

# **HPE Aruba Networking Central and ServiceNow Integration Guide**



**Hewlett Packard**  
Enterprise

## Copyright Information

© Copyright 2024 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



This document outlines the configuration process required on HPE Aruba Networking Central and ServiceNow to create a fully integrated IT incident reporting solution through a Webhook.

## 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>

ServiceNow is an IT service management platform that allows you to automatically create incidents or IT tickets based on a live data feed from a Webhook service. If you have a ServiceNow instance, you can configure a Webhook service on HPE Aruba Networking Central to send a notification feed. The ServiceNow integration enables your current IT Infrastructure management systems to automatically generate an IT incident or a ticket whenever an alert is triggered due to a user-generated event in HPE Aruba Networking Central.

## Before You Begin

Before you begin, ensure that you have a valid ServiceNow account. If you do not have a ServiceNow instance, create an instance before you proceed with the steps described in following sections.

For more information on creating a ServiceNow instance, see the [ServiceNow user documentation](#).

## Integration Workflow

Complete the following steps to enable ServiceNow integration with HPE Aruba Networking Central:

- [Step 1: Add the Hash Library to Your ServiceNow Instance](#)
- [Step 2: Create a Scripted REST API to Obtain a Webhook URL](#)
- [Step 3: Configure a Webhook in HPE Aruba Networking Central](#)
- [Step 4: Configure an Alert in HPE Aruba Networking Central](#)
- [Step 5: Verify the Integration Status](#)

### Step 1: Add the Hash Library to Your ServiceNow Instance

To get started with the ServiceNow integration, create a new script with the [hash library](#) in your ServiceNow instance. The hash library is required for header authentication.

1. Log in to [ServiceNow](#) with your user credentials.
2. Click **Manage > Instance** and log in to your instance.
3. Go to **System Definition > Script Includes**.
4. Click **New**.
5. Name the script as **Hashes**.
6. Select **All application scopes** from the **Accessible from** drop-down list.
7. Select the **Client callable** check box.
8. Go to the GitHub Gist website that hosts the hash library.
9. Copy the **snow\_hashes.js** file content and paste it in the **Script** text box.
10. Click **Submit**.

## Step 2: Create a Scripted REST API to Obtain a Webhook URL

To create a Scripted REST API to obtain a webhook URL, complete the following steps:

1. In your ServiceNow instance, go to **System Web Services > Scripted REST APIs**.
2. Click **New**. The REST API creation page is displayed.
3. Provide a name and the API ID.
4. Click **Submit**. The API is added to the list of REST APIs.
5. Open the REST API you just created.
6. To add a REST resource with header and query parameters, click **New** in the **Resources** tab. The **Scripted REST Resource New record** page is displayed.
7. Provide a name for the resource.
8. Select **POST** for the HTTP method.
9. Clear the **Requires authentication** check box.
10. In the **Script** section, add the following text:

```
(function process( /*RESTAPIRequest*/ request, /*RESTAPIResponse*/ response) {
    // Calculate signature for verification using request headers, data and
    token
    var centralService = request.getHeader('X-Central-Service');
    var centralDeliveryId = request.getHeader('X-Central-Delivery-ID');
    var centralDeliveryTimestamp = request.getHeader('X-Central-Delivery-
    Timestamp');
    var token = "<webhook_token>";
    var body = request.body.dataString;
    var message = body + centralService + centralDeliveryId +
    centralDeliveryTimestamp;
    var calculatedSign = new Hashes.SHA256().b64_hmac(token, message);
    var signFromServer = request.getHeader('X-Central-Signature'); // Signature
    sent by Aruba Central
    var low_severities = ["Minor", "Warning"];
    if (calculatedSign == signFromServer) {
        event = JSON.parse(body);
        // Only process events from Central which has status Open
        if (event.state == "Open") {
            var inc = new GlideRecord('incident');
            inc.initialize();
            inc.short_description = event.alert_type;
            inc.state = 1;
            if (low_severities.includes(event.severity)) {
                inc.impact = 3;
                inc.urgency = 3;
            } else if (event.severity == "Major") {
                inc.impact = 2;
                inc.urgency = 2;
            }
        }
    }
}
```

```

    } else if (event.severity == "Critical") {
        inc.impact = 1;
        inc.urgency = 1;
    }
    inc.description = event.description;
    inc.insert();
}
response.setStatus(200);
response.setBody({
    status: "success"
});
} else {
    response.setStatus(200);
    response.setBody({
        status: "failure"
    });
}
})(request, response);

```



After you create a Webhook in HPE Aruba Networking Central, replace the Webhook token (see highlighted text in the above code sample) in your Scripted REST API.

11. Click **Submit**. The Scripted REST API you just created is added to your list of APIs.

	Name	API ID	Base API path	Active	is versioned
<input type="checkbox"/>	Alerts	alerts	/api/2/0070/alerts	true	false
<input type="checkbox"/>	Benchmark Client API	benchmark_client_api	/api/sn_bm_client/benchmark_client_api	true	false
<input type="checkbox"/>	CAB Workbench (Internal API)	cab	/api/sn_change_cab/cab	true	false
<input type="checkbox"/>	Code Search	code_search	/api/sn_codesearch/code_search	true	true

12. Note the base API path. The base API path must be appended to your Webhook URL.
13. Ensure that your Webhook URL is in the following format:

<https://<yourInstanceName>.service-now.com/<baseApiPath>>.

## Step 3: Configure a Webhook in HPE Aruba Networking Central

To create a Webhook in HPE Aruba Networking Central, complete the following steps:

1. In the **Aruba Central** app, set the filter to **Global**.
2. Under **Maintain**, click **Organization > Platform Integration > Webhooks**. The **Webhooks** page is displayed.

- In the **Webhook** tab, click + sign. The **Add Webhook** pop-up window is displayed.

**Figure 1** Webhooks Page

	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 2** 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

- To create webhooks, enter the following details:
  - Name**—Enter a name for the Webhook
  - Retry Policy**— Select any one of the following options:
    - **None**—Select this to have no retry.
    - **Important**—Select this to have up to 5 retries over 6 minutes.
    - **Critical**—Select this to have up to 5 retries over 32 hours.
  - URLs**—Enter the URL. Click + to enter another URL. You can add up to three URLs.

<https://<yourInstanceName>.service-now.com/<baseApiPath>>

The URL must include your ServiceNow instance and the base API path generated for your Scripted REST API.

- Click **Save**. The Webhooks is created and listed in the **Webhook** table.
- Note the token ID.
- Go back to your ServiceNow instance and update the Webhook token in the script text of the Scripted REST API you created in [step 2](#).





You can also create a Webhook using the API interface. For more information, see [Webhooks](#) in HPE Aruba Networking Central documentation portal.

## Step 4: Configure an Alert in HPE Aruba Networking Central

To configure an alert in HPE Aruba Networking Central, complete the following steps:

1. In the WebUI, set the filter to **Global**.
2. Under **Analyze**, click **Alerts & Events** to view the alert and events dashboard.
3. To configure alerts, click the **Config** icon.
4. In the **Alert Severities & Notifications** page, click **All**.
5. Select an alert and click **+** to enable the alert with default settings.
6. Configure the following alert parameters.
  - a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning.
  - b. **Duration**—Enter the duration in minutes.
  - c. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting any of the following parameters:
    - **Group**—Select a group to limit the alert to a specific group.
    - **Label**—Select a label to limit the alert to a specific label.
    - **Device**—Select a device to limit the alert to a specific device.
  - d. Select **Webhook** check box under **Notification Options** and select a webhook from the drop-down list.
  - e. Click **Save**.

## Step 5: Verify the Integration Status

To verify if the integration is successful, complete the following steps:

1. Trigger an alert from HPE Aruba Networking Central.
2. Verify if an incident is created in your ServiceNow instance.

