Aruba Central Application Programming Interface

Reference Guide
Copyright Information

© Copyright 2020 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code 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, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA
### Contents

- **About this Guide** ................................................................. 5
  - Contacting Support ............................................................. 5
- **API Gateway** .................................................................. 6
  - API Gateway and NB APIs ..................................................... 6
  - Accessing API Gateway ...................................................... 7
    - Domain URLs ................................................................. 8
  - Viewing Swagger Interface .................................................. 8
  - List of Supported APIs ...................................................... 9
- **Creating Application and Token** .................................... 10
- **Using OAuth 2.0 for Authentication** ................................. 11
  - Access and Refresh Tokens .................................................. 12
    - Obtaining Access Token ................................................... 12
    - Accessing APIs ............................................................. 12
    - Viewing and Revoking Tokens ........................................... 13
    - Adding a New Token ....................................................... 14
- **Obtaining Token Using Offline Token Mechanism** .................. 14
- **Obtaining Token Using OAuth Grant Mechanism** .................... 15
  - **Step 1:** Authenticate a User and Create a User Session .......... 15
    - Example ........................................................................... 15
  - **Step 2:** [Optional] Generating Client Credentials .................. 16
    - Example ........................................................................... 16
  - **Step 3:** Generate Authorization Code ................................. 17
    - Example ........................................................................... 17
  - **Step 4:** Exchange Auth Code for a Token ............................ 18
    - Example ........................................................................... 18
  - **Step 5:** Refreshing a Token ............................................... 19
    - Example ........................................................................... 19
  - **Step 6:** Deleting a Token .................................................... 20
    - Example ........................................................................... 20
- **Viewing Usage Statistics** ................................................ 21
- **Webhooks** ....................................................................... 22
  - Creating and Updating Webhooks Through the UI .................... 23
  - Refreshing Webhooks Token Through the UI ............................ 24
  - Creating and Updating Webhooks Through the API Gateway ......... 24
List of Webhooks APIs ................................................................. 25
Sample Webhooks Payload Format for Alerts ................................. 26
Access Point Alerts—Sample JSON .................................................. 26
Switch Alerts—Sample JSON .......................................................... 34
Gateway Alerts—Sample JSON ....................................................... 39
Miscellaneous Alerts—Sample JSON .............................................. 46
This guide describes how to use Aruba Central Application Programming Interface (API) to configure your applications.

**Contacting Support**

**Table 1: Contact Information**

<table>
<thead>
<tr>
<th>Service</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Site</td>
<td>arubanetworks.com</td>
</tr>
<tr>
<td>Support Site</td>
<td>support.arubanetworks.com</td>
</tr>
<tr>
<td>Airheads Social Forums and Knowledge Base</td>
<td>community.arubanetworks.com</td>
</tr>
<tr>
<td>North American Telephone</td>
<td>1-800-943-4526 (Toll Free) 1-408-754-1200</td>
</tr>
<tr>
<td>International Telephone</td>
<td>arubanetworks.com/support-services/contact-support/</td>
</tr>
<tr>
<td>Software Licensing Site</td>
<td>lms.arubanetworks.com</td>
</tr>
<tr>
<td>End-of-life Information</td>
<td>arubanetworks.com/support-services/end-of-life/</td>
</tr>
<tr>
<td>Security Incident Response Team</td>
<td>Site: arubanetworks.com/support-services/security-bulletins/ Email: <a href="mailto:aruba-sirt@hpe.com">aruba-sirt@hpe.com</a></td>
</tr>
</tbody>
</table>
Aruba Central supports a robust set of REST APIs to enable users to build custom applications and integrate the APIs with their applications. The Aruba Central API framework uses OAuth protocol to authenticate and authorize third-party applications, and allows them to obtain secure and limited access to an Aruba Central service.

This section includes the following topics:
- API Gateway and NB APIs on page 6
- Accessing API Gateway on page 7
- Viewing Swagger Interface on page 8
- List of Supported APIs on page 9

API Gateway and NB APIs

The API Gateway feature in Aruba Central supports the REST API for all Aruba Central services. This feature allows Aruba 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 Aruba Central API Framework plug-in supports OAuth protocol for authentication and authorization. The access tokens provide a 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 following figure illustrates the API gateway workflow for the users:

Accessing API Gateway

To access the API Gateway:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.

   The **API Gateway** page is displayed. You can get new tokens and refresh old tokens. To obtain a new token application, you must set authentication parameters for a user session.

   ![API Gateway page](image)

   **ACCOUNT HOME**
   Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

   **APPS**
   - Network Operatives: Manage your wireless, wired, and WAN infrastructure.
   - **Launch**

   **GLOBAL SETTINGS**
   - **Users and Roles**
   - **Key Management**
   - **Device Inventory**
   - **Subscription Assignment**

   **API GATEWAY** Access the API Gateway and manage access tokens.

Important Points to Note

- The admin user profile of MSP has **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.

- Administrator role is specific to an app and hence the administrator account related RBAC library APIs and decorators must contain the application name as one of the parameters in the access verification query.
- The decorators associated with Account Home, Network Operations, or ClearPass Device Insight must contain account_setting, central, or optik as app names respectively, as one of the parameters.

**Domain URLs**

The following table shows the region-specific domain URLs for accessing API Gateway:

<table>
<thead>
<tr>
<th>Region</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>US-1</td>
<td>app1-apigw.central.arubanetworks.com</td>
</tr>
<tr>
<td>US-2</td>
<td>apigw-prod2.central.arubanetworks.com</td>
</tr>
<tr>
<td>EU-1</td>
<td>eu-apigw.central.arubanetworks.com</td>
</tr>
<tr>
<td>Canada-1</td>
<td>apigw-ca.central.arubanetworks.com</td>
</tr>
<tr>
<td>China-1</td>
<td>apigw.central.arubanetworks.com.cn</td>
</tr>
<tr>
<td>APAC-1</td>
<td>api-ap.central.arubanetworks.com</td>
</tr>
<tr>
<td>APAC-EAST1</td>
<td>apigw-apaceast.central.arubanetworks.com</td>
</tr>
<tr>
<td>APAC-SOUTH1</td>
<td>apigw-apacsouthcentral.arubanetworks.com</td>
</tr>
</tbody>
</table>

The procedures described in this article use app1-apigw.central.arubanetworks.com as an example. Ensure that you use the appropriate domain URL when accessing API Gateway or generating tokens.

**Viewing Swagger Interface**

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

1. In the Account Home page, under Global Settings, click API Gateway.
   The API Gateway page with the list of published APIs is displayed.
2. To view the Swagger interface, click the link in the Documentation column next to the specific published API name. The documentation is displayed in a new window.
### List of Supported APIs
Aruba Central supports the following APIs for the managed devices.

#### Table 3: APIs and Description

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitoring</strong></td>
<td>Gets network, client, and event details. It also allows you to manage labels and switches.</td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td>Allows you to configure and retrieve the following:</td>
</tr>
<tr>
<td></td>
<td>- Groups</td>
</tr>
<tr>
<td></td>
<td>- Templates</td>
</tr>
<tr>
<td></td>
<td>- Devices</td>
</tr>
<tr>
<td><strong>AppRF</strong></td>
<td>Gets Top N AppRF statistics.</td>
</tr>
<tr>
<td><strong>Guest</strong></td>
<td>Gets visitor and session details of the portal.</td>
</tr>
<tr>
<td><strong>MSP</strong></td>
<td>Allows you to manage and retrieve the following:</td>
</tr>
<tr>
<td></td>
<td>- Customers</td>
</tr>
<tr>
<td></td>
<td>- Users</td>
</tr>
<tr>
<td></td>
<td>- Resources</td>
</tr>
<tr>
<td></td>
<td>- Devices</td>
</tr>
<tr>
<td>Aruba has enforced a request limit for the following APIs:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- GET /msp_api/v1/customers</td>
</tr>
<tr>
<td></td>
<td>- GET /msp_api/v1/customers/(customer_id)/devices</td>
</tr>
<tr>
<td></td>
<td>- GET /msp_api/v1/devices</td>
</tr>
<tr>
<td></td>
<td>- PUT /msp_api/v1/customers/(customer_id)/devices</td>
</tr>
<tr>
<td>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: <strong>LIMIT_REQUEST_EXCEEDED</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>User Management</strong></td>
<td>Allows you to manage users and also allows you to configure various types of users with a specific level of access control.</td>
</tr>
<tr>
<td><strong>Audit Event Logs</strong></td>
<td>Gets a list of audit events and the details of an audit event.</td>
</tr>
<tr>
<td><strong>Device Inventory</strong></td>
<td>Gets device details and device statistics.</td>
</tr>
<tr>
<td><strong>Licensing</strong></td>
<td>Allows you to manage and retrieve subscription keys.</td>
</tr>
<tr>
<td><strong>Presence Analytics</strong></td>
<td>Allows you to configure the Presence Analytics application. It also retrieves site and loyalty data.</td>
</tr>
<tr>
<td><strong>Device Management</strong></td>
<td>Allows you to manage devices.</td>
</tr>
<tr>
<td><strong>Firmware</strong></td>
<td>Allows you to manage firmware.</td>
</tr>
<tr>
<td><strong>Troubleshooting</strong></td>
<td>Gets a list of troubleshooting commands for a specific type of device.</td>
</tr>
<tr>
<td><strong>Notification</strong></td>
<td>Gets notification alerts generated for events pertaining to device provisioning, configuration, and user management.</td>
</tr>
<tr>
<td><strong>Unified Communications</strong></td>
<td>Retrieves data for all sessions for a specific period of time. It also retrieves the total number of clients who made calls in the given time range and gets the Lync/Skype for Business URL for the Aruba Central cluster that you are using.</td>
</tr>
</tbody>
</table>
Table 3: APIs and Description

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh API Token</td>
<td>Allows you to refresh the API token.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Gets the list of configured reports for the given customer ID.</td>
</tr>
<tr>
<td>WAN Health</td>
<td>Allows you to the following:</td>
</tr>
<tr>
<td></td>
<td>■ Get list of configured WAN health policies.</td>
</tr>
<tr>
<td></td>
<td>■ Create a new WAN health policy.</td>
</tr>
<tr>
<td></td>
<td>■ Delete an existing WAN health policy.</td>
</tr>
<tr>
<td></td>
<td>■ Get the details of any specific WAN health policy.</td>
</tr>
<tr>
<td></td>
<td>■ Update an existing WAN health policy.</td>
</tr>
<tr>
<td></td>
<td>■ Get policy schedule details.</td>
</tr>
<tr>
<td></td>
<td>■ Create a schedule for a WAN health policy.</td>
</tr>
<tr>
<td></td>
<td>■ Get statistics for WAN health cookie generated for a site.</td>
</tr>
<tr>
<td></td>
<td>■ Get WAN health test results.</td>
</tr>
<tr>
<td></td>
<td>■ Get WAN health test results for a specific site.</td>
</tr>
<tr>
<td>Network Health</td>
<td>Allows you to get data for all the labels and sites.</td>
</tr>
<tr>
<td>Webhook</td>
<td>Allows you to add, or delete Webhooks, and get or refresh Webhook tokens. See Webhooks on page 22 for further details on Webhook.</td>
</tr>
<tr>
<td>VisualRF</td>
<td>Allows you retrieve information on floor plans, location of APs, clients and rogue devices.</td>
</tr>
<tr>
<td>DPS Monitoring</td>
<td>Gets DPS compliance and session statistics for all the links of a device belonging to a specific policy.</td>
</tr>
</tbody>
</table>

For a complete list of APIs and the corresponding documentation, see https://app1-apigw.central.arubanetworks.com/swagger/central.

Creating Application and Token

To create an application, complete the following steps:

1. In the Account Home page, under Global Settings, click API Gateway.
   The API Gateway page is displayed.

2. Click the My Apps & Tokens tab.
   The admin user will be able to create new apps for all the non-admin user by clicking + Add Apps & Tokens in the System Apps & Tokens tab.

3. Click + Add Apps & Tokens.
4. In the New Token pop-up window, do the following:
   a. Enter the application name. In 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. From the Application drop-down list, select the application.
   d. Click Generate. A new application is created and added to the My Apps & Tokens table. The 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, Network Operations.
      - **Tokens**—Token created for the application. The option is available to admin user profile only.
      - **Created At**—Date on which the application was created.

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

Only admin users 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.

---

**Using OAuth 2.0 for Authentication**

For secure access to the APIs, the Aruba Central API Framework plug-in supports 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 Aruba 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 [https://app1-apigw.central.arubanetworks.com](https://app1-apigw.central.arubanetworks.com).

**Access and Refresh 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 a 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 a long running applications (web app) or native mobile application you should refresh the token periodically. For more information, see Refreshing a token.

This section includes the following topics:

- Obtaining Access Token
- Accessing APIs
- Viewing and Revoking Tokens
- Adding a New Token

**Obtaining 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

**Accessing APIs**

To access the API, use the following URL:

[https://app1-apigw.central.arubanetworks.com/](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 4: Accessing the API**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td><a href="https://app1-apigw.central.arubanetworks.com/">https://app1-apigw.central.arubanetworks.com/</a></td>
<td>The API gateway URL. All APIs can be accessed from this URL by providing a correct access token.</td>
</tr>
</tbody>
</table>

The parameters for the API are as follows:

**Table 5: Parameters for the API**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_path</td>
<td>URL Path</td>
<td>URL path of an API, for example, to access monitoring APIs, use the path /monitoring/v1/aps.</td>
</tr>
</tbody>
</table>

**Table 6: Header for the API**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>Bearer ouzMaXEBbB6XqGtsWomK7MvaTuhrqDQ1</td>
<td>Pass the access token in the header.</td>
</tr>
</tbody>
</table>
Example

**Request Method:** GET

https://app1-apigw.central.arubanetworks.com/monitoring/v1/aps

**Request Header:**

**Authorization:** Bearer ouzMaXEBbB6XqGtsWomK7MvaTuhrqDQ1

**Response:**

```json
{
  "aps": [
    {
      "firmware_version": "6.4.4.4-4.2.3.1_54637",
      "group_name": "00TestVRK",
      "ip_address": "10.29.18.195",
      "labels": [
        "Filter_242",
        "ZiaomoE",
        "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": "e3bf1ba201a6f85f4b5eaedeedad5e502d85a9aef58d8e1d8a0",
      "swarm_master": true
    }
  ],
  "count": 1
}
```

**Viewing and Revoking Tokens**

To view or revoke tokens, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**. The **API Gateway** page is displayed.

2. 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 to. An application can be associated to multiple users.
- **Application**—Name of the application to which this token is associated to. For example, Network Operations.
- **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.

In MSP mode, the admin user profile has System Apps & Tokens tab which displays all the apps and tokens generated in all non-admin user profiles in addition to the apps and tokens created in the admin user profile. To view all the tokens of admin and non-admin user, go to Account Home > Global Settings > API Gateway > System Apps & Tokens.

### Adding a New Token
To add a new token, complete the following steps:

1. In the Account Home page, under Global Settings, click API Gateway. The API Gateway page is displayed.
2. Click My Apps & Tokens.
3. Click + Add Apps & Tokens to add a new token.
4. 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, the Redirect URI option is disabled for you in the My Apps and Tokens tab > 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.

### Obtaining Token Using Offline Token Mechanism
To obtain tokens using the offline token method, complete the following steps:

1. In the Account Home page, under Global Settings, click API Gateway. The API Gateway page is displayed.
2. Click My Apps & Tokens.

In the MSP mode, the admin user profile 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.

3. Click + Add Apps & Tokens. The New Token pane is displayed.
4. Enter the application name and redirect URI in the Application Name and Redirect URI fields respectively.
5. Choose the application from the Application drop-down list and click Generate to generate a new token.
6. 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 to. An application can be associated to multiple users.
- **Application**—Name of the application to which this token is associated to. For example, Network Operations.
- **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

**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. 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 URLs 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 7: Authentication and User session Response Codes**

<table>
<thead>
<tr>
<th>Header Key</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="https://app1-apigw.central.arubanetworks.com/oauth2/token">https://app1-apigw.central.arubanetworks.com/oauth2/token</a></td>
<td>csrftoken=xxxx; session=xxxx The server returns a CSRF token and identifies the user session, which must be used for all subsequent HTTP requests.</td>
</tr>
</tbody>
</table>

**Example**

**Request Method:** POST

**URL:** https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/login?client_id=<client_id> HTTP/1.1

**Host:** app1-apigw.central.arubanetworks.com

**Request Header:**
Accept: application/json
Content-Type: application/json

POST Request Body (JSON):
{
   "username": "xxxxx",
   "password": "xxxxx"
}

Error Response:
400: Bad Request
Response Body (JSON):
{
   "extra": {},
   "message": "<error string>"
}
401: Auth failure
Response Body (JSON):
{
   "message": "Auth failure",
   "status": false
}

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.

Table 8: URL to Generate Client Credentials

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/client_credentials?client_id=">https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/client_credentials?client_id=</a>&lt;msp_client_id&gt;</td>
<td>The &lt;msp_client_id&gt; variable is the client ID given from Central to that a Managed Service Provider that user registered the application.</td>
</tr>
</tbody>
</table>

Example

Request Method: POST

POST Request Body (JSON):
{
   "customer_id": "<tenant_id>"
}
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 9: URL for to Generate an Authorization Code

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api</code></td>
<td>The endpoint is a POST call to get an authorization code.</td>
</tr>
</tbody>
</table>

Query parameters for this API are as follows:

Table 10: Query Parameters for the Auth Code API

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client_id</td>
<td>client_id is a unique hexadecimal string</td>
<td>The client_id 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.</td>
</tr>
<tr>
<td>response_type</td>
<td>code</td>
<td>Use code as the response type to get the authorization code that can be exchanged for token</td>
</tr>
<tr>
<td>scope</td>
<td>all or read</td>
<td>Requested API permissions may be either all (for both read and write access) or read for read-only access.</td>
</tr>
</tbody>
</table>

Example

Request Method: POST

URL: `https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/?client_id=<client_id>&response_type=code&scope=all` HTTP/1.1

Host: app1-apigw.central.arubanetworks.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}

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 11: URL for to Generate an Auth Token

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://app1-apigw.central.arubanetworks.com/oauth2/token">https://app1-apigw.central.arubanetworks.com/oauth2/token</a></td>
<td>The endpoint is a POST call to get an access token using the authorization code obtained from the server.</td>
</tr>
</tbody>
</table>

Query parameters for this API are as follows:

Table 12: Query Parameters for the Auth Code API

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client_id</td>
<td>client_id is a unique hexadecimal string</td>
<td>The client_id 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.</td>
</tr>
<tr>
<td>client_secret</td>
<td>client_secret is a unique hexadecimal string</td>
<td>The client_secret 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.</td>
</tr>
<tr>
<td>grant_type</td>
<td>authorization_code</td>
<td>Use code to get the authorization code that can be exchanged for the token.</td>
</tr>
</tbody>
</table>
### Parameter Values Description

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

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

**Table 13: Auth Token Values**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>token_type</td>
<td>bearer</td>
<td>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>)</td>
</tr>
<tr>
<td>refresh_token</td>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>expires_in</td>
<td>seconds</td>
<td>The lifetime, in seconds, of the access token.</td>
</tr>
<tr>
<td>access_token</td>
<td>string</td>
<td>Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client.</td>
</tr>
</tbody>
</table>

**Example**

**Request Method:** POST

**URL:** https://apigw-prod2.central.arubanetworks.com/oauth2/token?client_id=<Ccentral-API-app-clientid>&client_secret=xxxx&grant_type=authorization_code&code=xxxx

**Content-Type:** application/json

**Response:**

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

**Step 5: Refreshing a Token**

You can use the refresh token obtained in the previous step to update the access token without repeating the entire authentication process.

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

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://apigw-central.arubanetworks.com/oauth2/token">https://apigw-central.arubanetworks.com/oauth2/token</a></td>
<td>The endpoint is a POST call to refresh the access token using the refresh token obtained from the server</td>
</tr>
</tbody>
</table>
Query parameters for this API are as follows:

**Table 15: Query Parameters for Refresh Tokens**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client_id</td>
<td>client_id is a unique hexadecimal string</td>
<td>The client_id 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.</td>
</tr>
<tr>
<td>client_secret</td>
<td>client_secret is a unique hexadecimal string</td>
<td>The client_secret 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.</td>
</tr>
<tr>
<td>grant_type</td>
<td>refresh_token</td>
<td>Specify refresh_token as the grant type to request that an authorization code be exchanged for a token</td>
</tr>
<tr>
<td>refresh_token</td>
<td>string</td>
<td>A string representing the authorization granted to the client by the resource owner.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>token_type</td>
<td>bearer</td>
<td>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>.</td>
</tr>
<tr>
<td>refresh_token</td>
<td>string</td>
<td>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.</td>
</tr>
<tr>
<td>expires_in</td>
<td>seconds</td>
<td>The expiration duration of the access tokens in seconds.</td>
</tr>
<tr>
<td>access_token</td>
<td>string</td>
<td>Access tokens are credentials used to access the protected resources. An access token is a string representing an authorization issued to the client.</td>
</tr>
</tbody>
</table>

**Example**

**Method:** POST


**Response**

```json
{
  "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>
<thead>
<tr>
<th>Table 16: URL to Delete a Token</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
</tr>
<tr>
<td><a href="https://app1-apigw.central.arubanetworks.com/oauth2/token">https://app1-apigw.central.arubanetworks.com/oauth2/token</a></td>
</tr>
</tbody>
</table>

**Example**

**Method**: DELETE

**URL**: https://app1-apigw.central.arubanetworks.com/oauth2/api/tokens

**JSON Body**:

```json
{
   "access_token": "<access_token_to_be_deleted>",
   "customer_id": "<customer_id_to_whom_token_belongs_to>"
}
```

**Headers**:

- **Content-Type**: application/json
- **X-CSRF-Token**: <CSRF_token_obatained_from_login_API>
- **Cookie**: "session=<session_obatained_from_login_API>"

**Viewing Usage Statistics**

The API Gateway page includes the Usage tab that displays the API usage. The Usage tab is available only for administrators and the usage data is stored only for the previous 30 days. The following details are displayed:

- Assigned rate limit.
- Total usage.
- Per user usage.
- MSP and tenant usage if you are in MSP mode.

The administrator receives an alert through text message or email when the API usage reaches a threshold. You can set the threshold to 75% of the rate limit value.

To view the usage statistics for users of API Gateway, complete the following steps:

1. In the Account Home page, under Global Settings, click API Gateway.
   
   The API Gateway page is displayed.

2. Click Usage. The following details are displayed:
- **Rate Limit**—The total rate limit assigned for API calls for a month.

- **Total Usage:**
  - **Date**—The date of usage.
  - **Usage Per Day**—Usage per day.
  - **Usage Percentage**—Usage percentage for a specific date.

- **Per User Usage:**
  - **User**—The name of the user.
  - **Date**—The date on which the application was accessed.
  - **Usage Per Day**—The total usage by the user per day. This is derived based on the total number of API calls made on a per day basis. This is an aggregate across all customers.

- If you are in MSP mode, the **MSP & Tenant Usage** table is displayed:
  - **Tenant ID**: ID of the tenant account.
  - **Date**: The date on which the application was accessed.
  - **Usage Per Day**: The total usage by the tenant account per day. This is derived based on the total number of API calls made on a per day basis.

The **Usage** tab is only available for administrators and the usage data is stored only for the previous 30 days.

---

**Webhooks**

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

Using Aruba Central, you can integrate Webhooks with other third-party applications such as ServiceNow, Zapier, IFTTT, and so on.

You can access the Webhooks service either through the Aruba Central UI or API Gateway. Aruba Central supports creating up to 10 Webhooks. To enable redundancy, Aruba Central allows you to add up to three URLs per Webhook.
From Aruba Central, you can add, list, or delete Webhooks; get or refresh Webhooks token; get or update Webhooks settings for a specific item; and test Webhooks notification.

This section includes the following topics:
- Creating and Updating Webhooks Through the UI on page 23
- Refreshing Webhooks Token Through the UI on page 24
- Creating and Updating Webhooks Through the API Gateway on page 24
- List of Webhooks APIs on page 25
- Sample Webhooks Payload Format for Alerts on page 26

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 Aruba Central integrates with third-party applications using Webhooks.

**Figure 1  Webhooks Integration**

---

**Creating and Updating Webhooks Through the UI**

To access the Webhooks service from the UI:

1. In the Account Home page, under Global Settings, click Webhooks. The Webhooks page is displayed.
2. In the Webhook tab, click +Webhook.
**a. Webhook Name**—Enter a name for the Webhook

**b. URLs**—Enter the URL. Click + to enter another URL. You can add up to three URLs.

3. Click **Save**. The Webhooks is created and listed in the **Webhook** table.

The **Webhook** table displays the following information and also allows you to edit or delete Webhooks:

- **Name**—Name of the Webhooks.
- **Number of URL Entries**—Number of URLs in Webhooks. Click the number to view the list of URLs.
- **Updated At**—Date and time at which Webhooks was updated.
- **Webhook ID**—Webhooks ID.
- **Token**—Webhooks token. Webhooks token enables header authentication and the third-party receiving service must validate the token to ensure authenticity.
- **Edit**—In the **Webhook** table, select the Webhook from the list and click ✉️ icon to edit the Webhook. You can refresh the token and add URLs. Click **Save** to save the changes.

- **Delete**—In the **Webhook** table, select the Webhook from the list and click ✗ icon and click **Yes** to delete the Webhook.

---

**Refreshing Webhooks Token Through the UI**

To refresh Webhooks token through the UI:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**. The **Webhooks** page is displayed.

2. In the **Webhook** table, select the Webhook from the list and click ✉️ icon to edit.

3. In the pop-up window, click the refresh icon next to the token. The token is refreshed.

---

**Creating and Updating Webhooks Through the API Gateway**

The following HTTP methods are defined for Aruba 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 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 **Account Home** page, under **Global Settings**, click **API Gateway**.
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.

For more information on Webhooks APIs, refer to https://app1-apigw.central.arubanetworks.com/swagger/central.

List of Webhooks APIs

Aruba Central supports the following Webhooks APIs:

- **GET /central/v1/webhooks**—Gets a list of Webhooks.
  
The following is a sample response:
  ```json
  {
    "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": "KEu5ZPTi44U04MnMiOqz"
      }
    ]
  }
  ```

- **POST /central/v1/webhooks**—Creates Webhooks.
  
The following is a sample response:
  ```json
  {
    "name": "AAA",
    "wid": "e829a0f6-1e36-42fe-bafd-631443c8d581"
  }
  ```

- **DELETE /central/v1/webhooks/{wid}**—Deletes Webhooks.
  
The following is a sample response:
  ```json
  {
    "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8"
  }
  ```

- **GET /central/v1/webhooks/{wid}**—Gets Webhooks settings for a specific item.
  
The following is a sample response:
  ```json
  {
    "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:

```json
{
    "name": "AAA",
    "wid": "e829a0f6-1e36-42fe-baf6-631443cbd581"
}
```

- **GET /central/v1/webhooks/{wid}/token**—Gets the Webhooks token for the Webhooks ID.
  
  The following is a sample response:
  
  ```json
  {
    "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:
  
  ```json
  {
    "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:
  ```text
  "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**: 2016-07-12T14:19:07:00
- **X-Central-Customer-ID**: <########>

Refer to the following topics to view sample JSON content:

- **Access Point Alerts—Sample JSON**
- **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 Disconnected**

```json
{
    "alert_type": "AP disconnected",
    "description": "AP with Name 84:d4:7e:c5:c8:8c and MAC address 84:d4:7e:c5:c8:8c disconnected, Group:unprovisioned",
    "timestamp": 1564326129,
}
```
"webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
"setting_id": "201804170291-4",
"state": "Open",
"nid": 4,
"details": {
  "rule_number": "0",
  "group": "1",
  "labels": "",
  "conn_status": "disconnected",
  "params": [
    "84:d4:7e:c5:c8:8c",
    "84:d4:7e:c5:c8:8c"
  ],
  "time": "2019-07-28 15:02:09 UTC"
},
"operation": "create",
"device_id": "CT0779239",
"id": "AWw5Gm2zVQOlZtiGF20e",
"severity": "Critical"

AP Connected Clients

{"alert_type": "AP_CONNECTED_CLIENTS",
"description": "Number of Clients connected to AP with name 84:d4:7e:c5:c8:8c has been above 1 for about 5 minutes since 2019-07-29 12:26:00 UTC.",
"timestamp": 1564326128,
"webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
"setting_id": "201804170291-1255",
"state": "Open",
"nid": 1255,
"details": {
  "rule_number": "0",
  "group": "1",
  "labels": "",
  "name": "84:d4:7e:c5:c8:8c",
  "duration": "5",
  "threshold": "1",
  "time": "2019-07-28 15:02:08 UTC"
},
"operation": "create",
"device_id": "CT0779239",
"id": "AWw5Gm2zVQOlZtiGF20d",
"severity": "Major"

AP CPU Over Utilization

{"alert_type": "AP_CPU_OVER_UTILIZATION",
"description": "CPU utilization for AP 84:d4:7e:c5:c8:8c with serial CT0779239 has been above 10% for about 5 minutes since 2019-07-28 14:21:00 UTC.",
"timestamp": 1564323960,
"webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
"setting_id": "201804170291-1250",
"state": "Open",
"nid": 1250,
"details": {
  "rule_number": "0",
  "group": "1",
  "name": "84:d4:7e:c5:c8:8c",
  "duration": "5",
  "threshold": "10",
  "time": "2019-07-28 14:21:00 UTC"}
AP Memory Over Utilization

{  "alert_type": "AP_MEMORY_OVER_UTILIZATION",  "description": "Memory utilization for AP iap-303-iphone456-offline with serial CNGHKGX004 has been above 40% for about 5 minutes since 2019-07-24 07:11:00 UTC.",  "timestamp": 1563952560,  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",  "setting_id": "201804170291-1251",  "state": "Open",  "nid": 1251,  "details": {    "_rule_number": "1",    "group": "3",    "name": "iap-303-iphone456-offline",    "labels": "3,118",    "duration": "5",    "time": "2019-07-24 07:11:00 UTC",    "threshold": "40",    "ds_key": "201804170291.CNGHKGX004.memory_utilization.5m",    "serial": "CNGHKGX004",    "unit": "%"  },  "operation": "create",  "device_id": "CNGHKGX004",  "id": "AWwi1jihVQO1ZtiGThDA",  "severity": "Major"}

AP Radio Noise Floor

{  "alert_type": "AP_RADIO_NOISE_FLOOR",  "description": "Noise floor on AP iap-303-iphone456-offline operating on Channel 10 and serving 0 clients has been above -110 dBm for about 10 minutes since 2019-07-24 07:06:00 UTC.",  "timestamp": 1563952560,  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",  "setting_id": "201804170291-1253",  "state": "Open",  "nid": 1253,  "details": {    "_rule_number": "0",    "group": "3",    "name": "iap-303-iphone456-offline",    "radio_num": "1",    "client_count": "0",    "labels": "3,118",    "_band": "0",    "duration": "10",    "time": "2019-07-24 07:06:00 UTC",    "threshold": "110",    "ds_key": "201804170291.CNGHKGX004.radio.noisefloor",    "serial": "CNGHKGX004",    "channel": "10"  },  "operation": "create"}
"device_id": "CNGHKGX004",
"id": "AWw1jjyVQ01ZtiGThDB",
"severity": "Critical"

AP Radio Over Utilization

{  
"alert_type": "AP_RADIO_OVER_UTILIZATION",
"description": "Radio utilization on AP 84:d4:7e:c5:c8:8c operating on Channel 36E and serving 0 clients has been above 1% for about 5 minutes since 2019-07-28 14:31:00 UTC."

"timestamp": 1564324560,
"webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
"setting_id": "201804170291-1252",
"state": "Open",
"nid": 1252,
"details": {
"_rule_number": "0",
"group": "1",
"name": "84:d4:7e:c5:c8:8c",
"_radio_num": "0",
"client_count": "0",
"_band": "1",
"duration": "5",
"unit": "%",
"time": "2019-07-28 14:31:00 UTC",
"threshold": "1",
"ds_key": "201804170291.CT0779239.radio.busy64",
"serial": "CT0779239",
"channel": "36E"
},
"operation": "create",
"device_id": "CT0779239",
"id": "AWww5An08VQO1ZtiGFpgm",
"severity": "Critical"

Client Attack detected

{  
"alert_type": "Client attack detected",
"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": "AWw9EmBxVQ01ZtiGO1Q8",
"severity": "Critical"

Connected Clients
**Connected Clients**

```
{  "alert_type": "CONNECTED_CLIENTS",  "description": "Number of Clients connected to swarm with name SetMeUp-CA:35:56 has been above 1 for about 5 minutes since 2019-07-29 12:26:00 UTC.",  "timestamp": 1564403460,  "webhook": "68612ee3-3ee9-4da4-b07b-13977a350344",  "setting_id": "b8be21720dc04a8e9f0028374b6a9bbd-1254",  "state": "Open",  "nid": 1254,  "details": {    "rule_number": "0",    "group": "1",    "name": "SetMeUp-CA:35:56",    "duration": "5",    "aggr_context": "swarm",    "time": "2019-07-29 12:26:00 UTC",    "threshold": "1",    "ds_key": "b8be21720dc04a8e9f0028374b6a9bbd.cluster.156.device.clients.5m",    "serial": "156"  },  "operation": "create",  "device_id": "156",  "id": "AWw9tmhNVQO1ZtiGQR5U",  "severity": "Critical"}
```

**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": "AWw9hCLAVQO1ZtiGP1ig",  "severity": "Critical"}
```

**Insufficient Power Alert**

```
{  "alert_type": "INSUFFICIENT_POWER_ALERT",  "description": "Insufficient inline power supplied to AP-205 with name 04:bd:88:c3:b6:f0",  "timestamp": 1564403450,  "webhook": "68612ee3-3ee9-4da4-b07b-13977a350344",  "setting_id": "b8be21720dc04a8e9f0028374b6a9bbd-21",  "state": "Open",  "nid": 21,  "details": {    "group": "0",    "name": "04:bd:88:c3:b6:f0",  },  "id": "AWw9tqj004",  "severity": "Critical"  }
```
"labels": [],
"label_site_desc": "",
"time": "2019-07-29 12:30:50 UTC",
"serial": "CM0381143",
"group_name": "default",
"ap_model": "AP-205"
},
"operation": "create",
"device_id": "CM0381143",
"id": "AWw9tkNGVQO1ZtiGQRz-",
"severity": "Major"
}

Modem Plugged
{
  "alert_type": "Modem Plugged",
  "description": "Modem plugged to ap with name 84:d4:7e:c5:c8:8c'and MAC address 84:d4:7e:c5:c8:8c",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-18",
  "state": "Open",
  "nid": 18,
  "details": {
    "rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5GmlzJKL90tiGF20d",
  "severity": "Critical"
}

Modem Unplugged
{
  "alert_type": "Modem Unplugged",
  "description": "Modem unplugged from ap with name 84:d4:7e:c5:c8:8c'and MAC address 84:d4:7e:c5:c8:8c",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-19",
  "state": "Open",
  "nid": 19,
  "details": {
    "rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5GmlzJKL90tiGF20d",
  "severity": "Critical"
}

New AP Detected
New AP Detected

```
"alert_type": "New AP detected",
"description": "New AP with Name 84:d4:7e:c5:c8:8c and MAC address 84:d4:7e:c5:c8:8c
detected, Group:unprovisioned",
"timestamp": 1564326128,
"webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
"setting_id": "201804170291-3",
"state": "Open",
"nid": 3,
"details": {
    "rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
        "84:d4:7e:c5:c8:8c",
        "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
},
"operation": "create",
"device_id": "CT0779239",
"id": "AWw5Gm1zVQOl2tiJH56e",
"severity": "Major"
```
Uplink Changed

{
    "alert_type": "Uplink Changed",
    "description": "Uplink changed from 0 to 1 for ap with name {params[2]} and MAC address {params[3]}",
    "timestamp": 1564326128,
    "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
    "setting_id": "201804170291-17",
    "state": "Open",
    "nid": 17,
    "details": {
        "_rule_number": "0",
        "group": "1",
        "labels": "",
        "params": [
            "0",
            "1",
            "84:d4:7e:c5:c8:8c",
            "84:d4:7e:c5:c8:8c"
        ],
        "time": "2019-07-28 15:02:08 UTC"
    },
    "operation": "create",
    "device_id": "CT0779239",
    "id": "AWw5Gm1zVQO1ztiJK891",
    "severity": "Critical"
}

Virtual Controller Disconnected

{
    "alert_type": "Virtual controller disconnected",
    "description": "Virtual Controller with Name SetMeUp-CA:51:D6, Version 8.4.0.0_69847 and IP address 10.29.43.70 disconnected, Group:unprovisioned",
    "timestamp": 1564326128,
    "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
    "setting_id": "201804170291-2",
    "state": "Open",
    "nid": 2,
    "details": {
        "_rule_number": "0",
        "group": "1",
        "labels": "",
        "conn_status": "disconnected",
        "params": [
            "SetMeUp-CA:51:D6",
            "0",
            "1",
            "84:d4:7e:c5:c8:8c",
            "84:d4:7e:c5:c8:8c"
        ],
        "time": "2019-07-28 15:02:08 UTC"
    },
    "operation": "create",
    "device_id": "CT0779239",
    "id": "AWw5Gm1zVQO1ztiJK891",
    "severity": "Critical"
}
Switch Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

**Switch Disconnected**

```
{  
    "alert_type": "Switch Disconnected",
    "timestamp": "2019-09-26 05:18:59 UTC",
    "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
    "setting_id": "e344d961bcd411db279bf92f61b989-203",
    "state": "Open",
    "nid": 203,
    "details": {
        "rule_number": "0",
        "group": "1",
        "labels": "",
        "conn_status": "disconnected",
        "params": [
            "CN8AHKW095",
            "10.22.41.3",
            "Aruba-2930F-24G-PoEP-4SFPP"
        ],
        "time": "2019-09-26 05:18:59 UTC"
    },
    "operation": "create",
    "device_id": "CN8AHKW095",
    "id": "AW1sAhfAYu0OgJ2anzUD",
    "severity": "Major"
}
```

**New Switch Connected**

```
{  
    "alert_type": "New Switch Connected",
    "timestamp": "2019-07-28 15:02:08 UTC",
    "device_id": "CT0779239",
    "id": "AWw5Gm1zVQO12tiGF20d",
    "severity": "Critical"
}
```
Switch Memory Over Utilization

{
    "alert_type": "SWITCH_MEMORY_OVER_UTILIZATION",
    "description": "Memory utilization for Switch Aruba-2930F-24G-PoEP-4SFPP with serial CN8AHKW095 has been above 10% for about 5 minutes since 2019-09-26 05:48:00 UTC",
    "timestamp": 1569477180,
    "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
    "setting_id": "e344d961bccd411dbd279bf92f61b989-1301",
    "state": "Open",
    "nid": 1301,
    "details": {
        "_rule_number": "0",
        "group": "1",
        "name": "Aruba-2930F-24G-PoEP-4SFPP",
        "duration": "5",
        "time": "2019-09-26 05:48:00 UTC",
        "threshold": "10",
        "ds_key": "e344d961bccd411dbd279bf92f61b989-CN8AHKW095.memory_utilization.5m",
        "serial": "CN8AHKW095",
        "unit": "%"
    },
    "operation": "create",
    "device_id": "CN8AHKW095",
    "id": "AW1sF81GYu00gJ2an0Aq",
    "severity": "Major"
}

Switch CPU Over Utilization

{
    "alert_type": "SWITCH_CPU_OVER_UTILIZATION",
    "description": "CPU utilization for Switch Aruba-2930F-48G-PoEP-4SFPP with serial CN88HKX1CR has been above 5% for about 5 minutes since 2019-09-26 06:07:00 UTC",
    "timestamp": 1569478320,
    "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
    "setting_id": "e344d961bccd411dbd279bf92f61b989-1300",
    "state": "Open",
    "nid": 1300,
    "details": {
        "_rule_number": "0",
        "group": "41",
        "name": "Aruba-2930F-48G-PoEP-4SFPP",
        "duration": "5",
        "time": "2019-09-26 06:07:00 UTC",
        "threshold": "5",
        "ds_key": "e344d961bccd411dbd279bf92f61b989-CN88HKX1CR.cpu_utilization.5m",
        "serial": "CN88HKX1CR",
        "unit": "%"
    },
    "operation": "create",
    "device_id": "CN88HKX1CR",
    "id": "AW1sMqB4Yu00gJ2an0UP",
    "severity": "Critical"
"severity": "Critical"
}

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": "e344d961bcdc411dbd279bf92f61b989-1303",
"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": "e344d961bcdc411dbd279bf92f61b989.CN8AHKW095.intf.rx_utilization.5m",
"serial": "CN8AHKW095",
"unit": "%"
},
"operation": "create",
"device_id": "CN8AHKW095",
"id": "AW1tvTgBYu0OgJ2aoCgl",
"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": "e344d961bcdc411dbd241dbd279bf92f61b989-1302",
"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": "e344d961bcdc411dbd279bf92f61b989.CN8AHKW095.intf.tx_utilization.5m",
"serial": "CN8AHKW095",
"unit": "%"
},
"operation": "create",
"device_id": "CN8AHKW095",
"id": "AW1tvTgBYu0OgJ2aoCgl",
"severity": "Critical"
}

Switch POE Utilization
Switch Interface Input Errors

```json
{
  "alert_type": "SWITCH_INTERFACE_INPUT_ERRORS",
  "description": "Input errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFP 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": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFP",
    "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

```json
{
  "alert_type": "SWITCH_INTERFACE_OUTPUT_ERRORS",
  "description": "Output errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFP 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": 1307,
  "details": {
```
Switch Mismatch Config
{
    "alert_type": "Switch Mismatch Config",
    "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-2930F-48G-PoEP-4SFPP",
    "timestamp": 1569505920,
    "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
    "setting_id": "e344d961bccc411dbd279bf92f61b989-1307",
    "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": "AW1t18ccYu00gJ2aoDYw",
    "severity": "Critical"
}

Switch Hardware Failure
{
    "alert_type": "SWITCH_HARDWARE_FAILURE",
    "description": "Switch with serial CN8AHKW095 : Fan 1 failed",
    "timestamp": 1569505920,
    "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
    "setting_id": "e344d961bccc411dbd279bf92f61b989-1307",
    "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": "AW1t18ccYu00gJ2aoDYw",
    "severity": "Critical"
}
Switch Interface Duplex Mode

```
{  
    "alert_type": "SWITCH_INTERFACE_DUPLEX_MODE",
    "description": "Interface 19 on switch Aruba-2930F-24G-PoEP-4SFPP with serial CN8AHKW095 is operating at Half-Duplex mode",
    "timestamp": 1569901561,
    "webhook": "c71404f4-00c1-4241-8bf4-c8d3f981ca2a",
    "setting_id": "e344d961bccd411dbd279bf92f61b989-1306",
    "state": "Open",
    "nid": 1306,
    "details": {  
        "group": "1",
        "name": "Aruba-2930F-24G-PoEP-4SFPP",
        "labels": "",
        "mode": "Half",
        "intf_name": "19",
        "time": "2019-10-01 03:46:01 UTC",
        "serial": "CN8AHKW095"
    },
    "operation": "create",
    "device_id": "CN8AHKW095",
    "id": "AW2FbMi0Yu00G2asaWh",
    "severity": "Critical"
}
```

Gateway Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

**WAN Uplink Flap**

```
{
    "alert_type": "WAN_UPLINK_FLAP",
    "description": "Uplink link1_inet link status flapped 1% on device with CNHHKLB031 for about 15 minutes since 2019-07-25 12:36:00 UTC.",
    "timestamp": 1564059060,
    "webhook": "394c7a3c-ca41-4476-8afc-857e54a4b3b",
    "setting_id": "abce082bef4a428bb31366f6d6ff223f-1600",
    "state": "Open",
    "nid": 1600,
    "details": {  
        "status": "DOWN",
        "_rule_number": "0",
        "group": "77",
        "labels": "8,661",
        "current_status": "UP",
        "duration": "15",
        "intf_name": "link1_inet",
        "time": "2019-07-25 12:36:00 UTC",
        "threshold": "1",
        "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.uplink.flap.5m",
        "serial": "CNHHKLB031",
        "uplink_tag": "link1_inet",
        "unit": "%"
    },
    "operation": "create",
    "device_id": "CNHHKLB031",
    "id": "AWwpL0fvVQO1ZtiGh-2_
    "severity": "Critical"
}
```

**WAN Tunnel Flap**
WAN Tunnel Flap

```
{  "alert_type": "WAN_TUNNEL_FLAP",  "description": "Tunnel data-vpnc-00:1a:1e:03:83:30-link1_inet status flapped 1% on device CNHHKLB031 for about 15 minutes since 2019-07-25 12:26:00 UTC.",  "timestamp": 1564058460,  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1601",  "state": "Open",  "nid": 1601,  "details": {    "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",    "rule_number": "0",    "group": "77",    "dst_ip": "172.168.101.9",    "labels": "8,661",    "src_ip": "192.168.51.254",    "duration": "15",    "time": "2019-07-25 12:26:00 UTC",    "threshold": "1",    "ds_key": "abce082bef4a428bb31366f6d6ff223f-CNHHKLB031.uplink.tunnel.flap.5m",    "serial": "CNHHKLB031",    "uplink_tag": "link1_inet",    "unit": "%"  },  "operation": "create",  "device_id": "CNHHKLB031",  "id": "AWwpJiAiVQQ1ZtiGh5tw",  "severity": "Critical"}
```

WAN Auto Negotiation Flap

```
{  "alert_type": "WAN_AUTO_NEGOTIATION_FLAP",  "description": "Uplink GE0/0/1 speed flapped 1% on device CNHHKLB031 for about 15 minutes since 2019-07-25 12:32:00 UTC.",  "timestamp": 1564058820,  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1602",  "state": "Open",  "nid": 1602,  "details": {    "new_speed": "Auto",    "group": "77",    "labels": "8,661",    "duration": "15",    "rule_number": "0",    "intf_name": "GE0/0/1",    "time": "2019-07-25 12:32:00 UTC",    "threshold": "1",    "ds_key": "abce082bef4a428bb31366f6d6ff223f-CNHHKLB031.uplink.speed.flap.5m",    "serial": "CNHHKLB031",    "speed": "1000",    "unit": "%"  },  "operation": "create",  "device_id": "CNHHKLB031",  "id": "AWwpK55sVQQ1ZtiGh8zr",  "severity": "Minor"}
```

WAN IPsec SA Establishment Failed

```
{  "alert_type": "WAN_IPSEC_SA_ESTABLISHMENT_FAILED",  "description": "IPSec Tunnel Establishment from 192.168.51.254 to 172.168.101.9 failed
```
WAN IPsec SA Down

```
{"alert_type": "WAN_IPSEC_SA_DOWN",
"description": "IPSec tunnel from 192.168.52.254 to 172.168.101.9 is DOWN on device CNHHKLB031.
"timestamp": "2019-07-25 12:49:56 UTC",
"webhook": "394c7a3c-ca41-4476-8afc-857e54a4b3b",
"setting_id": "abce082bef4a428bb31366f6d6ff223f-1550",
"state": "Open",
"nid": 1550,
"details": {
  "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",
  "group": "77",
  "name": "None",
  "labels": [
    "8",
    "661"
  ],
  "src_ip": "192.168.51.254",
  "link_tag": "link1_inet",
  "time": "2019-07-25 12:40:22 UTC",
  "dst_ip": "172.168.101.9",
  "serial": "CNHHKL031"
},
"operation": "create",
"device_id": "CNHHKLB031",
"id": "AWwpLlB0VQO1ZtiGh-WS",
"severity": "Minor"
}
```

WAN IPsec SA All Down

```
{"alert_type": "WAN_IPSEC_SA_ALL_DOWN",
"description": "All IPSec SAs down for device CNHHKL031 at 2019-07-25 12:40:22 UTC",
"timestamp": "2019-07-25 12:40:22 UTC",
"webhook": "394c7a3c-ca41-4476-8afc-857e54a4b3b",
"setting_id": "abce082bef4a428bb31366f6d6ff223f-1550",
"state": "Open",
"nid": 1551,
"details": {
  "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link2_mpls",
  "group": "77",
  "name": "None",
  "labels": [
    "8",
    "661"
  ],
  "src_ip": "192.168.52.254",
  "reason": "Administrator cleared IPSEC SA",
  "time": "2019-07-25 12:40:22 UTC",
  "dst_ip": "172.168.101.9",
  "serial": "CNHHKL031",
  "uplink_tag": "link2_mpls"
},
"operation": "create",
"device_id": "CNHHKLB031",
"id": "AWwpJY4aVQO1ZtiGh5c-",
"severity": "Minor"
}
```
CFG Set Advertisement Failure

```json
{  "alert_type": "CFG_SET_ADVERTISEMENT_FAILURE",  "description": "CFG-Set advertisement failure for Gateway with CNHHKLBO31 on tunnel data-vpnc-00:1a:1e:03:83:30-link1_inet from 192.168.51.254 to 172.168.101.9",  "timestamp": 1564059635,  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1554",  "state": "Open",  "nid": 1554,  "details": {  "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",  "group": "77",  "name": "None",  "labels": [  "8",  "661"  ],  "src_ip": "192.168.51.254",  "time": "2019-07-25 13:00:35 UTC",  "map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",  "dst_ip": "172.168.101.9",  "serial": "CNHHKLBO31"  },  "operation": "create",  "device_id": "CNHHKLBO31",  "id": "AWwpOBVQO1ZtiGlD0f",  "severity": "Major"}
```

Controller CPU Over Utilization

```json
{  "alert_type": "CONTROLLER_CPU_OVER_UTILIZATION",  "description": "CPU utilization for Gateway Aruba9004_40_0C_28 with serial CNHHKLBO31 has been above 1% for about 15 minutes since 2019-07-25 09:30:00 UTC.",  "timestamp": 1564047900,  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1351",  "state": "Open",  "nid": 1351,  "details": {  "_rule_number": "0",  "group": "77",  "name": "Aruba9004_40_0C_28",  "labels": "8,661",  "rule": ""}
```
Controller Memory Over Utilization

```
{  "alert_type": "CONTROLLER_MEMORY_OVER_UTILIZATION",  "description": "Memory utilization for Gateway Aruba9004_40_0C_28 with serial CNHHKLB031 has been above 1% for about 10 minutes since 2019-07-25 09:30:00 UTC.",  "timestamp": 1564047600,  "webhook": "394c7a3c-ca41-4476-8afc-857e54a4b3b",  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1352",  "state": "Open",  "nid": 1352,  "details": {    "_rule_number": "0",    "group": "77",    "name": "Aruba9004_40_0C_28",    "labels": "8,661",    "duration": "10",    "time": "2019-07-25 09:30:00 UTC",    "threshold": "1",    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.memory_utilization.5m",    "serial": "CNHHKLB031",    "unit": "%"  },  "operation": "create",  "device_id": "CNHHKLB031",  "id": "AWwohP4LVQO1ZtiGgfbQ",  "severity": "Critical"}
```

Controller OSPF Session Error

```
{  "alert_type": "CONTROLLER_OSPF_SESSION_ERROR",  "description": "OSPF session state change for Gateway with hostname GSK_VPN2 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": "b27f67fa44234c51a890fceeae7c9b3e-1354",  "state": "Open",  "nid": 1354,  "details": {    "dst_state": "Down State",    "neighbour_ip": "1.0.0.2",    "group": "4",    "uniq_identifier": "100-16777218",    "labels": [      "O",      "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"
}

Gateway Base License Capacity Exceeded
{
"alert_type": "GATEWAY_BASE_LICENSE_CAPACITY_EXCEEDED",
"description": "Base license capacity limit exceeded for Gateway with name: Dev-BR1-GW-Kafka, serial: CP0015859",
"timestamp": 1564141290,
"webhook": "1348bcc4-ce00-4180-b314-32849c3638a1",
"setting_id": "2fb4b8a7e77c496395950510a1d270bc-1356",
"state": "Open",
"nid": 1356,
"details": {
"serial": "CP0015859",
"labels": [],
"group": "1",
"name": "Dev-BR1-GW-Kafka",
"time": "2019-07-26 11:41:30 UTC"
},
"operation": "create",
"device_id": "CP0015859",
"id": "AWwuFgZqnGtA5yFV0hCr",
"severity": "Critical"
}

DHCP Pool Consumption Alert
{
"alert_type": "DHCP_POOL_CONSUMPTION_ALERT",
"description": "DHCP Pool Consumption on Gateway CNHHKL031 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": "abce082be4a428bb31366f6d6ff223f-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": "CNHHKL031",
"unit": "%"
},
"operation": "create",
"device_id": "CNHHKL031",
"id": "AWwpOfQAVQO1ZtiGiE2H",
"severity": "Critical"
}

WAN Auto Negotiation
WAN Uplink Status Change

{  "alert_type": "WAN_UPLINK_STATUS_CHANGE",  "description": "Uplink port link1_inet status change UP -> DOWN for device with CNHHKLB031 at 2019-07-25 09:22:31 UTC",  "timestamp": 1564046551,  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",  "setting_id": "abc210b2f4a428bb31366f6d6efb223f-1505",  "state": "Open",  "nid": 1505,  "details": {    "current_status": "DOWN",    "intf_name": "link1_inet",    "time": "2019-07-25 09:22:31 UTC",    "serial": "CNHHKLB031",    "uplink_tag": "link1_inet"  },  "operation": "create",  "device_id": "CNHHKLB031",  "id": "AWwocGtYVQO1ZtiGgT03",  "severity": "Major"}
Miscellaneous Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

**Device Config Change Detected**

```json
{
    "alert_type": "DEVICE_CONFIG_CHANGE_DETECTED",
    "description": "Config change detected on group nbapi_test for device type Switch by user example@hpe.com. 
    \n    Content: Template Updated 
    \n    ip address dhcp-bootp
    \n    vlan 13
    \n    no ip address
    
    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"
}
```

**User Account Deleted**

```json
{
    "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": "AW1dqe6rYu0OgJ2alXzT",
    "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": "AW1dq6nYu0OgJ2alX11",
  "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"
}