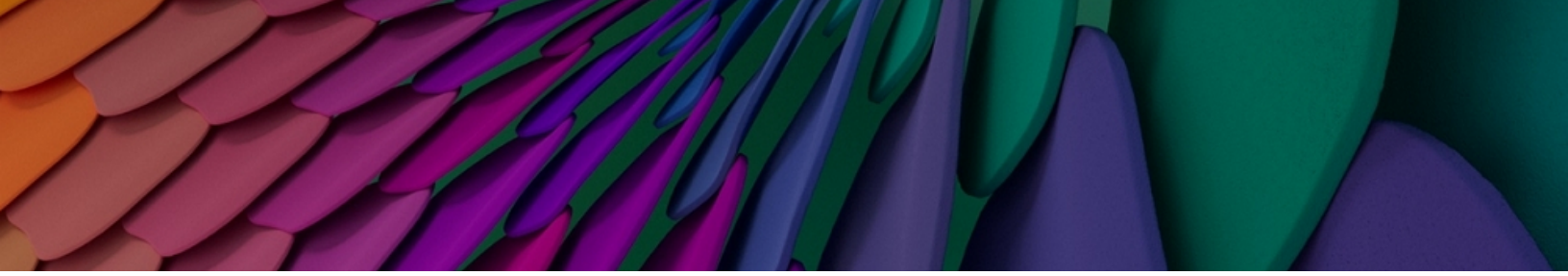


AOS-CX 10.14 Introduction to the Web UI Guide

4100i, 6000, 6100, 6200, 6300, 6400 Switch Series*

(excluding S3L75A, S3L76A, S3L77A)

aruba

a Hewlett Packard Enterprise company

May 2024
Edition: 1

Chapter 1
About this document

This document describes features of the AOS-CX network operating system. It is intended for administrators responsible for installing, configuring, and managing Aruba switches on a network.

Applicable products

This document applies to the following products:

- HPE Aruba Networking 4100i Switch Series (JL817A, JL818A)
- HPE Aruba Networking 6000 Switch Series (R8N85A, R8N86A, R8N87A, R8N88A, R8N89A, R9Y03A)
- HPE Aruba Networking 6100 Switch Series (JL675A, JL676A, JL677A, JL678A, JL679A)
- HPE Aruba Networking 6200 Switch Series (JL724A, JL725A, JL726A, JL727A, JL728A, R8Q67A, R8Q68A, R8Q69A, R8Q70A, R8Q71A, R8V08A, R8V09A, R8V10A, R8V11A, R8V12A, R8Q72A, JL724B, JL725B, JL726B, JL727B, JL728B, S0M81A, S0M82A, S0M83A, S0M84A, S0M85A, S0M86A, S0M87A, S0M88A, S0M89A, S0M90A, S0G13A, S0G14A, S0G15A, S0G16A, S0G17A)
- HPE Aruba Networking 6300 Switch Series (JL658A, JL659A, JL660A, JL661A, JL662A, JL663A, JL664A, JL665A, JL666A, JL667A, JL668A, JL762A, R8S89A, R8S90A, R8S91A, R8S92A, S0E91A, S0X44A)
- HPE Aruba Networking 6400 Switch Series (R0X31A, R0X38B, R0X38C, R0X39B, R0X39C, R0X40B, R0X40C, R0X41A, R0X41C, R0X42A, R0X42C, R0X43A, R0X43C, R0X44A, R0X44C, R0X45A, R0X45C, R0X26A, R0X27A, JL741A, S0E48A,S0E48A #0D1, S1T83A, S1T83A #0D1)

Latest version available online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in Support and Other Resources.

Command syntax notation conventions

Convention	Usage
`example-text`	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets (**[ ]**).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ■ *<example-text>* ■ <example-text> ■ *example-text* ■ *example-text*	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: ■ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (**< >**). Substitute the text—including the enclosing angle brackets—with an actual value.

Convention	Usage
	■ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.
`|`	Vertical bar. A logical **OR** that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.
`{ }`	Braces. Indicates that at least one of the enclosed items is required.
`[ ]`	Brackets. Indicates that the enclosed item or items are optional.
... or . . .	Ellipsis: ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

Examples in this document are representative and might not match your particular switch or environment.

The slot and port numbers in this document are for illustration only and might be unavailable on your switch.

Understanding the CLI prompts

When illustrating the prompts in the command line interface (CLI), this document uses the generic term **switch**, instead of the host name of the switch. For example:

```
switch>
```

The CLI prompt indicates the current command context. For example:

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

switch(*CONTEXT-NAME*)#

Indicates the configuration context for a feature. For example:

```
switch(config-if)#
```

Identifies the **interface** context.

Variable information in CLI prompts

In certain configuration contexts, the prompt may include variable information. For example, when in the VLAN configuration context, a VLAN number appears in the prompt:

```
switch(config-vlan-100)#
```

When referring to this context, this document uses the syntax:

```
switch(config-vlan-<VLAN-ID>)#
```

Where <*VLAN-ID*> is a variable representing the VLAN number.

Identifying switch ports and interfaces

Physical ports on the switch and their corresponding logical software interfaces are identified using the format:
member/slot/port

On the 4100i Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on the switch.

On the 6000 and 6100 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on the switch.

On the 6200 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 8. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 in slot 1 on member 1.

On the 6300 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 10. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on member 1.

On the 6400 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Specifies physical location of a module in the switch chassis.
  - Management modules are on the front of the switch in slots 1/1 and 1/2.
  - Line modules are on the front of the switch starting in slot 1/3.
- *port*: Physical number of a port on a line module.

For example, the logical interface **1/3/4** in software is associated with physical port 4 in slot 3 on member 1.

Identifying modular switch components

- Power supplies are on the front of the switch behind the bezel above the management modules. Power supplies are labeled in software in the format: *member/power supply*:
  - *member*: 1.
  - *power supply*: 1 to 4.
- Fans are on the rear of the switch and are labeled in software as: *member/tray/fan*:
  - *member*: 1.
  - *tray*: 1 to 4.
  - *fan*: 1 to 4.
- Fabric modules are not labeled on the switch but are labeled in software in the format: *member/module*:
  - *member*: 1.
  - *member*: 1 or 2.
- The display module on the rear of the switch is not labeled with a member or slot number.

Chapter 2
Accessing the AOS-CX Web UI

By default, the 6200, 6300, and 6400 switches have the HTTPS server enabled on the `mgmt` and `default` VRF. The 4100i, 6000, and 6100 switches have the HTTPS server enabled on the `default` VRF. On all switches, the REST API access mode is set to `read-write`. You must configure a static IP or use the IP address on the management port (6200, 6300, 6400 switches only; the 4100i, 6000, and 6100 switches do not have a management port) to access the Web UI.

When Aruba Central manages AOS-CX switches, it functions as the single source of truth and the Web UI operates in read-only mode.

The Web UI can be opened and accessed using both IPv4 and IPv6.

Prerequisites

The 6200 switches support two VRFs. One `mgmt` VRF and one default VRF.

The 4100i switch only include the `default` VRF; there is no `mgmt` VRF.

- Certificate-based authentication is not supported on 6000 and 6100 Switch Series.
- The 6000 and 6100 switches only include the `default` VRF; there is no `mgmt` VRF.

To use the Web UI to make configuration changes—such as adding users—the following must be true:

- The system that you are using to access the Web UI must be on the same network and the subnet as the switch.
- Proxy must be disabled on browsers through which you are accessing the Web UI.
- You must have a valid login user name and password or a valid certificate.
- The user name you use to log in must have administrator rights.

For information about configuring the management interface and REST API access, see the *AOS-CX Fundamentals Guide*.

For information about configuring and managing the certificates, see the AOS-CX*Security Guide*.

Procedure

1. Start a supported web browser and enter the IP address of the management port in the address bar. Use HTTPS.

   For example:
   ```
   https://192.0.2.5 or https://[1001::2]
   ```

You must use a supported browser, such as Chrome, Firefox, Edge, or Safari. For details on supported browser versions, see the *Release Notes* for the version of AOS-CX you are using.

2. Optionally a pre- and post-login message may be displayed. The message can be customized or disabled with the `banner` command.
3. For the password-based authentication, at the login page, enter your user name and password credentials, then click **Login**. For the certificate-based authentication, at the login page, click **LOGIN WITH CERTIFICATE**, select your certificate and click **Accept**.
4. After you log in, the main Web UI page is displayed.

Ensure that both the switch and the client where the Web UI is running are set to use NTP or to a time zone based on UTC time. If the switch and the client time are not in sync, then a message is displayed after you log in, indicating the time difference.

Troubleshooting Web UI access issues

View issue symptoms and causes, as well as actions to resolve common Web UI access issues.

HTTP 404 error when accessing the switch URL

Symptom

The switch is operational and you are using the correct URL for the switch, but attempts to access the REST API or Web UI result in an HTTP 404 "Page not found" error.

Cause

REST API access is not enabled on the VRF that corresponds to the access port you are using. For example, you are attempting to access the REST API or Web UI from the management (OOBM) port, and access is not enabled on the `mgmt` VRF. By default, `https-server` is enabled on the `mgmt` VRF for the 6300 and 6400 switches. The 4100i, 6000, and 6100 switches do not have a `mgmt` VRF, so `https-server` is enabled on the `default` VRF.

Action

Use the `https-server vrf` command to enable REST API access on the specified VRF.

For example:

```
switch(config)# https-server vrf mgmt
```

Or, on the 4100i, 6000, or 6100 switch:

```
switch(config)# https-server vrf default
```

HTTP 401 error "Login failed: session limit reached"

Symptom

A REST request or Web UI login attempt returns response code 401 and the response body contains the following text string:

```
Login failed: session limit reached
```

Cause

A user attempted to log into the REST API or the Web UI, but that user already has the maximum number of concurrent sessions running.

Action

1. Log out from one of the existing sessions.

   Browsers share a single session cookie across multiple tabs or even windows. However, scripts that POST to the login resource and later do not POST to the logout resource can easily create the maximum number of concurrent sessions.
2. If the session cookie is lost and it is not possible to log out of the session, then wait for the session idle time limit to expire.

   When the session idle timeout expires, the session is terminated automatically.
3. If it is required to stop all HTTPS sessions on the switch instead of waiting for the session idle time limit to expire, you can stop all HTTPS sessions using the `https-server session close all` command.

   This command stops and starts the `hpe-restd` service, so using this command affects all existing REST sessions, Web UI sessions, and real-time notification subscriptions.

"Not Authorized" is displayed instead of page content

Symptom

The message "Not Authorized" is displayed in the details pane of a Web UI page.

Cause

You have logged in as a user that is not authorized to view this page.

Action

Use the navigation pane to select a page you are authorized to access.

The AOS-CX Web UI provides quick and easy visibility into what is happening on your switch. With the Web UI, you get faster problem detection, diagnosis, and resolution.

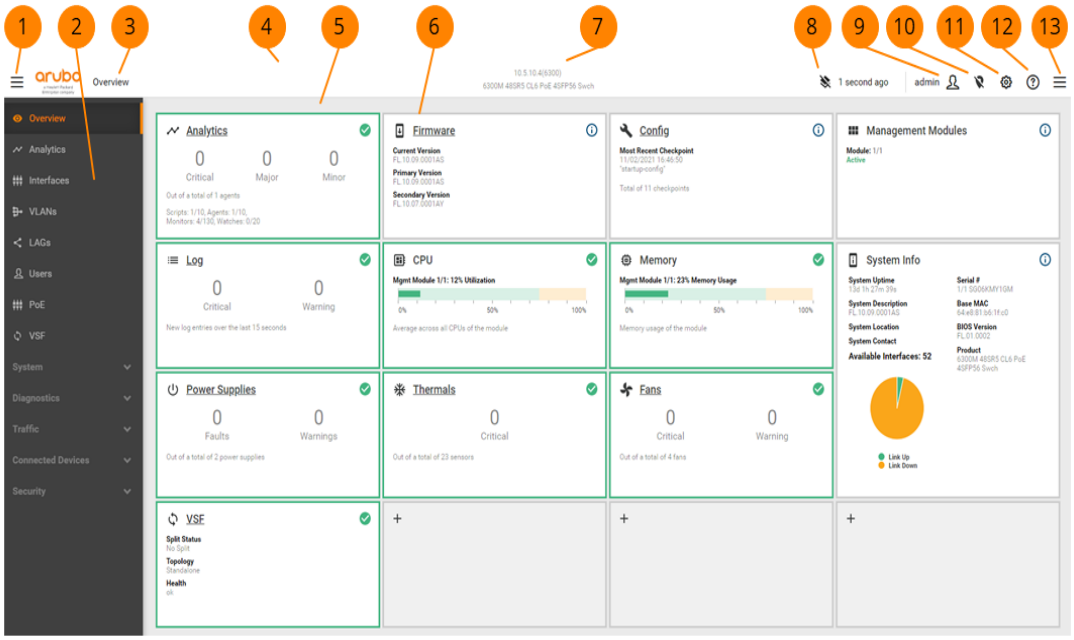
You can use the Web UI to do the following:

- Monitor the status of a switch from a single pane that shows easy-to-read indicators for power, temperature, fans, CPU use, memory use, log entries, system information, firmware, and various aspects of the network configuration.
- Identify issues when indicators turn red, and quickly locate and diagnose the problem.
- View and configure Network Analytics Engine agents, scripts, and alerts. Not applicable to the 4100i, 6000, or 6100 switches, which do not support the Network Analytics Engine.
- Modify some aspects of the switch configuration.
- Run diagnostics including the `ping`, `traceroute`, and `show tech` commands.
- Upgrade or downgrade the image build on the device.
- Reboot the switch.

AOS-CX Web UI framework

Descriptions for (numbered) common areas, buttons, menus, and controls in the Web UI are listed after the image.

Figure 1 *Overview page with callouts*



1. The  Show/Hide button on the left in the top banner, allows you to hide the navigation pane (slides the pane in and out).
2. The navigation pane. Expand or collapse the System or Diagnostics group to show or hide related items. For a description of each menu item in the navigation pane, see the description of the Navigation pane.
3. Breadcrumbs in the top banner show the path to your navigation selection.
4. The top banner provides information and other menu items.
5. The details pane shows information based on your selection.
6. Panels in the details pane display status, alerts, and other information and allow you to drill down to more information.
7. The IP address of the management (mgmt) interface through which the switch Web UI is opened and the name of the switch are displayed at the center of the top banner. If a switch does not have a mgmt interface or if the mgmt interface is not configured, then an IP address is not displayed.
8. The  Layout Management icon in the top banner allows you to unlock the details pane page layout. You can then resize and move panels, or reset the details pane page layout to the default layout. Changes are persistent in the local browser. The icon changes to  , when the layout is unlocked.
9. The  User Management menu in the top banner includes a logout selection.
10. The  Toggle Locator LED menu in the top banner allows you to turn the switch locator LED on or off. In the case of a stack, this menu lists all the member switches in the stack. You can turn the locator LED on or off for each member in the stack. The icon changes to  , when the switch locator LED is turned off for all switches.
11. The  System menu in the top banner includes the following:
    - **Save Config**: Save configuration changes
    - **Reboot**: Reboot the switch to either primary or secondary image.
    - **v10.04 API**: Access v10.04 REST APIs that you can use to read and/or write to the switch.
12. The  Help icon provides a link to AOS-CX user documentation.
13. The  Show/Hide button on the right side of the top banner displays the Log Summary pane (slides the pane in and out). The Log Summary provides a summary of the most recent critical level log entries in the last X seconds. It also shows counts of the number of critical, warning, and info log entries arriving in the last X seconds.

Customizing the Web UI

- You can customize the Web UI to change the page layout, include additional information, or filter to display selected information.
- The changes that you make to customize the Web UI are restricted to the browser session. For example, if you add a custom panel for an interface, the panel will be available only in the current browser session. That is, if you open a Web UI session in a different browser or device, the newly added panel will not be available.

Customizing page layouts

Some of the pages in the Web UI provide a user customizable layout. Each customization is persistent in the local browser. The customization is stored based on the switch URL (based on the management address of the switch). For example, if you change the management address, you will lose any page layout configuration that was tied to that URL.

Each page can be reset back to the default layout.

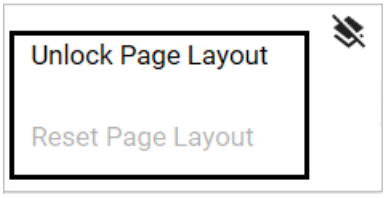
Prerequisites

You must be logged in to the Web UI. You must allow cookies to be stored.

Procedure

1. In the top banner, click the Layout Management icon, and select **Unlock Page Layout** to unlock the layout. The panel borders change to a dotted line, indicating that you can resize and move the panels in the details pane.

   Figure 1 *Unlock Page Layout menu*

   Some of the possible changes you can make to a panel are described in the following steps.
2. To resize a panel, drag the handle at the bottom-right corner of the panel, and change the width and height.
3. To reposition a panel, move the panel to a new position. The other panels will automatically rearrange to accommodate the position of the moved panel.
4. To lock the changes to the page layout, click the Layout Management icon, and select **Lock Page Layout**.
5. To reset the page layout to the default view, click the Layout Management icon, and select **Reset Page Layout**. The option to reset the page is available only when the page layout is unlocked.

Adding a custom panel to the Overview page

You can add a custom panel to the Overview page to display a custom indicator for an interface.

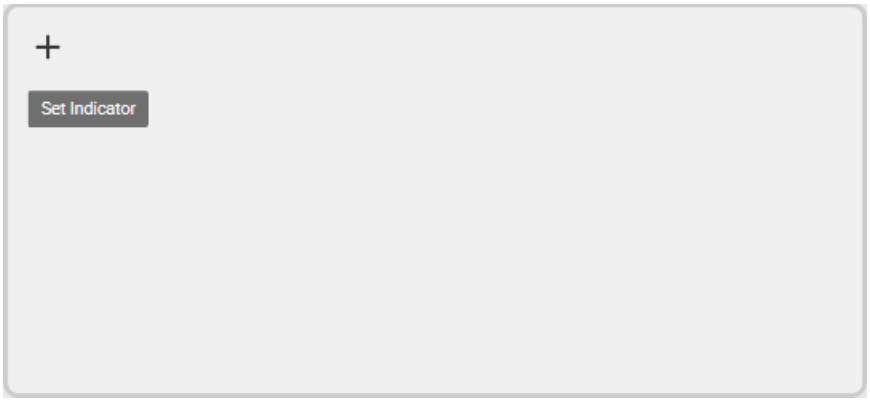
Prerequisites

You must be logged in to the Web UI.

Procedure

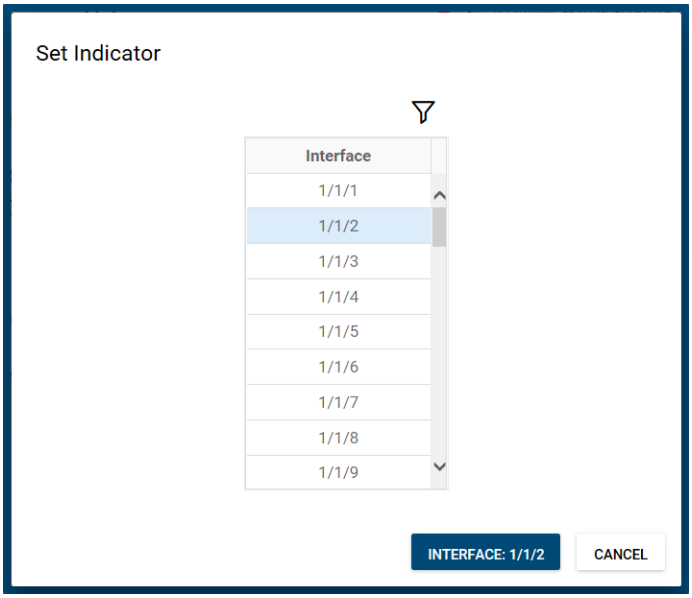
1. Select an empty panel in the Overview page and click the **+** plus button.

Figure 1 *Empty panel with + (plus) button*



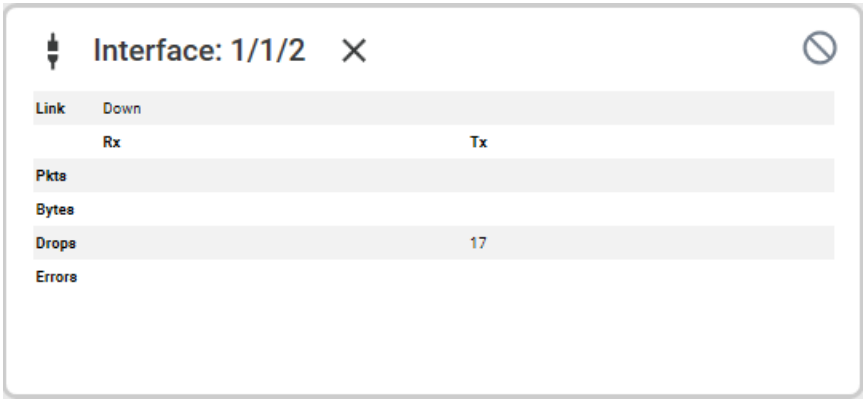
2. The Set Indicator dialog box is displayed. Select the interface you want to set an indicator for. Use the **Show/Hide Column Filters** button to show a specific interface in the list. Click **Interface: <*X/X/X*>** to set an indicator or **Cancel** to exit.

Figure 2 *Set Indicator dialog with example content*



3. A new panel showing an indicator for the interface you selected is added to the Overview page.

Figure 3 *Panel showing a selected interface*



4. If you want to move the panel you added or customize the new panel, click the Layout Management menu in the top banner and select **Unlock Page Layout** to change the layout.
   a. Move the new panel to where you want it to appear on the Overview page.
   b. Resize the new panel, if desired.
5. To remove a custom indicator panel from the Overview page, click the **X** in the custom panel.

Customizing tables

You can show or hide table columns and you can resize column widths. Column customization is persistent in the local browser. For how to filter column data, see Using Show/Hide filters in tables.

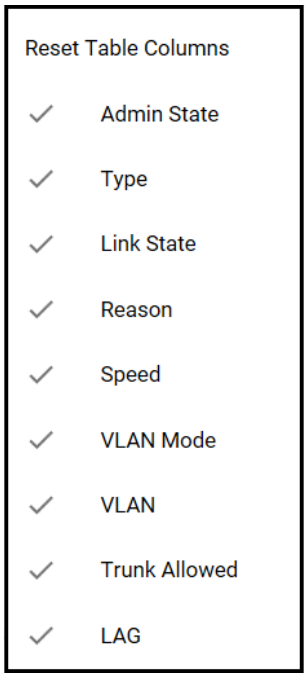
Prerequisites

You must be logged in to the Web UI.

Procedure

1. To hide a table column or show a hidden column, click the Column Settings button in the title bar of the table.
   - From the list of column headings displayed, click any of the headings in the list with a check mark to hide the column.
   - Click any of the headings in the list without a check mark to show the column.
   - Click **Reset Table Columns** to reset to the default.

Figure 1 *List of column headings with check marks*



2. To resize a column drag the column separators to expand or narrow the column. Columns cannot be reordered.
3. View additional pages of content in the table using the table scroll bar.

Using Show/Hide filters in tables

You can use filters to display a subset of data in the table. Filtering is not persistent, so when you leave the page, the filtering is removed.

Prerequisites

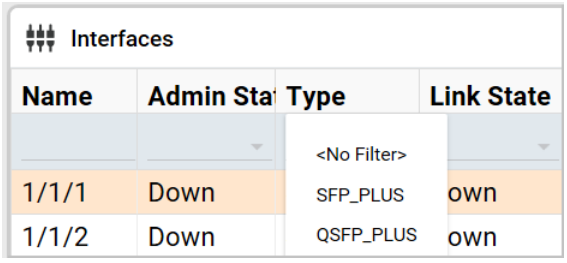
You must be logged in to the Web UI.

Procedure

To filter the data displayed in a table column, click Show/Hide Column Filters on the table title bar. The filter row is displayed below the column headings.

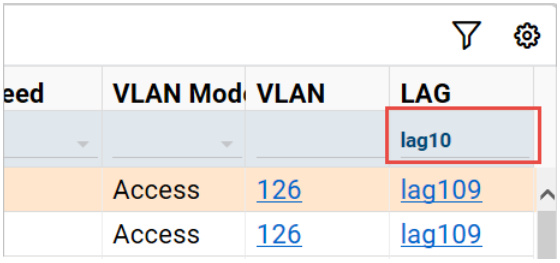
1. For columns that have a drop-down list as a filter, click the down arrow to display the list and select an item from the list. The data displayed in the column will be filtered to just the specified data.

   Figure 1 *Filtering a column by selecting from a list*

2. For columns without a drop-down list, type in a value to filter the data in the column. Any item that matches that value is then displayed. For example, entering lag10 will display data for lag10, lag100, lag109.

   Figure 2 *Filtering a column by typing text*

3. Turn off filters by clicking Show/Hide Column Filters a second time. The full set of data, without filtering, will be displayed in the table.

Chapter 4
AOS-CX Web UI pages

Descriptions of the AOS-CX Web UI pages, and workflows for using these pages.

Navigation pane

Navigate the Web UI by selecting an item in the navigation pane. Information for the selected item is displayed in a series of panels in the details pane. From the details pane, you can select links to drill down to more detailed pages.

Use the  Show/Hide button to show or hide the navigation pane.

In the navigation pane, expand and collapse the System, Diagnostics, or Traffic group to show or hide related items.

The user role (operators, administrators, or auditor) determines which items in the navigation pane you can access.

The navigation pane includes the following links to different feature pages. Click the links for more information.

Link	Description
Overview	Shows important information and statistics about the switch. Each indicator panel provides "roll-up" status (color and icon) of Analytics, Environmental, System, and so on. Empty titles allow you to select and save specific interfaces to monitor (packets, bytes, utilization).
Analytics Dashboard	Shows the Analytics Dashboard providing information related to Network Analytics Engine agents, scripts, alerts, and actions generated by these scripts. Not applicable to the 4100i, 6000, or 6100 Switch Series.
Interfaces	Shows information and status for each interface. Allows you to edit the interface details.
VLANs	Shows information for each VLAN and the status of the VLANs. Allows you to add, edit, and delete VLANs.
LAGs	Shows the information and the up or down status of the LAGs. Allows you to add, edit, and delete Lags.
Users	Shows user roles and names. Also allows you to add or delete a user and change user passwords. Administrator rights are required to access this selection.
PoE	Shows information for PoE ports in the switch. Allows you to configure PoE for the ports.

Link	Description
VSF	Shows the Aruba Virtual Switching Framework (VSF) configuration and status information. This link is displayed for the 6200 and 6300 switches that support VSF. Not applicable to the 4100i, 6000, or 6100 Switch Series.
VSX	Shows the Aruba Virtual Switching Extension (VSX) configuration and status information. This link is displayed only for the 6400 switches that support VSX.
System - Environmental	Shows power supply failures and warnings, temperatures, and fan information.
System - Log	Shows event log entries, event log queries, and message details.
System - Name Server	Shows primary and secondary name servers, and allows you to configure addresses for name servers.
System - SNMP	Shows the details of SNMPv3 users, SNMP communities, and trap receivers. Allows you to add and delete SNMPv3 users, SNMP community names, informs, and trap receivers.
System - Config Mgmt	Enables you to upload/download configurations to or from the running or startup configurations.
System - Firmware Update	Enables you to upload firmware files.
System - Firmware Mgmt	Enables you to configure the switch to distribute firmware to other switches.
Diagnostics - Ping	Enables you to run the `ping` command with various options.
Diagnostics - Traceroute	Enables you to run the `traceroute` command with various options.
Diagnostics - Show Tech	Enables you to run the `showtech` command. Administrator rights are required to run this command.
Traffic - Spanning Tree	Shows the details of the Spanning Tree configuration, assigned ports, and inconsistent ports. Allows you to enable Spanning Tree with Multiple Spanning Tree or Rapid Per-Vlan Spanning Tree mode.
Connected Device - Clients	Shows the details of the devices connected to the switch.
Connected Devices - Configuration	Shows the CDP, LLDP, and client tracking details of the devices connected to the switch. Allows you to configure the CDP, LLDP, and client tracking details at the switch and interface levels.
Security - PKI	Shows the details of the TA profile, EST profile, digital certificates, and associated applications in the switch. Allows you to add, edit, and delete TA profile; add, view, and delete EST profile; add, view, upload, and delete certificates; and edit associated applications.

Link	Description
Security - Port Security	Shows the access port security, authorized MACs, and authorized client limit details. Allows you to edit the port security violation action for the ports.

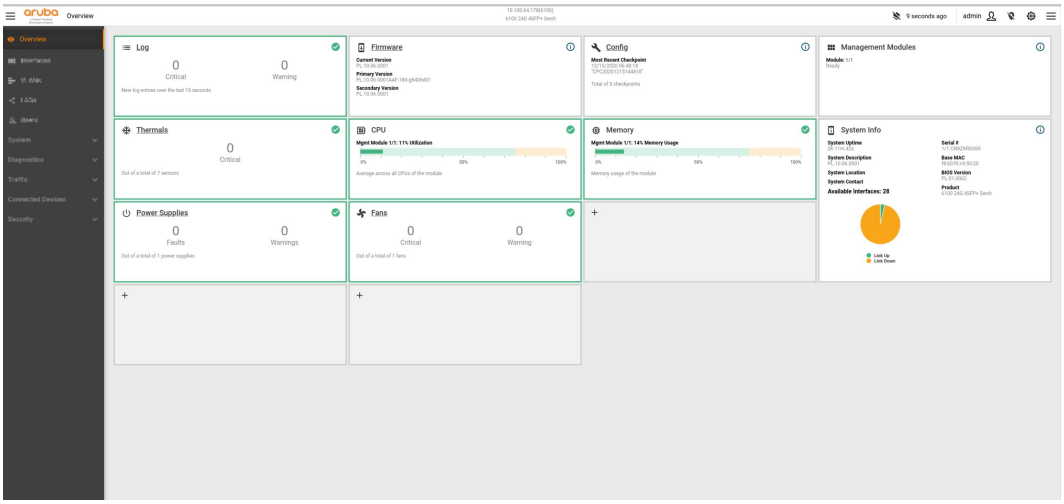
Overview page

The Overview page provides a quick view of the status of a switch. It shows easy-to-read indicators for: Analytics agents, power supply, thermal, fans, CPU use, memory use, log entries, checkpoints, firmware, management modules, and system information.

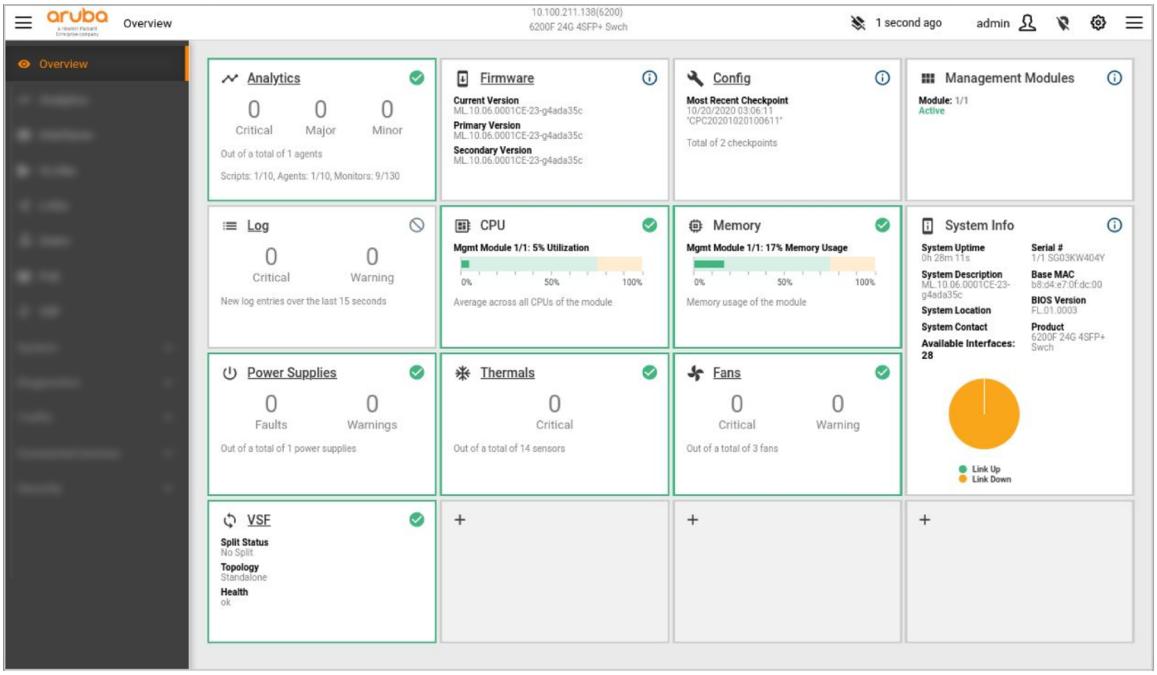
Custom indicator panels allow you to select specific interfaces to monitor and to add panels for those interfaces to the Overview page.

Ensure that both the switch and the client where the Web UI is running are set to use NTP or to a time zone based on UTC time. Otherwise, the NAE agent data might be incorrect or missing and the **System Uptime** will be incorrect. For example, if the time on the switch is set to 2 hours ahead of the client manually, instead of changing the time zone offset, the agent data is populated according to the new time on the switch. If the switch time is set back to match the client time later, the Time Series Database does not overwrite the old data. Therefore the client Web UI shows inaccurate data.

The following image shows the Overview page of the 6100 switch series.

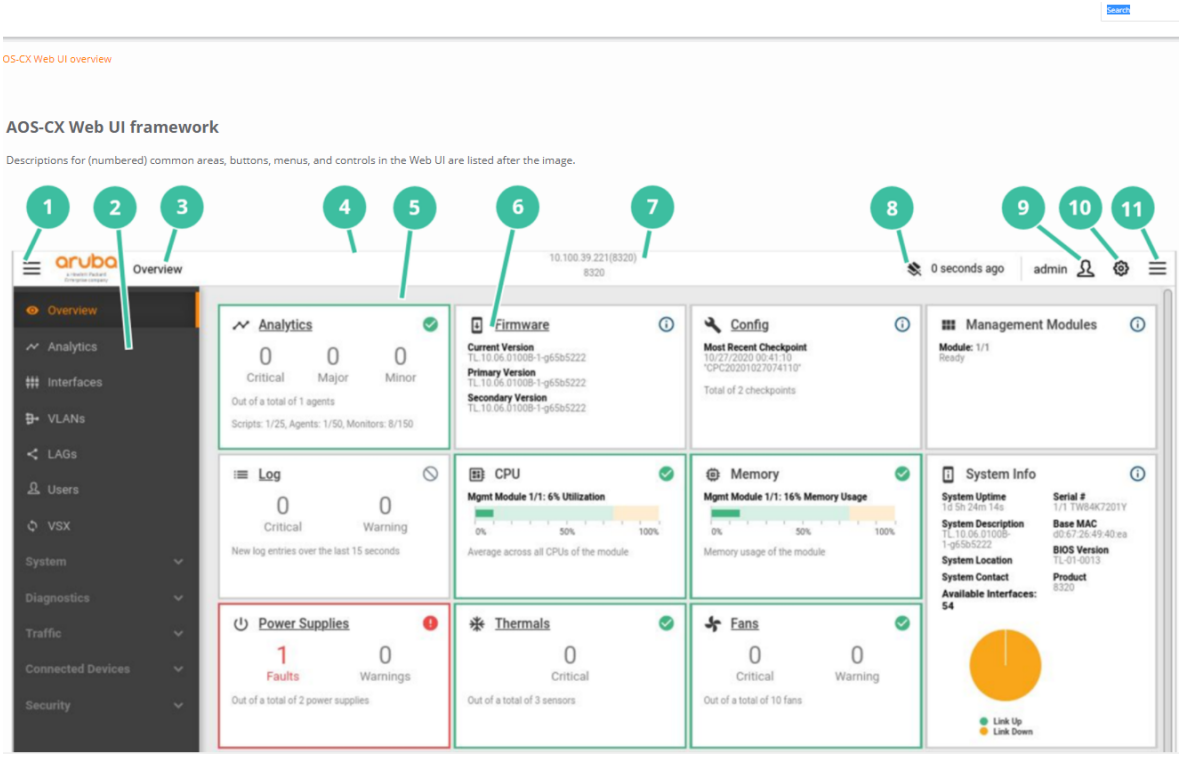


The following image shows the Overview page of the 6200 switch series.



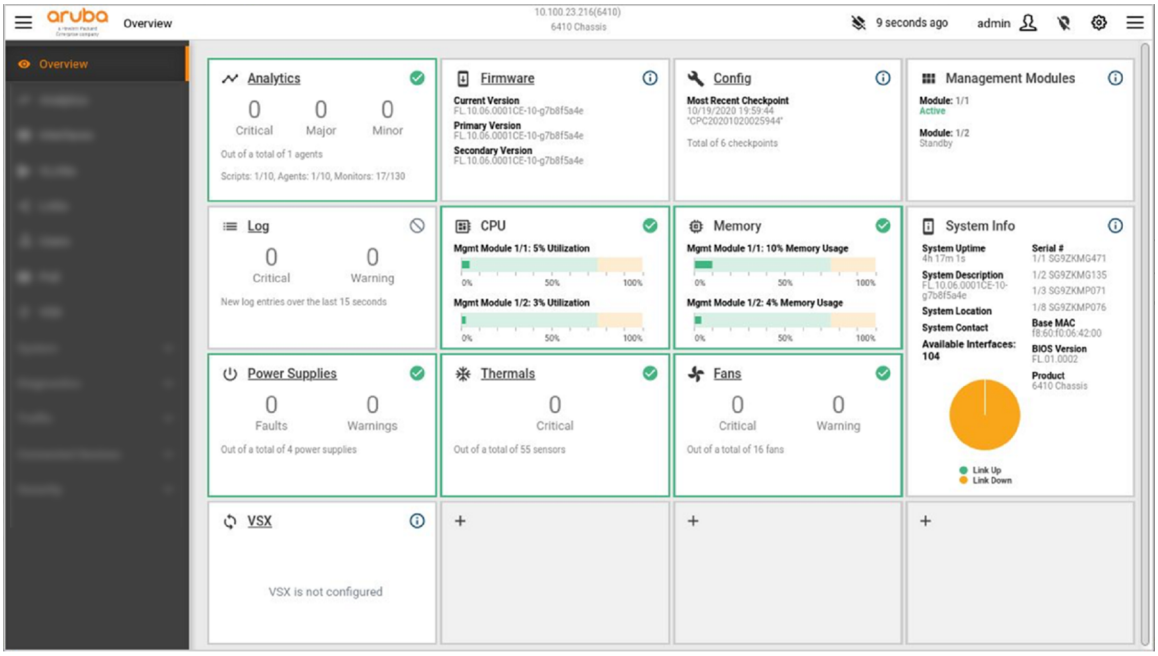
The following image shows the Overview page of the 6300 switch series.

Figure 1 *WebUI Overview Dashboard*



The following image shows the Overview page of the 6400 switch series.

Figure 2 *WebUI Overview Dashboard 6400*



The following table describes the different panels displayed on the Overview page.

Panel	Description
Analytics	Shows: Total number of agents in critical, major, or minor status; total number of agents scripts, agents, and monitors (both enabled and disabled) compared to the maximum number supported on the switch. For example, 7/25 indicates that there are a total of 7 out of a supported maximum of 25. Clicking the link displays the Analytics Dashboard. Not applicable to the 6000 or 6100 Switch Series.
Firmware	Shows: Current firmware version, Primary version, and Secondary version. Clicking the link displays the Firmware Update page.
Config	Shows: Most recent checkpoint and total number of checkpoints. Clicking the link displays the Config Mgmt page.
Management Modules	Shows: Detected module name, Active, and Standby status information.
Log	Shows: New log entries over the last 15 seconds. Clicking the link displays the Log page.
CPU	Shows: Current average CPU utilization per management module.
Memory	Shows: Percent memory usage per management module.
System Info	Shows: System Uptime, System Description, System Location, System Contact, Serial number, Base MAC, BIOS Version, Total number of available interfaces, and a pie chart for link status.
Power Supplies	Shows: Summary count of alerts. Clicking the link displays the Environmental page.
Thermal	Shows: Summary count of alerts. Clicking the link displays the Environmental page.
Fans	Shows: Summary count of alerts. Clicking the link displays the Environmental page.

Panel	Description
VSF	Shows: VSF information, including split status, topology, and health. This panel is displayed for the switches that support VSF. Clicking the link displays the VSF page.
VSX	Shows: VSX information, including inter-switch link (ISL) state, configuration synchronization state, and the role of this switch (primary or secondary). This panel is displayed for the 6400 switches that support VSX. Clicking the link displays the VSX page.

Analytics Dashboard

The 6000 and 6100 Switch Series do not support he Network Analytics Engine, so the there is no Analytics Dashboard in the Web UI for those switches.

The Analytics Dashboard shows information related to Network Analytics Engine agents, scripts, alerts, and information generated by these scripts. You can use the Network Analytics Engine to automate data collection so you can quickly troubleshoot problems on a switch.

To see the total number of agents scripts, agents, and monitors (both enabled and disabled) compared to the maximum number supported on the switch, see the Analytics panel on the Overview page.

From the Analytics Dashboard, you can drill down to other Analytics detail pages.

For some basic steps to using Analytics to monitor a switch, see Viewing agent information using the Web UI. For complete information about using the Network Analytics Engine, scripts, and agents, see the *Network Analytics Engine Guide*.

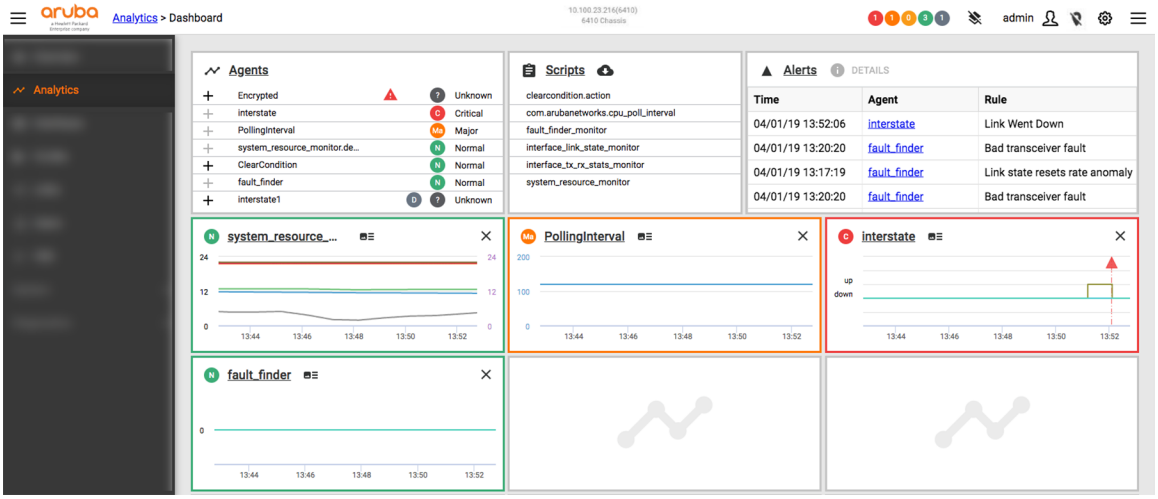
Ensure that both the switch and the client where Web UI is running are set to use NTP or to a time zone based on UTC time. Otherwise, NAE agent data might be incorrect or missing. For example, if the time on switch is set to 2 hours ahead of the client manually instead of by changing the time zone offset, the agent data is populated according to the new time on switch. If the switch time is set back to match client time later, the Time Series Database does not overwrite the old data. Therefore the client Web UI shows inaccurate data.

If the software detects that the switch time and browser time differs by more than one minute, the Web UI displays the following:

- A yellow warning triangle in the top banner of the Analytics Dashboard:

- When a user logs into the Web UI, the Web UI displays a warning message with the following title:
  `Switch Time and Browser Time are not in Sync`

Figure 1 *Analytics dashboard*



Agents panel

The Agents panel displays a list of agents and agent status (Normal, Minor, Major, Critical and Disabled).

Agents monitor what is specified in the script. You can view agent details like alerts, time series graph of alerts and changes, and parameter information. Agent status (reflecting any alerts or errors) is rolled up to display in the Analytics panel on the Overview page.

Click the **Agents** link to drill down to the Agents Management page. Click the link to an individual agent in the list to drill down to the Agent Details page.

Scripts panel

The Scripts panel displays a list of scripts.

Scripts specify what the Network Analytics Engine monitors. The script also specifies various conditions and corresponding actions when these conditions are met. Some read-only scripts are provided with the switch. You can create your own scripts or use scripts from other sources such as ones hosted on the Aruba Solutions Exchange (ASE).

Click the **Scripts** link to drill down to the Scripts Management page. Click the link to an individual script in the list to drill down to the Scripts Details page.

Alerts panel

The Alerts panel displays a list of alerts generated by the agents running on the switch. When a condition is met, an alert is generated.

Select an alert and click the **Details** button to display a dialog box with more information on the alert. Click the **Alerts** link to display the Alert History page. Click an agent name to drill down to the Agents Details page.

Analytics time series graph

Optionally, you can add an Analytics agent time series graph to the Analytics Dashboard by clicking the **+** plus sign next to any agent listed in the Agents panel. If an agent has multiple time series graphs, the graph displayed on the Analytics Dashboard is specified by the script. You cannot choose which graph to display on the Analytics Dashboard, but you can see all the graphs in the Agent Details page. The time series graph shows data collected by the Analytics agent.

Graphs added to the Analytics Dashboard are persistent only in the local browser. If you use a different system or browser, then you would need to customize to add the graphs for that browser instance.

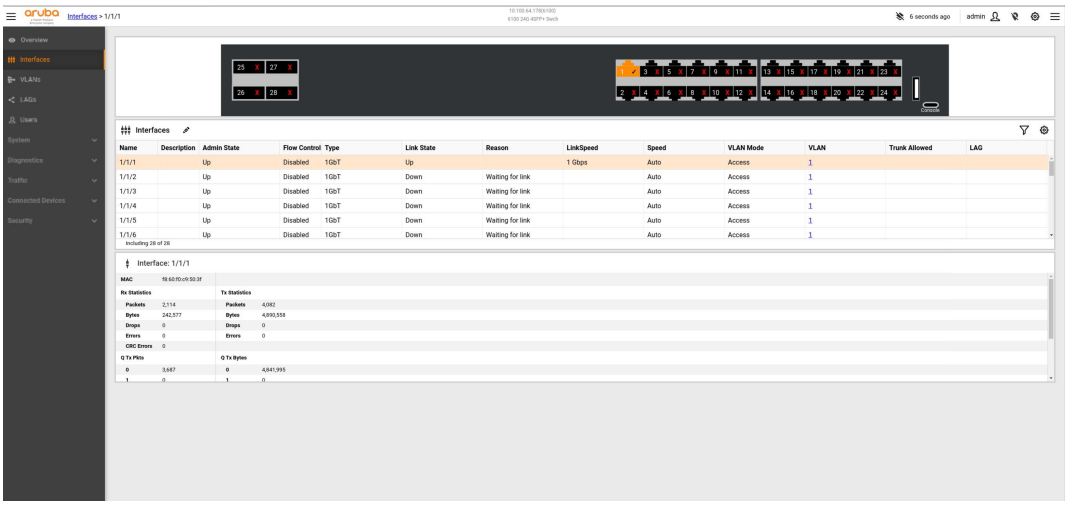
You can remove a graph by clicking **X** in the panel with the agent time series graph.

Click the link in the graph to drill down to the Agent Details page.

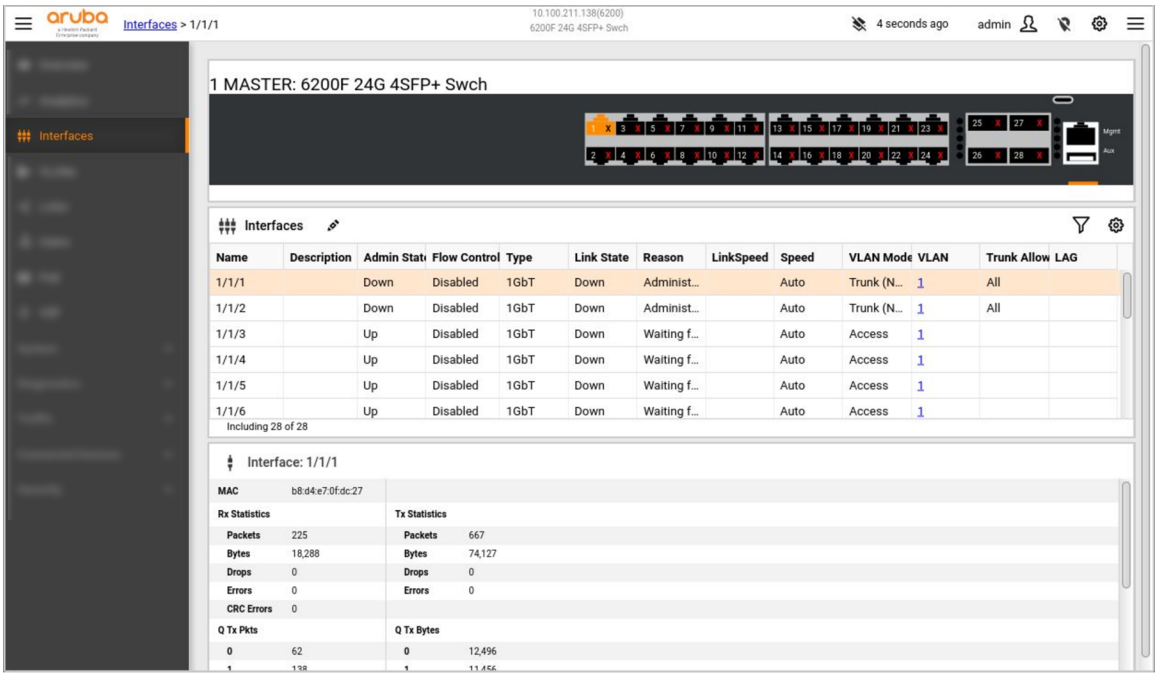
Interfaces page

The Interfaces page displays a list of interfaces. Details on the interface include: Name, Admin State, Type, Link Status, Reason for status, Speed, VLAN Mode, a list of VLANs, Trunk Allowed, and a list of LAGs.

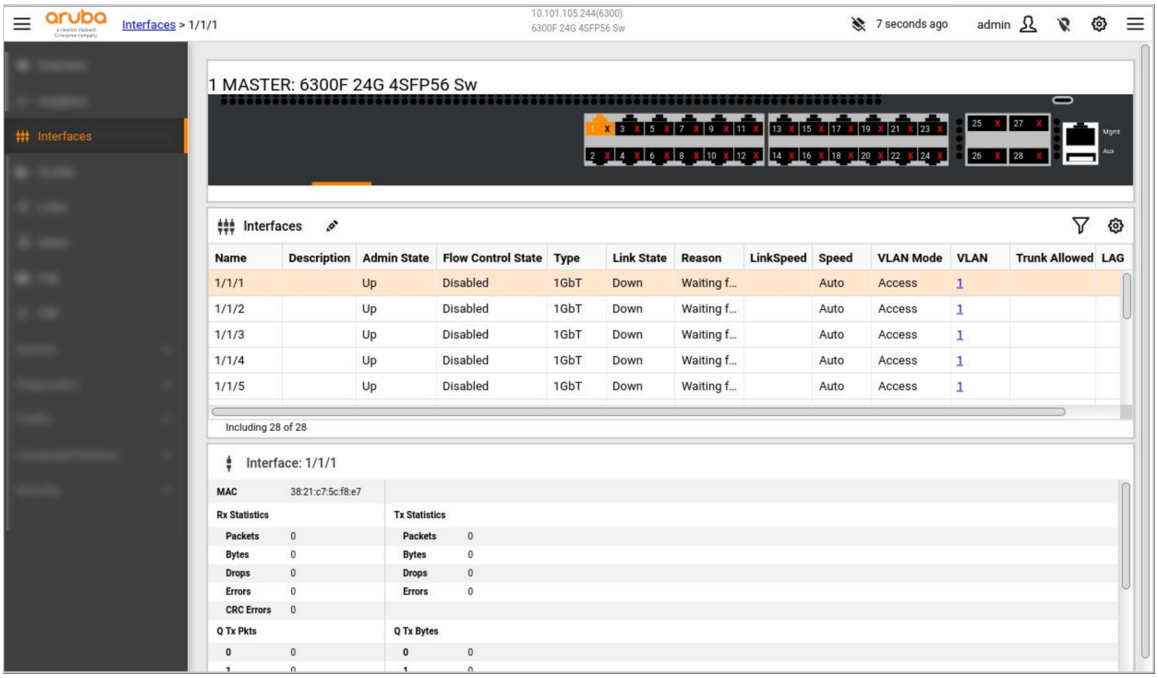
The following image shows the Interfaces page with the faceplate for the 6100 switch.



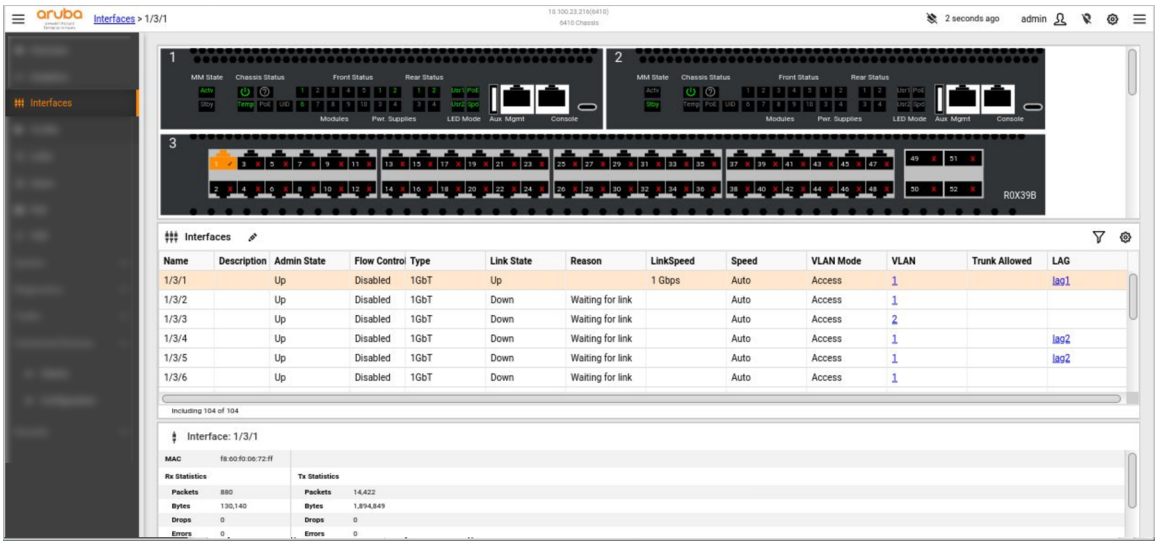
The following image shows the Interfaces page with the faceplate for the 6200 switch.



The following image shows the Interfaces page with the faceplate for the 6300 switch.



The following image shows the Interfaces page with the faceplate for the 6400 switch.



Links in the VLAN and LAG columns allow you to drill down to the respective VLANs or LAGs page, auto-selecting the appropriate resource. Selecting a row in the interfaces list, displays more information on the interface. Details include: duplex, MAC, IPv4, IPv6 address, Rx and Tx stats, packets, and more.

A graphical panel shows interface modules currently installed. Clicking an interface, selects the corresponding row in the table. Each interface displayed in the graph will dynamically change based on the current interface status.

Use the **Show/Hide Column Filters** button or **Column Settings** button to customize the table display. You can edit an interface and update the interface details.

The WebUI does not accurately display admin status or attributes for a LAG subinterface. Use the **show interface *<IFNAME>.<ID>*** command in the command-line interface to view details for a LAG subinterface.

Editing an interface

Use this procedure to perform the following tasks:

- Add an interface description
- Set the interface speed
- Set admin status
- Set flow control status
- Split interface

Procedure

1. In the navigation pane, select **Interfaces**.

   The Interfaces page is displayed.

2. In the **Interfaces** panel, select an interface, and click .

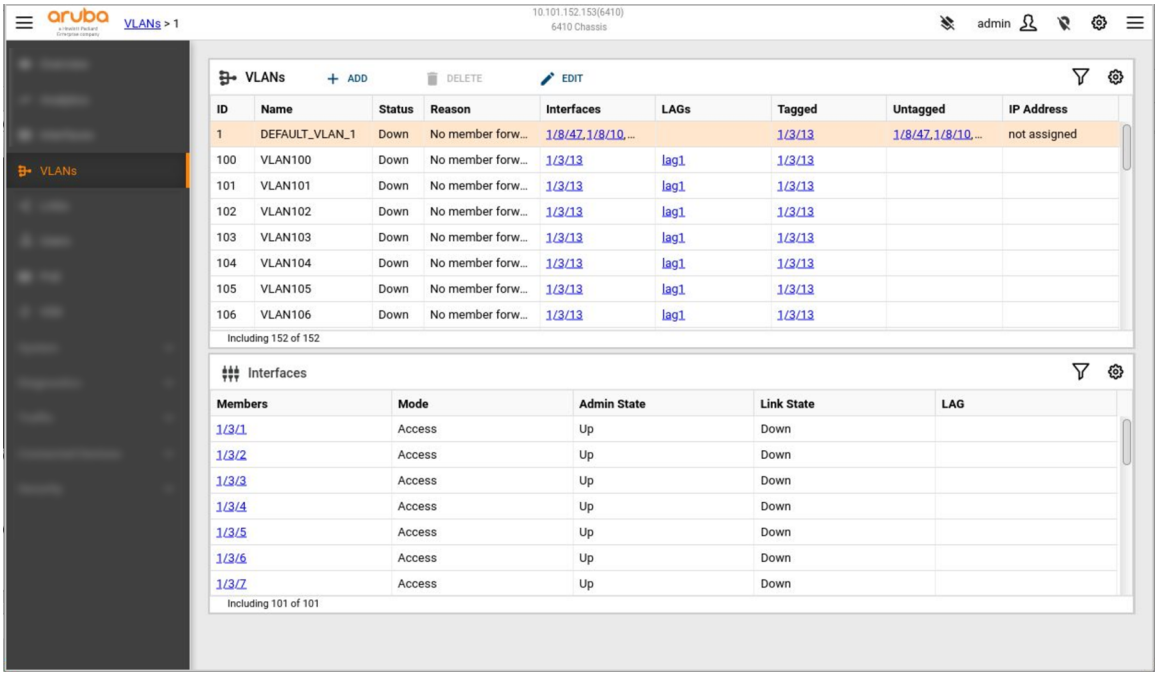
   The Configure Interface dialog box is displayed for the selected interface. You can select a different interface if required.
3. Enter a description for the interface. For example, **Guest connection**.
4. You can select one of the following values for the interface speed.
   - **10-full**
   - **10-half**
   - **100-full**
   - **100-half**
   - **auto**
5. Select **Up** or **Down** for the **Admin Status**.
6. Select **Enable** or **Disable** for the **Flow Control Status**.

   Only the Web UI for 6400 (SKU: ROX45A LC) switch has an additional setting called **Split** for the 40 Gb/s ports. Splitting a port disables the selected port, clears all port configuration, and splits the port into multiple interfaces. The split interfaces are not available until you reboot the switch or the module. For example, select the 40 Gb/s port, and select the **Split** checkbox to split the port into four 10 Gb/s interfaces.

7. Click **Update**.

VLANs page

The VLANs page displays a list of VLANs configured in the switch.



VLANs panel

The **VLANs** panel shows the details of each VLAN including the ID, Name, Status, Reason (errors such as No member port), a list of interfaces, LAGs, tagged and untagged ports, and IP address. The IP address column displays only an IPv4 address. IP address is blank if a VLAN interface is not created, and displays **not assigned** if the VLAN interface is created, but an IPv4 address is not configured.

Links in the Interfaces and LAGs columns allow you to drill down to the respective Interfaces or LAGs pages, auto-selecting the appropriate resource.

Interfaces panel

The **Interfaces** panel shows more information on the VLAN interfaces including Members, Mode, Admin State, Link State, and the associated LAG name.

Adding and deleting a VLAN

You can add from 1 to 4094 VLANs.

To add a VLAN:

1. In the navigation pane, select **VLANs**.

   The VLANs page is displayed.
2. In the **VLANs** panel, click **Add**.

   The Add VLAN dialog box is displayed.
3. Configure the following parameters:
   - **Vlan ID**: A unique number from 1 to 4094.
   - **Vlan Name**: A unique string to represent the VLAN. A default name is added with the VLAN ID that you enter. You can change the default name.
4. Click **OK**.

To delete a VLAN:

1. In the **VLANs** panel, select the VLAN, and click **Delete**.

   A confirmation message is displayed.

When you delete a VLAN, if the selected VLAN is used as an interface VLAN, then the VLAN interface is also deleted.

2. Click **Delete VLAN**.

Editing a VLAN

Use this procedure to perform the following tasks:

- Edit the VLAN name
- Add and delete ports
- Configure IPv4 address

For the default VLAN, you cannot edit the name or delete ports.

Procedure

1. To edit a VLAN name:
   a. In the navigation pane, select **VLANs**. The VLANs page is displayed.
   b. In the **VLANs** panel, select the VLAN, and click **Edit**. The Edit VLAN dialog box is displayed.
   c. Edit the name.
   d. Click **OK**.
2. To add ports:
   a. In the Edit Vlan dialog box, select **Add Ports**.
   b. Select the **Vlan Mode** as **Access** or **Trunk**.
      - If you select the **Vlan Mode** as **Access**, then you can add access ports. All access ports are displayed in the **Untagged** column in the **VLANs** panel.
      - If you select the **Vlan Mode** as **Trunk**, then you can select **Allowed** or **Native** under **Vlan Trunk**. All trunk ports are displayed in the **Tagged** column in the **VLANs** panel.
      - If you select the **Vlan Trunk** as **Allowed**, then you can select the **Allow all Vlans** checkbox to associate the entered port with all configured VLANs. By default, the port is associated to any new VLAN that you add.
      - If you select the **Vlan Trunk** as **Native**, then you can select the **Tag** checkbox to add the port as native-tagged. Not selecting the **Tag** checkbox, leaves the ports as native-untagged.
   c. Enter the port number in the **member/slot/port** notation.

      You can add multiple ports with comma separated port numbers. For example, 1/1/1,1/1/2,1/1/3. You can also add a LAG by entering the LAG name. For example, lag1, lag2.
   d. Click **OK**.

3. To delete ports:
   a. In the Edit Vlan dialog box, select **Delete Ports**.

b. Delete the port numbers that you want to retain. The ports that are displayed in the dialog box are deleted for the selected VLAN. Ports are displayed in the dialog box based on the option that you select for the **Vlan Mode** and **Vlan Trunk**.
c. Click **OK**.

4. To configure IP address:
   a. In the Edit Vlan dialog box, select **IP Configuration**.
   b. Select **Enable** to create a VLAN interface (if not created earlier) for the selected VLAN, and configure a static IPv4 address.

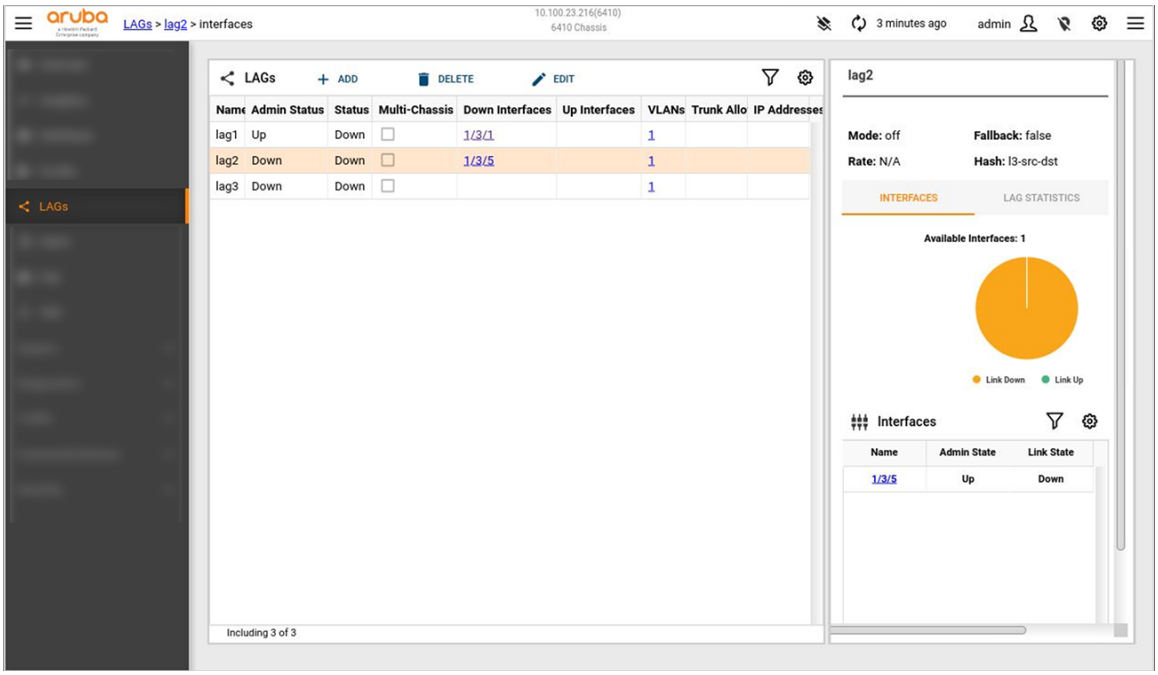
> Selecting **Disable**, removes any previously configured static IPv4 address on the selected interface. Only the default VLAN can have DHCP IP configuration. For the default VLAN, configuring a static IP through the Web UI, overrides the DHCP IP address. If you disable static IP configuration, the IP address changes to the DHCP IP.

   c. Enter the **IP Address** with the subnet mask in the IPv4 format (**x.x.x.x/x**).
   d. Click **OK**.

LAGs page

The LAGs page displays a list of LAGs. Details on each LAG include: Name of the LAG, whether the admin status is up or down, LAG bond status, whether the LAG is a multi-chassis LAG, a list of down interfaces, a list of up interfaces, a list of VLANs, whether trunk allowed or not allowed, and a list of IP addresses.

Figure 1 *LAGs Page*



Links in the Interfaces and VLANs columns allow you to drill down to the respective Interfaces or VLANs pages, auto-selecting the appropriate resource. Selecting a row in the LAGs list displays more information on the LAG. Details include Interfaces and LAG statistics.

You can add and delete static LAGs. You can edit a LAG and add or delete ports, and set the admin status.

Use the Show/Hide Column Filters button or Column Settings button to customize the table display.

Adding and deleting a LAG

To add a LAG:

1. In the navigation pane, select **LAGs**.

   The LAGs page is displayed.
2. In the **LAGs** panel, click **Add**.

   The Add Lag dialog box is displayed.
3. Enter a number between 1 to 256.
4. Click **OK**.

To delete a LAG:

1. In the **LAGs** panel, select the LAG, and click **Delete**.

   A confirmation message is displayed.
2. Click **Delete Lag**.

Editing a LAG

Use this procedure to perform the following tasks:

- Add and delete ports
- Set admin status

To add ports:

1. In the navigation pane, select **LAGs**.

   The LAGs page is displayed.
2. In the **LAGs** panel, select a lag, and click **Edit**.

   The Edit Lag dialog box is displayed.
3. Select **Add Ports**.
4. Enter the port number in the **member/slot/port** notation.

   You can add multiple ports with comma separated port numbers. For example, 1/1/1,1/1/2,1/1/3.
5. Click **Update**.

To delete ports:

1. In the Edit Lag dialog box, select **Delete Ports**.
2. Delete the port numbers that you want to retain. The ports that are displayed in the dialog box are deleted for the selected LAG.
3. Click **Update**.

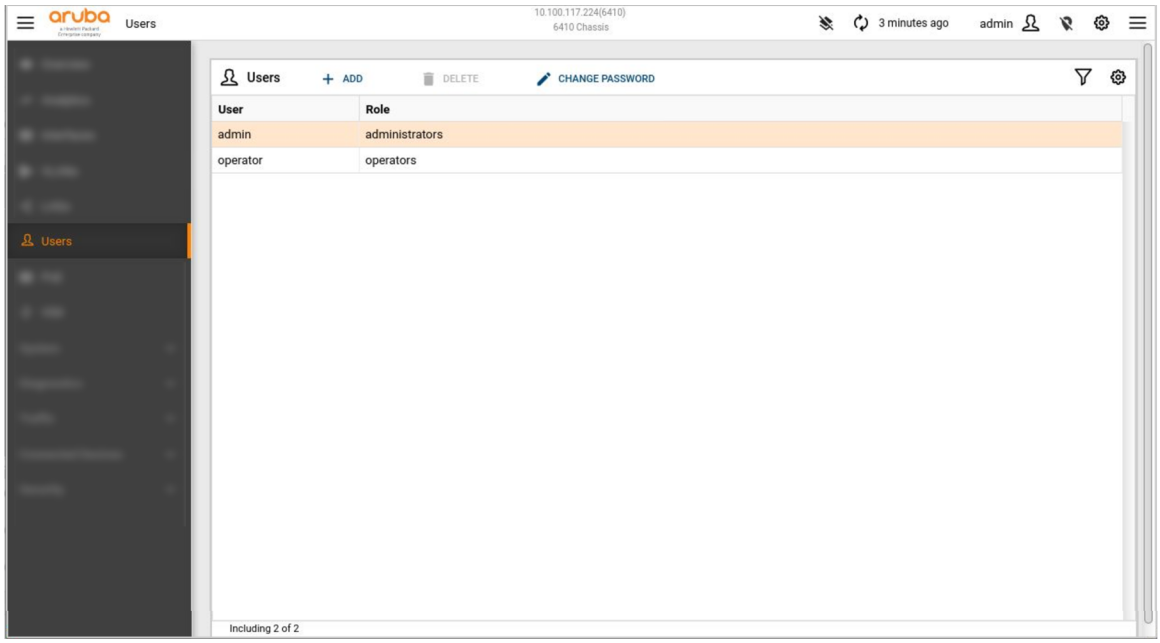
To set admin status:

1. In the Edit Lag dialog box, select **Set Admin Status**.
2. Select **Up** or **Down** as the admin status.
3. Click **Update**.

Users page

The Users page displays user names and roles. You can also add or delete a user, or change a password for the logged in user. A user with the administrator role can access this page.

Figure 1 *Users page showing an administrator user entry*



Adding and deleting a user

You can add users with the following roles:

- Administrators: An administrator can access all pages and perform all tasks in the Web UI. An administrator user is added by default.
- Operators: An operator can access all pages except the Users page and perform all tasks except adding or deleting users and changing password.
- Auditors: An auditor can access only the Log page, and generate and export log reports.

Prerequisites

You must have the administrator role to add or delete users.

Procedure

To add a user:

1. In the navigation pane, select **Users**.
   The Users page is displayed.
2. In the **Users** panel, click **Add**.
   The New User Info dialog box is displayed.
3. Select a role for the user: operators, administrators, or auditors.
4. Enter the user name.
   The user name can contain a maximum of 32 characters with only lowercase alphanumeric, dot, dash, and underscore characters.
5. Enter the new password and confirm the password.
   The password can contain a maximum of 32 characters without a space.

6. Click **Add User**.

To delete a user:

1. In the **Users** pane, select the user to delete, and click **Delete**. You cannot delete the default administrator user.

   A confirmation message is displayed.
2. Click **Delete User**.

Changing the password for a user

Prerequisites

You must have the administrator role to add or delete users.

Procedure

To change the password for a user:

1. In the navigation pane, select **Users**.

The Users page is displayed.

2. In the **Users** panel, select the user, and click **Change Password**.

The Changing Password dialog box is displayed.

3. Enter the current password.
4. Enter the new password and confirm the password.

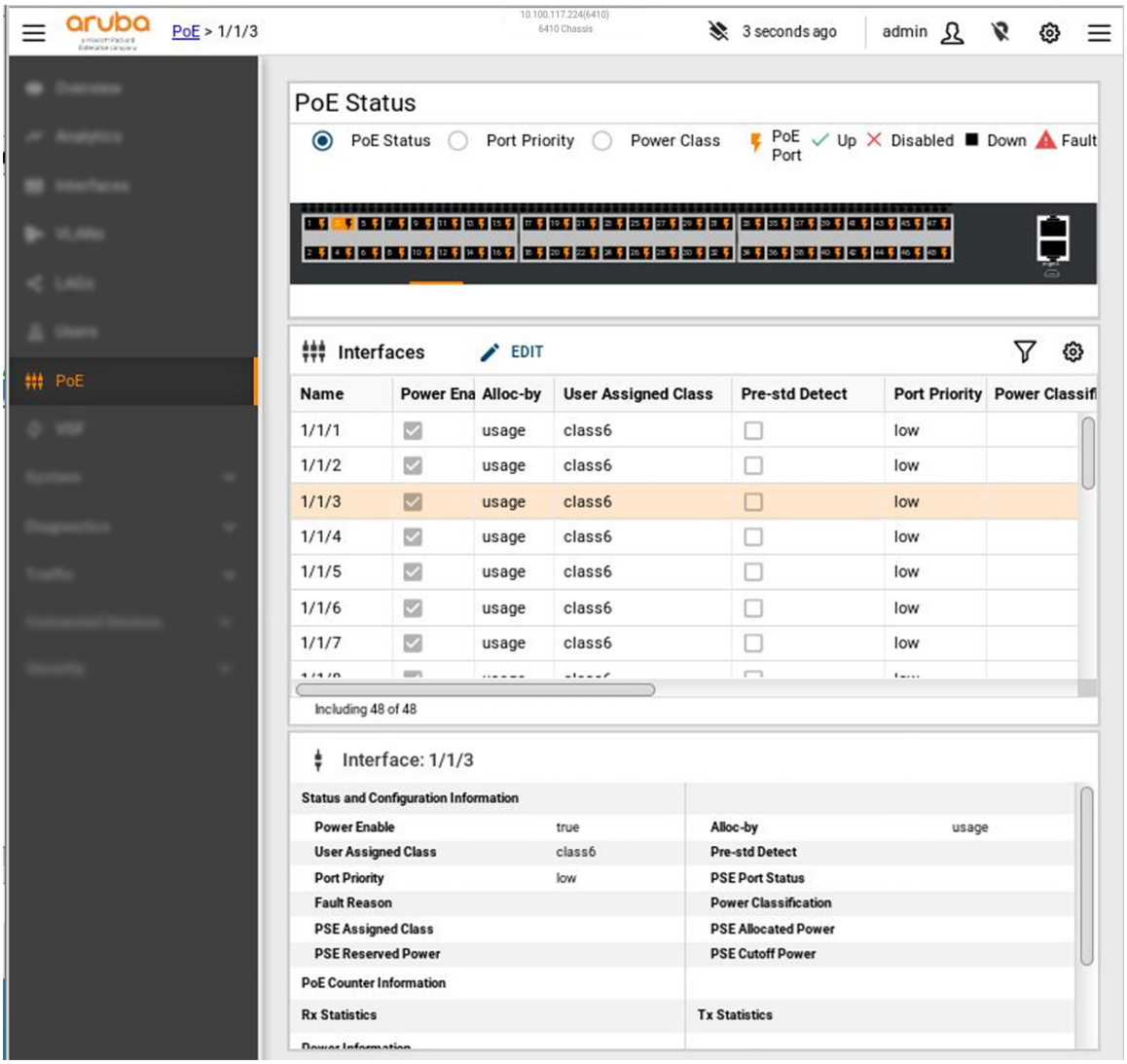
The password can contain a maximum of 32 characters without a space.

5. Click **Change Password**.

PoE page

The PoE page displays the details of the PoE enabled ports in the switch. This page is displayed for all switches that can be stacked and for switches that have PoE ports.

Figure 1 *PoE page*



PoE Status panel

The **PoE Status** panel displays the details by the PoE Status, Port Priority, and Power Class of the switch ports. The PoE details are displayed only for the ports that support PoE.

The PoE Status view displays the following status of the ports in the graphical representation of the switch:

- PoE Port: Indicates that the port is PoE enabled.
- Up: Indicates that the interface is up.
- Disabled: Indicates that the port is power enabled.
- Down: Indicates that the interface is down.
- Fault: Indicates that the port is faulty.
- Power Denied: Indicates that the power is denied to the interface.

The Port Priority view displays the priority as Low, High, and Critical in the ports in the graphical representation of the switch.

The Power Class view displays the color code for the power class in the ports in the graphical representation of the switch.

In the case of a stack, the graphical representation displays details for all the switches in the stack.

Interfaces panel

The **Interfaces** panel shows the details of all PoE ports. You can edit the PoE settings and enable or disable PoE on a port.

Interface panel

The **Interface** panel shows the details of the port selected in the **Interfaces** pane.

Editing the PoE settings for a switch port

To edit PoE settings:

1. In the navigation pane, select **PoE**.

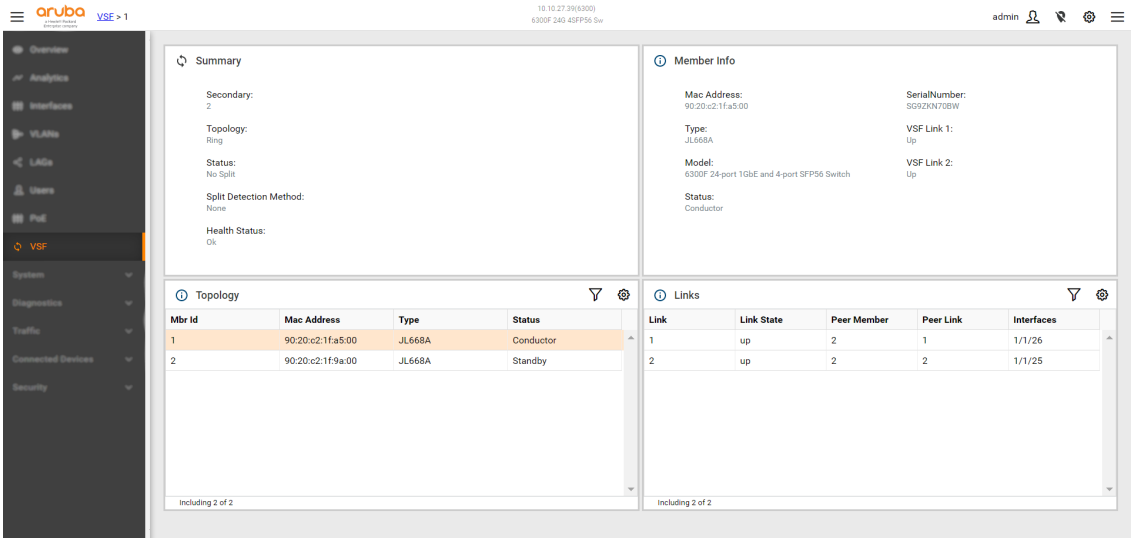
   The PoE page is displayed.
2. In the **Interfaces** panel, select the port, and click **Edit**.

   The Edit PoE Details dialog box is displayed.
3. Configure the following parameters:
   - **Priority**: The priority level—Critical, High, or Low.
   - **Class**: The PoE class assigned to the port.
   - **Alloc-by Configuration**: Power allocation by usage or class.
   - **Power Enable**: Enable or disable power on the port.
   - **Pre-Standard Detect**: Enable or disable pre-standard device detection.
4. Click **Change**.

VSF page

The VSF page displays the topology, link, and member details of the switches in a stack. This page is displayed only for all 6200 and 6300 switches that are VSF stacking capable.

Figure 1 *VSF page*



Summary panel

The **Summary** panel shows the topology, split status, split detection method, and health status of the switch in the stack.

Member Info panel

The **Member Info** panel shows the MAC address, product code, model, status (Conductor or member), serial number, and VSF link details of the switch.

Topology panel

The **Topology** panel lists the member switches and the Conductor switch with the MAC address, product code, and status (Conductor or member).

Links panel

The **Links** panel shows the link state, peer member, peer link, and interfaces details of the switch selected in the **Topology** pane.

VSX page

If Aruba Virtual Switching Extension (VSX) is configured, the VSX page (displayed only for the 6400 switches) shows configuration and status information about the VSX:

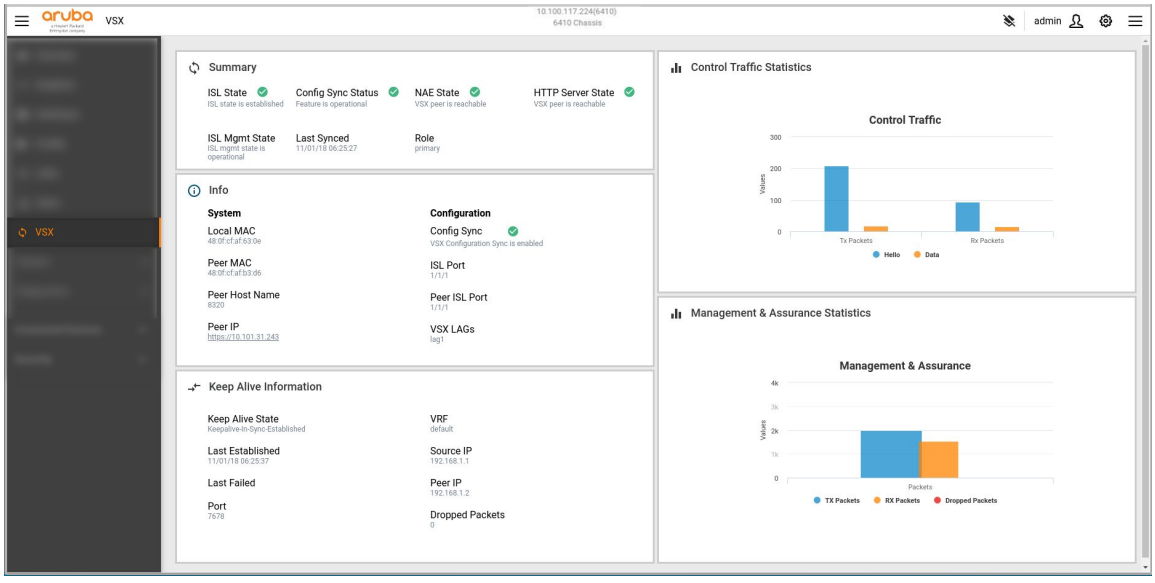
- The switch configurations include VSX LAGs that span both switches.
- Each switch has a user-configured role: either `primary` or `secondary`. If configuration synchronization is enabled, supported configuration changes performed on the primary switch are performed on the secondary switch automatically.
- The switches synchronize their configuration and state information over a user-configured inter-switch link (ISL).

The ISL is used for both datapath traffic forwarding and control path VSX protocol exchange.

- A separate IP-based keepalive mechanism completes the control plane by providing an integrity check if there is an ISL failure.

For more information about VSX, see the *Virtual Technologies Guide*.

Figure 1 *VSX page*



Summary panel

The **Summary** panel shows state information about the switch to which you are connected, including whether the switch role is primary or secondary and state information about the connections to the peer switch.

The IP address of the switch to which you are connected is shown in the top banner of the Web UI.

Info panel

The **Info** panel provides configuration information about the VSX switches, including the following:

- The system ID of this switch and of the peer switch.
- The ISL port of this switch and of the peer switch. If the ISL is a LAG, the name of the LAG is shown.
- The host name and IP address of the peer switch.
- Whether configuration synchronization between switches is enabled.
- The names of the VSX LAGs.

Keep Alive Information panel

The **Keep Alive Information** panel shows information and status information about the keep alive communications from the keep alive source IP address to the IP address of this switch (shown in the top banner of the Web UI) and IP address of the peer switch (shown under **Peer IP** in the panel).

Control Traffic Statistics panel

The **Control Traffic Statistics** panel shows information about control plane traffic between the primary and secondary VSX switches. The traffic shown in this panel is related to the coordination of information between VSX switches when the switches are acting as a single routing device.

Management & Assurance Statistics panel

The **Management & Assurance Statistics** panel shows information about management traffic between the primary and secondary VSX switches. Examples of management traffic between VSX switches include the following:

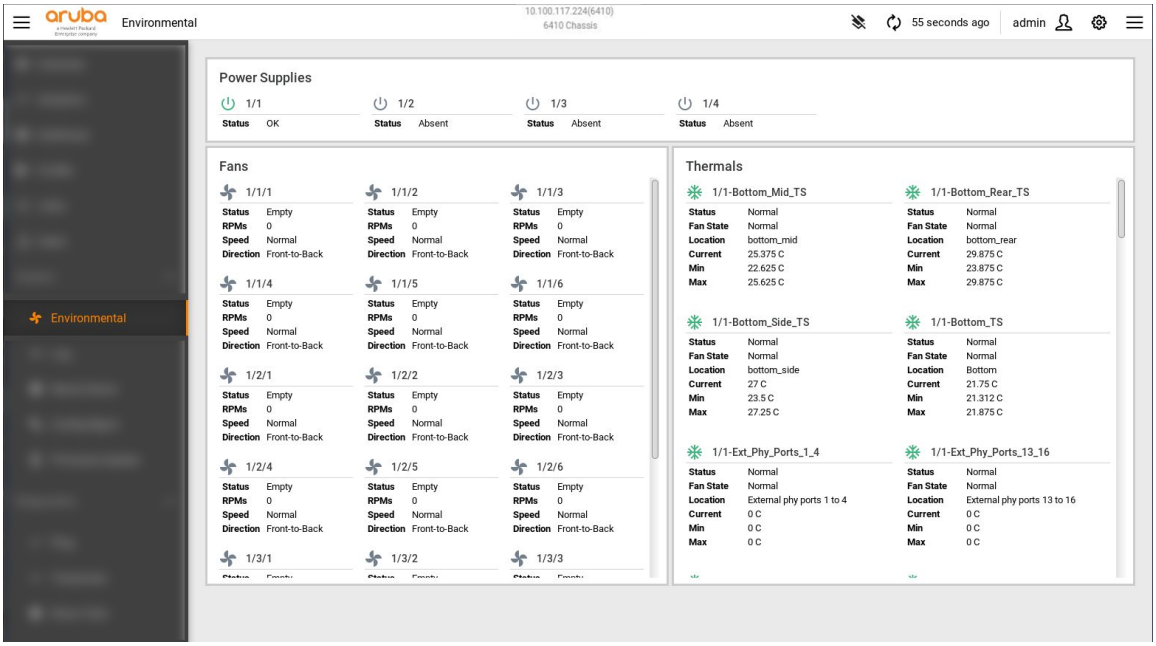
- Traffic related to synchronizing switch configuration data from the primary switch to the secondary switch.
- Traffic related to executing `show` commands that include the `vsx-peer` option to get data from the peer switch.
- Traffic related to Network Analytics Engine monitors or REST API calls that query the peer switch.

Environmental page

From the Environmental page you can view:

- Power supply failures or warnings.
- Fans' details such as status, RPMs, speed, and direction.
- Thermals' details such as status, fan state, location, temperature, maximum, and minimum values.

Figure 1 *Environmental page*



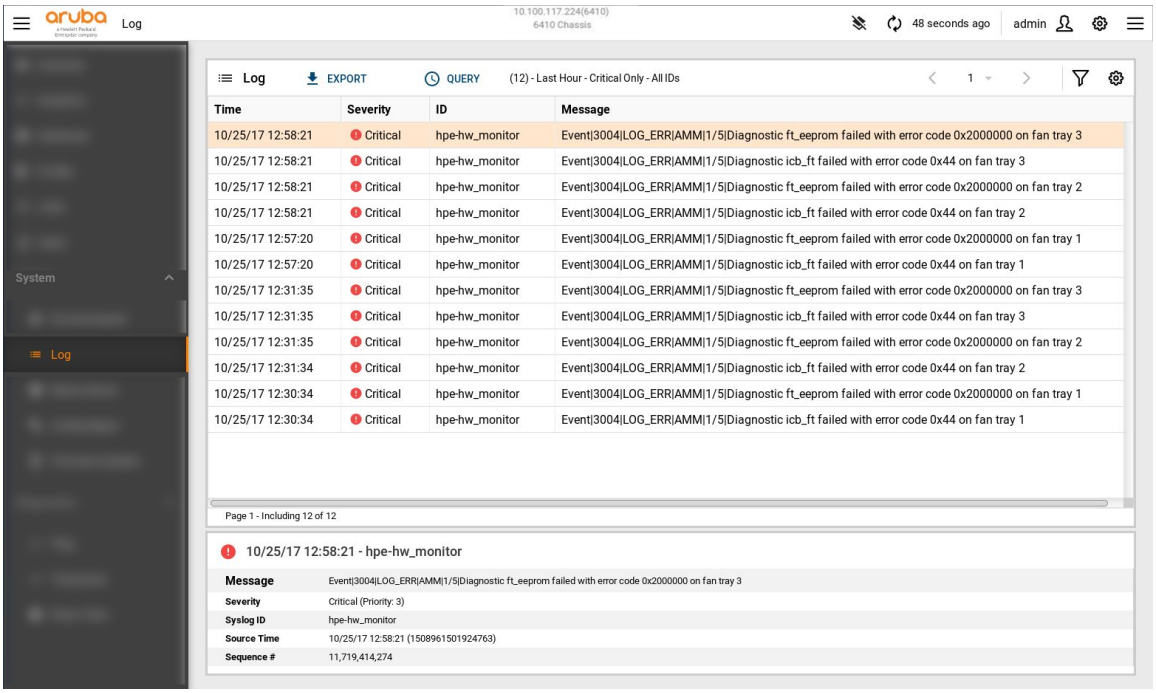
Log page

From the Log page you can view a list of event log entries. Each log entry displayed includes the following: Time, Severity (Critical, Warning, Info), ID, and Message. If you set filtering on the table the custom changes apply only to the data on the current page.

The WebUI reflects only those logging filters configured through the WebUI. Filters configured via the command-line interface will not be applied to WebUI logs.

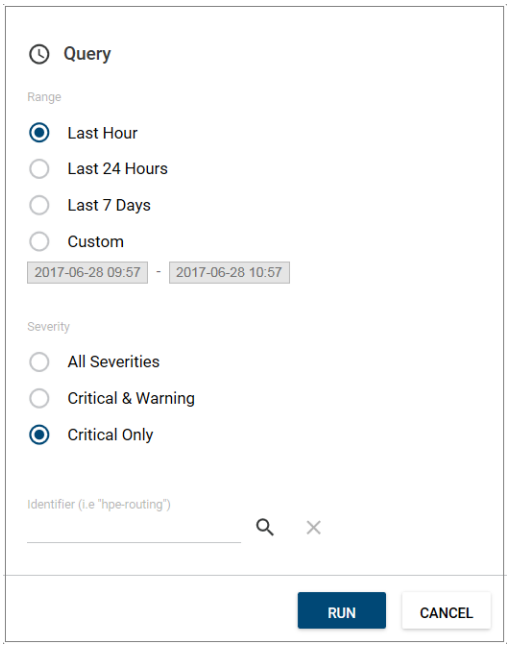
The Log page shows event log messages only. Accounting log messages must be accessed through the REST API or the CLI.

Figure 1 *Log page*



- You can select an entry from the list of log entries to view more information in the details pane.
- Click **Export** to download the current log query as a CSV file.
- To run a new server-side query, click **Query**. A Query dialog box is displayed. You can customize the query by Range, Severity, and identifier. Click **Run** to run the new query.

Figure 2 *Query page*



The following table shows how Syslog RFC 3164 severity levels are mapped to Web UI severity levels.

Web UI severity	Syslog severity
Critical	0 Emergency: system is unusable

Web UI severity	Syslog severity
	1 Alert: action must be taken immediately 2 Critical: critical conditions 3 Error: error conditions
Warning	4 Warning: warning conditions
Info	5 Notice: normal but significant condition 6 Informational: informational messages 7 Debug: debug-level messages

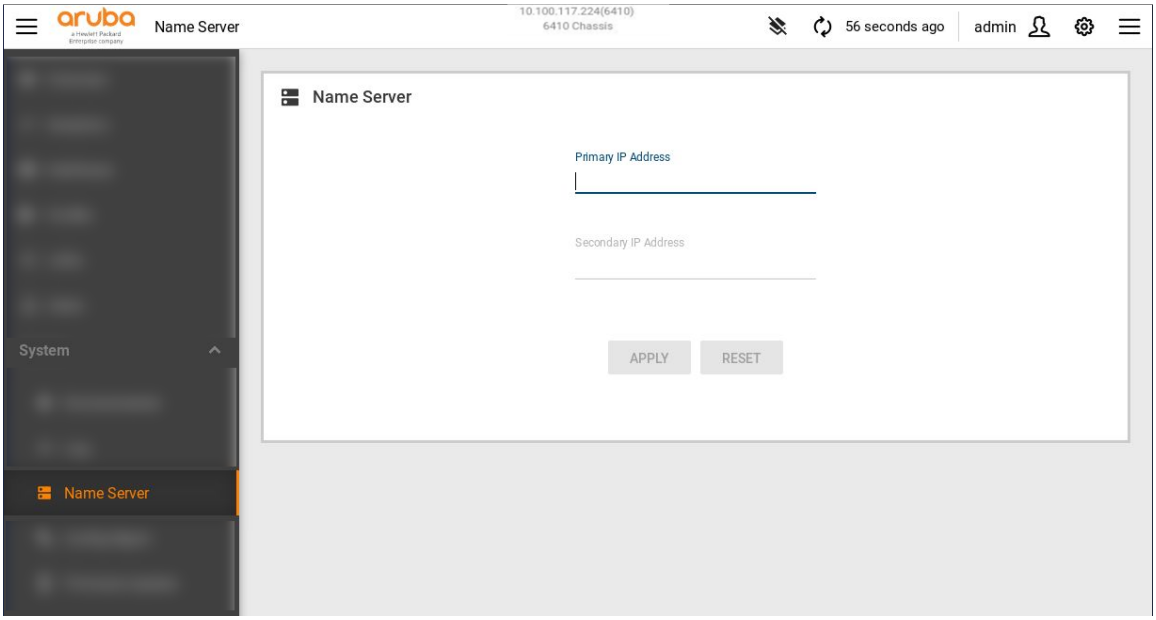
Name Server page

From the Name Server page, you can view the current primary and secondary name server addresses.

To configure the addresses, enter a **Primary IP Address** and **Secondary IP Address**, and click **Apply**. Primary and Secondary Name Server addresses can only be set when there is a static IP address on the management interface. If it has a DHCP address, the values passed from the DHCP server are used.

Click **Reset** to undo any change that are not applied.

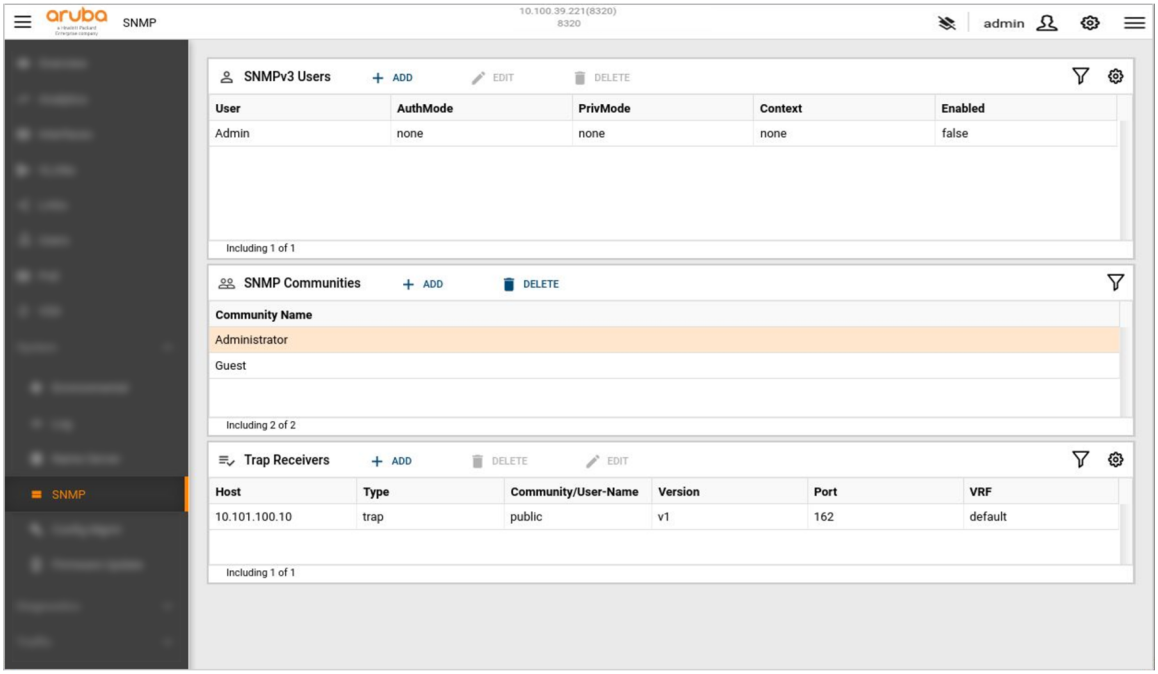
Figure 1 *Name Server page*



SNMP page

The SNMP page displays the SNMP community and trap receiver details.

Figure 1 *SNMP Page*



SNMPv3 Users panel

The **SNMPv3 Users** panel lists the SNMPv3 users added to the switch. You can add, edit, and delete SNMPv3 user details.

SNMP Communities panel

The **SNMP Communities** panel lists the communities added in the switch. You can add and delete SNMP community names.

Trap Receivers panel

The **Trap Receivers** panel shows the details of the trap receivers and SNMP informs added in the switch. You can add and delete trap receivers and SNMP informs.

Adding and deleting an SNMPv3 user

You can add SNMPv3 users to provide secured access to SNMP management stations. You can optionally associate an authentication protocol and a privacy protocol, with passwords, to each user.

The user names that you add can be used when adding SNMPv3 trap receivers.

Procedure

To add an SNMPv3 user:

1. In the navigation pane, expand **System**, and select **SNMP**.

   The SNMP page is displayed.
2. In the **SNMPv3 Users** panel, click **Add**.

   The New SNMPv3 User Info dialog box is displayed.
3. Enter a user name.

   The user name can contain a maximum of 32 characters without a space and must begin and end with an alphabet, a number, or an underscore. The user name cannot contain any special characters other than the underscore.

4. You can configure the following optional parameters:
   - **Authentication Protocol**: You can select either **md5** (Message Digest) or **sha** (Secure Hash Algorithm) as the standard cryptographic hash function, to provide secured access to the user.
   - **Authentication Password**: You must enter a password if you select an authentication protocol. The password must be 8 to 32 characters long, and can contain alphabets, numbers, and special characters.
   - **Privacy Protocol**: You can select either **aes** (Advanced Encryption Standard) or **des** (Data Encryption Standard) as the standard encryption method, to provide secured access to the user.
   - **Privacy Password**: You must enter a password if you select a privacy protocol. The password must be 8 to 32 characters long, and can contain alphabets, numbers, and special characters.
   - **Context**: You can enter an SNMPv3 context that exists in the switch. For more information about viewing and adding SNMPv3 context, see the *AOS-CX Command-Line Interface Guide*.
5. Click **Add**.

To delete an SNMPv3 user:

1. In the **SNMPv3 Users** panel, select the SNMPv3 user name that you want to delete, and click **Delete**.

   A confirmation message is displayed.
2. Click **Delete**.

Editing an SNMPv3 user

Use this procedure to edit each SNMPv3 user.

Procedure

1. In the navigation pane, expand **System**, and select **SNMP**.

   The SNMP page is displayed.
2. In the **SNMPv3 Users** panel, select the user, and click **Edit**.

   The Edit SNMPv3 User Info dialog box is displayed.
3. You can edit the following:
   - **User Name**
   - **Authentication Protocol** and **Authentication Password**
   - **Privacy Protocol** and **Privacy Password**
   - **Context**

   If you have set up the **Authentication Protocol** and **Privacy Protocol** for a user, you must re-enter the password when editing any of the details. You can enter a different password to change the password.
4. Click **Update**.

Adding and deleting an SNMP community

You can add SNMP communities to restrict access to the switch from the SNMP management stations. You must add community names that exist in the network.

The default community name is **public**. This default community is used when no community is added in the switch. After you add a new community name, the default community name **public** is not displayed in the SNMP Communities pane.

To add an SNMP community:

1. In the navigation pane, expand **System**, and select **SNMP**.

   The SNMP page is displayed.
2. In the **SNMP Communities** panel, click **Add**.

   The Add SNMP Community dialog box is displayed.
3. Enter a valid SNMP name.

   The name can contain a maximum of 32 characters without a space and must begin and end with an alphabet, a number, or an underscore.
4. Click **Add Community**.

To delete an SNMP community:

1. In the **SNMP Communities** panel, select the community name that you want to delete, and click **Delete**.

   A confirmation message is displayed.
2. Click **Delete Community**.

Adding and deleting an SNMP trap receiver

You can add trap receivers that can receive SNMPv1, SNMPv2c, and SNMPv3 traps or SNMPv2c and SNMPv3 inform messages.

To add an SNMP trap receiver:

1. In the navigation pane, expand **System**, and select **SNMP**.

   The SNMP page is displayed.
2. In the **Trap Receivers** panel, click **Add**.

   The Add Trap Host dialog box is displayed.
3. Configure the following parameters:
   - **Host**: A valid IPv4 or IPv6 address of the SNMP host.
   - **Type**: The type of SNMP message, trap or inform.
   - **Version**: The SNMP version, v1, v2c, or v3.
   - **User ID**: The user ID for authentication. The user ID is required only if the SNMP version is v3.
   - **Community**: The community name available in the switch. The default community name is **public**. The community name is not required when the SNMP version is v3.
   - **Port**: The SNMP port on which the host listens for the trap requests. The default port number is 162.
   - **VRF**: The VRF available on the switch.
4. Click **Add Host**.

To delete an SNMP trap receiver:

1. In the **Trap Receivers** panel, select the trap receiver that you want to delete, and click **Delete**.

   A confirmation message is displayed.
2. Click **Delete Host**.

Editing an SNMP trap receiver

Use this procedure to view and edit the SNMP trap receiver details. You can edit only the community that is added to the trap receiver.

Procedure

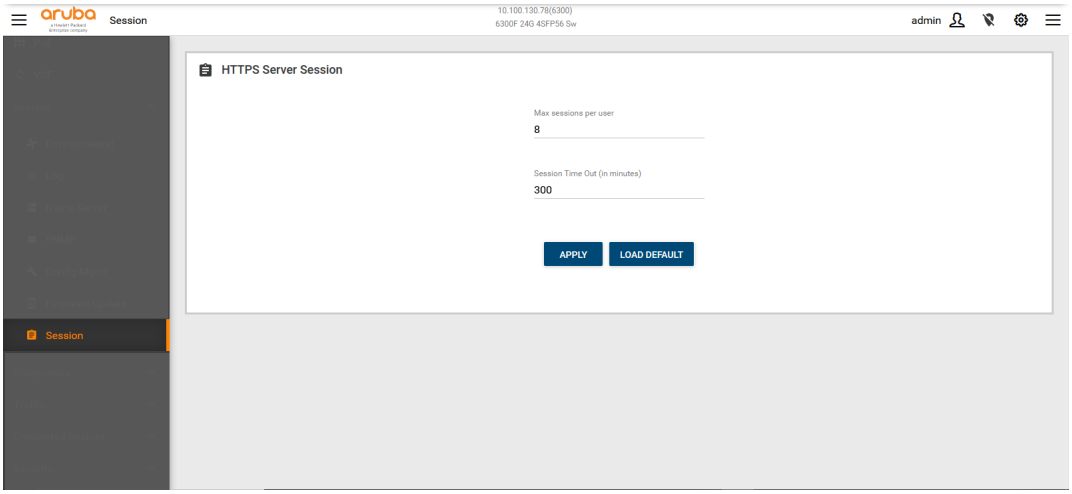
1. In the navigation pane, expand **System**, and select **SNMP**.

   The SNMP page is displayed.
2. In the **Trap Receivers** panel, select the trap receiver, and click **Edit**.

   The Edit Trap Host dialog box is displayed.
3. You can change the **Community**.
4. Click **Update**.

Session page

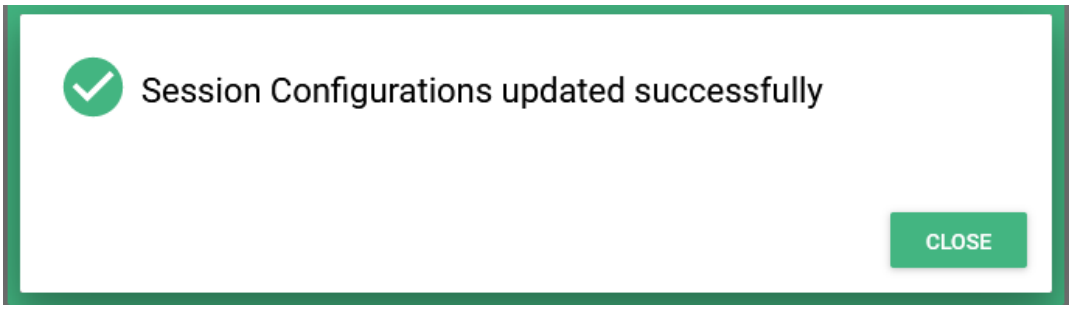
The **Session** page allows a way to configure values for the HTTPS server.



HTTPS Server Session panel

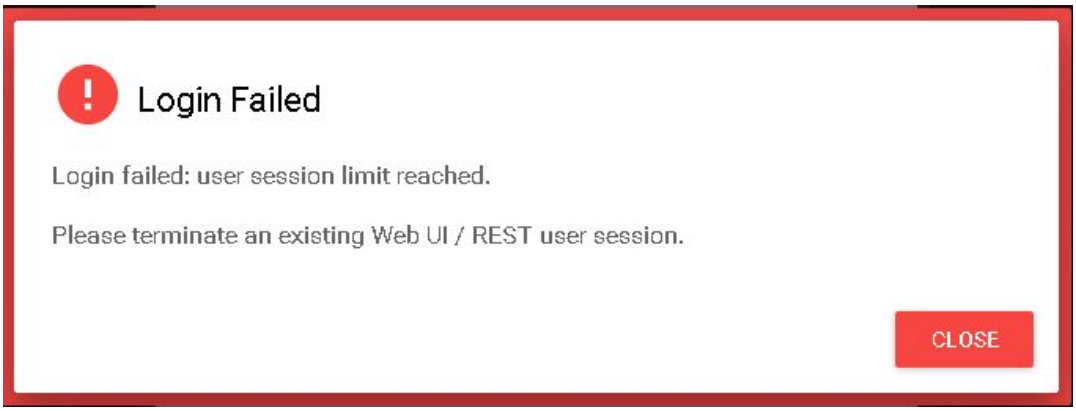
The **HTTPS Sever Session** panel allows the user to configure the max sessions per user and session idle timeout for the HTTPS server.

The **APPLY** button is used to configure the values provided by the user. The **LOAD DEFAULT** button configures default values for session parameters. The **APPLY** button is disabled on providing invalid values for the session parameters. On successful configuration of session parameters values, the following dialogue is displayed:



Max sessions

The functionality of maintaining the maximum number of sessions per user is handled by the REST module in the switch. The Web UI only provides configuration support. On attempting to establish a session beyond the configured max number of sessions, the following error dialogue is displayed:



Idle timer

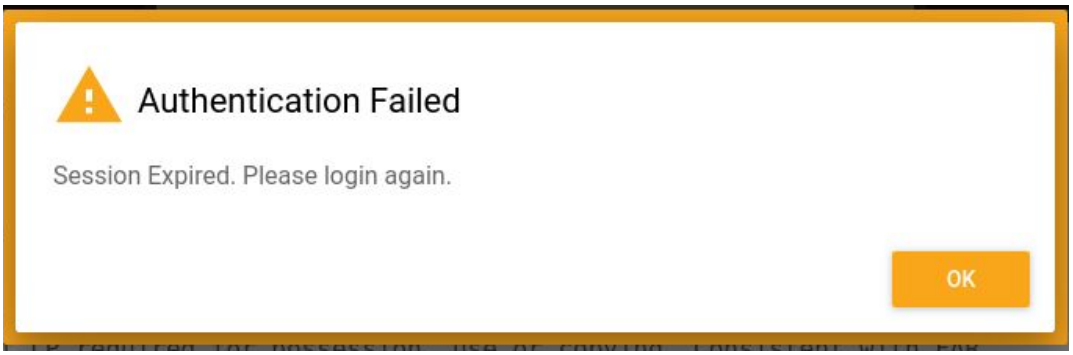
Web UI sessions are maintained by REST module and these Web UI sessions inactivity is monitored by REST deamon based on the RESTAPI request activity from each session. In Web UI implementation, many pages use periodic data polling (like every 10 secs) using the REST API to provide dynamic update of data. This causes the Web UI session to never timeout from the REST daemon perspective, because the REST API does not distinguish between the active polling API and the user-triggered REST API. Therefore, the REST Daemon will never timeout Web UI sessions even if the user is inactive. Because of this, the user activity idle timer is must be maintained by the Web UI and once the activity timer times out, the Web UI will automatically log out of the session.

A 10 second periodic timer is started on launching the Web UI. On timeout of this timer, a global *currSessTmr* counter is incremented. This counter is checked against the configured idle timer session timeout value. When the *currSessTmr* reaches the idle timeout timer value, a logout event is triggered, and the current session is terminated.

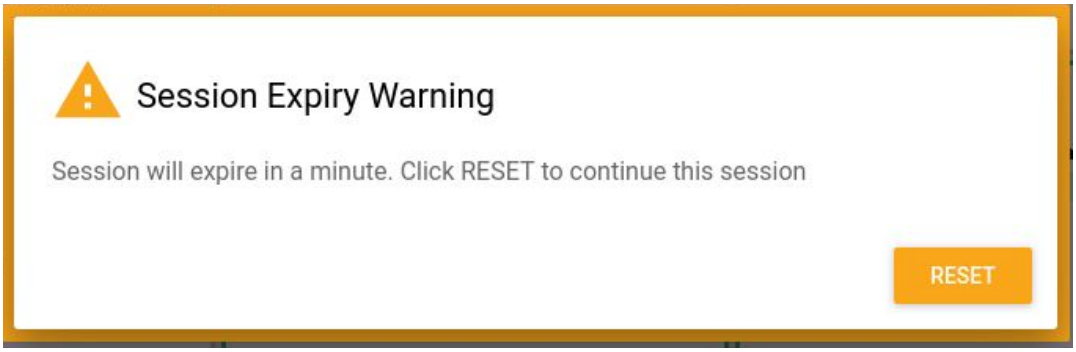
The idle timeout counter *currSessTmr* is reset on any user activity which is detected using the *addEventListener* function.

The configurable value for idle Timer is 0 to 480 (in minutes), where 0 disables the timer. On configuration of a value of zero, the 10 second timer is stopped and on any non-zero value, the timer is restarted.

When there is no user activity in the Web UI for the configured session idle timeout, the session is logged off and the following dialogue is displayed. The user needs to login again to access Web UI.



A warning message is displayed when the idle session timer has one-minute before expiring.



The user can reset the timer and continue the session by clicking the **RESET** button. If not reset, the session expires in one minute from the warning message display.

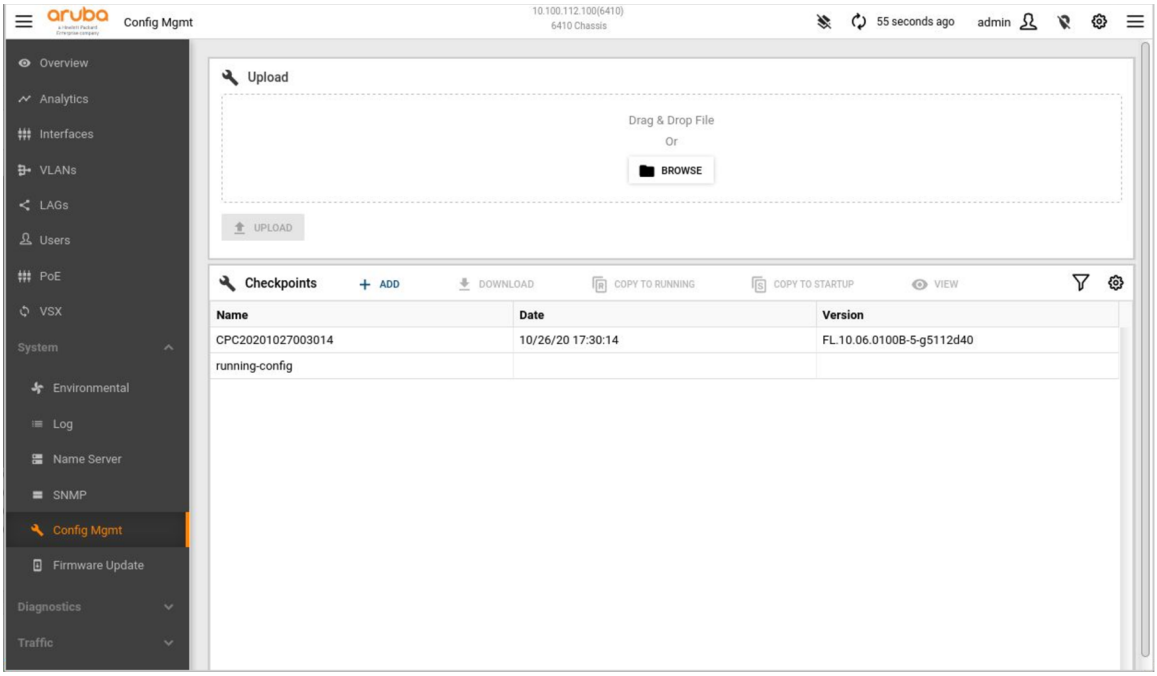
Config Mgmt page

From the Config Mgmt page you can:

- Upload or download configurations to or from the Running or Startup configuration.
- Create a configuration checkpoint.
- Download running, startup, and checkpoint configurations
- Copy from or to various configurations: running to startup, running to checkpoint, checkpoint to startup, checkpoint to running, startup to running.

Uploads and downloads are performed through the REST interface.

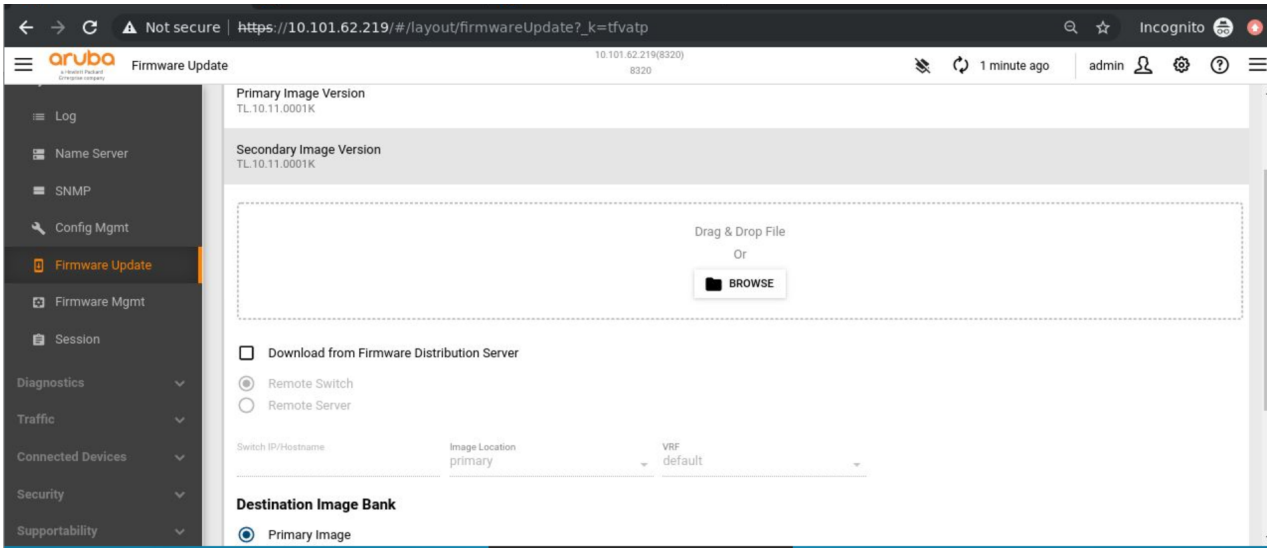
Figure 1 *Config Mgmt (configuration management) page*



Firmware Update page

From the Firmware Update page, you can see the current, primary, and secondary firmware versions and you can upload firmware files.

Figure 1 *Firmware update showing image versions*



Uploads are performed through the REST interface.

After the update starts it cannot be cancelled, however users can access other functionalities by opening a new browser tab for the same session.

Prior to updating, a message is displayed: `Are you sure you want to update the primary/secondary image?`

After the firmware upload is completed, a new dialog box is displayed that contains the message: `New firmware has been successfully uploaded. Verifying and writing system firmware...`

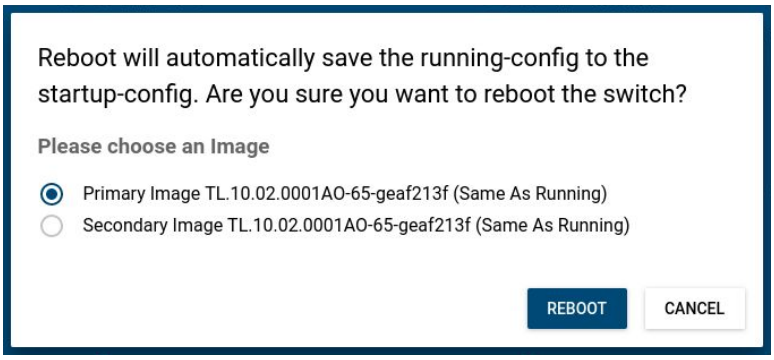
You may need to press **Reboot** on the page or select the Reboot item in the top right System menu for the image to take effect.

Selecting **Reboot** reboots the switch.

After you select **Reboot**, you cannot cancel the request.

After selecting **Reboot**, you will be prompted to verify that you want to reboot the switch and to choose an image to use when rebooting.

Figure 2 *Reboot confirmation dialog box*



Firmware site distribution

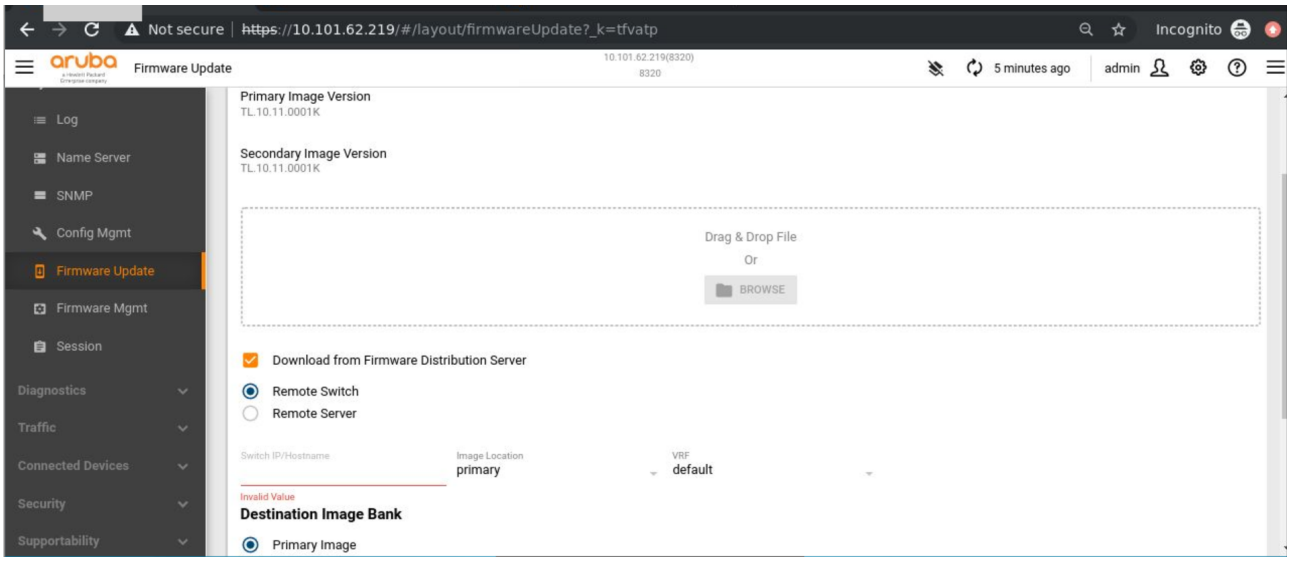
Firmware site distribution is a feature in which a switch can upgrade its firmware by downloading image from another switch in the network. It enables switches to download firmware from switch or remote server rather than all switches requesting multiple downloads from a remote location. This reduces the traffic to external networks, reduces network overhead, and speeds up the upgrade process.

The WebUI provides support for this feature through the **Firmware Update** page under the **System** group in the Navigation pane. Switches may download their firmware from a remote switch or from any HTTP server.

Selecting the **Download from Firmware Distribution Server** reveals additional options:

- Remote Switch
- Remote Server

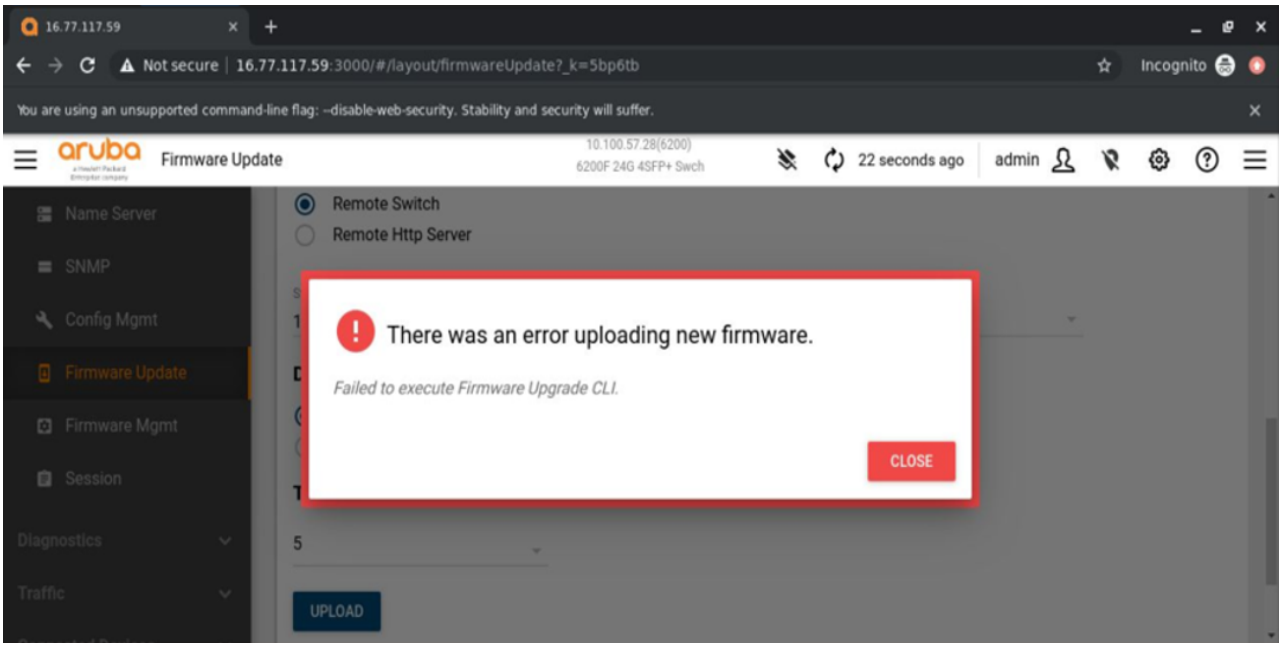
Figure 3 *Enabling the Firmware Distribution Server feature*



In the event that downloading firmware fails, the WebUI will display an error message sent by the REST module.

Only two switch clients can simultaneously install firmware from a remote switch. If the remote switch receives a request from a third client while currently serving two others, then firmware installation will fail for the 3rd client.

Figure 4 *Firmware download error message*

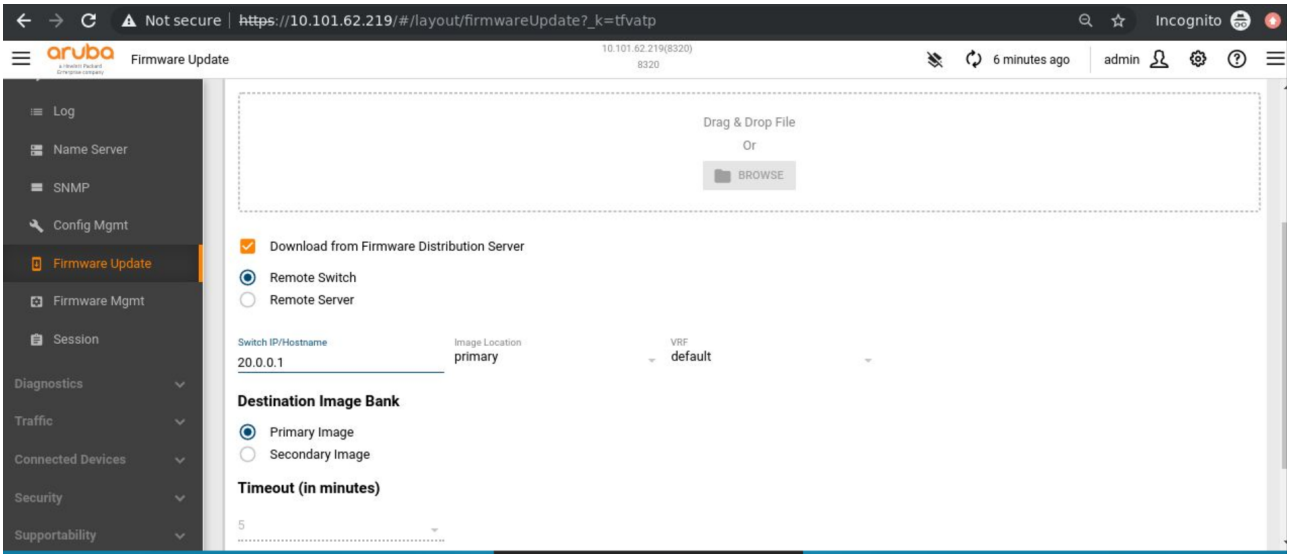


Downloading firmware from a remote switch

The following values are required to download firmware from a remote switch:

Value	Description
Switch IP/host name	IP address or hostname of the switch which has the firmware to be downloaded in its image bank.
Image location	Image bank in the remote switch. Firmware from either the primary or secondary bank can be downloaded.
VRF	Mgmt, Default, or any user-created VRF to reach the remote switch.

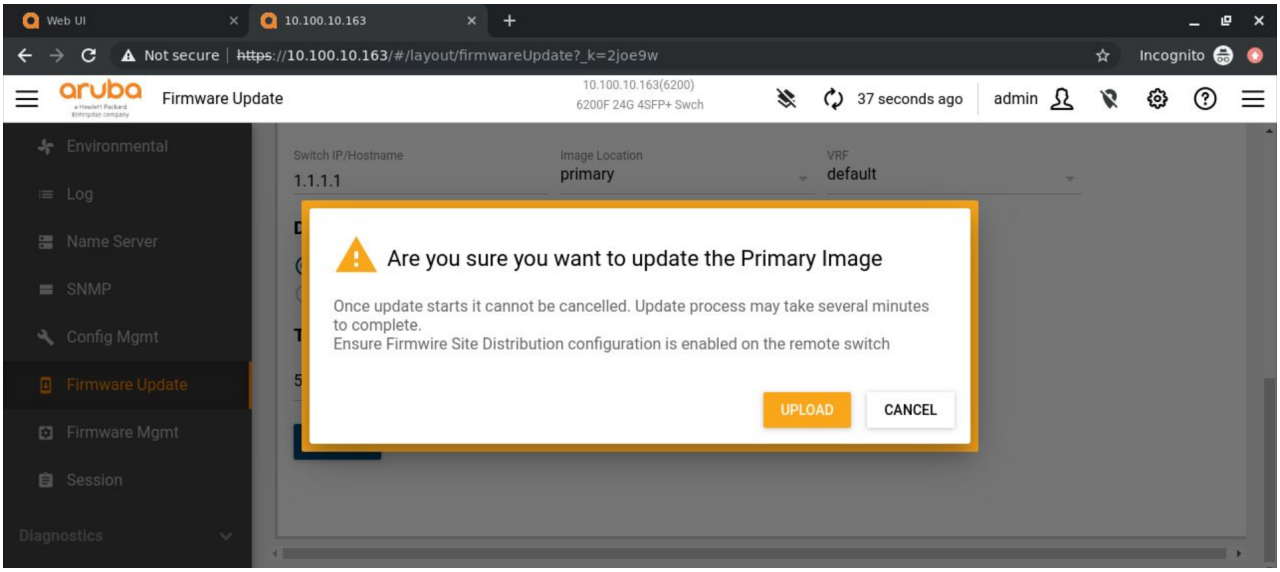
Figure 5 *Example of downloading an image from a remote switch*



In the example shown above the firmware is downloaded from primary bank of switch 20.0.0.1 using default VRF.

When trying to download firmware from another switch, the WebUI provides a warning message to user to ensure the configuration is done on the remote switch.

Figure 6 *WebUI warning before downloading firmware from a remote switch*

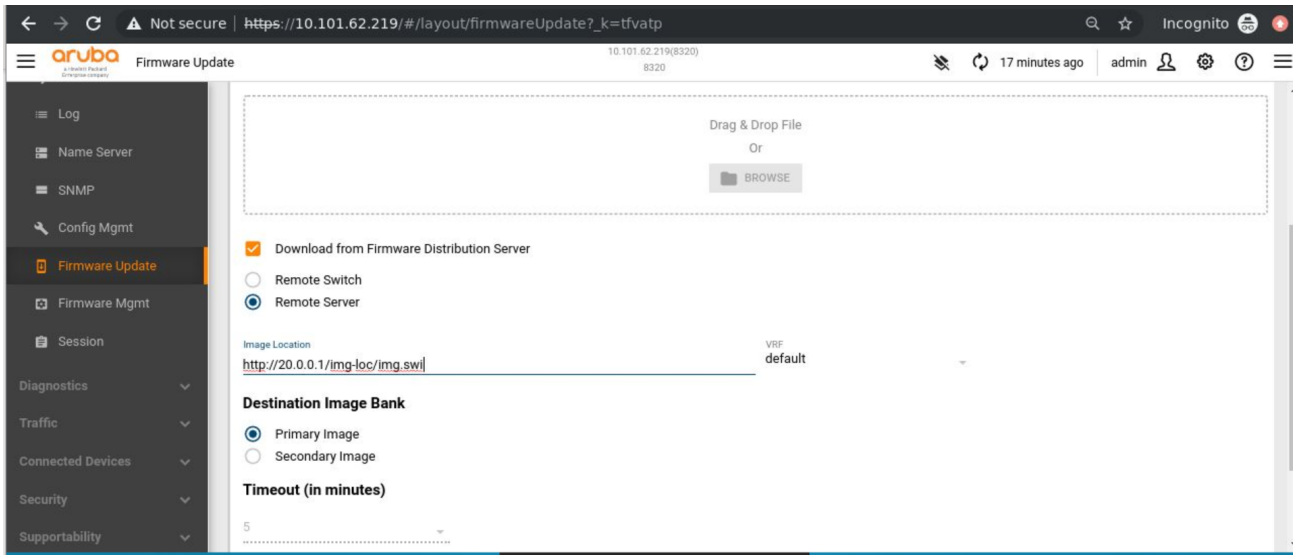


Downloading firmware from a remote HTTP server

The following values are required to download firmware from a remote HTTP server:

Value	Description
Image location	The complete URL of the image location in the remote HTTP server, for example, http://www.example.com/images/FL_10_06_0100AM.swi?merchantId=ACTIVATE_DROPBOX
VRF	VRF to reach the HTTP server.

Figure 7 *Example of downloading an image from a remote server*



To upgrade using firmware from another switch, the Firmware Site Distribution feature must be enabled in the remote switch. Please refer to the Firmware Mgmt page section for additional information.

Firmware Mgmt page

The Firmware Mgmt page contains the mechanism to enable the **Firmware Site Distribution** feature. This feature must enabled on a remote switch in order to allow it to share its firmware image(s) with other switches in your network and can be enable either via CLI or WebUI.

Enabling firmware site distribution using the CLI

Firmware site distribution can be enabled and verifies in the CLI using the following commands:

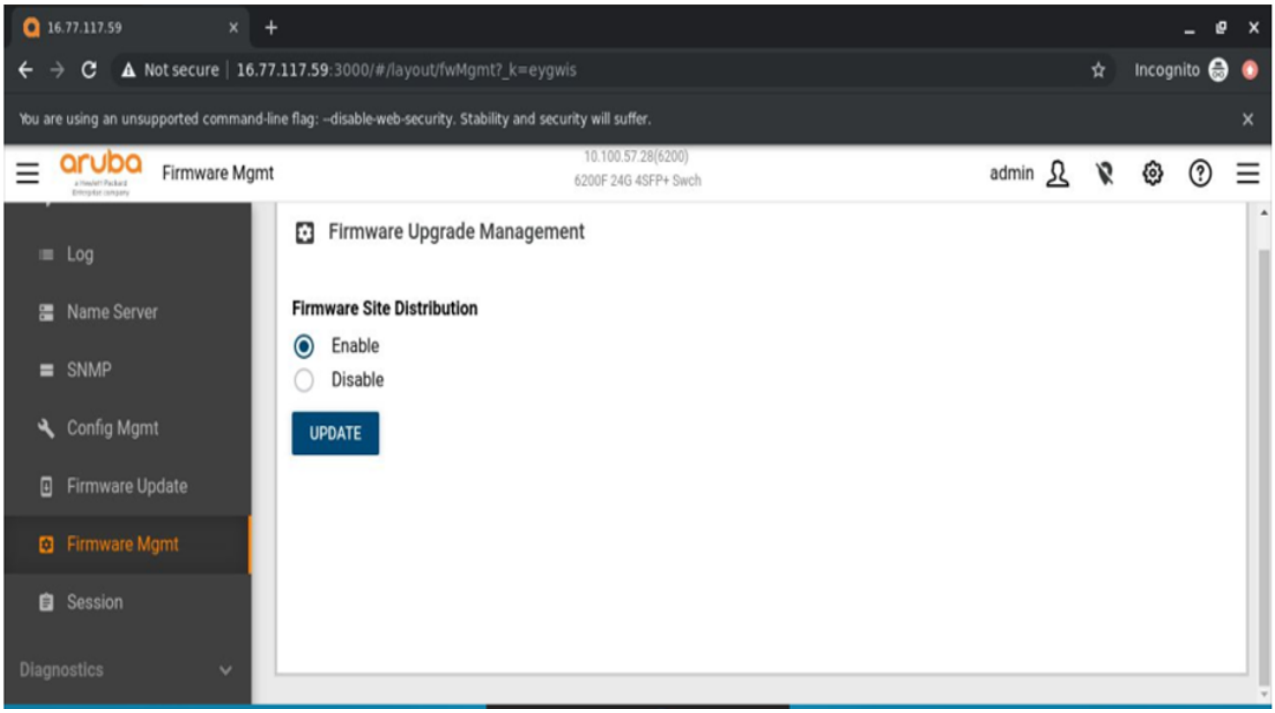
```
switch(config)# show https-server rest firmware-site-distribution
Firmware Site Distribution Configuration
----------------------------
 Status        : disabled

switch(config)# https-server rest firmware-site-distribution
switch(config)# show https-server rest firmware-site-distribution
Firmware Site Distribution Configuration
----------------------------
 Status        : enabled
```

Enabling firmware site distribution using the WebUI

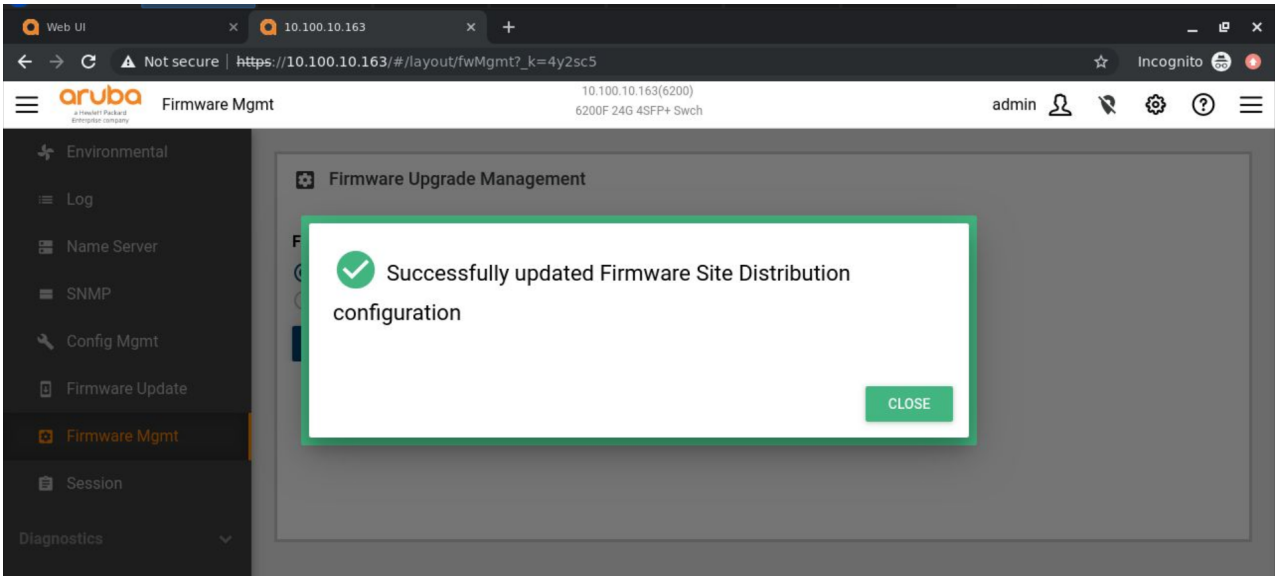
The Firmware Mgmt page also allows you to enable or disable the firmware site distribution feature and can be accessed through the following path: **Navigation pane > System > Firmware Mgmt**.

Figure 1 *Enabling firmware site distribution using the WebUI*



When the image has been successfully downloaded the system will display a confirmation message.

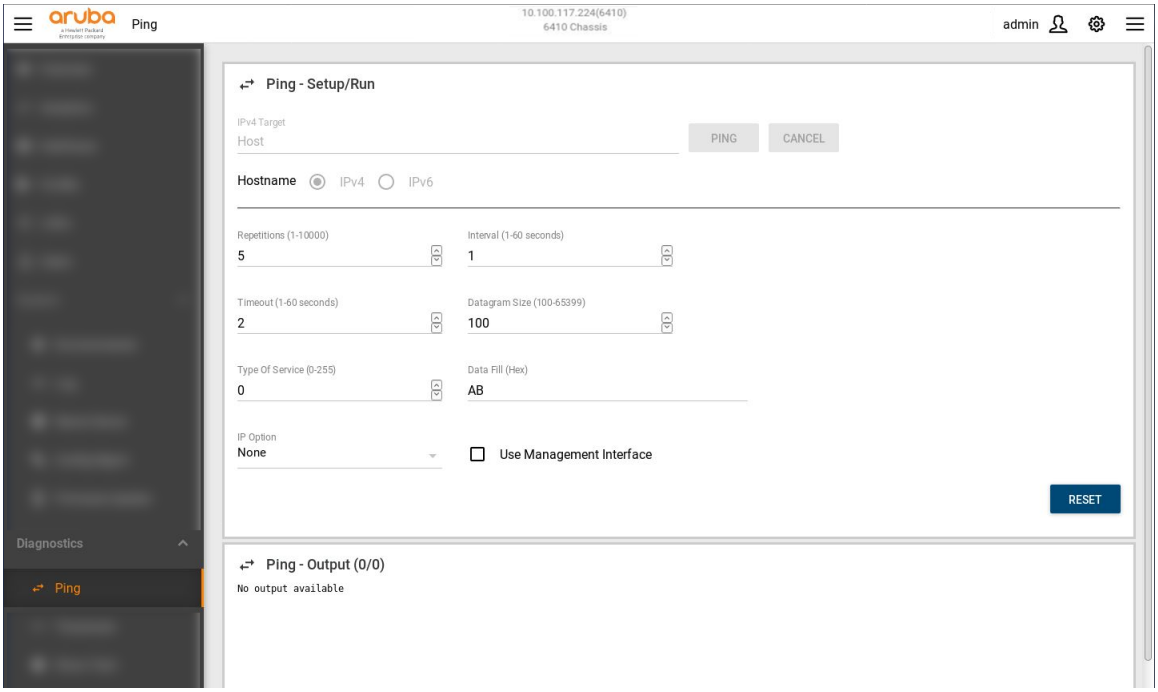
Figure 2 *WebUI firmware system update confirmation message*



Ping page

From the Ping page, you can run the `ping` command to the specified target hostname and view the output. Click **Ping** to run the command or **Cancel**.

Figure 1 *Ping page*



You can set the following parameters on the `ping` command:

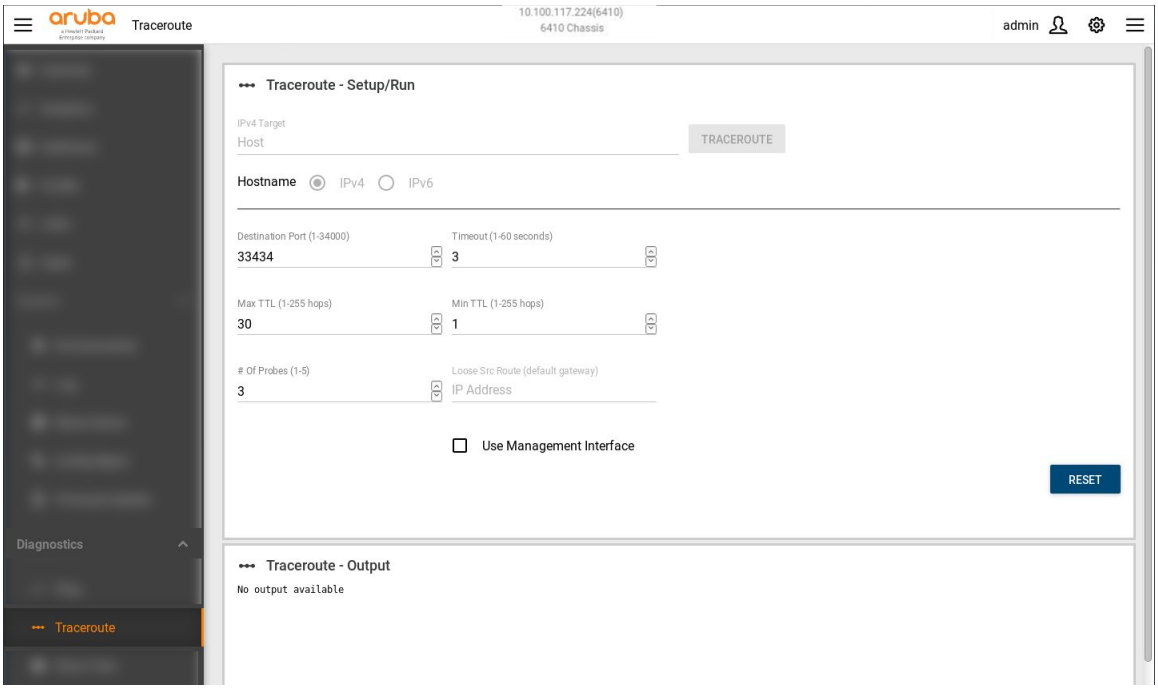
- Repetition: Specify the number of pings sent (1-10,000).
- Interval: Specify the interval between successive ping requests (1-60).
- Timeout: Specify the Ping Timeout in seconds (1-60).
- Datagram-Size: Specify the size of ping datagram (100 - 65,399).
- Type of Service (TOS): Specify IP TOS to be used in ping request (0 - 255).
- Data Fill: Specify the ping packet data pattern in hexadecimal digits.
- IP-Option: Specify an IP option to be used in ping packet.
- Use Management Interface: Specify the use of the management interface (check box).

Click **Reset** to reset options to the default.

Traceroute page

From the Traceroute page, you can run the `traceroute` command to the specified target hostname and view the output. Click **Traceroute** to run the command.

Figure 1 *Traceroute page*



You can set the following parameters on the `traceroute` command:

- Destination Port: Specify the destination port (1 - 34000).
- timeout: Specify the traceroute timeout in seconds (1-60).
- maxttl: Specify the maximum number of hops to reach the destination (1 - 255).
- minttl: Specify minimum number of hops to reach the destination (1 - 255).
- probes: Specify the number of probe packets per hop to send (1 - 5).
- Loose src Route: Specify routing information to be used by the gateways.
- Use Management Interface: Specify the use of the management interface (check box).

Click **Reset** to reset options to the default.

Show Tech page

From the Show Tech page, you can run the `showtech` command. Administrator rights are required.

Figure 1 *Show Tech page*

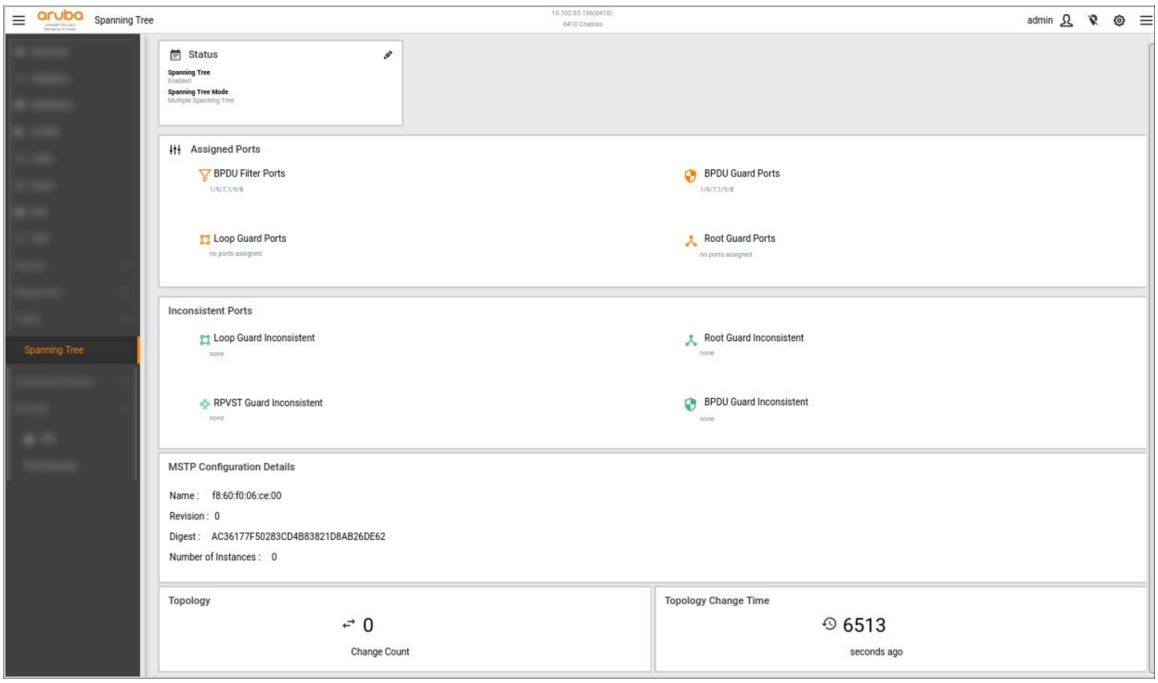
Click **Generate**, to start generating the report on the switch.

Click **Export** to download the `showtech` file locally. The exported file is in simple text format, the same as with the CLI output.

Spanning Tree page

The Spanning Tree page displays the spanning tree configuration details of the switch. The Spanning Tree Protocol (STP) eliminates Layer 2 loops in networks, by selectively blocking some ports and allowing other ports to forward traffic.

Figure 1 *Spanning Tree page*



Status panel

The **Status** panel shows information about the spanning tree configuration—whether spanning tree is enabled or disabled and the spanning tree mode that is selected.

You can enable spanning tree with Multiple Spanning Tree (MST) or Rapid Per-Vlan Spanning Tree (Rapid PVST) mode.

In the Multiple Spanning Tree mode, the Spanning Tree page displays additional details like the assigned ports, MSTP configuration details, the number of times the topology was changed, and the time since the topology changed.

In the Rapid Per-Vlan Spanning Tree mode, the Spanning Tree page displays only the details of the assigned ports. The Rapid Per-Vlan Spanning Tree mode enables a separate spanning tree in each VLAN, including the default VLAN.

Assigned Ports panel

The **Assigned Ports** panel shows the details of the ports based on the ports added in the spanning tree configuration. For example, if some ports are set as BPDU Filter or Guard Ports, then the port numbers are displayed in the **member/slot/port** notation.

Inconsistent Ports panel

The **Inconsistent Ports** panel shows the details of the ports that are in an inconsistent STP state. Inconsistent state occurs when the ports on both ends of a point-to-point link are untagged members of different VLANs or when the ports have different configurations on both end. For example, if one end is configured as trunk and the other end is configured as an access port.

MSTP Configuration Details panel

The **MSTP Configuration Details** panel shows the name of the region, the revision number, and a digest of the MST VLANs-to-instance mapping from the switch configuration.

Topology panel

The **Topology** panel shows the number of times the topology changed.

Topology Change Time panel

The **Topology Change Time** panel shows the time since the topology changed.

Editing the spanning tree settings

To edit the spanning tree settings:

1. In the navigation pane, expand **Traffic**, and select **Spanning Tree**.

   The Spanning Tree page is displayed.

2. In the **Status** panel, click .

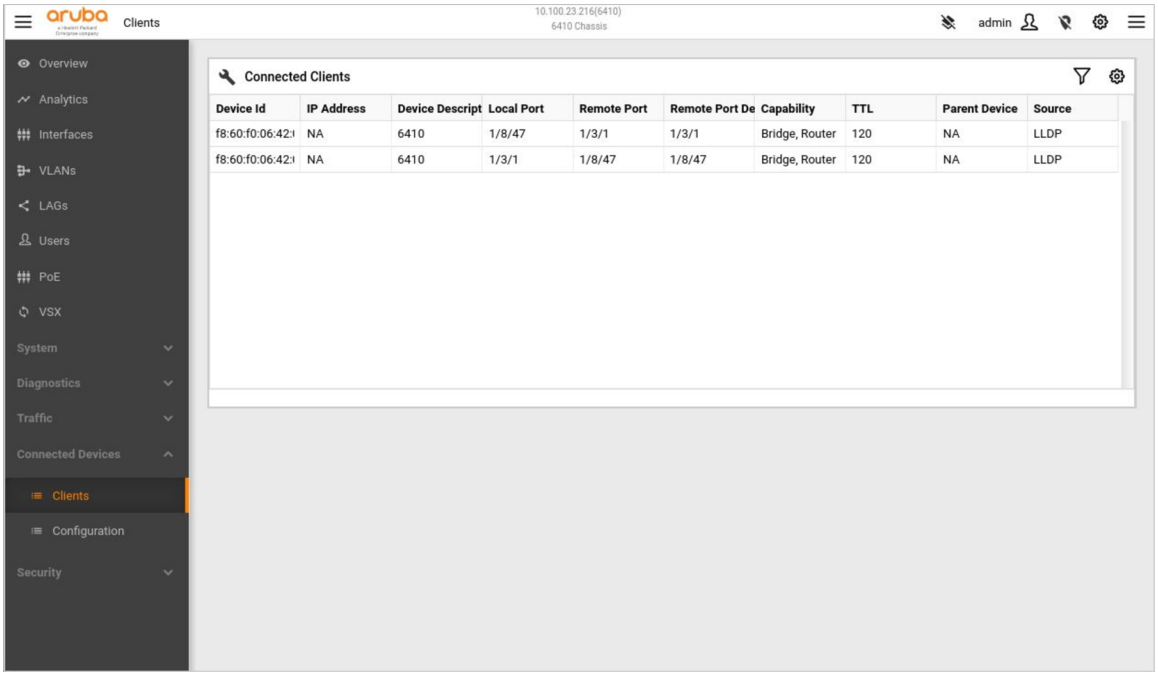
   The Edit Spanning Tree dialog box is displayed.

3. Configure the following parameters:
   - **Status**: Option to enable or disable spanning tree.
   - **Mode**: Option to select the Multiple Spanning Tree or Rapid Per-Vlan Spanning Tree mode.
   - **Config Name**: A name for the Multiple Spanning Tree configuration. This field is displayed only if the Multiple Spanning Tree mode is selected.
   - **Config Revision**: A revision number of the Multiple Spanning Tree configuration. This field is displayed only if the Multiple Spanning Tree mode is selected.
   - **Priority**: A priority for the spanning tree configuration.
4. Click **OK**.

Connected Clients page

The Connected Clients page displays details of the devices connected to the switch.

Figure 1 *Connected Devices page*



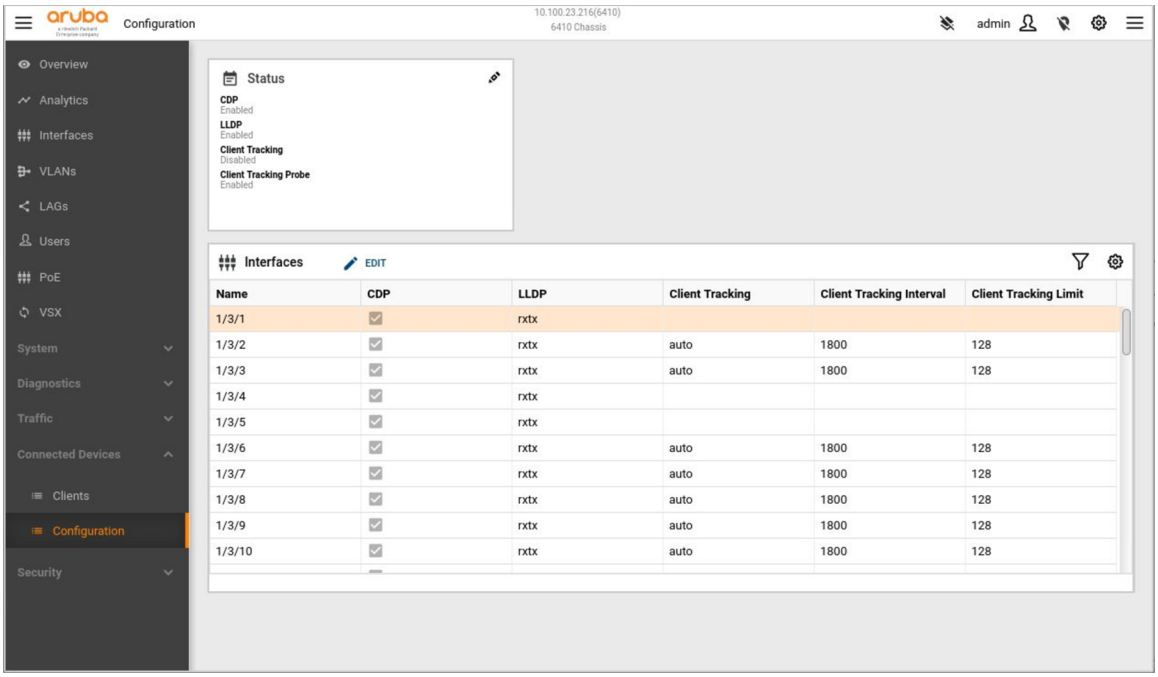
Connected Clients panel

The **Connected Clients** panel displays the device ID, IP address, device name, local and remote ports, capability, TTL time, parent device, and source details.

Connected Devices Configuration page

The Connected Devices Configuration page shows whether Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and client tracking are enabled or disabled at the switch and interface level. You can configure these settings to discover and share information about the connected network devices at the switch and interface level.

Figure 1 *Connected Devices page*



Status panel

The **Status** panel displays the status of CDP, LLDP, client tracking, and client tracking probe at the switch level. You can edit and change the configuration.

Interfaces panel

The **Interfaces** panel displays the port name, CDP status, LLDP type, client tracking status, client tracking interval, and client tracking limit details for each active interface. You can edit and change the configuration.

Editing connected devices at the switch level

Use this procedure to view and edit the connection statuses of devices connected to the different interfaces. Enabling or disabling settings at the switch level does not change the configuration on the interface.

1. In the navigation pane, expand **Connected Devices**, and select **Configuration**.

   The Configuration page is displayed.

2. In the **Status** panel, click .

   The Configuration dialog box is displayed.

3. You can configure the following parameters:
   - **CDP**: Enables or disables CDP support globally on all active interfaces. By default, CDP is enabled.
   - **LLDP**: Enables or disables LLDP support globally on all active interfaces. By default, LLDP is enabled.
   - **Client Tracking**: Enables or disables client tracking on all active interfaces.
   - **Client Tracking Probe**: Enables or disables client tracking probe on all active interfaces.
4. Click **OK**.

Editing connected devices configuration at interface level

Use this procedure to view and edit interface configuration.

1. In the navigation pane, expand **Connected Devices**, and select **Configuration**.

   The Configuration page is displayed.
2. In the **Interfaces** panel, select an interface, and click **Edit**.

   The Interface Configuration dialog box is displayed.
3. Configure the following parameters:
   - **CDP**: Select the checkbox to enable CDP. By default, CDP is enabled.
   - **LLDP**: Select one of the following values:
     - **rx**: Receive only. This setting enables a port to receive and read LLDP packets from LLDP neighbors and to store the packet data in the switch's MIB. However, the port does not transmit outbound LLDP packets. This prevents LLDP neighbors from learning about the switch through that port.
     - **tx**: Transmit only. This setting enables a port to transmit LLDP packets that can be read by LLDP neighbors. However, the port drops inbound LLDP packets from LLDP neighbors without reading them. This prevents the switch from learning about LLDP neighbors on that port.
     - **rxtx**: Transmit and receive. This is the default setting on all ports. It enables a given port to both transmit and receive LLDP packets and to store the data from received (inbound) LLDP packets in the switch's MIB.
     - **off**: This setting disables LLDP packet transmissions and reception on a port. In this state, the switch does not use the port for either learning about LLDP neighbors or informing LLDP neighbors of its presence.
   - **Client Tracking**: Select **auto**, **disable**, or **enable**. By default, **auto** is selected.
   - **Client Tracking Interval**: Enter a value from 60 to 28000. The default value is 1800.
   - **Client Tracking Limit**: Enter a value from 1 to 4096. The default value is 128.

   Client Tracking, **Client Tracking Interval**, and **Client Tracking Limit** parameters cannot be configured on interfaces that are associated with lags.
4. Click **OK**.

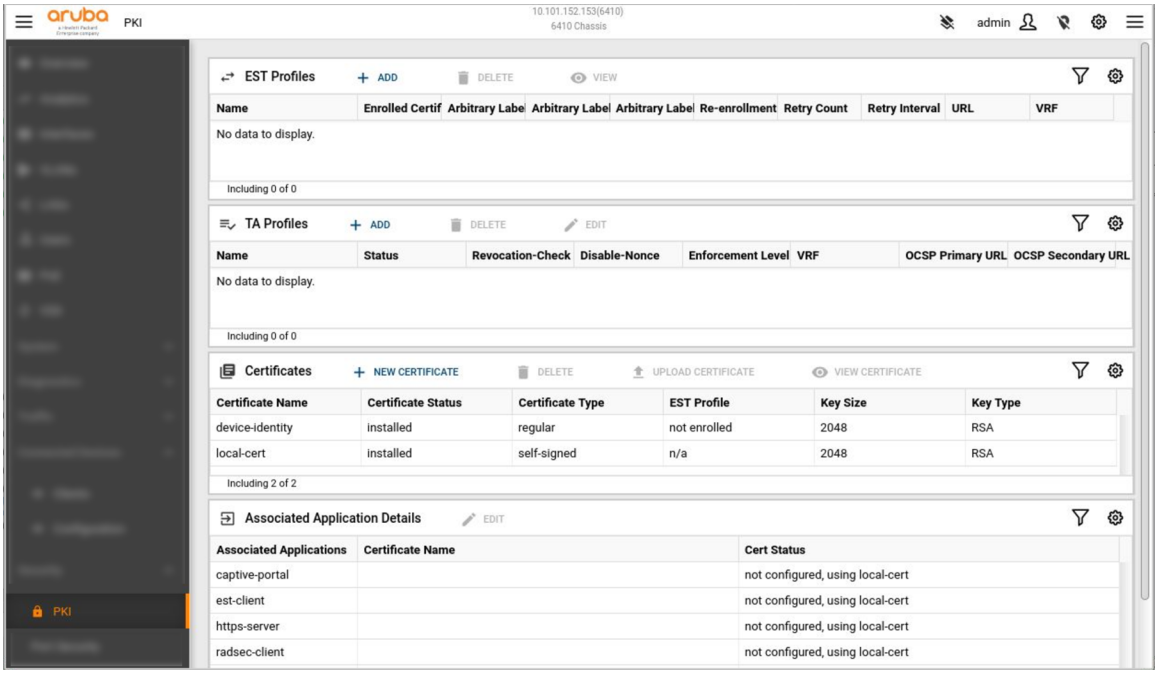
PKI page

Public Key Infrastructure (PKI) capability on the switch provides digital certificates to authenticate network entities. This page enables you to configure and manage digital certificates on the switch. The

switch uses certificates to validate SSH clients when acting as an SSH server and when communicating with syslog servers while TLS encryption is used.

Each entity in the PKI has their identity validated by a certificate authority (CA). The CA issues a digital certificate as part of enrolling each entity into the PKI. This digital certificate is used by the replying parties (for example, network connection peers) to set up secure communication. Based on the information present in the certificate of the sender, the receiving entity can validate the authenticity of the sender and subsequently establish a secure communication channel. For more information about PKI, see the *AOS-CX Security Guide*.

Figure 1 *WebUI Overview Dashboard*



EST Profiles panel

The **EST Profiles** panel displays the details of the EST profiles added to the switch. Enrollment over Secure Transport (EST) enhances the switch PKI infrastructure with a simpler, scalable, and more secure method of certificate provisioning, re-enrollment, and renewal.

TA Profiles panel

The **TA Profiles** panel displays information and status of TA profiles added to the switch. A Trust Anchor (TA) defines certificate-specific operations, such as enrollment and validations. Each TA profile stores the certificate for a trusted CA.

Certificates panel

The **Certificates** panel displays details about the digital certificates that can be used for applications in the switch. Certificates help secure digital transactions by enabling the end parties to validate each other's identity. Digital certificates are issued by a CA and are composed of an encoded string of characters (usually stored in a file).

Associated Application Details panel

The **Associated Application Details** panel displays the features (applications) on the switch to which you can associate certificates. The panel also displays the associated certificate name and status. By default, all features are associated with the default, self-signed certificate **local-cert**. This certificate is created by the switch the first time it starts.

Adding and deleting an EST Profile

To add an EST profile:

1. In the navigation pane, expand **Security**, and select **PKI**.
   The PKI page is displayed.
2. In the **EST Profiles** panel, click **Add**.
   The New EST Profile Info dialog box is displayed.
3. Enter a profile name for the EST profile.
4. Configure the following optional parameters:
   - **Arbitrary Label**: Enter an arbitrary label for the EST URI to distinguish it from the other EST profiles running on the EST server. The arbitrary label can contain alphabets, numbers, and special characters without a space. Only dot (.), underscore (_), tilde (~), colon (:), slash (/), and hyphen (-) are allowed as special characters.
   - **Arbitrary Label Enrollment**: Enter an arbitrary enrollment label for EST URI.
   - **Arbitrary Label Re-enrollment**: Enter an arbitrary re-enrollment label for EST URI.
   - **Re-enrollment Lead Time**: Enter the lead time to re-enroll a certificate before it expires. The time should be from 0 to 30 days. The default value is 2 days.
   - **Retry Count**: Enter the number of times to retry to enroll a certificate. The value should be from 0 to 32. The default value is 3 retries.
   - **Retry Interval**: Enter the interval after which the switch can retry to enroll a certificate. The value should be from 30 to 600 seconds. The default value is 30 seconds.
   - **URL**: Enter the URL for the EST server.
   - **Username**: Enter the username to access the EST server. The username can contain alphabets, numbers, and special characters without a space.
   - **Password**: Enter the password for the username in the plain-text format. The password can contain alphabets, numbers, and special characters without a space.
   - **VRF**: Select the VFR that the switch uses to communicate with the EST server. VRF **mgmt** is used by default.
5. Click **OK**.

To delete an EST profile:

1. In the **EST Profiles** panel, select the EST profile, and click **Delete**.
   A confirmation message is displayed.
2. Click **Delete**.

Viewing an EST Profile

To view the details of an EST profile:

1. In the navigation pane, expand **Security**, and select **PKI**.
   The PKI page is displayed.
2. In the **EST Profiles** panel, select the EST profile, and click **View**.
   The details are displayed in a dialog box.
3. Click **OK**.

Adding and deleting a TA Profile

To add a TA profile:

1. In the navigation pane, expand **Security**, and select **PKI**.
   The PKI page is displayed.
2. In the **TA Profiles** panel, click **Add**.
   The Add TA Profile dialog box is displayed.
3. Click **Browse** and select a certificate to associate with the TA profile. The certificate file must be in **.pem** format. The switch can import Privacy-Enhanced Mail (PEM) encoded ITU-T X.509 v3 certificates.

   The certificate with PEM data must be delimited with the following lines:

   ```
   -----BEGIN CERTIFICATE-----
   -----END CERTIFICATE-----
   ```

   For example:

   ```
   -----BEGIN CERTIFICATE-----
   MIIDsDCCApgCCQDJotuPPj9GCDANBgkqhkiG9w0BAQsAADCBqzELMAkGA
   UEBhVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExEDAOBgNVBAcBM1JvY2tsa
   W4xDDAKBgBAoMA0hQTjEVMBMGA1UECwwMSFBOUm9zZXZpbGxlMSokwAYD
   ...
   MioDy0096DvSMPsnOaI+jnZ3AozN8y+nLgotXUsg36pO/Ncc51oQhyUdc
   AbgA1rzSLgyTnpXZKumvlaoTk3pzrIf7m5V103GTbgHGSFCzgO6QWxVxu
   9d7ju1o59SaOIT7JSsYI5LsLpVz9ZqS599rj/lLoH+rLNlRDVXpS+J51U
   -----END CERTIFICATE-----
   ```

4. Enter a profile name for the TA profile. The profile name can have a maximum of 32 characters.
5. Configure the following optional parameters:
   - **Revocation-Check**: Select the **OCSP** checkbox to determining the revocation status of the certificate. Optionally, enter the primary and secondary OCSP responder URLs that the TA profile should use to verify the revocation status.
     Selecting the checkbox enables certificate revocation checking for the TA profile using the online certificate status protocol (OCSP). If no OCSP responder URLs are defined for a TA profile (default setting), then the OCSP responder URL in the peer certificate is used for revocation status checking. (The OCSP responder URL is contained in a certificate's Authority Information Access field, which is an X.509 v3 certificate extension.)
   - **OCSP Disable-Nounce**: Select the **Disable-Nounce** checkbox to exclude nonce from OCSP requests.
     A nonce is a unique identifier that an OCSP client inserts in an OCSP request and expects the OCSP responder to include it in the corresponding OCSP response. The nonce mechanism helps prevent replay attacks in which a malicious player attempts to masquerade as the OCSP responder. Although the nonce is included by default, it can be excluded. Some OCSP responders choose to not support the use of the nonce due to performance considerations
   - **OCSP Enforcement Level**: Select either **Strict** or **Optional** to enforce OCSP check on certificates. Strict enforcement is enabled by default.

- **Strict**: The certificate is accepted only if all possible checking (including validation failures, software system errors, configuration errors, transactional errors) is successful.
- **Optional**: The certificate is accepted unless one or more of the following validation errors occur: Response signature is invalid, nonce in response mismatch, or certificate is revoked, when revocation checking is possible. If revocation check is not possible, the certificate is still accepted if there are no other validation errors.

- **OCSP VRF**: Select the VRF that the switch uses to communicate with OCSP responders for OCSP checking. VRF **mgmt** is used by default.

6. Click **OK**.

To delete a TA profile:

1. In the **TA Profiles** panel, select the TA profile, and click **Delete**.
   A confirmation message is displayed.
2. Click **Delete**.

Editing a TA Profile

To edit a TA profile:

1. In the navigation pane, expand **Security**, and select **PKI**.
   The PKI page is displayed.
2. In the **TA Profiles** panel, click **Edit**.
   The Edit TA Profile dialog box is displayed.
3. Configure the following optional parameters:
   - **Revocation-Check**: Select or clear the **OCSP** checkbox.
   - **OCSP Disable-Nounce**: Select or clear the **OCSP Disable-Nounce** checkbox.
   - **OCSP Enforcement Level**: Select either **Strict** or **Optional** to enforce OCSP check on certificates.
   - **OCSP VRF**: Select the VRF that the switch uses to communicate with OCSP responders for OCSP checking.
4. Click **OK**.

Adding and deleting a certificate

To add a certificate:

1. In the navigation pane, expand **Security**, and select **PKI**.
   The PKI page is displayed.
2. In the **Certificates** panel, click **New Certificate**.
   The New Certificate Info dialog box is displayed.
3. In the **Certificate Name** field, enter a name for the certificate.
   The certificate name can contain lowercase alphanumeric, dot, hyphen, and underscore characters. The **device-identity** and **local-cert** certificates are added by default.
4. Configure the following optional parameters:
   - **Certificate Type**: Select either **regular** or **self-signed** from the drop-down. Regular certificates are signed by a CA. Self-signed certificates are signed by the switch or the user who is using the certificate and not signed by a CA.

- **EST Profile**: Select the EST profile to associate with the certificate. This field is displayed only for the **regular** certificate type.
- **Key Type**: Select either **RSA** or **ECDSA** from the drop-down for the encryption key type. The default type is RSA.
- **Key Size**: Select the key size from the drop-down for the key type selected.

RSA key type has longer key size with values: 2048, 3072, and 4096 bits. The default size for RSA is 2048. The ECDSA key type has shorter key size with values: 256, 381, and 521 bits. The default size for ECDSA is 256.

5. In the **Common Name** field, enter the IP address or domain name associated with the switch.

   Your web browser might warn you if this field does not match the URL entered into the web browser when accessing the switch.
6. Configure the following optional parameters:
   - **Org Unit**: Enter the name of the sub-entity (for example, the department) where the switch is used.
   - **Org Name**: Enter the name of the entity (for example, the company) where the switch is used.
   - **State**: Enter the name of the state where the switch is used.
   - **Locality**: Enter the name of the city where the switch is used.
7. In the **Country** field, enter the country where the switch is used.

   You must enter only two letters in uppercase for the country name, for example, US for the United States.
8. Click **OK**.

To delete a certificate:

1. In the **Certificates** pane, select the certificate, and click **Delete**.

   A confirmation message is displayed.
2. Click **Delete**.

You cannot delete the default **device-identity** and **local-cert** certificates.

Uploading a certificate

You can upload a certificate only for regular certificates that are in a **csr_pending** certificate status. You must upload a certificate to send a certificate signing request (CSR) for the regular certificate that you add in the switch. You cannot upload a certificate for the **device-identity** regular certificate and if the certificate status is **installed**.

The signed certificate that you upload must contain PEM data in the following chain format:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

For example:

```
-----BEGIN CERTIFICATE-----
```

```
MIIDsDCCApgCCQDJotuPPj9GCDANBgkqhkiG9w0BAQsAADCBqzELMAkGA
UEBhVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExEDAOBgNVBAcBM1JvY2tsa
W4xDDAKBgBAoMA0hQTjEVMBMGA1UECwwMSFBOUm9zZXZpbGxlMSokwAYD
...
MioDy0096DvSMPsnOaI+jnZ3AozN8y+nLgotXUsg36pO/Ncc51oQhyUdc
AbgA1rzSLgyTnpXZKumvlaoTk3pzrIf7m5V103GTbgHGSFCzgO6QWxVxu
9d7ju1o59SaOIT7JSsYI5LsLpVz9ZqS599rj/lLoH+rLNlRDVXpS+J51U
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDsDCCApgCCQDJotuPPj9GCDANBgkqhkiG9w0BAQsAADCBqzELMAkGA
UEBhVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExEDAOBgNVBAcBM1JvY2tsa
W4xDDAKBgBAoMA0hQTjEVMBMGA1UECwwMSFBOUm9zZXZpbGxlMSokwAYD
...
MioDy0096DvSMPsnOaI+jnZ3AozN8y+nLgotXUsg36pO/Ncc51oQhyUdc
AbgA1rzSLgyTnpXZKumvlaoTk3pzrIf7m5V103GTbgHGSFCzgO6QWxVxu
9d7ju1o59SaOIT7JSsYI5LsLpVz9ZqS599rj/lLoH+rLNlRDVXpS+J51U
-----END CERTIFICATE-----
```

To upload a certificate:

1. In the navigation pane, expand **Security**, and select **PKI**.
   The PKI page is displayed.
2. In the **Certificates** panel, select the certificate, and click **Upload Certificate**.
   The Upload Signed Certificate dialog box is displayed.
3. Click **Browse** and select the certificate in PEM format.
4. Click **OK**.

Viewing and downloading a certificate

You can view the details of the certificate and download the certificate in PEM format.

To view the details of a certificate:

1. In the navigation pane, expand **Security**, and select **PKI**.
   The PKI page is displayed.
2. In the **Certificates** panel, select the certificate, and click **View Certificate**.
   The certificate details are displayed in a dialog box.
3. To download a copy of the certificate in PEM format, click **Download Certificate**.
4. Click **OK**.

Editing associated application details

You can edit an associated application to change the certificate associated with the application. By default, the local-cert certificate is associated with all applications in the switch.

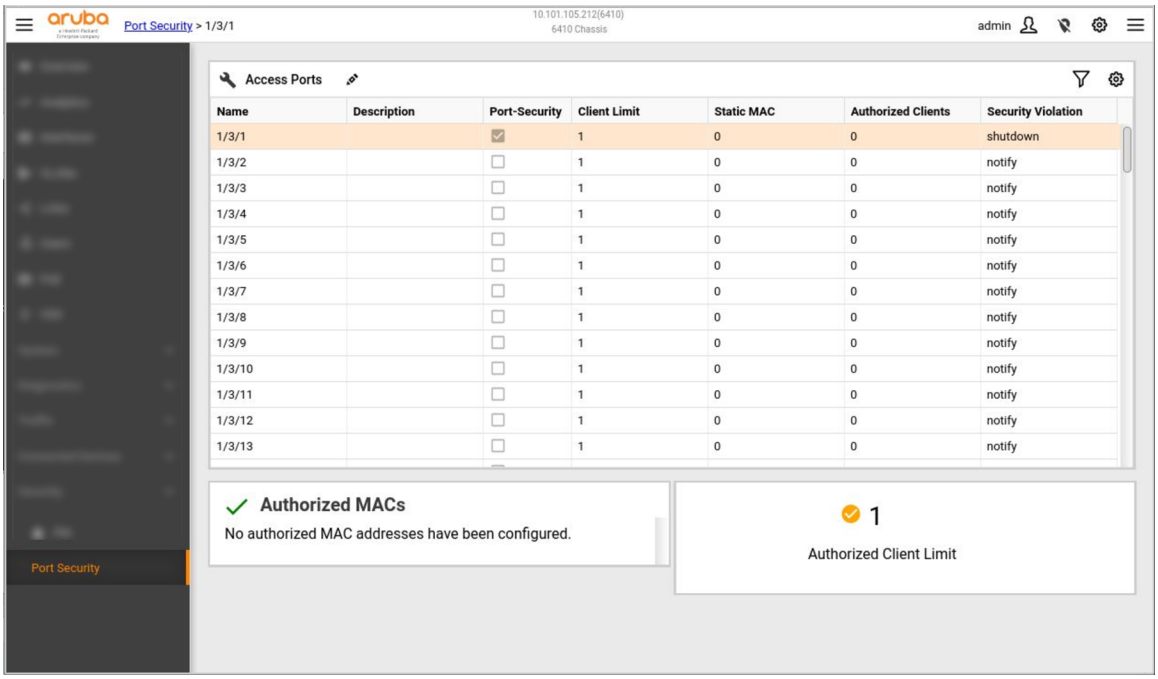
To edit an associated application:

1. In the navigation pane, expand **Security**, and select **PKI**.
   The PKI page is displayed.
2. In the **Associated Application Details** panel, click **Edit**.
   The Adding following Certificate dialog box for the associated application is displayed.
3. Select the required certificate name from the drop-down.
4. Click **OK**.

Port Security page

The Port Security page displays the access port security details, authorized MACs, and authorized client limit details. The page also allows you to edit the port security violation action for the ports.

Figure 1 *WebUI Overview Dashboard*



Access Ports panel

The **Access Ports** panel lists the ports with the port security details. The port security checkbox is selected for the ports that have port security enabled.

Authorized MACs panel

The **Authorized MACs** panel displays the static and dynamic MAC addresses authorized on the switch for the selected port. If you configure static MAC addresses on a port, the number of static MAC addresses configured is displayed in the **Static MAC** column in the **Access Ports** panel.

Authorized Client Limit panel

The **Authorized Client Limit** panel displays the maximum number of authenticated client sessions allowed on the selected port.

Editing port security

You can edit the action that the switch should take when a security violation is encounter on a port. You must enable port security using the CLI to apply the port security settings. For more information about port security commands, see the *AOS-CX Command-Line Interface Guide*.

To edit port security:

1. In the navigation pane, expand **Security**, and select **Port Security**.

The Port Security page is displayed.

2. In the **Access Ports** panel, click **Edit**.

The Edit Port-Security dialog box is displayed.

3. Configure the following optional parameters:
   - **Port**: Select a different port if required.
   - **Violation Action**: Select either **notify** or **shutdown** from the drop-down. The default action is **notify**.
4. Click **OK**.

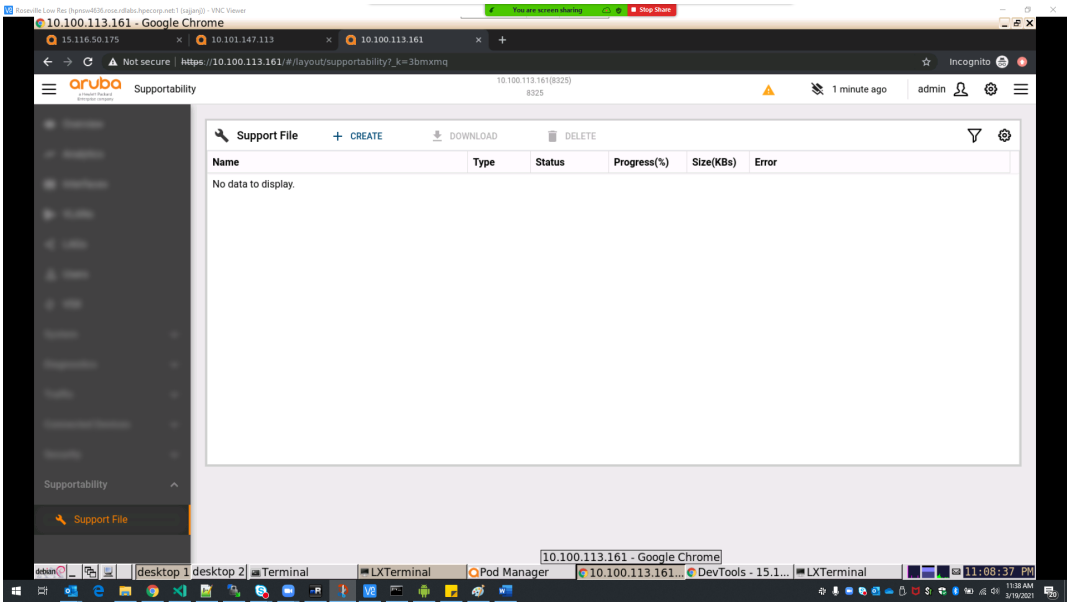
Support File page

Supported only on the 4100i, 6000, and 6100 Switch Series.

From the **Support file** page, you can create support files that can be used to troubleshoot issues in the switch. The support files contain the following information:

- Running configuration
- Events
- Errors
- Confidential information, such as usernames and passwords (in encrypted format)
- Support logs
- Previous boot logs
- Hardware information
- Software build version details
- Debugging information

Figure 1 *Support File Page*



Support File panel

The **Support File** panel displays the details of the support files created on the switch. Administrator rights are required.

The following information is displayed:

- **Name**: Name of the support file.
- **Type**: Type of the support file. By default, the value is **All** and no other type of support file can be generated.
- **Status**: Status of the support file. The following options are supported:
  - **Requested**: Appears immediately after a support file is created.
  - **In Progress**: Appears when the support file is being generated.
  - **Generated**: Appears when the support file is successfully generated.

    You can download the support file only when the status displays **Generated**.
  - **Failed**: Appears when the support file fails to generate with a specific error message.
- **Progress(%)**: Progress of support file generation (in percentage). This field displays 100% when the support file is successfully generated.
- **Size(KBs)**: Size of the support file in kilobytes. The size is displayed only after the support file is successfully generated.
- **Error**: Error message when the support file fails to be generated. The following error messages are supported:
  - Collection is aborted
  - File is not available in local file system
  - Collection process terminated
  - Collection process exceeded max collection time
  - Insufficient storage space available storing the collection
  - Insufficient RAM memory available for collection
  - Collection already in progress in another session
  - Collection is failed due to unexpected error

Creating and deleting support files

You can create support files to capture data about the switch.

You can generate a maximum of one support file. If you want to generate another support file, you must first download and delete the previously generated file, and then generate a new file.

Procedure

To create a support file:

1. In the navigation pane, expand **Supportability**, and select **Support File**.
   The Support File page is displayed.
2. In the **Support File** panel, click **Create**.
   The Support File Name dialog box is displayed.
3. Enter the file name.
   The file name can contain 5 to 64 alphanumeric characters.
4. Click **Create**.

To delete a support file:

1. In the **Support File** panel, select the support file that you want to delete, and click **Delete**.
   A confirmation message is displayed.
2. Click **Delete**.

Downloading a support file

To download a local copy of the support file:

You can download a support file only when the status is **Generated** and the progress displays **100%**.

1. In the navigation pane, expand **Supportability**, and select **Support File**.
   The Support File page is displayed.
2. In the **Support File** panel, select the support file, and click **Download**.
   A confirmation message is displayed.
3. Click **Close**.

Chapter 5
Finding alert details using the Web UI

This chapter is not applicable to the 6000 or 6100 Switch Series, which do not support the Network Analytics Engine.

You can view details on the alerts displayed in the Web UI.

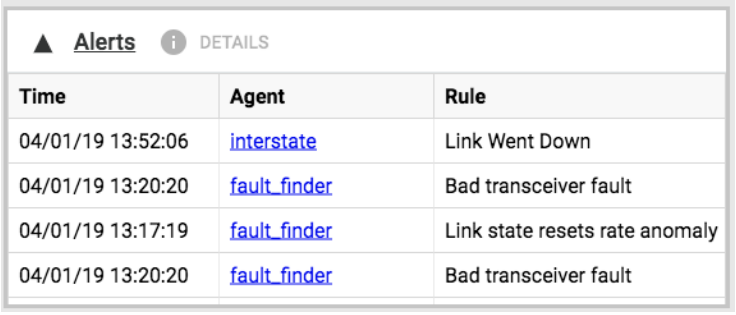
Prerequisites

You must be logged in to the Web UI.

Procedure

1. Select **Analytics** from the navigation pane.
2. In the Analytics Dashboard, the Alerts panel lists the alerts for all agents.

Figure 1 *Alerts panel on Analytics Dashboard*



3. To see the alerts for a specific agent, in the Analytics Dashboard Agents panel or Alerts panel, select an agent.
4. In the Agent Details page, the agent alerts are listed in the Alerts panel.

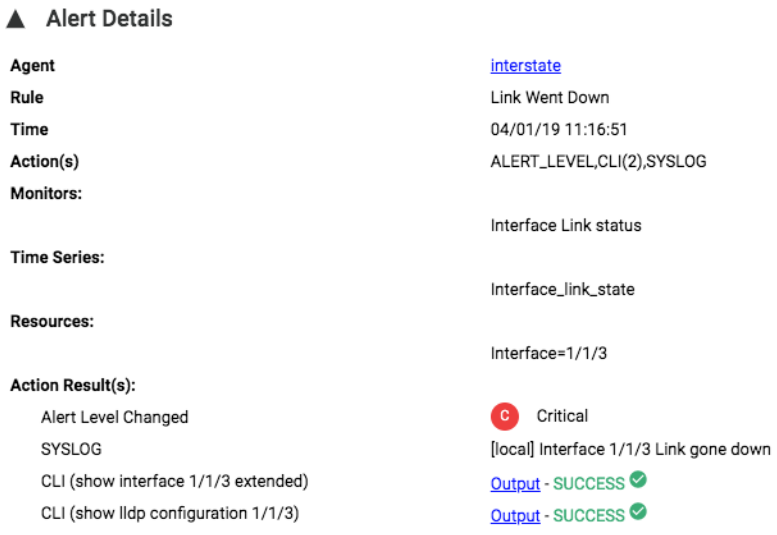
Figure 2 *Agent Details page*

5. In the Alerts panel, select an alert and click **Details** to view the Alert Details dialog box. To close the dialog box, click **Close**.

   You can also access alert details directly from the Analytics Dashboard by selecting an alert in the Alerts panel and clicking **Details**.

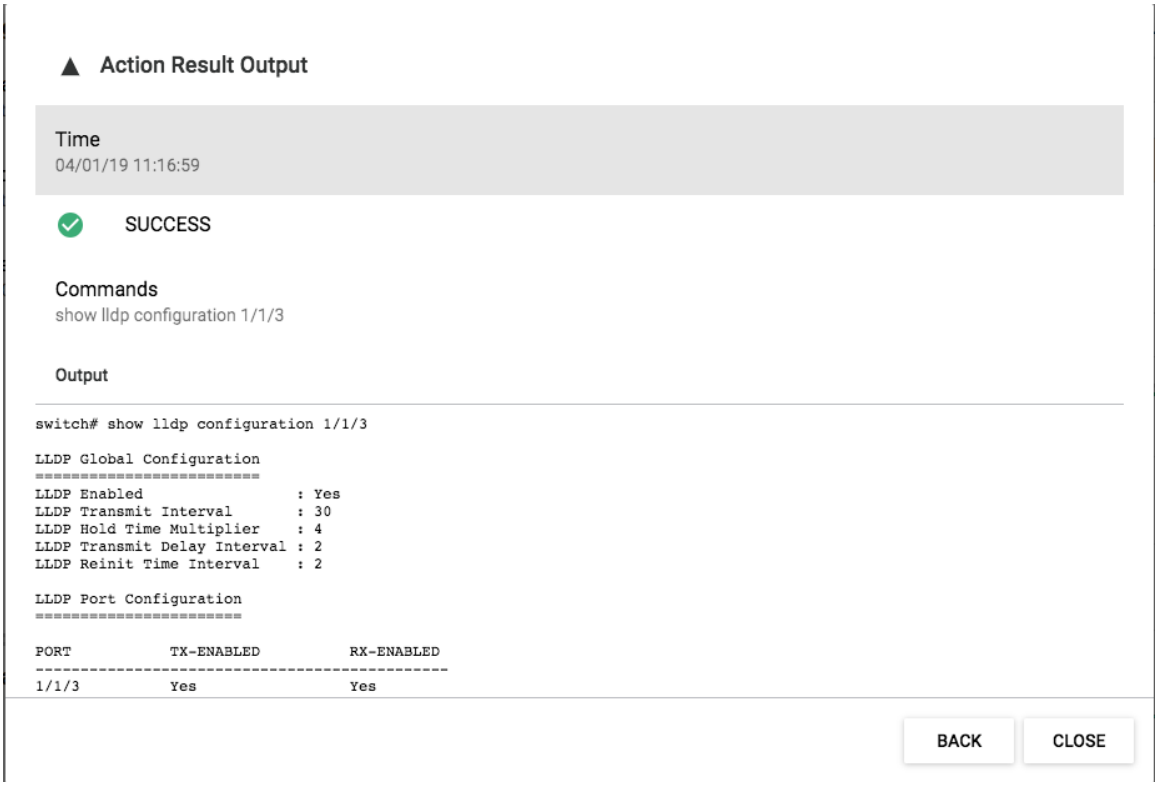
6. The **Action Result(s)** in Alert Details dialog box might include additional details about actions and links to the action result output.

Figure 3 *Alert Details dialog box*



To view the Action Result Output dialog box for an action, click the **Output** link.

Figure 4 *Action Result dialog box*



Chapter 6
Working with the network analytics features

This section describes the steps to view agent information using the Web UI, and work with an Analytics time series graph.

For more information on the Network Analytics Engine, including agents and scripts, see the *Network Analytics Engine Guide*.

Viewing agent information using the Web UI

You can view Analytics agent information including: agent status, script information, agent parameters, one or more time series graphs, and any alerts generated.

Prerequisites

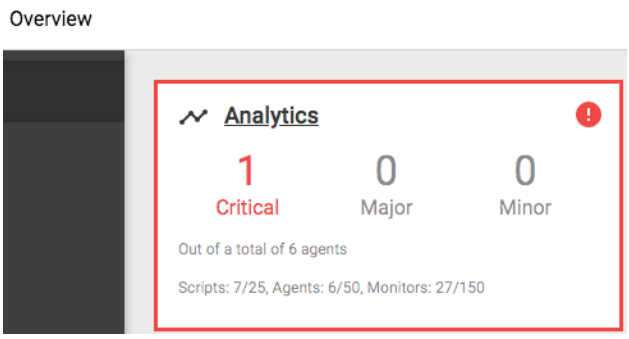
- You must be logged in to the Web UI.
- Ensure that the switch and the client where Web UI is running are set to use NTP or to a time zone based on UTC time. Otherwise, NAE agent data might be incorrect or missing.

For example, if the time on switch is set to 2 hours ahead of the client manually instead of by changing the time zone offset, the agent data is populated according to the new time on switch. If the switch time is set back to match client time later, the Time Series Database does not overwrite the old data. Therefore the client Web UI shows inaccurate data.

Procedure

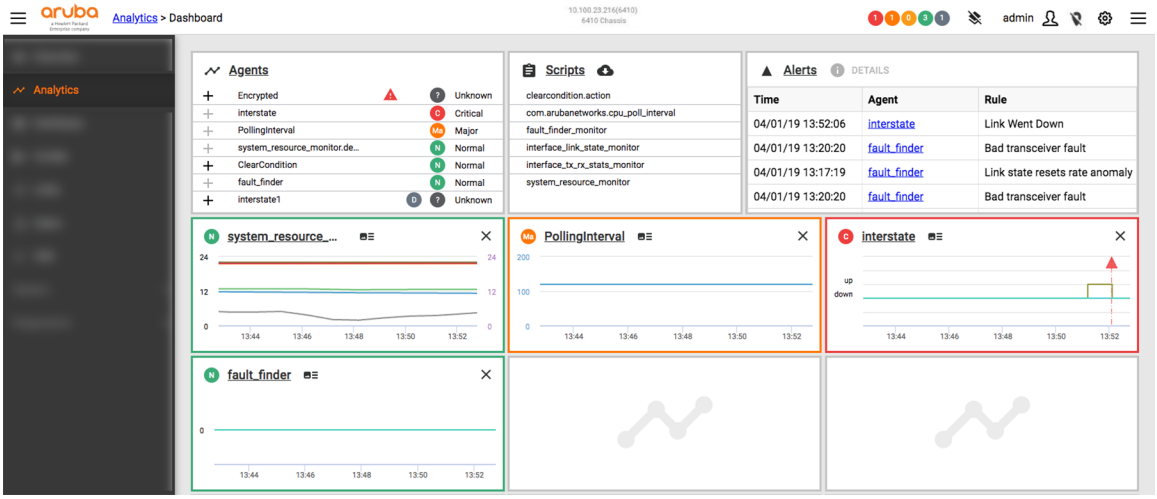
1. From the Overview page, look at the **Analytics** panel to see the total number of agents in critical, major, and minor status. If the panel is outlined in red, it indicates agent status issues.

Figure 1 *Analytics panel on Overview page*



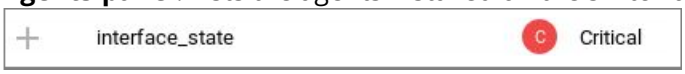
2. To go to the Analytics Dashboard, select the **Analytics** link in the Analytics panel on the Overview page.

Figure 2 *Analytics Dashboard*



The following information appears on the Analytics Dashboard:

- **Top banner**: Shows the number of agents with each type of status. 
- **Agents panel**: Lists the agents installed on the switch and indicates the status of each agent.



If there is an error in an agent, the Agents panel shows an error icon next to the agent status. 

Optionally, you can add an Analytics agent time series graph to the Analytics Dashboard by clicking the **+** plus sign next to any agent listed in the Agents panel.

The time series graph shows data collected by the Analytics agent. If an agent has multiple time series graphs, the graph displayed on the Analytics Dashboard is specified by the script. You cannot choose which graph to display on the Analytics Dashboard, but you can see all the graphs in the Agent Details page.

Click the **Agents** link to display the Agent Management page. On this page you can create, edit, delete, enable, and disable an agent.

- **Scripts panel**: Lists available scripts.

  Select a script from the list to display the Script Details page where you can view script details, create an agent to run the script, and download the script.

  Click the **Scripts** link to display the Script Management page. On this page you can upload, download or delete a script, create an agent, and access the Aruba Solution Exchange (ASE) to find more scripts.

  The Script Management page also shows the origin of the scripts:

  - System scripts: These are default scripts preloaded on the switch.
  - User scripts: These are scripts written by the user or downloaded from ASE.
  - Generated scripts: These are Watch or Monitor scripts generated by the switch.

    For generated scripts, the associated Agent is automatically created when the script is generated, so users cannot create another agent, thus the **CREATE AGENT** button is disabled. These scripts also cannot be disabled from this page so the **DELETE** button is also disabled. These scripts and agents can only be deleted from the CLI.

- **Alerts panel**: Lists alerts generated by all agents.

  Select an alert in the list and click **Details** to display the Alert Details dialog box.

Click the **Alerts** link to display a list of the alerts with information on the rule and actions for each alert.

Since watch-type agents do not have time series data, no graphs are displayed in the Alerts window. Alerts generated by these watch agents are listed in the window, but do not have navigate options as found with other agents. Finally, watch agents do not support parameters so the Parameters pane in this window will be empty.

- **Time series graphs**: If an agent time series graph has been added to the Analytics Dashboard, the graph is outlined in the agent status color. Agents can have more than one time series graph, but only one graph for the agent is displayed in the Analytics dashboard. Click the link in the graph to display the Agent Details page.

3. From the Analytics Dashboard, Agents panel, select the link to a specific agent. The Agent Details page is displayed.

Figure 3 *Agent Details panels example*

View the following information from the **Agent Details** page:

- **Agent Details panel**: Shows information about the agent.

Select the Edit button to enable or disable an agent and modify agent parameters.

Select the View Script button to display the Script Details page where you can view script information, create an agent to run the script, and download the script.

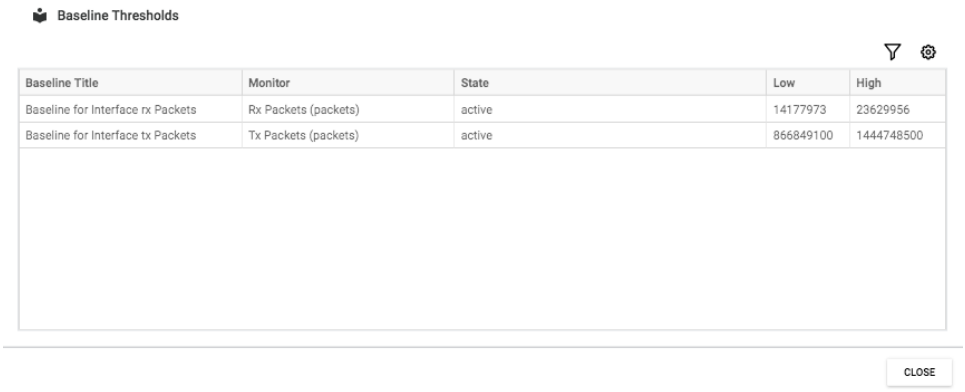
- **Status panel**: Shows the status of the agent and when the status was last updated. For some agents, you may see additional information. For example:
- **System Created**: If the Status panel includes the statement `System Created`, the agent cannot be deleted.
- **Baseline Thresholds:** If the Status panel includes Baseline Thresholds, the agent can learn about the activity being measured and set low thresholds and high thresholds based on what it learns. The Baseline Thresholds information shown in the Status panel includes the number of thresholds in the following states:

- **Active:** When a baseline threshold is in the active state, the agent has learned and established the high and low thresholds, and the agent executes actions and generates alerts based on those low or high thresholds.
- **Inactive:** When agent is disabled, the baseline stops collecting data and updating thresholds. After the agent is re-enabled, the baseline goes into the learning state again.
- **Learning:** While a baseline threshold is in the learning state:
  - The agent gathers data related to that baseline until the initial learning period completes. Low and high thresholds are determined using the learning algorithm defined in the script, and are set only after learning state is completed.
  - Default thresholds (if specified in the script) are used to determine whether to execute actions or generate alerts.

  Baseline thresholds remain in the learning state for a script-specified period of time after the agent is enabled.

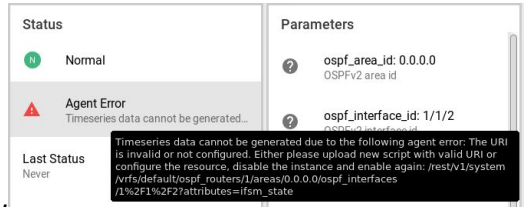
Selecting **Baseline Thresholds** displays a dialog box that shows additional information about all the baselines for the agent, including the name, the associated monitor, state, and the current learned low and high thresholds.

Figure 4 *Baseline Thresholds*



If there is an agent error, an error indicator is shown and you can hover over it for more information.

Figure 5 *Agent Status*



- **Parameters panel**: Shows the parameters used by the agent. For example, a parameter can be a threshold value that, when breached, causes the agent status to change and an alert to be generated. Selecting a parameter displays the description in a dialog box.
- **Time Series graph**: Graphs the data collected by the agent over time. Agents might have more than one time series graph. Alert indicators and configuration checkpoints are overlaid on the graph.

Alert indicators can include: a red or yellow triangle for an alert, a green triangle for return to normal, a blue triangle for an alert on several resources being monitored. An example of an alert on several resources: when monitoring multiple interfaces (wildcard), if an interface goes down, a

red alert is generated. If another interface goes down, then a blue alert is generated. A green alert will not be generated until all the interfaces are back up.

Configuration checkpoints are shown as purple diamonds on the graph.

Clicking an alert indicator on the graph displays the Alert Details dialog box.

- **Alerts panel**: Lists alerts.

Select the **Alerts** link to display a list of the alerts with information on the rule and actions for each alert.

Select an alert and click **Details** to display the Alert Details dialog box.

Select an alert and click **Navigate** to change the time series graph to show the time period with this alert.

Working with an Analytics time series graph

Data collected by an Analytics agent is displayed in the Web UI in one or more time series graphs. An agent has at least one graph. An agent can have multiple graphs as specified in the script, but only one graph represents the agent on the Analytics dashboard. The graph that represents the agent on the Analytics dashboard is specified in the script.

If the Analytics dashboard does not include a graph for an agent, you can add the graph that represents that agent from Analytics dashboard. Graphs on the Analytics dashboard represent a live view only. The graph customization toolbar is not available from the Analytics dashboard.

The Agent Details page displays all the graphs for an agent, with each graph displayed in a panel.

Configuration checkpoints and alert indicators are overlaid on the graph. Configuration checkpoints are shown as purple diamonds. Alert indicators can include the following:

- A red or yellow triangle for an alert
- A green triangle for a return to normal
- A blue triangle for an alert on several resources being monitored.

The graph displays alerts for all metrics being monitored. However, time series graphical information can be shown for a maximum of eight metrics. The metrics that are being shown on the graph are listed at the bottom of the graph.

Figure 1 *Agent Details panel including graph*

Procedure

1. Customizing data displayed on the graph
2. Zooming in on the graph
3. Downloading the graph as an image or .csv file
4. Viewing an alert on the graph

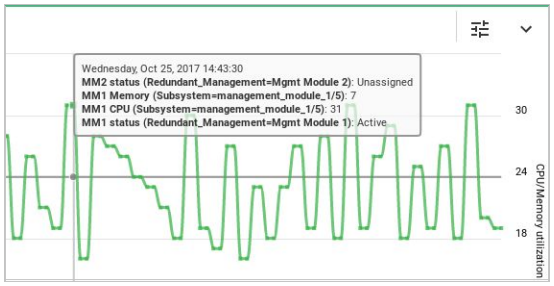
Customizing data displayed on the graph

There are several ways you can customize the data displayed on a time series graph to show more or less data.

1. View a tooltip for each data point on the graph by hovering the cursor over the data point.

   The tooltip displays the date, time range, and min-max range.

   Figure 1 *Graph with tooltip displayed*

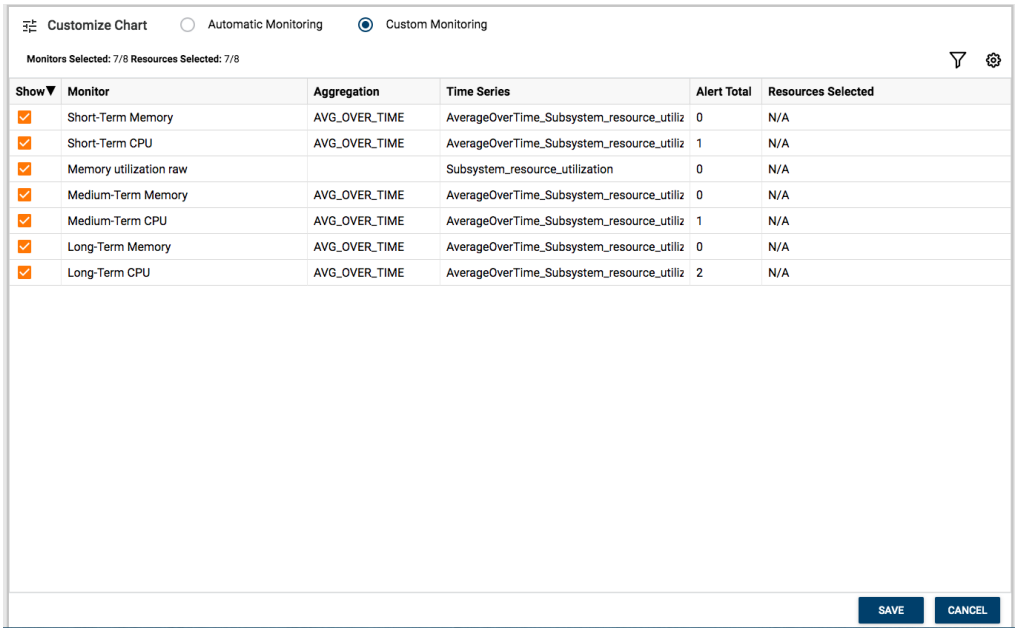
2. Hover over a specific item in the legend following the graph to show only that specific data line on the graph. The other data will be less visible.
3. From the graph shown on the Agent Details page, click the **Configure Chart** button to open the **Customize Chart** dialog box.

- The default mode is Automatic Monitoring, where the most meaningful monitors and resources are automatically selected to display on the agent graph. To customize what data (monitors and resources) you want displayed on the agent time series graph, select **Customize Monitoring**.
- You can sort and filter the Show column. If a monitor is a wildcard type, then you see a different icon from the check box, where you can click and select subresources under that monitor.

The graph displays alerts for all metrics being monitored. However, the graph can show graphed data for a maximum of eight metrics at a time. The metrics that are being shown on the graph are listed at the bottom of the graph. You can choose which metrics to show. To remove the metric from the graph, clear the box in the Show column of the metric you want to remove. To show a metric in the graph, select the box in the Show column of the metric you want to display.

- The Resources Selected column shows how many total resources are selected out of the total available resources.
- If a monitor can have an aggregation function, that function is displayed in the Aggregation column.

Figure 2 *Customize Chart*

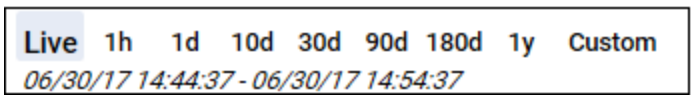


Zooming in on the graph

There are several different ways to zoom in on a specific time period on the time series graph.

1. Zoom in and out on the graph by selecting a zoom level from the options displayed at the top of the time series graph: 1 hour, 1 day, 10 days, 30 days, 90 days, 180 days, 1 year. You can also select **Custom** to enter a specific date and time range.

Figure 1 *Zoom options portion of a graph*

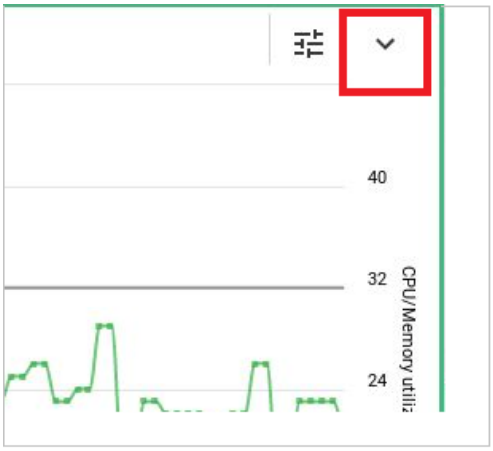


2. Or you can highlight a custom range of data on the graph as follows:
   a. Position the cursor on the time axis of the graph until a vertical line appears through the time.
   b. Drag the vertical line to the left or right to the beginning or end of the time period you want to view.
   c. The selected time period is highlighted and the begin and end dates are displayed next to the Custom zoom level.
   d. Release the mouse button and the graph is redrawn for just the time period selected.
3. Reset the graph to the default by selecting the **Live** zoom level.

Downloading the graph as an image or .csv file

You can download the graph either as an image or represented as a set of comma-separated values that can be opened in spreadsheet programs. The download options are accessed from the down arrow in the top right corner of the time series graph:

Figure 1 *Graph with down arrow highlighted*



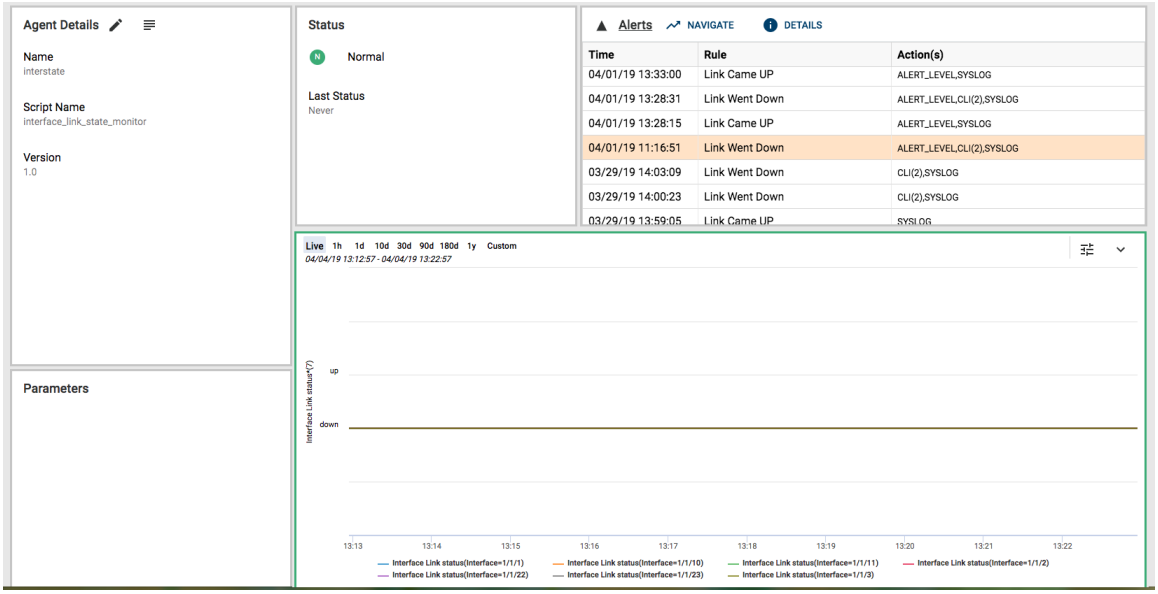
- To download the graph as an image, click the down arrow and select **Download Chart**.
  The graph is downloaded in a file in **.png** format.
- To download the graph as a set of comma-separated values, click the down arrow and select **Export to CSV**.
  The graph is downloaded in a file in **.csv** format.

Viewing an alert on the graph

The graph shown on the Agent Details page might not show the time period or resource associated with a specific alert. Use this procedure to change the graph to show the alert and the associated metric.

1. From the alerts panel on the Agent Details page, select an alert and click **Navigate**.

Figure 1 *Agent Details before navigating to an alert*



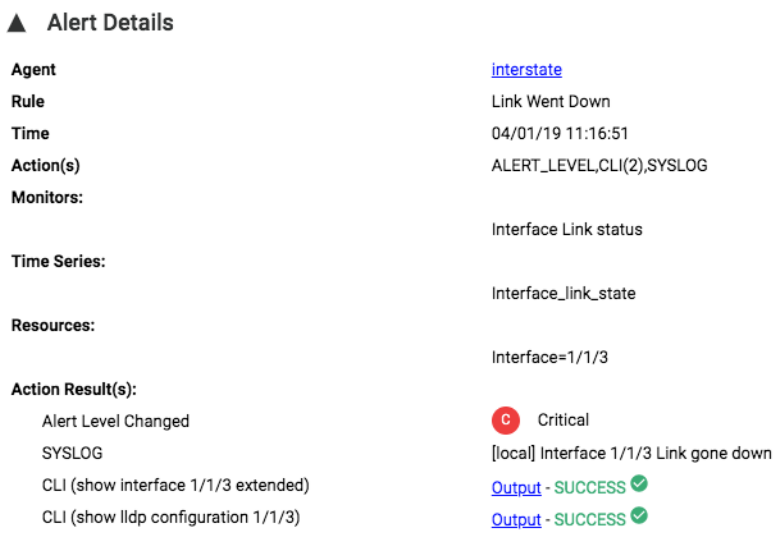
The graph is changed to display the time period containing the alert. However, the alert might be for a metric that is being monitored but that is not being shown in the graph.

The graph displays alerts for all metrics being monitored. However, the graph can show graphed data for a maximum of eight metrics at a time. The metrics that are being shown on the graph are listed at the bottom of the graph.

Figure 2 *Graph with alert but not metric for 1/1/3*

2. To adjust the graph display to show the metrics for the alert, do the following:
   a. Locate the alert on the graph and click the alert triangle flag. The **Alert Details** dialog box is displayed.

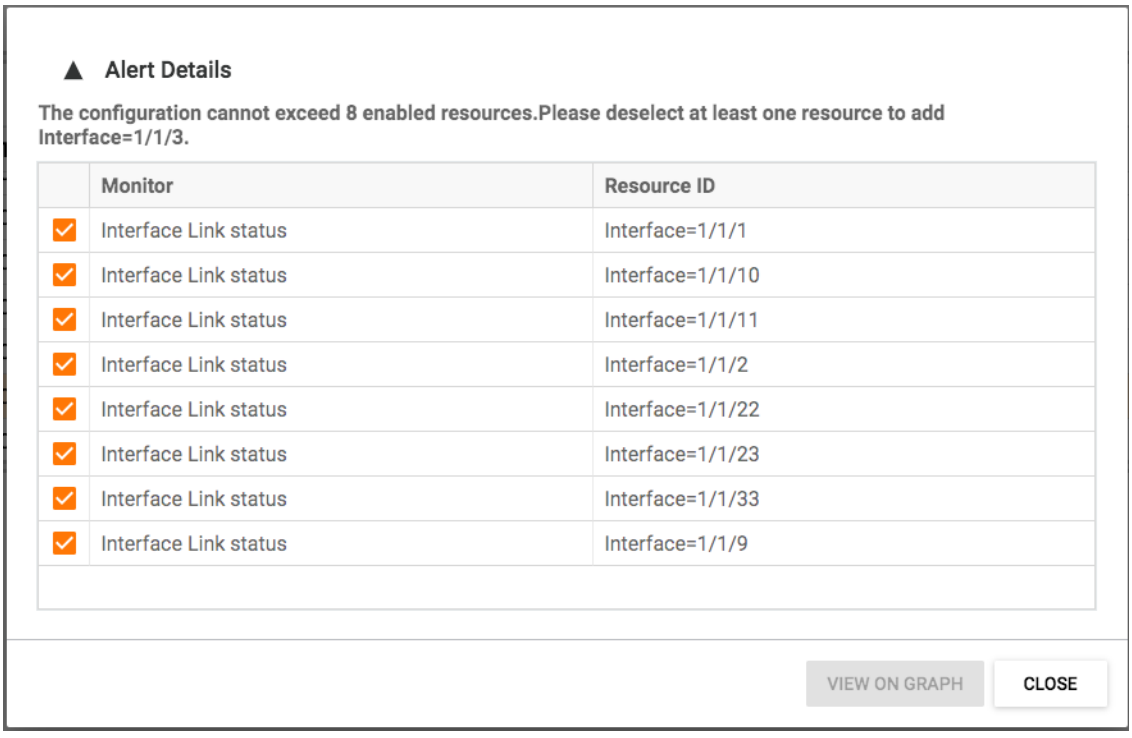
Figure 3 *Alert details box with **View on Graph** button displayed*



b. Click **View on Graph**.

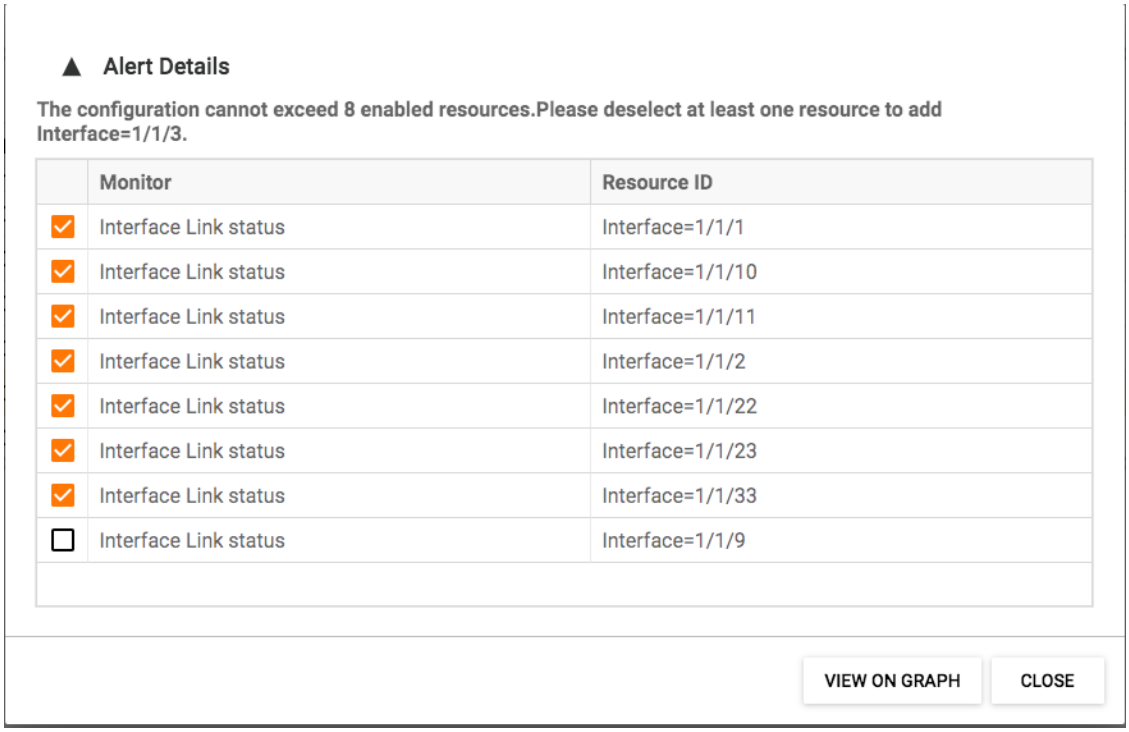
3. If the graph is showing eight metrics and the metric you want to display is the ninth metric, you must choose an existing metric to clear so that the graph can show the metric associated with the alert. For example:

Figure 4 *Dialog box prompting you to clear a metric*



a. Clear the selection box for the metrics you no longer want to show. For example:

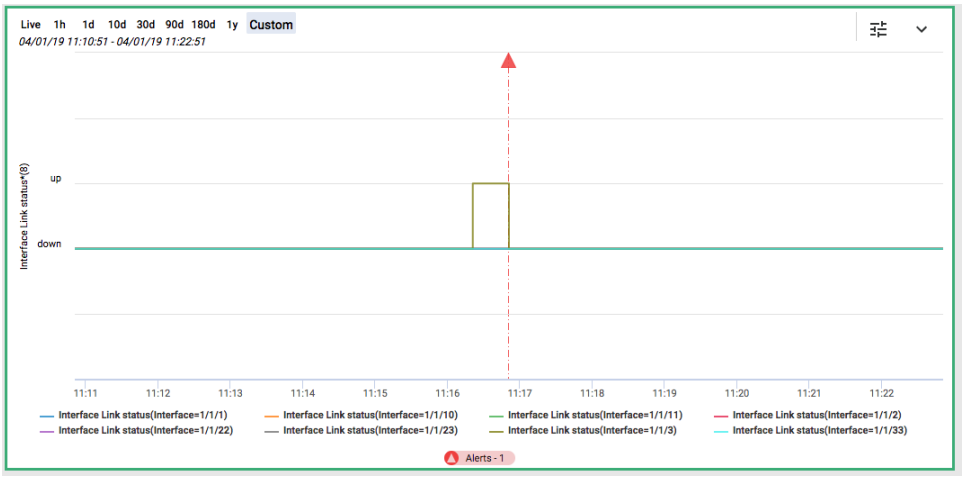
Figure 5 *Dialog box with 1/1/9 removed*



b. Click **View on Graph**.

The graph is changed to show the metric associated with the alert. For example:

Figure 6 *Graph showing alert and metric 1/1/3*



4. You can reset the graph to the default by selecting the **Live** zoom level.

Aruba Network Analytics Engine scripts, agents, and troubleshooting information

For detailed information about the Aruba Network Analytics Engine and the Analytics dashboard, see the *Network Analytics Engine Guide*. This guide includes information about using the Web UI to do the following:

- Create, modify, and delete agents.
- Enable and disable agents.
- Create, edit, download, and install scripts.
- Access scripts on the Aruba Solutions Exchange.
- Troubleshoot problems with agents and scripts.

In addition, the guide provides information about using the REST API to perform script and agent tasks and information about writing scripts.

Chapter 7
Support and Other Resources

Accessing HPE Aruba Networking Support

HPE Aruba Networking Support Services	https://www.arubanetworks.com/support-services/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
HPE Aruba Networking Support Portal	https://networkingsupport.hpe.com/home
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
HPE Aruba Networking Hardware Documentation and Translations Portal	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm

HPE Aruba Networking software	https://networkingsupport.hpe.com/downloads
Software licensing and Feature Packs	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
HPE Aruba Networking Developer Hub	https://developer.arubanetworks.com/

Accessing Updates

You can access updates from the HPE Aruba Networking Support Portal at https://networkingsupport.hpe.com.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

https://networkingsupport.hpe./notifications/subscriptions (requires an active HPE Aruba Networking Support Portal account to manage subscriptions). Security notices are viewable without an HPE Aruba Networking Support Portal account.

Warranty Information

To view warranty information for your product, go to https://www.arubanetworks.com/support-services/product-warranties/.

Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

HPE Aruba Networking is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see https://www.arubanetworks.com/company/about-us/environmental-citizenship/.

Documentation Feedback

HPE Aruba Networking is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback-switching@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help

content, include the product name, product version, help edition, and publication date located on the legal notices page.