USER GUIDE

RUCKUS FastIron Web Management Interface User Guide, 10.0.00

Supporting FastIron Software Release 10.0.00

Part Number: 53-1005757-03
Publication Date: 1 March 2023

Copyright, Trademark and Proprietary Rights Information

© 2023 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

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

Contact Information, Resources, and Conventions **5**
Contacting RUCKUS Customer Services and Support 5
What Support Do I Need? 5
Open a Case 5
Self-Service Resources 6
Document Feedback 6
RUCKUS Product Documentation Resources 6
Online Training Resources 6
Document Conventions 7
Notes, Cautions, and Safety Warnings 7
Command Syntax Conventions 7

About This Document **9**
New in This Document 9
Supported Hardware 9

Getting Started **11**
Access Requirements 11
Prerequisite Configuration 11
Logging In to the Web Management Interface 13
Navigating the Web Management Interface 14
Common Action Elements in the Interface 15
Accessing the Remote CLI 15

Dashboard and Stack Details **17**
Monitoring Device Information on the Dashboard 17
Displaying Stack Details 19

Device **23**
Global Configurations 23

Port Settings **25**
Port Settings Overview 25
Configuring Port Settings 26
Configuring Symmetric Flow Control 30
Configuring Flow Control 30

Layer 3 ..... **33**
Configuring IP Static Routes 33
Configuring a VE Port 34

Management **37**
Configuring an ICX Device to be Managed by SmartZone 37
Configuring Domain Name System Servers 38
Upgrading FastIron Software 39
Managing Running Configuration Backups 40
Restoring the Running Configuration 40
Configuration Archive 41
Configuring Archive Size 41
Saving the Running Configuration as an Archive File 42

Managing Configuration Archives 43
Managing Syslog Messages 49
Managing the Polling Intervals 51
Supportsave 51

Security 57
Access Control Lists 57
Configuring a Standard IPv4 ACL 57
Configuring an Extended IPv4 ACL 59
Configuring an IPv6 ACL 60
AAA Servers 61
Local User Accounts 61
Specifying Different Servers for Individual AAA Functions 61
Authentication 61
Authorization 61
Accounting 61
Configuring a Local User Account 62
Configuring a RADIUS Server 63
Configuring a TACACS+ Server 64
Managing AAA Settings 65

Contact Information, Resources, and Conventions

- Contacting RUCKUS Customer Services and Support 5
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 6
- Document Conventions 7
- Command Syntax Conventions 7

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://community.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

- New in This Document 9
- Supported Hardware..... 9

New in This Document

The following table describes changes to this guide for FastIron 10.0.00.

TABLE 2 Key Features and Enhancements in FastIron 10.0.00 (March 1, 2023)

Feature	Description	Reference
Minor editorial updates	**Updated**: Minor editorial updates and latest images were updated throughout the User Guide.	Throughout the guide.

TABLE 3 Key Features and Enhancements in FastIron 10.0.00 (December 15, 2022)

Feature	Description	Reference
RUCKUS ICX 8200	**New**: Added support for RUCKUS ICX 8200 devices.	Throughout the guide.
Discontinuation of support for a separate switch image	**Updated**: This release and future releases support a single image for ICX platforms that provides both switching and routing functionality. As a result, support for a separate switch ("Layer 2") image is discontinued.	References have been removed throughout the guide.
Unsupported hardware	**Updated**: This release and future releases do not support RUCKUS ICX 7150, 7250, and 7450 devices.	References have been removed throughout the guide.
Updates to address defects	**Updated**: Minor updates on content throughout to address defects.	Throughout the guide.
Minor editorial updates	**Updated**: Minor editorial updates and latest images were updated throughout the User Guide.	Throughout the guide.

Supported Hardware

This guide supports the following RUCKUS products:

- RUCKUS ICX 8200 Switches
- RUCKUS ICX 7850 Switches
- RUCKUS ICX 7650 Switches
- RUCKUS ICX 7550 Switches

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

Getting Started

- Access Requirements..... 11
- Prerequisite Configuration..... 11
- Logging In to the Web Management Interface..... 13
- Navigating the Web Management Interface..... 14

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).

   ```
   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 (for 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
   Upon upgrade to FastIron 09.0.00 or later, the web management HTTP configuration in a pre-09.0.00 image will be disabled, and web management access over HTTPS is 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

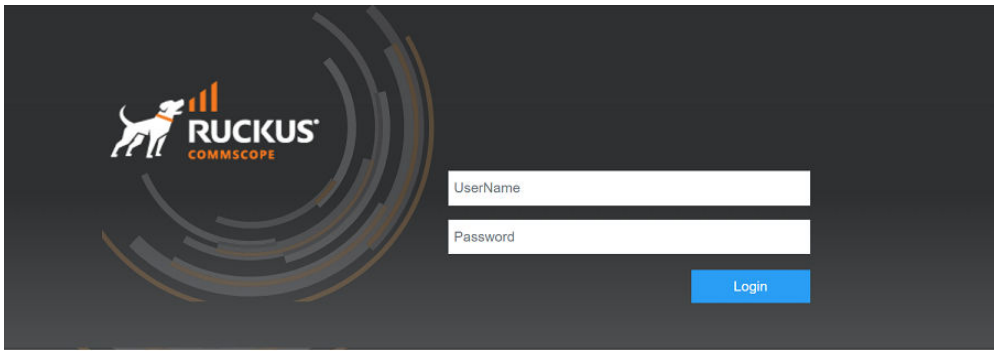
To log in to the Web Management Interface, perform the following steps.

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 the Management IP address, interface IP address, or VE IP address which is connected to the network.

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

   FIGURE 1 Web Management Interface Login Page



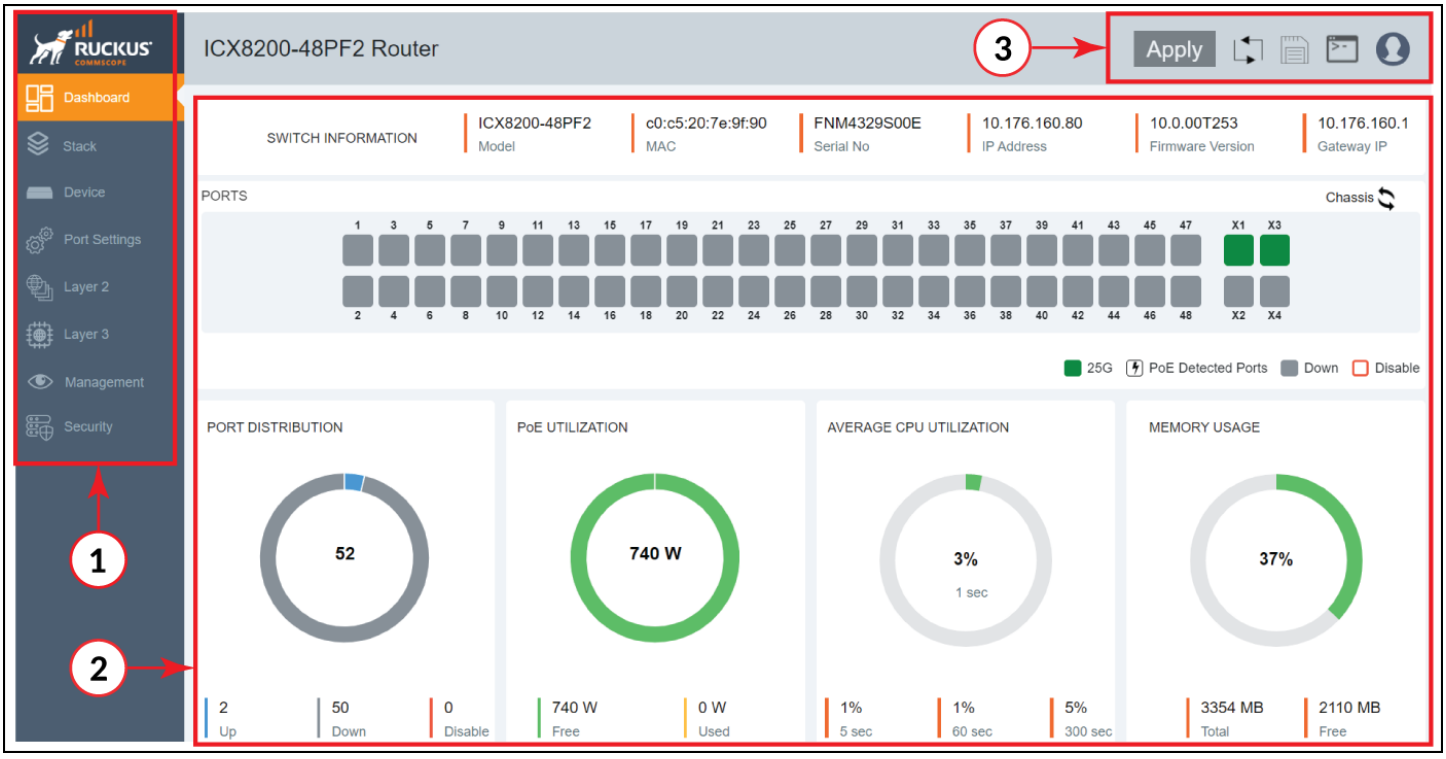
2. Enter the username and password.
3. Click **Login**.

   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



1. Menu
2. Main pane
3. Header pane

TABLE 4 Web Management Interface Elements

Number	Name	Description
1	Menu	Lists the menu and sub-menu items for administrative tasks.
2	Main pane	Displays configuration details, configuration options, charts, stack units, ports, and chassis panels, tables, lists, and miscellaneous information specific to the selected menu item.

TABLE 4 Web Management Interface Elements (continued)

Number	Name	Description
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.
- (Search icon): Allow you to search the existing information in an individual page.
- **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.
- **Reset**: Allows you to reset the configuration changes on individual pages to the default value.

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 the 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** dialog box is displayed.

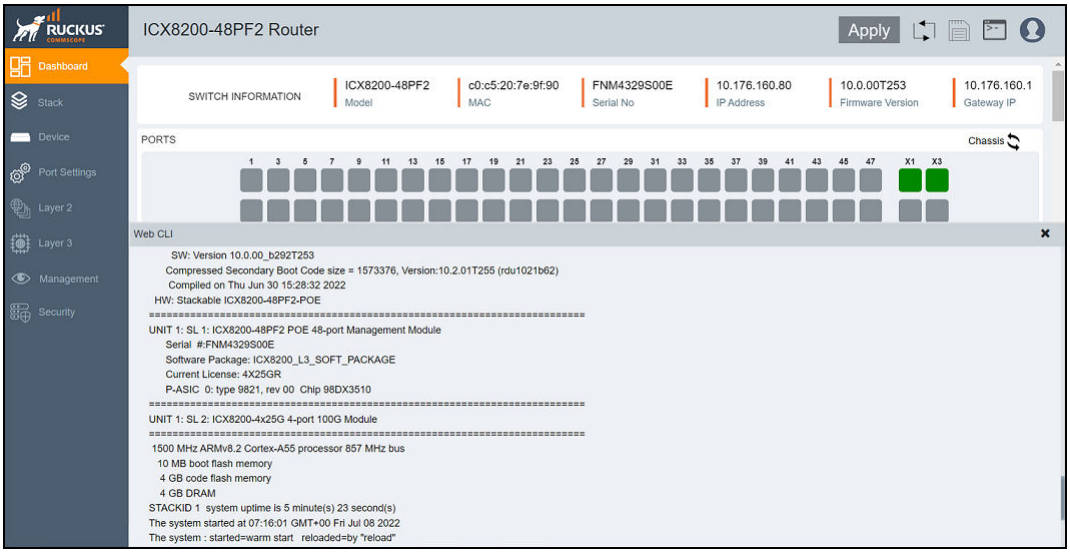
   FIGURE 3 Login Credentials



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



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

Dashboard and Stack Details

- Monitoring Device Information on the Dashboard..... 17
- Displaying Stack Details..... 19

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.

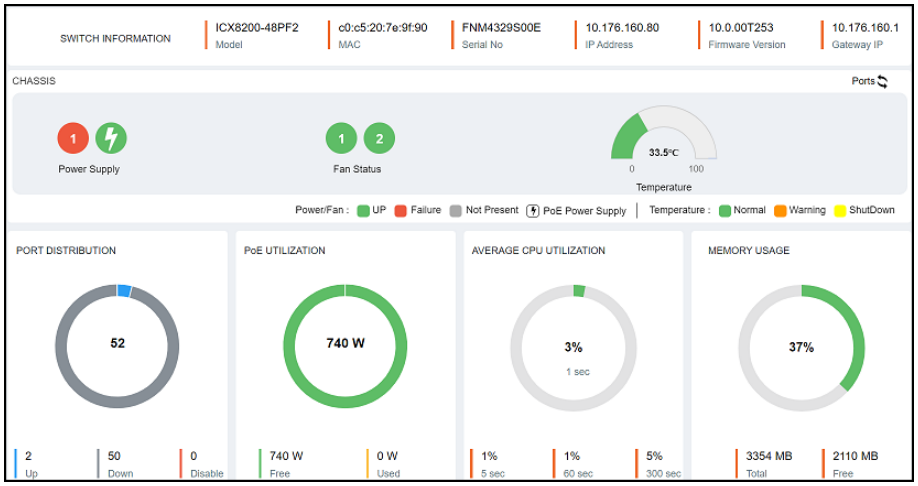
The figures are included for illustrative purposes only. The ports panel and port speed vary with different ICX models.

By default, the **Dashboard** is in Ports panel. Click on Chassis Icon Chassis to switch to Chassis panel and click on Ports Icon Ports to switch to Ports panel.

FIGURE 5 Dashboard: Ports Panel



FIGURE 6 Dashboard: Chassis Panel



The following table lists the infographic elements of the **Dashboard** that provide 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 by way of 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.

TABLE 5 Dashboard Elements (continued)

Dashboard Element	Description
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. – Grey: Power supply is not present. – Red: Power supply failure. 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. – Grey: Fan is not present. – Red: Fan is failure. **NOTE** If a fan is not present, the fan status will be "NO FAN". • **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. – Yellow: 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.

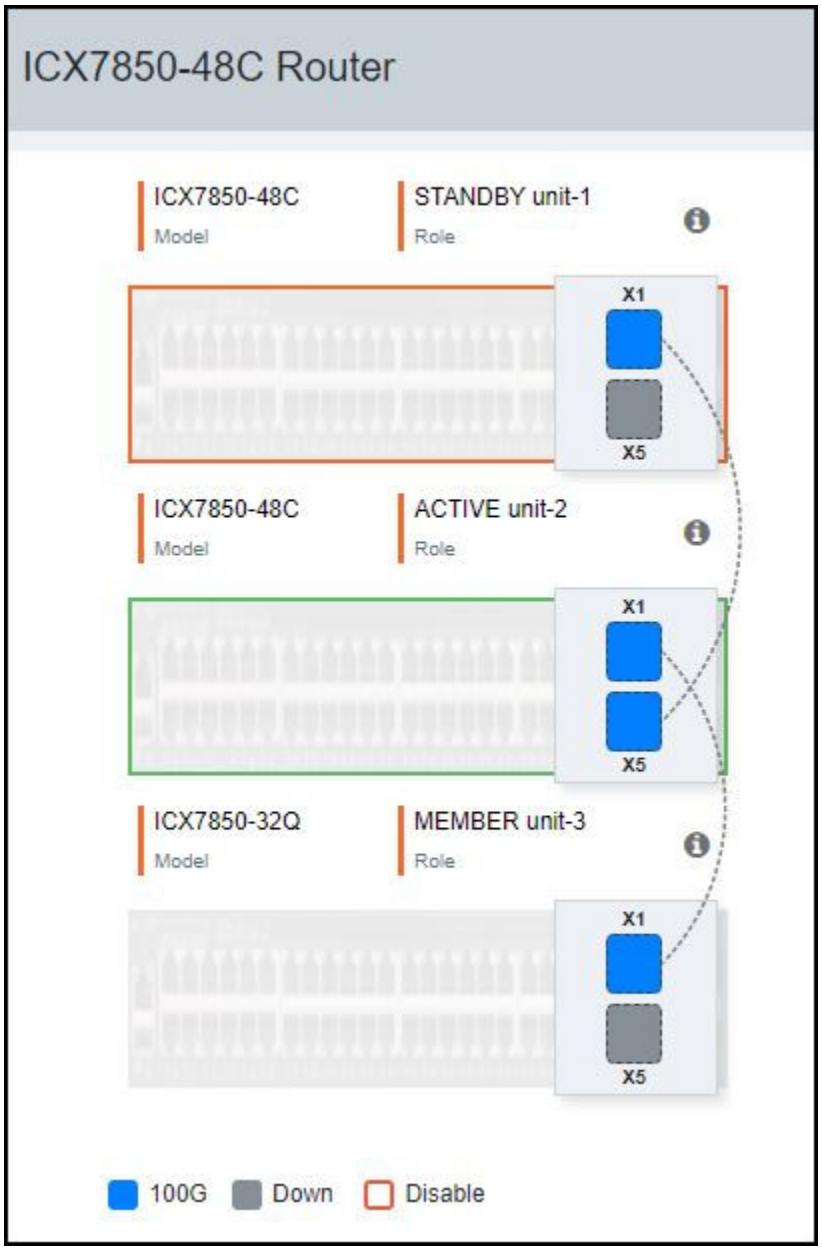
Displaying Stack Details

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 8200 stack or an ICX 7850 stack, but it cannot combine ICX 8200 and ICX 7850 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



   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 (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.

Device

- Global Configurations..... 23

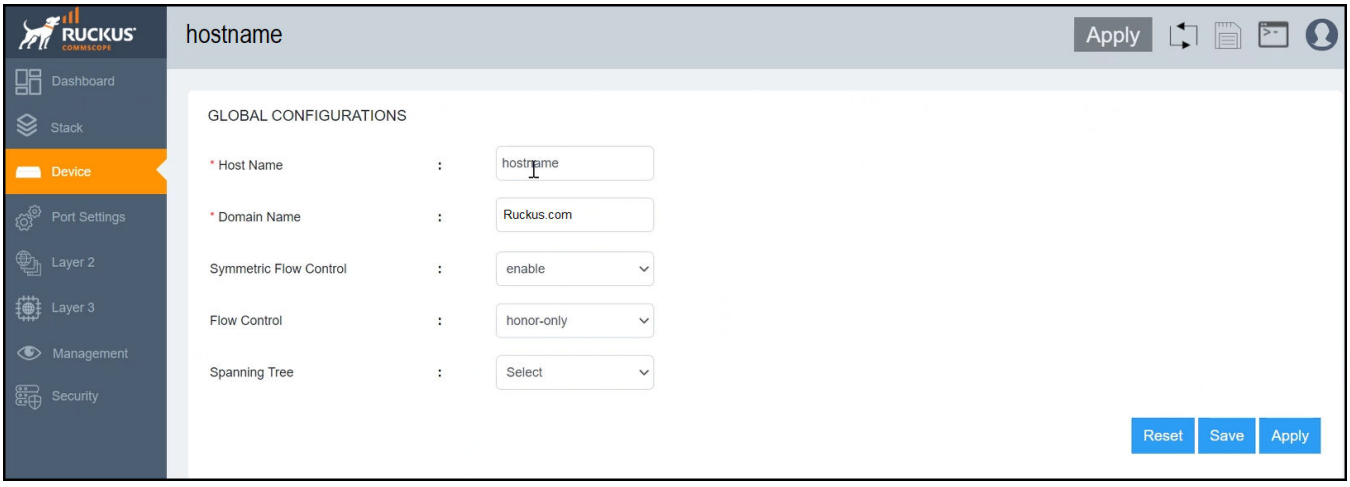
Global Configurations

Global configuration allows you to configure the symmetrical flow control (SFC), flow control (802.3x), and spanning tree at the global level.

Complete the following steps to configure global configurations.

1. On the menu, click **Device**.

FIGURE 8 Configuring Device: Global Configurations



2. In the **Global Configurations** tab you can perform the following actions:
   a) For **Host name**, configure the host name for the device.
   b) For **Domain Name**, configure the domain name. For example, ruckus.com.
   c) For **Symmetric Flow Control**, Select the following options from the 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.
   d) For **Flow Control**, select the following options from the list to configure flow control:
      - **both**: Configures flow control in PAUSE generation and honoring mode.
      - **generate-only**: Configures flow control in PAUSE generation mode only.
      - **honor-only**: Configures flow control in PAUSE honoring mode only.
      - **neg-on**: Enable flow control with negotiation.
      - **None**: Disables flow control configurations.
   e) For **Spanning Tree**, select the following options from the list to configure spanning tree:
      - **Single**: Enable single spannning tree.
      - **path-cost-method**: Configures spanning tree path cost method.
3. Click **Apply** to configure the **Global Configurations** settings.

Port Settings

- Port Settings Overview..... 25
- Configuring Port Settings..... 26

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.

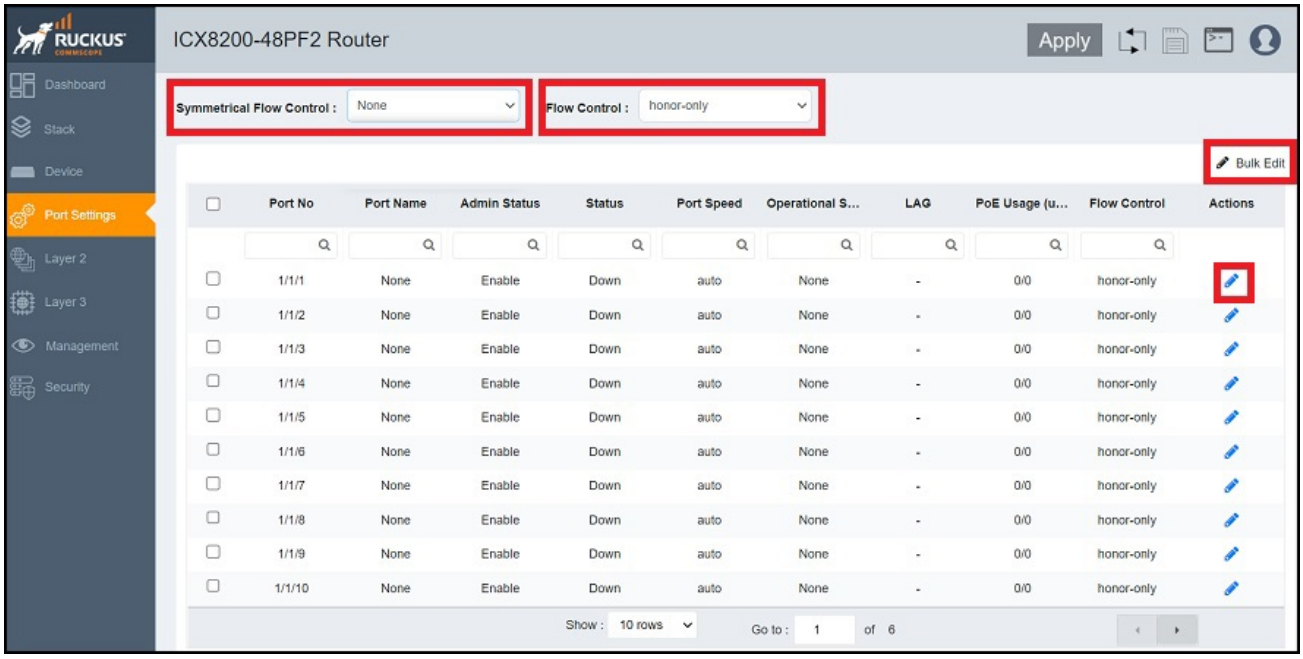
Complete the following steps to update the settings for a configured port, and to make bulk updates to some of the settings for all configured ports.

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

   The configured ports are listed in 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 30.
   - Configure flow control (globally): For more information, refer to Configuring Flow Control on page 30.
   - 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.

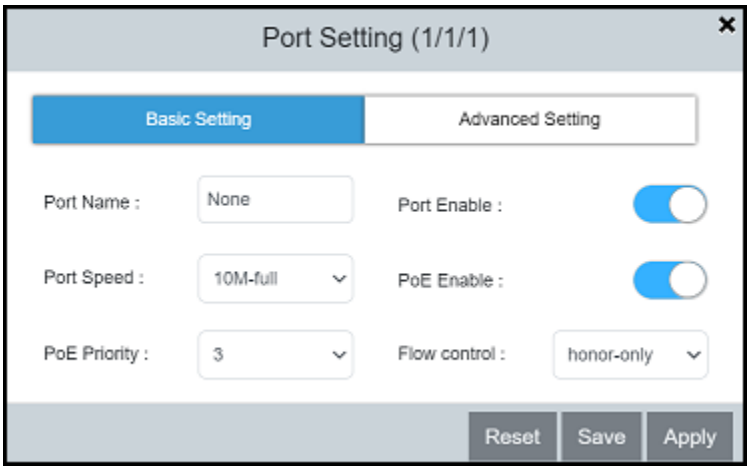
   FIGURE 9 Port Settings Web UI



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

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

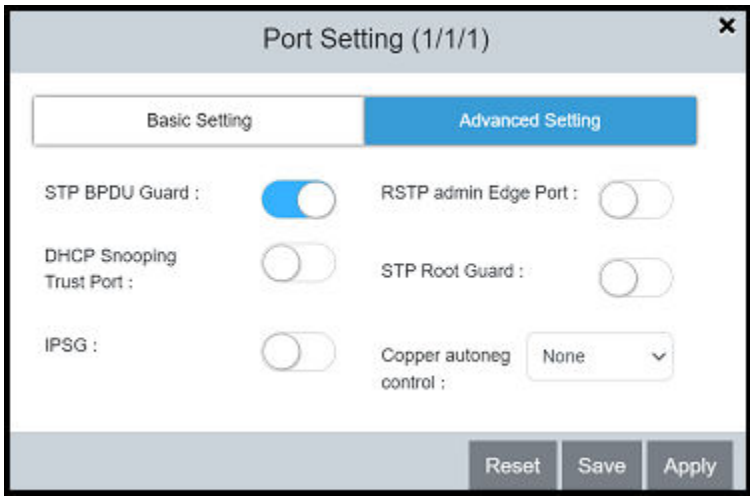
FIGURE 10 Port Setting: Basic Settings



- **Port Name**: Enter the updated port name.
- **Port Enable**: Enable or disable the port.
- **Port Speed**: Select the port speed.
- **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.
- **Flow control**: Select the following options from the list to configure flow control:
  - **both**: Configures flow control in PAUSE generation and honoring mode.
  - **generate-only**: Configures flow control in PAUSE generation mode only.
  - **honor-only**: Configures flow control in PAUSE honoring mode only.
  - **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, flow control is not negotiated with or advertised to the peer.
  - **None**: Disables flow control configurations.

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

   FIGURE 11 Port Setting: Advanced Settings



   - **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 autoneg 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 (Bulk Edit icon). The **Ports** dialog box is displayed.

FIGURE 12 Ports: Bulk Edit - Basic Setting

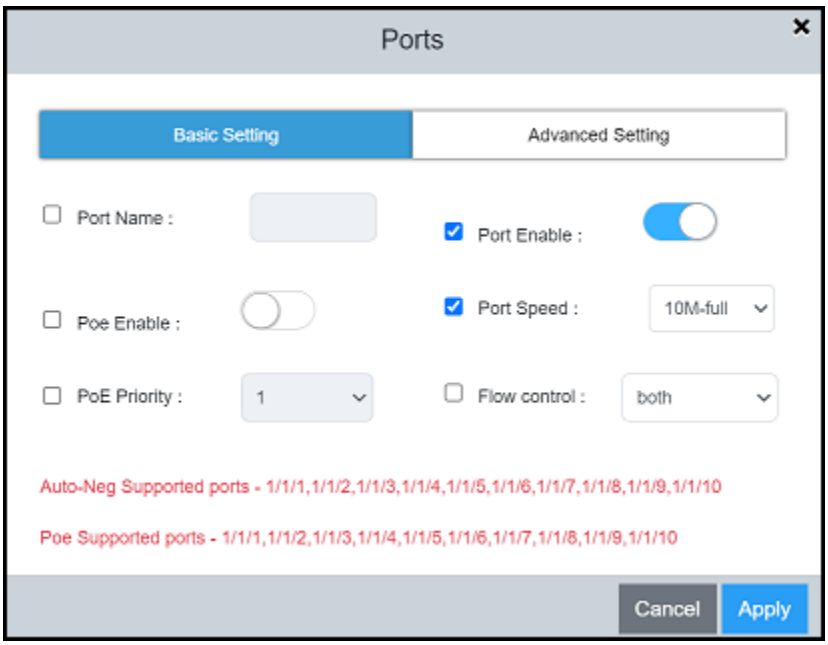
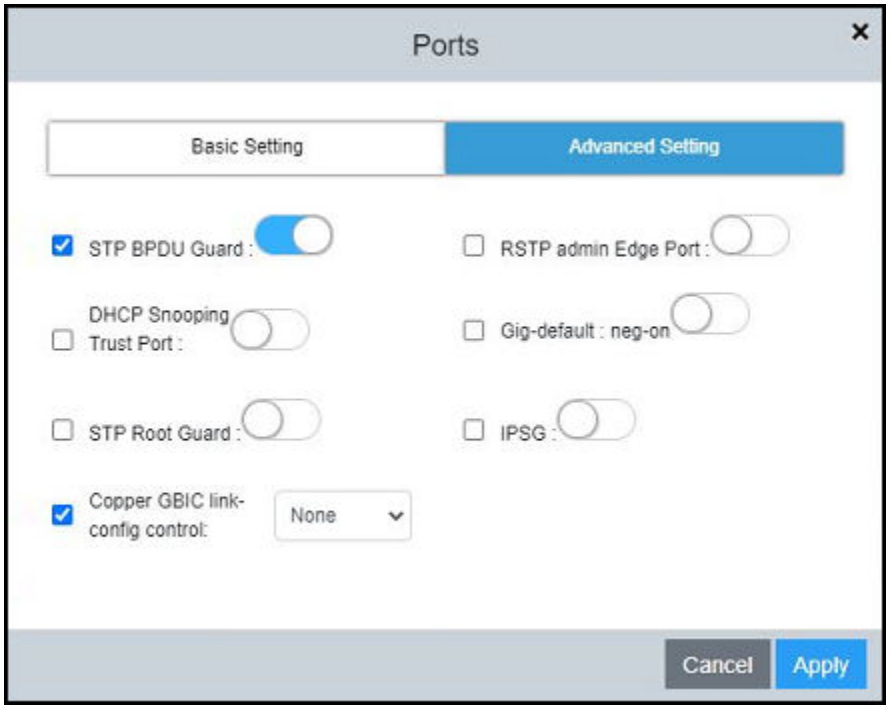


FIGURE 13 Ports: Bulk Edit - Advanced Setting



7. In the **Basic Setting** tab and the **Advanced Setting** tab, select the check box of each setting you want to enable and make the any other 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

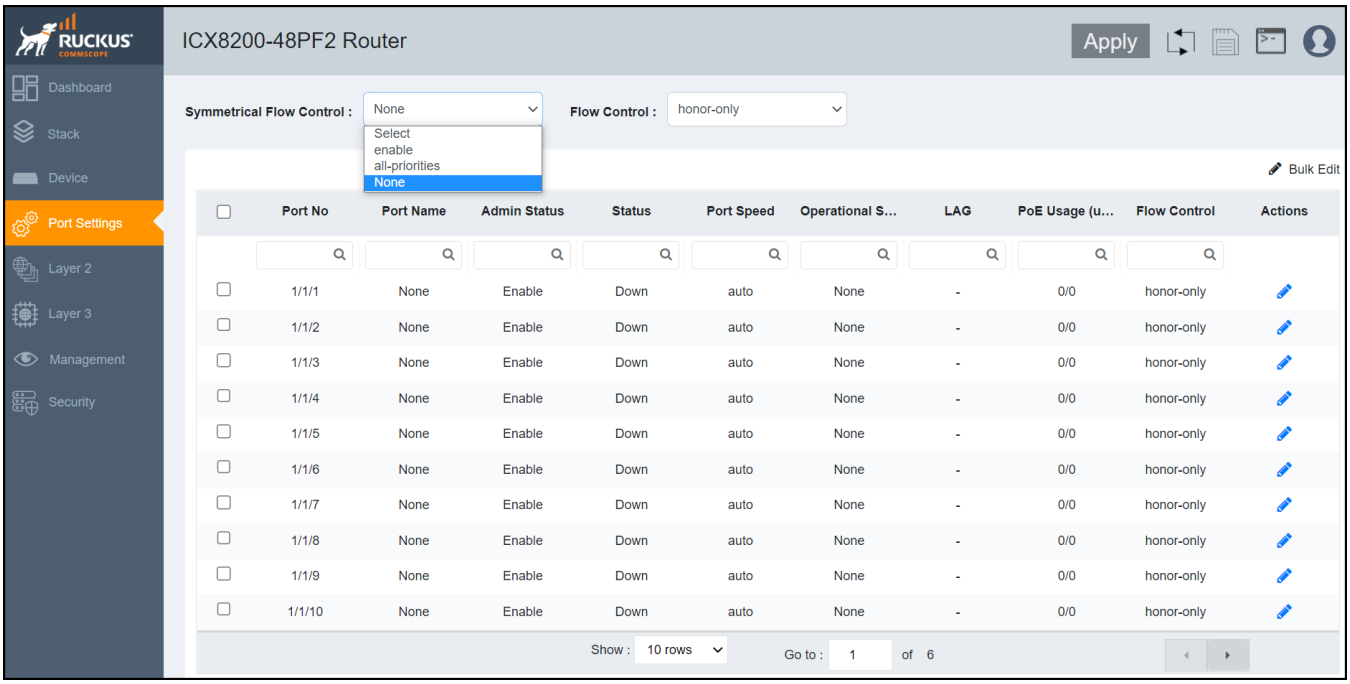
RUCKUS devices support symmetrical flow control (SFC), which means that the ports can both receive and transmit 802.3x PAUSE frames.

Complete the following steps to configure symmetric flow control.

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

   The configured ports are listed in the main pane.
2. For **Symmetric Flow Control**, select the following options from the 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.

FIGURE 14 Symmetric Flow Control Configuration



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 ICX 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.

Complete the following steps to configure flow control.

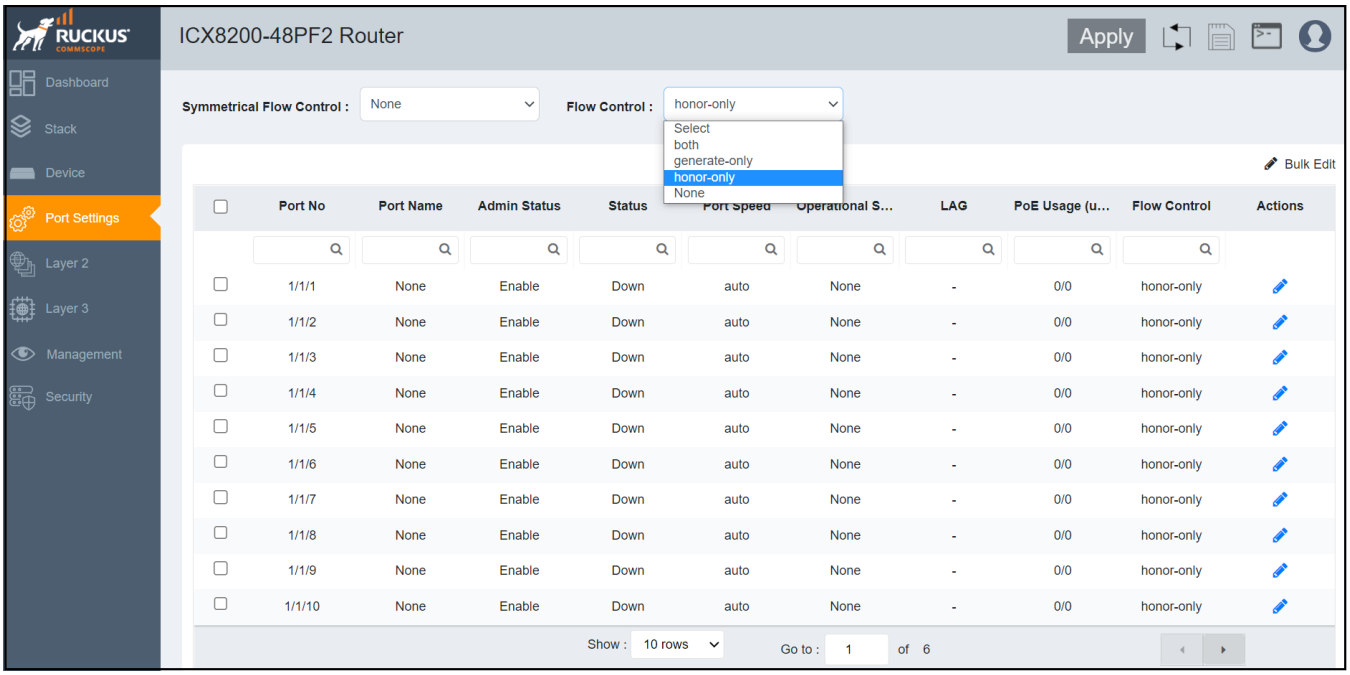
1. On the menu, click **Port Settings**.

   The configured ports are listed in the main pane.

2. For **Flow Control**, select the following options from the list to configure flow control:

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

FIGURE 15 Flow Control Configuration



Layer 3

- Configuring IP Static Routes..... 33
- Configuring a VE Port..... 34

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.

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 in the main pane.

   FIGURE 16 IP Routes

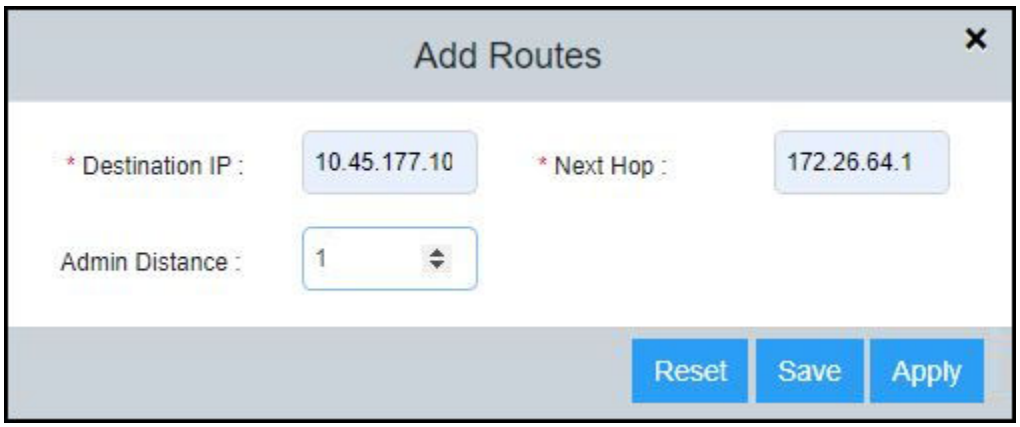


   You can perform the following actions:

   - 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 17 Adding Routes



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.

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

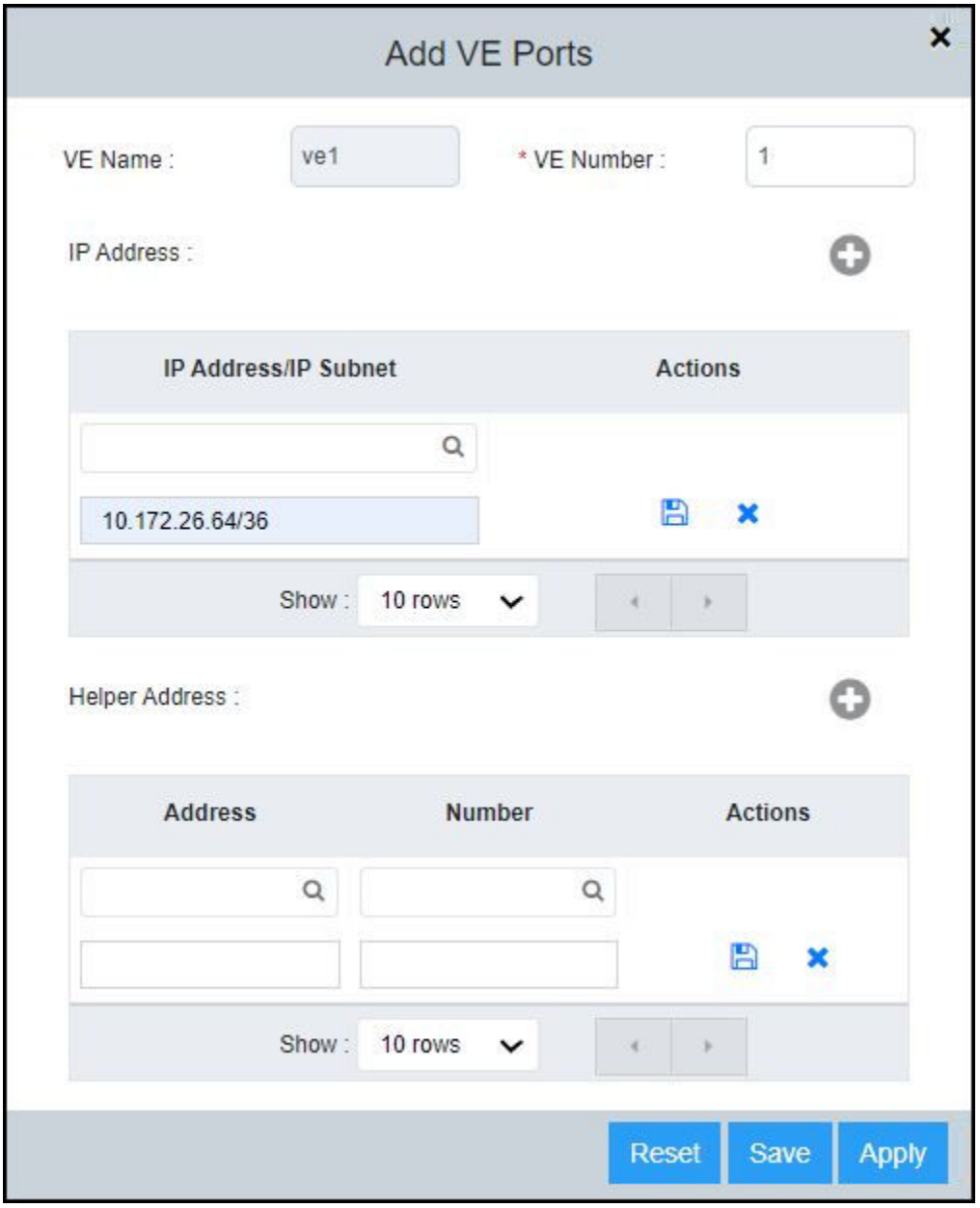
   All the configured Virtual Ethernet (VE) ports are listed in the main pane.

   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 the 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 18 Adding VE Ports



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

     NOTE
     A VE port is created only if the 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
     A helper address is displayed only if the 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..... 37
- Configuring Domain Name System Servers..... 38
- Upgrading FastIron Software..... 39
- Managing Running Configuration Backups..... 40
- Configuration Archive..... 41
- Managing Syslog Messages..... 49
- Managing the Polling Intervals..... 51
- Supportsave..... 51

Configuring an ICX Device to be Managed by SmartZone

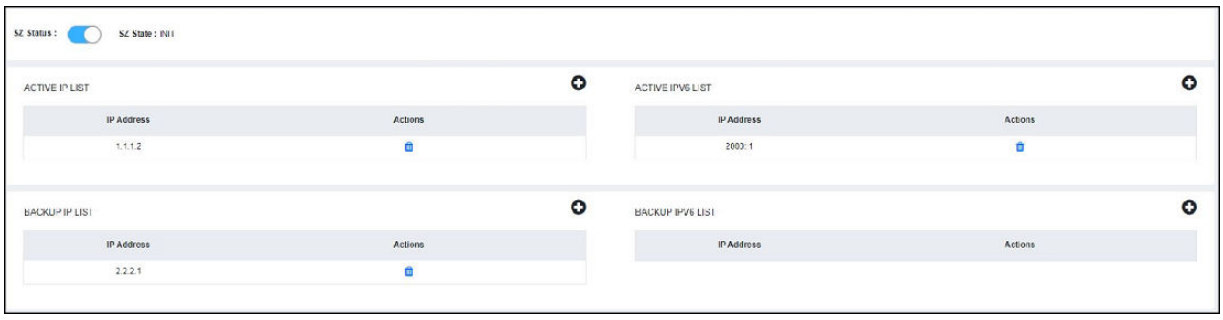
Beginning with SmartZone 5.0, SmartZone can be used to monitor and manage ICX switches. An ICX switch identifies SmartZone and initiates a connection based on the SmartZone IP addresses configured on the switch or discovered through DHCP Option 43. When SmartZone management is disabled, the ICX switch 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 19 SmartZone Connections



   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 the **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

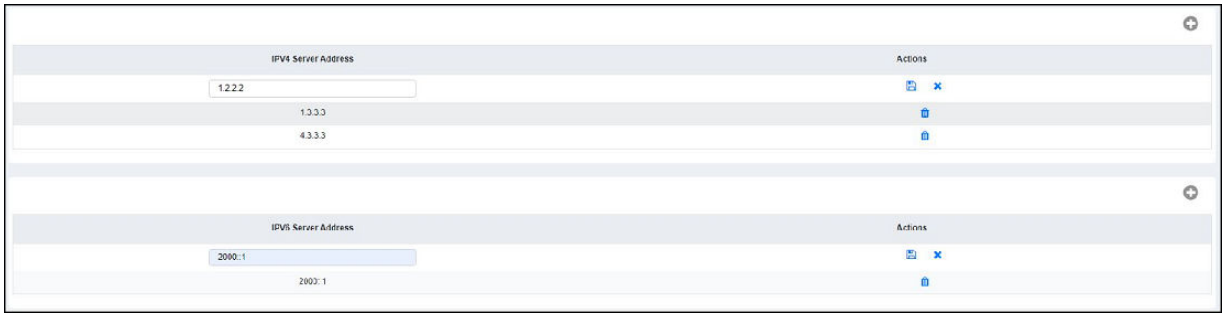
The Domain Name System (DNS) resolver is a feature in a Layer 3 device that sends and receives queries to and from the DNS server on behalf of a client. You can configure the RUCKUS device to recognize DNS servers. You can configure only up to four IPv4 server addresses and four IPv6 server addresses. 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 20 DNS Server Addresses



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

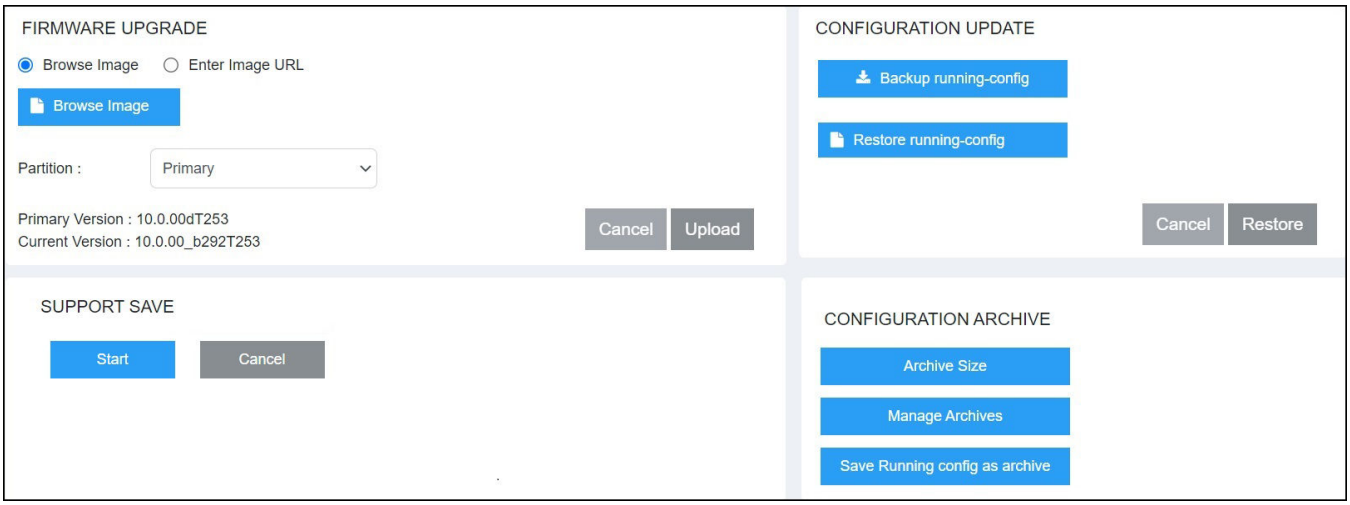
An ICX device can be upgraded to the latest software version to take advantage of new features and ensure optimal network performance.

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 an ICX 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 21 FastIron Firmware Upgrade



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.

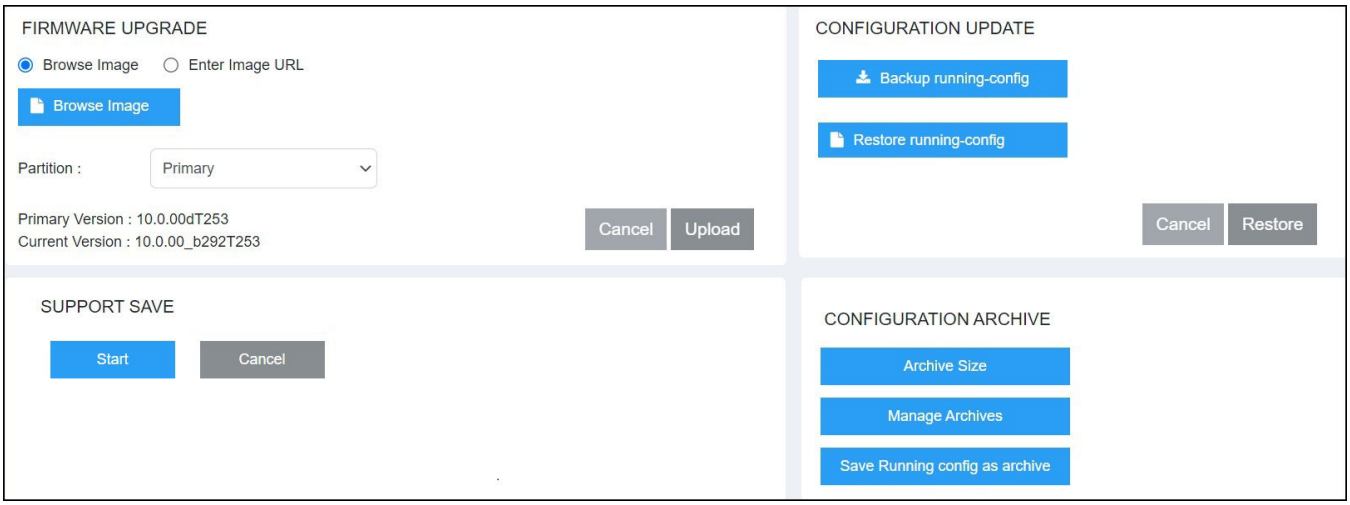
Managing Running Configuration Backups

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 22 Managing the Running Configuration File



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 memory, 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. The archive-naming convention requires archive names be prefixed with the predefined string "ICX7K_ARCHIVE". Configuration archive is supported on all RUCKUS ICX 7550, ICX 7650, ICX 7850, and ICX 8200 switches.

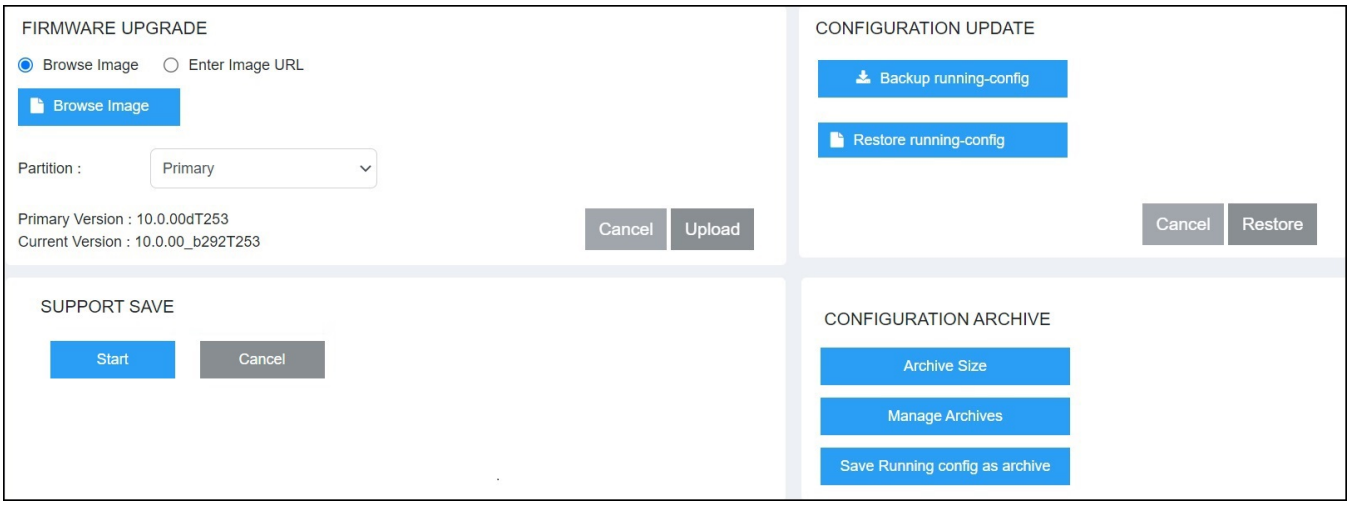
Configuring Archive Size

Archive size, which is a user-configurable value, determines the number of archives the system can maintain.

Complete the following steps to configure archive size.

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

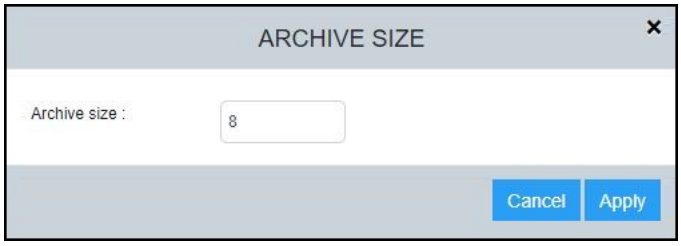
   FIGURE 23 Configuration Archive: Archive Size



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

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

   FIGURE 24 Setting Archive Size



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

   Valid values range from 5 through 100 archives. The default archive size is 100.

   If the existing number of archives in the system is greater than the user-configured archive size value, the oldest archives are deleted. For example, if the existing number of archives in the system is 8, and you configure the archive size to 6, the oldest two archive files to be deleted are listed in the dialog box. However, if you set the archive size to a value greater than the existing number of archive files, no archives are deleted.

4. Click **Apply**. A message is displayed indicating that the archive size has changed successfully, and details of the old value and the newly configured value.

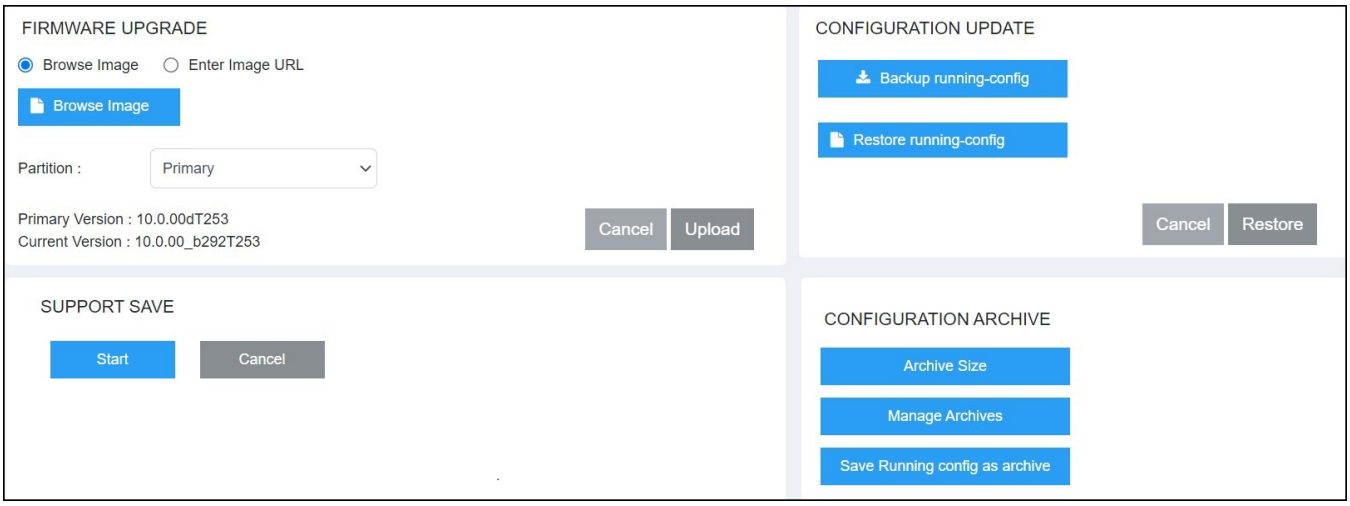
Saving the Running Configuration as an Archive File

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

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

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

   FIGURE 25 Configuration Archive: Saving the Running Configuration



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

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

   FIGURE 26 Saving the Running Configuration as an Archive



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

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

   If the number of archives in the system will exceed the configured archive size because of the addition of the new archive file, the oldest archive file that must be deleted is shown in the dialog box.

4. Click **Apply** to save the running configuration as an archive file. A message is displayed indicating that the running configuration has been saved successfully.

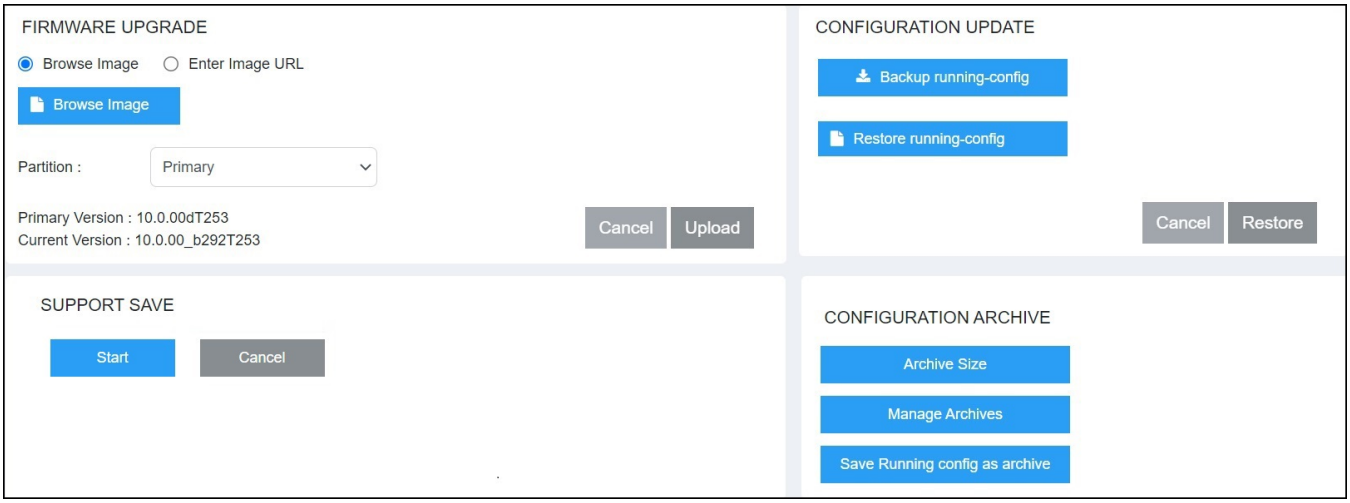
Managing Configuration Archives

You can perform various actions to manage the configuration archives. You can list, view, apply, copy, and delete the configuration archives.

Complete the following steps to manage configuration archives.

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

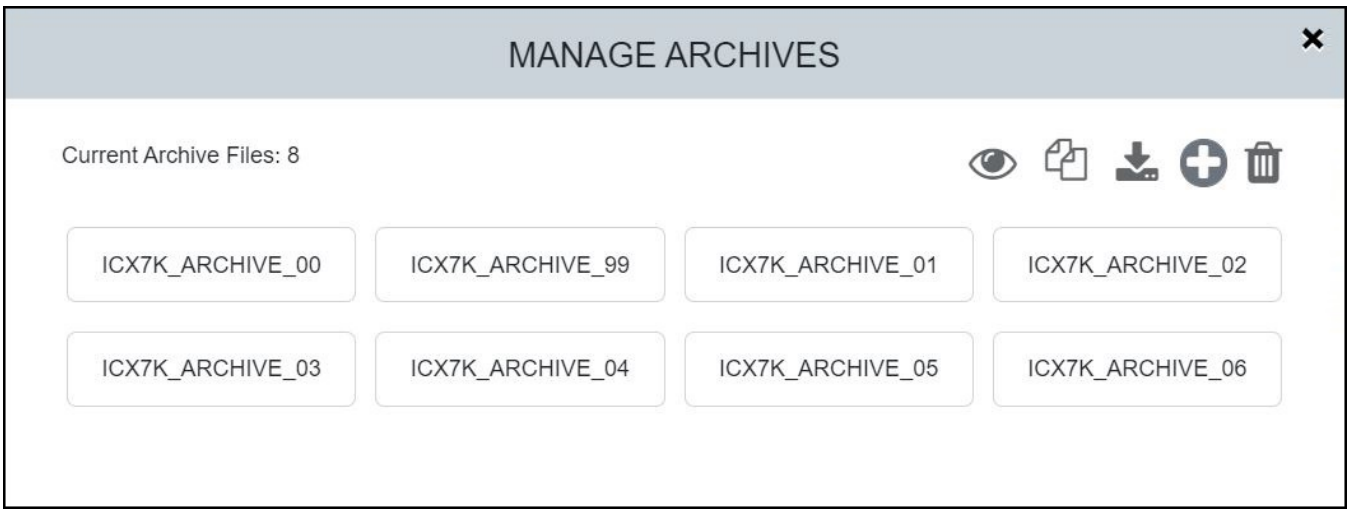
FIGURE 27 Configuration Archive: Managing Archives



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

   The **MANAGE ARCHIVES** dialog box is displayed. All the current configuration archive files are listed.

   FIGURE 28 Managing Archives



   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 configuration archives

Viewing Archive Content

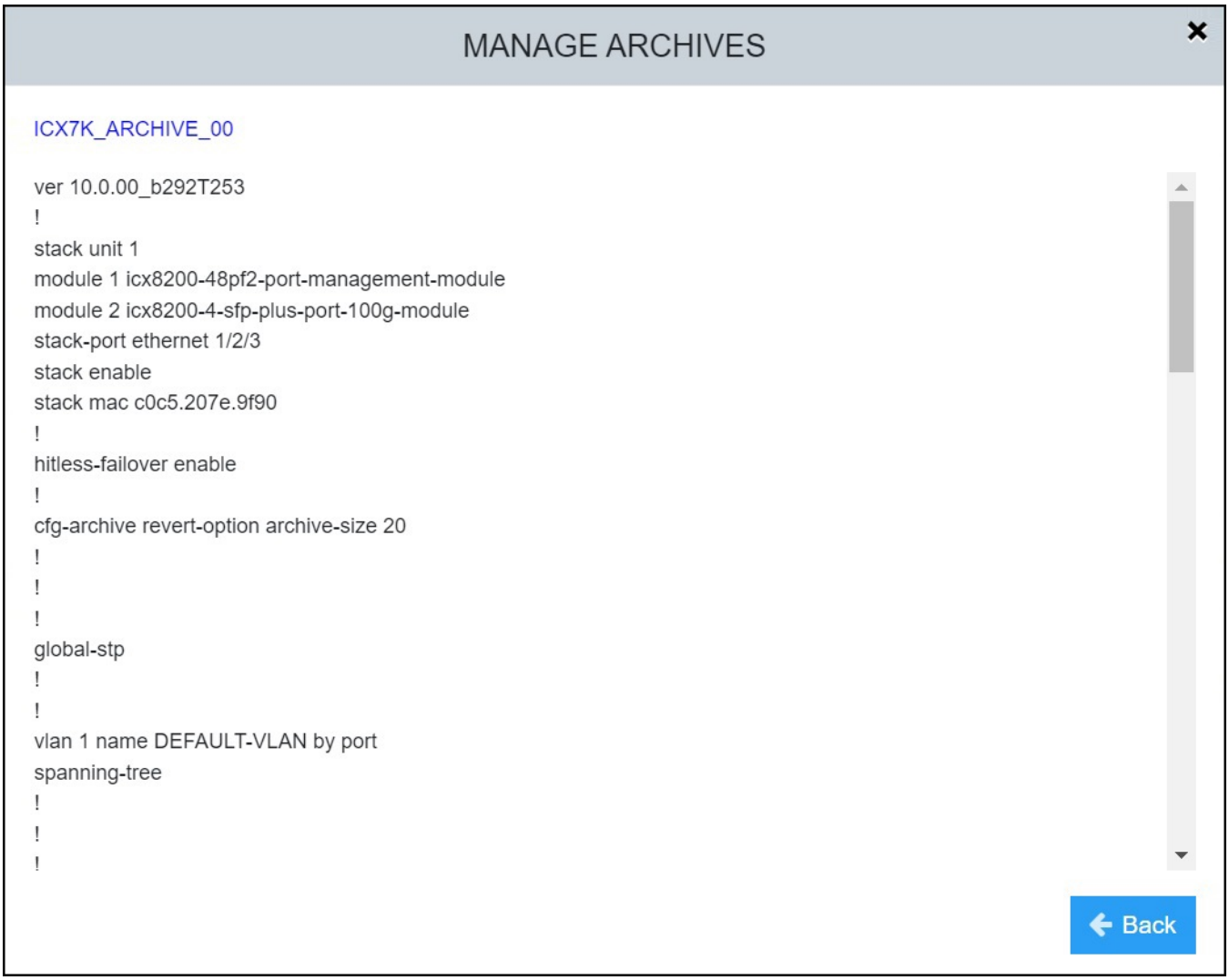
Complete the following steps to display the content of a specific archive.

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 configuration archive and click (View icon) to display the content of the selected configuration archive.

FIGURE 29 Viewing Archive Content



4. Click **Back** to return to the **MANAGE ARCHIVES** dialog box.

Copying an Archive to Another Archive

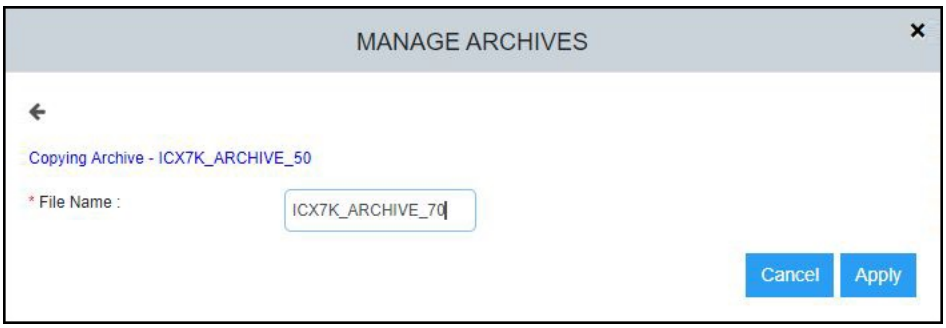
Complete the following steps to copy an archive to another archive.

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 configuration archive and click (Copy icon).

FIGURE 30 Copying a Configuration Archive



4. In the **File Name** field, enter a name following 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.

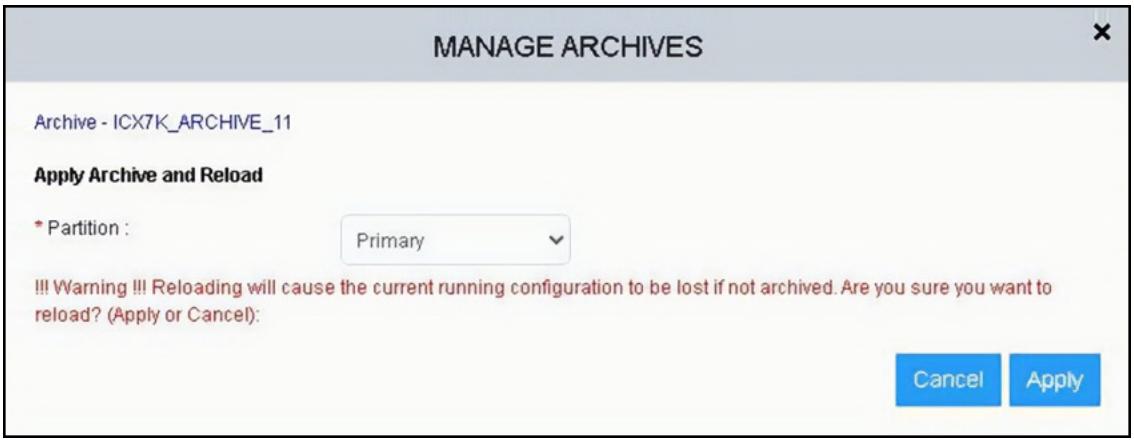
Applying an Archive to the System

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 31 Applying a Configuration Archive



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

Uploading an Archive to the System

Complete the following steps to upload an archive to the system.

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 saved configuration archive file from the local machine and click (Add icon) to upload the archive to the system.

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

   FIGURE 32 Uploading an Archive



   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 must be deleted is shown in the dialog box.

4. Click **Apply** to load the system with the specified configuration archive.

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

   FIGURE 33 Upload Archive Status



Deleting an Archive

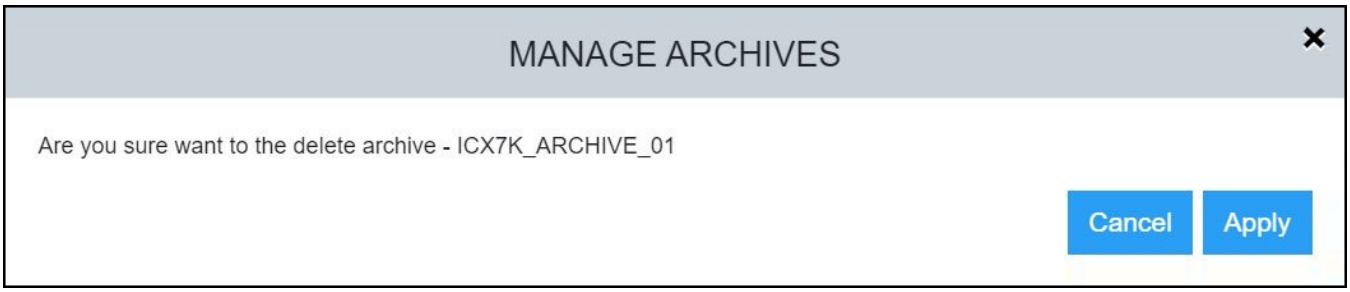
Complete the following steps to delete a specific archive.

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 configuration archive and click (Delete icon) to delete the selected configuration archive. A confirmation dialog box is displayed.

   FIGURE 34 Deleting a Configuration Archive



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

   A message is displayed indicating that the configuration archive has been deleted successfully.

5. Click **Back** to return to the **MANAGE ARCHIVES** dialog box.

Managing Syslog Messages

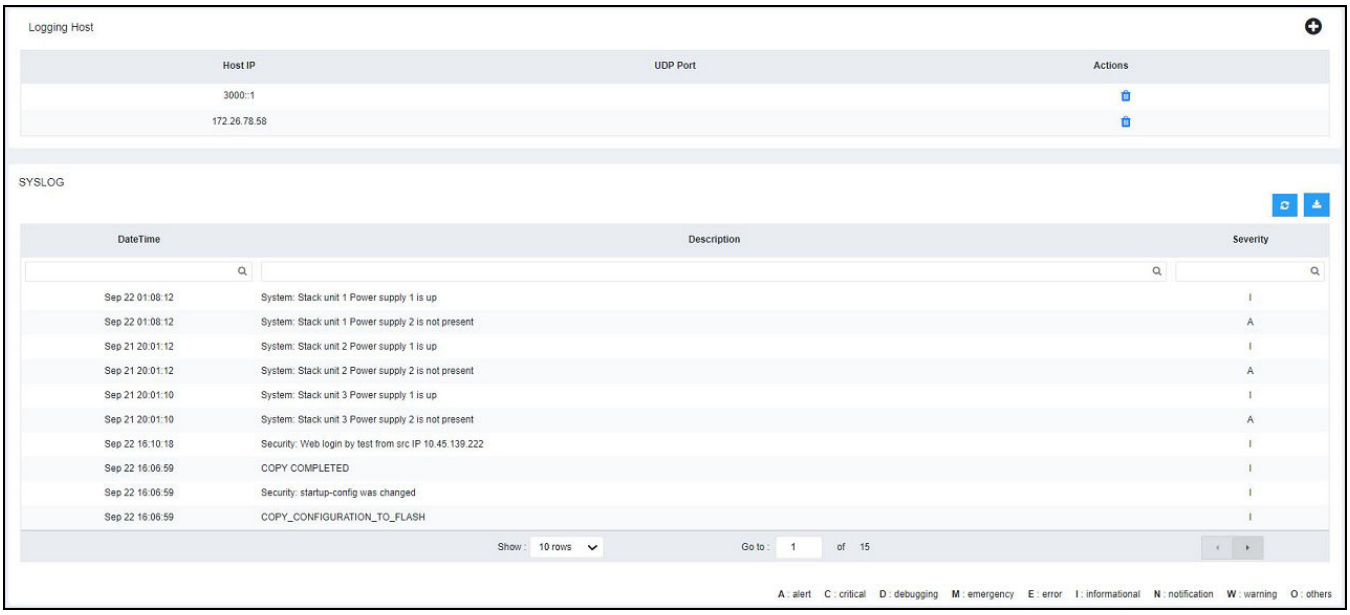
You can configure the logging host (syslog server) to which syslogs are sent. Events that are logged by the device can be viewed and downloaded for debugging and troubleshooting purposes.

Complete the following steps to configure the 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 35 Syslog Details



   You can perform the following actions:

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

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

FIGURE 36 Adding a Logging Host



3. Complete the following fields:
   - **Host IP**: Enter the remote host address (either an IPv4 address or IPv6 address).
   - **UDP Port**: Enter the UDP port number.
4. Click **Apply** to add the 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: • Emergency (M) • Alert (A) • Critical (C) • Error (E) • Warning (W) • Notification (N) • Informational (I) • Debugging (D) • Others (O)

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

Managing the Polling Intervals

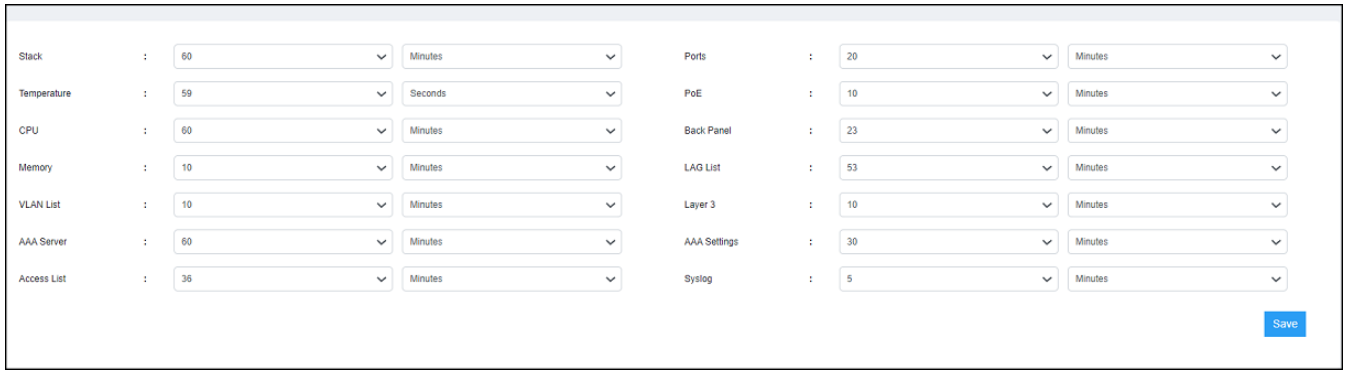
Polling the device at regular intervals helps you to monitor the device performance and the network health. The device polls the data to check system status, ports, connectivity, reachability, CPU, memory utilization, temperature, chassis, and so on. You can view and change the poll interval settings 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 37 Polling Interval Details



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 ICX modules. The collected logs are shared with technical support personnel for investigating issues experienced on an ICX device. RUCKUS recommends running supportsave before upgrading the firmware on a switch, so that you have the necessary information should an issue arise.

NOTE
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, supportsave sends a request to the ICX device, which begins to collect the supportsave logs and places them into two files with .tgz extensions. One of the .tgz files contains the core and log files. The other .tgz file contains **show** command output. The files are copied over an HTTPS channel to the download location.

If you are running supportsave 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.

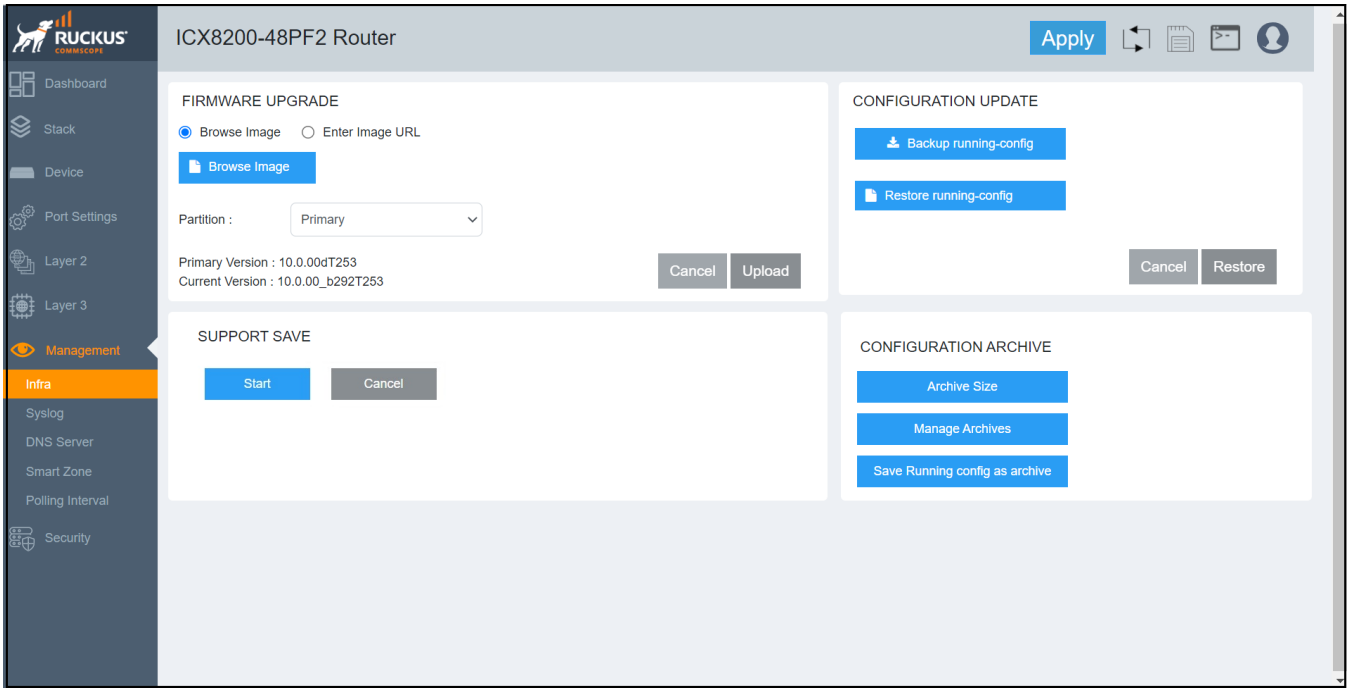
NOTE
You cannot click the **Start** botton in the **SUPPORT SAVE** pane again until the previous request is completed.

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

Complete the following steps to use supportsave to collect logs.

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

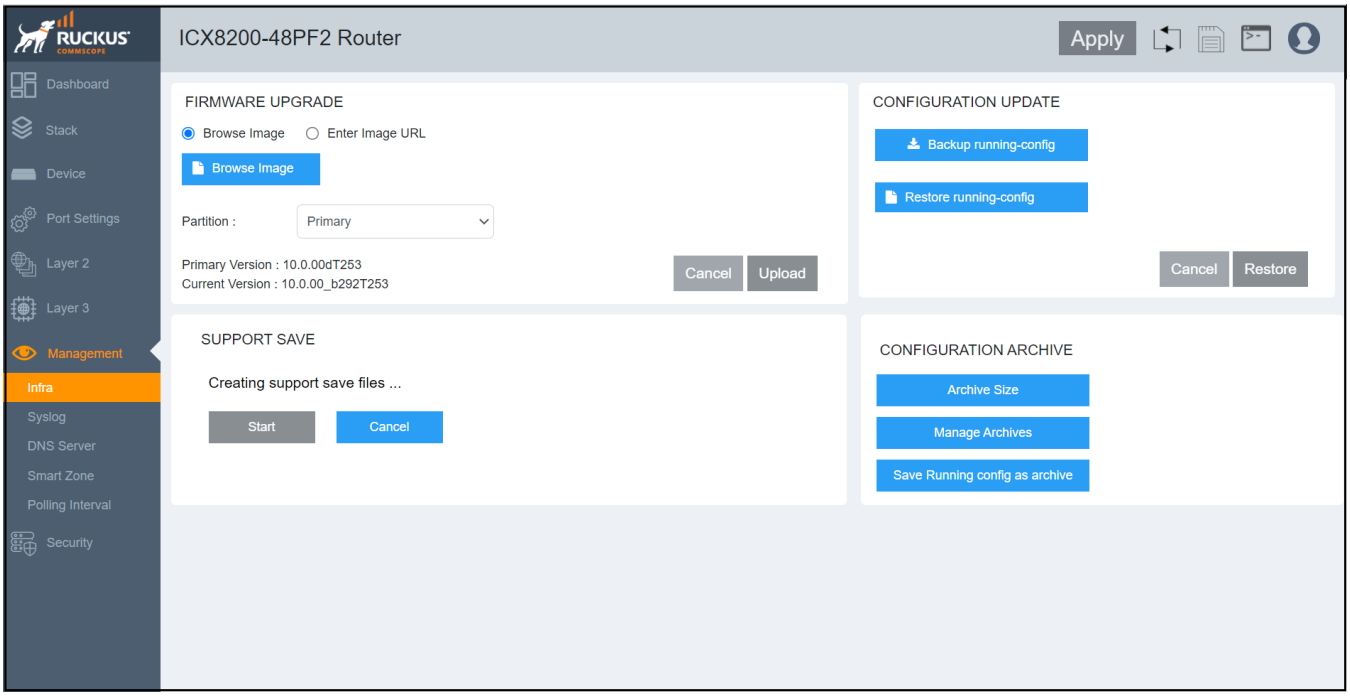
FIGURE 38 Infra Management Page



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

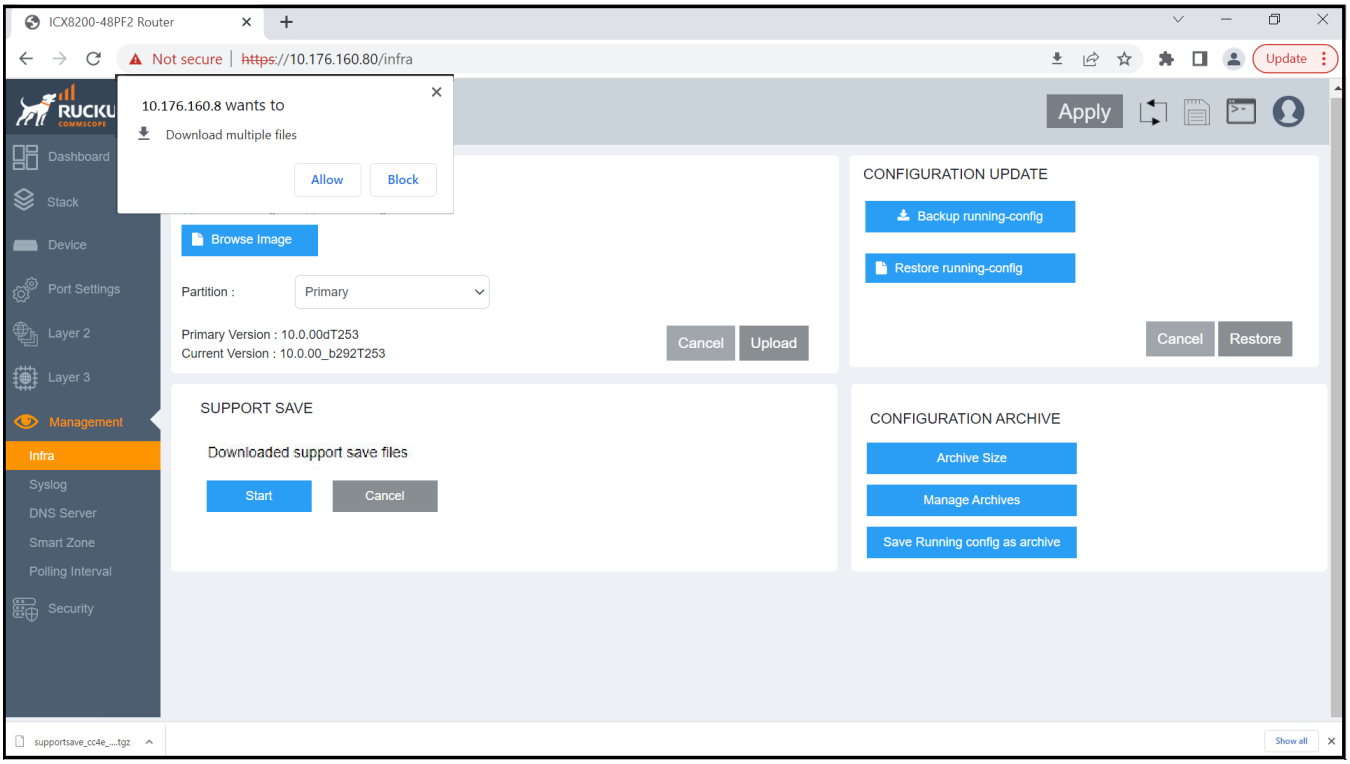
NOTE
To cancel a supportsave operation in progress, click **Cancel**. While the cancel operation is in progress, you cannot click **Start** or **Cancel**. The options become available again when the cancel operation is complete.

FIGURE 39 Supportsave in Progress



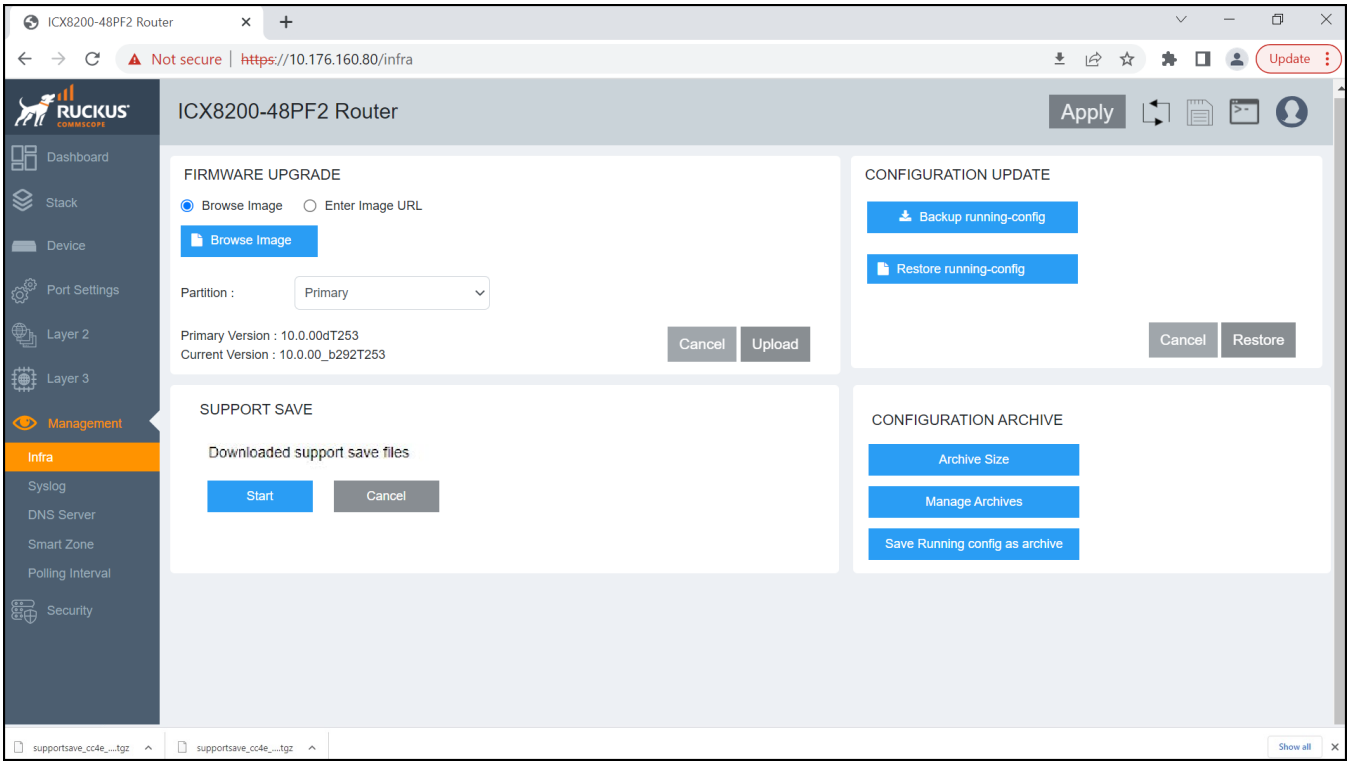
If you are running supportsave from the web interface for the first time, you must select **Allow** in the dialog box requesting permission to download multiple files to start the multiple file download.

FIGURE 40 Multiple File Confirmation



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 41 Supportsave Completed



Security

- Access Control Lists..... 57
- AAA Servers..... 61

Access Control Lists

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 a minimal number of 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 a Standard IPv4 ACL

Complete the following steps to configure a standard IPv4 ACL.

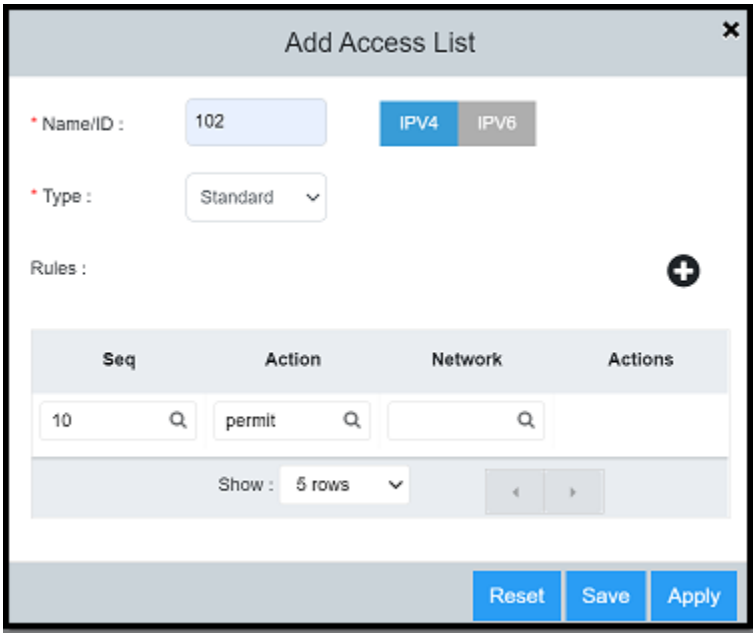
1. On the menu, click **Security** > **ACL**.

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

   - Add an ACL: Continue to step 2 to add a new ACL.
   - Edit an ACL: Click (Edit icon) to display the **Edit Access List** dialog box. You can delete the existing rule or add new rules. Make the necessary changes and click **Apply** to apply the changes.
   - Delete an ACL: Click (Delete icon) to display the **Delete Access List** dialog box. Click **Apply** to delete the ACL.

2. Click (Add icon) to display the **Add Access List** dialog box.

FIGURE 42 Adding an IPv4 Standard ACL



3. Select the **IPv4** tab and complete the following fields:
   - **Name/ID**: Enter a unique ACL name or number.
   - **Type**: Select **Standard** from the list to create a standard IPv4 ACL.
4. For **Rules**, click (Add icon) to add ACL rules with the following parameters:

   NOTE
   All the parameters are mandatory.

   - **Seq**: Assign a sequence number to the ACL rule.
   - **Action**: Select **permit** or **deny** from the list to filter the traffic according to the rules.
   - **Network**: Enter the source IP address.
5. Click **Apply** to create the standard IPv4 ACL.

Configuring an Extended IPv4 ACL

Complete the following steps to configure an extended IPv4 ACL.

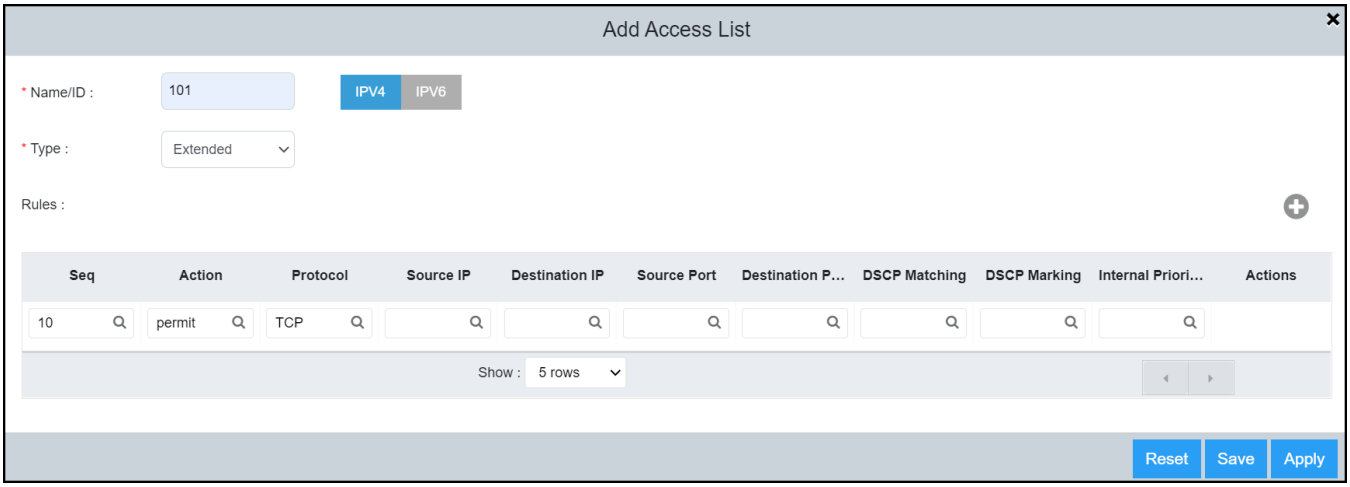
1. On the menu, click **Security** > **ACL**.

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

   - Add an ACL: Continue to step 2 to add a new ACL.
   - Edit an ACL: Click (Edit icon) to display the **Edit Access List** dialog box. You can delete the existing rule or add new rules. Make the necessary changes and click **Apply** to apply the changes.
   - Delete an ACL: Click (Delete icon) to display the **Delete Access List** dialog box. Click **Apply** to delete the ACL.

2. Click (Add icon) to display the **Add Access List** dialog box.

   FIGURE 43 Adding an Extended IPv4 ACL



3. Select the **IPv4** tab and complete the following fields:
   - **Name/ID**: Enter a unique ACL name or number.
   - **Type**: Select **Extended** from the list to create an extended IPv4 ACL.

4. For **Rules**, 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 list to filter the traffic according to the rules.
   - **Protocol**: Select the protocol type (IP, TCP, or UDP) to be specified as a match for filtering.
   - **Source IP**: Enter the source IP address for which you want to filter the subnet.
   - **Destination IP**: Enter the destination IP 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**: Allows filtering 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 the extended IPv4 ACL.

Configuring an IPv6 ACL

Complete the following steps to configure an IPv6 ACL.

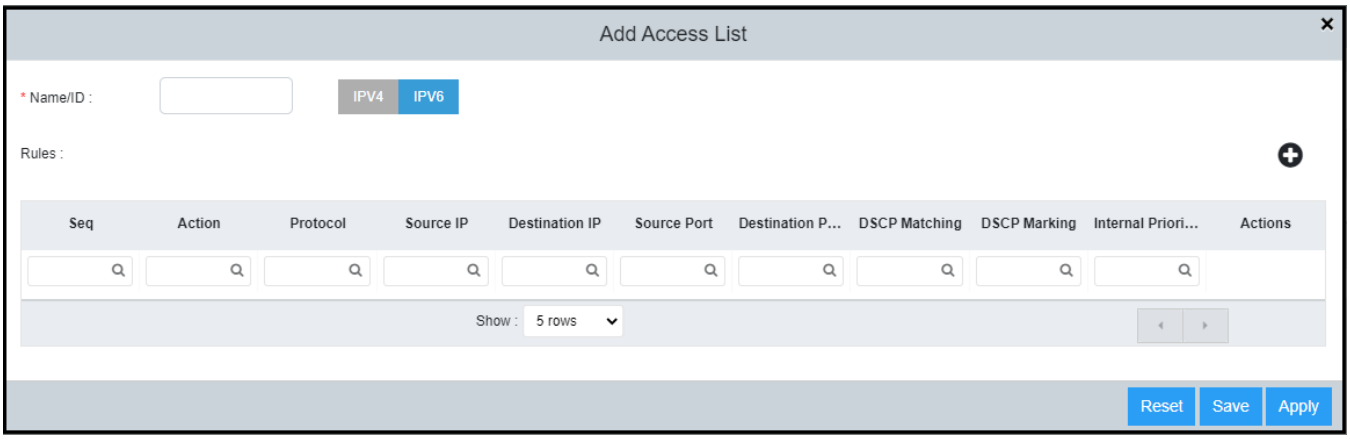
1. On the menu, click **Security** > **ACL**.

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

   - Add an ACL: Continue to step 2 to add new ACL.
   - Edit an ACL: Click (Edit icon) to display the **Edit Access List** dialog box. You can delete the existing rule or add new rules. Make the necessary changes and click **Apply** to apply the changes.
   - Delete an ACL: Click (Delete icon) to display the **Delete Access List** dialog box. Click **Apply** to delete the ACL.

2. Click (Add icon) to display the **Add Access List** dialog box.

   FIGURE 44 Adding an IPv6 ACL



3. Select the **IPv6** tab and enter a unique ACL name in the **Name/ID** field.
4. For **Rules**, 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 list to filter the traffic according to the rules.
   - **Protocol**: Select the protocol type (IPv6, TCP or UDP) to be specified as a match for filtering.
   - **Source IP**: Enter the source IP address for which you want to filter the subnet.
   - **Destination IP**: Enter the destination IP 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**: Allows filtering 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 the IPv6 ACL.

AAA Servers

Authentication, authorization, and accounting (AAA) is a set of services to regulate access to system resources, enforce privilege policies, and assess 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 purposes 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 levels 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 authorization level of the user. The authorization level 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 in to the device or the system is rebooted. Accounting information includes session start and stop time, the amount of system time, the services accessed, and the amount of data that a user has sent or received during a session.

If authorization is enabled and a 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 a Local User Account

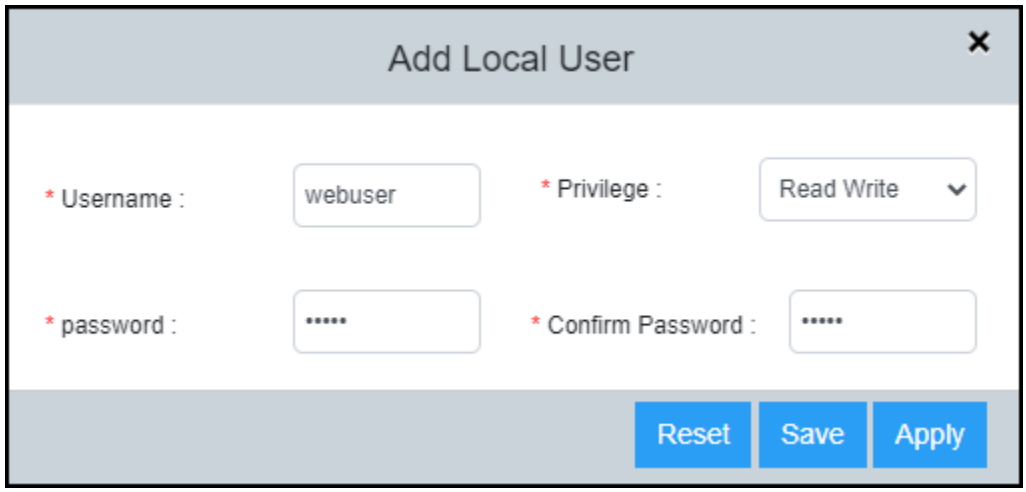
Complete the following steps to configure the user account in a local database.

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

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

   - Add a user account: Continue to step 3 to add a new user account.
   - Edit a user account: Click (Edit icon) to display the **Edit Local User** dialog box. Make the necessary changes and click **Apply** to apply the changes.
   - Delete a user account: Click (Delete icon) to display the **Delete Local User** dialog box. Click **Apply** to delete the user account.
3. In the **Local Users** tab, click (Add icon) to display the **Add Local User** dialog box.

   FIGURE 45 Adding a Local User Account



4. Complete the following fields:
   - **Username**: Enter a username for the user.
   - **Privilege**: Select the desired privilege level for the user from the 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 the 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 the local user account.

Configuring a RADIUS Server

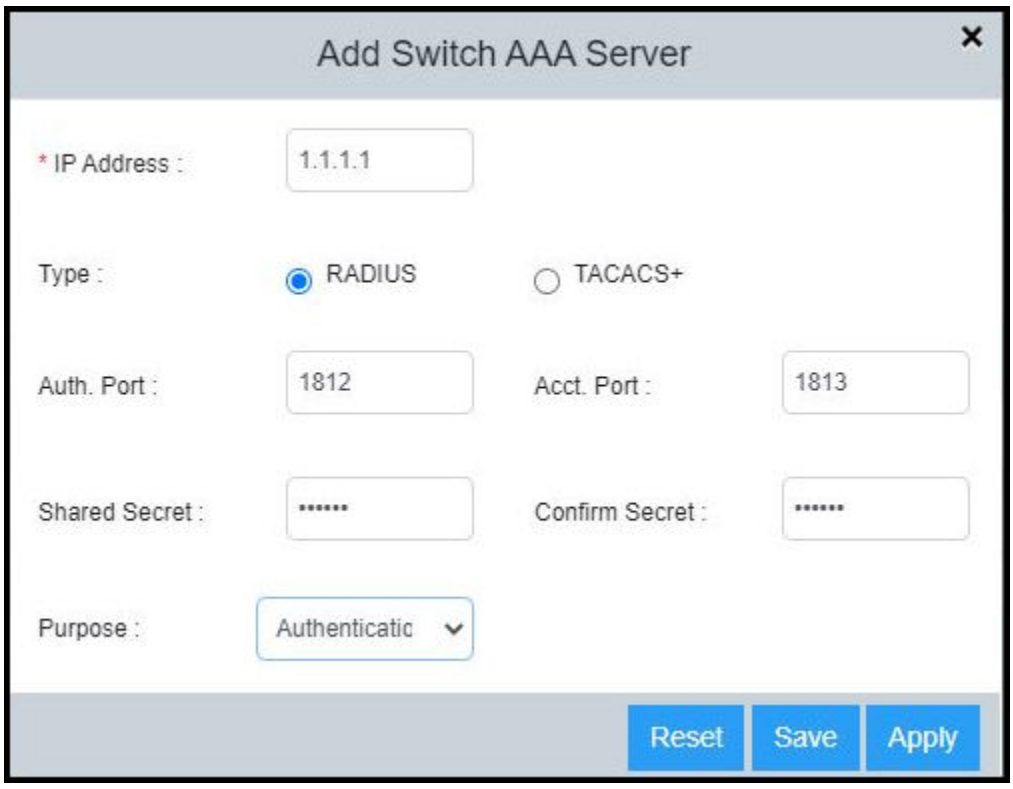
Complete the following steps to configure a RADIUS server.

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

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

   - Add a server: Continue to step 3 to add a new server.
   - Edit a server: Click (Edit icon) to display the **Edit Switch AAA Server** dialog box. Make the necessary changes and click **Apply** to apply the changes.
   - Delete a server: Click (Delete icon) to display the **Delete Switch AAA Server** dialog box. Click **Apply** to delete the server.
3. In the **AAA Servers** tab, click (Add icon) to display the **Add Switch AAA Server** dialog box.

   FIGURE 46 Adding a RADIUS Server



4. Select **Radius** as the AAA server type.

5. Complete the following fields:
   - **IP Address**: Assign an IP address to the RADIUS server. The IP address can be in the IPv4 format or IPv6 format.
   - **Auth. Port**: Enter the RADIUS authentication port number. The default value is 1812.
   - **Acct. Port**: Enter the RADIUS accounting port number. The default value 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 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 the RADIUS server.

Configuring a TACACS+ Server

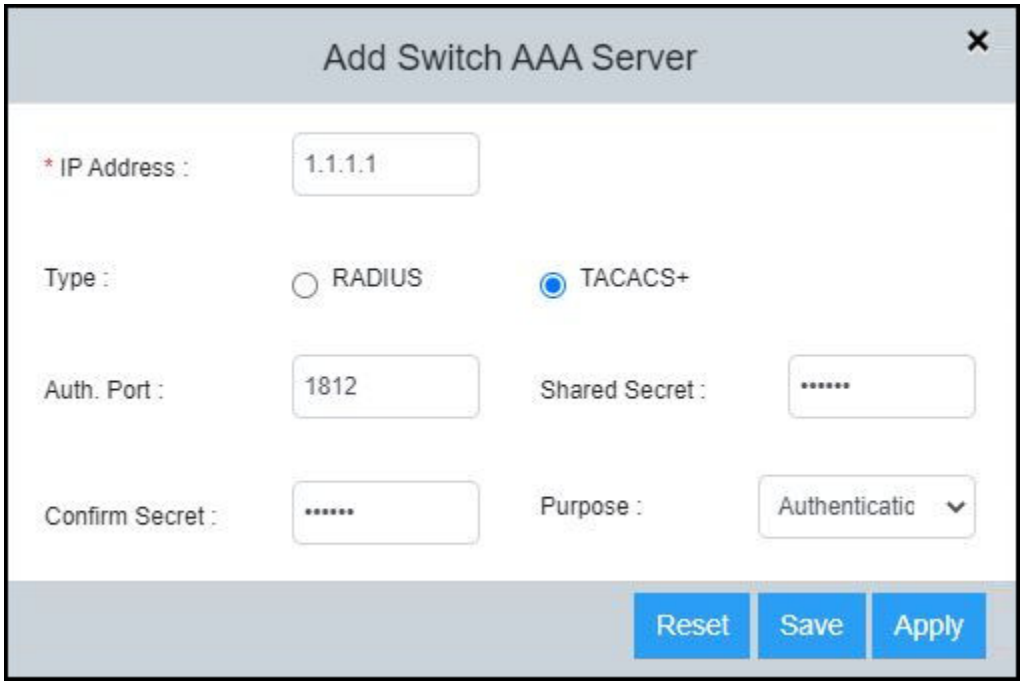
Complete the following steps to configure a TACACS+ server.

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

   All the configured servers are listed in the main pane. You can perform the following actions:
   - Add a server: Continue to step 3 to add a new server.
   - Edit a server: Click (Edit icon) to display the **Edit Switch AAA Server** dialog box. Make the necessary changes and click **Apply** to apply the changes.
   - Delete a server: Click (Delete icon) to display the **Delete Switch AAA Server** dialog box. Click **Apply** to delete the server.

3. In the **AAA Servers** tab, click (Add icon) to display the **Add Switch AAA Server** dialog box.

FIGURE 47 Adding a TACACS+ Server



4. Select **Tacacs+** as the AAA server type.
5. Complete the following fields:
   - **IP Address**: Assign an IP address to the TACACS+ server. The IP address can be in the 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 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 the TACACS+ server.

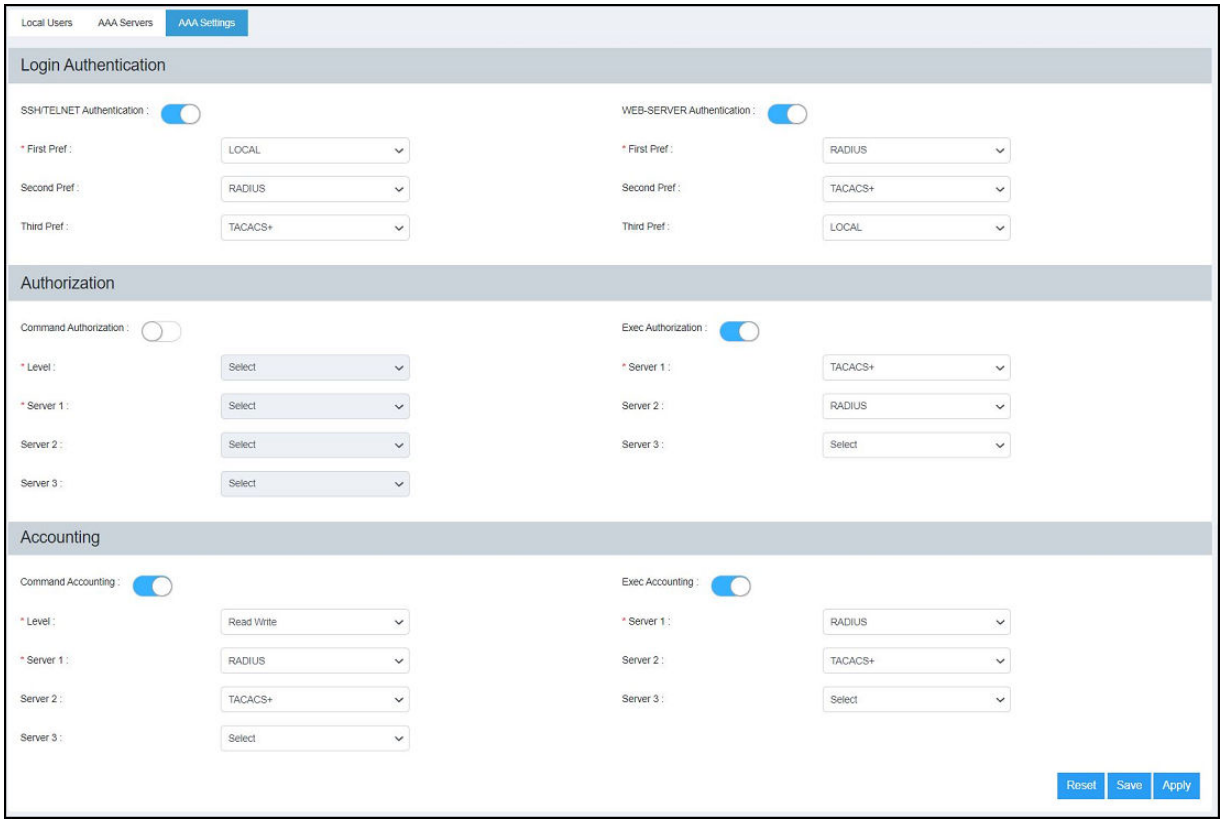
Managing AAA Settings

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 48 AAA Settings



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**: You can 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.



© 2023 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com