

# **HPE Aruba Networking Central API Reference Guide**



**Hewlett Packard**  
Enterprise

## Copyright Information

© Copyright 2025 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://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




---

<b>Contents</b> .....	<b>3</b>
<b>About this Guide</b> .....	<b>4</b>
Related Documents .....	4
Conventions .....	4
Terminology Change .....	5
Contacting Support .....	5
<b>API Gateway</b> .....	<b>6</b>
Accessing API Gateway Page .....	7
Viewing Swagger Interface .....	7
Example of Supported API Categories .....	8
Domain URL .....	9
Creating Application and Token .....	10
OAuth 2.0 for Authentication .....	11
Access Tokens .....	12
Access Token Best Practices .....	12
Obtain an Access Token .....	12
Access APIs .....	22
Access Tenant APIs Using MSP Access Token .....	24
Viewing and Revoking Tokens .....	24
Adding a New Token .....	25
API Gateway Usage Statistics .....	26
Changes to HPE Aruba Networking Central APIs .....	26
New APIs .....	26
Modified APIs .....	29
Deprecated APIs .....	31
Removed APIs .....	38
APIs Introduced In Previous Releases .....	43
APIs Modified In Previous Releases .....	56
<b>Webhooks</b> .....	<b>63</b>
Creating and Updating Webhooks Through the UI .....	64
Viewing and Editing Webhooks .....	65
Refreshing Webhooks Token Through the UI .....	66
Creating and Updating Webhooks Through the API Gateway .....	67
List of Webhooks APIs .....	67
Sample Webhooks Payload Format for Alerts .....	69
Access Point Alerts—Sample JSON .....	70
AOS-S Alerts—Sample JSON .....	82
AOS-CX Switch Alerts—Sample JSON .....	90
Gateway Alerts—Sample JSON .....	99
Miscellaneous Alerts—Sample JSON .....	123

This guide describes how to use **HPE Aruba Networking Central** application Programming Interface (API) to configure your applications.

## Related Documents

For more information about using HPE Aruba Networking Central, see the *HPE Aruba Networking Central Help Center* —To access the Help Center, click the  help icon on the HPE Aruba Networking Central UI, and select **Documentation Center**.

## Conventions

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

**Table 1:** *Typographical Conventions*

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
System items	This fixed-width font depicts the following: <ul style="list-style-type: none"><li>▪ Sample screen output</li><li>▪ System prompts</li></ul>
<b>Bold</b>	<ul style="list-style-type: none"><li>▪ Keys that are pressed</li><li>▪ Text typed into a GUI element</li><li>▪ GUI elements that are clicked or selected</li></ul>

The following informational icons are used throughout this guide:



---

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

---



---

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

---



---

Indicates a risk of personal injury or death.

---

# 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, HPE Aruba Networking 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	<a href="http://arubanetworks.com">arubanetworks.com</a>
Support Site	<a href="https://networkingsupport.hpe.com/home">https://networkingsupport.hpe.com/home</a>
Airheads Social Forums and Knowledge Base	<a href="http://community.arubanetworks.com">community.arubanetworks.com</a>
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	<a href="http://arubanetworks.com/support-services/contact-support/">arubanetworks.com/support-services/contact-support/</a>
Software Licensing Site	<a href="http://lms.arubanetworks.com">lms.arubanetworks.com</a>
End-of-life Information	<a href="http://arubanetworks.com/support-services/end-of-life/">arubanetworks.com/support-services/end-of-life/</a>
Security Incident Response Team	Site: <a href="http://arubanetworks.com/support-services/security-bulletins/">arubanetworks.com/support-services/security-bulletins/</a> Email: <a href="mailto:aruba-sirt@hpe.com">aruba-sirt@hpe.com</a>

# API Gateway

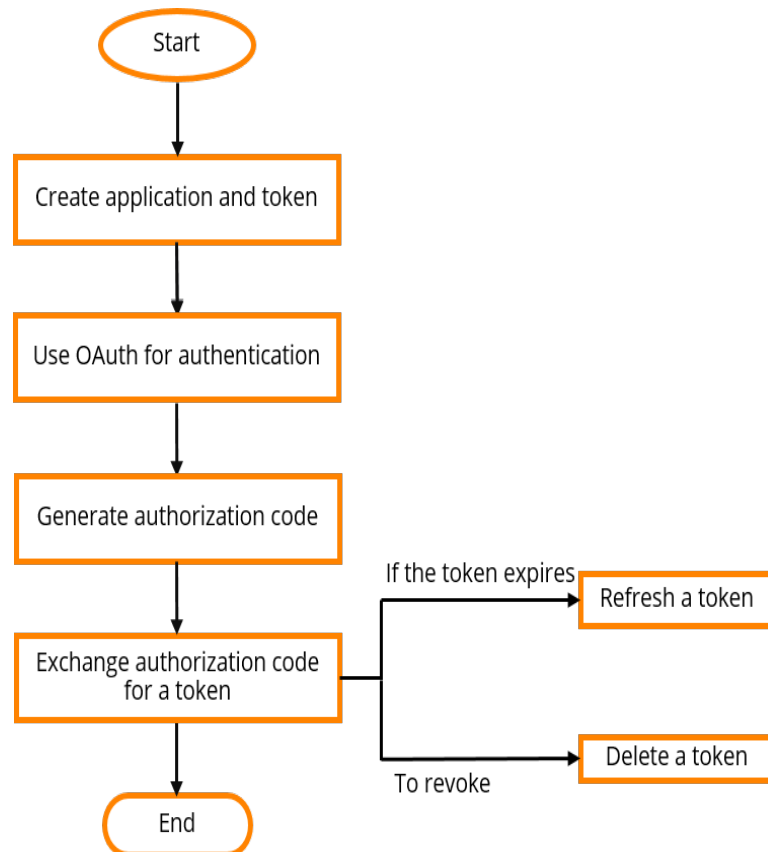
The **API Gateway** feature in HPE Aruba Networking Central supports the REST API for all HPE Aruba Networking Central services. This feature allows HPE Aruba Networking Central users to write custom applications, embed, or integrate the APIs with their own applications. The REST APIs support HTTP GET and POST operations by providing a specific URL for each query. The output for these operations is returned in the JSON format.

For secure access to the APIs, the HPE Aruba Networking Central API Framework plug-in supports the OAuth protocol for authentication and authorization. The access tokens provide temporary and secure access to the APIs. The access tokens have a limited lifetime for security reasons and the applications should use the refresh API to obtain new tokens periodically (every 2 hours).



- The API call volume rate-limit is seven (7) calls per second, per customer.
- You can update the device variables or parameter values for multiple devices using a single API call request.

The following figure illustrates the API gateway workflow for the users:



## Important Points to Note

- The admin user has a **System Apps & Tokens** tab which displays all the apps and tokens generated locally in the admin user profile. This tab also displays all the apps created in the non-admin user profiles. Clicking these apps lists out all the associated tokens created for the non-admin user profile.
- For users with limited group scope, the **Organization** menu will appear in the left menu when you click the keywords like Groups or Sites in the context selector.

For more information, see the following topics:

- [Accessing API Gateway Page](#)
- [Viewing Swagger Interface](#)
- [Example of Supported API Categories](#)
- [Domain URL](#)
- [Creating Application and Token](#)
- [OAuth 2.0 for Authentication](#)
- [API Gateway Usage Statistics](#)
- [Changes to HPE Aruba Networking Central APIs](#)

## Accessing API Gateway Page

To access the API Gateway, complete the following steps:

1. In the WebUI app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration**.
3. Under the **API Gateway** tile, click **Rest API**.  
Displays the **API Gateway** page.

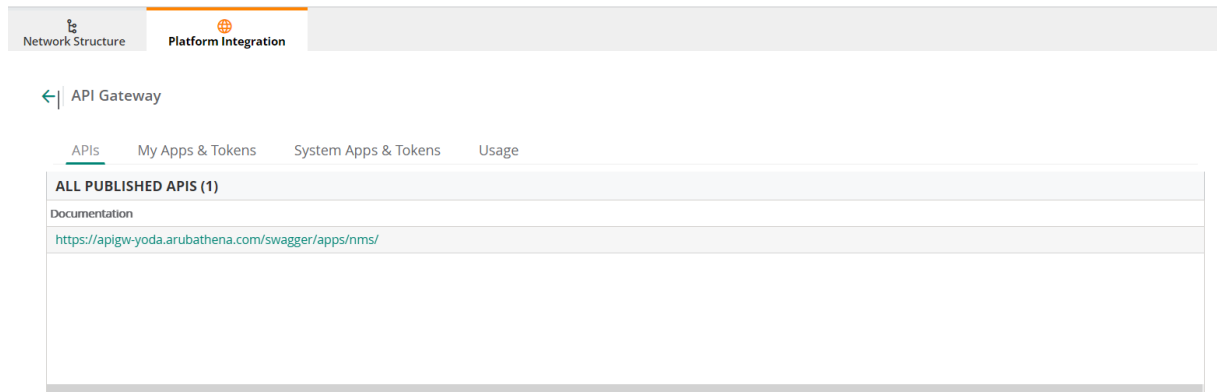
You can get new tokens and refresh old tokens. To obtain a new token application, you must set authentication parameters for a user session.

## Viewing Swagger Interface

To view the APIs managed through HPE Aruba Networking Central, complete the following steps:

1. In the WebUI app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration > Rest API**.
3. To view the Swagger interface, click the link in the **Documentation** column.  
Displays the Swagger documentation in a new window. If the **Documentation** column displays multiple accounts, select one of the accounts to view the Swagger documentation in a new window.  
On selecting the bookmarked Swagger documentation URL, displays a sign-in request window. To view the Swagger documentation, authenticate using the SSO and select one of the accounts.

**Figure 1** API Gateway Dashboard



## Example of Supported API Categories

The following table is an example of API Categories supported in HPE Aruba Networking Central.

**Table 3:** Example of API Categories and Description

API Category	Description
<b>Monitoring</b>	Gets network, client, and event details. It also allows you to manage labels and switches.
<b>Configuration</b>	<p>Allows you to configure and retrieve the following:</p> <ul style="list-style-type: none"> <li>Groups</li> <li>Templates</li> <li>Device Configuration</li> </ul> <p><b>NOTE:</b> For CX devices, only template groups support the template APIs and device configuration APIs.</p>
<b>AppRF</b>	Gets Top N AppRF statistics.
<b>Guest</b>	Gets visitor and session details of the portal.
<b>MSP</b>	<p>Allows you to manage and retrieve the following:</p> <ul style="list-style-type: none"> <li>Customers</li> <li>Users</li> <li>Resources</li> <li>Devices</li> </ul> <p>HPE Aruba Networking has enforced a request limit for the following APIs:</p> <ul style="list-style-type: none"> <li><b>GET /msp_api/v1/customers</b></li> <li><b>GET /msp_api/v1/customers/{customer_id}/devices</b></li> <li><b>GET /msp_api/v1/devices</b></li> <li><b>PUT /msp_api/v1/customers/{customer_id}/devices</b></li> </ul> <p>The maximum limit is set to 50 per API call. If you exceed this limit, the API call returns the HTTP error code 400 and the following error message: <b>LIMIT_REQUEST_EXCEEDED</b>.</p>
<b>User Management</b>	Allows you to manage users and also allows you to configure various types of users with a specific level of access control.
<b>Audit Event Logs</b>	Gets a list of audit events and the details of an audit event.



**Table 3: Example of API Categories and Description**

API Category	Description
<b>New Device Inventory</b>	Gets device details and device statistics.
<b>New Licensing</b>	Allows you to manage and retrieve subscription keys.
<b>Presence Analytics</b>	Allows you to configure the Presence Analytics application. It also retrieves site and loyalty data.
<b>Device Management</b>	Allows you to manage devices.
<b>Firmware</b>	Allows you to manage the firmware.
<b>Troubleshooting</b>	Gets a list of troubleshooting commands for a specific type of device.
<b>Notification</b>	Gets notification alerts generated for events pertaining to device provisioning, configuration, and user management.
<b>Unified Communications</b>	Retrieves data for all sessions for a specific time interval. It also retrieves the following: <ul style="list-style-type: none"> <li>▪ The total number of clients who made calls in the given time range.</li> <li>▪ Gets the Lync or Skype for Business URL for the HPE Aruba Networking Central cluster that you are using.</li> </ul>
<b>Refresh API Token</b>	Allows you to refresh the API token.
<b>Reporting</b>	Gets the list of configured reports for the given customer ID.
<b>Network Health</b>	Allows you to get data for all the labels and sites.
<b>Webhook</b>	Allows you to add, or delete Webhooks, and get or refresh Webhook tokens. See <a href="#">Webhooks</a> for further details on Webhook.
<b>VisualRF</b>	Allows you to retrieve information on floor plans, location of APs, clients, and rogue devices.
<b>DPS Monitoring</b>	Gets DPS compliance and session statistics for all the links of a device belonging to a specific policy.

Swagger documentation displays the complete list of APIs and the corresponding documentation. To access the Swagger documentation, see [Viewing Swagger Interface](#).

## Domain URL

To access the API Gateway or generating tokens, you must use the appropriate domain URL. The following table shows the region-specific domain URLs for accessing API Gateway:

**Table 4: Domain URLs for API Gateway Access**

Region	Domain Name
US-1	<a href="http://app1-apigw.central.arubanetworks.com">app1-apigw.central.arubanetworks.com</a>

Region	Domain Name
US-2	apigw-prod2.central.arubanetworks.com
US-East1	apigw-us-east-1.central.arubanetworks.com
US-WEST-4	apigw-uswest4.central.arubanetworks.com
EU-1	eu-apigw.central.arubanetworks.com
EU-Central2	apigw-eucentral2.central.arubanetworks.com
EU-Central3	apigw-eucentral3.central.arubanetworks.com
Canada-1	apigw-ca.central.arubanetworks.com
China-1	apigw.central.arubanetworks.com.cn
APAC-1	api-ap.central.arubanetworks.com
APAC-EAST1	apigw-apaceast.central.arubanetworks.com
APAC-SOUTH1	apigw-apacsouth.central.arubanetworks.com
UAE-NORTH1	apigw-uaenorth1.central.arubanetworks.com

## Creating Application and Token

To create an application, complete the following steps:

1. In the WebUI app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration > Rest API**.  
Displays the **API Gateway** page.
3. Click the **My Apps & Tokens** tab.



The user with the **HPE Aruba Networking Central Administrator** role will be able to create apps for all the non-admin users by clicking **+ Add Apps & Tokens** in the **System Apps & Tokens** tab.

4. Click **+ Add Apps & Tokens**.

**Figure 2** Add Apps and Tokens Option Page

The screenshot shows a web interface with two tables. The first table, titled 'MY APPS & TOKENS (1)', has columns: Name, Client ID, Client Secret, Redirect URI, and Created At. The second table, titled 'TOKEN LIST (1)', has columns: Token Id, User Name, Generated At, Revoke Token, and Download Token. Below the tables are pagination controls showing '5 10 25 50 Per Page' and 'Page: 1/1'.

5. In the **New Token** pop-up window, do the following:

a. Enter the application name.


In the non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable.

b. In the **Redirect URI** field, enter the redirect URL.

c. Click **Generate**. A new application is created and added to the

Creates and adds a new application to the **My Apps & Tokens** table. **My Apps & Tokens** table displays the following details:

- **Name**—Name of the application. In non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable. Any new tokens generated in non-admin user profile is associated with the same application name.
- **Client ID**—Unique ID for each application.
- **Client Secret**—Unique secret ID for each application.
- **Redirect URI**—Redirect URL.
- **Application**—Name of the application. For example, HPE Aruba Networking Central.
- **Tokens**—Token created for the application. The option is available to admin user profile only.
- **Created At**—Date on which the application was created.

To delete the added application, click delete  icon on the row corresponding to an application and click **Yes** to delete that application.



Only users with **HPE Aruba Networking Central Administrator** role will be able to generate tokens with multiple application names. In non-admin user profile, the **Application Name** field contains the user name and is non-editable. Any new tokens generated in non-admin user profile is associated with the same application name. However, all the multiple application names and the associated tokens in non-admin user profiles from the earlier versions is retained in the **Token List** table.

## OAuth 2.0 for Authentication

For secure access to the APIs, the HPE Aruba Networking Central API Framework plug-in supports the OAuth protocol for authentication and authorization. OAuth 2.0 is a simple and secure authorization framework. It allows applications to acquire an access token for HPE Aruba Networking Central through a variety of work flows supported within the OAuth 2.0 specification.

All OAuth 2.0 requests must use the SSL endpoint available at the Domain URL (for example, <https://app1-apigw.central.arubanetworks.com>).

## Access Tokens

The access token is a string that identifies a user, app, or web page and is used by the app to access an API. The access tokens provide temporary and secure access to the APIs.

The access tokens have a limited lifetime. If the application uses web server or user-agent OAuth authentication flows, a refresh token is provided during authorization that can be used to get a new access token.

If you are writing long running applications (web app) or native mobile applications, you must refresh the token periodically. For more information, see [Refreshing a token](#).

This section includes the following topics:

- [Access Token Best Practices](#)
- [Obtain an Access Token](#)
- [Access APIs](#)
- [Access Tenant APIs Using MSP Access Token](#)
- [Viewing and Revoking Tokens](#)
- [Adding a New Token](#)

## Access Token Best Practices

Listed below are basic considerations and practices that must be followed when using an access token:

- The access token generated must be stored safely.
- The access token generated must be used to execute all REST API call. To view the list of APIs managed through HPE Aruba Networking Central, see [Viewing Swagger Interface](#).
- You must use the same access token to execute an API call without generating new access tokens multiple times. For every API call you must not create new access token.
- You must save the latest refresh token generated. Once the validity of the access token expires, renew the access token using the saved refresh token.
- You must refresh the access token when it is invalid or at least once within 15 days so that HPE Aruba Networking Central can honor refreshing the token and does not revoke it.

## Obtain an Access Token

Read the [Access Token Best Practices](#) topic before generating and using an access token.

Users can generate the OAuth token using one of the following methods:

- [Obtaining Token Using Offline Token Mechanism](#)
- [Obtaining Token Using OAuth Grant Mechanism](#)

## Obtaining Token Using Offline Token Mechanism

To obtain tokens using the offline token method, complete the following steps:

1. In the WebUI app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration > Rest API**.  
The **API Gateway** page is displayed.
3. Click **My Apps & Tokens**.



---

Only the user with **HPE Aruba Networking Central Administrator** role can view the **System Apps & Tokens** tab which displays all the apps and tokens generated in all the non-admin user profiles in addition to the apps and tokens created in the admin user profile.

The user with the **HPE Aruba Networking Central Administrator** role cannot view or download tokens created by other users with the administrator or non-administrator roles. The user with the **HPE Aruba Networking Central Administrator** role can only revoke a token created by other users.

---

4. Click **+ Add Apps & Tokens**. The **New Token** pane is displayed.
5. Enter the application name and redirect URI in the **Application Name** and **Redirect URI** fields respectively.  
In non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable.
6. Click **Generate**.  
The token is generated and displayed in the **My Apps & Tokens** table.

**My Apps & Tokens** table displays the following details:

- **Token ID**—Token ID of the application.
- **User Name**—Name of the user to whom this token is associated to. An application can be associated to multiple users.
- **Application**—Name of the application to which this token is associated to. For example, HPE Aruba Networking Central.
- **Generated At**—Date on which the token was generated.
- **Revoke Token**—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
- **Download Token**—Click **Download Token** to download the token.

## Obtaining Token Using OAuth Grant Mechanism

The following section describes the steps for obtaining the access token and refresh token using the authorization code grant mechanism:

- [Step 1: Authenticate a User and Create a User Session](#)
- [Step 2: \[Optional\] Generating Client Credentials](#)
- [Step 3: Generate Authorization Code](#)
- [Step 4: Exchange Auth Code for a Token](#)
- [Step 5: Refreshing a Token](#)
- [Step 6: Deleting a Token](#)

- In previous releases, system users could be added to a Central account with the same domain as the configured SSO domain. Starting from this release, If you have a claimed domain name for SSO, you can no longer add system users with the same domain. For example, you cannot add a system users with **@example.com**, if the domain **example.com** is already claimed. Users of the system must be located outside of the domain.
- If you have SSO enabled and want to access HPE Aruba Networking Central's REST API, use the offline approach to create your token on the Central API Gateway and then use the refresh token API to update it as part of your automated workflows. To know more about the offline approach, see [Obtaining Token Using Offline Token Mechanism](#).
- The rate limit to generate a new access token for a client ID is restricted to 1 access token per 30 minutes. This is applicable in [Step 1](#) and [Step 3](#).
- It is recommended to refresh the access token when it is invalid or at least once within 15 days so that Central can honor refreshing the token and does not revoke it.



## Step 1: Authenticate a User and Create a User Session

The following API authenticates a user and returns a user session value that can be used to create future requests for a client with the specified username and password. The rate limit for user authentication is set to 3 login attempts per 30 minutes. If all 3 login attempts fail, the user is locked out and can retry the login attempt after 30 minutes.

It is assumed that you already have a client ID for your application. For more information on how to create an application and obtain tokens, see [Creating Application and Token](#).

[Domain URL](#) allow you to log in to the API gateway server and to establish the user session. This endpoint is accessible over SSL, and HTTP (non-SSL) connections are redirected to SSL port. The following table lists the region specific domain URLs for accessing the API gateway.

If user authentication is successful, the request will return HTTP code 200 and the response header will include the following attributes.

**Table 5: Authentication and User session Response Codes**

Header Key example	Values	Description
<a href="https://app1--&lt;FQDN of the HPE Aruba Networking Central instance&gt;.com/oauth2/authorize/central/api/login?client_id=&lt;client_id&gt;">https://app1--&lt;FQDN of the HPE Aruba Networking Central instance&gt;.com/oauth2/authorize/central/api/login?client_id=&lt;client_id&gt;</a>	csrfToken=xxxx; session=xxxx	The server returns a CSRF token and identifies the user session, which must be used for all subsequent HTTP requests.

### Example

**Request Method:** POST

**URL:** [https://app1- <FQDN of the HPE Aruba Networking Centralinstance>.com/oauth2/authorize/central/api/login?client\\_id=<client\\_id>](https://app1- <FQDN of the HPE Aruba Networking Centralinstance>.com/oauth2/authorize/central/api/login?client_id=<client_id>) HTTP/1.1

**Host:** app1--<FQDN of the HPE Aruba Networking Centralinstance>.com

**Request Header:**

**Accept:** application/json

**Content -Type:** application/json

**POST Request Body(JSON):**

```
{
  "username": "xxxxxx",
  "password": "xxxxxx"
}
```

### Error Response:

400: Bad Request

#### Response Body (JSON):

```
{
  "extra": {},
  "message": "<error string>"
}
```

401: Auth failure

#### Response Body (JSON):

```
{
  "message": "Auth failure",
  "status": false
}
```

429: API rate limit exceeded

#### Response Body (JSON):

```
{
  "message": "API rate limit exceeded. Please retry after xxxx seconds"
}
```

### Success Response:

200: OK

#### Response Body (JSON):

```
{
  "status": true
}
```

#### Response Header:

Set-Cookie: csrftoken=xxxx;session=xxxx;




---

The **csrf token** value received in the successful response message must be used as a parameter for all subsequent POST/PUT requests. The **session** value must also be used for all subsequent requests to maintain the user session context.

---

## Step 2: [Optional] Generating Client Credentials

The following API can be used to generate client credentials for a specific tenant using your Managed Service Provider (MSP) Client ID.

The rate limit to generate client credentials for a client ID is restricted to 2 seconds.

**Table 6: URL to Generate Client Credentials**

URL example	Description
<a href="https://app1--&lt;FQDN of the HPE Aruba Networking Central instance&gt;.com/oauth2/authorize/central/api/client_credentials?client_id=&lt;msp_client_id&gt;">https://app1--&lt;FQDN of the HPE Aruba Networking Central instance&gt;.com/oauth2/authorize/central/api/client_credentials?client_id=&lt;msp_client_id&gt;</a>	The <b>&lt;msp_client_id&gt;</b> variable is the client ID given from Central to that a Managed Service Provider that user registered the application.

### Example

**Request Method:** POST

**URI**—[https://app1--<FQDN of the HPE Aruba Networking Central instance>.com/oauth2/authorize/central/api/client\\_credentials?client\\_id=<msp\\_client\\_id>](https://app1--<FQDN of the HPE Aruba Networking Central instance>.com/oauth2/authorize/central/api/client_credentials?client_id=<msp_client_id>)

**POST Request Body(JSON):**

```
{
  "customer_id": "<tenant_id>"
}
```

```
}  
Request Header: (Values from login API request)
```

```
Set-Cookie: csrftoken=xxxx;session=xxxx;
```

**Response Body(JSON):**

```
{  
  "client_id": "<new-client-id>",  
  "client_secret": <new-client-secret>"  
}
```

**Error Response**

429: API rate limit exceeded

**Response Body (JSON):**

```
{  
  "message": "API rate limit exceeded. Please retry after xxxx seconds"  
}
```

### Step 3: Generate Authorization Code

After the user is authenticated and you have a valid session for that user, use this API to get authorization code. The authorization code is valid only for 5 minutes and must be exchanged for a token within that time.

**Table 7: URL for to Generate an Authorization Code**

URL example	Description
<a href="https://app1 -&lt;FQDN of the HPE Aruba Networking Centralinstance&gt;.com/oauth2/authorize/central/api?client_id=&lt;client_id&gt;&amp;response_type=code&amp;scope=all">https://app1 -&lt;FQDN of the HPE Aruba Networking Centralinstance&gt;.com/oauth2/authorize/central/api?client_id=&lt;client_id&gt;&amp;response_type=code&amp;scope=all</a> HTTP/1.1	The endpoint is a POST call to get an authorization code.

Query parameters for this API are as follows:

**Table 8: Query Parameters for the Auth Code API**

Parameter	Values	Description
client_id	<b>client_id</b> is a unique hexadecimal string	The <b>client_id</b> is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin.
response_type	<b>code</b>	Use <b>code</b> as the response type to get the authorization code that can be exchanged for token



Parameter	Values	Description
scope	all or read	Requested API permissions may be either <b>all</b> (for both read and write access) or <b>read</b> for read-only access.

### Example

**Request Method:** POST

**URL:** [https://app1-<FQDN of the HPE Aruba Networking Centralinstance>.com/oauth2/authorize/central/api/?client\\_id=<client\\_id>&response\\_type=code&scope=all](https://app1-<FQDN of the HPE Aruba Networking Centralinstance>.com/oauth2/authorize/central/api/?client_id=<client_id>&response_type=code&scope=all) HTTP/1.1

**Host:** app1--<FQDN of the HPE Aruba Networking Centralinstance>.com

**Request Header:**

**Accept:** application/json Cookie: "session=xxxx" X-CSRF-Token: xxxx

**Content -Type:** application/json

**POST Request Body(JSON):**

```
{
  "customer_id": "xxxxx"
}
```

**Error Response:**

400: Bad Request

**Response Body (JSON):**

```
{
  "extra": {},
  "message": "<error string>"
}
```

401: Auth failure

**Response Body (JSON):**

```
{
  "message": "Auth failure",
  "status": false
}
```

429: API rate limit exceeded

**Response Body (JSON):**

```
{
  "message": "API rate limit exceeded. Please retry after xxxx seconds"
}
```

**Success Response:**

200: OK

**Response Body (JSON):**

```
{
  " auth_code ": "xxxx"
}
```



Pass the **csrf-token** value you obtained in step one in the request header, otherwise the request will be rejected. Note the **auth\_code** value in the response, as you will use this code to obtain an OAuth token.

**Response Header:**

Set-Cookie: csrftoken=xxxx;session=xxxx;

## Step 4: Exchange Auth Code for a Token

Once you have an authorization code, you just use that code to request an access from the server. The exchanges should be done within 300 seconds of obtaining the auth code from the previous step, or the API will return an error.

**Table 9:** URL for to Generate an Auth Token

URL example	Description
<a href="https://app1-&lt;FQDN of the HPE Aruba Networking Centralinstance&gt;.com/oauth2/token">https:// app1 -&lt;FQDN of the HPE Aruba Networking Centralinstance&gt;.com/oauth2/token</a>	The endpoint is a POST call to get an access token using the authorization code obtained from the server.

Query parameters for this API are as follows:

**Table 10:** Query Parameters for the Auth Code API

Parameter	Values	Description
client_id	<b>client_id</b> is a unique hexadecimal string	The <b>client_id</b> is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin.
client_secret	<b>client_secret</b> is a unique hexadecimal string	The <b>client_secret</b> is a unique identifier provided to each developer at the time of registration. Application developers can obtain a client ID and client secret when they register with the API gateway admin.
grant_type	<b>authorization_code</b>	Use <b>code</b> to get the authorization code that can be exchanged for the token.

Parameter	Values	Description
code	<b>auth_code</b> received from step 1	The authorization code received from the authorization server.
redirect_uri	string	The redirect URI must be the same as the one given at the time of registration. This is an optional parameter.

The response to this API query is a JSON dictionary with following values:

**Table 11:** *Auth Token Values*

Parameter	Values	Description
token_type	bearer	Identifies the token type. Central supports only the bearer token type (See <a href="https://tools.ietf.org/html/rfc6750">https://tools.ietf.org/html/rfc6750</a> )
refresh_token	string	Refresh tokens are credentials used to renew or refresh the access_token when it expires without repeating the complete authentication flow. A refresh token is a string representing the authorization granted to the client by the resource owner.
expires_in	seconds	The lifetime, in seconds, of the access token.
access_token	string	Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client.

### Example

**Request Method:** POST

**URL:** <https://apigw- <FQDN of the HPE Aruba Networking Centralinstance>.com/oauth2/token>

**Content -Type:** application/json

**Body Parameters:** Enter the parameter values to call the API

- client\_id
- client\_secret
- grant\_type
- code

**Response:**

```
{
  "refresh_token": "xxxx",
  "token_type": "bearer",
  "access_token": "xxxx",
  "expires_in": 7200
}
```

## Step 5: Refreshing a Token

You can update the access token without having to repeat the authentication process by using the refresh token obtained in the previous step. Below are some of the important points to note:

- A token created on Central API Gateway contains access and refresh tokens, and is available for 15 days.
- An access token is valid for 2 hours (7200 seconds).
- On refreshing the access token consecutively within 15 minutes, you obtain the same access token. To generate a new access token you must wait for 15 minutes before you refresh the access token.
- If the token is not used or refreshed for a period of 15 days, it is revoked from Central API Gateway.
- After a token is revoked, you have to add or generate a new token through the API Gateway.
- It is recommended to refresh the access token when it is invalid or at least once within 15 days so that Central can honor refreshing the token and does not revoke it.

**Table 12:** *URL to Refresh a Token*

URL example	Description
<a href="https://app1- &lt;FQDN of the HPE Aruba Networking Central instance&gt;.com/oauth2/token">https://app1- &lt;FQDN of the HPE Aruba Networking Central instance&gt;.com/oauth2/token</a>	The endpoint is a POST call to refresh the access token using the refresh token obtained from the server

Query parameters for this API are as follows:

**Table 13:** *Query Parameters for Refresh Tokens*

Parameter	Value	Description
client_id	<b>client_id</b> is a unique hexadecimal string	The <b>client_id</b> is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin.

Parameter	Value	Description
client_secret	<b>client_secret</b> is a unique hexadecimal string	The <b>client_secret</b> is a unique identifier provided to each developer at the time of registration. Application developers obtain a client ID and a client secret when they register with the API gateway admin.
grant_type	<b>refresh_token</b>	Specify <b>refresh_token</b> as the grant type to request that an authorization code be exchanged for a token
refresh_token	string	A string representing the authorization granted to the client by the resource owner.

The response to this API query is a JSON dictionary with following values:

Parameter	Value	Description
token_type	bearer	Identifies the token type. Only the bearer token type is supported. For more information, see <a href="https://tools.ietf.org/html/rfc6750">https://tools.ietf.org/html/rfc6750</a> .
refresh_token	string	Refresh tokens are credentials used to renew or refresh the access token when it expires without going through the complete authorization flow. A refresh token is a string representing the authorization granted to the client by the resource owner.
expires_in	seconds	The expiration duration of the access tokens in seconds.
access_token	string	Access tokens are credentials used to access the protected resources. An access token is a string representing an authorization issued to the client.

## Example

### Method: POST

[https://apigw- -<FQDN of the HPE Aruba Networking Centralinstance>.com/oauth2/token?client\\_id=<Central-API-app-clientid>&client\\_secret=xxxx&grant\\_type=refresh\\_token&refresh\\_token=xxxx](https://apigw- -<FQDN of the HPE Aruba Networking Centralinstance>.com/oauth2/token?client_id=<Central-API-app-clientid>&client_secret=xxxx&grant_type=refresh_token&refresh_token=xxxx)

### Response

```
{
  "refresh_token": "xxxx",
  "token_type": "bearer",
  "access_token": "xxxx",
  "expires_in": 7200
}
```

## Step 6: Deleting a Token

To delete the access token, access the following URL:

**Table 14:** URL to Delete a Token

URL example	Description
<a href="https://app1- -&lt;FQDN of the Aruba Centralinstance&gt;.com/oauth2/api/tokens">https://app1- -&lt;FQDN of the Aruba Centralinstance&gt;.com/oauth2/api/tokens</a>	This endpoint is accessible over SSL. The HTTP (non-SSL) connections are redirected to SSL port. Customer ID is a string.

## Example

### Method : DELETE

**URL:**<https://app1- -<FQDN of the HPE Aruba Networking Centralinstance>.com/oauth2/api/tokens>

### JSON Body:

```
{
  "access_token": "<access_token_to_be_deleted>"
}
```

### Headers:

**Content-Type:** application/json

**X-CSRF-Token:** <CSRF\_token\_obatined\_from\_login\_API>

**Cookie:** "session=<session\_obatined\_from\_login\_API>"

## Access APIs

To access the API, use the Domain URL (for example, <https://app1-apigw.central.arubanetworks.com/>).

This endpoint is accessible over SSL and the HTTP (non-SSL) connections are redirected to the SSL port.

**Table 15:** Accessing the AP

URL	Description
Domain URL For example, <a href="https://app1-apigw.central.arubanetworks.com/">https://app1-apigw.central.arubanetworks.com/</a>	The API gateway URL. You can access the APIs from this URL by providing a correct access token.

The parameters for the API are as follows:

**Table 16: Parameters for the API**

Parameter	Value
request_path	URL Path

**Table 17: Header for the API**

Header	Value
Authorization	Bearer <access token>

### Example

**Request Method:** GET

**request\_path:** <https://app1-apigw.central.arubanetworks.com/monitoring/v1/aps>

**Request Header:**

**Authorization:** Bearer ouzMaXEBbB6XqGtsWomK7MvaTuhrqDQ1

**Response:**

```
{
  "aps": [
    {
      "firmware_version": "6.4.4.4-4.2.3.1_54637",
      "group_name": "00TestVRK",
      "ip_address": "10.29.18.195",
      "labels": [
        "Filter_242",
        "Ziaomof",
        "roster",
        "242455",
        "Diegso"
      ],
      "macaddr": "6c:f3:7f:c3:5d:92",
      "model": "AP-134",
      "name": "6c:f3:7f:c3:5d:92",
      "radios": [
        {
          "band": 0,
          "index": 1,
          "macaddr": "6c:f3:7f:b5:d9:20",
          "status": "Down"
        },
        {
          "band": 1,
          "index": 0,
          "macaddr": "6c:f3:7f:b5:d9:30",
          "status": "Down"
        }
      ],
      "serial": "AX0140586",
      "status": "Down",
      "swarm_id": "e3bf1ba201a6f85f4b5eaedead5e502d85a9aef58d8e1d8a0",
      "swarm_master": true
    }
  ],
}
```

```
"count": 1
}
```

## Access Tenant APIs Using MSP Access Token

MSP users can use their access token to perform the operation on their tenant accounts using NBAPI. User privileges as per the tenant role are applied for these operations. An MSP user must provide the tenant info (CID) as part of the request header.



---

The Rate-limit will be consumed from the MSP account quota.

---

**Table 18:** Header for the API

Header	Value
TenantID	267958b55d5a463e94a302c20f4a6b68

### Example

**Request Method:** GET

<https://app1-apigw.central.arubanetworks.com/central/v2/sites>

**Request Header:**

**TenantID:** 267958b55d5a463e94a302c20f4a6b68

**Response Code:** 200

**Response:**

```
{
  "count": 1,
  "sites": [
    {
      "address": "bangalore",
      "associated_device_count": 4,
      "city": "bangalore",
      "country": "India",
      "latitude": "12.9298689",
      "longitude": "77.6848366",
      "site_id": 1,
      "site_name": "test-pcap",
      "state": "Karnataka",
      "tags": null,
      "zipcode": "560103"
    }
  ],
  "total": 1
}
```

## Viewing and Revoking Tokens

To view or revoke tokens, complete the following steps:



1. In the WebUI app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration > Rest API**. The **API Gateway** page is displayed.
3. Click **My Apps & Tokens**. The **Token List** table displays the following:
  - **Token ID**—Token ID of the application.
  - **User Name**—Name of the user to whom this token is associated. An application can be associated to multiple users.
  - **Application**—Name of the application to which this token is associated. For example, HPE Aruba Networking Central.
  - **Generated At**—Token generated date.
  - **Revoke Token**—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
  - **Download Token**—Click **Download Token** to download the token.



---

The admin user has a **System Apps & Tokens** tab which displays all the apps and tokens generated in all non-admin user profiles. It also displays the apps and tokens created in the admin user profile. To view all the tokens of admin and non-admin users, go to **Organization > Platform Integration > Rest API > System Apps & Tokens**.

---

## Adding a New Token

To add a new token, complete the following steps:

1. In the WebUI app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration > Rest API**. The **API Gateway** page is displayed.
3. Click **My Apps & Tokens**. The **Token List** table displays the following:
  - **Token ID**—Token ID of the application.
  - **User Name**—Name of the user to whom this token is associated. An application can be associated to multiple users.
  - **Application**—Name of the application to which this token is associated. For example, HPE Aruba Networking Central.
  - **Generated At**—Date on which the token was generated.
  - **Revoke Token**—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
  - **Download Token**—Click **Download Token** to download the token.



---

The user with the **HPE Aruba Networking Central Administrator** role can create tokens for all non-admin users by clicking **+ Add Apps & Tokens** in the **System Apps & Tokens** tab.

---

4. Click **+ Add Apps & Tokens** to add a new token.
5. Enter the application name in the **Application Name** box and click **Generate**.



---

If you have registered a custom URI when creating a new app under **System Apps and Tokens**. Then the **Redirect URI** option is disabled for you in the **My Apps and Tokens > + Add Apps and Tokens > New Token**. In such cases, the **Redirect URI** option in **Add Apps and Tokens > New Token** under **My Apps and Tokens** populates your already registered URI.

---

## API Gateway Usage Statistics

The **API Gateway** page includes the **Usage** tab that displays the API usage. The **Usage** tab is available only for users with the **HPE Aruba Networking Central Administrator** role and the usage data is stored only for the previous 30 days. The tables on the **Usage** page display data for seven days.

The following details are displayed:

- Current Usage
- Last one week API usage data
- Per user usage
- MSP and tenant usage if you are in MSP mode

For more information on usage statistics, see [Viewing Usage Statistics](#) topic.

## Changes to HPE Aruba Networking Central APIs

The Swagger interface lists all the APIs that are managed through HPE Aruba Networking Central. For more information on how to access the swagger interface, see [API Gateway](#). Once you gain access to the HPE Aruba Networking Central APIs from swagger, select one of the service from the URL drop-down list. The URL allows you to access all the services and their respective APIs that are managed through HPE Aruba Networking Central. For example, to try out the monitoring service APIs, select the **Monitoring** service from the URL drop-down list and select one of the respective API under **API Reference**.

This section lists the new APIs, deprecated APIs, alternative APIs, and APIs removed from HPE Aruba Networking Central:

- [New APIs](#)
- [Modified APIs](#)
- [Deprecated APIs](#)
- [Removed APIs](#)
- [APIs Introduced In Previous Releases](#)
- [APIs Modified In Previous Releases](#)

## New APIs

The following table lists the APIs introduced in the current release:

**Table 19:** *New APIs*

New API	Description
Cloud Connect > Cloud connect	

**Table 19: New APIs**

New API	Description
<ul style="list-style-type: none"> <li>▪ [POST] /cloud-connect/v1/node_list/{node_id}/config/prisma</li> </ul>	This API is introduced to create the Cloud VPN Connect Service endpoint configurations for Prisma Cloud service provider.
<ul style="list-style-type: none"> <li>▪ [PUT] /cloud-connect/v1/node_list/{node_id}/config/prisma</li> </ul>	This API is introduced to update and modify the Cloud VPN Connect Service endpoint configurations for Prisma Cloud service provider.
<ul style="list-style-type: none"> <li>▪ [DELETE] /cloud-connect/v1/node_list/{node_id}/config/prisma</li> </ul>	This API is introduced to delete the Cloud VPN Connect Service endpoint configurations for Prisma Cloud service provider.
<ul style="list-style-type: none"> <li>▪ [GET] /cloud-connect/v1/all-tunnel-policy-configs</li> </ul>	This API is introduced to fetch the list of Tunnel Policy configurations.
<ul style="list-style-type: none"> <li>▪ [GET] /cloud-connect/v1/custom-account/{account_name}</li> </ul>	This API is introduced to fetch the custom cloud account configuration for the specified account name.
<ul style="list-style-type: none"> <li>▪ [PUT] /cloud-connect/v1/custom-account/{account_name}</li> </ul>	This API is introduced to update an existing custom cloud account configuration for the specified account name.
<ul style="list-style-type: none"> <li>▪ [POST] /cloud-connect/v1/custom-account/{account_name}</li> </ul>	This API is introduced to create a custom cloud account configuration for the specified account name.
<ul style="list-style-type: none"> <li>▪ [DELETE] /cloud-connect/v1/custom-account/{account_name}</li> </ul>	This API is introduced to delete custom cloud account configuration for the specified account name.
<ul style="list-style-type: none"> <li>▪ [GET] /cloud-connect/v1/prisma-account/{account_name}</li> </ul>	This API is introduced to fetch Prisma Cloud account configuration for the specified account name.
<ul style="list-style-type: none"> <li>▪ [PUT] /cloud-connect/v1/prisma-account/{account_name}</li> </ul>	This API is introduced to update the Prisma Cloud account configuration for the specified account name.
<ul style="list-style-type: none"> <li>▪ [POST] /cloud-connect/v1/prisma-account/{account_name}</li> </ul>	This API is introduced to create a new Prisma Cloud account configuration for the specified account name.
<ul style="list-style-type: none"> <li>▪ [DELETE] /cloud-connect/v1/prisma-account/{account_name}</li> </ul>	This API is introduced to delete Prisma Cloud account configuration for the specified account name.
<b>Device Replacement &gt; Offline Devices</b>	
<ul style="list-style-type: none"> <li>▪ [GET] /v1/offline_device</li> </ul>	This API is introduced to get a list of all offline devices.
<b>Device Replacement &gt; Request Replacement</b>	
<ul style="list-style-type: none"> <li>▪ [POST] /v1/request_replacement</li> </ul>	This API is introduced to request the replacement of a single device or devices in bulk.
<b>Device Replacement &gt; Check Compliance</b>	

**Table 19: New APIs**

New API	Description
<ul style="list-style-type: none"> <li>[POST] /v1/check_compliance</li> </ul>	<p>This API is introduced to determine whether the model numbers of the new and faulty devices match and if they are present in the inventory. These are pre-requisites before initiating a device replacement.</p> <p><b>NOTE:</b> The model number of the faulty and new devices must be the same for device replacement.</p>
<b>Device Replacement &gt; Initiate Replacement</b>	
<ul style="list-style-type: none"> <li>[POST] /v1/initiate_replacement</li> </ul>	<p>This API is introduced to initiate replacement for a single device or bulk devices.</p>
<b>Device Replacement &gt; Cancel Replacement</b>	
<ul style="list-style-type: none"> <li>[POST] /v1/cancel_replacement</li> </ul>	<p>This API is introduced to cancel replacement request for a single device or bulk devices.</p>
<b>Device Replacement &gt; Devices Under Replacement</b>	
<ul style="list-style-type: none"> <li>[GET] /v1/devices</li> </ul>	<p>This API is introduced to fetch the list of devices under replacement.</p>
<b>Device Replacement &gt; Devices Status</b>	
<ul style="list-style-type: none"> <li>[GET] /v1/device_status</li> </ul>	<p>This API is introduced to fetch the replacement status of a device using the devices serial number.</p>
<b>Device Replacement &gt; Devices count</b>	
<ul style="list-style-type: none"> <li>[GET] /v1/device_count</li> </ul>	<p>This API is introduced to get the count of devices under replacement for a given site. You can get the device count for following categories:</p> <ul style="list-style-type: none"> <li>Device requested for replacement</li> <li>Device initiated for replacement</li> <li>Devices that have completed replacement</li> </ul>
<b>Device Replacement &gt; Get MSP customers</b>	
<ul style="list-style-type: none"> <li>[GET] /v1/msp_customers</li> </ul>	<p>This API is introduced to get the list of tenants under the specified MSP account.</p>
<b>Device Replacement &gt; MSP Replacement Count</b>	
<ul style="list-style-type: none"> <li>[GET] /v1/msp_replacement_count</li> </ul>	<p>This API is introduced to get the count of devices under replacement for a MSP customer. You can get the device count for following categories:</p> <ul style="list-style-type: none"> <li>Device requested for replacement</li> <li>Device initiated for replacement</li> <li>Devices that have completed replacement</li> </ul>
<b>Device Replacement &gt; MSP replacement detail</b>	

**Table 19: New APIs**

New API	Description
<ul style="list-style-type: none"> <li>[GET] /v1/msp_replacement_details</li> </ul>	The API is introduced to get replacement information of all tenants under that MSP Account.
<b>IDS &gt; Detection Protection</b>	
<ul style="list-style-type: none"> <li>[GET] /network-config/v1/alpha1/ids/{name}/detection-protection/laa-counter-msg</li> </ul>	This API is introduced to fetch the Locally Administered Address (LAA) or random MAC address and interval parameters of a specific IDS profile.
<ul style="list-style-type: none"> <li>[POST] /network-config/v1/alpha1/ids/{name}/detection-protection/laa-counter-msg</li> </ul>	This API is introduced to create or configure the Locally Administered Address (LAA) or random MAC address and interval parameters for a specific IDS profile.
<b>Monitoring &gt; Switch</b>	
<ul style="list-style-type: none"> <li>[GET] /monitoring/v1/cx_switches/{serial}/neighbors</li> </ul>	This API is introduced to fetch lldp device neighbor list information for the AOS-CX switch. The serial number of the switch is required as an input parameter.
<ul style="list-style-type: none"> <li>[GET] /monitoring/v1/cx_switch_stacks/{stack_id}/neighbors</li> </ul>	This API is introduced to fetch lldp device neighbor list information for CX switch. The stack-id of the VSF-switch is required as an input parameter to call the API.
<b>Service UCC &gt; Aruba ucc</b>	
<ul style="list-style-type: none"> <li>[POST] /ucc-config/v1/node_list/{node_type}/{node_id}/config/ucc_alg/zoom/</li> </ul>	This API is introduced to create DSCP Priority configuration for Zoom using HPE Aruba Networking UCC.
<ul style="list-style-type: none"> <li>[PUT] /ucc-config/v1/node_list/{node_type}/{node_id}/config/ucc_alg/zoom/</li> </ul>	This API is introduced to update DSCP Priority configuration for Zoom using HPE Aruba Networking UCC.
<ul style="list-style-type: none"> <li>[GET] /ucc-config/v1/node_list/{node_type}/{node_id}/config/ucc_alg/zoom/</li> </ul>	This API is introduced to fetch information of DSCP Priority configuration for Zoom in HPE Aruba Networking UCC.
<ul style="list-style-type: none"> <li>[DELETE] /ucc-config/v1/node_list/{node_type}/{node_id}/config/ucc_alg/zoom/</li> </ul>	This API is introduced to delete DSCP Priority configuration for Zoom in HPE Aruba Networking UCC.s

To view the APIs introduced in previous releases, see [APIs Introduced In Previous Releases](#).

## Modified APIs

The following table lists the APIs modified in the current release:

**Table 20: Modified APIs**

Modified API	Description
<b>Authentication &amp; Policy &gt; User Policy</b>	
<ul style="list-style-type: none"> <li>[GET] /cloudAuth/api/v1/user_policy</li> </ul>	The API is enhanced to support the following: <ul style="list-style-type: none"> <li>Octa platform is supported along with Google and</li> </ul>

**Table 20: Modified APIs**

Modified API	Description
	<p>Azure.</p> <ul style="list-style-type: none"> <li>A new parameter <code>client_profile_tag</code> is added to the body. On setting a valid client tag, you can configure the user policy with a rule to include the <code>client_profile_tag</code> along with the user group and client role. If <code>client_profile_tag</code> is not specified, the default value is set to <b>Any</b> in the user policy rule. This is an optional parameter.</li> </ul>
<ul style="list-style-type: none"> <li>[PUT]/cloudAuth/api/v1/user_policy</li> </ul>	<p>A new parameter <code>client_profile_tag</code> is added to the body. On setting a valid client tag, you can configure the user policy with a rule to include the <code>client_profile_tag</code> along with the user group and client role. If <code>client_profile_tag</code> is not specified, the default value is set to <b>Any</b> in the user policy rule. This is an optional parameter.</p>
<b>Ble Beacon Service</b>	
<ul style="list-style-type: none"> <li>[POST] /ble_cfg_beacons/{group_name}</li> <li>[POST] /edit_beacon_profiles/{group_name}/{profile_id}</li> </ul>	<p>A new parameter <b>other_payload</b> is added to configure the OpenLocate service. Openlocate is a self-locating wireless network that supports location coordination information (LCI) over BLE. This is a service-based configuration, pushed by Air Range to the Access Point. The <b>config_method</b> must be set to <b>auto_generate</b>, and the <b>adv_format</b> must be set to <b>openlocate</b> to configure the OpenLocate service. OpenLocate feature is supported only for AOS-10.x group. The OpenLocate Beacon supports the following options:</p> <ul style="list-style-type: none"> <li>Measured Power</li> <li>Geo Location</li> <li>Floor Location</li> <li>Identity</li> <li>URL</li> <li>Signature</li> </ul> <p>Measured Power and Geo Location options are default parameters, these parameters must be added in the <b>other_payload</b> body. If you add Identity, then you must add at least one parameter in the <b>identity_option</b> body. The <b>identity_option</b> supports the following parameters:</p> <ul style="list-style-type: none"> <li>serial_number</li> <li>ap_name</li> <li>ap_eth_mac</li> <li>iot_radio_mac</li> </ul> <p>If the <b>URL</b> and <b>Signature</b> are added in the <b>other_payload</b> body, then you must define the <b>URL</b> and <b>passphrase</b> values.</p>

**Table 20: Modified APIs**

Modified API	Description
	The values for the parameters defined in the <b>other_payload</b> body are updated by the device.
<ul style="list-style-type: none"> <li>▪ [GET] /ble_cfg_beacons/{group_name}</li> <li>▪ [GET] /ble_run_beacons/{group_name}</li> <li>▪ [GET] /ble_beacon_profiles</li> </ul>	<p>In the response body <b>openlocate</b> parameter displays the OpenLocate options that are configured using the following APIs:</p> <ul style="list-style-type: none"> <li>▪ config ble beacon profiles API—[POST] /ble_cfg_beacons/{group_name}</li> <li>▪ edit ble beacon profiles API—[POST] /edit_beacon_profiles/{group_name}/{profile_id}</li> </ul>
<b>Configuration &gt; AP Configuration</b>	
<ul style="list-style-type: none"> <li>▪ [GET]/configuration/v1/ap_cli/{group_name_or_guid_or_serial_number}</li> <li>▪ [POST]/configuration/v1/ap_cli/{group_name_or_guid_or_serial_number}</li> </ul>	A new parameter <b>syslocation</b> is added to the response body. Use the <b>syslocation</b> parameter to add location information for the device.
<b>Monitoring &gt; Clients</b>	
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/clients/wireless</li> <li>▪ [GET] /monitoring/v1/clients/wired</li> <li>▪ [GET] /monitoring/v2/clients</li> </ul>	A new parameter <b>hostname</b> is added to the response body. The <b>hostname</b> parameter displays the hostname of the device.

To view the APIs modified in previous releases, see [APIs Modified In Previous Releases](#).

## Deprecated APIs

Deprecated APIs are listed below in the following tables. These APIs will continue to function but could be removed in a future release. HPE Aruba Networking strongly discourages the use of these APIs and recommends that you use the alternative API.

### APIs deprecated as part of HPE Aruba Networking Central 2.5.8 release:

No deprecated APIs in HPE Aruba Networking Central 2.5.8 release.

### APIs deprecated as part of HPE Aruba Networking Central 2.5.7 release:

Deprecated API	Alternative API
<b>Authentication &amp; Policy &gt; Client Policy</b>	
[DELETE] /cloudAuth/api/v1/client_policy	[PUT] /cloudAuth/api/v3/client_policy/reset
<b>Authentication &amp; Policy &gt; User Policy</b>	
[DELETE] /cloudAuth/api/v1/user_policy	[PUT] /cloudAuth/api/v3/user_policy/reset
APIs in the <b>Authentication &amp; Policy &gt; Client Registration</b> sub-category are marked as deprecated. The new APIs are available in the <b>Authentication &amp; Policy &gt; MAC Registration</b> sub-category.	

Deprecated API	Alternative API
[GET] /cloudAuth/api/v1/client_registration	[GET] /cloudauth/api/v3/client/mac/registration
[POST] /cloudAuth/api/v1/client_registration	[POST] /cloudauth/api/v3/client/mac/registration
[DELETE] /cloudAuth/api/v1/client_registration/{mac_address}	[DELETE] /cloudauth/api/v3/client/mac/registration/{mac_address}
[PATCH] /cloudAuth/api/v1/client_registration/{mac_address}	[PATCH] /cloudauth/api/v3/client/mac/registration/{mac_address}

#### Authentication & Policy > File Upload

[POST] /cloudAuth/api/v2/upload/{upload_type}	[POST] /cloudauth/api/v3/bulk/{upload_type}
[GET] /cloudAuth/api/v2/upload/{upload_type}/status	[GET] /cloudauth/api/v3/bulk/{upload_type}/status
[GET] /cloudAuth/api/v2/upload/{upload_type}/errors	[GET] /cloudauth/api/v3/bulk/{upload_type}/error
[PUT] /cloudAuth/api/v2/upload/{upload_type}/terminate	[PUT] /cloudauth/api/v3/bulk/{upload_type}/terminate

### APIs deprecated as part of HPE Aruba Networking Central 2.5.6 release:

No deprecated APIs in HPE Aruba Networking Central 2.5.6 release.

### APIs deprecated as part of HPE Aruba Networking Central 2.5.5 release:

**Table 21:** *Deprecated APIs in HPE Aruba Networking Central 2.5.5 release*

Deprecated API	Alternative API
<b>Configuration &gt; Pre Provisioned Group</b>	
[POST] /device_management/v1/group/assign	NA

### APIs deprecated as part of HPE Aruba Networking Central 2.5.4 release

**Table 22:** *Deprecated APIs in HPE Aruba Networking Central 2.5.4 release*

Deprecated API	Alternative API
<b>Monitoring &gt; MobilityController</b>	
[GET] /monitoring/v1/mobility_controllers	[GET] /monitoring/v1/gateways
[GET] /monitoring/v1/mobility_controllers/{serial}	[GET] /monitoring/v1/gateways/{serial}
[DELETE] /monitoring/v1/mobility_controllers/{serial}	[DELETE] /monitoring/v1/gateways/{serial}



**Table 22: Deprecated APIs in HPE Aruba Networking Central 2.5.4 release**

Deprecated API	Alternative API
[GET] /monitoring/v1/mobility_controllers/{serial}/uplinks	[GET] /monitoring/v1/gateways/{serial}/uplinks
[GET] /monitoring/v1/mobility_controllers/uplinks/bandwidth_usage	[GET] /monitoring/v1/gateways/{serial}/uplinks/bandwidth_usage
[GET] /monitoring/v1/mobility_controllers/{serial}/uplinks/tunnel_stats	[GET] /monitoring/v1/gateways/{serial}/tunnels/stats
[GET] /monitoring/v1/mobility_controllers/uplinks/wan_compression_stats	[GET] /monitoring/v1/gateways/{serial}/uplinks/wan_compression_stats
[GET] /monitoring/v1/mobility_controllers/uplinks/distribution	[GET] /monitoring/v1/gateways/{serial}/uplinks/distribution
[GET] /monitoring/v1/mobility_controllers/{serial}/ports/bandwidth_usage	[GET] /monitoring/v1/gateways/{serial}/ports/bandwidth_usage
[GET] /monitoring/v1/mobility_controllers/{serial}/ports	[GET] /monitoring/v1/gateways/{serial}/ports
[GET] /monitoring/v1/mobility_controllers/{serial}/tunnels	[GET] /monitoring/v1/gateways/{serial}/tunnels
[GET] /monitoring/v1/mobility_controllers/{serial}/dhcp_clients	[GET] /monitoring/v1/gateways/{serial}/dhcp_clients
[GET] /monitoring/v1/mobility_controllers/{serial}/dhcp_servers	[GET] /monitoring/v1/gateways/{serial}/dhcp_pools
[GET] /monitoring/v1/mobility_controllers/{serial}/vlan	[GET] /monitoring/v1/gateways/{serial}/vlan

## APIs deprecated as part of HPE Aruba Networking Central 2.5.3 release

**Table 23: Deprecated APIs in HPE Aruba Networking Central 2.5.3 release**

Deprecated API	Alternative API
<b>Monitoring &gt; Access Points</b>	
[GET] /monitoring/v1/aps	[GET] /monitoring/v2/aps
[GET] /monitoring/v2/aps/{serial}/rf_summary	[GET] /monitoring/v3/aps/{serial}/rf_summary
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/aps/bandwidth_usage</li> <li>▪ [GET] /monitoring/v2/aps/bandwidth_usage</li> </ul>	[GET] /monitoring/v3/aps/bandwidth_usage

**Table 23: Deprecated APIs in HPE Aruba Networking Central 2.5.3 release**

Deprecated API	Alternative API
[GET] /monitoring/v1/aps/{serial}/uplink_history	NA
[GET] /monitoring/v1/aps/{serial}/neighbouring_clients	NA
[GET] /monitoring/v1/bssids	[GET] /monitoring/v2/bssids
[GET] /monitoring/v1/aps/bandwidth_usage/topn	[GET] /monitoring/v2/aps/bandwidth_usage/topn
<b>Monitoring &gt; Network</b>	
[GET] /monitoring/v1/networks	[GET] /monitoring/v2/networks
[GET] /monitoring/v1/networks/{network_name}	[GET] /monitoring/v2/networks/{network_name}
[GET] /monitoring/v1/networks/bandwidth_usage	[GET] /monitoring/v2/networks/bandwidth_usage
<b>Deprecated Licensing</b>	
[GET] /subscriptions	[GET] /platform/licensing/v1/subscriptions
[GET] /subscriptions/stats	[GET] /platform/licensing/v1/subscriptions/stats
[GET] /services/enabled	[GET] /platform/licensing/v1/services/enabled
[GET] /subscriptions/assign	[POST] /platform/licensing/v1/subscriptions/assign
[POST] /subscriptions/unassign	[POST] /platform/licensing/v1/subscriptions/unassign
[GET] /services/config	[GET] /platform/licensing/v1/services/config
[DELETE] /subscriptions/devices/all	[DELETE] /platform/licensing/v1/subscriptions/devices/all
[POST] /subscriptions/devices/all	[POST] /platform/licensing/v1/subscriptions/devices/all
[DELETE] /msp/subscriptions/devices/all	[DELETE] /platform/licensing/v1/msp/subscriptions/devices/all
[POST] /msp/subscriptions/devices/all	[POST] /platform/licensing/v1/msp/subscriptions/devices/all
[GET] /autolicensing/services/{service}/status	[GET] /platform/licensing/v1/autolicensing/services/{service}/status

**Table 23: Deprecated APIs in HPE Aruba Networking Central 2.5.3 release**

Deprecated API	Alternative API
[DELETE] /customer/settings/autolicense	[DELETE] /platform/licensing/v1/customer/settings/autolicense
[GET] /customer/settings/autolicense	[GET] /platform/licensing/v1/customer/settings/autolicense
[POST] /customer/settings/autolicense	[POST] /platform/licensing/v1/customer/settings/autolicense
[DELETE] /msp/customer/settings/autolicense	[DELETE] /platform/licensing/v1/msp/customer/settings/autolicense
[GET] /msp/customer/settings/autolicense	[GET] /platform/licensing/v1/msp/customer/settings/autolicense
[POST] /msp/customer/settings/autolicense	[POST] /platform/licensing/v1/msp/customer/settings/autolicense
<b>User Management</b>	
[POST] /v2/subscriptions/assign	[POST] /platform/licensing/v1/subscriptions/assign

## APIs deprecated as part of HPE Aruba Networking Central 2.5.2 release

**Table 24: Deprecated APIs in HPE Aruba Networking Central 2.5.2 release**

Deprecated API	Alternative API
<b>Presence Analytics</b>	
[GET] /presence/v2/config/thresholds	[GET] /presence/v3/config/thresholds
[POST] /presence/v2/config/thresholds	[POST] /presence/v3/config/thresholds
[GET] /presence/v2/analytics/aggregates	NA
[GET] /presence/v2/analytics/trends	[GET] /presence/v3/analytics/trends/passersby_visitors
[GET] /presence/v2/insights/top_sites	NA
[GET] /presence/v2/insights/bottom_sites	NA
[GET] /presence/v2/insights/sites/aggregates	[GET] /presence/v3/insights/sites/aggregates
[GET] /presence/v2/loyalty/aggregates	NA

**Table 24: Deprecated APIs in HPE Aruba Networking Central 2.5.2 release**

Deprecated API	Alternative API
[GET] /presence/v2/loyalty/trends	[GET] /presence/v3/analytics/trends/loyal_visitors
[GET] /presence/v2/loyalty/visits	[GET] /presence/v3/visit_frequency
<ul style="list-style-type: none"> <li>▪ [GET] /presence/v2/loyalty/aggregates/top_sites</li> <li>▪ [GET] /presence/v2/loyalty/aggregates/bottom_sites</li> <li>▪ [GET] /presence/v2/loyalty/trends/top_sites</li> <li>▪ [GET] /presence/v2/loyalty/trends/bottom_sites</li> </ul>	NA
<b>NOTE:</b> Expected to be slow for customers with large number of sites.	
[GET] /presence/v2/loyalty/sites/aggregates	[GET] /presence/v3/insights/sites/aggregates

**Monitoring > VPN**

<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/vpn/usage</li> <li>▪ [GET] /monitoring/v2/vpn/usage</li> </ul>	[POST] /monitoring/v3/vpn/usage
--	---------------------------------

**User Management**

[POST] /v2/subscriptions/assign	[POST] /platform/licensing/v1/subscriptions/assign
---------------------------------	--

**APIs deprecated as part of HPE Aruba Networking Central 2.5.1 release**

No deprecated APIs in HPE Aruba Networking Central 2.5.1 release.

**APIs deprecated as part of HPE Aruba Networking Central 2.5.0 release****Table 25: Deprecated APIs in HPE Aruba Networking Central 2.5.0 release**

Deprecated API	Alternative API
<b>Clarity</b>	
[GET] /clarity/v1/overview/healthscore	NA
[GET] /clarity/v1/overview/healthscore/dns	NA
[GET] /clarity/v1/overview/network_stats	NA

**Table 25: Deprecated APIs in HPE Aruba Networking Central 2.5.0 release**

Deprecated API	Alternative API
[GET] /clarity/v1/ssid/names	NA
[GET] /clarity/v1/overview/reasons	NA
[GET] /clarity/v1/overview/attempts	NA
[GET] /clarity/v1/overview/attempts	NA
[GET] /clarity/v1/overview/device_attempts	NA
[GET] /clarity/v1/trend/healthscore	NA
[GET] /clarity/v1/trend/healthscore/dns	NA
[GET] /clarity/v1/trend/network_stats	NA
[GET] /clarity/v1/clients/search/partial	NA
[GET] /clarity/v1/clients/search/absolute	NA
[GET] /clarity/v1/clients/details	NA
[GET] /clarity/v1/clients/stats	NA
[GET] /clarity/v1/insights	NA
[GET] /clarity/v1/insights/details	NA
[GET] /clarity/v1/insights/distribution	NA
[GET] /clarity/v1/license	NA
<b>User Management</b>	
[GET] /accounts/v2/users	[GET] /platform/rbac/v1/users
[POST] /accounts/v2/users	[POST] /platform/rbac/v1/users
[POST] /accounts/v1/users/change_password	[POST] /platform/rbac/v1/users/{user_id}/password
[POST] /accounts/v1/users/reset_password	[POST] /platform/rbac/v1/users/{user_id}/password/reset
[GET] /accounts/v2/users/{user_id}	[GET] /platform/rbac/v1/users/{user_id}
[PATCH] /accounts/v2/users/{user_id}	[PATCH] /platform/rbac/v1/users/{user_id}
[POST] /accounts/v1/bulk_users	[POST] /platform/rbac/v1/bulk_users
[PATCH] /accounts/v1/bulk_users	[PATCH] /platform/rbac/v1/bulk_users
[GET] /accounts/v1/status/{cookie_name}	[GET] /platform/rbac/v1/status/{cookie_name}

**Table 25: Deprecated APIs in HPE Aruba Networking Central 2.5.0 release**

Deprecated API	Alternative API
[GET] /accounts/v1/roles	[GET] /platform/rbac/v1/roles
[POST] /accounts/v1/roles	[POST] /platform/rbac/v1/apps/{app_name}/roles
[GET] /accounts/v1/roles/{rolename}	[GET] /platform/rbac/v1/apps/{app_name}/roles/{rolename}
[DELETE] /accounts/v1/roles/{rolename}	[DELETE] /platform/rbac/v1/apps/{app_name}/roles/{rolename}
[PATCH] /accounts/v1/roles/{rolename}	[PATCH] /platform/rbac/v1/apps/{app_name}/roles/{rolename}
[GET] /accounts/v3/users	[GET] /platform/rbac/v1/users
[GET] /accounts/v1/users	[GET] /platform/rbac/v1/users
[POST] /accounts/v1/users	[GET] /platform/rbac/v1/users
[GET] /accounts/v1/users/{user_id}	[GET] /platform/rbac/v1/users/{user_id}
[PATCH] /accounts/v1/users/{user_id}	[PATCH] /platform/rbac/v1/users/{user_id}

## Removed APIs

The following table lists the APIs that have been removed and the alternative APIs:  
**APIs removed as part of HPE Aruba Networking Central 2.5.8 release:**

**Table 26: Removed and Alternative APIs in HPE Aruba Networking Central 2.5.8 release**

Removed API	Alternative API
<b>Monitoring &gt; VPN</b>	
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/vpn/usage</li> <li>▪ [GET] /monitoring/v2/vpn/usage</li> </ul>	<ul style="list-style-type: none"> <li>▪ [POST] /monitoring/v3/vpn/usage</li> </ul>
<b>Monitoring &gt; AP</b>	
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/aps</li> </ul>	<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v2/aps</li> </ul>
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v2/aps/{serial}/rf_summary</li> </ul>	<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v3/aps/{serial}/rf_summary</li> </ul>
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/aps/bandwidth_usage</li> <li>▪ [GET] /monitoring/v2/aps/bandwidth_usage</li> </ul>	<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v3/aps/bandwidth_usage</li> </ul>
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/aps/{serial}/neighbouring_clients</li> </ul>	No alternate API

Removed API	Alternative API
▪ [GET] /monitoring/v1/bssids	▪ [GET] /monitoring/v2/bssids
▪ [GET] /monitoring/v1/aps/bandwidth_usage/topn	▪ [GET] /monitoring/v2/aps/bandwidth_usage/topn
<b>Monitoring &gt; Network</b>	
▪ [GET] /monitoring/v1/networks	▪ [GET] /monitoring/v2/networks
▪ [GET] /monitoring/v1/networks/{network_name}	▪ [GET] /monitoring/v2/networks/{network_name}
▪ [GET] /monitoring/v1/networks/bandwidth_usage	▪ [GET] /monitoring/v2/networks/bandwidth_usage
<b>UnitedCommunications</b>	
▪ [GET] /v1/summery	No alternate API
▪ [GET] /v1/client/count	No alternate API
▪ [GET] /v1/session/trend	No alternate API
▪ [GET] /v1/session/count/alg	No alternate API
▪ [GET] /v1/session/quality/type	No alternate API
▪ [GET] /v1/session/quality/ssid	No alternate API
▪ [GET] /v1/insights/count	No alternate API
▪ [GET] /v1/insights	No alternate API
▪ [GET] /v1/cdr/list	No alternate API
▪ [GET] /v1/cdr/export	No alternate API
▪ [GET] /v1/SkypeCentralURL	No alternate API

## APIs removed as part of HPE Aruba Networking Central 2.5.7 release:

**Table 27:** *Removed and Alternative APIs in HPE Aruba Networking Central 2.5.7 release*

Removed API	Alternative API
<b>Rapids &gt; SSIDs</b>	
The list of APIs in Rapids > SSIDs are removed. You can now configure RAPIDS from the RAPIDS configuration page. For more information, see Configuring RAPIDS section in <i>User Guide for HPE Aruba Networking Central and AOS 10</i> .	
▪ [GET] /rapids/v1/ssid_allow	-
▪ [POST] /rapids/v1/ssid_allow	-

Removed API	Alternative API
<ul style="list-style-type: none"> <li>▪ [DELETE] /rapids/v1/ssid_allow</li> <li>▪ [GET] /rapids/v1/ssid_block</li> <li>▪ [POST] /rapids/v1/ssid_block</li> <li>▪ [DELETE] /rapids/v1/ssid_block</li> </ul>	

### APIs removed as part of HPE Aruba Networking Central 2.5.6 release:

**Table 28:** Removed and Alternative APIs in HPE Aruba Networking Central 2.5.6 release

Removed API	Alternative API
<b>Service Cloud Security</b>	
<ul style="list-style-type: none"> <li>▪ [GET] /cloud-security-config/v1/node_list/</li> </ul>	No alternate API
<ul style="list-style-type: none"> <li>▪ [GET] /cloud-security-config/v1/node_list/{node_type}/{node_id}/config/</li> </ul>	No alternate API
<ul style="list-style-type: none"> <li>▪ [GET] /cloud-security-config/v1/node_list/{node_type}/{node_id}/config/zscaler/</li> </ul>	No alternate API

### APIs removed as part of HPE Aruba Networking Central 2.5.5 release:

No APIs removed in HPE Aruba Networking Central 2.5.5 release.

### APIs removed as part of HPE Aruba Networking Central 2.5.4 release:

**Table 29:** Removed and Alternative APIs in HPE Aruba Networking Central 2.5.4 release

Removed API	Alternative API
<b>Configuration &gt; Groups</b>	
<ul style="list-style-type: none"> <li>▪ [PATCH] /configuration/v1/groups/{group}</li> </ul>	No alternate API
<ul style="list-style-type: none"> <li>▪ [PATCH] /configuration/v1/groups/{group}/properties</li> </ul>	No alternate API

### APIs removed as part of HPE Aruba Networking Central 2.5.3 release:

**Table 30:** Removed and Alternative APIs in HPE Aruba Networking Central 2.5.3 release

Removed API	Alternative API
<b>WIDS</b>	
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/wids/rogue_aps</li> <li>▪ [GET] /monitoring/v1/wids/interfering_aps</li> </ul>	<ul style="list-style-type: none"> <li>▪ [GET] /rapids/v1/rogue_aps</li> <li>▪ [GET] /rapids/v1/interfering_aps</li> </ul>



**Table 30: Removed and Alternative APIs in HPE Aruba Networking Central 2.5.3 release**

Removed API	Alternative API
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/wids/infrastructure_attacks</li> </ul>	<ul style="list-style-type: none"> <li>▪ [GET] /rapids/v1/wids/infrastructure_attacks</li> </ul>
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/wids/client_attacks</li> </ul>	<ul style="list-style-type: none"> <li>▪ [GET] /rapids/v1/wids/client_attacks</li> </ul>
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/wids/events</li> </ul>	<ul style="list-style-type: none"> <li>▪ [GET] /rapids/v1/wids/events</li> </ul>
<h3>Configuration</h3>	
<ul style="list-style-type: none"> <li>▪ [PUT] /configuration/v1/msp/templates—This API updates the MSP customer level template to all template groups for the end customers.</li> <li>▪ [PUT] /configuration/v1/msp/templates/customer/{cid}—This API updates the end customer-level template and applies the template to all template groups.</li> </ul> <p><b>NOTE:</b> To achieve the functionality of [PUT] /configuration/v1/msp/templates API, it is recommended that you use the combination of 1, 3, and 4 numbered APIs from the alternate API column.</p> <p><b>NOTE:</b> To achieve the functionality of [PUT] /configuration/v1/msp/templates/customer/{cid} API, it is recommended that you use the combination of 2 and 4 numbered APIs from the alternate API column.</p>	<ol style="list-style-type: none"> <li>1. [PUT] /configuration/v2/msp/templates—This API is used to update the template at MSP level.</li> <li>2. [PUT] /configuration/v2/msp/templates/customer/{cid}—This API is used to update the template at end customer level.</li> <li>3. [POST] /configuration/v2/msp/templates/end_customers/{device_type}/{version}/{model}—This API is used to apply the MSP level template to end customers.</li> <li>4. [POST] /configuration/v2/msp/templates/end_customers/{cid}/{device_type}/{version}/{model}/group—This API is used to apply end customer-level templates to the end customer's template groups.</li> </ol>
<h3>Attributes</h3>	
<ul style="list-style-type: none"> <li>▪ [GET] /monitoring/v1/attribute_values</li> </ul>	No alternate API
<h3>Presence Analytics</h3>	
<ul style="list-style-type: none"> <li>▪ [POST] /presence/v1/config/thresholds</li> </ul>	No alternate API
<ul style="list-style-type: none"> <li>▪ [GET] /presence/v1/config/thresholds</li> </ul>	No alternate API
<ul style="list-style-type: none"> <li>▪ [GET] /presence/v1/analytics/aggregates</li> </ul>	No alternate API
<ul style="list-style-type: none"> <li>▪ [GET] /presence/v1/analytics/trends</li> </ul>	No alternate API

**Table 30: Removed and Alternative APIs in HPE Aruba Networking Central 2.5.3 release**

Removed API	Alternative API
▪ [GET] /presence/v1/insights/top_sites	No alternate API
▪ [GET] /presence/v1/insights/bottom_sites	No alternate API
▪ [GET] /presence/v1/insights/sites/aggregates	No alternate API

**APIs removed as part of HPE Aruba Networking Central 2.5.2 release:**

No APIs removed in HPE Aruba Networking Central 2.5.2 release.

**APIs removed as part of HPE Aruba Networking Central 2.5.1 release:****Table 31: Removed and Alternative APIs in HPE Aruba Networking Central 2.5.1 release**

Removed API	Alternative API
<b>Device Management</b>	
▪ [GET] /configuration/v1/devices/{device_serial}/mobility_master/	▪ [GET] /device_management/v1/mobility_master/{device_serial}
[POST] /configuration/v1/devices/{device_serial}/mobility_master/{mm_name}	▪ [POST] /device_management/v1/mobility_master/{device_serial}/{mm_name}
<b>ACP MSP</b>	
▪ [GET] /platform/msp_api/v1/customers/{customer_id}	No alternate API
▪ [PUT] /platform/msp_api/v1/customers/{customer_id}	No alternate API
▪ [DELETE] /platform/msp_api/v1/customers/{customer_id}	No alternate API
▪ [GET] /platform/msp_api/v1/customers	No alternate API
▪ [POST] /platform/msp_api/v1/customers	No alternate API
<b>Clarity</b>	
▪ [GET] /clarity/v1/overview/healthscore	No alternate API
▪ [GET] /clarity/v1/overview/healthscore/dns	No alternate API
▪ [GET] /clarity/v1/overview/network_	No alternate API

**Table 31: Removed and Alternative APIs in HPE Aruba Networking Central 2.5.1 release**

Removed API	Alternative API
stats	
▪ [GET] /clarity/v1/overview/reasons	No alternate API
▪ [GET] /clarity/v1/overview/attempts	No alternate API
▪ [GET] /clarity/v1/overview/device_attempts	No alternate API
▪ [GET] /clarity/v1/trend/healthscore	No alternate API
▪ [GET] /clarity/v1/trend/healthscore/dns	No alternate API
▪ [GET] /clarity/v1/trend/network_stats	No alternate API
▪ [GET] /clarity/v1/clients/search/partial	No alternate API
▪ [GET] /clarity/v1/clients/search/absolute	No alternate API
▪ [GET] /clarity/v1/clients/details	No alternate API
▪ [GET] /clarity/v1/clients/stats	No alternate API
▪ [GET] /clarity/v1/insights	No alternate API
▪ [GET] /clarity/v1/insights/details	No alternate API
▪ [GET] /clarity/v1/insights/distribution	No alternate API
▪ [GET] /clarity/v1/license	No alternate API

### APIs removed as part of HPE Aruba Networking Central 2.5.0 release:

**Table 32: Removed and Alternative APIs in HPE Aruba Networking Central 2.5.0 release**

Removed API	Alternative API
<b>User Management</b>	
▪ [DELETE] /accounts/v1/users/{user_id}	▪ [DELETE] /platform/rbac/v1/users/{user_id}
▪ [DELETE] /accounts/v1/bulk_users	▪ [DELETE] /platform/rbac/v1/bulk_users

## APIs Introduced In Previous Releases

The section list the APIs introduced in the previous releases of HPE Aruba Networking Central.

### HPE Aruba Networking Central 2.5.7

**Table 33: New APIs in HPE Aruba Networking Central 2.5.7 release**

API
<b>Authentication &amp; Policy &gt; Client Policy</b>
<ul style="list-style-type: none"><li>▪ [PUT] /cloudAuth/api/v3/client_policy/reset</li></ul>
<b>Authentication &amp; Policy &gt; User Policy</b>
<ul style="list-style-type: none"><li>▪ [PUT] /cloudAuth/api/v3/user_policy/reset</li></ul>
<b>Authentication &amp; Policy &gt; Download</b>
<ul style="list-style-type: none"><li>▪ [GET] /cloudAuth/api/v2/download/mpsk</li><li>▪ [GET] /cloudauth/api/v3/bulk/mac</li></ul>
<b>Authentication &amp; Policy &gt; MPSK Networks Configs</b>
<ul style="list-style-type: none"><li>▪ [GET] /cloudAuth/api/v2/mpsk</li><li>▪ [GET] /cloudAuth/api/v2/mpsk/{mpsk_id}</li><li>▪ [GET] /cloudAuth/api/v2/mpsk/{mpsk_id}/namedMPSK</li><li>▪ [GET] /cloudAuth/api/v2/mpsk/{mpsk_id}/namedMPSK/{named_mpsk_id}</li><li>▪ [GET] /cloudAuth/api/v2/usage/mpsk</li></ul>
<ul style="list-style-type: none"><li>▪ [PATCH] /cloudAuth/api/v2/mpsk/{mpsk_id}/namedMPSK/{named_mpsk_id}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /cloudAuth/api/v2/mpsk</li><li>▪ [POST] /cloudAuth/api/v2/mpsk/{mpsk_id}/namedMPSK /v2/mpsk</li></ul>
<ul style="list-style-type: none"><li>▪ [PUT] /cloudAuth/api/v2/mpsk/{mpsk_id}</li><li>▪ [PUT] /cloudAuth/api/v2/mpsk/{mpsk_id}/namedMPSK/{named_mpsk_id}</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /cloudauth/api/v2/mpsk/{mpsk_id}</li><li>▪ [DELETE] /cloudAuth/api/v2/mpsk/{mpsk_id}/namedMPSK/{named_mpsk_id}</li></ul>
<b>Authentication &amp; Policy &gt; File Upload</b>
<ul style="list-style-type: none"><li>▪ [GET] /cloudauth/api/v3/bulk/{upload_type}/error</li><li>▪ [GET] /cloudauth/api/v3/bulk/{upload_type}/status</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /cloudauth/api/v3/bulk/{upload_type}</li></ul>
<ul style="list-style-type: none"><li>▪ [PUT] /cloudauth/api/v3/bulk/{upload_type}/terminate</li></ul>
<b>Authentication &amp; Policy &gt; MAC Registration</b>
<ul style="list-style-type: none"><li>▪ [GET] /cloudauth/api/v3/client/mac/registration</li></ul>
<ul style="list-style-type: none"><li>▪ [PATCH] /cloudauth/api/v3/client/mac/registration/{mac_address}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /cloudauth/api/v3/client/mac/registration</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /cloudauth/api/v3/client/mac/registration/{mac_address}</li></ul>

**Table 33: New APIs in HPE Aruba Networking Central 2.5.7 release**

API
<b>Authentication &amp; Policy &gt; User Management</b>
<ul style="list-style-type: none"><li>▪ [GET] /cloudauth/api/v3/user/certificate</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /cloudauth/api/v3/user/certificate/revocation</li></ul>
<b>Cloud Connect</b>
<ul style="list-style-type: none"><li>▪ [GET] /cloud-connect/topology-scan</li><li>▪ [GET] /cloud-connect/topology-eps</li><li>▪ [GET] /cloud-connect/zscaler/node-scan</li><li>▪ [GET] /cloud-connect/vlan-cfg</li><li>▪ [GET] /cloud-connect/config-summary</li><li>▪ [GET] /cloud-connect/v1/tunnel-policy-config-metadata</li><li>▪ [GET] /cloud-connect/v1/tunnel-policy-config/{policy_name}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /cloud-connect/v1/node_list/{node_id}/config/custom</li><li>▪ [POST] /cloud-connect/v1/node_list/{node_id}/config/zscaler</li><li>▪ [POST] /cloud-connect/v1/node_list/{node_id}/config/aws</li><li>▪ [POST] /cloud-connect/v1/node_list/{node_id}/config/azure</li><li>▪ [POST] /cloud-connect/v1/tunnel-policy-config/{policy_name}</li></ul>
<ul style="list-style-type: none"><li>▪ [PUT] /cloud-connect/v1/node_list/{node_id}/config/custom</li><li>▪ [PUT] /cloud-connect/v1/node_list/{node_id}/config/zscaler</li><li>▪ [PUT] /cloud-connect/v1/node_list/{node_id}/config/aws</li><li>▪ [PUT] /cloud-connect/v1/node_list/{node_id}/config/azure</li><li>▪ [PUT] /cloud-connect/v1/tunnel-policy-config/{policy_name}</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /cloud-connect/v1/node_list/{node_id}/config/custom</li><li>▪ [DELETE] /cloud-connect/v1/node_list/{node_id}/config/zscaler</li><li>▪ [DELETE] /cloud-connect/v1/node_list/{node_id}/config/aws</li><li>▪ [DELETE] /cloud-connect/v1/node_list/{node_id}/config/azure</li><li>▪ [DELETE] /cloud-connect/v1/tunnel-policy-config/{policy_name}</li></ul>
<b>Install Manager &gt; Sites</b>
<ul style="list-style-type: none"><li>▪ [POST] /v1/update_site_status</li></ul>
<b>Service RAPIDS &gt; Aruba Rapids</b>
<ul style="list-style-type: none"><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rule/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rule/{rule_name}/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rule/{rule_name}/match_criteria/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_excludes/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_excludes/{name}/</li></ul>

**Table 33: New APIs in HPE Aruba Networking Central 2.5.7 release**

API
<ul style="list-style-type: none"><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_includes/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_includes/{name}/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_excludes/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_excludes/{essid}/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_includes/</li><li>▪ [GET] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_includes/{essid}/</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /rapids-config/v1/node_list/{node_type}/{node_id}/config/</li><li>▪ [POST] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rule/{rule_name}/</li><li>▪ [POST] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rule/{rule_name}/match_criteria/</li><li>▪ [POST] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_excludes/{name}/</li><li>▪ [POST] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_includes/{name}/</li><li>▪ [POST] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_excludes/{essid}/</li><li>▪ [POST] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_includes/{essid}/</li></ul>
<ul style="list-style-type: none"><li>▪ [PUT] /rapids-config/v1/node_list/{node_type}/{node_id}/config/</li><li>▪ [PUT] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rule/{rule_name}/</li><li>▪ [PUT] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rule/{rule_name}/match_criteria/</li><li>▪ [PUT] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_excludes/{name}/</li><li>▪ [PUT] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_includes/{name}/</li><li>▪ [PUT] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_excludes/{essid}/</li><li>▪ [PUT] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_includes/{essid}/</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /rapids-config/v1/node_list/{node_type}/{node_id}/config/</li><li>▪ [DELETE] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rule/{rule_name}/</li><li>▪ [DELETE] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rule/{rule_name}/match_criteria/</li><li>▪ [DELETE] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_excludes/{name}/</li></ul>

**Table 33:** *New APIs in HPE Aruba Networking Central 2.5.7 release*

API
<ul style="list-style-type: none"><li>▪ [DELETE] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/site_includes/{name}/</li><li>▪ [DELETE] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_excludes/{ssid}/</li><li>▪ [DELETE] /rapids-config/v1/node_list/{node_type}/{node_id}/config/classification_rules/{rule_name}/match_criteria/ssid_includes/{ssid}/</li></ul>
<b>VisualRF &gt; GeoFence</b>
<ul style="list-style-type: none"><li>▪ [GET] /visualrf_api/v1/geofence</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /visualrf_api/v1/geofence</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /visualrf_api/v1/geofence</li></ul>

## HPE Aruba Networking Central 2.5.6

**Table 34:** *New APIs in HPE Aruba Networking Central 2.5.6 release*

API
<b>Authentication &amp; Policy &gt; Authentication and Sessions</b>
<ul style="list-style-type: none"><li>▪ [GET] /auth/air_pass/list</li><li>▪ [GET] /auth/cloud_identity/list</li><li>▪ [GET] /auth/{request_id}</li><li>▪ [GET] /session/air_pass/list</li><li>▪ [GET] /session/cloud_identity/list</li></ul>
<b>Authentication &amp; Policy &gt; Wi-Fi Easy Connect</b>
<ul style="list-style-type: none"><li>▪ [GET] /dpp_registration</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /dpp_registration</li><li>▪ [POST] /dpp_registration/{id}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /dpp_registration/{id}</li></ul>
<b>Ble Beacon Service</b>
<ul style="list-style-type: none"><li>▪ [GET] /ble_cfg_beacons/{profile_id}</li><li>▪ [GET] /ble_run_beacons/{profile_id}</li><li>▪ [GET] /ble_beacon_profiles</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /ble_beacon/{iot_radio_mac}/{profile_id}</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /ble_beacon/{iot_radio_mac}/{profile_id}</li></ul>
<b>Client Match</b>

**Table 34: New APIs in HPE Aruba Networking Central 2.5.6 release**

API
<ul style="list-style-type: none"><li>▪ [GET] /bandsteer-6ghz-enable/v1/{tenant_id}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /bandsteer-6ghz-enable/v1/{tenant_id}</li></ul>
<b>Configuration &gt; Certificates</b>
<ul style="list-style-type: none"><li>▪ [PUT] /configuration/v1/non_msp/certificate</li></ul>
<b>Configuration &gt; AOS-S</b>
<ul style="list-style-type: none"><li>▪ [GET] /configuration/v1/aos_switch/system/groups/{group_name}</li><li>▪ [GET] /configuration/v1/aos_switch/system/devices/{device_serial}</li><li>▪ [GET] /configuration/v1/aos_switch/system_time/groups/{group_name}</li><li>▪ [GET] /configuration/v1/aos_switch/system_time/devices/{device_serial}</li></ul>
<ul style="list-style-type: none"><li>▪ [PUT] /configuration/v1/aos_switch/system/groups/{group_name}</li><li>▪ [PUT] /configuration/v1/aos_switch/system/devices/{device_serial}</li><li>▪ [PUT] /configuration/v1/aos_switch/system_time/groups/{group_name}</li><li>▪ [PUT] /configuration/v1/aos_switch/system_time/devices/{device_serial}</li></ul>
<b>Configuration &gt; AP Configuration</b>
<ul style="list-style-type: none"><li>▪ [GET] /configuration/v1/group/ssh_credential/{group_name}</li><li>▪ [GET] /configuration/v1/device/ssh_credential/{serial_number_or_guid}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /configuration/v1/group/ssh_credential/{group_name}</li><li>▪ [POST] /configuration/v1/device/ssh_credential/{serial_number_or_guid}</li></ul>
<b>Configuration &gt; CX Configuration</b>
<ul style="list-style-type: none"><li>▪ [GET] /configuration/v1/switch/cx/port-access-auth</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /configuration/v1/switch/cx/port-access-auth</li></ul>
<b>MSP &gt; Customers</b>
<ul style="list-style-type: none"><li>▪ [POST] /msp_api/v2/customers</li></ul>
<ul style="list-style-type: none"><li>▪ [PUT] /msp_api/v2/customers/{customer_id}</li></ul>
<b>MSP &gt; Get Country code</b>
<ul style="list-style-type: none"><li>▪ [GET] /msp_api/v2/get_country_code</li></ul>
<b>MSP &gt; Devices</b>
<ul style="list-style-type: none"><li>▪ [PUT] /msp_api/v2/{customer_id}/devices</li></ul>
<b>Service Airgroup</b>
<ul style="list-style-type: none"><li>▪ [GET] /airgroup-config/v2/custom_services/{name}/service_ids/{service_id}/</li></ul>



**Table 34: New APIs in HPE Aruba Networking Central 2.5.6 release**

API
<ul style="list-style-type: none"> <li>▪ [GET] /airgroup-config/v2/custom_services/{name}/service_ids/</li> <li>▪ [GET] /airgroup-config/v2/custom_services/{name}/</li> <li>▪ [GET] /airgroup-config/v2/custom_services/</li> </ul>
<ul style="list-style-type: none"> <li>▪ [POST] /airgroup-config/v2/custom_services/{name}/service_ids/{service_id}/</li> <li>▪ [POST] /airgroup-config/v2/custom_services/{name}/</li> </ul>
<ul style="list-style-type: none"> <li>▪ [PUT] /airgroup-config/v2/custom_services/{name}/service_ids/{service_id}/</li> <li>▪ [PUT] /airgroup-config/v2/custom_services/{name}/</li> </ul>
<ul style="list-style-type: none"> <li>▪ [DELETE] /airgroup-config/v2/custom_services/{name}/service_ids/{service_id}/</li> <li>▪ [DELETE] /airgroup-config/v2/custom_services/{name}/</li> </ul>
<b>Troubleshooting</b>
<ul style="list-style-type: none"> <li>▪ [GET] /troubleshooting/v1/cxcommands</li> </ul>
<ul style="list-style-type: none"> <li>▪ [POST] /troubleshooting/v1/cxdevices/{serial}</li> </ul>
<b>VisualRF &gt; Import</b>
<ul style="list-style-type: none"> <li>▪ [GET] /visualrf_api/v1/restore_sites/status</li> </ul>
<ul style="list-style-type: none"> <li>▪ [POST] /visualrf_api/v1/restore_sites</li> </ul>
<b>VisualRF &gt; Anonymization</b>
<ul style="list-style-type: none"> <li>▪ [GET] /visualrf_api/v1/anonymization</li> </ul>
<ul style="list-style-type: none"> <li>▪ [POST] /visualrf_api/v1/anonymization</li> </ul>
<ul style="list-style-type: none"> <li>▪ [DELETE] /visualrf_api/v1/anonymization</li> </ul>

## HPE Aruba Networking Central 2.5.5

**Table 35: New APIs in HPE Aruba Networking Central 2.5.5 release**

API
<b>Configuration &gt; AOS-S</b>
<ul style="list-style-type: none"> <li>▪ [GET] /configuration/v1/aos_switch/ports/groups/{group_name}</li> <li>▪ [GET] /configuration/v1/aos_switch/ports/devices/{device_serial}</li> <li>▪ [GET] /configuration/v1/aos_switch/vlans/groups/{group_name}</li> <li>▪ [GET] /configuration/v1/aos_switch/vlans/devices/{device_serial}</li> </ul>
<ul style="list-style-type: none"> <li>▪ [PUT] /configuration/v1/aos_switch/ports/groups/{group_name}</li> <li>▪ [PUT] /configuration/v1/aos_switch/ports/devices/{device_serial}</li> <li>▪ [PUT] /configuration/v1/aos_switch/vlans/groups/{group_name}</li> <li>▪ [PUT] /configuration/v1/aos_switch/vlans/devices/{device_serial}</li> </ul>

**Table 35: New APIs in HPE Aruba Networking Central 2.5.5 release**

API
<b>Configuration &gt; Pre Provisioned Group</b>
<ul style="list-style-type: none"><li>[POST] /configuration/v1/preassign</li></ul>

## HPE Aruba Networking Central 2.5.4

**Table 36: New APIs in HPE Aruba Networking Central 2.5.4 release**

API
<b>AI OPs &gt; AI Insights Details</b>
<ul style="list-style-type: none"><li>[GET] /aiops/v2/insights/global/id/{insight_id}/export</li><li>[GET] /aiops/v2/insights/site/{site_id}/id/{insight_id}/export</li><li>[GET] /aiops/v2/insights/ap/{ap_serial}/id/{insight_id}/export</li><li>[GET] /aiops/v2/insights/client/{sta_mac}/id/{insight_id}/export</li><li>[GET] /aiops/v2/insights/gateway/{gw_serial}/id/{insight_id}/export</li><li>[GET] /aiops/v2/insights/switch/{sw_serial}/id/{insight_id}/export</li></ul>
<b>AI OPs &gt; AI Insights List</b>
<ul style="list-style-type: none"><li>[GET] /aiops/v2/insights/global/list</li><li>[GET] /aiops/v2/insights/site/{site_id}/list</li><li>[GET] /aiops/v2/insights/ap/{ap_serial}/list</li><li>[GET] /aiops/v2/insights/client/{sta_mac}/list</li><li>[GET] /aiops/v2/insights/gateway/{gw_serial}/list</li><li>[GET] /aiops/v2/insights/switch/{sw_serial}/list</li></ul>
<b>AI OPs &gt; Wi-Fi Connectivity at Global</b>
<ul style="list-style-type: none"><li>[GET] /aiops/v1/connectivity/global/stage/{stage}/export</li><li>[GET] /aiops/v1/connectivity/site/{site_id}/stage/{stage}/export</li><li>[GET] /aiops/v1/connectivity/group/{group}/stage/{stage}/export</li></ul>
<b>Authentication &amp; Policy &gt; Client Policy</b>
<ul style="list-style-type: none"><li>[GET] /client_policy</li><li>[PUT] /client_policy</li><li>[DELETE] /client_policy</li></ul>
<b>Authentication &amp; Policy &gt; Client Registration</b>
<ul style="list-style-type: none"><li>[GET] /client_registration</li><li>[POST] /client_registration</li><li>[PATCH] /client_registration/{mac_address}</li></ul>

**Table 36:** *New APIs in HPE Aruba Networking Central 2.5.4 release*

API
<ul style="list-style-type: none"><li>▪ [DELETE] /client_registration/{mac_address}</li></ul>
<b>Authentication &amp; Policy &gt; User policy</b>
<ul style="list-style-type: none"><li>▪ [GET] /user_policy</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /user_policy</li></ul>
<ul style="list-style-type: none"><li>▪ [PUT] /user_policy</li></ul>
<b>Client Match &gt; Status</b>
<ul style="list-style-type: none"><li>▪ [GET] /loadbal-enable/v1/{tenant_id}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /loadbal-enable/v1/{tenant_id}</li></ul>
<b>Configuration &gt; Groups</b>
<ul style="list-style-type: none"><li>▪ [POST] /configuration/v3/groups</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /configuration/v2/groups/{group}/properties</li></ul>
<b>Configuration &gt; WLAN Configuration</b>
<ul style="list-style-type: none"><li>▪ [GET] /configuration/full_hotspot/{group_name_or_guid}</li><li>▪ [GET] /configuration/full_hotspot/{group_name_or_guid}/{mode_name}</li><li>▪ [GET] /configuration/full_hotspot/{group_name_or_guid}/template</li><li>▪ [GET] /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name}</li></ul>
<ul style="list-style-type: none"><li>▪ [PUT] /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name}</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /configuration/full_hotspot/{group_name_or_guid}/{hotspot_name}/{mode_name}</li></ul>
<b>Guest &gt; Summary</b>
<ul style="list-style-type: none"><li>▪ [GET] /guest/v1/summary</li></ul>
<b>Monitoring &gt; Clients</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v2/clients</li><li>▪ [GET] /monitoring/v2/clients/{macaddr}</li></ul>
<b>MSP &gt; Groups</b>

**Table 36:** *New APIs in HPE Aruba Networking Central 2.5.4 release*

API
<ul style="list-style-type: none"><li>[GET] /msp_api/v1/groups/{group_name}/customers</li></ul>
<b>Service IPMS &gt; Aruba ipms</b>
<ul style="list-style-type: none"><li>[GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/</li><li>[GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/</li><li>[GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/</li><li>[GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/</li><li>[GET] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/</li><li>[GET] /ipms-config/v1/node_list/{node_type}/{node_id}/</li></ul>
<ul style="list-style-type: none"><li>[POST] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/</li><li>[POST] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/</li></ul>
<ul style="list-style-type: none"><li>[PUT] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/</li><li>[PUT] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/</li></ul>
<ul style="list-style-type: none"><li>[DELETE] /ipms-config/v1/node_list/{node_type}/{node_id}/config/</li><li>[DELETE] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/</li><li>[DELETE] /ipms-config/v1/node_list/{node_type}/{node_id}/config/address_pool/{pool_name}/ip_range/{range_id}/</li></ul>
<b>Troubleshooting</b>
<ul style="list-style-type: none"><li>[GET] /troubleshooting/v1/running-config-backup/serial/{serial}</li><li>[GET] /troubleshooting/v1/running-config-backup/serial/{serial}/prefix/{prefix}</li><li>[GET] /troubleshooting/v1/running-config-backup/name/{name}</li></ul>
<ul style="list-style-type: none"><li>[POST] /troubleshooting/v1/running-config-backup/serial/{serial}/prefix/{prefix}</li><li>[POST] /troubleshooting/v1/running-config-backup/group_name/{group_name}/prefix/{prefix}</li></ul>

## HPE Aruba Networking Central 2.5.3

**Table 37:** *New APIs in HPE Aruba Networking Central 2.5.3 release*

API
<b>Configuration &gt; Groups</b>
<ul style="list-style-type: none"><li>[GET] /configuration/v1/groups/properties</li></ul>

**Table 37: New APIs in HPE Aruba Networking Central 2.5.3 release**

API
<ul style="list-style-type: none"><li>▪ [PATCH] /configuration/v1/groups/{group}/properties</li></ul>
<b>New Licensing</b>
<ul style="list-style-type: none"><li>▪ [GET] /platform/licensing/v1/subscriptions</li><li>▪ [GET] /platform/licensing/v1/subscriptions/stats</li><li>▪ [GET] /platform/licensing/v1/services/enabled</li><li>▪ [GET] /platform/licensing/v1/services/config</li><li>▪ [GET] /platform/licensing/v1/autolicensing/services/{service}/status</li><li>▪ [GET] /platform/licensing/v1/customer/settings/autolicense</li><li>▪ [GET] /platform/licensing/v1/msp/customer/settings/autolicense</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /platform/licensing/v1/subscriptions/assign</li><li>▪ [POST] /platform/licensing/v1/subscriptions/unassign</li><li>▪ [POST] /platform/licensing/v1/subscriptions/devices/all</li><li>▪ [POST] /platform/licensing/v1/msp/subscriptions/devices/all</li><li>▪ [POST] /platform/licensing/v1/customer/settings/autolicense</li><li>▪ [POST] /platform/licensing/v1/msp/customer/settings/autolicense</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /platform/licensing/v1/subscriptions/devices/all</li><li>▪ [DELETE] /platform/licensing/v1/msp/subscriptions/devices/all</li><li>▪ [DELETE] /platform/licensing/v1/customer/settings/autolicense</li><li>▪ [DELETE] /platform/licensing/v1/msp/customer/settings/autolicense</li></ul>
<b>Monitoring &gt; AP</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v2/bssids</li><li>▪ [GET] /monitoring/v3/aps/bandwidth_usage</li><li>▪ [GET] /monitoring/v2/aps/bandwidth_usage/topn</li><li>▪ [GET] /monitoring/v2/aps</li></ul>
<b>Monitoring &gt; Label</b>
<ul style="list-style-type: none"><li>▪ [POST] /central/v2/labels/associations</li><li>▪ [POST] /central/v1/labels</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /central/v2/labels/associations</li></ul>
<b>Monitoring &gt; Network</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v2/networks</li><li>▪ [GET] /monitoring/v2/networks/{network_name}</li><li>▪ [GET] /monitoring/v2/networks/bandwidth_usage</li></ul>
<b>Monitoring &gt; Site</b>
<ul style="list-style-type: none"><li>▪ [POST] /central/v2/sites/associations</li><li>▪ [POST] /central/v2/sites</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /central/v2/sites/associations</li></ul>

**Table 37: New APIs in HPE Aruba Networking Central 2.5.3 release**

API
<b>Topology</b>
<ul style="list-style-type: none"><li>▪ [GET] /vlans/{site_id}</li><li>▪ [GET] /unreachableDevices/{site_id}</li></ul>

## HPE Aruba Networking Central 2.5.2

**Table 38: New APIs in HPE Aruba Networking Central 2.5.2 release**

API
<b>Dynamic Path Steering</b>
<ul style="list-style-type: none"><li>▪ [GET] /dps_site_monitoring/datapoints/v1/sdwan_site/site_policy_stats/{site_name}</li></ul>
<b>Configuration &gt; AP Configuration</b>
<ul style="list-style-type: none"><li>▪ [GET] /configuration/v1/ap_cli/{group_name_or_guid}</li><li>▪ [GET] /configuration/v1/ap_settings_cli/{serial_number}</li><li>▪ [GET] /configuration/v1/iap_variables/{group_name_or_guid}</li><li>▪ [GET] /configuration/v1/dirty_diff/{group_name_or_guid}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /configuration/v1/ap_cli/{group_name_or_guid}</li><li>▪ [POST] /configuration/v1/ap_settings_cli/{serial_number}</li><li>▪ [POST] /configuration/v1/iap_variables/{group_name_or_guid}</li></ul>
<b>Configuration &gt; Groups</b>
<ul style="list-style-type: none"><li>▪ [POST] /configuration/v2/groups/clone</li></ul>
<b>Monitoring &gt; AP</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v3/aps/{serial}/rf_summary</li><li>▪ [GET] /monitoring/v2/aps/bandwidth_usage</li></ul>
<b>Monitoring &gt; Switch</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/cx_switches/{serial}/poe_detail</li><li>▪ [GET] /monitoring/v1/cx_switches/{serial}/vlan</li><li>▪ [GET] /monitoring/v1/cx_switch_stacks/{stack_id}/vlan</li><li>▪ [GET] /monitoring/v1/cx_switches/{serial}/ports/errors</li><li>▪ [GET] /monitoring/v1/cx_switches/{serial}/ports/bandwidth_usage</li><li>▪ [GET] /monitoring/v1/cx_switches/{serial}/ports</li><li>▪ [GET] /monitoring/v1/cx_switch_stacks/{stack_id}/ports</li><li>▪ [GET] /monitoring/v1/cx_switches/{serial}/vsx</li></ul>
<b>Presence Analytics</b>
<ul style="list-style-type: none"><li>▪ [GET] /presence/v3/config/thresholds</li><li>▪ [GET] /presence/v3/sites/config</li><li>▪ [GET] /presence/v3/visitor_status</li></ul>

**Table 38:** *New APIs in HPE Aruba Networking Central 2.5.2 release*

API
<ul style="list-style-type: none"><li>▪ [GET] /presence/v3/visit_frequency</li><li>▪ [GET] /presence/v3/analytics/trends/loyal_visitors</li><li>▪ [GET] /presence/v3/analytics/trends/passersby_visitors</li><li>▪ [GET] /presence/v3/sites/devicelicense</li><li>▪ [GET] /presence/v3/insights/sites/aggregates</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /presence/v3/config/thresholds</li><li>▪ [POST] /presence/v3/license</li></ul>

## HPE Aruba Networking Central 2.5.1

No new APIs introduced in HPE Aruba Networking Central 2.5.1 release.

## HPE Aruba Networking Central 2.5.0

**Table 39:** *New APIs in HPE Aruba Networking Central 2.5.0 release*

API
<b>GDPR</b>
<ul style="list-style-type: none"><li>▪ [GET] /gdpr/v1/opt_out_clients</li><li>▪ [GET] /gdpr/v1/opt_out_clients/{mac}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /gdpr/v1/opt_out_clients</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /gdpr/v1/opt_out_clients</li></ul>
<b>Monitoring &gt; MobilityController</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/mobility_controllers/{serial}/vlan</li><li>▪ [GET] /monitoring/v1/mobility_controllers/{serial}/uplinks</li></ul>
<b>Monitoring &gt; Site</b>
<ul style="list-style-type: none"><li>▪ [POST] /central/v2/sites/associate</li><li>▪ [POST] /central/v2/sites/associations</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /central/v2/sites/associate</li><li>▪ [DELETE] /central/v2/sites/associations</li></ul>
<b>RAPIDS &gt; WIDS</b>
<ul style="list-style-type: none"><li>▪ [GET] /rapids/v1/wids/infrastructure_attacks</li><li>▪ [GET] /rapids/v1/wids/client_attacks</li><li>▪ [GET] /rapids/v1/wids/events</li></ul>
<b>RAPIDS &gt; Rogues</b>
<ul style="list-style-type: none"><li>▪ [GET] /rapids/v1/rogue_aps</li><li>▪ [GET] /rapids/v1/interfering_aps</li><li>▪ [GET] /rapids/v1/suspect_aps</li></ul>

**Table 39: New APIs in HPE Aruba Networking Central 2.5.0 release**

API
<ul style="list-style-type: none"> <li>[GET] /rapids/v1/neighbor_aps</li> </ul>
<b>User Management &gt; Users</b>
<ul style="list-style-type: none"> <li>[GET] /platform/rbac/v1/users</li> <li>[GET] /platform/rbac/v1/users/{user_id}</li> </ul>
<ul style="list-style-type: none"> <li>[PATCH] /platform/rbac/v1/users/{user_id}</li> </ul>
<ul style="list-style-type: none"> <li>[POST] /platform/rbac/v1/users</li> <li>[POST] /platform/rbac/v1/users/{user_id}/password</li> <li>[POST] /platform/rbac/v1/users/{user_id}/password/reset</li> </ul>
<ul style="list-style-type: none"> <li>[DELETE] /platform/rbac/v1/users/{user_id}</li> </ul>
<b>User Management &gt; Roles</b>
<ul style="list-style-type: none"> <li>[GET] /platform/rbac/v1/roles</li> <li>[GET] /platform/rbac/v1/apps/{app_name}/roles/{rolename}</li> </ul>
<ul style="list-style-type: none"> <li>[PATCH] /platform/rbac/v1/apps/{app_name}/roles/{rolename}</li> </ul>
<ul style="list-style-type: none"> <li>[POST] /platform/rbac/v1/apps/{app_name}/roles</li> </ul>
<ul style="list-style-type: none"> <li>[DELETE] /platform/rbac/v1/apps/{app_name}/roles/{rolename}</li> </ul>
<b>User Management &gt; Bulk Users</b>
<ul style="list-style-type: none"> <li>[POST] /platform/rbac/v1/bulk_users</li> </ul>
<ul style="list-style-type: none"> <li>[PATCH] /platform/rbac/v1/bulk_users</li> </ul>

## APIs Modified In Previous Releases

The section list the APIs modified in the previous releases of HPE Aruba Networking Central.

### HPE Aruba Networking Central 2.5.7

**Table 40: Modified APIs in HPE Aruba Networking Central 2.5.7 release**

API
<b>VisualRF &gt; Client Location</b>
<ul style="list-style-type: none"> <li>[GET] /visualrf_api/v1/floor/{floor_id}/client_location</li> <li>[GET] /visualrf_api/v1/client_location/{macaddr}</li> <li>[GET] /visualrf_api/v1/floor/{floor_id}/client_location</li> </ul>
<b>VisualRF &gt; Rogue Location</b>
<ul style="list-style-type: none"> <li>[GET] /visualrf_api/v1/floor/{floor_id}/rogue_location</li> <li>[GET] /visualrf_api/v1/rogue_location/{macaddr}</li> </ul>



**Table 40: Modified APIs in HPE Aruba Networking Central 2.5.7 release**

API
<ul style="list-style-type: none"><li>▪ [GET] /visualrf_api/v1/floor/{floor_id}/rogue_location</li></ul>
<b>VisualRF &gt; Floorplan</b>
<ul style="list-style-type: none"><li>▪ [GET] /visualrf_api/v1/campus</li><li>▪ [GET] /visualrf_api/v1/campus/{campus_id}</li></ul>
<b>User Management&gt; Users</b>
<ul style="list-style-type: none"><li>▪ [GET] /platform/rbac/v1/users</li></ul>
<ul style="list-style-type: none"><li>▪ [PATCH] /platform/rbac/v1/users/{user_id}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /platform/rbac/v1/users}</li><li>▪ [POST] /platform/rbac/v1/users/{user_id}/password</li><li>▪ [POST] /platform/rbac/v1/users/{user_id}/password/reset</li></ul>
<b>User Management&gt; Roles</b>
<ul style="list-style-type: none"><li>▪ [GET] /platform/rbac/v1/roles</li><li>▪ [GET] /platform/rbac/v1/apps/{app_name}/roles/{rolename}</li></ul>
<ul style="list-style-type: none"><li>▪ [PATCH] /platform/rbac/v1/apps/{app_name}/roles/{rolename}</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /platform/rbac/v1/apps/{app_name}/roles</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /platform/rbac/v1/apps/{app_name}/roles/{rolename}</li></ul>
<b>Service Airmatch</b>
<ul style="list-style-type: none"><li>▪ [GET] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/system/</li><li>▪ [GET] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/</li><li>▪ [GET] /airmatch-config/v1/node_list/{node_type}/{node_id}/</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/system/</li><li>▪ [POST] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/</li></ul>
<ul style="list-style-type: none"><li>▪ [PUT] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/system/</li><li>▪ [PUT] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/</li></ul>
<b>Monitoring &gt; Site</b>
<ul style="list-style-type: none"><li>▪ [POST] /central/v2/sites</li></ul>
<ul style="list-style-type: none"><li>▪ [PATCH] /central/v2/sites/{site_id}</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /central/v2/sites/{site_id}</li></ul>
<b>Monitoring &gt; Label</b>

**Table 40: Modified APIs in HPE Aruba Networking Central 2.5.7 release**

API
<ul style="list-style-type: none"><li>▪ [DELETE] /central/v1/labels/{label_id}</li></ul>
<b>MSP &gt; Customers</b>
<ul style="list-style-type: none"><li>▪ [DELETE] /msp_api /v1/customers/{customer_id}</li></ul>
<b>Configuration &gt; Devices</b>
<ul style="list-style-type: none"><li>▪ [GET] /configuration/v1/devices/{device_serial}/configuration</li></ul>
<b>Configuration &gt; WLAN Configuration</b>
<b>Configuration &gt; AP Configuration</b>

## HPE Aruba Networking Central 2.5.6

**Table 41: Modified APIs in HPE Aruba Networking Central 2.5.6 release**

API
<b>VisualRF &gt; Client Location</b>
<ul style="list-style-type: none"><li>▪ [GET] /visualrf_api/v1/floor/{floor_id}/client_location</li><li>▪ [GET] /visualrf_api/v1/client_location/{macaddr}</li><li>▪ [GET] /visualrf_api/v1/floor/{floor_id}/client_location</li></ul>
<b>VisualRF &gt; Rogue Location</b>
<ul style="list-style-type: none"><li>▪ [GET] /visualrf_api/v1/floor/{floor_id}/rogue_location</li><li>▪ [GET] /visualrf_api/v1/rogue_location/{macaddr}</li><li>▪ [GET] /visualrf_api/v1/floor/{floor_id}/rogue_location</li></ul>
<b>VisualRF &gt; Floorplan</b>
<ul style="list-style-type: none"><li>▪ [GET] /visualrf_api/v1/campus</li><li>▪ [GET] /visualrf_api/v1/campus/{campus_id}</li></ul>
<b>User Management&gt; Users</b>
<ul style="list-style-type: none"><li>▪ [GET] /platform/rbac/v1/users</li><li>▪ [PATCH] /platform/rbac/v1/users/{user_id}</li><li>▪ [POST] /platform/rbac/v1/users}</li><li>▪ [POST] /platform/rbac/v1/users/{user_id}/password</li><li>▪ [POST] /platform/rbac/v1/users/{user_id}/password/reset</li></ul>
<b>User Management&gt; Roles</b>
<ul style="list-style-type: none"><li>▪ [GET] /platform/rbac/v1/roles</li><li>▪ [GET] /platform/rbac/v1/apps/{app_name}/roles/{rolename}</li></ul>

**Table 41: Modified APIs in HPE Aruba Networking Central 2.5.6 release**

API
▪ [PATCH] /platform/rbac/v1/apps/{app_name}/roles/{rolename}
▪ [POST] /platform/rbac/v1/apps/{app_name}/roles
▪ [DELETE] /platform/rbac/v1/apps/{app_name}/roles/{rolename}
<b>Service Airmatch</b>
▪ [GET] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/system/
▪ [GET] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/
▪ [GET] /airmatch-config/v1/node_list/{node_type}/{node_id}/
▪ [POST] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/system/
▪ [POST] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/
▪ [PUT] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/system/
▪ [PUT] /airmatch-config/v1/node_list/{node_type}/{node_id}/config/
<b>Monitoring &gt; Site</b>
▪ [POST] /central/v2/sites
▪ [PATCH] /central/v2/sites/{site_id}
▪ [DELETE] /central/v2/sites/{site_id}
<b>Monitoring &gt; Label</b>
▪ [DELETE] /central/v1/labels/{label_id}
<b>MSP &gt; Customers</b>
▪ [DELETE] /msp_api /v1/customers/{customer_id}
<b>Configuration &gt; Devices</b>
▪ [GET] /configuration/v1/devices/{device_serial}/configuration
<b>Configuration &gt; WLAN Configuration</b>
<b>Configuration &gt; AP Configuration</b>

## HPE Aruba Networking Central 2.5.5

**Table 42: Modified APIs in HPE Aruba Networking Central 2.5.5 release**

API
<b>Configuration &gt; Groups</b>
▪ [GET] /configuration/v2/groups

**Table 42: Modified APIs in HPE Aruba Networking Central 2.5.5 release**

API
<ul style="list-style-type: none"><li>▪ [GET] /configuration/v1/groups/properties</li></ul>
<ul style="list-style-type: none"><li>▪ [POST] /configuration/v2/groups/clone</li></ul>
<b>Configuration &gt; Pre Provisioned Group</b> The location for the APIs in <b>Pre Provisioned Group</b> are moved from <b>Device Management</b> to <b>Configuration</b> .
<b>MSP &gt; Customers</b>
<ul style="list-style-type: none"><li>▪ [GET] /msp_api/v1/customers</li><li>▪ [GET] /msp_api /v1/customers/{customer_id}</li></ul>
<ul style="list-style-type: none"><li>▪ [DELETE] /msp_api /v1/customers/{customer_id}</li></ul>
<b>User Management &gt; Roles</b>
<ul style="list-style-type: none"><li>▪ [PATCH] /platform/rbac/v1/apps/{app_name}/roles/{rolename}</li><li>▪ [POST] /platform/rbac/v1/apps/{app_name}/roles</li></ul>

## HPE Aruba Networking Central 2.5.4

**Table 43: Modified APIs in HPE Aruba Networking Central 2.5.4 release**

API
<b>Configuration &gt; Groups</b>
<ul style="list-style-type: none"><li>▪ [GET] /configuration/v1/groups/properties</li><li>▪ [POST] /configuration/v2/groups</li><li>▪ [POST] /configuration/v2/groups/clone</li></ul>
<b>Monitoring &gt; Clients</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/clients/wireless</li><li>▪ [GET] /monitoring/v1/clients/wired</li></ul>
<b>Monitoring &gt; Switches</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/switches</li></ul>
<b>Topology</b>
<ul style="list-style-type: none"><li>▪ [GET] /{site_id}</li><li>▪ [GET] /devices/{device_serial}</li></ul>

## HPE Aruba Networking Central 2.5.3

**Table 44:** Modified APIs in HPE Aruba Networking Central 2.5.3 release

API
<b>Configuration &gt; Groups</b>
<ul style="list-style-type: none"><li>▪ [POST] /configuration/v2/groups</li></ul>
<b>Monitoring &gt; Switch</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/switches</li><li>▪ [GET] /monitoring/v1/switches/{serial}</li><li>▪ [GET] /monitoring/v1/switch_stacks</li></ul>
<b>Monitoring &gt; Client</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/clients/wireless</li><li>▪ [GET] /monitoring/v1/clients/wired</li></ul>
<b>Monitoring &gt; Gateway</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/gateways</li></ul>
<b>Monitoring &gt; AP</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/aps/{serial}</li></ul>
<b>Monitoring &gt; Swarm</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/swarms</li></ul>
<b>Topology</b>
<ul style="list-style-type: none"><li>▪ [GET] /{site_id}</li></ul>

## HPE Aruba Networking Central 2.5.2

**Table 45:** Modified APIs in HPE Aruba Networking Central 2.5.2 release

API
<b>Audit Event Logs</b>
<ul style="list-style-type: none"><li>▪ [GET] /auditlogs/v1/events</li><li>▪ [GET] /platform/auditlogs/v1/logs</li></ul>
<b>Monitoring &gt; Switch APIs</b>
<ul style="list-style-type: none"><li>▪ [GET] /monitoring/v1/switch_stacks/{stack-id}/ports</li><li>▪ [GET] /monitoring/v1/switches/{serial}/ports</li><li>▪ [GET] /monitoring/v1/switches/{serial}</li><li>▪ [GET] /monitoring/v1/switch_stacks/{stack_id}</li></ul>
<b>Audit Event Logs</b>
<ul style="list-style-type: none"><li>▪ [GET] /auditlogs/v1/events</li><li>▪ [GET] /platform/auditlogs/v1/logs</li></ul>

## HPE Aruba Networking Central 2.5.1

No APIs modified in HPE Aruba Networking Central 2.5.1 release

## HPE Aruba Networking Central 2.5.0

**Table 46:** *Modified APIs in HPE Aruba Networking Central 2.5.0 release*

API
<b>RAPIDS &gt; WIDS</b>
<ul style="list-style-type: none"><li>▪ [GET] /rapids/v1/wids/infrastructure_attacks</li><li>▪ [GET] /rapids/v1/wids/client_attacks</li><li>▪ [GET] /rapids/v1/wids/events</li></ul>
<b>RAPIDS &gt; Rogues</b>
<ul style="list-style-type: none"><li>▪ [GET] /rapids/v1/rogue_aps</li><li>▪ [GET] /rapids/v1/interfering_aps</li><li>▪ [GET] /rapids/v1/suspect_aps</li><li>▪ [GET] /rapids/v1/neighbor_aps</li></ul>

Webhooks allow you to implement event reactions by providing real-time information or notifications to other applications. HPE Aruba Networking Central allows you to create and select webhooks as the notification delivery option for all alerts.

Using HPE Aruba Networking Central, you can integrate Webhooks with other third-party applications such as ServiceNow, Zapier, IFTTT, etc.

You can access the Webhooks service either through the HPE Aruba Networking Central UI or API Gateway. HPE Aruba Networking Central supports creating up to 10 Webhooks. To enable redundancy, HPE Aruba Networking Central allows you to add up to three URLs per Webhook.

From HPE Aruba Networking Central, you can do the following

- Add, list, or delete Webhooks
- Get or refresh Webhooks token
- Get or update Webhooks settings for a specific item
- Test Webhooks notification.

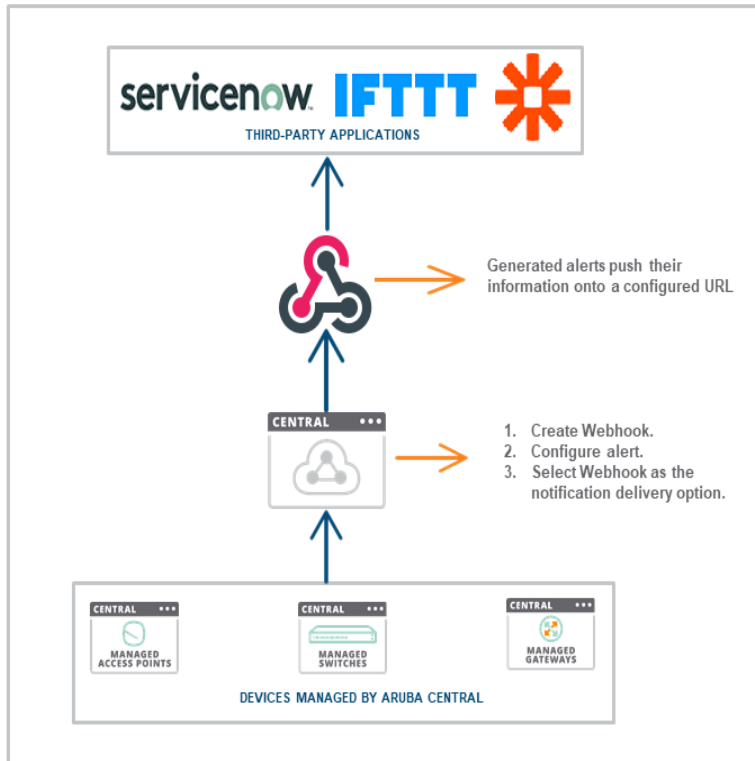
This section includes the following topics:

- [Creating and Updating Webhooks Through the UI](#)
- [Viewing and Editing Webhooks](#)
- [Refreshing Webhooks Token Through the UI](#)
- [Creating and Updating Webhooks Through the API Gateway](#)
- [List of Webhooks APIs](#)
- [Sample Webhooks Payload Format for Alerts](#)

In the **Alerts & Events** page, click the **Configuration** icon to configure and enable an alert. In the **Notification Options**, select **Webhooks** as the notification delivery option.

The following figure illustrates how HPE Aruba Networking Central integrates with third-party applications using Webhooks.

**Figure 3** Webhooks Integration



## Creating and Updating Webhooks Through the UI

To access the Webhooks service from the UI:



Only users with **edit** permission to NMS service resources can modify webhooks.

1. In the WebUI app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration > Webhooks**. The **Webhooks** page is displayed.
3. In the **Webhook** tab, click **+ sign**. The **Add Webhook** pop-up window is displayed.

**Figure 4** Webhooks Page

Webhooks (6)				
Name	URL	Last Update	Retry Policy	
>	1	Mar 15, 2022, 21:16	None	
>	1	Jan 31, 2022, 15:24	None	
>	1	Mar 7, 2022, 21:20	None	
>	1	Jan 31, 2022, 23:37	None	
>	1	Feb 9, 2022, 19:45	Important	
>	1	Feb 8, 2022, 12:03	None	



**Figure 5** Add Webhooks Page

← | Add Webhook

Name \_\_\_\_\_ URL +

Retry Policy

None

Important (up to 5 retries over 6 minutes)

Critical (up to 5 retries over 32 hours)

Cancel Add

4. To create webhooks, enter the following details:
  - a. **Name**—Enter a name for the Webhook.
  - b. **Retry Policy**—Select one of the following options:
    - **None**—No retries.
    - **Important**—Up to 5 retries over 6 minutes.
    - **Critical**—Up to 5 retries over 32 hours.
  - c. **URLs**—Enter the URL. Click + to enter another URL. You can add up to three URLs.
5. Click **Save**. The Webhooks is created and listed in the **Webhook** table.

## Viewing and Editing Webhooks

To view the Webhooks, complete the following steps:


1. In the WebUI app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration > Webhooks**.
3. The **Webhooks** page with Webhook table is displayed.

The **Webhook** table allows you to test, view dispatch logs, and delete Webhooks. The webhooks table displays the following information:

  - **Name**—Name of the Webhooks.
  - **URL**—Number of URLs in Webhooks.
  - **Last Updated**—Date and time at which Webhooks was updated.
  - **Retry Policy**—Displays the selected retry policy.
  - **Test Webhooks**—Hover over a Webhook from the list and click the **Test Webhooks** icon to test the Webhook by posting sample webhook payload to the configured URL. The **Test Webhooks** table provides the **URL** and **Status** of the selected Webhook.
  - **View Dispatch Logs**—Hover over a Webhook from the list and click the **View Dispatch Log** icon to view the **Dispatch Logs** for the selected Webhook. The **Dispatch Logs** table provides the **URL**, **Status**, and **Dispatched Time**. Click the arrow against each row to view the **Log Details** and **Attempts** in the drop-down for the respective URL.

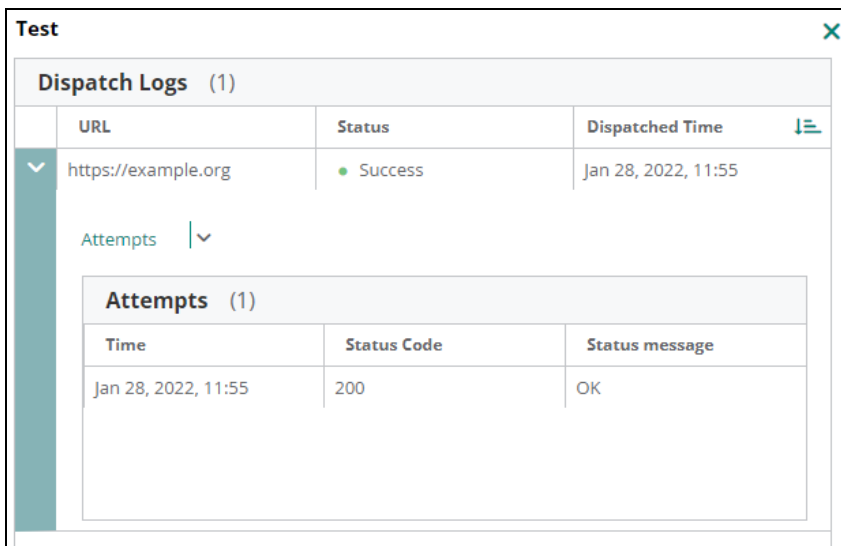
- **Delete**—Hover over a Webhook from the list and click the **Delete** icon and click **Yes** to delete the Webhook.

To edit a Webhooks, complete the following steps:

1. Select a webhook from the list of webhooks and click  icon. The following information are displayed:
  - **Name**—Name of the Webhooks.
  - **Webhook ID**—Displays the webhooks ID.
  - **Retry Policy**—Displays the selected retry policy. You can select any policy from the **Retry Policy** drop-down option.
  - **Token**—Webhooks token. Webhooks token enables header authentication and the third-party receiving service must validate the token to ensure authenticity. To refresh a token, click the refresh icon.
  - **URL**—Number of URLs in Webhooks. Click **+** to enter another URL. You can add up to three URLs.
2. Click **Save** to save the settings.

The following figure displays the dispatch log details for a webhook.

**Figure 6** Dispatch Logs Details Page



The screenshot shows a 'Test' window with a 'Dispatch Logs (1)' table. The table has columns for URL, Status, and Dispatched Time. A single entry is shown for 'https://example.org' with a 'Success' status and a dispatch time of 'Jan 28, 2022, 11:55'. Below the table, there is an 'Attempts' section with a dropdown arrow. The 'Attempts (1)' table has columns for Time, Status Code, and Status message. A single entry is shown for 'Jan 28, 2022, 11:55' with a status code of '200' and a status message of 'OK'.


Dispatch Logs (1)		
URL	Status	Dispatched Time
https://example.org	Success	Jan 28, 2022, 11:55

Attempts (1)		
Time	Status Code	Status message
Jan 28, 2022, 11:55	200	OK

## Refreshing Webhooks Token Through the UI

To refresh the Webhooks token through the UI:

1. In the WebUI app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration > Webhooks**. Displays the **Webhooks** page.
3. In the **Webhook** table, select the Webhook from the list and click  icon to edit.
4. Click the **Refresh** icon next to the token.

# Creating and Updating Webhooks Through the API Gateway

The following HTTP methods are defined for HPE Aruba Networking Central API Webhooks resource:

- **GET**
- **POST**
- **PUT**
- **DELETE**

You can perform CRUD operation on the Webhooks URL configuration. The key configuration elements that are required to use API Webhooks service are Webhooks URL and a shared secret.

A shared secret token is generated for the Webhooks URL when you register for Webhooks. A hash key is generated using the SHA256 algorithm by using the payload and the shared secret token. The API required to refresh the shared secret token is provided for a specific Webhooks configuration. You can choose the frequency at which you want to refresh the secret token.

To access and use the API Webhooks service:

1. In the HPE Aruba Networking Central app, under **Maintain**, click **Organization > Platform Integration > Rest API**. The **API Gateway** page is displayed.
2. In the **APIs** tab, click the **Swagger** link under the **Documentation** header. The Swagger website opens.
3. In the Swagger website, from the **URL** drop-down list, select **Webhook**. All available Webhooks APIs are listed under **API Reference**.



---

Swagger documentation displays more information on Webhook APIs. To access the Swagger documentation, see [API Gateway](#).

---

## List of Webhooks APIs

HPE Aruba Networking Central supports the following Webhooks APIs:

- **GET /central/v1/webhooks**—Gets a list of Webhooks.

The following is a sample response:

```
{
  "count": 1,
  "settings": [
    {
      "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8",
      "name": "AAA",
      "updated_ts": 1523956927,
      "urls": [
        "https://example.org/webhook1",
        "https://example.org/webhook1"
      ],
      "secure_token": "KEu5ZPTi44UO4MnMiOqz"
    }
  ]
}
```

```
}
]
}
```

- **POST /central/v1/webhooks**—Creates Webhooks.

The following is a sample response:

```
{
  "name": "AAA",
  "wid": "e829a0f6-1e36-42fe-bafd-631443cbd581"
}
```

- **DELETE /central/v1/webhooks/{wid}**—Deletes Webhooks.

The following is a sample response:

```
{
  "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8"
}
```

- **GET /central/v1/webhooks/{wid}**—Gets Webhooks settings for a specific item.

The following is a sample response:

```
{
  "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8",
  "name": "AAA",
  "updated_ts": 1523956927,
  "urls": [
    "https://example.org/webhook1",
    "https://example.org/webhook1"
  ],
  "secure_token": "KEu5ZPTi44U04MnMiOqz"
}
```

- **PUT /central/v1/webhooks/{wid}**—Updates Webhooks settings for a specific item.

The following is a sample response:

```
{
  "name": "AAA",
  "wid": "e829a0f6-1e36-42fe-bafd-631443cbd581"
}
```

- **GET /central/v1/webhooks/{wid}/token**—Gets the Webhooks token for the Webhooks ID.

The following is a sample response:

```
{
  "name": "AAA",
```

```
"secure_token": "[{"token": "zSMrzuYrblgBfByy2JrM", "ts": 1523957233}]"
```

- **PUT /central/v1/webhooks/{wid}/token**—Refreshes the Webhooks token for the Webhooks ID.

The following is a sample response:

```
{  
  "name": "AAA",  
  "secure_token": "[{"token": "zSMrzuYrblgBfByy2JrM", "ts": 1523957233}]"  
}
```

- **GET /central/v1/webhooks/{wid}/ping**—Tests the Webhooks notification and returns whether success or failure.

The following is a sample response:

```
"Ping Response [{"url": "https://example.org", "status": 404}]"
```

## Sample Webhooks Payload Format for Alerts

URL POST <webhook-url>

### Custom Headers

```
Content-Type: application/json  
X-Central-Service: Alerts  
X-Central-Event: Radio-Channel-Utilization  
X-Central-Delivery-ID: 72d3162e-cc78-11e3-81ab-4c9367dc0958  
X-Central-Delivery-Timestamp: 2016-07-12T13:14:19-07:00  
X-Central-Customer-ID: <#####>
```

Refer to the following topics to view sample JSON content:

- [Access Point Alerts—Sample JSON](#)
- [AOS-S Alerts—Sample JSON](#)
- [AOS-CX Switch Alerts—Sample JSON](#)
- [Gateway Alerts—Sample JSON](#)
- [Miscellaneous Alerts—Sample JSON](#)

## Sample Webhooks Payload Format for Alerts

URL POST <webhook-url>

### Custom Headers

```
Content-Type: application/json  
X-Central-Service: Alerts  
X-Central-Event: Radio-Channel-Utilization  
X-Central-Delivery-ID: 72d3162e-cc78-11e3-81ab-4c9367dc0958  
X-Central-Delivery-Timestamp: 2016-07-12T13:14:19-07:00  
X-Central-Customer-ID: <#####>
```

Refer to the following topics to view sample JSON content:

- [Access Point Alerts—Sample JSON](#)
- [AOS-S Alerts—Sample JSON](#)
- [AOS-CX Switch Alerts—Sample JSON](#)
- [Gateway Alerts—Sample JSON](#)
- [Miscellaneous Alerts—Sample JSON](#)

## Access Point Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

### AP Connected Clients

```
{
  "id": "AXdhYi4Eo68tULajREh0",
  "nid": 1255,
  "alert_type": "AP_CONNECTED_CLIENTS",
  "setting_id": "55ef4ae129a24c2180e010708202b502-1255",
  "device_id": "CNDSHN74L6",
  "description": "Number of clients connected to AP 20:a6:cd:cc:17:58 has been
above 1 for about 5 minutes since 2021-02-02 06:11:00 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612246560,
  "details": {
    "customer_id": "55ef4ae129a24c2180e010708202b502",
    "name": "20:a6:cd:cc:17:58",
    "serial": "CNDSHN74L6",
    "group": "1",
    "labels": "3",
    "_rule_number": "0",
    "ds_key": "55ef4ae129a24c2180e010708202b502.CNDSHN74L6.device.clients.5m",
    "duration": "5",
    "threshold": "1",
    "time": "2021-02-02 06:11:00 UTC"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "Number of clients connected to AP 20:a6:cd:cc:17:58 has been
above 1 for about 5 minutes since 2021-02-02 06:11:00 UTC"
}
```

### AP CPU Over Utilization

```
{
  "id": "AXdhYjAko68tULajREiC",
  "nid": 1250,
  "alert_type": "AP_CPU_OVER_UTILIZATION",
  "setting_id": "55ef4ae129a24c2180e010708202b502-1250",
  "device_id": "CNDSHN74L6",
  "description": "CPU utilization for AP 20:a6:cd:cc:17:58 with serial CNDSHN74L6 has
been
above 1% for about 5 minutes since 2021-02-02 06:11:00 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612246560,
  "details": {
    "name": "20:a6:cd:cc:17:58",

```

```

    "unit": "%",
    "serial": "CNDSHN74L6",
    "group": "1",
    "labels": "3",
    "_rule_number": "0",
    "ds_key": "55ef4ae129a24c2180e010708202b502.CNDSHN74L6.cpu_utilization.5m",
    "duration": "5",
    "threshold": "1",
    "time": "2021-02-02 06:11:00 UTC"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "CPU utilization for AP 20:a6:cd:cc:17:58 with serial CNDSHN74L6 has been
  above 1% for about 5 minutes since 2021-02-02 06:11:00 UTC"
}

```

---

## AP Disconnected

```

{
  "id": "AXdhbSf7o68tULajRFQy",
  "nid": 4,
  "alert_type": "AP disconnected",
  "setting_id": "55ef4ae129a24c2180e010708202b502-4",
  "device_id": "DZ0001581",
  "description": "AP f0:5c:19:c9:f7:6a with MAC address f0:5c:19:c9:f7:6a disconnected,
  Group:unprovisioned",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612247279,
  "details": {
    "params": [
      "DZ0001581",
      "f0:5c:19:c9:f7:6a",
      "10.29.6.170",
      "f0:5c:19:c9:f7:6a",
      "",
      ""
    ],
    "group": "1",
    "ts": "1612246960735",
    "labels": "",
    "serial": "DZ0001581",
    "conn_status": "disconnected",
    "time": "2021-02-02 06:27:59 UTC",
    "group_name": "unprovisioned"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "AP f0:5c:19:c9:f7:6a with MAC address f0:5c:19:c9:f7:6a disconnected,
  Group:unprovisioned"
}

```

---

## AP Memory Over Utilization

```

{
  "id": "AXdhYi_Bo68tULajREh_",
  "nid": 1251,
  "alert_type": "AP_MEMORY_OVER_UTILIZATION",
  "setting_id": "55ef4ae129a24c2180e010708202b502-1251",

```

```

"device_id": "CNDSHN74L6",
"description": "Memory utilization for AP 20:a6:cd:cc:17:58 with serial CNDSHN74L6
has been
above 10% for about 5 minutes since 2021-02-02 06:11:00 UTC",
"state": "Open",
"severity": "Critical",
"operation": "create",
"timestamp": 1612246560,
"details": {
  "name": "20:a6:cd:cc:17:58",
  "unit": "%",
  "serial": "CNDSHN74L6",
  "group": "1",
  "labels": "3",
  "_rule_number": "0",
  "ds_key": "55ef4ae129a24c2180e010708202b502.CNDSHN74L6.memory_utilization.5m",
  "duration": "5",
  "threshold": "10",
  "time": "2021-02-02 06:11:00 UTC"
},
"webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
"text": "Memory utilization for AP 20:a6:cd:cc:17:58 with serial CNDSHN74L6 has been
above 10% for about 5 minutes since 2021-02-02 06:11:00 UTC"
}

```

## AP Radio Noise Floor

```

{
  "id": "AXdhYFmQo68tULajREe3",
  "nid": 1253,
  "alert_type": "AP_RADIO_NOISE_FLOOR",
  "setting_id": "55ef4ae129a24c2180e010708202b502-1253",
  "device_id": "DZ0001581",
  "description": "Noise floor on AP f0:5c:19:c9:f7:6a operating on channel 132E and
serving 0 clients has been above -100 dBm for about 5 minutes since 2021-02-02
06:09:00 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612246440,
  "details": {
    "name": "f0:5c:19:c9:f7:6a",
    "_band": "1",
    "_radio_num": "0",
    "channel": "132E",
    "client_count": "0",
    "unit": "%",
    "serial": "DZ0001581",
    "group": "1",
    "_rule_number": "0",
    "ds_key": "55ef4ae129a24c2180e010708202b502.DZ0001581.radio.noisefloor",
    "duration": "5",
    "threshold": "100",
    "time": "2021-02-02 06:09:00 UTC"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "Noise floor on AP f0:5c:19:c9:f7:6a operating on channel 132E and serving
0 clients has been above -100 dBm for about 5 minutes since 2021-02-02 06:09:00
UTC"
}

```



## AP Radio Over Utilization

```
{
  "id": "AXdhYFm6o68tULajREe4",
  "nid": 1252,
  "alert_type": "AP_RADIO_OVER_UTILIZATION",
  "setting_id": "55ef4ae129a24c2180e010708202b502-1252",
  "device_id": "DZ0001581",
  "description": "Radio utilization on AP f0:5c:19:c9:f7:6a operating on channel 132E
and
  serving 0 clients has been above 5% for about 5 minutes since 2021-02-02 06:09:00
UTC",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612246440,
  "details": {
    "name": "f0:5c:19:c9:f7:6a",
    "_band": "1",
    "_radio_num": "0",
    "channel": "132E",
    "client_count": "0",
    "unit": "%",
    "serial": "DZ0001581",
    "group": "1",
    "_rule_number": "0",
    "ds_key": "55ef4ae129a24c2180e010708202b502.DZ0001581.radio.busy64",
    "duration": "5",
    "threshold": "5",
    "time": "2021-02-02 06:09:00 UTC"
  }
}
```

## AP\_Radio\_Non\_Wifi\_Over\_Utilization

```
{
  "id": "AXdhYFnIo68tULajREe5",
  "nid": 1259,
  "alert_type": "AP_RADIO_NON_WIFI_OVER_UTILIZATION",
  "setting_id": "55ef4ae129a24c2180e010708202b502-1259",
  "device_id": "DZ0001581",
  "description": "Radio Non-Wifi utilization on AP f0:5c:19:c9:f7:6a operating on
channel 6
  and serving 0 clients has been above 1% for about 5 minutes since 2021-02-02
06:09:00 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612246440,
  "details": {
    "name": "f0:5c:19:c9:f7:6a",
    "_band": "0",
    "_radio_num": "1",
    "channel": "6",
    "client_count": "0",
    "unit": "%",
    "serial": "DZ0001581",
    "group": "1",
    "_rule_number": "0",
    "ds_key": "55ef4ae129a24c2180e010708202b502.DZ0001581.radio.interference",
    "duration": "5",
    "threshold": "1",
    "time": "2021-02-02 06:09:00 UTC"
  }
}
```

```
},
"webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
"text": "Radio Non-Wifi utilization on AP f0:5c:19:c9:f7:6a operating on channel 6
and serving 0 clients has been above 1% for about 5 minutes since 2021-02-02
06:09:00 UTC"
}
```

---

## AP\_Tunnel\_Down

```
{
  "id": "AXdhfDSyo68tULajRGTZ",
  "nid": 1257,
  "alert_type": "AP_TUNNEL_DOWN",
  "setting_id": "55ef4ae129a24c2180e010708202b502-1257",
  "device_id": "CNDSHN74L6",
  "description": "AP tunnel vpn_tun_default_0 from 0.0.0.0 to 0.0.0.0 is DOWN on
device 20:a6:cd:cc:17:58 with serial CNDSHN74L6 at 2021-02-02 06:44:25 UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612248265,
  "details": {
    "src_ip": "0.0.0.0",
    "dst_ip": "0.0.0.0",
    "alias_map_name": "vpn_tun_default_0",
    "name": "20:a6:cd:cc:17:58",
    "serial": "CNDSHN74L6",
    "group": "86",
    "labels": "3",
    "rule_number": "0",
    "time": "2021-02-02 06:44:25 UTC"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "AP tunnel vpn_tun_default_0 from 0.0.0.0 to 0.0.0.0 is DOWN on
device 20:a6:cd:cc:17:58 with serial CNDSHN74L6 at 2021-02-02 06:44:25 UTC."
}
```

---

## AP With Missing Radios

```
{
  "id": "AXdhvfeko68tULajRJM",
  "nid": 1249,
  "alert_type": "AP With Missing Radios",
  "setting_id": "6f00c6501c5c4331b7934845815ef078-1249",
  "device_id": "FVZP000008",
  "description": "AP FVZP000008 reporting 2 out of 1 radios. Reported radio
MAC 76:d6:07:35:60:00, b1:66:99:ed:f0:00.",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612252575,
  "details": {
    "serial": "FVZP000008",
    "labels": [
      "5",
      "4",
      "1"
    ],
    "group": "34",
  },
}
```

```

    "params": [
      "FVZP000008",
      "2",
      "1",
      "76:d6:07:35:60:00, b1:66:99:ed:f0:00"
    ],
    "time": "2021-02-02 07:56:15 UTC"
  },
  "webhook": "f383ee40-888b-4dee-97d5-bcbbcf5db946",
  "text": "AP FVZP000008 reporting 2 out of 1 radios. Reported radio
  MAC 76:d6:07:35:60:00, b1:66:99:ed:f0:00."
}

```

---

## Client Attack detected

```

{
  "alert_type": "Client attack detected",
  "description": "An AP (NAME iap-303-iphone456-o and MAC 90:4c:81:cf:27:74 on RADIO 1)
  detected an unencrypted frame
  between a valid client (88:63:df:bb:2a:9d) and access point (BSSID
  90:4c:81:72:77:55) with source 88:63:df:bb:2a:9d
  and receiver ff:ff:ff:ff:ff:ff SNR value is 55",
  "timestamp": 1564392710,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-13",
  "state": "Open",
  "nid": 13,
  "details": {
    "group": "3",
    "labels": "3,142,141",
    "params": "None",
    "_rule_number": "0",
    "time": "2019-07-29 09:31:50 UTC"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWw9EmBxVQ01ZtiG01Q8",
  "severity": "Critical"
}

```

---

## Connected Clients

```

{
  "id": "AXdhWQbro68tULajREA9",
  "nid": 1254,
  "alert_type": "CONNECTED_CLIENTS",
  "setting_id": "55ef4ae129a24c2180e010708202b502-1254",
  "device_id": "cf62d07c019cd6bca90e6079e351251070d9e286f310c87541",
  "description": "Number of clients connected to VC SetMeUp-C9:F7:6A has been
  above 1 for about 5 minutes since 2021-02-02 06:01:00 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612245960,
  "details": {
    "customer_id": "55ef4ae129a24c2180e010708202b502",
    "name": "SetMeUp-C9:F7:6A",
    "serial": "cf62d07c019cd6bca90e6079e351251070d9e286f310c87541",
    "group": "1",
  }
}

```

```
  "_rule_number": "0",
  "ds_key": "55ef4ae129a24c2180e010708202b502.cluster.363.device.clients.5m",
  "duration": "5",
  "threshold": "1",
  "time": "2021-02-02 06:01:00 UTC"
},
"webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
"text": "Number of clients connected to VC SetMeUp-C9:F7:6A has been above 1 for about 5 minutes since 2021-02-02 06:01:00 UTC"
}
```

---

## IAP Firmware Upgrade Failed

```
{
  "id": "AXdheDego68tULajRGB5",
  "nid": 2200,
  "alert_type": "IAP_FW_UPGRADE_FAILURE",
  "setting_id": "55ef4ae129a24c2180e010708202b502-2200",
  "device_id": "",
  "description": "Firmware upgrade failed for AP CNDSHN74L6 with serial None and MAC address 20:a6:cd:cc:17:58",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612248004,
  "details": {
    "mac": "20:a6:cd:cc:17:58",
    "hostname": "CNDSHN74L6",
    "serial": "None",
    "group": "86",
    "labels": "",
    "_rule_number": "0",
    "params": "None",
    "time": "2021-02-02 06:40:04 UTC"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "Firmware upgrade failed for AP CNDSHN74L6 with serial None and MAC address 20:a6:cd:cc:17:58"
}
```

---

## Infrastructure Attack Detected

```
{
  "alert_type": "Infrastructure attack detected",
  "description": "An AP (NAME iap-303-iphone456-o and MAC 90:4c:81:cf:27:74 on RADIO 1) detected that the Access Point with MAC f0:5c:19:23:56:10 and BSSID f0:5c:19:23:56:10 has sent a beacon for SSID tan This beacon advertizes channel 149 but was received on channel 161 with SNR 50 ",
  "timestamp": 1564400165,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-12",
  "state": "Open",
  "nid": 12,
  "details": {
    "group": "3",
    "labels": "3,142,141",
    "params": "None",
    "_rule_number": "0",
  }
}
```

```
    "time": "2019-07-29 11:36:05 UTC"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWw9hCLAVQ0lZtiGPlig",
  "severity": "Critical"
}
```

---

## Insufficient Power Alert

```
{
  "id": "AXdhan_Zo68tULajRFB6",
  "nid": 21,
  "alert_type": "INSUFFICIENT_POWER_ALERT",
  "setting_id": "55ef4ae129a24c2180e010708202b502-21",
  "device_id": "CNDSHN74L6",
  "description": "Insufficient inline power supplied to AP-325 with name
20:a6:cd:cc:17:58",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612247105,
  "details": {
    "name": "20:a6:cd:cc:17:58",
    "ap_model": "AP-325",
    "group": "1",
    "labels": [
      "3"
    ],
    "serial": "CNDSHN74L6",
    "rule_number": "0",
    "time": "2021-02-02 06:25:05 UTC"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "Insufficient inline power supplied to AP-325 with name 20:a6:cd:cc:17:58"
}
```

---

## Modem Plugged

```
{
  "id": "AXdhmYueo68tULajRH6n",
  "nid": 18,
  "alert_type": "Modem Plugged",
  "setting_id": "b8be21720dc04a8e9f0028374b6a9bbd-18",
  "device_id": "GRUT000002",
  "description": "Modem plugged to AP GRUT000002 with MAC address 4a:36:66:b8:50:00",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612250188,
  "details": {
    "group": "0",
    "labels": "",
    "rule_number": "0",
    "params": [
      "GRUT000002",
      "4a:36:66:b8:50:00"
    ],
    "serial": "GRUT000002",
  }
}
```

```
    "time": "2021-02-02 07:16:28 UTC"
  },
  "webhook": "31a75d0a-dfd4-4c22-a32b-09d7b033d41e",
  "text": "Modem plugged to AP GRUT000002 with MAC address 4a:36:66:b8:50:00"
}
```

---

## Modem Unplugged

```
{
  "id": "AXdhp2Uwo68tULajRIVC",
  "nid": 19,
  "alert_type": "Modem Unplugged",
  "setting_id": "b8be21720dc04a8e9f0028374b6a9bbd-19",
  "device_id": "GRUT000001",
  "description": "Modem unplugged from AP GRUT000001 with MAC address
64:2a:90:97:f0:00",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612251096,
  "details": {
    "group": "0",
    "labels": "",
    "_rule_number": "0",
    "params": [
      "GRUT000001",
      "64:2a:90:97:f0:00"
    ],
    "serial": "GRUT000001",
    "time": "2021-02-02 07:31:36 UTC"
  },
  "webhook": "31a75d0a-dfd4-4c22-a32b-09d7b033d41e",
  "text": "Modem unplugged from AP GRUT000001 with MAC address 64:2a:90:97:f0:00"
}
```

---

## New AP Detected

```
{
  "id": "AXdhcXF1o68tULajRFld",
  "nid": 3,
  "alert_type": "New AP detected",
  "setting_id": "55ef4ae129a24c2180e010708202b502-3",
  "device_id": "DZ0001581",
  "description": "New AP f0:5c:19:c9:f7:6a with MAC address f0:5c:19:c9:f7:6a
detected, Group:unprovisioned",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612247560,
  "details": {
    "group": "1",
    "labels": "",
    "_rule_number": "0",
    "params": [
      "f0:5c:19:c9:f7:6a",
      "f0:5c:19:c9:f7:6a"
    ],
    "serial": "DZ0001581",
    "time": "2021-02-02 06:32:40 UTC",
  }
}
```

---

```

    "group_name": "unprovisioned"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "New AP f0:5c:19:c9:f7:6a with MAC address f0:5c:19:c9:f7:6a detected,
Group:unprovisioned"
}

```

---

## New Virtual Controller Detected

```

{
  "id": "AXdhcJgro68tULajRFjG",
  "nid": 1,
  "alert_type": "New Virtual Controller detected",
  "setting_id": "55ef4ae129a24c2180e010708202b502-1",
  "device_id": "",
  "description": "New Virtual controller SetMeUp-C9:F7:6A with version 8.7.1.0_77203
and IP address 10.29.6.170 detected, Group:unprovisioned",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612247504,
  "details": {
    "group": "1",
    "labels": "",
    "_rule_number": "0",
    "params": [
      "SetMeUp-C9:F7:6A",
      "8.7.1.0_77203",
      "10.29.6.170",
      "DZ0001581"
    ],
    "serial": "None",
    "time": "2021-02-02 06:31:44 UTC",
    "group_name": "unprovisioned"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "New Virtual controller SetMeUp-C9:F7:6A with version 8.7.1.0_77203
and IP address 10.29.6.170 detected, Group:unprovisioned"
}

```

---

## Rogue AP Detected

```

{
  "alert_type": "Rogue AP detected",
  "description": "An AP (NAME 84:d4:7e:c5:c8:8c and MAC address 84:d4:7e:c5:c8:8con
RADIO 1)
detected an access point
(BSSID 0c:00:01:34:69:62 and SSID ssid1 on CHANNEL 52) as rogue",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-10",
  "state": "Open",
  "nid": 10,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",

```

```
      "84:d4:7e:c5:c8:8c",
      "1",
      "0c:00:01:34:69:62",
      "ssid1",
      "52"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5GmlzVQ01ZtiJK891",
  "severity": "Critical"
}
```

---

## Radio Frames Retry Percent

```
{
  "id": "AXdrc2PMo68tULajSvRF",
  "nid": 1256,
  "alert_type": "AP_TX_RETRY_PERCENT",
  "setting_id": "2a35217e2f114cd8958f00a676258785-1256",
  "device_id": "VEYB000004",
  "description": "Radio frames retry percent for AP VEYB000004 with serial VEYB000004
has been
  above 1% for about 5 minutes since 2021-02-04 05:06:00 UTC",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612415460,
  "details": {
    "name": "VEYB000004",
    "_band": "0",
    "_radio_num": "0",
    "channel": "11",
    "client_count": "1",
    "unit": "%",
    "serial": "VEYB000004",
    "group": "2",
    "labels": "4",
    "_rule_number": "0",
    "ds_key": "2a35217e2f114cd8958f00a676258785.VEYB000004.radio.retry_percent",
    "duration": "5",
    "threshold": "1",
    "time": "2021-02-04 05:06:00 UTC"
  },
  "webhook": "bd4f20e6-55e6-4360-ab55-da2829f1a390",
  "text": "Radio frames retry percent for AP VEYB000004 with serial VEYB000004 has
been
  above 1% for about 5 minutes since 2021-02-04 05:06:00 UTC"
}
```

---

## Uplink Changed

```
{
  "id": "AXdhmSSKo68tULajRH4M",
  "nid": 17,
  "alert_type": "Uplink Changed",
  "setting_id": "b8be21720dc04a8e9f0028374b6a9bbd-17",
}
```



```

"device_id": "GRUT000003",
"description": "Uplink changed from Ethernet to WiFi Mesh for AP GRUT000003 with MAC
address 3d:62:d4:3f:90:00",
"state": "Open",
"severity": "Major",
"operation": "create",
"timestamp": 1612250162,
"details": {
  "group": "0",
  "labels": "",
  "_rule_number": "0",
  "params": [
    "Ethernet",
    "WiFi Mesh",
    "GRUT000003",
    "3d:62:d4:3f:90:00"
  ],
  "serial": "GRUT000003",
  "time": "2021-02-02 07:16:02 UTC"
},
"webhook": "31a75d0a-dfd4-4c22-a32b-09d7b033d41e",
"text": "Uplink changed from Ethernet to WiFi Mesh for AP GRUT000003 with MAC
address 3d:62:d4:3f:90:00"
}

```

---

## Virtual Controller Disconnected

```

{
  "id": "AXdheuQH068tULajRGQ5",
  "nid": 2,
  "alert_type": "Virtual controller disconnected",
  "setting_id": "55ef4ae129a24c2180e010708202b502-2",
  "device_id": "DZ0001581",
  "description": "Virtual controller SetMeUp-C9:F7:6A with version 8.7.1.0_77203 and
IP address 10.29.6.170 disconnected, Group:unprovisioned",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612248179,
  "details": {
    "params": [
      "DZ0001581",
      "f0:5c:19:c9:f7:6a",
      "10.29.6.170",
      "SetMeUp-C9:F7:6A",
      "8.7.1.0_77203",
      ""
    ],
    "group": "1",
    "ts": "1612247876960",
    "labels": "",
    "serial": "DZ0001581",
    "conn_status": "disconnected",
    "time": "2021-02-02 06:42:59 UTC",
    "group_name": "unprovisioned"
  },
  "webhook": "110576c0-59fb-4295-b53b-fdbafbc95dee",
  "text": "Virtual controller SetMeUp-C9:F7:6A with version 8.7.1.0_77203 and
IP address 10.29.6.170 disconnected, Group:unprovisioned"
}

```

---

# AOS-S Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

## Switch Disconnected

```
{
  "id": "AXbhjMPpKHBn24BIWnGc",
  "nid": 203,
  "alert_type": "Switch Disconnected",
  "setting_id": "flae23ba9025490cb53efb0993e05f17-203",
  "device_id": "CN80HKW2Z6",
  "description": "Switch with serial CN80HKW2Z6, MAC address 54:80:28:61:b3:20 IP
address 10.21.20.231
and Hostname Aruba-2930F-24G-PoEP-4SFPP reconnected",
  "state": "Close",
  "severity": "Major",
  "operation": "update",
  "timestamp": 1612383547,
  "details": {
    "params": [
      "CN80HKW2Z6",
      "54:80:28:61:b3:20",
      "10.21.20.231",
      "Aruba-2930F-24G-PoEP-4SFPP",
      "",
      ""
    ],
    "serial": "CN80HKW2Z6",
    "time": "2021-01-08 10:31:07 UTC",
    "conn_status": "reconnected"
  },
  "webhook": "8077a55e-f8d3-43af-a67f-12263f5b778e",
  "text": "Switch with serial CN80HKW2Z6, MAC address 54:80:28:61:b3:20 IP address
10.21.20.231
and Hostname Aruba-2930F-24G-PoEP-4SFPP reconnected"
}
```

## New Switch Connected

```
{
  "id": "AXdpfWeFo68tULajsfwu",
  "nid": 201,
  "alert_type": "New Switch Connected",
  "setting_id": "flae23ba9025490cb53efb0993e05f17-201",
  "device_id": "CN80HKW2Z6",
  "description": "New Switch with serial CN80HKW2Z6, MAC address 54:80:28:61:b3:20 IP
address 10.21.20.231
and Hostname Aruba-2930F-24G-PoEP-4SFPP connected, Group:unprovisioned,
Site:Bangalore Site",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612382562,
  "details": {
    "group": "1",
    "labels": "46",
  }
}
```

```

    "_rule_number": "0",
    "params": [
      "CN80HKW2Z6",
      "54:80:28:61:b3:20",
      "10.21.20.231",
      "Aruba-2930F-24G-PoEP-4SFPP"
    ],
    "serial": "CN80HKW2Z6",
    "time": "2021-02-03 20:02:42 UTC",
    "group_name": "unprovisioned",
    "site_name": "Bangalore Site"
  },
  "webhook": "8077a55e-f8d3-43af-a67f-12263f5b778e",
  "text": "New Switch with serial CN80HKW2Z6, MAC address 54:80:28:61:b3:20 IP address
10.21.20.231
and Hostname Aruba-2930F-24G-PoEP-4SFPP connected, Group:unprovisioned,
Site:Bangalore Site"
}

```

---

## Switch Memory Over Utilization

```

{
  "id": "AXdr9zozo68tULajS0Xo",
  "nid": 1301,
  "alert_type": "SWITCH_MEMORY_OVER_UTILIZATION",
  "setting_id": "f1ae23ba9025490cb53efb0993e05f17-1301",
  "device_id": "SG92GPT00K",
  "description": "Memory utilization for Switch with serial SG92GPT00K
has been above 1% for
about 5 minutes since 2021-02-04 07:30:00 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612424100,
  "details": {
    "name": "",
    "unit": "%",
    "serial": "SG92GPT00K",
    "group": "212",
    "_rule_number": "0",
    "ds_key": "f1ae23ba9025490cb53efb0993e05f17.SG92GPT00K.memory_utilization.5m",
    "duration": "5",
    "threshold": "1",
    "time": "2021-02-04 07:30:00 UTC"
  },
  "webhook": "8077a55e-f8d3-43af-a67f-12263f5b778e",
  "text": "Memory utilization for Switch with serial SG92GPT00K has been above 1% for
about 5 minutes since 2021-02-04 07:30:00 UTC"
}

```

---

## Switch CPU Over Utilization

```

{
  "id": "AXdrVwIbo68tULajSsgm",
  "nid": 1300,
  "alert_type": "SWITCH_CPU_OVER_UTILIZATION",
  "setting_id": "f1ae23ba9025490cb53efb0993e05f17-1300",
  "device_id": "SG53FLZ0RX",

```

```

"description": "CPU utilization for Switch HP-2920-48G-POEP with serial SG53FLZ0RX
has been
  above 1% for about 5 minutes since 2021-02-04 04:35:00 UTC.",
"state": "Open",
"severity": "Critical",
"operation": "create",
"timestamp": 1612413600,
"details": {
  "name": "HP-2920-48G-POEP",
  "unit": "%",
  "serial": "SG53FLZ0RX",
  "group": "211",
  "_rule_number": "0",
  "ds_key": "flae23ba9025490cb53efb0993e05f17.SG53FLZ0RX.cpu_utilization.5m",
  "duration": "5",
  "threshold": "1",
  "time": "2021-02-04 04:35:00 UTC"
},
"webhook": "8077a55e-f8d3-43af-a67f-12263f5b778e",
"text": "CPU utilization for Switch HP-2920-48G-POEP with serial SG53FLZ0RX has been
above 1% for about 5 minutes since 2021-02-04 04:35:00 UTC."
}

```

## Switch Interface Rx Rate

```

{
  "alert_type": "SWITCH_INTERFACE_RX_RATE",
  "description": "Receive rate for Interface 15 on Switch Aruba-2930F-24G-PoEP-4SFPP
has been
  above 1 % for about 5 minutes since 2019-09-26 13:18:00 UTC.",
  "timestamp": 1569504180,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1303",
  "state": "Open",
  "nid": 1303,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "max_value_for_percentage": "1000.0",
    "threshold": "1",
    "intf_name": "15",
    "time": "2019-09-26 13:18:00 UTC",
    "duration": "5",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.intf.rx_utilization.5m",
    "serial": "CN8AHKW095",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1tvTgBYu00gJ2 aoCg1",
  "severity": "Critical"
}

```

## Switch Interface Tx Rate

```

{
  "alert_type": "SWITCH_INTERFACE_TX_RATE",

```

```

"description": "Transfer rate for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP
has been
  above 1 % for about 5 minutes since 2019-09-26 13:18:00 UTC.",
"timestamp": 1569504180,
"webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
"setting_id": "e344d961bccd411dbd279bf92f61b989-1302",
"state": "Open",
"nid": 1302,
"details": {
  "_rule_number": "0",
  "group": "1",
  "name": "Aruba-2930F-24G-PoEP-4SFPP",
  "max_value_for_percentage": "1000.0",
  "threshold": "1",
  "intf_name": "19",
  "time": "2019-09-26 13:18:00 UTC",
  "duration": "5",
  "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.intf.tx_utilization.5m",
  "serial": "CN8AHKW095",
  "unit": "%"
},
"operation": "create",
"device_id": "CN8AHKW095",
"id": "AW1tvTgBYu0OgJ2aoCgk",
"severity": "Critical"
}

```

---

## Switch POE Utilization

```

{
  "alert_type": "SWITCH_POE_UTILIZATION",
  "description": "PoE utilization for Switch Aruba-2930F-24G-PoEP-4SFPP with serial
CN69HKW05T
  MAC address e0:07:1b:c4:8d:80 and IP address 10.22.182.78 has been above 1%",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}

```

---

## Switch Interface Input Errors

```

{

```

```
"alert_type": "SWITCH_INTERFACE_INPUT_ERRORS",
"description": "Input errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP
has been
  above 90% for about 30 minutes since 2019-09-26 06:07:00 UTC .",
"timestamp": 1569505920,
"webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
"setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
"state": "Open",
"nid": 1304,
"details": {
  "group": "0",
  "name": "Aruba-2930F-24G-PoEP-4SFPP",
  "ip": "10.22.182.78",
  "labels": [],
  "mac": "e0:07:1b:c4:8d:80",
  "time": "2019-09-26 13:52:00 UTC",
  "threshold": "1",
  "serial": "CN69HKW05T"
},
"operation": "create",
"device_id": "CN69HKW05T",
"id": "AW1t18ccYu0OgJ2aoDYw",
"severity": "Critical"
}
```

---

## Switch Interface Output Errors

```
{
  "alert_type": "SWITCH_INTERFACE_OUTPUT_ERRORS",
  "description": "Output errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-
4SFPP has been
  above 90% for about 30 minutes since 2019-09-26 06:07:00 UTC. ",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1305,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```

---

## Switch Mismatch Config

```
{
  "alert_type": "SWITCH_CONFIG_MISMATCH",
  "description": "Config mismatch occurred in switch with serial CN69HKW05T MAC
```

```

address e0:07:1b:c4:8d:80
  and IP address 10.22 .182 .78 and Hostname Aruba - 2930 F - 48 G - PoEP - 4 SFPP
",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 206,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}

```

---

## Switch Hardward Failure

```

{
  "alert_type": "SWITCH_HARDWARE_FAILURE",
  "description": "Switch with serial CN8AHKW095 : Fan 1 failed ",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 207,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}

```

---

## Switch Port Duplex Mode

```

{
  "id": "AXvFH4hFo68tULajPlc9",
  "nid": 1306,
  "alert_type": "SWITCH_INTERFACE_DUPLEX_MODE",
  "setting_id": "6ec75df161974434b54e298a353d11f3-1306",
  "device_id": "SG9ZKN7050",

```

```
"description": "Interface 1/1/2 on switch 6300 with serial
  SG9ZKN7050 is operating at Half-Duplex mode",
"state": "Open",
"severity": "Critical",
"operation": "create",
"timestamp": 1631099783,
"details": {
  "group": "2848",
  "labels": "",
  "name": "6300",
  "serial": "SG9ZKN7050",
  "intf_name": "1/1/2",
  "mode": "Half",
  "time": "2021-09-08 11:16:23 UTC"
},
"webhook": "76f4af2c-a47c-4726-b9d3-133c45e8f436",
"text": "Interface 1/1/2 on switch 6300 with serial
  SG9ZKN7050 is operating at Half-Duplex mode",
"cluster_hostname": "app-yoda.arubathena.com"
}
```

## Switch AOS-S Reboot

```
{
  "id": "AXt5CJ51o68tULaj30iP",
  "nid": 1312,
  "alert_type": "SWITCH_REBOOT",
  "setting_id": "flae23ba9025490cb53efb0993e05f17-1312",
  "device_id": "FFFWA7Y5B",
  "description": "Switch Aruba-3810M-24G-PoEP-1-slot  with FFFWA7Y5B on group -
  default
  rebooted. Reason: Operator reboot from Aruba CENTRAL session.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1629823213,
  "details": {
    "name": "Aruba-3810M-24G-PoEP-1-slot",
    "serial": "FFFWA7Y5B",
    "group_name": "default",
    "site_name": "",
    "reboot_reason": "Operator reboot from Aruba CENTRAL session.",
    "ts": "1629823080",
    "group": "0",
    "labels": "46",
    "time": "2021-08-24 16:40:13 UTC"
  },
  "webhook": "8077a55e-f8d3-43af-a67f-12263f5b778e",
  "text": "Switch Aruba-3810M-24G-PoEP-1-slot  with FFFWA7Y5B on group - default
  rebooted. Reason: Operator reboot from Aruba CENTRAL session."
}
```

## Switch STP Root Change

```
{
  "id": "AXt4qBL_fvwY_x8ol-sJ",
  "nid": 1308,
```



```

"alert_type": "SWITCH_STP_ROOT_CHANGE",
"setting_id": "417fc95887044bcba9b3e2ce3830aecb-1308",
"device_id": "QXRF011180",
"description": "CST Root changed on Sep 24 10:57:09 from Switch QXRF011180.
dummy with Serial: QXRF011180, IP Address: 75.200.87.30 and Priority: 24576 to
Switch 70:10:6f:84:0c:80 with Serial: QXRF011180, IP Address: 75.200.87.30 and
Priority 20480",
"state": "Open",
"severity": "Critical",
"operation": "create",
"timestamp": 1629816886,
"details": {
  "ts": "Sep 24 10:57:09",
  "pr1": "24576",
  "pr2": "20480",
  "host1": "QXRF011180.dummy",
  "host2": "70:10:6f:84:0c:80",
  "ip1": "75.200.87.30",
  "ip2": " ",
  "serial1": "QXRF011180",
  "serial2": " ",
  "type": "CST",
  "group": "16336",
  "labels": "5844",
  "serial": "QXRF011180",
  "time": "2021-08-24 14:54:46 UTC"
},
"webhook": "34000e8a-475c-46e3-9bec-79c5f281e868",
"text": "CST Root changed on Sep 24 10:57:09 from Switch QXRF011180.dummy with
Serial: QXRF011180, IP Address: 75.200.87.30 and Priority: 24576 to Switch
70:10:6f:84:0c:80
with Serial: QXRF011180, IP Address: 75.200.87.30 and Priority 20480
}

```

---

## Switch Uplink Port Over Utilization

```

{
  "id": "AXwISXRxuaNimYkpzKTQ",
  "nid": 1311,
  "alert_type": "SWITCH_UPLINK_PORT_OVER_UTILIZATION",
  "setting_id": "111952054-1311",
  "device_id": "SG87GYW05B",
  "description": "Uplink usage on Switch Aruba-3810M-24G-PoEP-1-slot
exceeded 2GB in 30 minutes",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1632226604,
  "details": {
    "name": "Aruba-3810M-24G-PoEP-1-slot",
    "duration": "30",
    "usage": "2",
    "site_str": "",
    "ts": "1632226604",
    "group": "1",
    "labels": "",
    "serial": "SG87GYW05B",
    "time": "2021-09-21 11:46:44 UTC"
  },
  "webhook": "e62eb85b-0547-4fba-9cfb-c8d36fb2b0c3",
  "text": "Uplink usage on Switch Aruba-3810M-24G-PoEP-1-slot

```

```
exceeded 2GB in 30 minutes",
"cluster_hostname": "sol-central.arubathena.com"
}
```

## AOS-CX Switch Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

### New Switch Connected

```
{
  "id": "AXdpfWeFo68tULajSfwu",
  "nid": 201,
  "alert_type": "New Switch Connected",
  "setting_id": "flae23ba9025490cb53efb0993e05f17-201",
  "device_id": "CN80HKW2Z6",
  "description": "New Switch with serial CN80HKW2Z6, MAC address 54:80:28:61:b3:20 IP
address 10.21.20.231
and Hostname Aruba-2930F-24G-PoEP-4SFPP connected, Group:unprovisioned,
Site:Bangalore Site",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612382562,
  "details": {
    "group": "1",
    "labels": "46",
    "_rule_number": "0",
    "params": [
      "CN80HKW2Z6",
      "54:80:28:61:b3:20",
      "10.21.20.231",
      "Aruba-2930F-24G-PoEP-4SFPP"
    ],
    "serial": "CN80HKW2Z6",
    "time": "2021-02-03 20:02:42 UTC",
    "group_name": "unprovisioned",
    "site_name": "Bangalore Site"
  },
  "webhook": "8077a55e-f8d3-43af-a67f-12263f5b778e",
  "text": "New Switch with serial CN80HKW2Z6, MAC address 54:80:28:61:b3:20 IP address
10.21.20.231
and Hostname Aruba-2930F-24G-PoEP-4SFPP connected, Group:unprovisioned,
Site:Bangalore Site"
}
```

### Switch Disconnected

```
{
  "id": "AXbhjMPpKHBn24BIWnGc",
  "nid": 203,
  "alert_type": "Switch Disconnected",
  "setting_id": "flae23ba9025490cb53efb0993e05f17-203",
  "device_id": "CN80HKW2Z6",
  "description": "Switch with serial CN80HKW2Z6, MAC address 54:80:28:61:b3:20 IP
address 10.21.20.231
and Hostname Aruba-2930F-24G-PoEP-4SFPP reconnected",
  "state": "Close",
}
```

```

"severity": "Major",
"operation": "update",
"timestamp": 1612383547,
"details": {
  "params": [
    "CN80HKW2Z6",
    "54:80:28:61:b3:20",
    "10.21.20.231",
    "Aruba-2930F-24G-PoEP-4SFPP",
    "",
    ""
  ],
  "serial": "CN80HKW2Z6",
  "time": "2021-01-08 10:31:07 UTC",
  "conn_status": "reconnected"
},
"webhook": "8077a55e-f8d3-43af-a67f-12263f5b778e",
"text": "Switch with serial CN80HKW2Z6, MAC address 54:80:28:61:b3:20 IP address
10.21.20.231
and Hostname Aruba-2930F-24G-PoEP-4SFPP reconnected"
}

```

---

## Switch Memory Over Utilization

```

{
  "id": "AXdr9zozo68tULajS0Xo",
  "nid": 1301,
  "alert_type": "SWITCH_MEMORY_OVER_UTILIZATION",
  "setting_id": "flae23ba9025490cb53efb0993e05f17-1301",
  "device_id": "SG92GPT00K",
  "description": "Memory utilization for Switch with serial SG92GPT00K
has been above 1% for
about 5 minutes since 2021-02-04 07:30:00 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612424100,
  "details": {
    "name": "",
    "unit": "%",
    "serial": "SG92GPT00K",
    "group": "212",
    "_rule_number": "0",
    "ds_key": "flae23ba9025490cb53efb0993e05f17.SG92GPT00K.memory_utilization.5m",
    "duration": "5",
    "threshold": "1",
    "time": "2021-02-04 07:30:00 UTC"
  },
  "webhook": "8077a55e-f8d3-43af-a67f-12263f5b778e",
  "text": "Memory utilization for Switch with serial SG92GPT00K has been above 1% for
about 5 minutes since 2021-02-04 07:30:00 UTC"
}

```

---

## Switch CPU Over Utilization

```

{
  "id": "AXdrVwIbo68tULajSsgm",
  "nid": 1300,

```

```

"alert_type": "SWITCH_CPU_OVER_UTILIZATION",
"setting_id": "flae23ba9025490cb53efb0993e05f17-1300",
"device_id": "SG53FLZ0RX",
"description": "CPU utilization for Switch HP-2920-48G-POEP with serial SG53FLZ0RX
has been
  above 1% for about 5 minutes since 2021-02-04 04:35:00 UTC.",
"state": "Open",
"severity": "Critical",
"operation": "create",
"timestamp": 1612413600,
"details": {
  "name": "HP-2920-48G-POEP",
  "unit": "%",
  "serial": "SG53FLZ0RX",
  "group": "211",
  "_rule_number": "0",
  "ds_key": "flae23ba9025490cb53efb0993e05f17.SG53FLZ0RX.cpu_utilization.5m",
  "duration": "5",
  "threshold": "1",
  "time": "2021-02-04 04:35:00 UTC"
},
"webhook": "8077a55e-f8d3-43af-a67f-12263f5b778e",
"text": "CPU utilization for Switch HP-2920-48G-POEP with serial SG53FLZ0RX has been
  above 1% for about 5 minutes since 2021-02-04 04:35:00 UTC."
}

```

---

## Switch Interface Rx Rate

```

{
  "alert_type": "SWITCH_INTERFACE_RX_RATE",
  "description": "Receive rate for Interface 15 on Switch Aruba-2930F-24G-PoEP-4SFPP
has been
  above 1 % for about 5 minutes since 2019-09-26 13:18:00 UTC.",
  "timestamp": 1569504180,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1303",
  "state": "Open",
  "nid": 1303,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "max_value_for_percentage": "1000.0",
    "threshold": "1",
    "intf_name": "15",
    "time": "2019-09-26 13:18:00 UTC",
    "duration": "5",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.intf.rx_utilization.5m",
    "serial": "CN8AHKW095",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1tvTgBYu0OgJ2 aoCg1",
  "severity": "Critical"
}

```

---

## Switch Interface Tx Rate

```

{
  "alert_type": "SWITCH_INTERFACE_TX_RATE",
  "description": "Transfer rate for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP
has been
  above 1 % for about 5 minutes since 2019-09-26 13:18:00 UTC.",
  "timestamp": 1569504180,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1302",
  "state": "Open",
  "nid": 1302,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "max_value_for_percentage": "1000.0",
    "threshold": "1",
    "intf_name": "19",
    "time": "2019-09-26 13:18:00 UTC",
    "duration": "5",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.intf.tx_utilization.5m",
    "serial": "CN8AHKW095",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1tvTgBYu0OgJ2aoCgk",
  "severity": "Critical"
}

```

---

## Switch POE Utilization

```

{
  "alert_type": "SWITCH_POE_UTILIZATION",
  "description": "PoE utilization for Switch Aruba-2930F-24G-PoEP-4SFPP with serial
CN69HKW05T
  MAC address e0:07:1b:c4:8d:80 and IP address 10.22.182.78 has been above 1%",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}

```

---

## Switch Interface Input Errors

```
{
  "alert_type": "SWITCH_INTERFACE_INPUT_ERRORS",
  "description": "Input errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP
has been
  above 90% for about 30 minutes since 2019-09-26 06:07:00 UTC .",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1304,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```

---

## Switch Interface Output Errors

```
{
  "alert_type": "SWITCH_INTERFACE_OUTPUT_ERRORS",
  "description": "Output errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-
4SFPP has been
  above 90% for about 30 minutes since 2019-09-26 06:07:00 UTC. ",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1305,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```

---

## Switch Config Mismatch

```
{
  "alert_type": "SWITCH_CONFIG_MISMATCH",
```

```

    "description": "Config mismatch occurred in switch with serial CN69HKW05T MAC
address e0:07:1b:c4:8d:80
    and IP address 10.22 .182 .78 and Hostname Aruba - 2930 F - 48 G - PoEP - 4 SFPP
",
    "timestamp": 1569505920,
    "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
    "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
    "state": "Open",
    "nid": 206,
    "details": {
        "group": "0",
        "name": "Aruba-2930F-24G-PoEP-4SFPP",
        "ip": "10.22.182.78",
        "labels": [],
        "mac": "e0:07:1b:c4:8d:80",
        "time": "2019-09-26 13:52:00 UTC",
        "threshold": "1",
        "serial": "CN69HKW05T"
    },
    "operation": "create",
    "device_id": "CN69HKW05T",
    "id": "AW1t18ccYu0OgJ2aoDYw",
    "severity": "Critical"
}

```

## Switch Hardware Failure

```

{
    "id": "AXvJXn_oo68tULajUT9W",
    "nid": 207,
    "alert_type": "SWITCH_HARDWARE_FAILURE",
    "setting_id": "6ec75df161974434b54e298a353d11f3-207",
    "device_id": "SG9ZKN7078",
    "description": "Switch with serial SG9ZKN7078 : eMMC storage reached
critical utilization level.Please contact HPE Aruba support for further
assistance.",
    "state": "Open",
    "severity": "Critical",
    "operation": "create",
    "timestamp": 1631171018,
    "details": {
        "group": "1",
        "labels": "",
        "serial": "SG9ZKN7078",
        "name": "6300",
        "site": "",
        "device_id": "SG9ZKN7078",
        "hostname": "6300",
        "description": "eMMC storage reached critical utilization level.Please contact
HPE Aruba support for further assistance.",
        "event_id": "9104",
        "time": "2021-09-09 07:03:38 UTC"
    },
    "webhook": "5ef178b6-4916-46e6-bed2-ab61a8cd7271",
    "text": "Switch with serial SG9ZKN7078 : eMMC storage reached critical utilization
level.Please contact HPE Aruba support for further assistance.",
    "cluster_hostname": "app-yoda.arubathena.com"
}

```

## Switch NAE Status

```

{
  "id": "AXs01pfTKYUYZt8Vft9m",
  "nid": 208,
  "alert_type": "Switch NAE Status",
  "setting_id": "424a17fea2a24d46859a33699cd6b3d4-208",
  "device_id": "SG9ZEFB7F2",
  "description": "Aggregated NAE status reached or exceeds the desired severity level
for the switch with
  serial SG9ZEFB7F2 MAC address 70:72:cf:ef:b7:f2 IP address 10.101.60.40 and
  Hostname 6300",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1628679083,
  "details": {
    "group": "1",
    "labels": "",
    "serial": "SG9ZEFB7F2",
    "name": "{\\'hostname\\': \\'6300\\'}",
    "site": "",
    "device_id": "SG9ZEFB7F2",
    "mac": "70:72:cf:ef:b7:f2",
    "ip": "10.101.60.40",
    "hostname": "6300",
    "time": "2021-08-11 10:51:23 UTC"
  },
  "webhook": "b18819a2-75a1-4bf8-951e-037b9fd1914a",
  "text": "Aggregated NAE status reached or exceeds the desired severity level for the
switch with
  serial SG9ZEFB7F2 MAC address 70:72:cf:ef:b7:f2 IP address 10.101.60.40 and
  Hostname 6300"
}

```

## Switch Stack Commander Change

```

{
  "id": "AXvGFP59KFHq3kj2r0Ju",
  "nid": 1310,
  "alert_type": "SWITCH_STACK_COMMANDER_CHANGE",
  "setting_id": "698e8e55b6294a7daf4de0f80f51b231-1310",
  "device_id": "SG9ZKN709Y",
  "description": "New Commander with Serial ID: SG9ZKN70B5,
  MAC Address: 38:21:c7:5c:c4:c0, Hostname: Commander,
  Stack ID: 6a9cb0fb-2346-48df-a0c4-90237ea71afa, Group: 322 Connected,
  Old Commander Serial ID: SG9ZKN709Y, Mac Address: 38:21:c7:5d:70:c0",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1631115869,
  "details": {
    "old_serial": "SG9ZKN709Y",
    "old_mac": "38:21:c7:5d:70:c0",
    "new_serial": "SG9ZKN70B5",
    "new_mac": "38:21:c7:5c:c4:c0",
    "host": "Commander",
    "stack_id": "6a9cb0fb-2346-48df-a0c4-90237ea71afa",
    "group": "322",
    "labels": "",
    "serial": "SG9ZKN709Y",
    "time": "2021-09-08 15:44:29 UTC"
  },
}

```



```

"webhook": "374b4438-dff9-464c-a03e-a781c6c9a68f",
"text": "New Commander with Serial ID: SG9ZKN70B5,
MAC Address: 38:21:c7:5c:c4:c0, Hostname: Commander,
Stack ID: 6a9cb0fb-2346-48df-a0c4-90237ea71afa, Group: 322 Connected,
Old Commander Serial ID: SG9ZKN709Y, Mac Address: 38:21:c7:5d:70:c0"
}

```

---

## Stack Member Added

```

{
  "id": "AXvGRNvsKFHq3kj2rOYF",
  "nid": 1309,
  "alert_type": "SWITCH_STACK_MEMBER_ADDED_REMOVED",
  "setting_id": "698e8e55b6294a7daf4de0f80f51b231-1309",
  "device_id": "SG9ZKN702T",
  "description": "Stack Member with Serial ID: SG9ZKN702T,
MAC Address: 38:21:c7:5a:c5:80, Member ID: 4 and Role: ['Member']
Added To stack with Hostname: 6300, Stack ID: 6a9cb0fb-2346-48df-a0c4-
90237ea71afa",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1631119006,
  "details": {
    "serial": "SG9ZKN702T",
    "mac": "38:21:c7:5a:c5:80",
    "mem_id": "4",
    "role": [
      "Member"
    ],
    "action": "Added To",
    "host": "6300",
    "stack_id": "6a9cb0fb-2346-48df-a0c4-90237ea71afa",
    "group": "326",
    "time": "2021-09-08 16:36:46 UTC"
  },
  "webhook": "374b4438-dff9-464c-a03e-a781c6c9a68f",
  "text": "Stack Member with Serial ID: SG9ZKN702T,
MAC Address: 38:21:c7:5a:c5:80, Member ID: 4 and Role: ['Member']
Added To stack with Hostname: 6300, Stack ID: 6a9cb0fb-2346-48df-a0c4-90237ea71afa"
}

```

---

## Stack Member Removed

```

{
  "id": "AXvGQ0JcKFHq3kj2rOXu",
  "nid": 1309,
  "alert_type": "SWITCH_STACK_MEMBER_ADDED_REMOVED",
  "setting_id": "698e8e55b6294a7daf4de0f80f51b231-1309",
  "device_id": "SG9ZKN702T",
  "description": "Stack Member with Serial ID: SG9ZKN702T,
MAC Address: , Member ID: 4 and Role: ['Member'] Removed
From stack with Hostname: 6300, Stack ID: 6a9cb0fb-2346-48df-a0c4-90237ea71afa",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1631118901,
  "details": {
    "serial": "SG9ZKN702T",

```

```

    "mac": "",
    "mem_id": "4",
    "role": [
      "Member"
    ],
    "action": "Removed From",
    "host": "6300",
    "stack_id": "6a9cb0fb-2346-48df-a0c4-90237ea71afa",
    "group": "326",
    "time": "2021-09-08 16:35:01 UTC"
  },
  "webhook": "374b4438-dff9-464c-a03e-a781c6c9a68f",
  "text": "Stack Member with Serial ID: SG9ZKN702T,
  MAC Address: , Member ID: 4 and Role: ['Member'] Removed From stack with
  Hostname: 6300, Stack ID: 6a9cb0fb-2346-48df-a0c4-90237ea71afa"
}

```

## Stack Member Is Down In

```

{
  "id": "AXvGQ0JcKFHq3kj2rOXu",
  "cid": "3122e38585dc611ee96af8e3a091b384f",
  "nid": 1309,
  "alert_type": "SWITCH_STACK_MEMBER_ADDED_REMOVED",
  "setting_id": "698e8e55b6294a7daf4de0f80f51b231-1309",
  "device_id": "SG42L52016",
  "description": "Stack Member with Serial ID: SG42L52016,
  MAC Address: , Member ID: 4 and Role: ['Member'] Removed
  From stack with Hostname: 6300, Stack ID: 6a9cb0fb-2346-48df-a0c4-90237ea71afa",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1631118901,
  "details": {
    "__base_url": "https://xyz.hpe.com",
    "serial": "SG42L52016",
    "mac": "",
    "mem_id": "4",
    "role": [
      "Member"
    ],
    "action": "Removed From",
    "host": "6300",
    "stack_id": "6a9cb0fb-2346-48df-a0c4-90237ea71afa",
    "group": "326",
    "time": "2021-09-08 16:35:01 UTC"
  },
  "webhook": "374b4438-dff9-464c-a03e-a781c6c9a68f",
  "text": "Stack Member with Serial ID: SG42L52016,
  MAC Address: , Member ID: 4 and Role: ['Member'] Removed From stack with
  Hostname: 6300, Stack ID: 6a9cb0fb-2346-48df-a0c4-90237ea71afa"
}

```

## Switch Port Duplex Mode

```

{
  "id": "AXvFH4hFo68tULajP1c9",
  "nid": 1306,

```

```

"alert_type": "SWITCH_INTERFACE_DUPLEX_MODE",
"setting_id": "6ec75df161974434b54e298a353d11f3-1306",
"device_id": "SG9ZKN7050",
"description": "Interface 1/1/2 on switch 6300 with serial
SG9ZKN7050 is operating at Half-Duplex mode",
"state": "Open",
"severity": "Critical",
"operation": "create",
"timestamp": 1631099783,
"details": {
  "group": "2848",
  "labels": "",
  "name": "6300",
  "serial": "SG9ZKN7050",
  "intf_name": "1/1/2",
  "mode": "Half",
  "time": "2021-09-08 11:16:23 UTC"
},
"webhook": "76f4af2c-a47c-4726-b9d3-133c45e8f436",
"text": "Interface 1/1/2 on switch 6300 with serial
SG9ZKN7050 is operating at Half-Duplex mode",
"cluster_hostname": "app-yoda.arubathena.com"
}

```

## Gateway Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

### BGP Neighbor Route Limit

```

{
  "id": "AXeDCfY2o68tULajXkth",
  "nid": 1358,
  "alert_type": "CONTROLLER BGP NEIGHBOR ROUTE LIMIT",
  "setting_id": "a847a3aea73d4ba7b34c00323fb9ee7a-1358",
  "device_id": "CV0012105",
  "description": "BGP neighbor 172.30.1.102 route limit exceeded on device
MDC1-VPNC1-KSA-03_E1_A0(router_id=10.53.9.44, ASN=3002, serial=CV0012105,
limit=1,action=warning)",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612811204,
  "details": {
    "serial": "CV0012105",
    "action": "warning",
    "hostname": "MDC1-VPNC1-KSA-03_E1_A0",
    "limit": "1",
    "nbr_addr": "172.30.1.102",
    "nbr_id": "10.53.9.44",
    "nbr_as": "3002",
    "group": "12",
    "time": "2021-02-08 19:06:44 UTC"
  },
  "webhook": "f6f2b19a-31d5-445c-b340-eb1ca8a6fdd8",
  "text": "BGP neighbor 172.30.1.102 route limit exceeded on device
MDC1-VPNC1-KSA-03_E1_A0(router_id=10.53.9.44, ASN=3002, serial=CV0012105,
limit=1,action=warning)"
}

```

### CFG-SET Advertisement Failure

```
{
  "id": "AXdnqE9jo68tULajSR8X",
  "nid": 1554,
  "alert_type": "CFG_SET_ADVERTISEMENT_FAILURE",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1554",
  "device_id": "BIM0010001",
  "description": "CFG-Set advertisement failure for Gateway BIM0010001 with serial BIM0010001 on tunnel default-local-vpnip-data-ipsecmap-00:1a:1e:04:27:48-link6 from 10.1.1.1 to 200.1.1.6",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612351819,
  "details": {
    "src_ip": "10.1.1.1",
    "dst_ip": "200.1.1.6",
    "alias_map_name": "default-local-vpnip-data-ipsecmap-00:1a:1e:04:27:48-link6",
    "map_name": "default-local-vpnip-data-ipsecmap-00:1a:1e:04:27:48-link6",
    "hostname": "BIM0010001",
    "serial": "BIM0010001",
    "group": "0",
    "labels": [],
    "time": "2021-02-03 11:30:19 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "CFG-Set advertisement failure for Gateway BIM0010001 with serial BIM0010001 on tunnel default-local-vpnip-data-ipsecmap-00:1a:1e:04:27:48-link6 from 10.1.1.1 to 200.1.1.6"
}
```

---

## BGP Session Error

```
{
  "id": "AXeCfcXbbbaB9p462rCU",
  "nid": 1355,
  "alert_type": "CONTROLLER_BGP_SESSION_ERROR",
  "setting_id": "417fc95887044bcba9b3e2ce3830a ECB-1355",
  "device_id": "DL0002986",
  "description": "BGP neighbor 103.1.1.2 is down (router-id=197.0.0.3, ASN=103, serial=DL0002986)",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612802016,
  "details": {
    "serial": "DL0002986",
    "nbr_addr": "103.1.1.2",
    "nbr_as": "103",
    "nbr_id": "197.0.0.3",
    "group": "57",
    "time": "2021-02-08 16:33:36 UTC"
  },
  "webhook": "5cbc87e4-9eb5-45d2-b890-b21db89ca5b4",
  "text": "BGP neighbor 103.1.1.2 is down (router-id=197.0.0.3, ASN=103, serial=DL0002986)"
}
```

---

## EST Enrolment Failure

```

{
  "id": "AXvSPH4-Kzx3k2rgh7",
  "nid": 1701,
  "alert_type": "EST enrollment failure",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1504",
  "device_id": "CZ0003243",
  "description": " EST enrollment failure for Virtual Gateway with
    name : 7024-HF-254, serial :CZ0003243, mac :00:0b:86:f9:0d:d1.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1648194475,
  "details": {
    "mac": "00:0b:86:f9:0d:d1",
    "hostname": "7024-HF-254",
    "serial": "CZ0003243",
    "group": "6",
    "labels": "2",
    "_rule_number": "0",
    "params": "",
    "time": "2022-03-25 13:17:51 UTC"
  },
  "webhook": "87fae42a-78ec-45c0-a22a-4f81417cad56",
  "text": "EST enrollment failure for Virtual Gateway with
    name : 7024-HF-254, serial :CZ0003243, mac :00:0b:86:f9:0d:d1."
}

```

---

## Gateway CPU Utilization

```

{
  "id": "AXdi7ppYo68tULajRvEA",
  "nid": 1351,
  "alert_type": "CONTROLLER_CPU_OVER_UTILIZATION",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1351",
  "device_id": "CNJJKLB0HB",
  "description": "CPU utilization for Gateway WTH_9004-2 with serial CNJJKLB0HB has
    been
    above 10% for about 5 minutes since 2021-02-02 13:24:00 UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612272540,
  "details": {
    "name": "WTH_9004-2",
    "unit": "%",
    "serial": "CNJJKLB0HB",
    "group": "36",
    "labels": "8",
    "_rule_number": "0",
    "ds_key": "6039f9543bac449291bfcd19eb10d1eb.CNJJKLB0HB.cpu_utilization.5m",
    "duration": "5",
    "threshold": "10",
    "time": "2021-02-02 13:24:00 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "CPU utilization for Gateway WTH_9004-2 with serial CNJJKLB0HB has been
    above 10% for about 5 minutes since 2021-02-02 13:24:00 UTC."
}

```

---

## Gateway Emergency Mode

```

{
  "id": "AXdjJsYpo68tULajRXTU",
  "nid": 1353,
  "alert_type": "CONTROLLER_EMERGENCY_UP_LINK_MODE",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1353",
  "device_id": "BIM0010002",
  "description": "Gateway BIM0010002 with serial BIM0010002 is operating on emergency
mode
  at 2021-02-02 14:30:21 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612276221,
  "details": {
    "name": "BIM0010002",
    "serial": "BIM0010002",
    "group": "0",
    "labels": [],
    "time": "2021-02-02 14:30:21 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "Gateway BIM0010002 with serial BIM0010002 is operating on emergency mode at
2021-02-02 14:30:21 UTC"
}

```

## VGW VM Down

```

{
  "id": "AXeBVwDSXFtba20Mo_fm",
  "nid": 1702,
  "alert_type": "VGW_HEALTH_STATE_CHANGE_DETECTED",
  "setting_id": "417fc95887044bcba9b3e2ce3830aecb-1702",
  "device_id": "VG2101216619",
  "description": "VGW VM DOWN -- User: jagwani.karan+aruba@gmail.com Cloud-Account:
Karan-Azure
  Cloud-Provider: Azure Region-Id: canadacentral VPC-Id: /karan_res_
canada/canadavnet VM-Id:
  /subscriptions/2bf1e338-5361-470d-bcba-78c50b2b7f16/resourceGroups/karan_res_
canada/providers/Microsoft.
  Compute/virtualMachines/ArubaVGW-92-1A-3A Serial-Number: VG2101216619 Mac-Address:
02:1A:1E:92:1A:3A",
  "state": "Open",
  "severity": "Major",
  "operation": "create",
  "timestamp": 1612782698,
  "details": {
    "account_id": "4c0116d9-a26b-4b4b-8be0-350631e434be",
    "mac": "02:1A:1E:92:1A:3A",
    "serial": "VG2101216619",
    "vm_id": "/subscriptions/2bf1e338-5361-470d-bcba-
78c50b2b7f16/resourceGroups/karan_res_canada
  /providers/Microsoft.Compute/virtualMachines/ArubaVGW-92-1A-3A",
    "account_name": "Karan-Azure",
    "region_id": "canadacentral",
    "customer_name": "jagwani.karan+aruba@gmail.com",
    "health": "DOWN",
    "vpc_id": "/karan_res_canada/canadavnet",
    "provider_name": "Azure",
    "customer_id": "417fc95887044bcba9b3e2ce3830aecb",
    "time": "2021-02-08 11:11:38 UTC"
  },
}

```

```
"webhook": "5cbc87e4-9eb5-45d2-b890-b21db89ca5b4",
"text": "VGW VM DOWN -- User: jagwani.karan+aruba@gmail.com Cloud-Account: Karan-
Azure
  Cloud-Provider: Azure Region-Id: canadacentral VPC-Id: /karan_res_
canada/canadavnet VM-Id:
  /subscriptions/2bf1e338-5361-470d-bcba-78c50b2b7f16/resourceGroups/karan_res_
canada/providers/Microsoft.
  Compute/virtualMachines/ArubaVGW-92-1A-3A Serial-Number: VG2101216619 Mac-Address:
02:1A:1E:92:1A:3A"
}
```

---

## VPN Peer Failover

```
{
  "id": "AXvSPH4-Kzxaq3kj2rgh7",
  "nid": 1504,
  "alert_type": "WAN_UPLINK_LOAD_BALANCE_VPNC_PEER_FAILOVER",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1504",
  "device_id": "CZ0003243",
  "description": " VPN peer failover for gateway 7024-HF-254 with serial CZ0003243",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1648061695,
  "details": {
    "mac": "00:0b:86:f9:0d:d1",
    "hostname": "7024-HF-254",
    "serial": "CZ0003243",
    "group": "6",
    "labels": "2",
    "_rule_number": "0",
    "params": "",
    "time": "2022-03-23 00:24:51 UTC"
  },
  "webhook": "87fae42a-78ec-45c0-a22a-4f81417cad56",
  "text": "VPN peer failover for gateway 7024-HF-254 with serial CZ0003243"
}
```

---

## Gateway Memory Utilization

```
{
  "id": "AXdiyfwQo68tULajRTiG",
  "nid": 1352,
  "alert_type": "CONTROLLER_MEMORY_OVER_UTILIZATION",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1352",
  "device_id": "CNJJKLB0G6",
  "description": "Memory utilization for Gateway WTH_9004-1 with serial CNJJKLB0G6 has
been
  above 30% for about 30 minutes since 2021-02-02 12:19:00 UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612270140,
  "details": {
    "name": "WTH_9004-1",
    "unit": "%",
    "serial": "CNJJKLB0G6",
    "group": "36",
    "labels": "8",
  }
}
```

---

```
    "_rule_number": "0",
    "ds_key": "6039f9543bac449291bfcd19eb10d1eb.CNJJCLB0G6.memory_utilization.5m",
    "duration": "30",
    "threshold": "30",
    "time": "2021-02-02 12:19:00 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "Memory utilization for Gateway WTH_9004-1 with serial CNJJCLB0G6 has been
  above 30% for about 30 minutes since 2021-02-02 12:19:00 UTC."
}
```

---

## OSPF Session Error

```
{
  "alert_type": "CONTROLLER OSPF SESSION ERROR",
  "description": "OSPF session state change for Gateway with hostname GSK_VPNC2 and
  serial CW0003307 from Init State to Down State
  for neighbor 1.0.0.2 on interface 100 with reason No hello packets received from
  neighbour.Inactivity timer fired",
  "timestamp": 1564121712,
  "webhook": "60785e88-9513-4352-94d6-ec25fedbeddc",
  "setting_id": "b27f67fa44234c51a890fccea7c9b83e-1354",
  "state": "Open",
  "nid": 1354,
  "details": {
    "dst_state": "Down State",
    "neighbour_ip": "1.0.0.2",
    "group": "4",
    "uniq_identifier": "100-16777218",
    "labels": [
      "2",
      "11",
      "12",
      "15",
      "13",
      "8"
    ],
    "src_state": "Init State",
    "reason": "No hello packets received from neighbour.Inactivity timer fired",
    "time": "2019-07-26 06:15:12 UTC",
    "interface": "100",
    "serial": "CW0003307",
    "hostname": "GSK_VPNC2"
  },
  "operation": "create",
  "device_id": "CW0003307",
  "id": "AWws60Yxon2R5PyMmUU4",
  "severity": "Major"
}
```

---

## DHCP Pool Consumption Alert

```
{
  "alert_type": "DHCP_POOL_CONSUMPTION_ALERT",
  "description": "DHCP Pool Consumption on Gateway CNHKL031 is 12% at 2019-07-25
  13:02:39 UTC for 192.168.53.0/24",
  "timestamp": 1564059759,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d66ff223f-1510",
}
```



```

"state": "Open",
"nid": 1510,
"details": {
  "subnet": "192.168.53.0/24",
  "group": "77",
  "name": "None",
  "labels": "8,661",
  "time": "2019-07-25 13:02:39 UTC",
  "threshold": "12",
  "serial": "CNHHKLB031",
  "unit": "%"
},
"operation": "create",
"device_id": "CNHHKLB031",
"id": "AWwpOfQAVQO1ZtiGiE2H",
"severity": "Critical"
}

```

---

## SLA DPS Compliance Alert

```

{
  "ack_by": null,
  "ack_ts": 1579828824000,
  "acknowledge": 0,
  "cid": "201804172180",
  "description": "SLA DPS Compliance Violations for Customer : aruba, Device Hostname :
bg2-ha2, Policy : all,
  Uplink : 400_lte, Probe Ip: 52.52.253.87, Threshold Profile : {u'dps_threshold_
profile_name': u'BestForInternet',
  u'dps_threshold_profile_packet_loss_value': 1, u'dps_threshold_profile_bw_util_
value': 80,
  u'dps_threshold_profile_latency_value': 1}, Violation Reason: Latency, Violation
Value: 1.363ms",
  "group_name": "",
  "id": "AW_VItEnenGOhQ4XrMp_",
  "labels": [],
  "nid": 20,
  "severity": 5,
  "sites": [
    {
      "id": 38,
      "name": "site_2"
    }
  ],
  "ts": 1579828824000,
  "type": "DPS_COMPLIANCE_ALERT",
  "type_desc": "SLA DPS Compliance Violations"
}

```

---

## Gateway Joining Cluster

```

{
  "id": "AXd9xwjio68tULajWyCm",
  "nid": 1802,
  "alert_type": "GATEWAY_CONNECTED_TO_CLUSTER",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1802",
  "device_id": "None",
  "description": "Gateway with name: c2c-7010-4-1 and serial: CG0020729 joined

```

```
  cluster: C2C-253-YODA.",
  "state": "Open",
  "severity": "Warning",
  "operation": "create",
  "timestamp": 1612722931,
  "details": {
    "group": "278",
    "labels": [],
    "name": "c2c-7010-4-1",
    "serial": "None",
    "gateway": "CG0020729",
    "cluster_name": "C2C-253-YODA",
    "alert_key": "CG0020729",
    "time": "2021-02-07 18:35:31 UTC"
  },
  "webhook": "52e0abbd-cdda-45f2-bd68-3107fef43841",
  "text": "Gateway with name: c2c-7010-4-1 and serial: CG0020729 joined
  cluster: C2C-253-YODA."
}
```

---

## Gateway Leaving Cluster

```
{
  "id": "AXd9vPKro68tULajWxzi",
  "nid": 1803,
  "alert_type": "GATEWAY_DISCONNECTED_FROM_CLUSTER",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1803",
  "device_id": "54",
  "description": "Gateway with name: c2c-7010-4-1 and serial: CG0020729 left
  cluster: C2C-253-YODA.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612722270,
  "details": {
    "group": "278",
    "labels": [],
    "name": "c2c-7010-4-1",
    "serial": "54",
    "gateway": "CG0020729",
    "cluster_name": "C2C-253-YODA",
    "alert_key": "CG0020729",
    "time": "2021-02-07 18:24:30 UTC"
  },
  "webhook": "52e0abbd-cdda-45f2-bd68-3107fef43841",
  "text": "Gateway with name: c2c-7010-4-1 and serial: CG0020729 left
  cluster: C2C-253-YODA."
}
```

---

## Gateway Cluster Leader Change

```
{
  "id": "AXd9wglqo68tULajWx7a",
  "nid": 1804,
  "alert_type": "GATEWAY_CLUSTER_LEADER_CHANGE",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1804",
  "device_id": "54",
  "description": "Gateway with name: c2c-7010-3 and serial: CG0021234 became the
```

```

leader of
  cluster: C2C-253-YODA.",
  "state": "Open",
  "severity": "Minor",
  "operation": "create",
  "timestamp": 1612722604,
  "details": {
    "group": "278",
    "labels": [],
    "name": "c2c-7010-3",
    "serial": "54",
    "gateway": "CG0021234",
    "cluster_name": "C2C-253-YODA",
    "alert_key": "CG0021234",
    "time": "2021-02-07 18:30:04 UTC"
  },
  "webhook": "52e0abbd-cdda-45f2-bd68-3107fef43841",
  "text": "Gateway with name: c2c-7010-3 and serial: CG0021234 became the leader of
cluster: C2C-253-YODA."
}

```

---

## Gateway Cluster Client Capacity

```

{
  "id": "AXvSPH4-Kzxaq3kj2rgh7",
  "nid": 1805,
  "alert_type": "GATEWAY_CLUSTER_CLIENT_CAPACITY_EXCEEDED",
  "setting_id": "6039f9543bac449291bfcd19eb10dleb-1805",
  "device_id": "CZ0003243",
  "description": " Client Capacity for Gateway Cluster C2C-254
has been above 90% for about 30 minutes since 2022-03-24 16:14:00 UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1648095240,
  "details": {
    "mac": "00:0b:86:f9:0d:d1",
    "hostname": "7024-HF-254",
    "serial": "CZ0003243",
    "group": "6",
    "labels": "2",
    "_rule_number": "0",
    "params": "",
    "time": "2021-09-11 00:24:51 UTC"
  },
  "webhook": "87fae42a-78ec-45c0-a22a-4f81417cad56",
  "text": "Client Capacity for Gateway Cluster C2C-254 has been above
90% for about 30 minutes since 2022-03-24 16:14:00 UTC"
}

```

---

## Gateway Base License Capacity Limit Exceeded

```

{
  "id": "AXdr-dsfo68tULajS0bj",
  "nid": 1356,
  "alert_type": "GATEWAY_BASE_LICENSE_CAPACITY_EXCEEDED",
  "setting_id": "6039f9543bac449291bfcd19eb10dleb-1356",
  "device_id": "SCA0000073",
  "description": "Base license capacity limit exceeded for Gateway with

```

```
  name: CSIM_SCA0000073, serial: SCA0000073",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612424272,
  "details": {
    "group": "0",
    "labels": [],
    "name": "CSIM_SCA0000073",
    "serial": "SCA0000073",
    "time": "2021-02-04 07:37:52 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "Base license capacity limit exceeded for Gateway with
  name: CSIM_SCA0000073, serial: SCA0000073"
}
```

## Gateway Threat Count

```
{
  "alert_type": "GW_IDS_IPS_ALERT_THREAT_OVER_A_PERIOD",
  "id": "AXX7N0IhaFBUFq6FQ2R1",
  "nid": 2305,
  "setting_id": "8fc0df01a43b42aa9f8e9fbc3d3b9d35-2305",
  "device_id": "TWJ6KSP005",
  "description": "Aruba Branch Gateway aruba9004_lte with serial number TWJ6KSP005
  exceeded 50 threat events in last 10 minutes",
  "state": "Close",
  "severity": "Critical",
  "operation": "update",
  "timestamp": 1606238738,
  "details__threshold": 50,
  "details__agg_field_name": "device",
  "details__duration": 10,
  "details__device": "TWJ6KSP005",
  "details__severity": "CRITICAL",
  "details__rule_id": 0,
  "details__serial": "TWJ6KSP005",
  "details__name": "aruba9004_lte",
  "details__group_id": 73,
  "details__time": "2020-11-24 16:55:04 UTC",
  "webhook": "001378a5-bfb1-465e-a955-0034ef801136",
  "text": "Aruba Branch Gateway aruba9004_lte with serial number TWJ6KSP005
  exceeded 50 threat events in last 10 minutes"
}
```

## Gateway Disconnected

```
{
  "id": "AXdmLPpwo68tULajSch_",
  "nid": 303,
  "alert_type": "GATEWAY_DISCONNECTED",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-303",
  "device_id": "CNJJKLB0NZ",
  "description": "Gateway WTH-9004-3 with serial CNJJKLB0NZ, MAC address
  20:4c:03:b1:e0:22 and
  IP address 192.168.142.2 disconnected. , Group:UTM, Site:UTM",
  "state": "Open",
}
```

```

"severity": "Critical",
"operation": "create",
"timestamp": 1612326959,
"details": {
  "params": [
    "CNJJKLB0NZ",
    "20:4c:03:b1:e0:22",
    "192.168.142.2",
    "WTH-9004-3",
    "",
    ""
  ],
  "group": "36",
  "ts": "1612326547369",
  "labels": "8",
  "serial": "CNJJKLB0NZ",
  "conn_status": "disconnected",
  "time": "2021-02-03 04:35:59 UTC",
  "group_name": "UTM",
  "site_name": "UTM"
},
"webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
"text": "Gateway WTH-9004-3 with serial CNJJKLB0NZ, MAC address 20:4c:03:b1:e0:22
and
IP address 192.168.142.2 disconnected. , Group:UTM, Site:UTM"
}

```

---

## Gateway Threat Count per User

```

{
  "id": "AXdr6Yf3o68tULajSz5Z",
  "nid": 2308,
  "alert_type": "GW_IDS_IPS_ALERT_THREAT_USER_OVER_A_PERIOD",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-2306",
  "device_id": "2821300",
  "description": "Threat events for user id emp52342
exceeded the threshold 50 in last 10 minutes.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612423202,
  "details": {
    "threshold": "50",
    "agg_field_name": "user",
    "duration": "10",
    "rule_id": "0",
    "severity": "CRITICAL",
    "serial": "TWJ6KSP005",
    "time": "2021-02-04 06:50:02 UTC"
    "user": "emp52342"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ff",
  "text": "Threat events for user id emp52342 exceeded
the threshold 50 in last 10 minutes."
}

```

---

## Gateway Threat Count per Signature

```
{
  "id": "AXdr6Yf3o68tULajSz4Y",
  "nid": 2306,
  "alert_type": "GW_IDS_IPS_ALERT_THREAT_SID_OVER_A_PERIOD",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-2306",
  "device_id": "2821300",
  "description": "Threat events of signature id 2821300
  exceeded the threshold 50 in last 30 minutes.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612423202,
  "details": {
    "threshold": "50",
    "agg_field_name": "signature",
    "duration": "30",
    "signature": "2821300",
    "severity": "CRITICAL",
    "rule_id": "0",
    "serial": "2821300",
    "time": "2021-02-04 06:50:02 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "Threat events of signature id 2821300
  exceeded the threshold 50 in last 30 minutes"
}
```

---

## Gateway IDS/IPS Engine Error State

```
{
  "id": "AXdq-8_vo68tULajSqJi",
  "nid": 2301,
  "alert_type": "GW_IDS_IPS_ENGINE_ERROR_STATE_ALERT",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-2301",
  "device_id": "CNJJKLB0G6",
  "description": "IDS/IPS engine on Gateway WTH_9004-1 with serial CNJJKLB0G6 has
  moved to an error (Stopped) state.",
  "state": "Close",
  "severity": "Critical",
  "operation": "update",
  "timestamp": 1612407706,
  "details": {
    "serial": "CNJJKLB0G6",
    "hostname": "WTH_9004-1",
    "state": "Stopped",
    "time": "2021-02-04 03:00:23 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "IDS/IPS engine on Gateway WTH_9004-1 with serial CNJJKLB0G6 has moved to an
  error (Stopped) state."
}
```

---

## Gateway IDS IPS Engine CPU Utilization

```
{
  "id": "AXdq9flmo68tULajSqDN",
  "nid": 2302,
  "alert_type": "GW_IDS_IPS_ENGINE_CPU_OVER_UTILIZATION",
```

```

"setting_id": "6039f9543bac449291bfcd19eb10d1eb-2302",
"device_id": "CNJJKLB0HB",
"description": "CPU utilization for IDS/IPS engine on Gateway WTH_9004-2 with serial
  CNJJKLB0HB has been above 10% for about 11 minutes since 2021-02-04 02:43:01 UTC.",
"state": "Open",
"severity": "Critical",
"operation": "create",
"timestamp": 1612407241,
"details": {
  "name": "WTH_9004-2",
  "unit": "%",
  "serial": "CNJJKLB0HB",
  "group": "36",
  "labels": "8",
  "_rule_number": "0",
  "ds_key": "6039f9543bac449291bfcd19eb10d1eb.CNJJKLB0HB.idps.cpu.5m",
  "duration": "11",
  "threshold": "10",
  "time": "2021-02-04 02:43:01 UTC"
},
"webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
"text": "CPU utilization for IDS/IPS engine on Gateway WTH_9004-2 with serial
  CNJJKLB0HB has been above 10% for about 11 minutes since 2021-02-04 02:43:01 UTC."
}

```

---

## Gateway IDS IPS Engine Memory Utilization

```

{
  "id": "AXdq9fkVo68tULajSqDL",
  "nid": 2303,
  "alert_type": "GW_IDS_IPS_ENGINE_MEMORY_OVER_UTILIZATION",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-2303",
  "device_id": "CNJJKLB0HB",
  "description": "Memory utilization for IDS/IPS engine on Gateway WTH_9004-2 with
  serial
  CNJJKLB0HB has been above 2% for about 5 minutes since 2021-02-04 02:49:00 UTC.",
  "state": "Open",
  "severity": "Minor",
  "operation": "create",
  "timestamp": 1612407240,
  "details": {
    "name": "WTH_9004-2",
    "unit": "%",
    "serial": "CNJJKLB0HB",
    "group": "36",
    "labels": "8",
    "_rule_number": "0",
    "ds_key": "6039f9543bac449291bfcd19eb10d1eb.CNJJKLB0HB.idps.mem.5m",
    "duration": "5",
    "threshold": "2",
    "time": "2021-02-04 02:49:00 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "Memory utilization for IDS/IPS engine on Gateway WTH_9004-2 with serial
  CNJJKLB0HB has been above 2% for about 5 minutes since 2021-02-04 02:49:00 UTC."
}

```

---

## Gateway IDS IPS Engine Packet Dropped Detected

```

{
  "id": "AXdr8CPmo68tULajS0K8",
  "nid": 2304,
  "alert_type": "GW_IDS_IPS_ENGINE_PACKET_DROPPED_DETECTED",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-2304",
  "device_id": "SCA0000004",
  "description": "Packet drop for IDS/IPS engine on Gateway CSIM_SCA0000004 with
serial
  SCA0000004 has been above 75% for about 5 minutes since 2021-02-04 07:22:15 UTC.",
  "state": "Open",
  "severity": "Minor",
  "operation": "create",
  "timestamp": 1612423635,
  "details": {
    "name": "CSIM_SCA0000004",
    "serial": "SCA0000004",
    "threshold": "75",
    "duration": "5",
    "time": "2021-02-04 07:22:15 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "Packet drop for IDS/IPS engine on Gateway CSIM_SCA0000004 with serial
  SCA0000004 has been above 75% for about 5 minutes since 2021-02-04 07:22:15 UTC."
}

```

## GW Cluster VLAN Mismatch

```

{
  "id": "AXd9rMzXo68tULajWxbZ",
  "nid": 1801,
  "alert_type": "GW_CLUSTER_VLAN_MISMATCH",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1801",
  "device_id": "54",
  "description": "There is a VLAN mismatch in cluster C2C-253-YODA between Gateway
with
  serial: CG0020729 and Gateway with serial: CG0021234.",
  "state": "Close",
  "severity": "Minor",
  "operation": "update",
  "timestamp": 1612722281,
  "details": {
    "gateway2": "CG0021234",
    "gateway1": "CG0020729",
    "serial": "54",
    "alert_key": "CG0020729-CG0021234",
    "time": "2021-02-07 18:06:52 UTC",
    "cluster-name": "C2C-253-YODA",
    "group": "278",
    "labels": []
  },
  "webhook": "52e0abbd-cdda-45f2-bd68-3107fef43841",
  "text": "There is a VLAN mismatch in cluster C2C-253-YODA between Gateway with
  serial: CG0020729 and Gateway with serial: CG0021234."
}

```

## New Gateway Connected

```

{

```



```

{id": "AXd96oFqo68tULajWy28",
nid": 301,
alert_type": "NEW_GATEWAY_DETECTED",
setting_id": "abce082bef4a428bb31366f6d6ff223f-301",
device_id": "CP0021763",
description": "New Gateway GSK-7005-2 with serial CP0021763, MAC address
20:4c:03:11:eb:78 and IP
address 172.168.1.1 connected, Group:unprovisioned",
state": "Open",
severity": "Warning",
operation": "create",
timestamp": 1612725256,
details": {
group": "1",
labels": "",
_rule_number": "0",
params": [
"CP0021763",
"20:4c:03:11:eb:78",
"172.168.1.1",
"GSK-7005-2"
],
serial": "CP0021763",
time": "2021-02-07 19:14:16 UTC",
group_name": "unprovisioned"
},
webhook": "52e0abbd-cdda-45f2-bd68-3107fef43841",
text": "New Gateway GSK-7005-2 with serial CP0021763, MAC address 20:4c:03:11:eb:78
and IP
address 172.168.1.1 connected, Group:unprovisioned"
}

```

---

## Overlay Route Orchestrator Connection

```

{
{id": "AXeC5dlWo68tULajXiwK",
nid": 1359,
alert_type": "CONTROLLER OAP CONNECTION",
setting_id": "a847a3aea73d4ba7b34c00323fb9ee7a-1359",
device_id": "CP0048220",
description": "Overlay Route Orchestrator control connection is down for
Legacy2.0-BGW1-A7005-39_82_AC (serial=CP0048220)",
state": "Open",
severity": "Critical",
operation": "create",
timestamp": 1612808837,
details": {
hostname": "Legacy2.0-BGW1-A7005-39_82_AC",
serial": "CP0048220",
group": "22",
time": "2021-02-08 18:27:17 UTC"
},
webhook": "f6f2b19a-31d5-445c-b340-eb1ca8a6fdd8",
text": "Overlay Route Orchestrator control connection is down for
Legacy2.0-BGW1-A7005-39_82_AC (serial=CP0048220)"
}
}

```

---

## Route Table Limit

```
{
  "id": "AXeEaOYlo68tULajX4gT",
  "nid": 1357,
  "alert_type": "CONTROLLER ROUTE TABLE CAPACITY",
  "setting_id": "a847a3aea73d4ba7b34c00323fb9ee7a-1357",
  "device_id": "CP0059047",
  "description": "Routing table for device Legacy-2.1-BGW2-A7005_5F_9A_2A exceeded threshold(serial=CP0059047, IP=111.1.10.1, count=3463, max=4096)",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612834203,
  "details": {
    "serial": "CP0059047",
    "ip_address": "111.1.10.1",
    "count": "3463",
    "hostname": "Legacy-2.1-BGW2-A7005_5F_9A_2A",
    "max": "4096",
    "group": "21",
    "time": "2021-02-09 01:30:03 UTC"
  },
  "webhook": "f6f2b19a-31d5-445c-b340-eb1ca8a6fdd8",
  "text": "Routing table for device Legacy-2.1-BGW2-A7005_5F_9A_2A exceeded threshold(serial=CP0059047, IP=111.1.10.1, count=3463, max=4096)"
}
```

## Route Table Capacity

```
{
  "id": "AXeCfX4pPppb5nv9WSDi",
  "nid": 1357,
  "alert_type": "CONTROLLER ROUTE TABLE CAPACITY",
  "setting_id": "417fc95887044bcba9b3e2ce3830a ECB-1357",
  "device_id": "DL0003539",
  "description": "Routing table for device DC3_VPNC8_7240XM exceeded threshold (serial=DL0003539, IP=2.3.1.5, count=29268, max=32768)",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612801998,
  "details": {
    "serial": "DL0003539",
    "ip_address": "2.3.1.5",
    "count": "29268",
    "hostname": "DC3_VPNC8_7240XM",
    "max": "32768",
    "group": "57",
    "time": "2021-02-08 16:33:18 UTC"
  },
  "webhook": "5cbc87e4-9eb5-45d2-b890-b21db89ca5b4",
  "text": "Routing table for device DC3_VPNC8_7240XM exceeded threshold (serial=DL0003539, IP=2.3.1.5, count=29268, max=32768)"
}
```

## WAN Uplink Autonegotiation State Change

```
{
  "id": "AXdnjuvwo68tULajSQyc",
```

```

"nid": 1506,
"alert_type": "WAN_UPLINK_AUTONEGOTIATION_STATE_CHANGE",
"setting_id": "6039f9543bac449291bfcd19eb10d1eb-1506",
"device_id": "CNJJKLB0NZ",
"description": "WAN ports autonegotiaton speed changed from 1000 Mbps to Auto Mbps
for device WTH-9004-3 with serial CNJJKLB0NZ for uplink GE0/0/1 at 2021-02-03
11:02:35 UTC",
"state": "Open",
"severity": "Critical",
"operation": "create",
"timestamp": 1612350155,
"details": {
  "intf_name": "GE0/0/1",
  "speed": "1000",
  "new_speed": "Auto",
  "hostname": "WTH-9004-3",
  "serial": "CNJJKLB0NZ",
  "group": "36",
  "labels": [
    "g"
  ],
  "time": "2021-02-03 11:02:35 UTC"
},
"webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
"text": "WAN ports autonegotiaton speed changed from 1000 Mbps to Auto Mbps for
device WTH-9004-3 with serial CNJJKLB0NZ for uplink GE0/0/1 at 2021-02-03 11:02:35
UTC"
}

```

---

## WAN Health-check failure

```

{
  "id": "AXdk2LK6o68tULajRvY4",
  "nid": 1501,
  "alert_type": "WAN_UPLINK_REACHABILITY_HEALTH_CHECK_IP_FAILED",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1501",
  "device_id": "CNJJKLB0HB",
  "description": "WAN reachability check failed for Gateway WTH_9004-2 with serial
CNJJKLB0HB to Health Check IP 52.52.253.87 on uplink inet2_inet. Default-gateway is
reachable.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612304659,
  "details": {
    "default_gw_status": "reachable",
    "intf_name": "inet2_inet",
    "ip": "52.52.253.87",
    "hostname": "WTH_9004-2",
    "serial": "CNJJKLB0HB",
    "group": "36",
    "labels": [
      "g"
    ],
    "time": "2021-02-02 22:24:19 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "WAN reachability check failed for Gateway WTH_9004-2 with serial CNJJKLB0HB
to Health Check IP 52.52.253.87 on uplink inet2_inet. Default-gateway is reachable."
}

```

## WAN VPN-Peer unreachable

```
{
  "id": "AXdncVpfo68tULajSPzi",
  "nid": 1502,
  "alert_type": "WAN_UPLINK_REACHABILITY_VPN_PEER_FAILED",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1502",
  "device_id": "CNJJKLB0HB",
  "description": "WAN reachability check failed for Gateway WTH_9004-2 with serial
CNJJKLB0HB
to VPN peer 192.168.103.99 on uplink inet2_inet. Default-gateway is unreachable.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612348217,
  "details": {
    "ip": "192.168.103.99",
    "intf_name": "inet2_inet",
    "default_gw_status": "unreachable",
    "hostname": "WTH_9004-2",
    "serial": "CNJJKLB0HB",
    "group": "36",
    "labels": [
      "8"
    ],
    "time": "2021-02-03 10:30:17 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "WAN reachability check failed for Gateway WTH_9004-2 with serial CNJJKLB0HB
to
VPN peer 192.168.103.99 on uplink inet2_inet. Default-gateway is unreachable."
}
```

## WAN Uplink Status Change

```
{
  "id": "AXdnjgBlo68tULajSQwz",
  "nid": 1505,
  "alert_type": "WAN_UPLINK_STATUS_CHANGE",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1505",
  "device_id": "CNJJKLB0NZ",
  "description": "Uplink port inet_inet status change UP -> DOWN for device WTH-9004-3
with serial CNJJKLB0NZ at 2021-02-03 11:01:35 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612350095,
  "details": {
    "intf_name": "inet_inet",
    "status": "UP",
    "current_status": "DOWN",
    "uplink_tag": "inet_inet",
    "hostname": "WTH-9004-3",
    "serial": "CNJJKLB0NZ",
    "group": "36",
    "labels": [
      "8"
    ],
    "time": "2021-02-03 11:01:35 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "Uplink port inet_inet status change UP -> DOWN for device WTH-9004-3"
}
```

```
with serial CNJJKLB0NZ at 2021-02-03 11:01:35 UTC"
}
```

---

## Uplink Flapping

```
{
  "id": "AXe2GwY1o68tULajexWO",
  "nid": 1600,
  "alert_type": "WAN_UPLINK_FLAP",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1600",
  "device_id": "CNJJKLB0G6",
  "description": "Uplink inet_inet link status flapped 1% on device WTH_9004-1 with
serial CNJJKLB0G6
  for about 15 minutes since 2021-02-18 16:51:00 UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1613667960,
  "details": {
    "intf_name": "inet_inet",
    "status": "DOWN",
    "current_status": "UP",
    "uplink_tag": "inet_inet",
    "hostname": "WTH_9004-1",
    "unit": "%",
    "serial": "CNJJKLB0G6",
    "group": "36",
    "labels": "8",
    "_rule_number": "0",
    "ds_key": "6039f9543bac449291bfcd19eb10d1eb.CNJJKLB0G6.uplink.flap.5m",
    "duration": "15",
    "threshold": "1",
    "time": "2021-02-18 16:51:00 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "Uplink inet_inet link status flapped 1% on device WTH_9004-1 with serial
CNJJKLB0G6
  for about 15 minutes since 2021-02-18 16:51:00 UTC."
}
```

---

## Tunnel Flapping

```
{
  "id": "AXe2H5oGo68tULajexfD",
  "nid": 1601,
  "alert_type": "WAN_TUNNEL_FLAP",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1601",
  "device_id": "CNJJKLB0G6",
  "description": "Tunnel WTH_9004-1:inet_inet::GSK_VPNC2:vlan103 status flapped 1% on
device
WTH_9004-1 with serial CNJJKLB0G6 for about 15 minutes since 2021-02-18 16:56:00
UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1613668260,
  "details": {
    "src_ip": "192.168.32.10",

```

---

```

    "dst_ip": "192.168.103.99",
    "alias_map_name": "WTH_9004-1:inet_inet::GSK_VPNC2:vlan103",
    "uplink_tag": "inet_inet",
    "hostname": "WTH_9004-1",
    "unit": "%",
    "serial": "CNJJKLB0G6",
    "group": "36",
    "labels": "8",
    "_rule_number": "0",
    "ds_key": "6039f9543bac449291bfcd19eb10d1eb.CNJJKLB0G6.uplink.tunnel.flap.5m",
    "duration": "15",
    "threshold": "1",
    "time": "2021-02-18 16:56:00 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "Tunnel WTH_9004-1:inet_inet::GSK_VPNC2:vlan103 status flapped 1% on device
WTH_9004-1 with serial CNJJKLB0G6 for about 15 minutes since 2021-02-18 16:56:00
UTC."
}

```

## IPSec Establishment Failure

```

{
  "id": "AXdi4-5Bo68tULajRU_R",
  "nid": 1550,
  "alert_type": "WAN_IPSEC_SA_ESTABILSHMENT_FAILED",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1550",
  "device_id": "CNJJKLB0NZ",
  "description": "IPSec Tunnel Establishment from 192.168.36.10 to 192.168.103.99
failed on
device WTH-9004-3 with serial CNJJKLB0NZ at 2021-02-02 13:17:20 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612271840,
  "details": {
    "src_ip": "192.168.36.10",
    "dst_ip": "192.168.103.99",
    "alias_map_name": "WTH-9004-3:inet_inet::GSK_VPNC2:vlan103",
    "link_tag": "inet_inet",
    "hostname": "WTH-9004-3",
    "serial": "CNJJKLB0NZ",
    "group": "36",
    "labels": [
      "8"
    ],
    "time": "2021-02-02 13:17:20 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "IPSec Tunnel Establishment from 192.168.36.10 to 192.168.103.99 failed on
device WTH-9004-3 with serial CNJJKLB0NZ at 2021-02-02 13:17:20 UTC"
}

```

## IPSec SA Down

```

{
  "id": "AXdi4Qjgo68tULajRUzp",

```

```

"nid": 1551,
"alert_type": "WAN_IPSEC_SA_DOWN",
"setting_id": "6039f9543bac449291bfcd19eb10d1eb-1551",
"device_id": "CNJJKLB0G6",
"description": "IPSec tunnel WTH_9004-1:inet2_inet::GSK_VPNC2:vlan103 from
192.168.31.10 to
192.168.103.99 is DOWN on device WTH_9004-1 with serial CNJJKLB0G6. Reason:
Administrator
cleared IPSEC SA at 2021-02-02 13:14:11 UTC",
"state": "Open",
"severity": "Critical",
"operation": "create",
"timestamp": 1612271651,
"details": {
  "src_ip": "192.168.31.10",
  "dst_ip": "192.168.103.99",
  "reason": "Administrator cleared IPSEC SA",
  "alias_map_name": "WTH_9004-1:inet2_inet::GSK_VPNC2:vlan103",
  "uplink_tag": "inet2_inet",
  "hostname": "WTH_9004-1",
  "serial": "CNJJKLB0G6",
  "group": "36",
  "labels": [
    "8"
  ],
  "time": "2021-02-02 13:14:11 UTC"
},
"webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
"text": "IPSec tunnel WTH_9004-1:inet2_inet::GSK_VPNC2:vlan103 from 192.168.31.10 to
192.168.103.99 is DOWN on device WTH_9004-1 with serial CNJJKLB0G6. Reason:
Administrator
cleared IPSEC SA at 2021-02-02 13:14:11 UTC"
}

```

---

## All IPsec SAs Down

```

{
  "id": "AXdi4Qoyo68tULajRUzs",
  "nid": 1552,
  "alert_type": "WAN_IPSEC_SA_ALL_DOWN",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1552",
  "device_id": "CNJJKLB0G6",
  "description": "All IPsec SAs down for device WTH_9004-1 with serial CNJJKLB0G6 at
2021-02-02 13:14:11 UTC",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1612271651,
  "details": {
    "hostname": "WTH_9004-1",
    "serial": "CNJJKLB0G6",
    "group": "36",
    "labels": [
      "8"
    ],
    "time": "2021-02-02 13:14:11 UTC"
  },
  "webhook": "a82456c8-1402-4fe1-a195-0131e6b392ee",
  "text": "All IPsec SAs down for device WTH_9004-1 with serial CNJJKLB0G6 at
2021-02-02 13:14:11 UTC"
}

```

---

## Gateway Cellular Data Usage

```
{
  "id": "AXuqDamDKFHq3kj2qihO",
  "nid": 1511,
  "alert_type": "CELLULAR_DATA_USAGE",
  "setting_id": "082445a5b8264597bce334f932c9a3a4-1511",
  "device_id": "TWJCKSP01C",
  "description": "Cellular data usage 11 MB has exceeded the configured limit 1 MB
    for Gateway Aruba9004-LTE with serial TWJCKSP01C",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1630645627,
  "details": {
    "usage": "11 MB",
    "limit": "1 MB",
    "name": "Aruba9004-LTE",
    "serial": "TWJCKSP01C",
    "group": "6",
    "labels": [],
    "time": "2021-09-03 05:07:07 UTC"
  },
  "webhook": "a7b7f0de-2465-4340-b491-d9ea676326f3",
  "text": "Cellular data usage 11 MB has exceeded the configured limit 1 MB
    for Gateway Aruba9004-LTE with serial TWJCKSP01C"
}
```

## Gateway Firmware Upgrade Failed

```
{
  "id": "AXvSPH4-KFHq3kj2rcg9",
  "nid": 2201,
  "alert_type": "GW_FW_UPGRADE_FAILURE",
  "setting_id": "082445a5b8264597bce334f932c9a3a4-2201",
  "device_id": "",
  "description": "Firmware upgrade failed for gateway
    (NAME Aruba9004-LTE_95_EA_76 SN MAC 20:4c:03:95:ea:76)",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1631319891,
  "details": {
    "mac": "20:4c:03:95:ea:76",
    "hostname": "Aruba9004-LTE_95_EA_76",
    "serial": "",
    "group": "6",
    "labels": "",
    "_rule_number": "0",
    "params": "",
    "time": "2021-09-11 00:24:51 UTC"
  },
  "webhook": "87fae42a-78ec-45c0-a22a-4f81417cad56",
  "text": "Firmware upgrade failed for gateway
    (NAME Aruba9004-LTE_95_EA_76 SN MAC 20:4c:03:95:ea:76)"
}
```

## Uplink Speed Flapping



```

{
  "id": "AXwCtmSrKFHq3kj2s2hh",
  "nid": 1602,
  "alert_type": "WAN_AUTO_NEGOTIATION_FLAP",
  "setting_id": "082445a5b8264597bce334f932c9a3a4-1602",
  "device_id": "TWJCKSP01C",
  "description": "Uplink GE0/0/1 speed flapped 1% on device Aruba9004-LTE_95_EA_76 with
    serial TWJCKSP01C for about 15 minutes since 2021-09-20 10:03:00 UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1632133080,
  "details": {
    "intf_name": "GE0/0/1",
    "speed": "1000",
    "new_speed": "100",
    "hostname": "Aruba9004-LTE_95_EA_76",
    "serial": "TWJCKSP01C",
    "group": "6",
    "labels": "8,7",
    "unit": "%",
    "_rule_number": "0",
    "ds_key": "082445a5b8264597bce334f932c9a3a4.TWJCKSP01C.uplink.speed.flap.5m",
    "duration": "15",
    "threshold": "1",
    "time": "2021-09-20 10:03:00 UTC"
  },
  "webhook": "4a1b58b1-3371-471e-8093-73c07fb6b384",
  "text": "Uplink GE0/0/1 speed flapped 1% on device Aruba9004-LTE_95_EA_76 with
    serial TWJCKSP01C for about 15 minutes since 2021-09-20 10:03:00 UTC."
}

```

---

## WAN Uplink Input Errors

```

{
  "id": "AX0Jamv1J_Ty_F5wJkqF",
  "nid": 1507,
  "alert_type": "WAN_UPLINK_INPUT_ERRORS",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1507",
  "device_id": "SCA0000006",
  "description": "Input errors for Uplink Interface GE 0/0/0 on Gateway
    CSIM_SCA0000006 with serial SCA0000006 has been above 1% for about 5 minutes
    since 2021-11-10 10:30:09 UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1636540509,
  "details": {
    "intf_name": "GE 0/0/0",
    "hostname": "CSIM_SCA0000006",
    "serial": "SCA0000006",
    "group": "0",
    "labels": "48",
    "_rule_number": "0",
    "ds_key": "6039f9543bac449291bfcd19eb10d1eb.SCA0000006.intf.inerrors_percent.5m",
    "duration": "5",
    "threshold": "1",
    "time": "2021-11-10 10:30:09 UTC"
  },
  "webhook": "4c09b716-eb38-4c4f-8a3f-61f476eb9ca6",
  "text": "Input errors for Uplink Interface GE 0/0/0 on Gateway CSIM_SCA0000006"
}

```

```
with serial SCA0000006 has been above 1% for about 5 minutes since 2021-11-10
10:30:09 UTC.",
"cluster_hostname": "app-yoda.arubathena.com"
}
```

## WAN Uplink Output Errors

```
{
  "id": "AX0JazwZJ_Ty_F5wJkqp",
  "nid": 1508,
  "alert_type": "WAN_UPLINK_OUTPUT_ERRORS",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1508",
  "device_id": "SCA0000096",
  "description": "Output errors for Uplink Interface GE 0/0/2 on Gateway
  CSIM_SCA0000096 with serial SCA0000096 has been above 1% for about 5 minutes
  since 2021-11-10 10:31:02 UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1636540562,
  "details": {
    "intf_name": "GE 0/0/2",
    "hostname": "CSIM_SCA0000096",
    "serial": "SCA0000096",
    "group": "0",
    "_rule_number": "0",
    "ds_key": "6039f9543bac449291bfcd19eb10d1eb.SCA0000096.intf.outerrors_percent.5m",
    "duration": "5",
    "threshold": "1",
    "time": "2021-11-10 10:31:02 UTC"
  },
  "webhook": "4c09b716-eb38-4c4f-8a3f-61f476eb9ca6",
  "text": "Output errors for Uplink Interface GE 0/0/2 on Gateway CSIM_SCA0000096
  with serial SCA0000096 has been above 1% for about 5 minutes since 2021-11-10
  10:31:02 UTC.",
  "cluster_hostname": "app-yoda.arubathena.com"
}
```

## WAN Uplink PHY Errors

```
{
  "id": "AX0Jamx2J_Ty_F5wJkqG",
  "nid": 1509,
  "alert_type": "WAN_UPLINK_PHY_ERRORS",
  "setting_id": "6039f9543bac449291bfcd19eb10d1eb-1509",
  "device_id": "SCA0000006",
  "description": "PHY errors for Uplink Interface GE 0/0/2 on Gateway
  CSIM_SCA0000006 with serial SCA0000006 has been above 1% for about
  5 minutes since 2021-11-10 10:30:09 UTC.",
  "state": "Open",
  "severity": "Critical",
  "operation": "create",
  "timestamp": 1636540509,
  "details": {
    "intf_name": "GE 0/0/2",
    "hostname": "CSIM_SCA0000006",
    "serial": "SCA0000006",
    "group": "0",
    "labels": "48",
  }
}
```

```

    "_rule_number": "0",
    "ds_key": "6039f9543bac449291bfcd19eb10d1eb.SCA0000006.intf.phyerrors_percent.5m",
    "duration": "5",
    "threshold": "1",
    "time": "2021-11-10 10:30:09 UTC"
  },
  "webhook": "4c09b716-eb38-4c4f-8a3f-61f476eb9ca6",
  "text": "PHY errors for Uplink Interface GE 0/0/2 on Gateway CSIM_SCA0000006
with serial SCA0000006 has been above 1% for about 5 minutes since 2021-11-10
10:30:09 UTC.",
  "cluster_hostname": "app-yoda.arubathena.com"
}

```

## Miscellaneous Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

### Device Config Change Detected

```

{
  "alert_type": "DEVICE_CONFIG_CHANGE_DETECTED",
  "description": "Config change detected on group nbapi_test for device type Switch by
user
example@hpe.com.\n\nSerial: None, \nMacAddress: None,
\nConfig Content: Template Updated
\nmodel: ALL\nversion: ALL\ndevice_type: HPPC\ntemplate changes: \n @@ -18,6 +18,6
@@\n\n\n
ip address dhcp-bootp\n\n exit\n\n vlan 13\n\n- name \"vlan_8888\"\n\n+ name
\"vlan_44\"\n\n no ip address\n\n exit ",
  "timestamp": "1564383294",
  "webhook": "272eda1a-f79b-4192-ad6f-b35da11515bc",
  "setting_id": "715e45fe3ff8453da355cd34aff2afa5-2000",
  "state": "Open",
  "nid": "2000",
  "details": {
    "config_change": "Template Updated\nmodel: ALL\nversion: ALL\ndevice_type:
HPPC\ntemplate changes: \n @@ -18,6 +18,
6 @@\n\n\n ip address dhcp-bootp\n\n exit\n\n vlan 13\n\n- name \"vlan_8888\"\n\n+
name \"vlan_44\"\n\n no ip address\n\n exit ",
    "macaddr": "None",
    "group": "8",
    "dev_type": "Switch",
    "labels": "None",
    "group_name": "nbapi_test",
    "_rule_number": "0",
    "params": "None",
    "user": "example@hpe.com",
    "time": "2019-07-29 06:54:54 UTC",
    "serial": "None"
  },
  "operation": "create",
  "device_id": "",
  "id": "AWw8grSBeZ6A6PlBvMk4",
  "severity": "Warning"
}

```

### User Account Deleted

```

{

```

```
"alert_type": "User account deleted",
"description": "User with name v@gmail.com deleted.",
"timestamp": 1569234480,
"webhook": "057b0a95-9f06-4a0f-b4bf-149a28d749b3",
"setting_id": "573b0412517a41c8a73a80f3e74ff0d2-15",
"state": "Open",
"nid": 15,
"details": {
  "group": "-1",
  "labels": "None",
  "params": [
    "v@gmail.com"
  ],
  "_rule_number": "0",
  "time": "2019-09-23 10:28:00 UTC"
},
"operation": "create",
"device_id": "",
"id": "AWldqe6rYu0OgJ2alXzT",
"severity": "Major"
}
```

---

## New User Account Added

```
{
  "alert_type": "New User account added",
  "description": "User account setting updated for user: newuser@gmail.com with
language:en_US and idle timeout: 1800",
  "timestamp": 1569234534,
  "webhook": "057b0a95-9f06-4a0f-b4bf-149a28d749b3",
  "setting_id": "573b0412517a41c8a73a80f3e74ff0d2-14",
  "state": "Open",
  "nid": 14,
  "details": {
    "group": "-1",
    "labels": "None",
    "params": [],
    "_rule_number": "0",
    "time": "2019-09-23 10:28:54 UTC"
  },
  "operation": "create",
  "device_id": "",
  "id": "AWldqr6nYu0OgJ2alX1l",
  "severity": "Major"
}
```

---

## User Account Edited

```
{
  "alert_type": "User account edited",
  "description": "User with Name newuser@gmail.com, role readwrite and access []
updated.",
  "timestamp": 1569235100,
  "webhook": "057b0a95-9f06-4a0f-b4bf-149a28d749b3",
  "setting_id": "573b0412517a41c8a73a80f3e74ff0d2-16",
  "state": "Open",
  "nid": 16,
  "details": {
    "group": "-1",
```

```
"labels": "None",
"params": [
  "newuser@gmail.com",
  "readwrite",
  "[]"
],
"_rule_number": "0",
"time": "2019-09-23 10:38:20 UTC"
},
"operation": "create",
"device_id": "",
"id": "AW1ds2LcYu0OgJ2alYM2",
"severity": "Major"
}
```

---