Monitoring Aruba Central

Aruba Central PowerPack version 200

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Aruba Central in SL1 using the *Aruba Central* PowerPack.

This chapter covers the following topics:

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is Aruba Central?

Aruba Central is a cloud-based platform that provides management tools and built-in analytics for Aruba Instant Access Points (IAPs), switches, and gateways. In each Aruba network, one IAP acts as a virtual controller, which is a single configuration and management point for the network.

What Does the Aruba Central PowerPack Monitor?

To monitor Aruba Central using SL1, you must install the *Aruba Central* PowerPack. This PowerPack enables you to discover, model, and collect data about Aruba Central virtual controllers and their components.

The *Aruba Central* PowerPack includes:

- Dynamic Applications to discover and monitor Aruba Central virtual controllers and their component devices
- Device Classes for each of the Aruba Central components that the *Aruba Central* PowerPack can monitor
- Event Policies that are triggered when Aruba Central component devices meet certain status criteria
- Two samples of SOAP/XML Credential that you can use to create your own Aruba Central Credential
- A Device Template that aligns Dynamic Applications to the Aruba Central virtual controller and enables you to discover component devices for that virtual controller
- Device Dashboards that display information about Aruba Central component devices

Installing the Aruba Central PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Aruba Central* PowerPack.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. For more information, see t *Global Settings*.

IMPORTANT: The minimum required MySQL version is 5.6.0.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.

4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

TIP: If you are currently using a version prior to 103 of this PowerPack, a direct upgrade to version 200 is not supported and a fresh install and re-discovery of devices may be required with version 200. Versions 103, 104, and 104.1 can be upgraded directly to version 200 if there is only one DCM tree discovered per Aruba Central account. If separate API keys are being used to discover sites individually as their own DCM tree, a fresh install and re-discovery is also required. The steps for both methods can be found below. Follow those procedures to ensure accurate data collection post upgrade.

After upgrading the PowerPack to version 200, follow the steps below:

1. Disable the listed Dynamic Applications.
    - Aruba: Central AP Container Discovery
    - Aruba: Central SD-WAN Gateway Container Discovery
    - Aruba: Central Switch Container Discovery

NOTE: For instructions on disabling Dynamic Applications, see the section on "Performing Other Tasks in the Dynamic Application Manager Page " in the ***Dynamic Application Development*** manual.

2. Disable the listed container device components.
    - AP Container
    - SD-WAN Gateway Container
    - Switch Container
3. Apply the new Aruba template included in this version of the PowerPack to the root virtual device. This will cause devices to move from the container component devices to sites.

NOTE: For instructions on applying a template, see the see the *Aligning the Device Template to Your Aruba Central Virtual Device* section.

4. Once all components have been migrated to sites, remove the empty container device components listed in step 2.
5. Delete the disabled Dynamic Applications listed in step 1.

To ensure accurate data collection after upgrading PowerPack from any of the previous versions, perform the additional steps to authenticate using Oauth Grant Mechanism:

1. Go to the **Credential Management** page (System > Manage > Credentials). Identify your current credential and click on the credential's name to edit.
2. In the ***Embed Password [%P]*** field, type your Aruba Central client secret key.
3. In the ***Embed Value [%1]*** field, type "AuthOauth2".
4. In the ***Embed Value [%2]*** field, type your Aruba Central customer ID.
5. In the ***Embed Value [%3]*** field, type your Aruba Central client ID.
6. In the ***Embed Value [%4]*** field, set a page size between 1 and 1000.
7. Remove all HTTP Headers.
8. Remove any ***CURL Option*** and set the ***SSLVERIFYPEER Curl Option*** to 0 as the value and click ***Save***.

To authenticate using the Offline Token Mechanism:

1. Go to the**Credential Management** page (System > Manage > Credentials). Identify your current credential and click on the credential's name to edit.
2. In the ***Embed Password [%P]*** field, type your Aruba Central client secret key.
3. In the ***Embed Value [%1]*** field, type "OfflineToken".
4. In the ***Embed Value [%2]*** field, type the refresh token.
5. In the ***Embed Value [%3]*** field, type your Aruba Central client ID.
6. In the ***Embed Value [%4]*** field, set a page size between 1 and 1000.
7. Remove all HTTP Headers.
8. Remove any ***CURL Option*** and set the ***SSLVERIFYPEER Curl Option*** to 0 as the value and click ***Save***.

NOTE: The following Dynamic Applications will be disabled by default, and all collection for them will stop. You should manually enable these Dynamic Applications to restart collection, being conscious of the number of APs in the field: "Aruba: Central AP Cache", "Aruba: Central AP Configuration", "Aruba: Central AP Discovery" and "Aruba: Central AP Performance". If the number of devices is higher than 8000, you must configure your scale settings appropriately. You can follow the steps outlined in the **SL1 Scale Settings** section.

Chapter 2

Configuration and Discovery

Overview

The following sections describe how to configure and discover Aruba Central virtual controllers for monitoring by SL1 using the *Aruba Central* PowerPack.

This chapter covers the following topics:

Prerequisites for Monitoring Aruba Central

Before you can monitor Aruba Central virtual controllers and their component devices using the *Aruba Central* PowerPack, you must first have the following information:

To authenticate using the Oauth Grant Mechanism:

- Aruba Central username and password
- Aruba Central customer ID
- Aruba Central client ID
- Aruba Central client secret key

To authenticate using the Offline Token Mechanism:

- Aruba Central client ID
- Aruba Central client secret key
- Aruba Central refresh token

You can request these items by registering with Aruba Technical Support.

Configuring Aruba Central Credentials

To use the Dynamic Applications in the Aruba Central PowerPack, you must configure a SOAP/XML credential for the Aruba Central web service.

SL1 includes an Aruba Central credential type that you can use to connect with the Aruba Central web service during guided discovery. This credential type uses field names and terminology that are specific to Aruba Central.

The PowerPack includes two example SOAP/XML credential examples (**Aruba Central Example**) and **Aruba Central SSO Example**) that you can edit for your own use.

NOTE: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the ***Duplicate*** option for sample credential(s). ScienceLogic recommends that you use ***the classic user interface and the Save As button*** to create new credentials from sample credentials. This will prevent you from overwriting the sample credential(s).

Configuring Aruba Central Credential using Oauth Grant Mechanism

To configure a SOAP/XML credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the **Aruba Central Example** sample credential, then click its **Actions** icon (⋯) and select ***Duplicate***. A copy of the credential, called **Aruba Central Example copy** appears.
3. Supply values in the following fields:

- ***Name***. Type a new name for your Aruba Central credential.
- ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***Select the organizations the credential belongs to**** drop-down field to align the credential with those specific organizations.
- ***Timeout (ms)***. Type a timeout value of at least 2000.
- ***Content Encoding***. Keep the default value.
- ***Method***. Keep the default value.
- ***HTTP Version***. Keep the default value.
- ***URL***. Type your Aruba Central URL.
- ***HTTP Auth User***. Type your Aruba Central username email address.
- ***HTTP Auth Password***. Type your Aruba Central password.
- ***Embedded Password [%P]***. Type your Aruba Central client secret key.
- ***Embed Value [%1]***. Type "AuthOauth2".
- ***Embed Value [%2]***. Type your Aruba Central customer ID.
- ***Embed Value [%3]***. Type your Aruba Central client ID.
- ***Embed Value [%4]***. Type the page size for pagination between 1 and 1000. ScienceLogic recommends setting the ***Embed Value [%4***] field to a value close to 1,000 for large Aruba Central systems and only lowering this value if you see SIGTERMs. You cannot set the page size to 0 in this field. Aruba Central deployments of more than 5,000 devices need a dedicated collector.
- ***CURL Options***. Ensure that SSLVERIFYPEER is selected and set to 0. There should be no other CURL Options configured.

Proxy Settings

NOTE: You must complete the ***Proxy Settings*** fields only if you connect to Aruba Central through a third-party proxy server. If you do not use a proxy to connect to Aruba Central, then you can leave these fields blank.

- ***Proxy Hostname/IP***. Type the server's hostname or IP address.
- ***Proxy Port***.Type the port on the proxy server to which you will connect.
- ***Proxy User***. Type the username used to access the proxy server.
- ***Proxy Password***. Type the password used to access the proxy server.

HTTP Headers

- ***Add a header***. Click **[Add a header]** to connect a proxy server using http or https.
    - ***proxy_url_protocol:http***.Enter this schema if the proxy server does not have https configured.
    - ***proxy_url_protocol:https***. Enter this schema if the proxy server has https configured.

4. Click **[Save & Close]**.

NOTE: The SOAP/XML credential tester is not supported by the Aruba Central PowerPack.

Configuring Aruba Central Credentials using Oauth Grant Mechanism for SL1 in the Classic User Interface

To configure SL1 to monitor Aruba Central devices, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Aruba Central* PowerPack to use your Aruba Central user account to retrieve information from the Aruba Central virtual controller and component devices.

The PowerPack includes an example SOAP/XML credential (**Aruba Central Example**) that you can edit for your own use.

To configure a SOAP/XML credential to access Aruba Central:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Aruba Central Example** credential, and then click its wrench icon (). The **Edit SOAP/XML Credential** modal appears.
3. Complete the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the Aruba Central credential.
- ***URL***. Type your Aruba Central URL.
- ***HTTP Auth User***. Type your Aruba Central username email address.
- ***HTTP Auth Password***. Type your Aruba Central password.
- ***Timeout***. Type a value of at least 2.

SOAP Options

- *Embedded Password [%P]*. Type your Aruba Central client secret key.
- *Embed Value [%1]*. Type "AuthOauth2".
- *Embed Value [%2]*. Type your Aruba Central customer ID.
- *Embed Value [%3]*. Type your Aruba Central client ID.
- *Embed Value [%4]*. Type the page size for pagination between 1 and 1000.

> **NOTE:** ScienceLogic recommends setting the ***Embed Value [%4***] field to a value close to 1,000 for large Aruba Central systems and only lowering this value if you see SIGTERMs. You cannot set the page size to 0 in the Embed Value [%4] field. Aruba Central deployments of more than 5,000 devices need a dedicated collector.

- *CURL Options*. Ensure that SSLVERIFYPEER is selected and set to 0. There should be no other CURL Options configured.

Proxy Settings

> **NOTE:** You must complete the ***Proxy Settings*** fields only if you connect to Aruba Central through a third-party proxy server. If you do not use a proxy to connect to Aruba Central, then you can leave these fields blank.

- *Hostname/IP*. Type the server's hostname or IP address.
- *Port*.Type the port on the proxy server to which you will connect.
- *User*. Type the username used to access the proxy server.
- *Password*. Type the password used to access the proxy server.

HTTP Headers

- *Add a header*. Click **[Add a header]** to connect a proxy server using http or https.
  - *proxy_url_protocol:http*.Enter this schema if the proxy server does not have https configured.
  - *proxy_url_protocol:https*. Enter this schema if the proxy server has https configured.

4. For the remaining fields, use the default values.
5. Click the **[Save As]** button.

Configuring Aruba Central Credentials Using Offline Token Mechanism

To configure SL1 to monitor Aruba Central devices, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Aruba Central* PowerPack to use your Aruba Central user account to

retrieve information from the Aruba Central virtual controller and component devices.

Aruba Central Power Pack supports SSO (Single Sign-On) using the Offline Token mechanism. This method generates a ***Refresh Token*** that's required when creating a SOAP/XML credential. The token file contains both an access token and a refresh token. Access tokens can be renewed with refresh tokens once expired.

To generate a token:

1. Navigate to the Aruba Central API Gateway User Interface.
2. Go to the **Rest API** page (***Organization*** > ***Platform Integration*** > ***Rest API***).
3. Click the ***System Apps & Tokens*** tab, and then click ***View Tokens***.
4. Click the ***Download Token*** button to open the token file, and locate the series of characters next to the field ***refresh_token***.

For more information about generating a refresh token, see the Aruba Central documentation at https://www.arubanetworks.com/techdocs/central/latest/nms /api/offline-token.htm.

To configure a SOAP/XML credential to access Aruba Central:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the **Aruba Central SSO Example** credential, then click its **Actions** icon (⋯) and select ***Duplicate***. A copy of the credential, called **Aruba Central SSO Example copy** appears.
3. Complete the following fields:

    - ***Name***. Type a new name for the Aruba Central credential.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***Select the organizations the credential belongs to**** drop-down field to align the credential with those specific organizations.
    - ***Timeout (ms)***. Type a timeout value of at least 2000.
    - ***Content Encoding***. Keep the default value.
    - ***Method***. Keep the default value.
    - ***HTTP Version***. Keep the default value.
    - ***URL***. Type your Aruba Central URL.
    - ***Embedded Password [%P]***. Type your Aruba Central client secret key.
    - ***Embed Value [%1]***. Type "OfflineToken" in the field.
    - ***Embed Value [%2]***. Type your Refresh Token.
    - ***Embed Value [%3]***. Type your Aruba Central client ID.
    - ***Embed Value [%4]***. Type the page size for pagination between 1 and 1000. ScienceLogic recommends setting the ***Embed Value [%4***] field to a value close to 1,000 for large Aruba Central systems and only lowering this value if you see SIGTERMs. You cannot set the page size to 0 in the Embed Value [%4] field. Aruba Central deployments of more than 5,000 devices need a dedicated collector.
    - ***CURL Options***. Ensure that SSLVERIFYPEER is selected and set to 0. There should be no other CURL Options configured.

    Proxy Settings

NOTE: You must complete the ***Proxy Settings*** fields only if you connect to Aruba Central through a third-party proxy server. If you do not use a proxy to connect to Aruba Central, then you can leave these fields blank.

- ***Proxy Hostname/IP***. Type the server's hostname or IP address.
- ***Proxy Port***.Type the port on the proxy server to which you will connect.
- ***Proxy User***. Type the username used to access the proxy server.
- ***Proxy Password***. Type the password used to access the proxy server.

HTTP Headers

- ***Add a header***. Click **[Add a header]** to connect a proxy server using http or https.
  - ***proxy_url_protocol:http***.Enter this schema if the proxy server does not have https configured.
  - ***proxy_url_protocol:https***. Enter this schema if the proxy server has https configured.

4. For the remaining fields, use the default values.
5. Click the **[Save & Close]** button.

Configuring Aruba Central Credentials Using Offline Token Mechanism in the Classic User Interface

To configure a SOAP/XML credential to access Aruba Central:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Aruba Central SSO Example** credential and click its wrench icon (). The **Edit SOAP/XML Credential** modal appears:
3. Complete the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the Aruba Central credential.
- ***URL***. Type your Aruba Central URL.
- ***Timeout***. Type a value of at least 2.

SOAP Options

- *Embedded Password [%P]*. Type your Aruba Central client secret key.
  - *Embed Value [%1]*. Type "OfflineToken" in the field.
  - *Embed Value [%2]*. Type your Refresh Token.
  - *Embed Value [%3]*. Type your Aruba Central client ID.
  - *Embed Value [%4]*. Type the page size for pagination between 1 and 1000.

NOTE: ScienceLogic recommends setting the ***Embed Value [%4]*** field to a value close to 1,000 for large Aruba Central systems and only lowering this value if you see SIGTERMs. You cannot set the page size to 0 in the Embed Value [%4] field. Aruba Central deployments of more than 5,000 devices need a dedicated collector.

Proxy Settings

NOTE: You must complete the ***Proxy Settings*** fields only if you connect to Aruba Central through a third-party proxy server. If you do not use a proxy to connect to Aruba Central, then you can leave these fields blank.

- ***Hostname/IP***. Type the server's hostname or IP address.
- ***Port***.Type the port on the proxy server to which you will connect.
- ***User***. Type the username used to access the proxy server.
- ***Password***. Type the password used to access the proxy server.

HTTP Headers

- ***Add a header***. Click **[Add a header]** to connect a proxy server using http or https.
  - ***proxy_url_protocol:http***.Enter this schema if the proxy server does not have https configured.
  - ***proxy_url_protocol:https***. Enter this schema if the proxy server has https configured.
- ***CURL Options***. Ensure that SSLVERIFYPEER is selected and set to 0. There should be no other CURL Options configured.

4. For the remaining fields, use the default values.
5. Click the **[Save As]** button.

Discovering Aruba Central Devices

To discover and monitor your Aruba Central virtual controller, you must do the following:

- Create a virtual device representing the virtual controller
- Configure the Aruba Central device template that is included in the *Aruba Central* PowerPack
- Align the device template to the Aruba Central virtual device

Each of these steps is documented in the following sections.

Creating an Aruba Central Virtual Device

Because the Aruba Central virtual controller does not have a static IP address, you cannot discover an Aruba Central device by running a discovery session. Instead, you must create a ***virtual device*** that represents

the Aruba Central virtual controller. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Aruba Central virtual controller:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Complete the following fields:
    - ***Device Name***. Type a name for the device.
    - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
    - ***Device Class***. Select *HPE Aruba | Central Controller*.
    - ***Collector***. Select the collector group that will monitor the device.
4. Click **[Add]** to create the virtual device.

Configuring the Aruba Central Device Template

A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *Aruba Central* PowerPack includes the "Aruba Central Template," which enables SL1 to align all of the necessary Dynamic Applications to the virtual controller root component device.

Before you can use the "Aruba Central Template", you must configure the template so that each Dynamic Application in the template aligns with the ***credential you created earlier***.

To configure the Aruba Central device template:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the SL1 classic user interface).
2. Locate the "Aruba Central Template" and click its wrench icon (). The **Device Template Editor** modal page appears.
3. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears:
4. Click on ***Credentials***, and then select the credential that you created for Aruba Central from the drop-down list.
5. Click the next Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page and then select the credential you created in the ***Credentials*** field.
6. Repeat step 5 until you have selected your Aruba Central credential in the ***Credentials*** field for all of the Dynamic Applications listed in the **Subtemplate Selection** section.
7. Click **[Save]**.

NOTE: To maintain a "clean" version of the template, type a new name in the ***Template Name*** field and then click **[Save As]** instead of **[Save]**.

Aligning the Device Template to Your Aruba Central Virtual Device

After you have configured the Aruba Central device template so that each Dynamic Application in the template aligns with your Aruba Central credential, you can use that template to align the Dynamic Applications to the virtual device that you created to act as the root device for your Aruba Central virtual controller. When you do so, SL1 discovers and models all of the components in your Aruba Central virtual controller.

To align the Aruba Central device template to the Aruba Central virtual device:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the classic user interface).
2. On the **Device Manager** page, select the checkbox for the Aruba Central virtual device.
3. In the ***Select Action*** field, in the lower right corner of the page, select the option *MODIFY by Template* and then click the **[Go]** button. The **Device Template Editor** page appears.
4. In the ***Template*** drop-down list, select your Aruba Central device template.
5. Click the **[Apply]** button, and then click **[Confirm]** to align the Dynamic Applications to the root component device.

NOTE: After discovering your Aruba devices, ensure that Configuration and Performance Dynamic Applications for a device type run at the same interval or less often than the respective discovery Dynamic Application for that device. For example, if the "Aruba: Central AP Discovery" Dynamic Application runs every 15 minutes, then the "Aruba: Central AP Performance" Dynamic Application must run at 15 minutes or less.

Creating Log Policies for Dynamic Applications

Optionally, you can create dedicated log policies that enable deeper analysis of the Dynamic Applications in the *Aruba Central* PowerPack.

To do so:

1. Either go to the console of the Data Collector or use SSH to access the Data Collector.
2. At the shell prompt, enter the following command:

```
sudo -u s-em7-core
/opt/em7/envs/186BDE253319BF2A2AD30E0C5C4932B9/bin/python -m silo.low_
code.cli log-policy create --name=<name> --app_id=<app_id> --
did=<device_id> --duration="<duration>"
```

You can insert the following durations:

- ***#w***. Week.
- ***#d*** **.** Day.
- ***#h*** . Hour.
- ***#m***. Minute.
- ***#s***. Second.

TIP: For more information, you can enter one of the following commands to access the help files:

```
sudo -u s-em7-core
/opt/em7/envs/186BDE253319BF2A2AD30E0C5C4932B9/bin/python -m
silo.low_code.cli log-policy --help
```

```
sudo -u s-em7-core
/opt/em7/envs/186BDE253319BF2A2AD30E0C5C4932B9/bin/python -m
silo.low_code.cli log-policy create --help
```

3. The system will create the log file in the directory **/var/log/em7**, using the name you define.

Viewing Aruba Central Component Devices

In addition to the **Devices** page, you can view your Aruba Central devices in the following places in the user interface:

- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device.
- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1. The **Device Components** page displays all root devices and component devices in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with an Aruba Central device, find the device and click its plus icon (**+**).
- The **Component Map** page (Maps>Classic Maps>Device Maps>Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for an Aruba Central device, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.

SL1 Scale Settings

If Aruba Central has more than 8,000 devices to collect information from, follow the steps outlined below to configure and apply the appropriate settings:

Recommended settings in SL1:

1. Go to the **Process Editor** page (System > Settings > Processes).
2. Search for "Data Collection: Dynamic App" and click its wrench icon (🔧).
3. Set the ***Batch Factor (Jobs)*** field to ***[2]***, and then click ***[Save]***.
4. You will also need the set the ***Maximum Devices*** to 400 on the "Aruba: Central AP Configuration" and "Aruba: Central AP Performance" Dynamic Applications.

Recommended settings in the Collector Unit (CU):

1. Set the memory limit of the Data Collection: Dynamic App process to 4294967296 (4GB) by connecting the Collector Unit and adding the following lines to the file ***/etc/silo.conf***:

```
...
[PROC_VIRTUAL_MEM_LIMIT]
11 = 4294967296
```

NOTE: The 11 represents the id of the Data Collection: Dynamic App process. This setting will be applied during execution, so you do not need to restart the collector.

NOTE: The memory limit set is in bytes and can be increased. You may need to increase this limit if there is "MemoryError: Out Of Memory" exception or if there are SIGTERMS for a period of time.

Recommended Specs And Settings

Collection Unit (CU):

Number of devices	Specs	Settings
• **Up to ~8000 Access Points** • **Up to ~100 Gateways** • **Up to ~500 Switches**	CPU: 16 cores Memory: 24 GB Disk: 150 GB	*Memory Limit 11: 4294967296
• ***Up to ~15000 Access Points*** • ***Up to ~500* Gateways** • ***Up to ~500* Switches**	CPU: 16 cores Memory: 32 GB Disk: 150 GB	*Memory Limit 11: 6442450944
• ***Up to ~20000 Access Points*** • ***Up to ~500* Gateways** • ***Up to ~500* Switches**	CPU: 16 Cores Memory: 32 GB Disk: 150 GB	*Memory Limit 11: 8589934592

For more details on how to configure these settings, refer to the **Recommended Settings in the Collector Unit** section above.

Central Database (CDB) Specs:

- CPU: 16 cores
- Memory: 74 GB
- Disk: 600 GB

ScienceLogic recommends checking disk space along with other specs in the CDB and increase them as needed based on the VM DataBase Specifications (above 1000 devices) table:

		Minimum at 1000 Devices			Addition Resource per 1000 to 6000 Devices			Addition Resource beyond 6000 Devices		
Type	Description	CPU Cores	Memory RAM (GB)	Hard Disk (GB)	CPU Cores	Memory RAM (GB)	Hard Disk (GB)	CPU Cores	Memory RAM (GB)	Hard Disk (GB)
DB	Database Server	4	24	300	2	16	150	1	16	100

NOTE: For more information, see the documentation at https://support.sciencelogic.com/s/system-requirements?tabset-e65a2=60f0a.

Chapter 3

Aruba Central Dashboards

Overview

The following sections describe the device dashboards that are included in the *Aruba Central* PowerPack.

This chapter covers the following topics:

Device Dashboards

The *Aruba Central* PowerPack includes device dashboards that provide summary information for Aruba Central component devices. Each of the device dashboards in the *Aruba Central* PowerPack is set as the default device dashboard for the equivalent device class.

NOTE: Some widgets will not display data for the "Aruba: Central Controller," "Aruba: Wireless Access Points," "Aruba: Gateway Summary," "Aruba: Gateway," and "Aruba: Switches" SL1 dashboards because the "REST: Performance Metrics Monitor (Aruba Central)" Dynamic Application is disabled by default for this version.

Aruba: AP

The **Aruba: AP** dashboard displays the following information:

- The basic information about the device
- The device's CPU and memory utilization vitals
- A list of active events and open tickets associated with the device
- The total number of AP clients
- Three instances of the Multi-series Performance Widget that display the following metrics trended over the specified period of time:
    - Radio channel transmit power
    - Radio channel utilization
    - Radio transmit power

Aruba: Central Controller

The **Aruba: Central Controller** dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Four instances of the Gauge Widget that display the following metrics trended over the specified period of time:
    - Total SL1 components
    - Total access points

    - Total switches
    - Total gateways

- The top devices by CPU utilization over the specified period of time
- The total requests sent from SL1 to Aruba Central over the specified period of time
- The errors received back from Aruba Central over the specified period of time

Aruba: Gateway

The **Aruba: Gateway** dashboard displays the following information:

- The basic information about the device
- The device's CPU and memory utilization vitals
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Three instances of the Multi-series Performance Widget that display the following metrics trended over the specified period of time:
    - Bandwidth usage
    - Bandwidth limit
    - AP count

Aruba: Switch

The **Aruba: Switch** dashboard displays the following information:

- The basic information about the device
- The device's CPU and memory utilization vitals
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Four instances of the Multi-series Performance Widget that display the following metrics trended over the specified period of time:
    - Switch temperature
    - Power consumption
    - Power over Ethernet consumption
    - Client count

Appendix

3

Aruba Central Dynamic Application Details

Overview

This appendix describes the relationship of the Dynamic Applications in the Aruba CentralPowerPack.

Aruba Central Dynamic Application Relationships

The table below lists the Dynamic Applicationsin this PowerPack, whether they are enabled by default, and the data they collect.

Dynamic Applications	Enabled by Default?	Data Collection
Aruba: Central AP Cache	No	`"/monitoring/v2/aps?show_resource_details=true&calculate_client_count=true&calculate_total=true&offset=<OFFSET>&limit=<LIMIT>"`
Aruba: Central AP Discovery	No	Aruba: Central AP Cache
Aruba: Central AP Performance	No	Aruba: Central AP Cache
Aruba: Central AP Configuration	No	Aruba: Central AP Cache
Aruba: Central Component Counts	Yes	Aruba: Central AP Cache, Aruba: Central SD-WAN Gateway Cache, Aruba: Central Switch Cache
Aruba: Central Notifications	Yes	`"/central/v1/notifications"`
Aruba: Central SD-WAN Gateway Cache	Yes	`"/monitoring/v1/gateways?calculate_total=true&offset=<OFFSET>&limit=<LIMIT>"`

Dynamic Applications	Enabled by Default?	Data Collection
Aruba: Central SD-WAN Gateway Configuration	Yes	Aruba: Central SD-WAN Gateway Cache
Aruba: Central SD-WAN Gateway Discovery	Yes	Aruba: Central SD-WAN Gateway Cache
Aruba: Central SD-WAN Gateway Performance	Yes	Aruba: Central SD-WAN Gateway Cache
Aruba: Central Site Discovery	Yes	`"/central/v2/sites?limit=100"`
Aruba: Central Switch Cache	Yes	`"/monitoring/v1/switches?show_resource_details=true&calculate_client_count=true&calculate_total=true&offset=<OFFSET>&limit=<LIMIT>"`
Aruba: Central Switch Configuration	Yes	Aruba: Central Switch Cache
Aruba: Central Switch Discovery	Yes	Aruba: Central Switch Cache
Aruba: Central Switch Performance	Yes	Aruba: Central Switch Cache
REST: Performance Metrics Monitor (Aruba Central)	No	N/A

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010