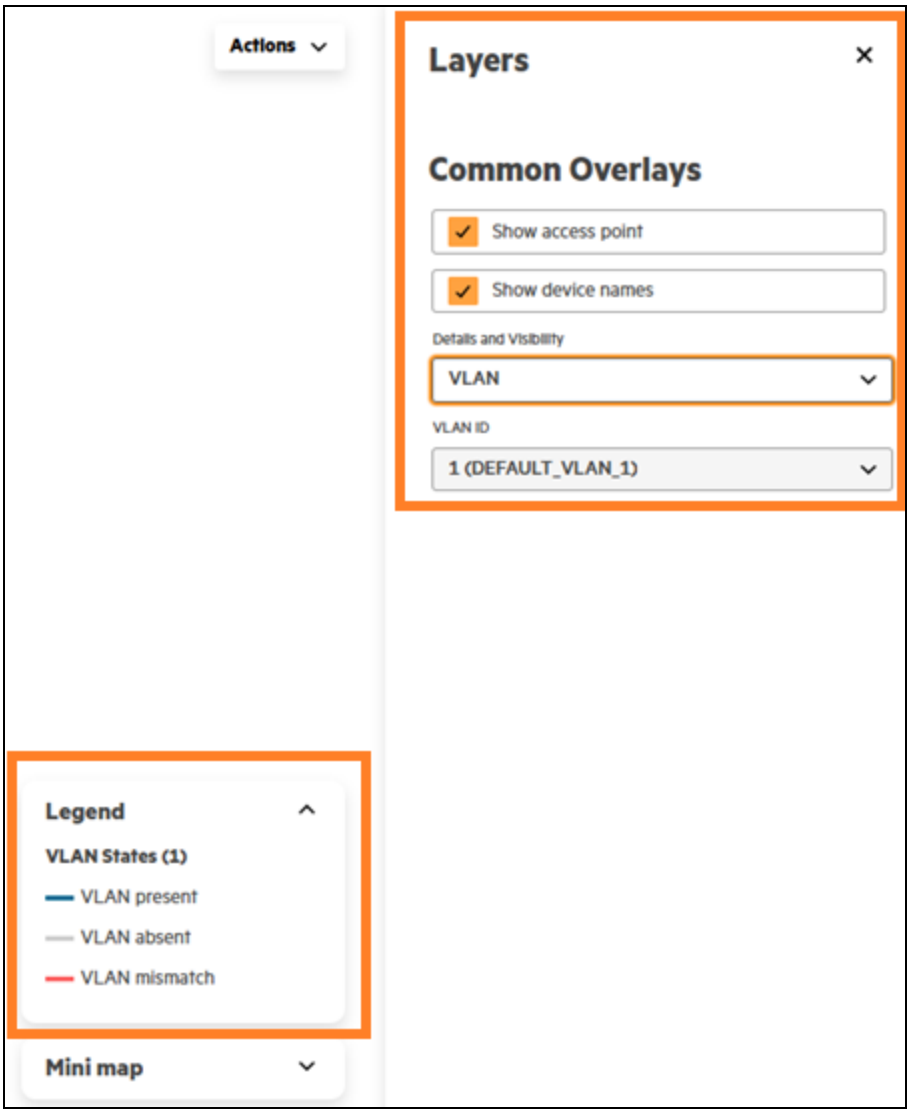
The **Layers** panel is now reorganized for improved clarity. It is grouped into **Common Overlays** and **Details and Visibility**. Within the **Details and Visibility** menu, you can now easily select filtering options to view only the data you need in the link node topology.

The VLAN filter now highlights detailed VLAN states directly in the topology view, including:

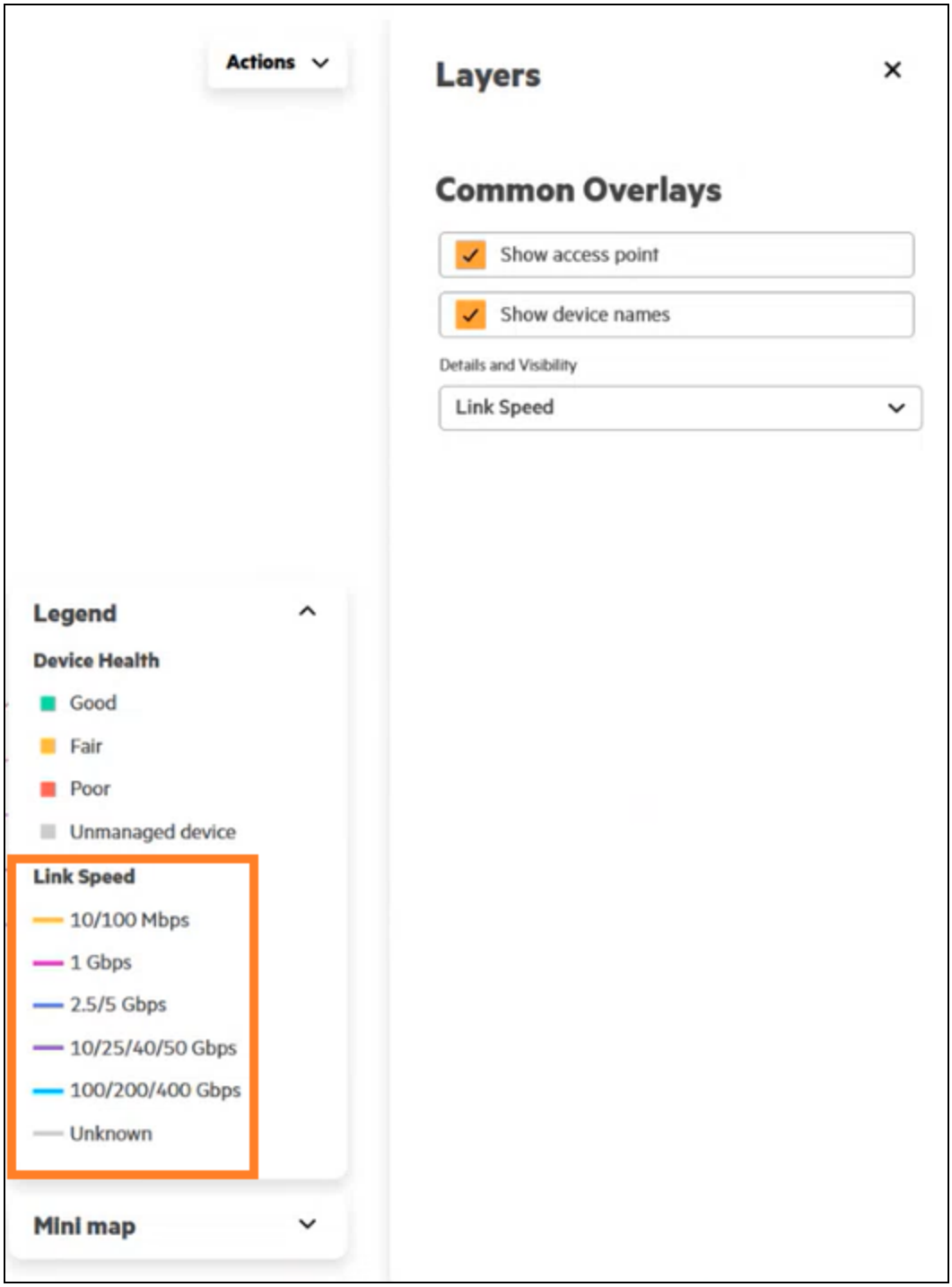
The **Layers** is now categorized clearly under **Common Overlays** and **Details and Visibility**. In the **Details and Visibility** drop-down list, you can now select the different options to filter and required data in the link node topology view. The VLAN filter now displays detailed VLAN states in the topology view:

- **VLAN present**
- **VLAN absent**
- **VLAN mismatch**

This enhancement gives users a clearer understanding of VLAN status across nodes and connections.



Additionally, link node speeds in the **Layers** panel are now grouped into categories for better readability, with each speed range displayed using distinct color codes within the topology.



For more information, see Link Node Navigation.

You can now view client roaming events directly in the Floorplan Manager, along with other client details. Roaming events show a client's network transitions between access points, indicating changes in connectivity—not physical movement. For more information, see Client Details.

Previously, planned APs were treated as dummy APs, and a replace action occurred only when the planned AP's name, MAC address, or serial number matched a real AP.

HPE Aruba Networking Central On-Premises now enables you to edit the properties of a planned AP directly, allowing you to convert it into a real AP. After updating the AP details, you can choose **Match and Replace Access Points** from the **Action** menu in the floorplan manager to complete the conversion.

> **Note:**
> The editable properties of the planned AP is visible based on the type of the AP configuration.

For more information, see Convert Planned APs to Real APs on the Floorplan.

HPE Aruba Networking Central On-Premises now provides intelligent recommendations to enhance Auto AP placement when errors occur. If you are unable to complete Automatic Placement during the Place Devices workflow, the system will proactively display actionable recommendations to help improve the success of Auto AP placement. For more information, see Automatic AP Placement.

In the Link Node topology view, the Alerts and Clients counts are now clickable. Selecting an alert or client number takes you directly to the site-specific **Alerts** or **Clients** page for detailed insights.

For more information, see Topology Link Node View and Link Node Navigation.

You can now use the following options on the floorplan manager:

- **Signal Bleed-Through**—You can now view the signal from APs on floors above or below a selected floor on the Heatmap. For more information, see Heatmap.
- **Rogue Objects** —You can now view rogue devices on the floorplan using the **Show Overlay Objects** Pane. For more information, see Floorplan Details.

Enhancements to Location Analytics

Only users with admin rights- (read and write permission) can see the **Enable** button for accessing the location analytics data. Once the location analytics feature is enabled, any user with read permission can also view the analytics data. For more information, see Viewing Location Analytics Data.

From the **Location Analytics** page, when you navigate to a specific site context by either clicking the site name under the **Sites** card, or by clicking the site location icon, you can now view the building information. You can view details such as the building name and the number of floors associated with that site. This view is

dynamic, and the details are generated using data from the floorplan manager. To access building details, you must first assign the AP to a floor, and then place it on the floorplan. For more information on assigning devices and placing devices on the floor, see Assigning Devices to Floorplans in Floorplan Manager and Planning Access Point Deployment.

> **Note:**
> Building information will not be displayed if the floorplan management feature is not enabled.

For more information, see Viewing Location Analytics Data.

Enhancements to Reports

The following KPIs are now available:

New KPIs

Report	KPI	Chart Type
WIDS	ROGUE AP Summary	Table Chart
Security Compliance	ROGUE APs List, WIDS List	Table Chart
Capacity Planning	Top Switches by Unused Ports	Table Chart
Subscription Renewal Schedule	Subscription Renewal Schedule	Bar Chart
Licenses	Subscription Keys	Table Chart
Network Usage	Maximum Wireless Clients Trend, Average Wireless Clients Trend	Trend Chart

The following enhancements are made to Reports:

- The field **Deployment Mode** is available in the **Inventory Report**.
- The CSV file export of reports includes the reporting time period.

Enhancement to RF Profile

RF Profile now enables users to specify the IoT antenna gain values while creating a new profile.

Role-Based Access Control (RBAC)

HPE GreenLake Account Home now supports custom scope groups, giving you more granular control over user role permissions in HPE Aruba Networking Central On-Premises. When assigning a role, you can limit a user's access to a specific set of Sites, Site Collections, or Device Groups. This enhancement allows you to define exactly which scopes a user can interact with, ensuring applications enforce permissions based on the scope group you configure.

For more information, see Role-Based Access Control (RBAC) .

Enhancements to Troubleshooting Tools

The following enhancements are added to Troubleshooting tools:

- You can now initiate troubleshooting tests on Wired Interfaces from the **Wired Interfaces** card of a switch.
- Enable debug logs-to-cloud on a device from the troubleshooting icon on the device page.
- All troubleshooting tests now include a **Repeat** field that can be used to schedule tests periodically within a specified time frame.
- You can now select multiple devices having the same device type and reboot or locate them in a single, bulk operation.
- You can now monitor spectrum statistics from access points to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, identify interference and classify its sources. For more information, see Spectrum Monitoring.
- Live Connectivity Performance provides visibility into AP radio performance in access mode, updating key metrics such as noise floor, channel quality, and frame data every 5 seconds for up to 15 minutes on supported firmware. For more information, see Live Connectivity Performance.

Enhancements to Unified Device List

You can now view neighbor information for Access Points in the **Connected To** field of the Unified Device List.

Alerts

The following features and enhancements are added to the Alerts module:

- The HPE Aruba Networking Central On-Premises now supports the following alerts:
  - **802.1X Authentication Rejected - AOS-S Switch**—Generates an alert when 802.1X authentication server rejects the User's credentials.
  - **MAC Authentication Rejected - AOS-S Switch**—Generates an alert when MAC authentication server rejects the User's credentials.
  - **WPA Passphrase is Incorrect**—Generates an alert when the 4-Way handshake fails for WPA-PSK clients.
  - **MAC Authentication Server Timeout - AOS-CX Switch**—Generates an alert when no response from the MAC authentication server is detected during the authentication process.
  - **802.1X Authentication Timeout - AOS-CX Switch**—Generates an alert when no response is received from the 802.1X authentication server during the authentication process.
  - **Maximum Associations**—Generates an alert when the maximum number of Wi-Fi associations configured for the AP is met.
  - **Roaming Latency**—Generates an alert when wireless clients experience unusually long roaming periods.
  - **MAC Authentication Server Timeout**—Generates an alert when no response is received from the MAC authentication server during the authentication process.

Insights

The following feature is added to the Insights module:

- **AP Health Insights - Country Code Mismatch**—Generates insights when the AP is configured with incorrect country code. An AP is considered to be in a misconfigured state if the country code derived from Google Latitude or Longitude data does not match the country code specified by the user.
- **Optimize WLAN DFS Configuration to Improve Performance** Insight—This insight uses global HPE Aruba Networking Central On-Premises data on channel occupancy and channel change reasons, as well as AP latitude and longitude data, to train AI models that educate users about the right set of channels to configure for optimum network performance on a per-site basis.
- **Optimize Bandwidth on 5 GHz Radio to Improve WLAN Performance** Insight—The insight analyzes each customer deployment and client behavior to recommend the optimal bandwidth for optimal TX rate gains, adequate SNR coverage, and reduced channel utilization.
- **Enabling 6 GHz Radio with Optimal Bandwidth to Improve WLAN Performance** Insight—The WLAN performance insight uses the transmission rates for various network and client configurations to predict the data transmission rate when 6GHz (Wi-Fi 6E) is enabled on the network.
- **Improve Access Point Coverage Resiliency** Insight—Access Point (AP) Coverage Resiliency is a feature designed to ensure uninterrupted wireless connectivity within enterprise networks, even during planned or unplanned AP downtimes.
- **Roaming Recommender** Insight—The insight provides a thorough review of client roaming behavior and the potential impact of activating Fast Transition (FT). Users can now optimize network performance by examining roaming information, client distribution (FT-capable and non-capable), and expected latency improvements.

API Change Log in 3.0.3.0 Release

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.
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**		

Table 2: New Configuration APIs

Method	Path	Description
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**		
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 ■ 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	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

Table 3: Modified MRT APIs

Method	Description
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 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	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/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	
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,

Table 3: Modified MRT APIs

Method	Description
	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 • 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.

Table 3: Modified MRT APIs

Method	Description
	■ 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_**

Table 4: Modified Configuration APIs

Method	Description
	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

Table 4: Modified Configuration APIs

Method	Description
	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-

Table 4: Modified Configuration APIs

Method	Description
	gateway-mode enabled. ■ 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

Table 4: Modified Configuration APIs

Method	Description
	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**.	

Table 4: Modified Configuration APIs

Method	Description
[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 **hostname-alias** value was derived from the **ALIAS_HOSTNAME** parameter configured through the Alias API call. Now, the **hostname-alias** parameter has been removed, and users must explicitly define the **hostname** 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
Most **v1**, **v1alpha2**, and **v1beta1** APIs are marked as deprecated. You must use the corresponding **v1** APIs available under the same category.	

Resolved Issues

The following sections provide a comprehensive list of resolved issues for 3.0.3.0 release:

- Network Management Resolved Issues

Table 1: Network Management Resolved Issues

Issue ID	Description
CNX-52321	In the HPE Aruba Networking Central On-Premises **Alerts** page, **Switch Disconnected** alerts were not automatically cleared. This issue occured when a switch was converted from stack to standalone or from standalone to stack. The fix ensures that **Switch Disconnected** alerts are automatically cleared.
CNX-178495	While editing a route map policy, the system displayed an error: **failed to parse data tree: Node 'seq-no-op-type' not found as a child of 'route-map' node**. This issue occurred when the object name matched the module name, which prevented the profile from being updated and blocked configuration from being pushed to the device. The fix ensures that route map policies are parsed correctly even when the object name matches the module name.
CNX-195861	In the **Device Groups** page, the search functionality was not working when a user tried to create or update a device group or add devices to an existing device group within a specific device group context. The fix ensures that the search functionality works as expected.
CNX-206605	The AP configured only to the first port from a NetService when multiple ports are defined. This issue occurred on **Named Objects** > **Services** section when the services configured with multiple comma-separated ports and then mapped to role-based policies. This is expected behavior, as AP configuration does not support comma-separated service ports and the parser enforces only the first port in the list.

Table 1: Network Management Resolved Issues

Issue ID	Description
CNX-208324	On expanding the **Insights** card, in the **Switch Firmware Recommendation Available** > **Popularity of Recommended Firmware** section displayed an error message **Failed to retrieve content**. The fix ensures that **Popularity of Recommended Firmware** section works as expected.
CNX-230321	In HPE Aruba Networking Central On-Premises, resynchronization failed when a device was powered on after being associated with a site and assigned a persona. The fix ensures that synchronization is successful regardless of whether the device is powered on before or after assigning a site or persona.
CNX-238439	After establishing an SSH connection and navigating to **System Configuration** using option 4, **Datacenter Redundancy** was displayed as option 8 in the CLI, but it was not supported. The fix ensures that the CLI no longer displays **Datacenter Redundancy**, and option 8 is now displayed as **Disaster Recovery**.

Known Issues

System Management Known Issues

The following sections provide a comprehensive list of known issues for 3.0.3.0 release:

- System Management Known Issues
- Network 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-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-246290	During an upgrade operation, a **System Disk I/O High Utilization** alert is displayed in the **System Management** > **Manage** > **System Alerts** table.
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 because 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.

Table 1: System Management Known Issues

Issue ID	Description
GLCP-352477	In HPE Aruba Networking Central On-Premises the radius authentication fails in a dual-stack cluster setup when using an IPv6 address. **Workaround**: As a workaround use the RADIUS server IPv4 address for authentication.
CNX-245881	In FIPS mode, USB-based ISO installation is not supported.
CNX-235850	Kingston USB drive is not detected on the HPE DL360 Gen10 server.
CNX-245860	Adding a node after auto download fails because of an image synchronization failure on the new nodes. **Workaround**: Perform the **Add Node** operation before the auto download process or after the upgrade operation is complete.
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-251032	The Air Gap option is disabled in the backend even though it appears as enabled in the Web UI under **Menu** > **System Management** > **Configuration** > **Network** tab. This issue occurs when the Air Gap option is enabled before initiating a system upgrade. After the system upgrade completes successfully, the Air Gap feature gets disabled in the backend. **Workaround**: After the upgrade, and before enabling the Disaster Recovery (DR) feature, disable and then re-enable Air Gap option on both setups designated for the DR cluster. After Air Gap mode is re-enabled on both setups, proceed to enable the DR feature.

Table 1: System Management Known Issues

Issue ID	Description
CNX-244528	During disaster recovery (DR), the device function assignment was lost for a pre-configured VSF stack after a failover from DC1 to DC2. The VSF stack was onboarded to DC1 and was in a synchronized state. Following the fail-over, the VSF stack remained synchronized; however, the device function assignment was removed.

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**.
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.

Table 2: Network Management Known Issues

Issue ID	Description
CNX-232542	In the **Insights** > **Device Firmware Recommendation** > **Switch Firmware Recommendation** page, it recommends end of support firmware version for AOS-CX 10.13.Xxxx series.
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-242947	Location override and HTTPS certificate configurations were removed from the HPE Aruba Networking Central On-Premises CLI after performing a firmware upgrade via HTTPS. This issue occurs because the full configurations push failed to preserve the **hpe-anw-central location-override** and **crypto pki ta-profile root-cert** settings, prompting an automatic rollback to the previous configuration.
CNX-243321	After creating a VLAN and navigating to the Unified Devices list, the device displays a **Configuration Status** of **Out of Sync**. On the A**udit Trail** page, the system indicates that the device configuration push fails.
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-250071	Authentication fails because gateways resolve the captive portal to the default server group, which has no RADIUS servers configured. As a result, no authentication request is sent to ClearPass.