USER GUIDE

RUCKUS FastIron Web Management Interface User Guide, 09.0.10

Supporting FastIron Software Release 09.0.10

Part Number: 53-1005718-02
Publication Date: 3 February 2022

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://forums.ruckuswireless.com/
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.commscope.com/ruckus .

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	**Description**
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Document

Supported Hardware

This guide supports the following RUCKUS products:

- RUCKUS ICX 7850 Switch
- RUCKUS ICX 7650 Switch
- RUCKUS ICX 7550 Switch
- RUCKUS ICX 7450 Switch
- RUCKUS ICX 7250 Switch
- RUCKUS ICX 7150 Switch

For information about what models and modules these devices support, refer to the hardware installation guide for the specific product family.

What's New in This Document

The following table includes descriptions of new information added to this guide for the FastIron 09.0.10 software release and subsequent patch releases.

TABLE 2 Summary of Enhancements in FastIron 09.0.10s Release

Feature	Description	Location
Support Save	The Supportsave configuration section has been updated to reflect the latest capabilities and to add screen graphics.	Supportsave on page 50

TABLE 3 Summary of Enhancements in FastIron 09.0.10 Release

Feature	Description	Location
Web Management - VLAN Settings	Made enhancements to support the following: Clone VLAN Change Default VLAN	Configuring a VLAN on page 28
Support Save	Supportsave collects the logs and information that can be useful when troubleshooting an issue.	Supportsave on page 50
Web Management - AAA Settings	Configures the settings to enable web user authentication.	Managing AAA Settings on page 63
Icon changes	Changed the icons in menu and sub-menu windows	Throughout the guide.

Getting Started

Access Requirements

The Web Management Interface is a browser-based interface that allows administrators to manage and monitor a single RUCKUS device or a group of RUCKUS devices connected together. For many of the features on a RUCKUS device, the Web Management Interface can be used as an alternative to the command line interface (CLI) for creating new configurations, modifying existing ones, and monitoring the traffic on a device.

The Web Management Interface can be accessed from a management station using a web browser through an HTTP connection.

NOTE
The Web Management Request will be rejected during HTTPS image download. The device will respond with "503 service unavailable". In such cases, wait until the HTTPS image download is complete, and try accessing the Web Management Interface again.

Before logging in to the web interface, verify that you are using one of the following supported web browsers:

- Google Chrome
- Mozilla Firefox
- Safari
- Chromium
- Microsoft Edge
- Opera

Prerequisite Configuration

The following steps must be completed to enable access to the Web Management Interface.

1. Connect a PC by way of a serial connection to the device using the console port. Use a terminal program such as PuTTY to access the command line interface (CLI).

   If the switch is already connected to a network, the switch will automatically receive its IP configuration through DHCP. To check the IP configuration of the switch, use the **show ip** command.

   If the switch is not connected to a network or you want to assign an IP address manually, use the commands described in step 2; otherwise, go to step 3.

2. Assign an IP address to the device using the command line interface (CLI).

   Assigning an IP address for a switch image:

   ```
   device> enable
   device# configure terminal
   device(config)# ip address 10.37.71.212/24
   device(config)# ip default-gateway 10.37.71.129
   ```

   Assigning an IP address for a router image:

   ```
   device(config)# interface management 1
   device(config-if-mgmt1)# ip address 10.37.71.212/24
   device(config)# ip route 0.0.0.0 0.0.0.0 172.26.64.1
   ```

   Alternatively, the IP address can also be assigned on a router interface (example VE 1). For more information on assigning IP addresses for a device, refer to the *RUCKUS FastIron Layer 3 Routing Configuration Guide*.

3. Configure a user account with a password and privilege levels for authentication purposes.

   You can also use external AAA servers (RADIUS and TACACS+) to perform user authentication. To do so, you must configure the RADIUS server host and RADIUS server key and the TACACS+ server host and TACACS+ server key. For more information, refer to the *RUCKUS FastIron Security Configuration Guide*.

   ```
   device(config)# username user1 privilege 0 password xpassx
   ```

   Depending on the privilege level defined for the user account, the user can have complete read-and-write access or read-only permission while using the Web Management Interface.

4. Configure device authentication methods to identify a user by verifying the authentication credentials before access is granted.

   ```
   device(config)# aaa authentication web-server default local radius tacacs+
   ```

   For more information about the authentication method list, refer to the *RUCKUS FastIron Security Configuration Guide*.

5. (Optional) Enable web management access.

   Web management access over HTTPS is enabled by default. For TPM-enabled devices, TPM certificates are available by default to establish encrypted communication between the server and the client.

   NOTE
   Web management HTTP configuration in pre-09.0.00 image will be disabled on upgrade to 09.0.00 release and web management access over HTTPS gets enabled by default.

   You can also import a digital certificate issued by a third-party certificate using the **copy tftp flash 192.168.9.210 certfile certificate-data-file** command. ICX devices that are not TPM-capable, for example, legacy devices deployed to the field, may use an auto-generated non-TPM certificate. Non-TPM certificates are stored on the device in flash memory.

   Once a valid certificate is present, it remains available, unless the user erases the startup configuration or uses a command to zeroize (clear) the certificate.

   When no certificate is present, the RUCKUS ICX device is unable to use applications that require a certificate.

   When more than one certificate is stored in the RUCKUS ICX device, the device selects the certificate for use based on the following order of priority:

   a. User-imported (SSL) certificate

   b. TPM certificate

   c. Non-TPM (auto-generated legacy) certificate

   For more information on ICX digital certificates, refer to the *RUCKUS FastIron Security Configuration Guide*.

6. View the web login details.

```
device# show web
HTTP server status: Disabled
HTTPS server status: Enabled

Web session management:
User     Privilege     IP address         Timeout(secs)  CONNECTION
admin    READ-WRITE    10.37.71.212/24    10             HTTPS
```

Logging In to the Web Management Interface

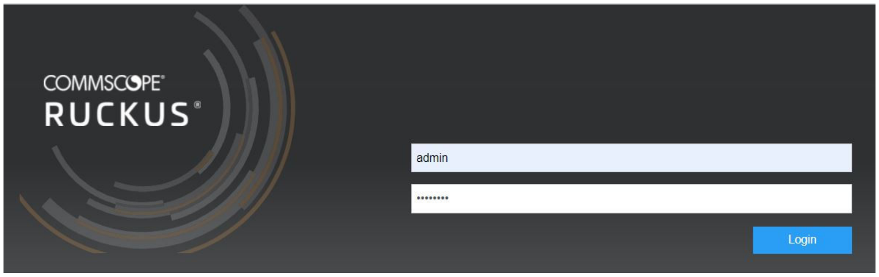
To log in to the Web Management Interface, perform the following steps.

1. Launch a web browser and enter the IP address of the management port in the address bar.

   You can also access the device using Management IP, interface IP, or VE IP which is connected to the network.

   The **Web Management Interface Login** page is displayed.

   FIGURE 1 Web Management Interface Login Page



admin

••••••••

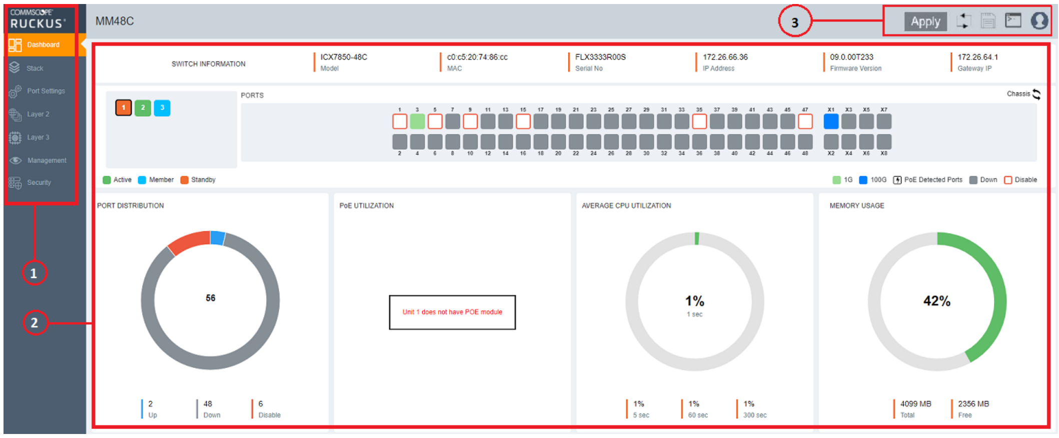
2. Enter the username and password.
3. Click **Login**.

   The **Dashboard** of the Web Management Interface is displayed.

Navigating the Web Management Interface

The Web Management Interface is divided into three panes which provide various user interface elements to display device information, perform administrative tasks, and monitor configuration status.

FIGURE 2 Web Management Interface Elements



SWITCH INFORMATION
ICX7850-48C Model
c0:c5:20:74:86:cc MAC
FLX3333R00S Serial No
172.26.66.36 IP Address
09.0.00T233 Firmware Version
172.26.64.1 Gateway IP

2 Up | 48 Down | 6 Disable

Unit 1 does not have POE module

1% 5 sec | 1% 60 sec | 1% 300 sec

4099 MB Total | 2356 MB Free

TABLE 4 Web Management Interface Elements

Number	Name	Description
1	Menu	Lists the menu and sub-menu items for administrative tasks.
2	Middle pane	Displays configuration details, configuration options, charts, stack units, ports, and chassis panels, tables, lists, and miscellaneous information specific to the selected menu item.
3	Header pane	Provides the following options common to the web interface: • ⇄ (**Device Reload**): Allows you to reload the device. The **Device Reload** window provides the option to select either the primary or secondary partition. • 🖫 (**Write memory**): Allows you to save the running configuration to the memory. • **Apply**: Allows you to globally apply all the configuration changes that are saved on multiple pages to the device. • >_ (**Terminal**): Launches the remote CLI access to the management port that provides access to the management functions and can run all the configuration commands and show commands. Refer to Accessing the Remote CLI on page 15. • 👤 (**User Account**): Displays the following options: – **User**: Displays the currently logged-in user profile. Depending on the privilege levels, there are two types of users: › **Admin**: Admin users have read-write permission and can perform all actions (add, edit, and delete) on the device from the Web Management Interface. › **Non-admin**: Non-admin users have read-only permission and can only view the configurations on the device. The add, edit, and delete options are unavailable for a non-admin user. – **Logout**: Allows you to log out from the Web Management Interface.

Common Action Elements in the Interface

The following elements are available across all pages:

- ⊕ (Add icon): Allows you to add a new configuration instance or parameters for the selected feature.
- ✎ (Edit icon) : Allows you to edit an existing configuration.
- 🗑 (Delete icon): Allows you to delete an existing configuration.
- **Save**: Allows you to save the configuration changes on individual pages. You can save the configuration updates on multiple pages and choose to apply the changes to the device later. To apply all the changes together to the device, use the global **Apply** option available on the header pane.
- **Apply**: Allows you to apply the configuration changes to the device immediately.

Accessing the Remote CLI

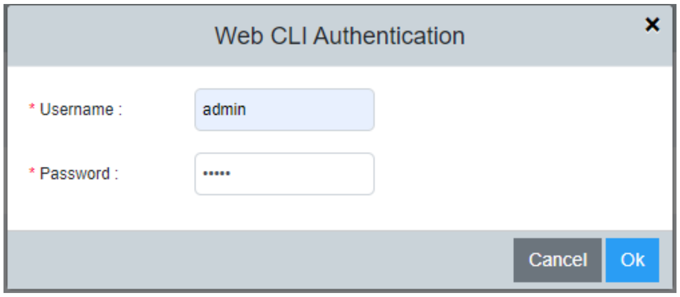
The **Terminal** option provides access to the remote command line interface (CLI) through the web interface. The functionality and behavior of the remote CLI available through the **Web CLI** pane is the same as that of the CLI session available through console, SSH, or Telnet. Using the remote CLI, you can configure, monitor, and manage the switch. The configurations performed in the remote CLI are reflected in the Web Management Interface and vice versa.

Complete the following steps to access the remote CLI.

1. From the header pane, click >- (Terminal icon).

   The Web CLI Authentication window is displayed.

   FIGURE 3 Login Credentials



Web CLI Authentication

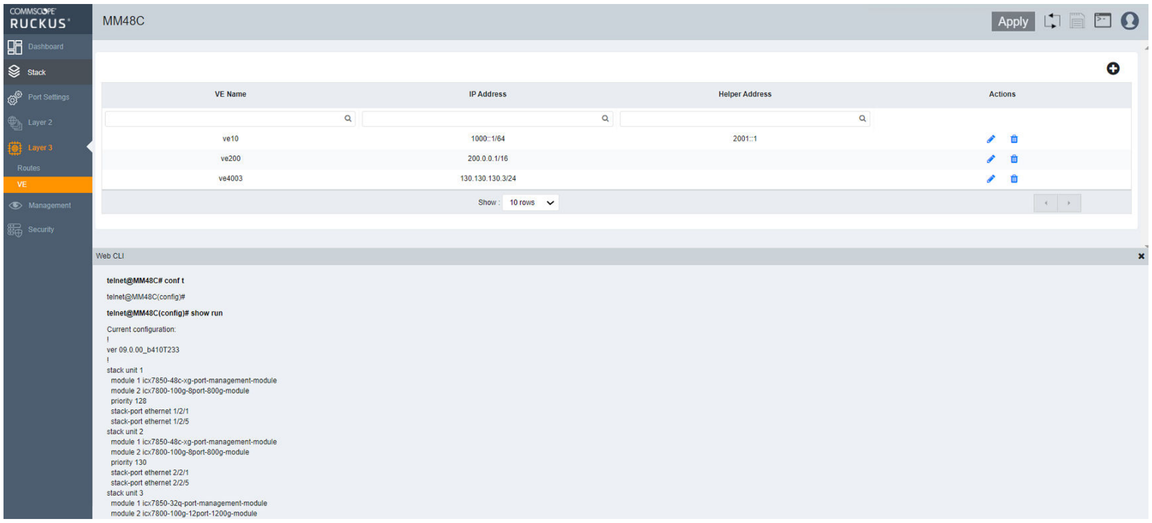
* Username : admin

* Password : •••••

2. Enter the username and password configured for user authentication and click **Ok**. For more information about user account configuration and AAA authentication, refer to the *RUCKUS FastIron Security Configuration Guide*.

   After successful authentication, the remote Telnet session of the switch management port is displayed in the **Web CLI** pane.

   FIGURE 4 Web CLI Pane

VE Name	IP Address	Helper Address	Actions
ve10	1000::1/64	2001::1	
ve200	200.0.0.1/16		
ve4003	130.130.130.3/24		

```
telnet@MM48C# conf t
telnet@MM48C(config)#
telnet@MM48C(config)# show run
Current configuration:
!
ver 09.0.00_b410T233
!
stack unit 1
  module 1 icx7850-48c-xg-port-management-module
  module 2 icx7800-100g-8port-800g-module
  priority 128
  stack-port ethernet 1/2/1
  stack-port ethernet 1/2/5
stack unit 2
  module 1 icx7850-48c-xg-port-management-module
  module 2 icx7800-100g-8port-800g-module
  priority 130
  stack-port ethernet 2/2/1
  stack-port ethernet 2/2/5
stack unit 3
  module 1 icx7850-32q-port-management-module
  module 2 icx7800-100g-12port-1200g-module
```

3. View, add, edit or delete the configurations from **Web CLI** pane. It is similar to console, SSH, or Telnet session to the device.

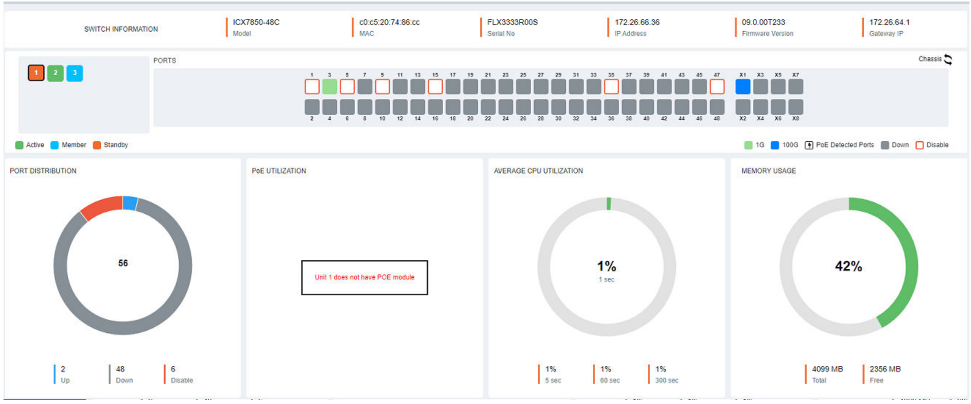
Dashboard and Stack Details

Monitoring Device Information on the Dashboard

The **Dashboard**, which is the first page that appears after you log in to the Web Management Interface, provides a snapshot of the ICX device or group of ICX devices connected together. The **Dashboard** provides a centralized monitoring pane for the ICX device and displays the operational status and statistics.

The figures are included for illustrative purposes only. The ports panel and port speed vary with different ICX models.

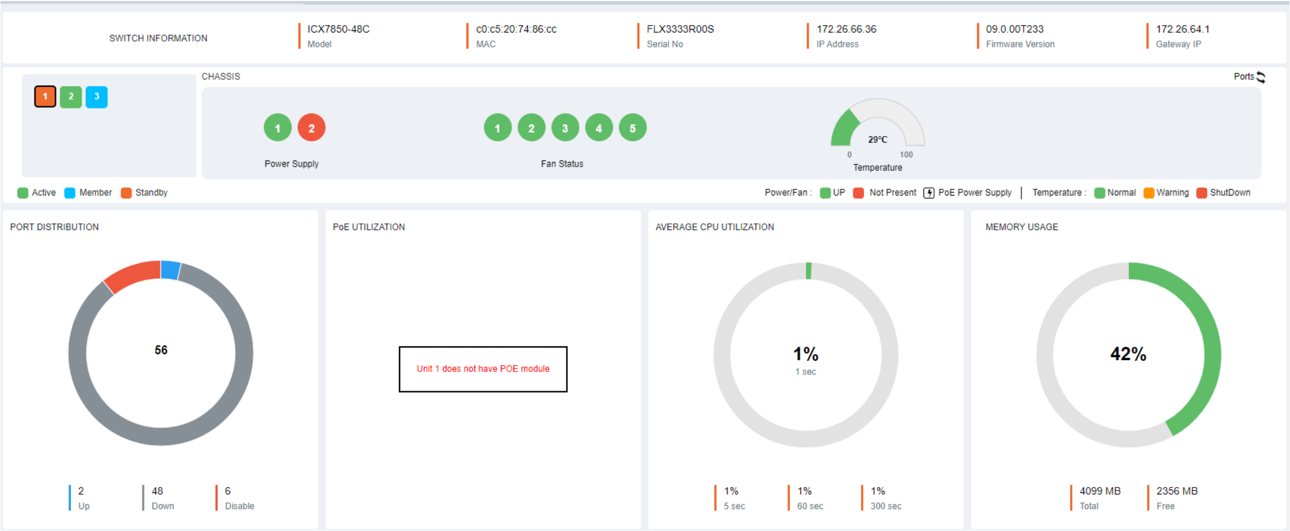
FIGURE 5 Dashboard: Ports Panel



SWITCH INFORMATION

ICX7850-48C Model | c0:c5:20:74:86:cc MAC | FLX3333R00S Serial No | 172.26.66.36 IP Address | 09.0.00T233 Firmware Version | 172.26.64.1 Gateway IP

FIGURE 6 Dashboard: Chassis Panel



SWITCH INFORMATION

ICX7850-48C Model | c0:c5:20:74:86:cc MAC | FLX3333R00S Serial No | 172.26.66.36 IP Address | 09.0.00T233 Firmware Version | 172.26.64.1 Gateway IP

The following table lists the infographic elements of the **Dashboard** that provides the basic device information and its operational status and statistics.

TABLE 5 Dashboard Elements

Dashboard Element	Description
SWITCH INFORMATION	Displays the following device information: ● **Model**: Displays the ICX model details. ● **MAC**: Displays the MAC address of the device. ● **Serial No**: Displays the serial number of the device. ● **IP Address**: Displays the IP address which is used to access the device via web management. ● **Firmware Version**: Displays the firmware version number. ● **Gateway IP**: Displays the gateway IP address.
Stack	Displays the total number of units in a stack. The numbers displayed within each color-coded box indicate the unit IDs. The color code represents the role of each unit: ● Green: Represents an active unit. ● Blue: Represents a member unit. ● Red: Represents a standby unit.
PORTS	Displays the ports in a stack unit and their capabilities. The number above or below each port indicates the port number. The color code represents different port speeds. The ⚡ power icon on the ports indicates detected Power over Ethernet (PoE) ports.
CHASSIS	Displays the following chassis information: ● **Power Supply**: Displays the total number of power supply connectors and their status. The following color code represents their status: – Green: Power supply is up. – Red: Power supply is not present. The ⚡ power icon indicates a Power over Ethernet (PoE) power supply. ● **Fan Status**: Displays the total number of cooling fans and their status. The following color code represents their status: – Green: Fan is up. – Red: Fan is not present. ● **Temperature**: Displays the current temperature. The following color code indicates the severity level: – Green: Temperature is within the normal operating range. – Orange: Temperature has reached the warning level. – Red: Temperature has reached the shutdown level.
PORT DISTRIBUTION	Displays the total number of ports per unit; also displays the breakdown of the port count based on the operational status (up, down, and disable).
PoE UTILIZATION	Displays the total number of watts available for consumption; also displays the breakdown of consumed and free power per unit.
AVERAGE CPU UTILIZATION	Displays the percentage of CPU being used by the device at 5-second, 1-minute, and 500-second intervals.
MEMORY USAGE	Displays the total number of megabytes in dynamic memory, including the number of megabytes that are used, and the percentage of the available memory.

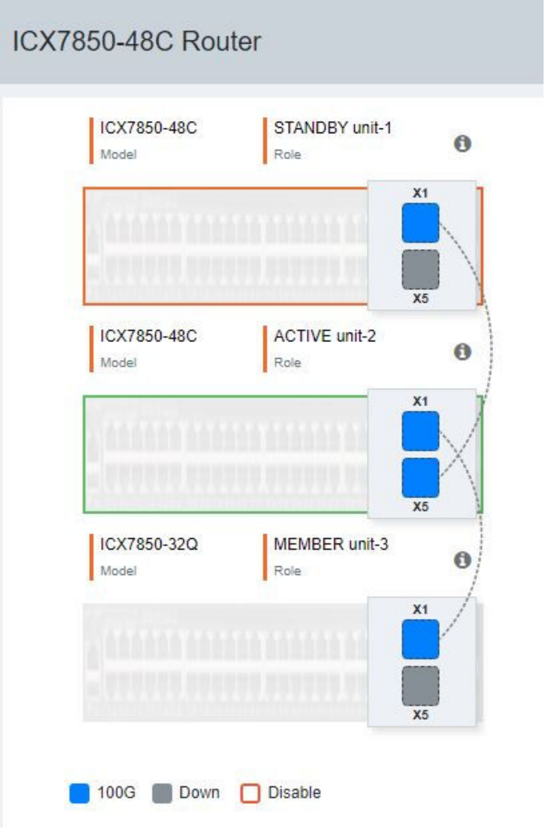
Displaying Stack Details

A stack is a group of devices that operate as a single chassis. A RUCKUS stack contains 2 to 12 units configured in a ring or linear topology. The units in a stack are from the same model family; for example, a stack can be an ICX 7150 stack or an ICX 7250 stack, but it cannot combine ICX 7150 and ICX 7250 devices. Stack members can be physically separated or located together. For example, top-of-rack (ToR) switches can form a stack that acts as a single switch to manage data center access. Stack members can be physically separated, and the distance between stacking members depends on the type of connector cables used.

Complete the following steps to display stack details.

1. On the menu, click **Stack**. In the main pane you can view the stack topology, stacking ports, and connection details, among other information. Only the connected and configured ports are displayed.

   FIGURE 7 Stack Information



ICX7850-48C Router

ICX7850-48C
Model

STANDBY unit-1
Role

ICX7850-48C
Model

ACTIVE unit-2
Role

ICX7850-32Q
Model

MEMBER unit-3
Role

The following details are displayed:

- **Model**: Displays the model of the ICX device that is part of the stack.
- **Role**: Displays the role of the unit within the stack: active, standby, or member.

The color code on each port represents different port speeds displayed at the bottom of the page.

2. Pause the pointer over the ℹ (Information icon) to display the following details:
   - **Unit**: Displays the unit number.
   - **Mac**: Displays the MAC address of the device.
   - **Priority**: Displays the priority assigned to the unit.
   - **State**: Displays the operational state of the unit: local or remote.
   - **Comment**: Displays additional information about the unit.

Port Settings

Port Settings Overview

The properties of all configured ports can be viewed and modified. On the menu, click **Port Settings** to display the properties of all configured ports.

The following options for updating the port settings are available:

- Basic settings: Options that are frequently changed by the user can be modified in the **Basic Setting** tab.
- Advanced settings: Options that are changed less frequently by the user can be modified in the **Advanced Setting** tab.
- Bulk edit: The port status, port speed, and the maximum advertised speed for the port can be changed for several selected or all ports at once.

Configuring Port Settings

The settings for a specific port, or all configured ports, can be modified, including the port name, status, and speed. Various security settings can be enabled or disabled.

Complete the following steps to update the settings for a configured port, and to make bulk updates to some of the settings for all configured ports.

1. On the menu, click **Port Settings**.

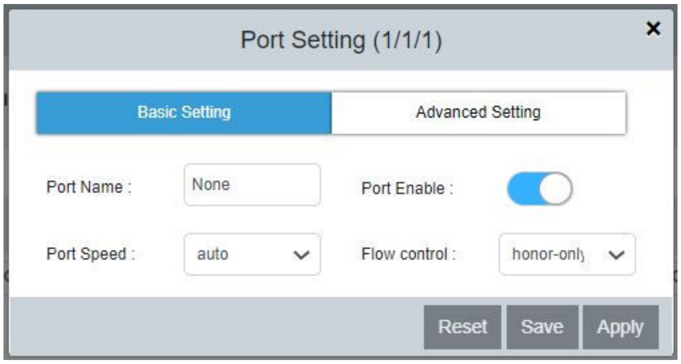
   The configured ports are listed on the main pane. You can perform the following actions:

   - Configure Symmetric Flow Control (globally): For more information, refer to Configuring Symmetric Flow Control on page 24.
   - Configure Flow Control (globally): For more information, refer to Configuring Flow Control on page 24.
   - Edit port settings: To edit port settings, continue to step 2.
   - Bulk edit port settings: To edit port settings for several or all ports, continue to step 6.

2. Click the ✎ (Edit icon) of a port to display the **Port Setting** dialog box.

3. On the **Basic Setting** tab, complete the following fields, as required:

FIGURE 8 Port Setting: Basic Settings



Port Name : None

Port Enable :

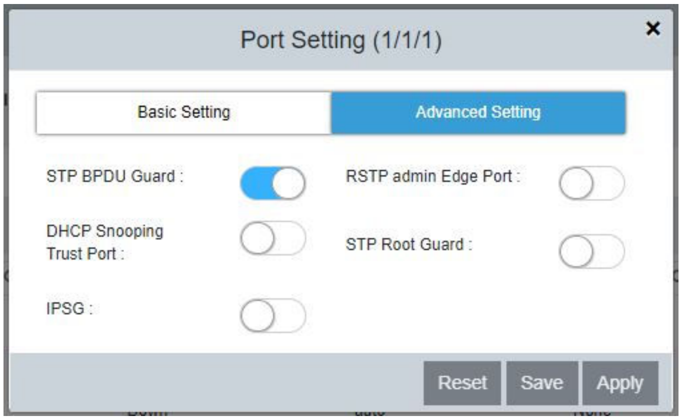
Port Speed : auto

Flow control : honor-onl

- **Port Name**: Enter the updated port name.
- **Port Enable**: Enable or disable the port.
- **Port Speed**: Select the port speed.
- **Flow control**: Select the following options from the dropdown list to configure flow control:
  - **both**: Configures flow control in PAUSE generation and honoring mode.
  - **generate-only**: Configures flow control in PAUSE generation only mode.
  - **honor-only**: Configures flow control in PAUSE honoring mode.
  - **neg-on**: Enables flow control negotiation. If selected, flow control is enabled or disabled depending on the peer advertisement. When flow control is enabled globally and auto-negotiation is on, flow control is advertised on 10/100/1000M ports. If auto-negotiation is off or if the port speed was configured manually, then flow control is not negotiated with or advertised to the peer.
  - **None**: Disables flow control configurations.
- **PoE Enable** (Available only for PoE-capable ports): Enable or disable the port for PoE.
- **PoE Priority** (Available only for PoE-capable ports): Select the priority.

4. On the **Advanced Setting** tab, complete the following fields, as required:

FIGURE 9 Port Setting: Advanced Settings



STP BPDU Guard : ●

DHCP Snooping Trust Port : ○

IPSG : ○

RSTP admin Edge Port : ○

STP Root Guard : ○

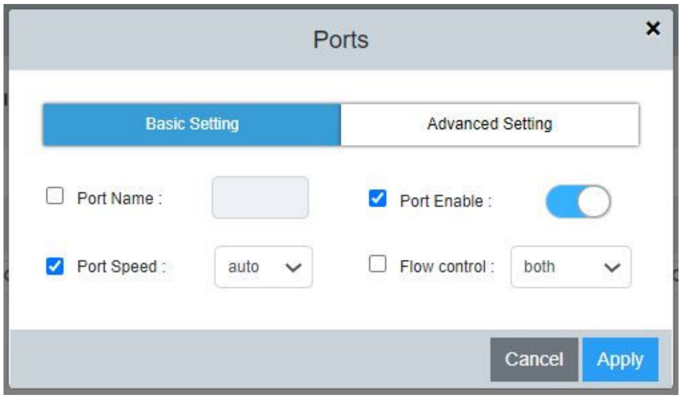
- **STP BPDU Guard**: Enable or disable the STP BPDU Guard on the port.
- **DHCP Snooping Trust Port**: Enable or disable trust for the port.
- **IPSG**: Enable or disable IP Source Guard (IPSG) protection for the port.
- **RSTP admin Edge Port**: Enable or disable the port as an edge port with Rapid Spanning Tree Protocol (RSTP).
- **STP Root Guard**: Enable or disable STP root guard.
- **Copper GBIC link-config control**: Select the maximum advertised speed for the port.

5. Click **Apply** and click **OK** in the confirmation dialog box to apply the changes.

6. To update the settings for several or all configured ports at once, select the ports that you want to update and click ✎ (Edit icon) of one of the selected ports.

   The **Ports** dialog box is displayed.

FIGURE 10 Ports: Bulk Edit



☐ Port Name :

☑ Port Enable : ●

☑ Port Speed : auto

☐ Flow control : both

7. In the **Basic Setting** tab and **Advanced Setting** tab, select the check box against each setting to enable and make the required changes.
8. Click **Apply** and click **OK** in the confirmation dialog box to apply the changes to the selected ports.

Configuring Symmetric Flow Control

RUCKUS devices support symmetrical flow control (SFC), which means that the ports can both receive and transmit 802.3x PAUSE frames.

To configure symmetric flow control, complete the following steps:

1. On the menu, click **Port Settings**.

   The configured ports are listed on the main pane.

2. **Symmetric Flow Control**: Select the following options from the dropdown list to configure symmetric flow control:

   - **enable**: Enables SFC globally for priorities from 0 through 4 by default and optionally for all priorities from 0 through 7.
   - **all-priorities**: Specifies SFC on all priorities. If you do not specify this option, SFC is enabled only on priorities from 0 through 4.
   - **None**: Disables all SFC configurations.

Configuring Flow Control

Flow control (802.3x) is a QoS mechanism created to manage the flow of data between two full-duplex Ethernet devices. Specifically, a device that is oversubscribed (is receiving more traffic than it can handle) sends an 802.3x PAUSE frame to its link partner to temporarily reduce the amount of data the link partner is transmitting. Without flow control, buffers would overflow, packets would be dropped, and data retransmission would be required. All FastIron devices support asymmetric flow control, which means they can receive PAUSE frames but cannot transmit them. In addition, devices also support symmetrical flow control, which means they can both receive and transmit 802.3x PAUSE frames.

To configure flow control, complete the following steps:

1. On the menu, click **Port Settings**.

   The configured ports are listed on the main pane.

2. **Flow Control**: Select the following options from the dropdown list to configure flow control:

   - **both**: Configures flow control in PAUSE generation and honoring mode.
   - **generate-only**: Configures flow control in PAUSE generation only mode.
   - **honor-only**: Configures flow control in PAUSE honoring mode.
   - **None**: Disables flow control configurations.

Layer 2

Link Aggregation Group

Link aggregation allows you to bundle multiple physical Ethernet links to form a single logical trunk providing enhanced performance and redundancy. The aggregated trunk is referred to as a Link Aggregation Group (LAG). The LAG is viewed as a single logical link by connected devices, the Spanning Tree Protocol (STP), IEEE 802.1Q VLANs, and so on. When one physical link in the LAG fails, the other links stay up. A small drop in traffic is experienced when the link carrying the traffic fails. To configure links to form a LAG, the physical links must be of the same speed.

You can use a single interface to configure any of the following LAG types:

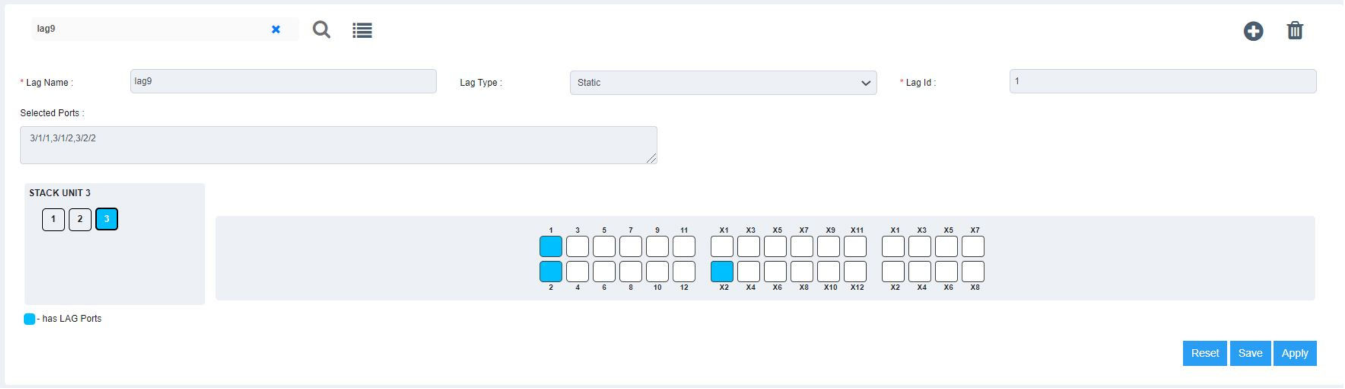
- Static LAGs: Static LAGs are manually configured aggregate links containing multiple ports. In static link aggregation, links are added into a LAG without exchanging any control packets between the partner systems. The distribution and collection of frames on static links is determined by the operational status and administrative state of the link.
- Dynamic LAGs: A dynamic LAG type uses the Link Aggregation Control Protocol (LACP), to maintain aggregate links over multiple ports. Typically, two partner systems sharing multiple physical Ethernet links can aggregate a number of those physical links using LACP. LACP creates a LAG on both partner systems and identifies the LAG by the LAG ID. All links with the same administrative key, and all links that are connected to the same partner switch become members of the LAG. LACP PDUs are exchanged between ports on each device to determine if the connection is active. The LAG shuts down ports if their connections are no longer active.
- Keep-alive LAGs: In a keep-alive LAG, a single connection between a single port on two RUCKUS devices is established. In a keep-alive LAG, LACP PDUs are exchanged between the two ports to determine if the connection between the devices is still active. If it is determined that the connection is no longer active, the ports are blocked.

Configuring a Link Aggregation Group

Complete the following steps to configure a Link Aggregation Group (LAG).

1. On the menu, click **Layer 2** > **LAG**.

   FIGURE 11 Link Aggregation Group Configuration



lag9 ✖

* Lag Name : lag9

Lag Type : Static

* Lag Id : 1

Selected Ports : 3/1/1,3/1/2,3/2/2

STACK UNIT 3

1 2 3

🟦 - has LAG Ports

Reset Save Apply

   You can perform the following actions:

   - Add a LAG: Continue to step 2 to configure a new LAG.
   - Search and view existing LAGs: To view existing LAGs, follow one of the following methods:
     - Click ☰ (List LAGs icon) and the configured LAGs appear as a list. Select a LAG to view the configuration details.
     - Click inside the search field after clicking "x" to search for the configured LAGs. Search the LAG by name or ID in the search field to view the configuration details.
   - Edit a LAG: Select an existing LAG from the list. Click the required ports to add or remove the ports from the LAG.

     NOTE
     You cannot edit the LAG type or the LAG ID from the Web Management Interface.

   - Delete a LAG: Select a configured LAG from the list and click 🗑 (Delete LAG icon). The **Delete LAG** confirmation dialog box is displayed. Click **Apply** to delete the selected LAG.

2. Click ⊕ (Add icon) to create a new LAG.
3. Complete the following fields:
   - **Lag Name**: Enter a name for the LAG. The LAG name can be up to 64 characters in length.
   - **Lag Type**: From the dropdown list, select the type of LAG that you want to create:
     - **Static**: Configures a static LAG.
     - **Dynamic**: Configures a dynamic LAG.
     - **Keep-alive**: Configures a keep-alive LAG.
   - **Lag Id**: Enter an ID for the LAG. The LAG ID parameter is applicable for static and dynamic LAGs only. No explicit configuration of a LAG ID is allowed for keep-alive LAGs.

4. Add ports to the LAG by performing the following actions:
    a) Select a unit ID box in the **STACK UNIT** panel to view the corresponding port panel of the stack unit.
    b) Select the ports that you want to add to the LAG from the ports panel.

        The ports that are added to LAG are displayed in the **Selected Ports** panel. To deselect a port, click the selected port again on the ports panel.

        The color code of the stack unit indicates that the ports of that unit are associated with the LAG. The color of the ports in the ports panel indicates that the ports are part of the LAG.
5. Click **Apply** and click **OK** in the confirmation dialog box to apply the LAG configuration to the device.

VLAN

A virtual LAN (VLAN) is used to partition a computer network at Layer 2 into a broadcast domain, which is uniquely identified by a VLAN ID. A VLAN helps to split a network that acts as a separate network, but is connected to a physical network. Using VLAN tagging, the network administrators can virtually group networks together even if they are not physically connected to the same network switch.

By default, all the ports on a RUCKUS device are members of the default VLAN. Thus, all the ports on the device constitute a single Layer 2 broadcast domain. On all RUCKUS devices, you can configure port-based VLANs. A port-based VLAN is a subset of ports on a RUCKUS device that constitutes a Layer 2 broadcast domain.

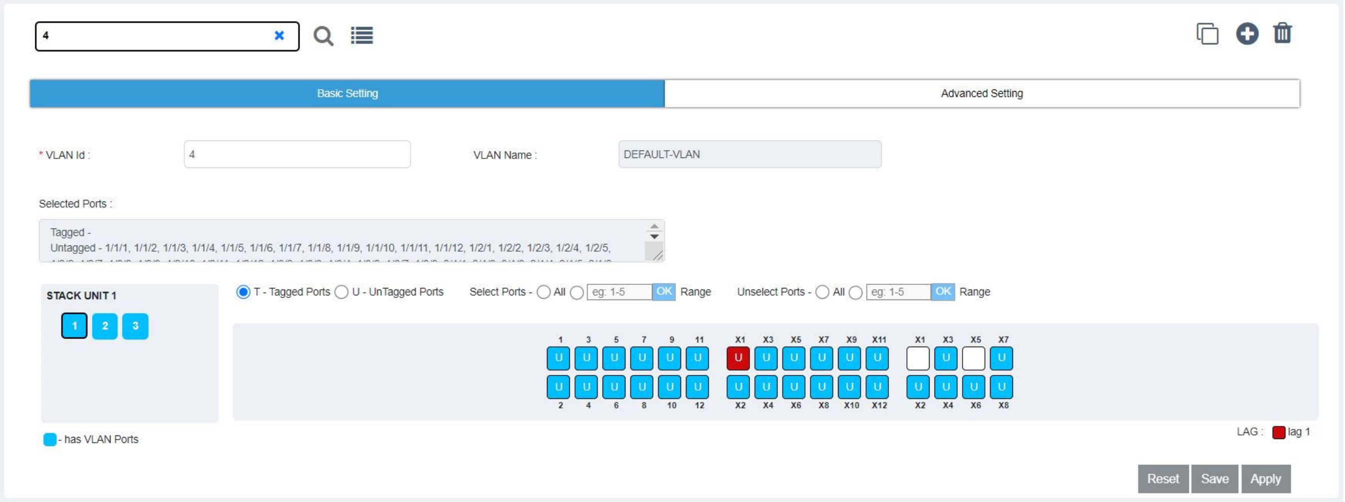
You can configure multiple port-based VLANs. You can configure up to 4094 port-based VLANs on a Layer 2 switch or Layer 3 switch. On both device types, valid VLAN IDs are 1 through 4095. You can configure up to the maximum number of VLANs within the ID range.

Configuring a VLAN

Complete the following steps to configure VLAN.

1. On the menu, click **Layer 2** > **VLAN**.

   FIGURE 12 Configuring a VLAN: Basic Settings

   4 ✖

   Basic Setting | Advanced Setting

   * VLAN Id : 4
   VLAN Name : DEFAULT-VLAN

   Selected Ports :
   Tagged -
   Untagged - 1/1/1, 1/1/2, 1/1/3, 1/1/4, 1/1/5, 1/1/6, 1/1/7, 1/1/8, 1/1/9, 1/1/10, 1/1/11, 1/1/12, 1/2/1, 1/2/2, 1/2/3, 1/2/4, 1/2/5,

   ● T - Tagged Ports ○ U - UnTagged Ports Select Ports - ○ All ○ eg: 1-5 OK Range Unselect Ports - ○ All ○ eg: 1-5 OK Range

   You can perform the following actions:

   - Clone a VLAN: Refer to Cloning a VLAN on page 30 to know more informaton about VLAN cloning.
   - Add a VLAN: Continue to step 2 to configure a new VLAN.
   - Search and view existing VLANs: To view existing VLANs, follow one of the following methods:
     - Click ☰ (List VLANs icon) and the configured VLANs appear as a list. Select a VLAN to view the configuration details.
     - Search the VLAN by name or ID in the search field to view the configuration details.
   - Edit a VLAN: Select an existing VLAN from the list. Click the required ports to add or remove the ports from the VLAN. Make necessary changes and click **Apply**.

     NOTE
     If you want to use the VLAN ID "VLAN 1" as a configurable VLAN, you can assign a different VLAN ID to the default VLAN. You must specify a valid VLAN ID that is not already in use. Reassigning a different VLAN ID to the default VLAN does not change the properties of the default VLAN, but allows you to use the VLAN ID "1" as a configurable VLAN.

     NOTE
     VLAN name is non-editable after a VLAN is configured.

   - Delete a VLAN: Select a configured VLAN from the list and click 🗑 (Delete VLAN icon). The **Delete VLAN** confirmation dialog box is displayed. Click **Apply** to delete the selected VLAN.

2. Click ⊕ (Add icon) to create a new VLAN.

3. Complete the following fields:
   - **VLAN Id**: Enter an ID for the VLAN.

     You can configure up to 4094 port-based VLANs on a Layer 2 Switch or Layer 3 Switch. On both device types, valid VLAN IDs are 1 - 4095. You can configure up to the maximum number of VLANs within that ID range. By default, all the ports on a RUCKUS device are in a single port-based VLAN. This VLAN is called the DEFAULT-VLAN and is VLAN number 1.
   - **VLAN Name**: Enter a name for the VLAN. The name can be up to 32 characters in length.
4. In the **Basic Setting** tab, add ports to the VLAN by performing the following actions:

   a) Select a unit ID box in the **STACK UNIT** panel to view the corresponding port panel of the stack unit.

   b) To add tagged ports, select **T-Tagged Ports** and click the required ports on the ports panel. To remove the added ports, click the selected ports again on the ports panel.

   c) To add untagged ports, select **U-UnTagged Ports** and click the required ports on the ports panel. To remove the added ports, click the selected ports again on the ports panel.

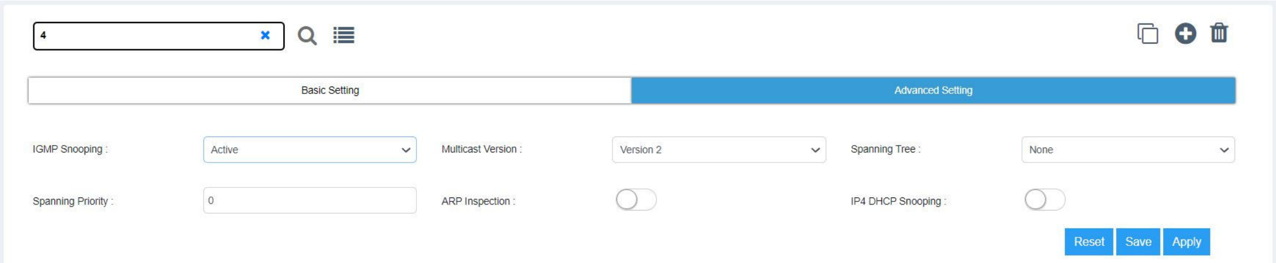
   The color code of the stack unit indicates that the ports of that unit are associated with the VLAN. The color of the ports in the ports panel that the ports are part of the VLAN. The letter T represents a tagged port and the letter U represents an untagged port.

   d) Choose the following options common to tagged ports and untagged ports:
   - **Select Ports**: Select and add multiple ports to the VLAN.
     - **All**: Select and add all ports.
     - **Range**: Enter a range of ports and click **OK** to add the range of ports.

     The ports that are added to the VLAN are displayed in the **Selected Ports** panel.
   - **Unselect Ports**: Remove multiple ports from the VLAN.
     - **All**: Select and remove all ports.
     - **Range**: Enter a range of ports and click **OK** to remove the range of ports.

5. In the **Advanced Setting** tab, configure the required features at the VLAN level:

FIGURE 13 Configuring a VLAN: Advanced Settings



IGMP Snooping : Active
Multicast Version : Version 2
Spanning Tree : None
Spanning Priority : 0
ARP Inspection : ○
IP4 DHCP Snooping : ○

- **IGMP Snooping**: Configures IGMP snooping for a VLAN, and sets the IGMP mode as active or passive.
  - **Active**: Configures IGMP active mode so that the device actively sends out IGMP queries to identify multicast groups on the network, and makes entries in the IGMP table based on the group membership reports it receives.
  - **Passive**: Configures IGMP passive mode so that the device does not send queries but forwards reports to the router ports that receive queries. When passive mode is configured on a VLAN, queries are forwarded to the entire VLAN.
- **Multicast Version**: Configures the IGMP version for snooping on a VLAN.
  - **Version 2**: Configures IGMP version 2.
  - **Version 3**: Configures IGMP version 3.
- **Spanning Tree**
  - STP: Enables STP on a VLAN.
  - RSTP: Enables 802.1w on a VLAN.
- **Spanning Priority**: Configures the priority of the bridge in a spanning tree (instance of STP). The bridge with the lowest value has the highest priority and is the root. A higher numerical value means a lower priority; thus, the highest priority is 0.
- **ARP Inspection**: Enables or disables ARP inspection.
- **IP4 DHCP Snooping**: Enables or disables IP4 DHCP snooping.

6. Click **Apply**. The **Port Setting** dialog box is displayed which shows the tagged and untagged ports that are selected and removed as part of the VLAN configuration.
7. Click **OK** to apply the VLAN configuration to the device.

Cloning a VLAN

An existing VLAN can be cloned to create a new VLAN with all the configurations of the originally configured VLAN.

To clone a VLAN, complete the following steps:

1. On the menu, click **Layer 2** > **VLAN**.
2. Select an existing VLAN from the list.
3. Click ⧉ (Clone VLAN icon). The **VLAN Id** field becomes editable.
4. In the **VLAN Id** field specify a valid VLAN ID that is not already in use.
5. Click **Apply** to clone the existing VLAN and create a new VLAN with all the configurations of the originally configured VLAN.

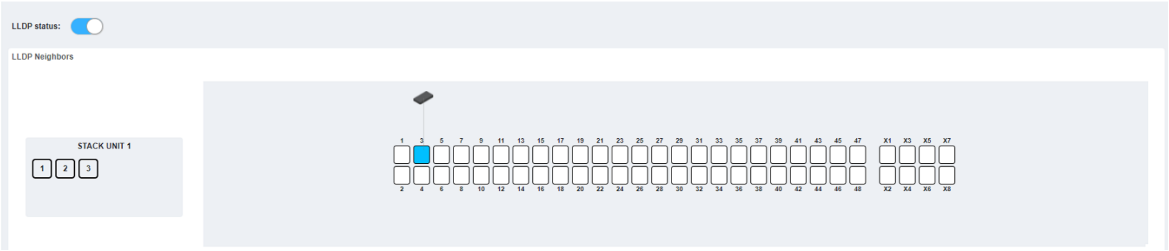
Monitoring LLDP Neighbors

Link Layer Discovery Protocol (LLDP) is a Layer 2 neighbor discovery protocol that allows devices to advertise device information to other devices on the network. LLDP enables a station attached to an IEEE 802 LAN or MAN to advertise its capabilities to, and to discover, other stations in the same 802 LAN segments. By default, the system capabilities are automatically advertised when LLDP is enabled on a global basis.

Complete the following steps to view the LLDP neighbor devices and the ports through which they are connected.

1. On the menu, click **Layer 2** > **LLDP**.

   FIGURE 14 Displaying LLDP Neighbor Devices

2. Click **LLDP status** to enable or disable LLDP globally.

   LLDP is enabled by default.

3. Select a unit ID box in the stack panel to view the corresponding ports panel of the stack unit.

   All the LLDP neighbor devices in the network and the ports to which they are connected are displayed.

4. Pause the pointer over a remote device to view the device information such as port number, name, device type, and the MAC address.
5. Pause the pointer over a connecting port to view the MAC address.

Layer 3

Configuring IP Static Routes

Static routes are manually configured entries in the IP routing table. You can configure a static IP route and specify the destination address for the route and the next-hop gateway through which the Layer 3 device can reach the route.

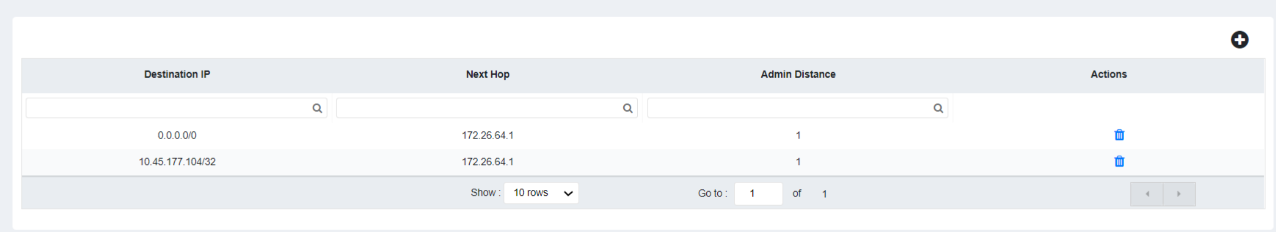
In Switch image, Layer3 options will not be displayed under the menu.

Complete the following steps to configure an IP static route and add an administrative distance to the static route.

1. On the menu, click **Layer 3** > **Routes**.

   The configured routes are listed on the main pane.

   FIGURE 15 IP Routes



Destination IP	Next Hop	Admin Distance	Actions
0.0.0.0/0	172.26.64.1	1	🗑
10.45.177.104/32	172.26.64.1	1	🗑

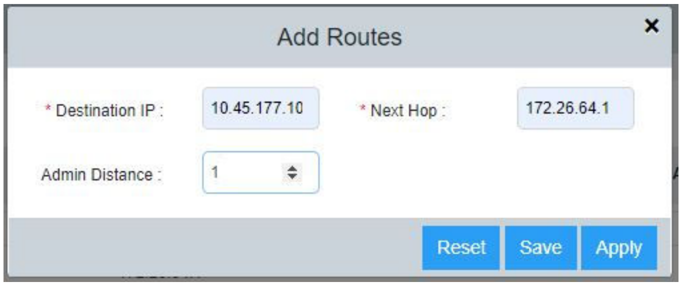
Show : 10 rows   Go to : 1 of 1

   You can perform the following actions:

   - Add a route: Continue to step 2 to add a new IP static route.
   - Delete a route: Click 🗑 (Delete icon) to display the **Delete Routes** dialog box. Click **Apply** to delete the specified IP static route.

2. Click ⊕ (Add icon) to display the **Add Routes** dialog box.

   FIGURE 16 Adding Routes



Add Routes

* Destination IP : 10.45.177.10   * Next Hop : 172.26.64.1

Admin Distance : 1

3. Complete the following fields:
   - **Destination IP**: Enter the destination IP address and subnet mask for the route path.
   - **Next Hop**: Enter the IP address for the next hop.
   - **Admin Distance**: Enter the administrative distance of the route.
4. Click **Apply** to create the IP static route.

Configuring a VE Port

Complete the following steps to configure a VE interface, add an IP address and network mask for the interface, and associate a helper IP address with the interface.

In Switch image, Layer3 options will not be displayed under the menu.

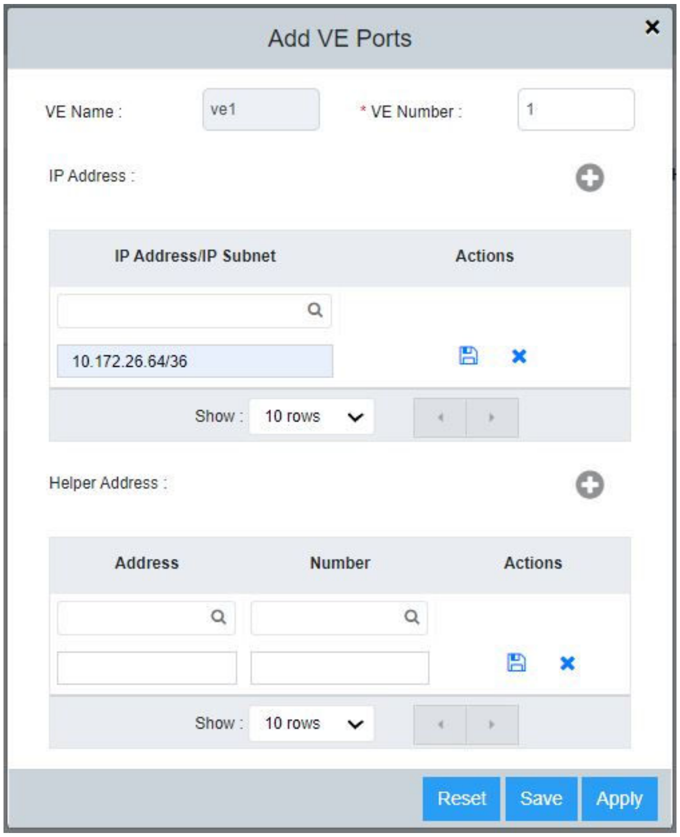
1. On the menu, click **Layer 3** > **VE**.

   All the configured Virtual Ethernet (VE) ports are listed on the main pane.

   You can perform the following actions:
   - Add a VE port: Continue to step 2 to add a new VE port.
   - Edit a VE Port: Click ✎ (Edit icon) to display the **Ve Ports** dialog box. Make necessary changes and click **Apply** to apply the changes.
   - Delete a VE Port: Click 🗑 (Delete icon) to display the **Delete VE Ports** dialog box. Click **Apply** to delete the specified VE port.

2. Click ⊕ (Add icon) to display the **Add VE Ports** dialog box.

FIGURE 17 Adding VE Ports



Add VE Ports

VE Name : ve1

* VE Number : 1

IP Address :

IP Address/IP Subnet	Actions
10.172.26.64/36	💾 ✖

Helper Address :

Address	Number	Actions
		💾 ✖

3. Complete the following fields:
   - **VE Number**: Enter the number of the VE port.

     NOTE
     VE is created only if corresponding VLAN is present in the device.

   - **IP Address/IP Subnet**: Enter the IP address and network mask. Click ⊕ to add the IP address and network mask. Click 💾 (Save icon) to add the entry. You can further add AP addresses by clicking ⊕ (Add icon).
   - **Helper Address**: Enter the helper address. Click ⊕ to add the helper address. Click 💾 (Save icon) to add the entry.

     NOTE
     Helper address is displayed only if VE IP address is configured.

   The **VE Name** field is automatically populated after you enter the number of the VE port. The helper address needs to be entered only once and applies to VE ports configured thereafter.
4. Click **Apply** and click **OK** in the confirmation dialog box to create the VE port.

Management

Configuring an ICX Device to be Managed by SmartZone

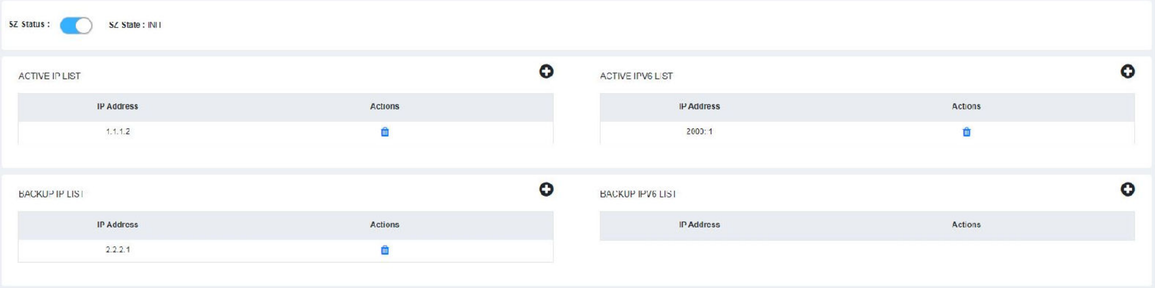
Beginning with SmartZone 5.0, SmartZone can be used to monitor and manage ICX switches. ICX devices running either router or switch images can be managed by SmartZone. An ICX switch identifies SmartZone and initiates a connection based on the SmartZone IP addresses configured on the switch or discovered through DHCP Option 43. When SmartZone management is disabled, the ICX switch will not initiate a connection with SmartZone, even if SmartZone IP addresses are available. Both "active" and "backup" SmartZone IP addresses can be configured on the ICX switch. Active IP addresses are given the highest priority; backup IP addresses are lowest priority and are provided for redundancy. Both IPv4 addresses and IPv6 addresses can be added. You can add up to three IP addresses each for active and backup IP addresses. The ICX device attempts to create a connection beginning with the first IP address. If the attempt fails, the ICX device moves to the second and then the third IP address.

Complete the following steps to configure an ICX device to be managed by SmartZone.

1. On the menu, click **Management** > **SmartZone**.

   The SmartZone connection status and the SmartZone IP addresses configured on the device are displayed in the main pane.

   FIGURE 18 SmartZone Connections

   SZ Status : ● SZ State : INIT

   ACTIVE IP LIST

IP Address	Actions
1.1.1.2	🗑

   ACTIVE IPV6 LIST

IP Address	Actions
2000::1	🗑

   BACKUP IP LIST

IP Address	Actions
2.2.2.1	🗑

   BACKUP IPV6 LIST

IP Address	Actions

   You can perform the following actions:

   - Enable or disable SmartZone status: Click **SZ Status** to enable or disable SmartZone management of the ICX device.
   - Add SmartZone IP addresses: Continue to step 2 to add active and backup SmartZone IP addresses.
   - Delete SmartZone IP addresses: Click 🗑 (Delete icon) to display **SZ IP** confirmation dialog box. Click **Apply** to delete the IP address.

2. Perform the following actions to add active SmartZone IP addresses.

   a) Under **ACTIVE IP LIST** and **ACTIVE IPv6 LIST**, click ⊕ (Add icon) to display a new field to add an active SmartZone IPv4 or IPv6 address.

   b) Click 💾 (Save icon) and click **Apply** in the confirmation dialog box to add the active IPv4 or IPv6 address.

3. Perform the following actions to add backup SmartZone IP addresses.

   a) Under **BACKUP IP LIST** and **BACKUP IPv6 LIST**, click ⊕ (Add icon) to display a new field to add a passive SmartZone IPv4 or IPv6 address.

   b) Click 💾 (Save icon) and click **Apply** in the confirmation dialog box to add the passive IPv4 or IPv6 address.

Configuring Domain Name System Servers

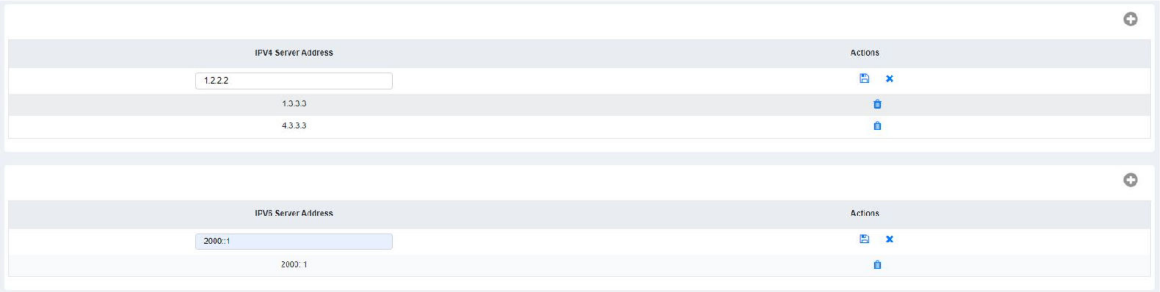
The Domain Name System (DNS) resolver is a feature in a Layer 2 or Layer 3 device that sends and receives queries to and from the DNS server on behalf of a client. You can configure the RUCKUS device to recognize DNS servers. You can configure only up to four IPv4 server addresses and four IPv6 server addresses. The first entry serves as the default primary address. If a query to the primary address fails to be resolved after three attempts, the next DNS address is queried (also up to three times). This process continues for each defined DNS address until the query is resolved. The order in which the default DNS addresses are polled is the same as the order in which you enter them.

Complete the following steps to configure DNS servers.

1. On the menu, click **Management** > **DNS Server**.

   All DNS server address information is displayed for the IPv4 DNS servers and the IPv6 DNS servers.

   FIGURE 19 DNS Server Addresses



IPV4 Server Address	Actions
1.2.2.2	💾 ✖
1.3.3.3	🗑
4.3.3.3	🗑

IPV6 Server Address	Actions
2000::1	💾 ✖
2000::1	🗑

2. To add an IPv4 server address, click ⊕ (Add icon) in the top right corner of the **IPv4 Server Address** table.

   A new field is added in the **IPv4 Server Address** table.

   a) Enter the IPv4 address of the DNS server.

   b) Click 💾 and click **Apply** in the confirmation dialog box to add the IPv4 DNS server address. You can add additional IPv4 addresses by clicking ⊕ (Add icon).

      NOTE
      Only four IPv4 server addresses can be saved.

3. To add an IPv6 server address, click (Add icon) in the top right corner of the **IPv6 Server Address** table.

   A new field is added in the **IPv6 Server Address** table.

   a) Enter the IPv6 address of the DNS server.

   b) Click and click **Apply** in the confirmation dialog box to add the IPv6 DNS server address. You can add additional IPv6 addresses by clicking (Add icon).

      NOTE
      Only four IPv6 server addresses can be saved.

4. To delete an IPv4 or IPv6 server address, click (Delete icon) for the corresponding IPv4 or IPv6 server address.

Upgrading FastIron Software

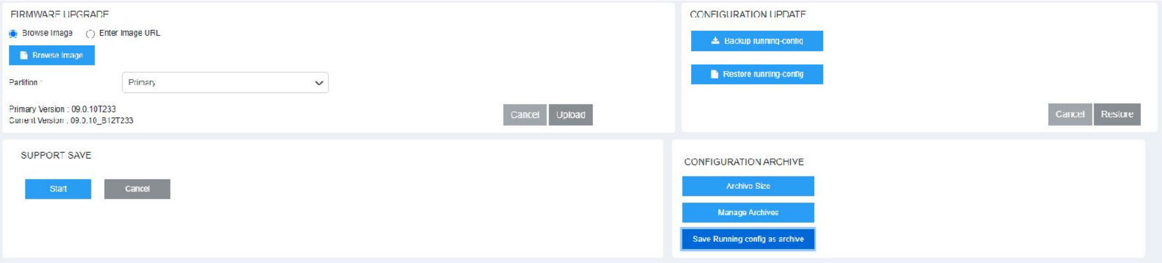
A FastIron device can be upgraded to the latest software version to take advantage of new features and ensure optimal network performance.

NOTE
Download the required software images for the target release to your local machine from the Software Downloads page on the RUCKUS Support website. For the list of software image files available for a FastIron device, refer to the release notes for the specific release.

Complete the following steps to upgrade the software.

1. On the menu, click **Management** > **Infra**.

   FIGURE 20 FastIron Firmware Upgrade



FIRMWARE UPGRADE

● Browse Image ○ Enter Image URL

Partition : Primary

Primary Version : 09.0.10T233
Current Version : 09.0.10_B12T233

CONFIGURATION UPDATE

SUPPORT SAVE

CONFIGURATION ARCHIVE

2. In the **FIRMWARE UPGRADE** pane, flash the new image to the device using one of the following options:
   - **Browse Image**: Browse and select the file from the local machine.
   - **Enter Image URL**: Enter the URL where the image file is present. Only https image download is supported. For example https://10.171.17.67/SPR09000_b201ufi.bin
3. In the **Partition** list, select one of the following flash memory modules:
   - **Primary**: Specifies to upload the software image to the primary flash memory.
   - **Secondary**: Specifies to upload the software image to the secondary flash memory.
4. Click **Upload** to upload and upgrade the software.

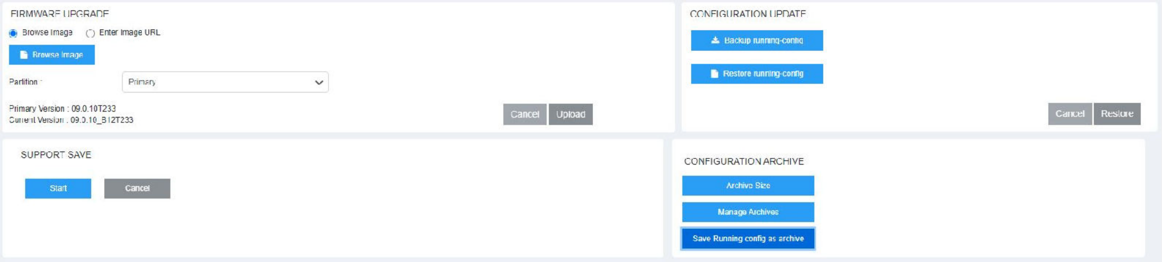
Managing Running Configuration Backups

The running configuration file stores the configuration that is currently active on the device, including any changes applied in any management sessions since the last reboot. The running configuration file is not persistent; that is, the configuration changes made while the device is running are not retained after a reboot. You can back upthe running configuration file to a local machine and restore the file at a later point in time based on your requirements.

Complete the following steps to back up the running configuration file.

1. On the menu, click **Management** > **Infra**.

   FIGURE 21 Managing the Running Configuration File

   Partition : Primary

   Primary Version : 09.0.10T233
   Current Version : 09.0.10_B12T233

2. In the **CONFIGURATION UPDATE** pane, click **Backup running-config**.

   The running configuration is downloaded to the local machine.

Restoring the Running Configuration

Complete the following steps to restore the running configuration file.

1. On the menu, click **Management** > **Infra**.
2. In the **CONFIGURATION UPDATE** pane, click **Restore running-config**.
3. Browse and select the saved running configuration file.
4. Click **Restore** to restore the running configuration file to the device.

Configuration Archive

ICX devices can manage multiple configuration files in flash, providing the flexibility to save multiple configuration files and to change the system configuration when needed. An archive is a text file to change the system configuration with the same syntax as a startup-config.txt file. You can create, copy, and delete archives. Archives are saved in a designated folder in the flash memory. Archive naming convention requires archive names to be prefixed with a pre-defined string 'ICX7K_ARCHIVE'. This feature is supported on all RUCKUS ICX 7xxx series devices.

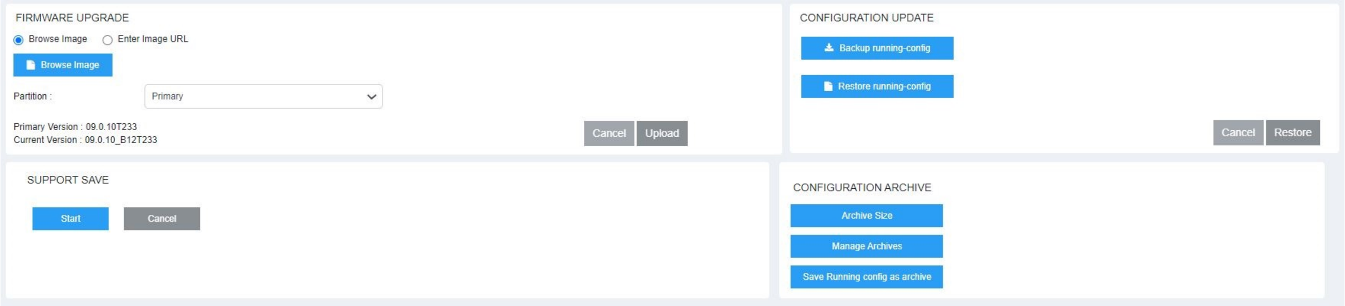
Configuring Archive Size

Archive size, which is a user configurable value, determines the number of archives the system can maintain. Valid values range from 5 through 100. The default maximum value for archive size is 100.

Complete the following steps to configure archive size.

1. On the menu, click **Management** > **Infra**.

   FIGURE 22 Configuration Archive - Archive Size

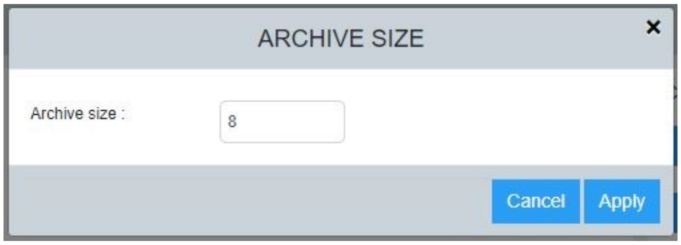
   Partition : Primary

   Primary Version : 09.0.10T233
   Current Version : 09.0.10_B12T233

2. In the **CONFIGURATION ARCHIVE** pane, click **Archive Size**.

   The **ARCHIVE SIZE** dialog box is displayed.

   FIGURE 23 Setting Archive Size

   Archive size : 8

3. In the **Archive size** field, enter a value to change the archive size.

   Valid values range from 5 through 100. The default is 100.

   If the existing number of archives in the system is greater than the user-configured archive size value, the old archives get deleted. For example, if the existing number of archives in the system is 8, and the user configures the archive size value as 6, the oldest 2 archive files that are to be deleted are listed in the window. However, if the user sets the archive size to value higher than the existing number of archive files, no archives are deleted.

4. Click **Apply**. A message is displayed to indicate that the archive size is changed successfully along with details of the old value and newly configured value.

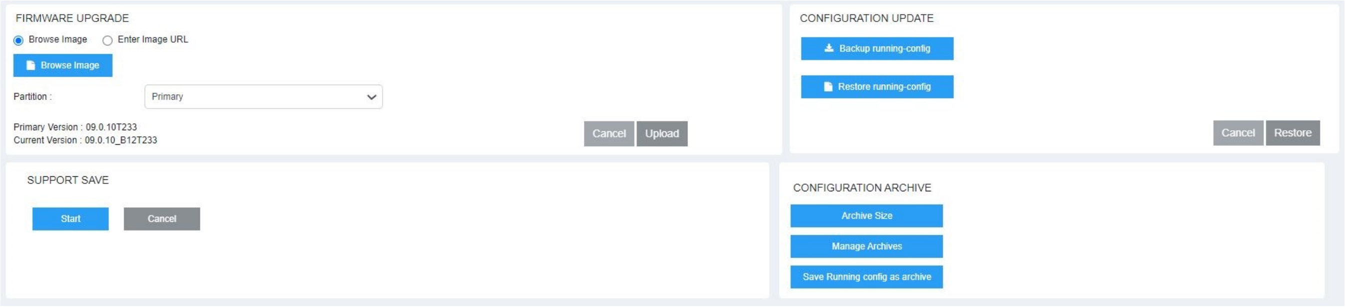
Saving Running Configuration as Archive File

The current running configuration in the system can be saved as archive files.

Complete the following steps to save the running configuration as archive file.

1. On the menu, click **Management** > **Infra**.

   FIGURE 24 Configuration Archive - Saving Running Config

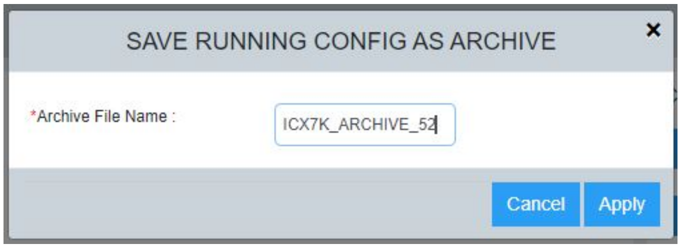
   Partition : Primary

   Primary Version : 09.0.10T233
   Current Version : 09.0.10_B12T233

2. In the **CONFIGURATION ARCHIVE** pane, click **Save Running config as archive**.

   The **SAVE RUNNING CONFIG AS ARCHIVE** dialog box is displayed.

   FIGURE 25 Save Running Config as Archive

   *Archive File Name : ICX7K_ARCHIVE_52

3. In the **Archive File Name** field, enter a name as per the archive naming convention (prefixed with a pre-defined string 'ICX7K_ARCHIVE’).

   If a configuration archive with same name exists, the running configuration will not be saved.

   If the number of archives in the system exceeds the configured archive size with the addition of the new archive file, the oldest archive file that needs to be deleted gets listed.

4. Click **Apply** to save the running configuration as archive file. A message is displayed to indicate that the data is saved succesffully.

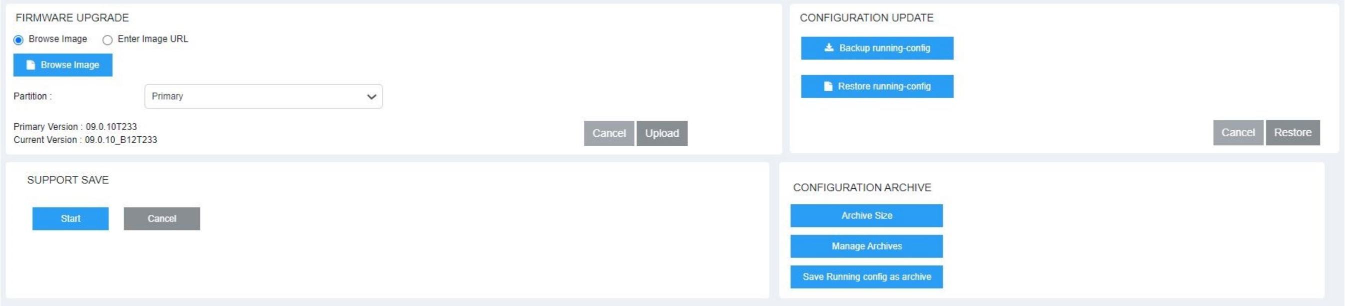
Managing Configuration Archives

You can perform various actions as part of managing the configuration archives. The system allows you to list, view, apply, copy, and delete the config archives.

Complete the following steps to see the exiting archives in the system.

1. On the menu, click **Management** > **Infra**.

   FIGURE 26 Configuration Archive - Manage Archives



FIRMWARE UPGRADE

● Browse Image ○ Enter Image URL

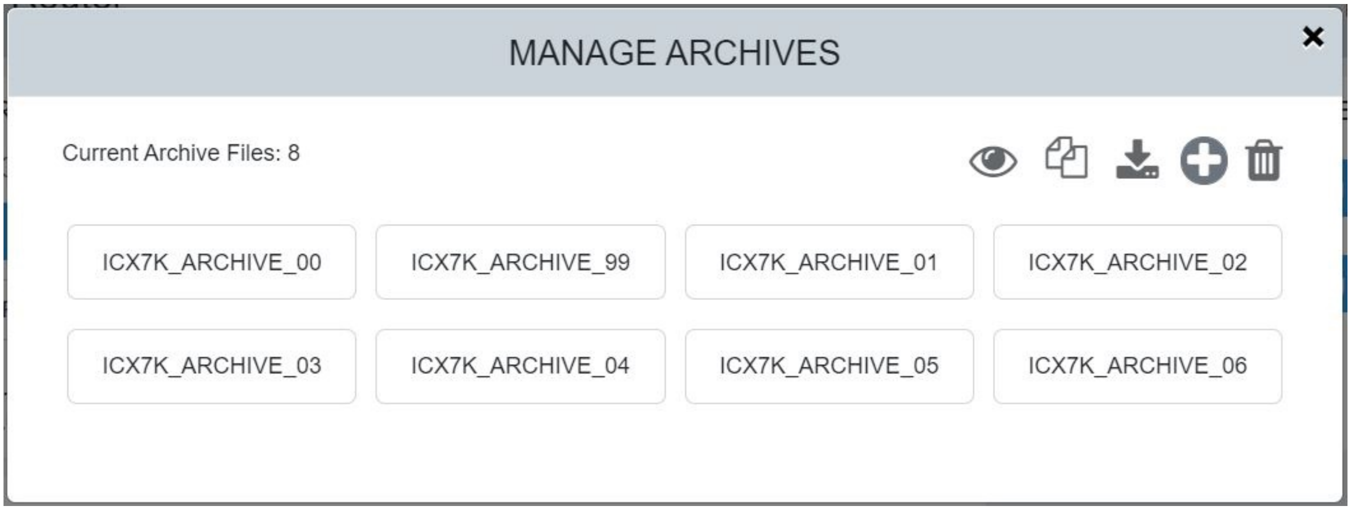
Partition : Primary

Primary Version : 09.0.10T233
Current Version : 09.0.10_B12T233

2. In the **CONFIGURATION ARCHIVE** pane, click **Manage Archives**.

   The **MANAGE ARCHIVES** dialog box is displayed. All the current config archives existing in the system are listed.

   FIGURE 27 Manage Archives



MANAGE ARCHIVES

Current Archive Files: 8

ICX7K_ARCHIVE_00
ICX7K_ARCHIVE_99
ICX7K_ARCHIVE_01
ICX7K_ARCHIVE_02
ICX7K_ARCHIVE_03
ICX7K_ARCHIVE_04
ICX7K_ARCHIVE_05
ICX7K_ARCHIVE_06

You can perform the following actions:

- View the content of a specific archive
- Copy an archive to another archive
- Apply and reload the system with a specific archive without changing the startup configuration
- Delete config archives

Viewing Archive Content

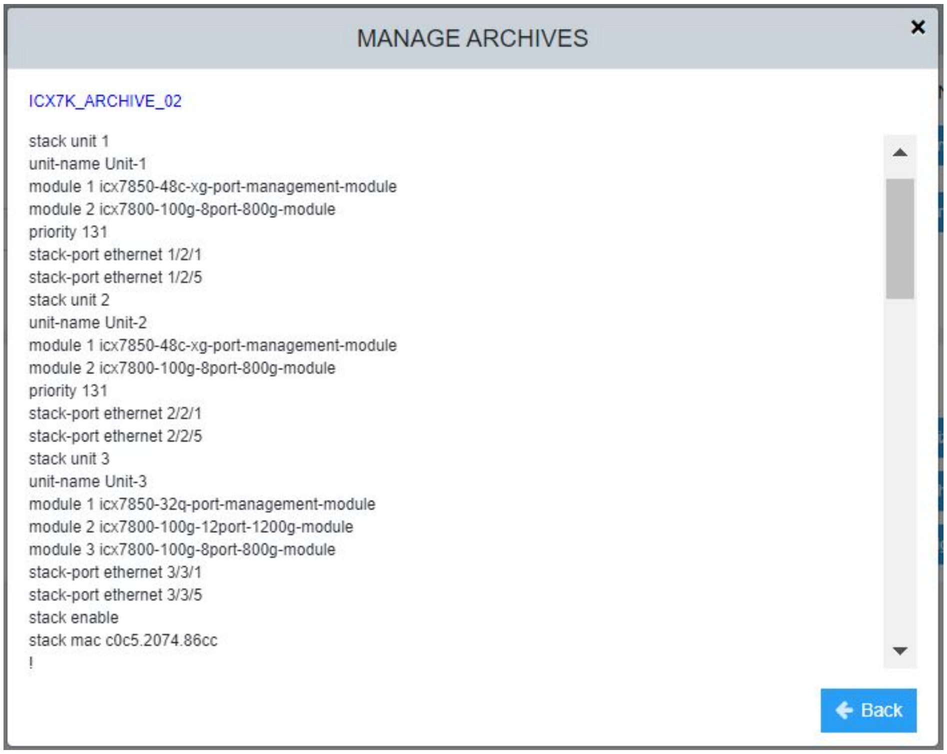
Complete the following steps to display the content of a specific archive.

1. On the menu, click **Management** > **Infra**.
2. In the **CONFIGURATION ARCHIVE** pane, click **Manage Archives**.

   The **MANAGE ARCHIVES** dialog box is displayed.

3. Select a config archive and click 👁 (View) icon to display the content of the selected config archive.

   FIGURE 28 View Archive Content



```
stack unit 1
unit-name Unit-1
module 1 icx7850-48c-xg-port-management-module
module 2 icx7800-100g-8port-800g-module
priority 131
stack-port ethernet 1/2/1
stack-port ethernet 1/2/5
stack unit 2
unit-name Unit-2
module 1 icx7850-48c-xg-port-management-module
module 2 icx7800-100g-8port-800g-module
priority 131
stack-port ethernet 2/2/1
stack-port ethernet 2/2/5
stack unit 3
unit-name Unit-3
module 1 icx7850-32q-port-management-module
module 2 icx7800-100g-12port-1200g-module
module 3 icx7800-100g-8port-800g-module
stack-port ethernet 3/3/1
stack-port ethernet 3/3/5
stack enable
stack mac c0c5.2074.86cc
!
```

4. Click **Back** button to go back to the **MANAGE ARCHIVES** dialog box.

Copying an Archive to Another Archive

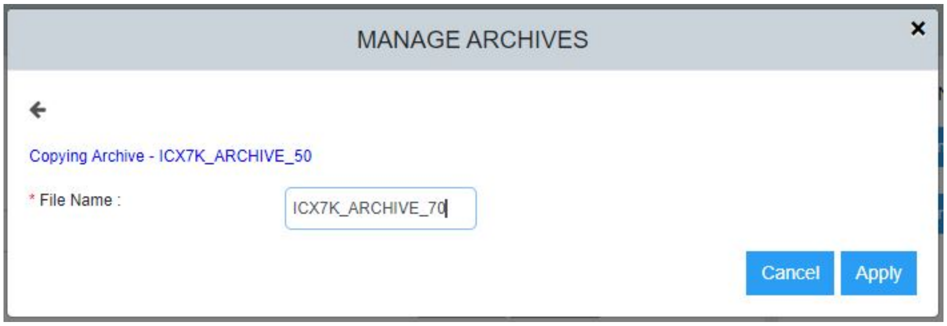
Complete the following steps to copy an archive to another archive.

1. On the menu, click **Management** > **Infra**.
2. In the **CONFIGURATION ARCHIVE** pane, click **Manage Archives**.

   The **MANAGE ARCHIVES** dialog box is displayed.

3. Select a config archive and click ⧉ (Copy) icon.

FIGURE 29 Copying Config Archive



Copying Archive - ICX7K_ARCHIVE_50

* File Name : ICX7K_ARCHIVE_70

4. In the **File Name** field, enter a name as per the archive naming convention (prefixed with a pre-defined string 'ICX7K_ARCHIVE’).
5. Click **Apply** to copy the selected archive to the new archive file.

Applying an Archive to the System

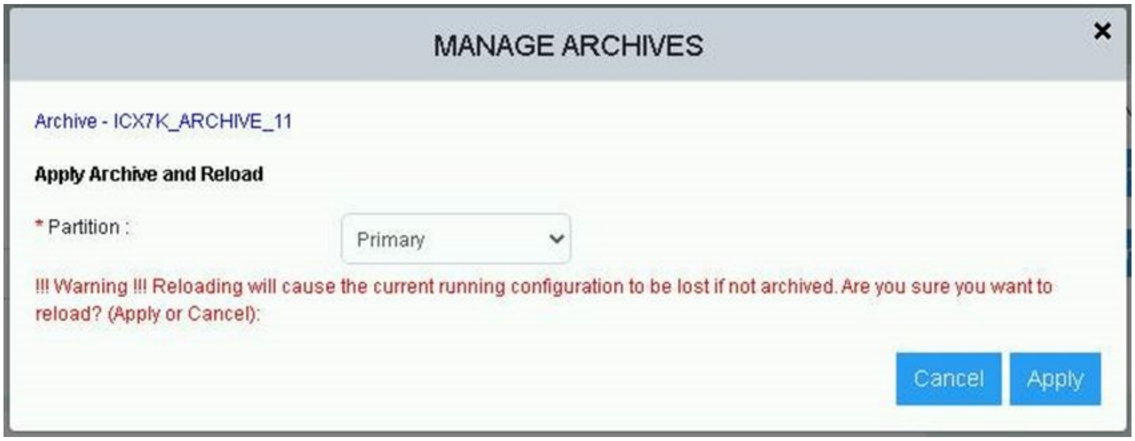
Complete the following steps to apply and reload the system with a specific archive without changing the startup configuration.

1. On the menu, click **Management** > **Infra**.
2. In the **CONFIGURATION ARCHIVE** pane, click **Manage Archives**.

   The **MANAGE ARCHIVES** dialog box is displayed.

3. Select a config archive and Click ⤓ (Apply) icon.

FIGURE 30 Applying Config Archive



Archive - ICX7K_ARCHIVE_11

Apply Archive and Reload

* Partition : Primary

!!! Warning !!! Reloading will cause the current running configuration to be lost if not archived. Are you sure you want to reload? (Apply or Cancel):

4. In the **Partition** dropdown, select **Primary** or **Secondary** partition to which you want to apply the config archive.
5. Click **Apply** to load the system with the specified config archive.

Uploading an Archive to the System

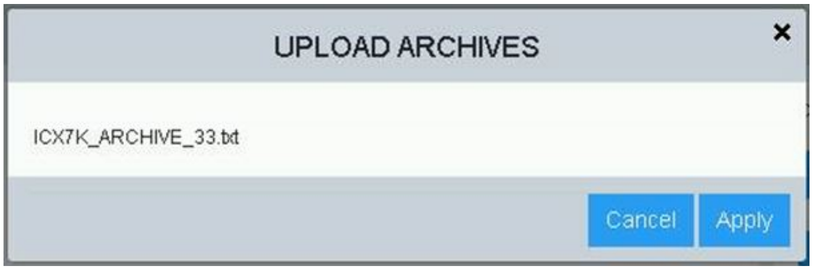
Complete the following steps to apply and reload the system with a specific archive without changing the startup configuration.

1. On the menu, click **Management** > **Infra**.
2. In the **CONFIGURATION ARCHIVE** pane, click **Manage Archives**.

   The **MANAGE ARCHIVES** dialog box is displayed.
3. Click ⊕ (Upload) icon and browse and select the saved configuration archive file from the local machine.

   The **UPLOAD ARCHIVES** dialog box is displayed.

   FIGURE 31 Upload Archive

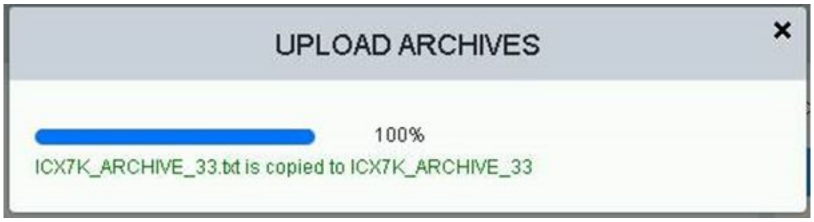
   

   ICX7K_ARCHIVE_33.txt

   If the number of archives in the system exceeds the configured archive size with the addition of the new archive file, the oldest archive file that needs to be deleted gets listed.
4. Click **Apply** to load the system with the specified config archive.

   When the archive is uploaded to the device, the completion status is displayed.

   FIGURE 32 Upload Archive - Status

   100%

   ICX7K_ARCHIVE_33.txt is copied to ICX7K_ARCHIVE_33

Deleting an Archive

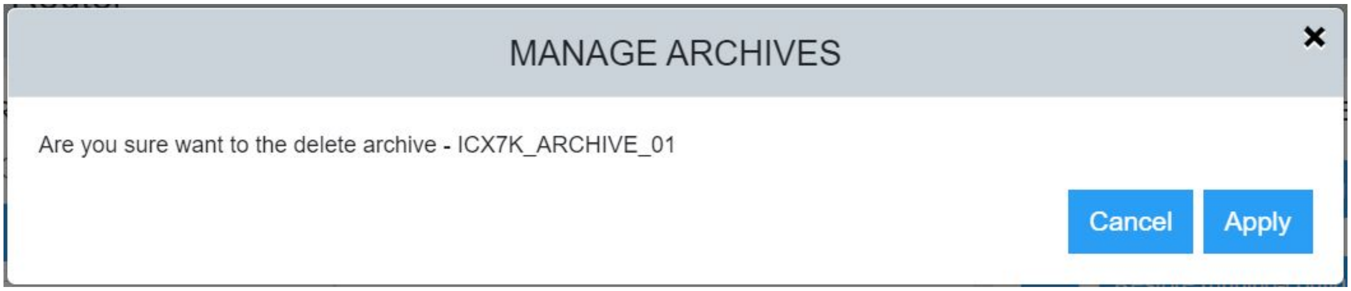
Complete the following steps to delete a specific archive.

1. On the menu, click **Management** > **Infra**.
2. In the **CONFIGURATION ARCHIVE** pane, click **Manage Archives**.

   The **MANAGE ARCHIVES** dialog box is displayed.

3. Select a config archive and click 🗑 (Delete) icon to delete the selected config archive. A confirmation dialog box is displayed.

FIGURE 33 Deleting Config Archive



MANAGE ARCHIVES

Are you sure want to the delete archive - ICX7K_ARCHIVE_01

4. Click **Apply** to delete the selected config archive.

   A dialog box is displayed with a message to indicate that the archive size is deleted successfully.
5. Click **Back** button to go back to the **MANAGE ARCHIVES** dialog box.

Managing Syslog Messages

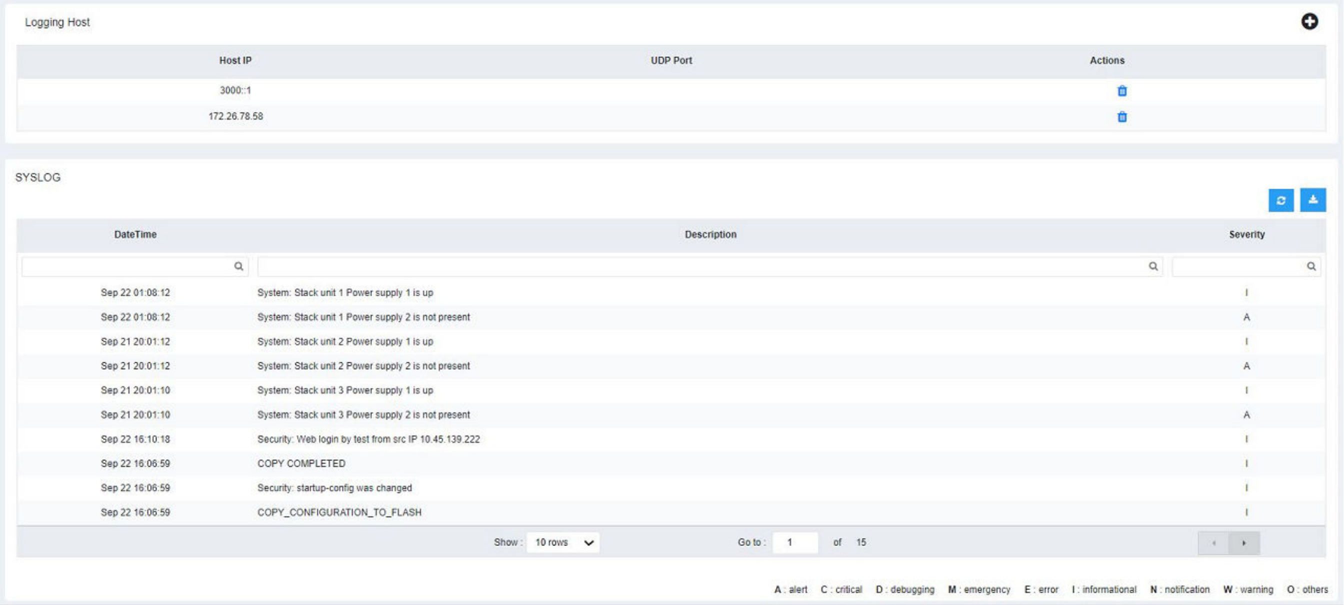
You can configure logging host (syslog server) to which syslogs are sent. Events that are logged by the device can be viewed and downloaded for debugging and troubleshooting purposes.

Complete the following steps to configure logging host and view and download the syslog messages.

1. On the menu, click **Management** > **Syslog**.

   The configured servers are displayed in the **Logging Host** pane.

   FIGURE 34 Syslog Details

   Logging Host

Host IP	UDP Port	Actions
3000::1		🗑
172.26.78.58		🗑

   SYSLOG

DateTime	Description	Severity
Sep 22 01:08:12	System: Stack unit 1 Power supply 1 is up	I
Sep 22 01:08:12	System: Stack unit 1 Power supply 2 is not present	A
Sep 21 20:01:12	System: Stack unit 2 Power supply 1 is up	I
Sep 21 20:01:12	System: Stack unit 2 Power supply 2 is not present	A
Sep 21 20:01:10	System: Stack unit 3 Power supply 1 is up	I
Sep 21 20:01:10	System: Stack unit 3 Power supply 2 is not present	A
Sep 22 16:10:18	Security: Web login by test from src IP 10.45.139.222	I
Sep 22 16:06:59	COPY COMPLETED	I
Sep 22 16:06:59	Security: startup-config was changed	I
Sep 22 16:06:59	COPY_CONFIGURATION_TO_FLASH	I

   Show : 10 rows Go to : 1 of 15

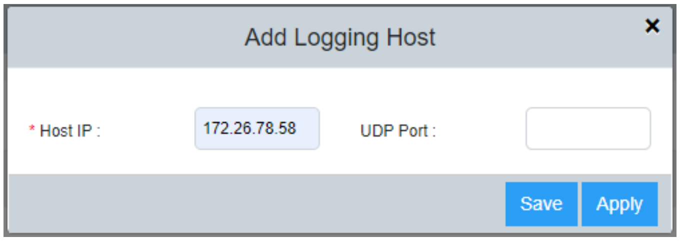
   A : alert C : critical D : debugging M : emergency E : error I : informational N : notification W : warning O : others

   You can perform the following actions:

   - Add logging host: To add logging host, continue to step 2.
   - Delete logging host: Click 🗑 (Delete icon) to delete the existing servers.

2. In the **Logging Host** pane, click ⊕ (Add icon) to display the **Add Logging Host** window.

   FIGURE 35 Adding Logging Host

   Add Logging Host

   * Host IP : 172.26.78.58 UDP Port :

3. Complete the following fields:
   - **Host IP**: Enter the remote host address that can be IPv4 address or IPv6 address.
   - **UDP Port**: Enter the transport protocol - UDP port number.
4. Click **Apply** to add logging host.

   The **SYSLOG** pane displays the log details described in the following table.

TABLE 6 Syslog Details

Field	Description
Date Time	Displays the date and time when the message was generated.
Description	Displays a description of the event.
Severity	Displays the severity level. The messages are listed by severity level in the following order: ● Emergencies (E) ● Alerts (A) ● Critical (C) ● Errors (Err) ● Warnings (W) ● Notifications (N) ● Informational (I) ● Debugging (D)

5. Click 🔄 (Refresh icon) to refresh the data in the log table.
6. Click ⬇ (Download icon) to download the logs to the local machine.

Managing the Polling Intervals

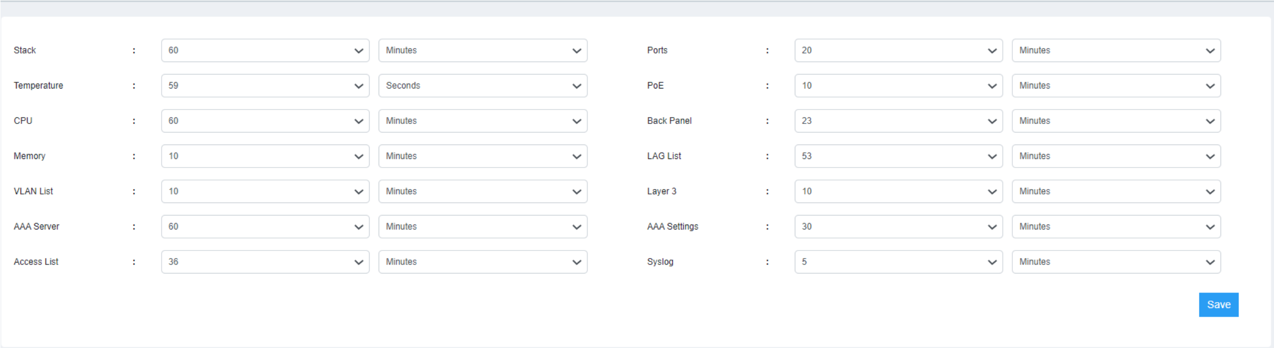
Polling the device at regular intervals helps you to monitor the device performance and the network health. The device polls the data to check system status, ports, connectivity, reachability, CPU, memory utilization, temperature, chassis, and so on. You can view and change the poll interval settings for many supported features.

Complete the following steps to view and edit the polling intervals.

1. On the menu, click **Management** > **Polling Interval**.

   The polling interval details of supported features are displayed.

   FIGURE 36 Polling Interval Details

Stack	:	60	Minutes	Ports	:	20	Minutes
Temperature	:	59	Seconds	PoE	:	10	Minutes
CPU	:	60	Minutes	Back Panel	:	23	Minutes
Memory	:	10	Minutes	LAG List	:	53	Minutes
VLAN List	:	10	Minutes	Layer 3	:	10	Minutes
AAA Server	:	60	Minutes	AAA Settings	:	30	Minutes
Access List	:	36	Minutes	Syslog	:	5	Minutes

2. Select the required time value and unit of time (seconds, minutes, or hours) from the list for each feature you want to edit the polling interval.
3. Click **Save** to save the changes made to the polling intervals.

Supportsave

Supportsave collects logs that can be useful when troubleshooting an issue.

Supportsave collects logs from different FastIron modules. The collected logs are shared with technical support personnel for investigating issues seen on the ICX device. RUCKUS recommends running the supportsave process before upgrading the firmware on a switch, so that you have the necessary information should an issue arise. Supportsave data collection can take several minutes.

When you click the Start button in the Support Save pane on the web interface of a remote device, the request is sent to the ICX device, which begins to collect the supportsave logs and put them into two files with .tgz extensions. One of the .tgz files contains the core and log files. The second .tgz file contains **show** command output. The files are copied over an HTTPS channel to the download location.

If you are running the supportsave process from the web interface for the first time, a dialog box is displayed requesting permission to download multiple files. You must select Allow to confirm the multiple file download.

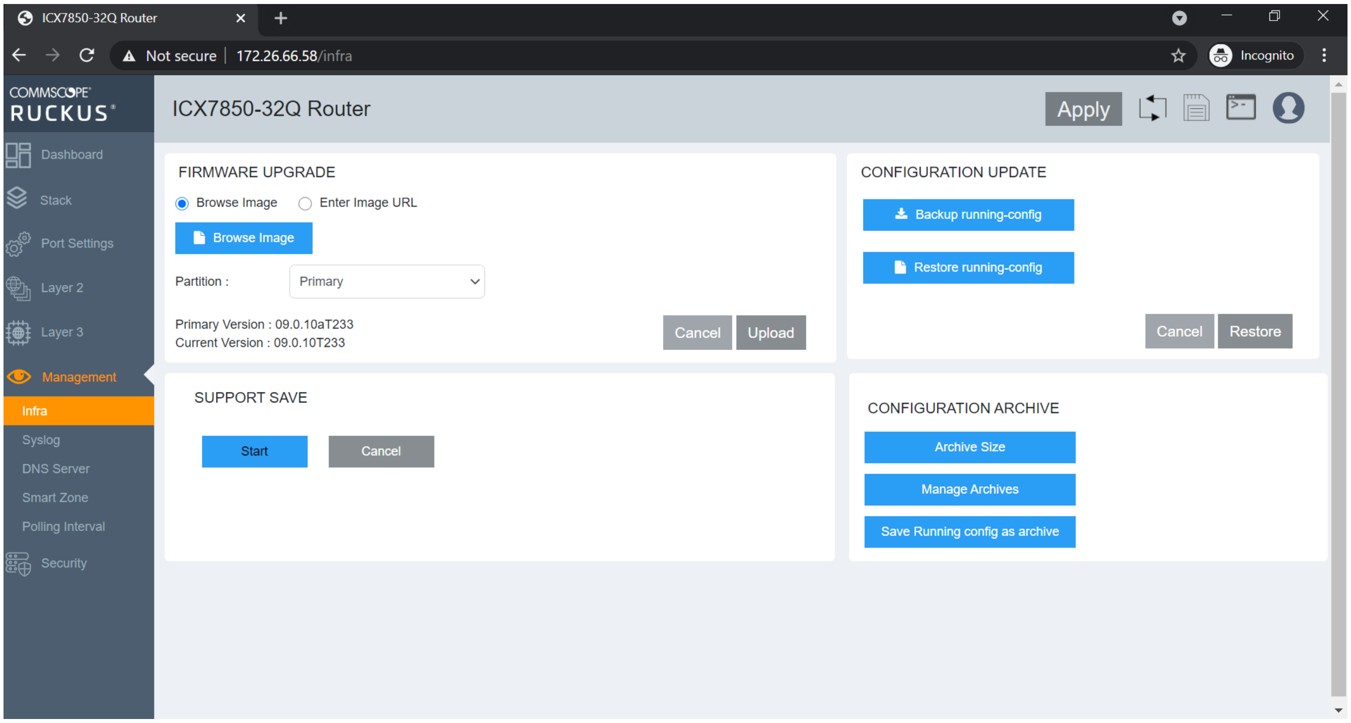
> **NOTE**
> You are not allowed to click the supportsave button again until the previous request is completed.

> **NOTE**
> You cannot access other web interface pages until an active supportsave request is completed.

Complete the following steps to collect the logs.

1. On the menu, click **Management** > **Infra**.

   FIGURE 37 Infra Management Page



● Browse Image ○ Enter Image URL

Partition : Primary

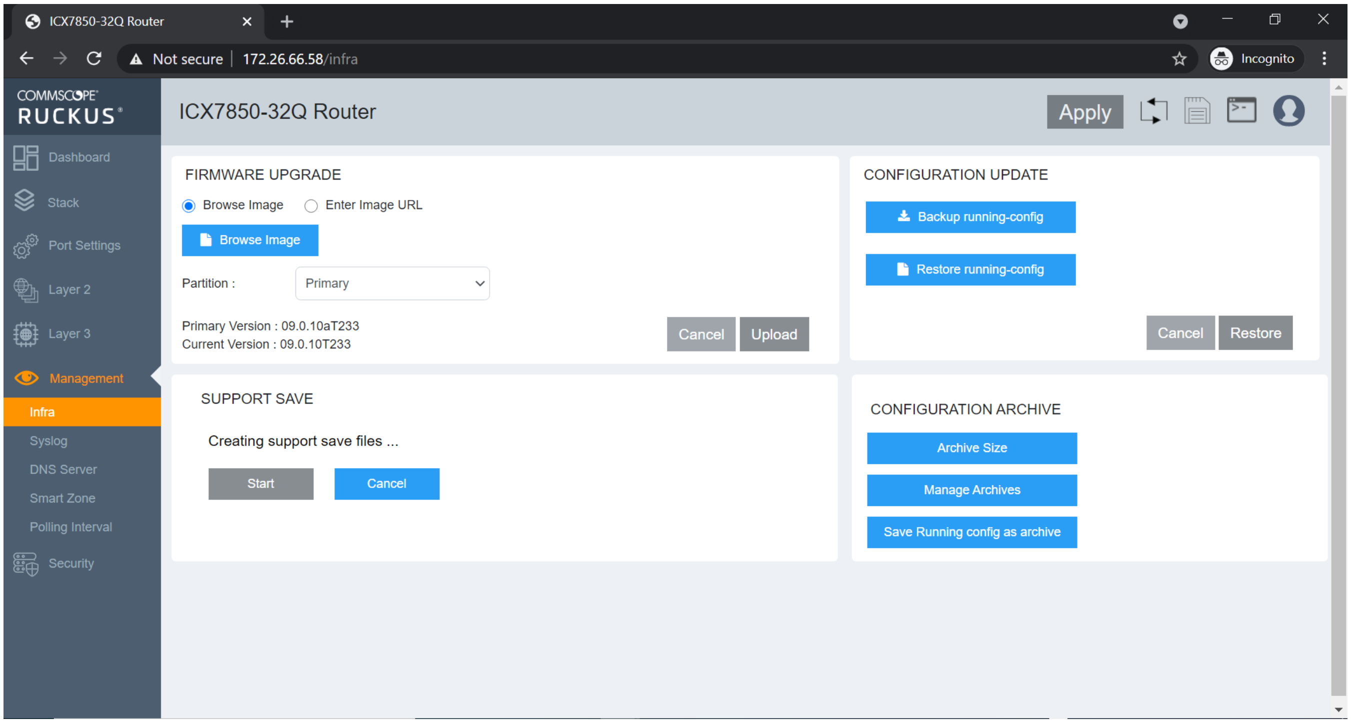
Primary Version : 09.0.10aT233
Current Version : 09.0.10T233

2. In the **SUPPORT SAVE** pane, click **Start**.

   NOTE

   To cancel a supportsave operation in progress, click **Cancel**. While the cancel operation is in progress, you cannot click **Start** or **Cancel**. The options become available again when the cancel operation is complete.

FIGURE 38 Supportsave in Progress

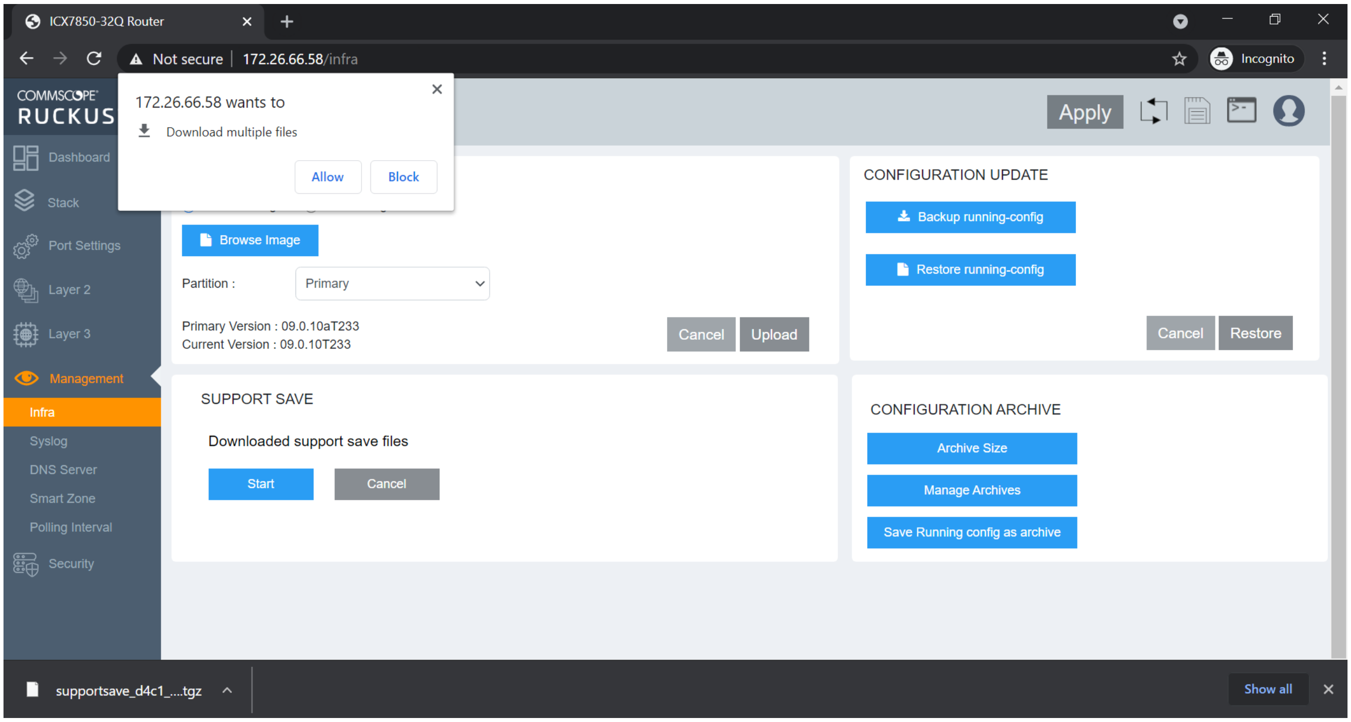


Primary Version : 09.0.10aT233
Current Version : 09.0.10T233

Creating support save files ...

If you are running supportsave from the web interface for the first time, you must select **Allow** in the dialog box to start the multiple file download.

FIGURE 39 Multiple File Confirmation



ICX7850-32Q Router

Not secure | 172.26.66.58/infra

172.26.66.58 wants to

Download multiple files

Allow | Block

CONFIGURATION UPDATE

Partition : Primary

Primary Version : 09.0.10aT233
Current Version : 09.0.10T233

SUPPORT SAVE

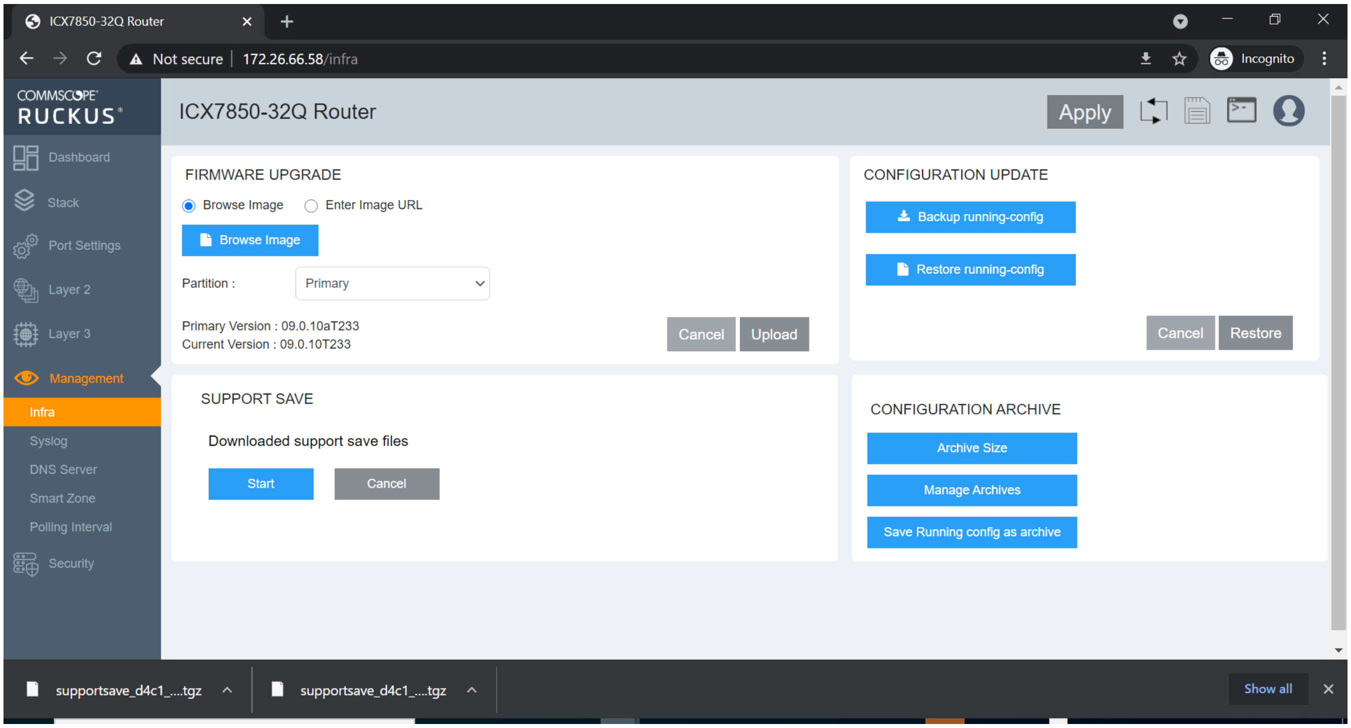
Downloaded support save files

CONFIGURATION ARCHIVE

supportsave_d4c1_....tgz

The system begins to collect logs. This operation can take several minutes. Once the operation is complete, the logs are downloaded to a specified location for the remote device.

FIGURE 40 Supportsave Completed



Not secure | 172.26.66.58/infra

ICX7850-32Q Router

Partition : Primary

Primary Version : 09.0.10aT233
Current Version : 09.0.10T233

Downloaded support save files

Security

Access Control List

Layer 3 (IPv4 and IPv6) access control lists (ACLs) permit or deny packets according to rules included in the ACLs. When a packet is received or sent, the device compares its header fields against the rules in applied ACLs. This comparison is done sequentially, in the order the rules are entered or on the sequence numbers you specify. Based on the comparison, the device either forwards or drops the packet. Only minimal ACL configurations are supported in the web interface.

Regarding the range of filtering options, there are two types of IPv4 ACLs:

- Standard ACLs: Permit or deny traffic according to source address only.
- Extended ACLs: Permit or deny traffic according to source and destination addresses, as well as other parameters. For example, in an extended ACL, you can also filter by one or more of the following parameters:
  - Port name or number
  - Protocol (for example, TCP or UDP)

ACLs include the following benefits:

- Providing security and traffic management
- Monitoring network and user traffic
- Saving network resources by classifying traffic
- Protecting against Denial of Service (DoS) attacks
- Reducing debug output

Because applied ACLs are programmed into the Content Addressable Memory (CAM), packets are permitted or denied in the hardware, without sending the packets to the CPU for processing. Named ACLs and numbered ACLs are supported for IPv4 ACLs. IPv6 ACLs are named. Named ACLs must begin with an alphabetical character and can contain up to 47 alphanumeric characters.

Configuring Standard IPv4 ACL

Complete the following steps to configure standard IPv4 ACL:

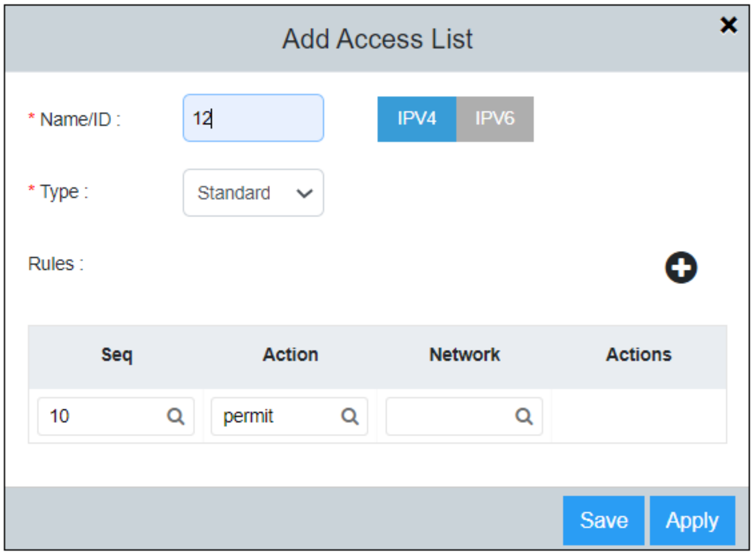
1. On the menu, click **Security** > **ACL**.

   All the configured ACLs are listed in the main pane. You can perform the following actions:

   - Add ACL: To add new ACL, continue to step 2.
   - Edit ACL: Click ✏ (Edit icon) to display the **Edit Access List** window. You can delete the existing rule or add new rules. Make necessary changes and click **Apply** to apply the changes.
   - Delete ACL: Click 🗑 (Delete icon) to display **Delete Access List** window. Click **Apply** to delete the ACL.

2. Click ⊕ (Add icon) to display the **Add Access List** window.

FIGURE 41 IPv4 Standard ACL



* Name/ID : 12

* Type : Standard

Rules :

Seq	Action	Network	Actions
10	permit		

3. Select **IPv4** tab and complete the following fields:
   - **Name/ID**: Enter a unique ACL name or number.
   - **Type**: Select **Standard** from the dropdown list to create standard IPv4 ACL.
4. Click ⊕ (Add icon) to add ACL rules with the following parameters. All the parameters are mandatory.
   - **Seq**: Assign a sequence number to the ACL rule.
   - **Action**: Select Permit or Deny from the dropdown list to filter the traffic according to the rules.
   - **Network**: Enter the source IP address.
5. Click **Apply** to create standard IPv4 ACL.

Configuring Extended IPv4 ACL

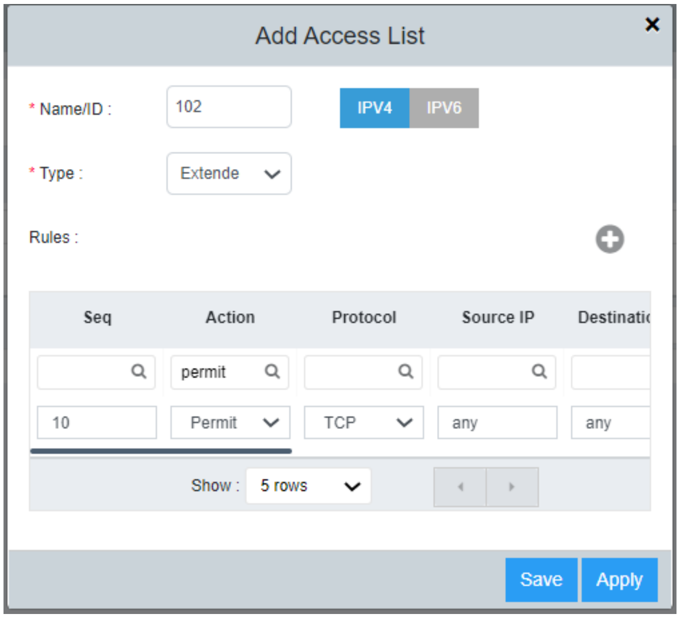
Complete the following steps to configure extended IPv4 ACL:

1. On the menu, click **Security** > **ACL**.

   All the configured ACLs are listed in the main pane. You can perform the following actions:
   - Add ACL: To add new ACL, continue to step 2.
   - Edit ACL: Click ✎ (Edit icon) to display the **Edit Access List** window. You can delete the existing rule or add new rules. Make necessary changes and click **Apply** to apply the changes.
   - Delete ACL: Click 🗑 (Delete icon) to display **Delete Access List** window. Click **Apply** to delete the ACL.

2. Click ⊕ (Add icon) to display the **Add Access List** window.

FIGURE 42 Extended IPv4 ACL



* Name/ID : 102

* Type : Extende

Rules : ⊕

Seq	Action	Protocol	Source IP	Destinatic
	permit			
10	Permit	TCP	any	any

Show : 5 rows

3. Select **IPv4** tab and complete the following fields:
   - **Name/ID**: Enter a unique ACL name or number.
   - **Type**: Select **Extended** from the dropdown list to create standard IPv4 ACL.
4. Click ⊕ (Add icon) to add ACL rules with the following parameters:
   - **Seq**: Assign a sequence number to the ACL rule.
   - **Action**: Select **Permit** or **Deny** from the dropdown list to filter the traffic according to the rules.
   - **Protocol**: Select the protocol type to be specified as a match for filtering. The available protocols are IP, TCP, and UDP.
   - **Source IP**: Enter the source address for which you want to filter the subnet.
   - **Destination IP**: Enter the destination address for which you want to filter the subnet.
   - **Source Port**: Specify the source port of the specified protocol.
   - **Destination Port**: Specify the destination port of the specified protocol.
   - **DSCP Matching**: Filters by DSCP value.
   - **DSCP Marking**: Assign the DSCP value for the packet.
   - **Internal Priority**: Assign the internal queuing priority (traffic class) for the packet.
5. Click **Apply** to create extended IPv4 ACL.

Configuring IPv6 ACL

Complete the following steps to configure IPv6 ACL:

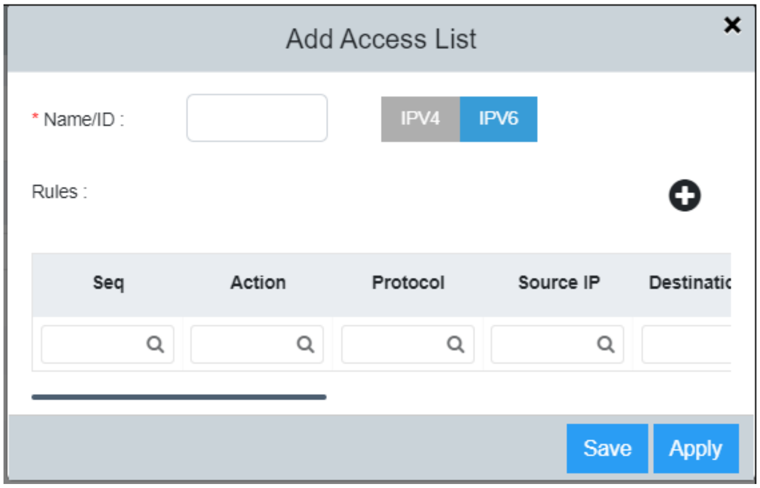
1. On the menu, click **Security** > **ACL**.

   All the configured ACLs are listed in the main pane. You can perform the following actions:

   - Add ACL: To add new ACL, continue to step 2.
   - Edit ACL: Click ✎ (Edit icon) to display the **Edit Access List** window. You can delete the existing rule or add new rules. Make necessary changes and click **Apply** to apply the changes.
   - Delete ACL: Click 🗑 (Delete icon) to display **Delete Access List** window. Click **Apply** to delete the ACL.

2. Click ⊕ (Add icon) to display the **Add Access List** window.

   FIGURE 43 IPv6 ACL



3. Select **IPv6** tab and complete the following fields:

   - **Name/ID**: Enter a unique ACL name.

4. Click ⊕ (Add icon) to add ACL rules with the following parameters:

   - **Seq**: Assign a sequence number to the ACL rule.
   - **Action**: Select **Permit** or **Deny** from the dropdown list to filter the traffic according to the rules.
   - **Protocol**: Select the protocol type to be specified as a match for filtering. The available protocols are IPv6, TCP, and UDP.
   - **Source IP**: Enter the source address for which you want to filter the subnet.
   - **Destination IP**: Enter the destination address for which you want to filter the subnet.
   - **Source Port**: Specify the source port of the specified protocol.
   - **Destination Port**: Specify the destination port of the specified protocol.
   - **DSCP Matching**: Filters by DSCP value.
   - **DSCP Marking**: Assign the DSCP value for the packet.
   - **Internal Priority**: Assign the internal queuing priority (traffic class) for the packet.

5. Click **Apply** to create IPv6 ACL.

AAA Servers

AAA is a set of services to regulate access to system resources, enforcing privilege policies, and assessing usage. These processes ensure effective network management and security. The AAA server is a network server that is used for access control which handles user requests for access to computer resources and provides AAA services - authentication, authorization, and accounting.

You can configure the following servers to provide AAA services:

- RADIUS
- Tacacs+

You can specify up to eight RADIUS servers and eight TACACS+ servers. If you add multiple AAA servers to the device, the device tries to reach them in the order they are added.

Local User Accounts

User accounts regulate who can access the management functions. You can create accounts for local users with passwords for authentication purpose which are stored in a local database. You can use a local database instead of AAA servers to provide user authentication. You can also specify various privilege level of access for users. Up to 32 local user accounts can be defined on a RUCKUS device. When a user tries to gain access to the device, the authentication credentials are verified against the user credentials stored in the database.

Specifying Different Servers for Individual AAA Functions

Separate RADIUS and TACACS+ servers can be configured and assigned for specific AAA tasks. For example, you can designate one RADIUS or TACACS+ server to handle authentication and another RADIUS or TACACS+ server to handle accounting. You can specify individual servers for authentication and accounting, but not for authorization. By default, RADIUS and TACACS+ servers perform all AAA functions. After authentication takes place, the server that performed authentication is used for authorization and accounting. If the authenticating server cannot perform the requested function, the next server in the configured list of servers is tried. This process repeats until a server that can perform the requested function is found or until every server in the configured list has been tried.

Authentication

Authentication is a means to identify a user by verifying the authentication credentials before access is granted. The AAA server compares the username and password entered by the user with other login credentials stored in a database. If the credentials match, the user is granted access to the network.

Authorization

Authorization is a method of setting control on the privilege level for the user after authentication. The amount of information and the amount of services the user has access to depend on the user's authorization level. It largely determines what types of activities a user can perform and the management commands that an authenticated user is authorized to use.

Accounting

Accounting records and measures the information about user activity and system events such as when a user logs into the device or the system is rebooted. Accounting information include session start and stop time, the amount of system time and the services accessed and the amount of data that a user has sent or received during a session.

If authorization is enabled and the command requires authorization, authorization is performed before accounting takes place. If authorization fails for the command, no accounting takes place. You can use authentication alone or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

Configuring Local User Account

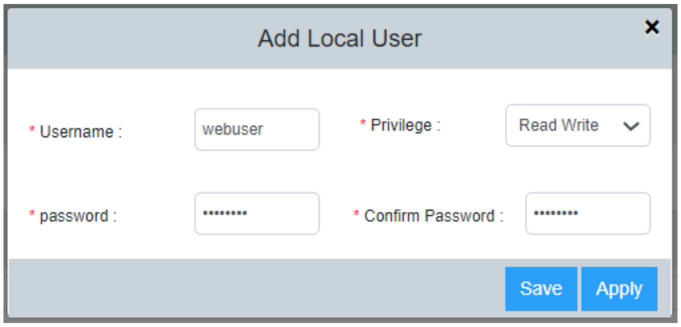
Complete the following steps to configure user account in a local database:

1. On the menu, click **Security** > **AAA Servers**.
2. Select **Local Users** tab.

   All the configured user accounts are listed in the main pane. You can perform the following actions:

   - Add user account: To add new user account, continue to step 3.
   - Edit user account: Click ✎ (Edit icon) to display the **Edit Local User** window. Make necessary changes and click **Apply** to apply the changes.
   - Delete user account: Click 🗑 (Delete icon) to display **Delete Local User** window. Click **Apply** to delete the user account.
3. In the **Local Users** tab, click ⊕ (Add icon) to display the **Add Local User** window.

   FIGURE 44 Add Local User



Add Local User

* Username : webuser

* Privilege : Read Write

* password : ••••••••

* Confirm Password : ••••••••

4. Complete the following fields:
   - **Username**: Enter a username for the user.
   - **Privilege**: Select the desired privilege level for the user from the dropdown list.
     - **Read Write**: Specifies to provide complete read-and-write access to the system.
     - **Read Only**: Specifies to provide limited read-only access.
     - **Port Config**: Specifies to provide read-and-write access at port configuration level (but not for global parameters).
     - **Cloud User**: Specifies to provide access to cloud users.
   - **Password**: Enter the password for the user.
   - **Confirm Password**: Re-enter the password for confirmation.
5. Click **Apply** to add local user account.

Configuring RADIUS Server

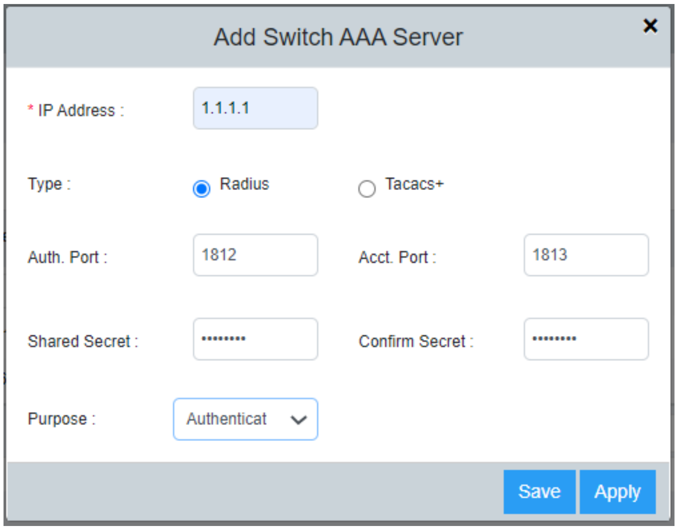
Complete the following steps to configure RADIUS server:

1. On the menu, click **Security** > **AAA Servers**.
2. Select **AAA Servers** tab.

   All the configured servers are listed in the main pane. You can perform the following actions:

   - Add server: To add new server, continue to step 3.
   - Edit server: Click ✎ (Edit icon) to display the **Edit Switch AAA Server** window. Make necessary changes and click **Apply** to apply the changes.
   - Delete server: Click 🗑 (Delete icon) to display the **Delete Switch AAA Server** window. Click **Apply** to delete the server.
3. In the **AAA Servers** tab, click ⊕ (Add icon) to display the **Add Switch AAA Server** window.

   FIGURE 45 AAA - RADIUS Server



Add Switch AAA Server

* IP Address : 1.1.1.1

Type : ● Radius ○ Tacacs+

Auth. Port : 1812 Acct. Port : 1813

Shared Secret : •••••••• Confirm Secret : ••••••••

Purpose : Authenticat

4. Select **Radius** as the AAA server type.
5. Complete the following fields:
   - **IP Address**: Assign an IP address to the RADIUS server. IP address can be in IPv4 format or IPv6 format.
   - **Auth. Port**: Enter the RADIUS authentication port number. Default is 1812.
   - **Acct. Port**: Enter the RADIUS accounting port number. Default is 1813.
   - **Shared Secret**: Specify the shared secret text string (RADIUS key) used between the device and the RADIUS server to authenticate user access.
   - **Confirm Secret**: Re-enter the shared secret.
   - **Purpose**: Designate the RADIUS server to handle a specific AAA operation selected from the dropdown list.
     - Default: Configures the RADIUS server to be used for any AAA operation.
     - Authentication: Configures the RADIUS server to be used only for authentication.
     - Accounting: Configures the RADIUS server to be used only for accounting.
6. Click **Apply** to add RADIUS server.

Configuring TACACS+ Server

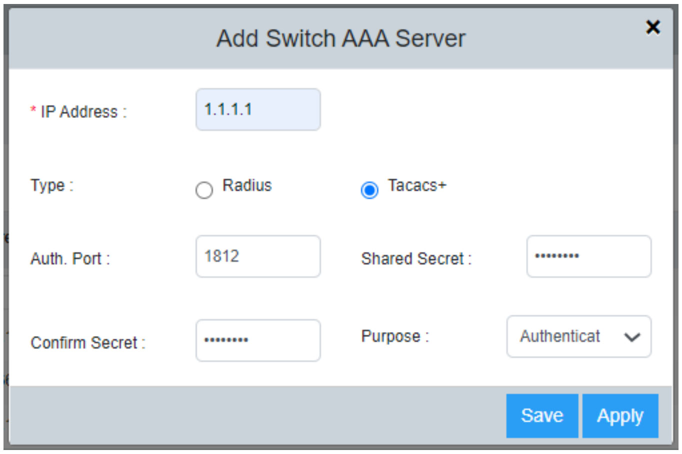
Complete the following steps to configure TACACS+ server:

1. On the menu, click **Security** > **AAA Servers**.
2. Select **AAA Servers** tab.

   All the configured servers are listed in the main pane. You can perform the following actions:

   - Add server: To add new server, continue to step 3.
   - Edit server: Click ✎ (Edit icon) to display the **Edit Switch AAA Server** window. Make necessary changes and click **Apply** to apply the changes.
   - Delete server: Click 🗑 (Delete icon) to display **Delete Switch AAA Server** window. Click **Apply** to delete the server.
3. In the **AAA Servers** tab, click ⊕ (Add icon) to display the **Add Switch AAA Server** window.

   FIGURE 46 AAA - Tacacs+ Server



Add Switch AAA Server ✕

* IP Address : 1.1.1.1

Type : ○ Radius ● Tacacs+

Auth. Port : 1812

Shared Secret : ••••••••

Confirm Secret : ••••••••

Purpose : Authenticat

4. Select **TACACS+** as the AAA server type.
5. Complete the following fields:
   - **IP Address**: Assign an IP address to the TACACS+ server. IP address can be in IPv4 format or IPv6 format.
   - **Auth. Port**: Enter the TACACS+ authentication port number. The default value is 1812.
   - **Shared Secret**: Specify the shared secret text string (TACACS+ key) used between the device and the TACACS+ server to authenticate user access.
   - **Confirm Secret**: Re-enter the shared secret text.
   - **Purpose**: Designate the TACACS+ server to handle a specific AAA operation selected from the dropdown list.
     - Default: Configures the TACACS+ server to be used for any AAA operation.
     - Authentication: Configures the TACACS+ server to be used only for authentication.
     - Authorization: Configures the TACACS+ server to be used only for authorization.
     - Accounting: Configures the TACACS+ server to be used only for accounting.
6. Click **Apply** to add TACACS+ server.

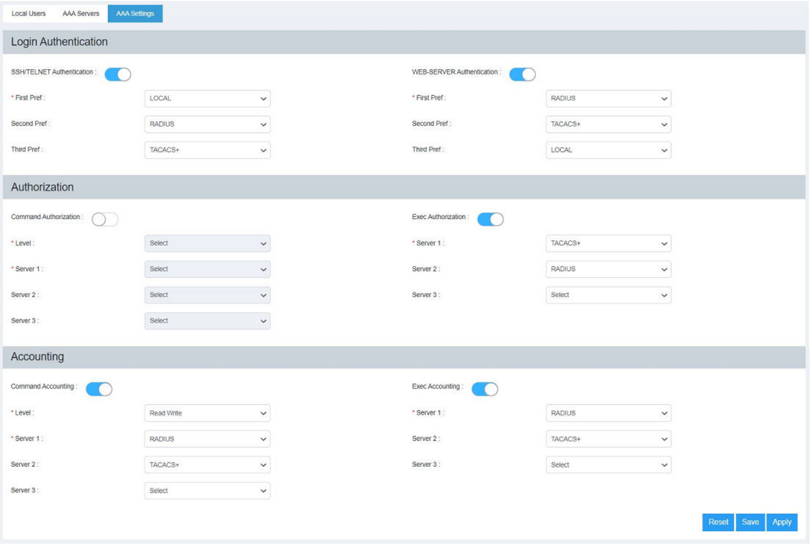
Managing AAA Settings

The AAA settings allow you to configure the method list and the sequence in which they are performed for AAA operations when a user tries to gain access to the device using Telnet or SSH. You can configure primary method lists and backup methods for each AAA service. You can use authentication alone or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

Complete the following steps to configure AAA settings.

1. On the menu, click **Security** > **AAA Servers**.

   FIGURE 47 AAA Settings



Login Authentication

SSH/TELNET Authentication :	●	WEB-SERVER Authentication :	●
* First Pref :	LOCAL	* First Pref :	RADIUS
Second Pref :	RADIUS	Second Pref :	TACACS+
Third Pref :	TACACS+	Third Pref :	LOCAL

Authorization

Command Authorization :	○	Exec Authorization :	●
* Level :	Select	* Server 1 :	TACACS+
* Server 1 :	Select	Server 2 :	RADIUS
Server 2 :	Select	Server 3 :	Select
Server 3 :	Select		

Accounting

Command Accounting :	●	Exec Accounting :	●
* Level :	Read Write	* Server 1 :	RADIUS
* Server 1 :	RADIUS	Server 2 :	TACACS+
Server 2 :	TACACS+	Server 3 :	Select
Server 3 :	Select		

2. Select the **AAA Settings** tab to configure server priority and privilege levels for authentication, authorization, and accounting.

3. Under **Login Authentication**, complete the following fields:
   - **SSH/Telnet Authentication**: Enabled by default. The Telnet or SSH access request is authenticated based on the configured authentication method. You can set the authentication methods in a sequential order based on your preference. If authentication service is not available from the first method, the second method is used, and so on. The available options are RADIUS, TACACS+, and Local Users.

     NOTE
     Login authentication cannot be disabled from the web interface.

     - **First Pref**: Select the primary authentication method from the list.
     - **Second Pref**: Select a backup authentication method as the second choice of preference to perform authentication when the primary authentication fails.
     - **Third Pref**: Select a backup authentication method as the third choice of preference to perform authentication when the first two authentication methods fail.
   - **WEB-SERVER Authentication**: Users gain access to the network by opening a Web browser and entering a valid URL address using HTTP or HTTPS services.The web access request is authenticated based on the configured authentication method. You can set the authentication methods in a sequential order based on your preference. If authentication service is not available from the first method, the second method is used, and so on. The available options are RADIUS, TACACS+, and Local Users.

     NOTE
     Login authentication cannot be disabled from the web interface.

     - **First Pref**: Select the primary authentication method from the list.
     - **Second Pref**: Select a backup authentication method as the second choice of preference to perform authentication when the primary authentication fails.
     - **Third Pref**: Select a backup authentication method as the third choice of preference to perform authentication when the first two authentication methods fail.
4. Under **Authorization**, complete the following fields:
   - **Command Authorization**: If enabled, command authorization allows you to determine the management privilege level and the associated set of commands an authenticated user is authorized to use. You can set three method lists for authorization and the available options are RADIUS, TACACS+, and None (which disables the authorization service, allowing all command access attempts to succeed).
     - **Level**: Select the privilege level (Port Config, Read Only, or Read Write) from the list.
     - **Server 1**: Select the primary method by which authorization should occur.
     - **Server 2**: Select the backup method by which authorization should occur.
     - **Server 3**: Select a backup method list as the third choice of preference to perform authorization.
   - **Exec Authorization**: If enabled, EXEC authorization allows you to control user privilege levels for authenticated users. You can set three method lists for authorization and the available options are RADIUS, TACACS+, and None (which disables the authorization service, allowing all command access attempts to succeed).
     - **Server 1**: Select the primary authorization method.
     - **Server 2**: Select the backup method for authorization.
     - **Server 3**: Select a backup method list as the third choice of preference to perform authorization.

5. Under **Accounting**, complete the following fields:
   - **Command Accounting**: If enabled, command accounting allows you to configure the device to perform AAA accounting for the commands available at the specified privilege level. You can set three method lists for accounting and the available options are RADIUS, TACACS+, and None (which disables the accounting service).
     - **Level**: Select the privilege level (Port Config, Read Only, or Read Write) from the list.
     - **Server 1**: Select the primary method by which accounting should occur.
     - **Server 2**: Select the backup method by which accounting should occur.
     - **Server 3**: Select a backup method list as the third choice of preference to perform accounting.
   - **Exec Accounting**: If enabled, EXEC accounting allows you to record the user activity and system events. You can set three method lists for accounting and the available options are RADIUS, TACACS+, and None (which disables the accounting service).
     - **Server 1**: Select the primary accounting method.
     - **Server 2**: Select the backup method for accounting.
     - **Server 3**: Select a backup method list as the third choice of preference to perform accounting.
6. Click **Apply** to save the AAA settings.

COMMSCOPE®
RUCKUS®

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com