

# RUCKUS SmartZone (ST-GA) Switch Management Guide, 7.0.0

**Supporting SmartZone 7.0.0**

© 2024 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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

## Patent Marking Notice

For applicable patents, see [www.cs-pat.com](http://www.cs-pat.com).

# Contents

---

<b>Contact Information, Resources, and Conventions.....</b>	<b>5</b>
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
<b>About This Guide.....</b>	<b>9</b>
New in This Document.....	9
<b>Managing ICX Switches from SmartZone.....</b>	<b>11</b>
Supported ICX Models.....	11
Overview of ICX Switch Management.....	14
Preparing ICX Devices to be Managed by SmartZone.....	14
ICX Switch Behavior with SmartZone.....	15
Enabling an ICX Device to Be Managed by SmartZone.....	16
Configuring the ICX Source Address to Be Used by SmartZone.....	16
Configuring a Custom Port Number for Connection to SmartZone.....	17
Setting Up Switch Registrar Discovery.....	18
How Switch Registrar Discovery Works.....	18
Disabling or Enabling Switch Registrar Discovery.....	18
Confirming Successful Switch Registrar Discovery.....	19
Troubleshooting Switch Registrar Discovery.....	20
Preparing Stacking Devices to Connect to SmartZone.....	20
Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch.....	21
Manually Configuring the SmartZone IP Address on an ICX Switch.....	21
Displaying the SmartZone Connection Status.....	21
Disconnecting the ICX Switch from SmartZone.....	22
Disabling SmartZone Management on the ICX Switch.....	22
<b>Working with Switches.....</b>	<b>23</b>
SmartZone Switch Management.....	23
Using Controller Settings to Manage Switch Groups.....	23
Creating Switch Groups.....	23
Creating Switch Registration Rules.....	27
Moving the Switches between Groups.....	30
Deleting Switches.....	31
Backing up and Restoring Switch Configuration.....	32
Improving Switch Configuration Change Management.....	35
Rehoming Switches.....	36
Switching Over Clusters.....	37
Scheduling a Firmware Upgrade for Switch Group.....	37
Scheduling a Firmware Upgrade for Selected Switches.....	40

Viewing Switch Information.....	44
Configuring the Switch.....	47
Data Synching on the Switch Table.....	62
Switch Level Configuration.....	63
Generic CLI Configuration.....	71
Creating Config Backup for Switch Group.....	89
Viewing Configuration Alerts.....	90
Port Settings.....	91
Creating Routing Configurations.....	104
Managing Link Aggregation Groups (LAGs).....	107
Creating a Switch Stack.....	109
Viewing Port Details.....	110
Viewing Switch Health.....	114
Viewing Alarms.....	117
Viewing the Events.....	120
Viewing LLDP Neighbor Information.....	120
Viewing Traffic Trends in the Switch.....	121
Viewing Firmware History of the Switch.....	123
Deleting the Firmware Upgrade Schedules.....	123
Configuring the Group Firmware Settings.....	125
Accessing the Switch CLI through Controller (Remote CLI).....	127
Viewing PoE Utilization and Health Status of the Switch.....	130
Ability to Convert Standalone Switch to Stack.....	133
Troubleshooting Switch Issues.....	137
Troubleshooting Using Custom Events.....	138
Troubleshooting Using Remote Operations.....	140
Cable Testing on ICX Ports.....	143
Viewing Switches on the Dashboard.....	146

# 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.ruckusnetworks.com> 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](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](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](mailto:#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.ruckusnetworks.com>.

## 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	<code>device(config)# interface ethernet 1/1/6</code>
<b>bold</b>	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> 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
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	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, <i>member[member...]</i> .
\	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 Guide

- [New in This Document](#)..... 9

## New in This Document

**TABLE 2** Key Features and Enhancements in *SmartZone 7.0.0 Rev A*

Feature	Description	Reference
Providing feedback on the firmware upgrade.	<b>New:</b> The feature allows you to view six stages of firmware upgrade process on the controller.	<a href="#">Scheduling a Firmware Upgrade for Selected Switches</a> on page 40
Improving the usability of port templates.	<b>Updated:</b> The feature allows you to apply the port template without selecting a port in the beginning .	<a href="#">Creating and Managing Port Templates</a> on page 91
Enabling support for switch breakout ports on the controller.	<b>Updated:</b> The feature allows you to view and configure breakout ports with VLAN, LAG (Link Aggregation Group), and IP Port functions deployments.	<ul style="list-style-type: none"> <li>• <a href="#">Managing Link Aggregation Groups (LAGs)</a> on page 107</li> <li>• <a href="#">Creating Switch Model-Based Configurations</a> on page 52</li> <li>• <a href="#">Creating Routing Configurations</a> on page 104</li> <li>• <a href="#">Viewing Port Details</a> on page 110</li> </ul>
Allowing controller to have separate Auth and Acctn servers.	<b>Updated:</b> The feature allows you to configure multiple RADIUS servers with Authentication and Accounting usages, respectively.	<a href="#">Creating a Common Configuration</a> on page 48
Improving Configuration Change.	<b>New:</b> The feature allows the controller to verify the switch with a Master backup every hour for any configuration changes.	<a href="#">Improving Switch Configuration Change Management</a> on page 35
Showing Configuration History in Switch Configuration.	<b>Updated:</b> The feature allows you to view the configuration history of a selected switch or switch group.	<a href="#">Viewing the Configuration History of Switches</a> on page 60
SZ initiated ICX log events should indicate the SZ admin account	<b>New:</b> The feature aims to include the name of the administrator in the log entry.	<ul style="list-style-type: none"> <li>• <a href="#">Creating Switch Groups</a> on page 23</li> <li>• <a href="#">Creating Switch Model-Based Configurations</a> on page 52</li> </ul>



# Managing ICX Switches from SmartZone

- Supported ICX Models..... 11
- Overview of ICX Switch Management..... 14
- ICX Switch Behavior with SmartZone..... 15
- Enabling an ICX Device to Be Managed by SmartZone..... 16
- Configuring the ICX Source Address to Be Used by SmartZone..... 16
- Configuring a Custom Port Number for Connection to SmartZone..... 17
- Setting Up Switch Registrar Discovery..... 18
- Preparing Stacking Devices to Connect to SmartZone..... 20
- Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch..... 21
- Manually Configuring the SmartZone IP Address on an ICX Switch..... 21
- Displaying the SmartZone Connection Status..... 21
- Disconnecting the ICX Switch from SmartZone..... 22
- Disabling SmartZone Management on the ICX Switch..... 22

## Supported ICX Models

The following ICX switch models can be managed from SmartZone:

**TABLE 3** ICX Firmware Versions Compatible with SmartZone

ICX Model	First Supported FastIron Release	Last Supported FastIron Release
ICX 7150	08.0.80a	09.0.10a and subsequent patches
ICX 7150-C08P, -C08PT, -24F, -10ZP	08.0.92	09.0.10a and subsequent patches
ICX 7250	08.0.80a	09.0.10a and subsequent patches
ICX 7450	08.0.80a	09.0.10a and subsequent patches
ICX 7550	08.0.95a	-
ICX 7650	08.0.80a	-
ICX 7750	08.0.80a	08.0.95 and subsequent patches
ICX 7850	08.0.90	-
ICX 7850-48C	09.0.10a	-
ICX 8200	10.0.00	-
ICX 8200-24ZP, -48ZP2, -24FX, -24F, -48F, -C08ZP	10.0.10	-

The following table defines ICX and SmartZone release compatibility.

**NOTE**

ICX switches must be running FastIron 08.0.80a at a minimum to connect to SmartZone.

An ICX switch running unsupported firmware can still connect to the SmartZone controller. After the switch is connected, you must upgrade it to a firmware version that is compatible with the SmartZone controller version. This can be achieved using the switch firmware upgrade option in the Switch Group or by selecting one or more switches and performing the upgrade.

**NOTE**

FastIron 09.0.10a and later releases support management by SmartZone 6.1 and later.

**Managing ICX Switches from SmartZone**  
Supported ICX Models

**NOTE**

ICX switches with FIPS mode enabled do not support management by SmartZone.

**TABLE 4** ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.1 <sup>1</sup>	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1	SmartZone 6.1.2	SmartZone 7.0.0
FastIron 08.0.80	Yes	Yes <sup>1</sup>	No	No	No	No	No	No	No	No
FastIron 08.0.90a	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No
FastIron 08.0.91	No	Yes	Yes	Yes	No	No	No	No	No	No
FastIron 08.0.92	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No
FastIron 08.0.95 and subsequent patches	No	No	No	No	No	Yes	Yes	Yes	Yes	No
FastIron 09.0.10a and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes
FastIron 10.0.00 and subsequent patches	No	No	No	No	No	No	No	Yes	Yes	Yes
FastIron 10.0.10 and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes	Yes

The following table provides details on switch management feature compatibility between ICX and SmartZone releases.

**TABLE 5** Switch Management Feature Compatibility Matrix

Feature	SmartZone Release	ICX FastIron Release
Switch Registration	5.0 and later	08.0.80 and later
Switch Inventory	5.0 and later	08.0.80 and later
Switch Health and Performance Monitoring	5.0 and later	08.0.80 and later
Switch Firmware Upgrade	5.0 and later	08.0.80 and later
Switch Configuration File Backup and Restore	5.0 and later	08.0.80 and later
Client Troubleshooting: Search by Client MAC Address	5.1 and later	08.0.80 and later
Remote Ping and Traceroute	5.1 and later	08.0.80 and later
Switch Custom Events	5.1 and later	08.0.80 and later

<sup>1</sup> Does not support ICX configuration.

**TABLE 5** Switch Management Feature Compatibility Matrix (continued)

Feature	SmartZone Release	ICX FastIron Release
Remote CLI Change	5.2.1 and later	08.0.90 and later
Switch Configuration: Zero-Touch Provisioning	5.1.1 and later	08.0.90a and later
Switch-specific Settings: Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server	5.1.1 and later	08.0.90a and later
Switch Port Configuration	5.1.1 and later	08.0.90a and later
Switch AAA Configuration	5.1.1 and later	08.0.90a and later
Switch Client Visibility	5.1.2 and later	08.0.90a and later
Manage Switches from Default Group in SZ-100 / vSZ-E	5.1.2 and later	08.0.90a and later
DNS-based SmartZone Discovery	5.1.2 and later	08.0.95c and later
Download Syslogs for a Selected Switch <sup>2</sup>	5.2.1 and later	08.0.92 and later
Switch Topology	5.2 and later	08.0.92 and later
Designate a VLAN as Management VLAN	5.2.1 and later	08.0.92 and later <sup>3</sup>
Change Default VLAN	5.2.1 and later	08.0.95 and later
Configure the PoE Budget per Port on ICX through the Controller GUI with 1W Granularity	5.2.1 and later	08.0.95 and later
Configuring Protected Ports	5.2.1 and later	08.0.95 and later
Configuring QoS	5.2.1 and later	08.0.95 and later
Configuring Syslog	5.2.1 and later	08.0.95 and later
Geo Redundancy Active-Standby Mode	6.0 and later	08.0.95b and later
Generic CLI Configuration	6.0 and later	08.0.95b and later
Port-Level Override	6.0 and later	08.0.95b and later
Port-Level Storm Control Configuration	6.1 and later	08.0.95 and later
IPv6 Support (connection through static configuration only)	6.1 and later	09.0.10a and later
Save Boot Preference	6.1 and later	09.0.10a and later
Virtual Cable Testing	6.1 and later	09.0.10a and later
Blink LEDs	6.1 and later	09.0.10a and later
Send Event Email Notifications at Tenant Level	6.1 and later	09.0.10a and later
Update the status of a Switch	6.1 and later	09.0.10a and later
Convert Standalone Switch	6.1 and later	09.0.10a and later
Flexible Authentication Configuration	6.1 and later	09.0.10a and later
Network Segmentation	6.1.1 and later	09.0.10d and later <sup>4</sup>
Breakout Port Support	7.0.0 and later	09.0.10h and later
Enhancement in Firmware Upgrade Status	7.0.0 and later	09.0.10h and later
SmartZone Usernames in ICX Syslogs	7.0.0 and later	09.0.10h and later, 10.0.10c and later
Configuring Separate Authentication and Accounting in AAA server	7.0.0 and later	09.0.10h and later

<sup>2</sup> To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.

<sup>3</sup> FastIron 10.0.00 and later releases do not support management VLANs.

<sup>4</sup> As an exception, FastIron release 10.0.00 does not support this feature.

## Overview of ICX Switch Management

Beginning with SmartZone 5.0, the SmartZone administrator can monitor and manage switches and routers in the ICX 7000 series. SmartZone 5.1.1 introduced the capability to configure switches.

SmartZone ICX-Management supports the following ICX switch activities:

- Registration and authentication
- Switch inventory (for example, model, firmware version, and last backup)
- Health and performance monitoring (for example, status, traffic statistics, errors, and clients) with alarms
- Zero-touch provisioning
- Configuration changes
- Port settings
- Configuration copy
- Configuration file backup and restore
- Firmware upgrade
- Client troubleshooting
- Remote Ping and Traceroute
- CLI templates and provisioning

### NOTE

Refer to the [Supported ICX Models](#) on page 11 for more details.

## Preparing ICX Devices to be Managed by SmartZone

### NOTE

For more information on ICX device capabilities and configuration, refer to the RUCKUS FastIron documentation set available at the following URL: <https://support.ruckuswireless.com>. On the site, select **Products > Ruckus ICX Switches > Technical Documents**, and choose the platform and document of interest.

ICX devices can be managed by SmartZone. The following items are required to manage ICX devices:

### NOTE

Refer to the [Supported ICX Models](#) on page 11 for detailed information on software compatibility requirements and feature availability.

- The SmartZone IP address must be reachable by the ICX device through the Management interface or through switch or router interfaces.
- The ICX device must be made aware of the configured SmartZone IP address in one of the following ways:
  - Configure the DHCP server to use DHCP option 43.
  - Issue the following command at the global configuration level:

```
ICX(conf)# manager active-list SmartZone_Control_IP_Address
```
  - Add an entry in the DNS server with the hostname `ruckuscontroller` or `ruckuscontroller.local domain` that points to the SmartZone IP address.
- On ICX 7250, ICX 7450, and ICX 7750 devices, self-signed certificates are used. SmartZone honors these certificates when the **non-tpm-switch-cert-validate** command is entered on the SmartZone console, as shown in the following example.

FIGURE 1 Command Required to Disable Certificate Check

```
SZ# conf
SZ(config)# non-tpm-switch-cert-validate
Successful operation

SZ(config)# end
SZ#
```

- When SmartZone or ICX devices are behind network address translation (NAT), be sure to forward TCP ports 443 and 22 through NAT.
- Virtual platform requirements for supporting ICX devices are listed in the following table.

**NOTE**

Each unit in a stack is considered a separate switch unit for capacity management purposes.

TABLE 6 Virtual Platform Requirements for Supporting ICX Devices

Platform	Maximum Number of Switches Per Node	RAM	vCPU	Disk Storage
vSZ-E	200	18 GB	4	100 GB
vSZ-H	2000	30 GB	12	300 GB

The scaling limits in the table apply to switch-only deployments. For a mix of APs and switches, the scaling limits vary accordingly. SmartZone supports a 5-to-1 AP-to-switch ratio.

vSZ-E Example: vSZ-E supports up to 1,000 APs on a single node. If 200 APs are currently managed by SmartZone, there is room for 800 more APs or 160 ICX switches (800 divided by 5).

vSZ-H Example: vSZ-H supports up to 2,000 ICX switches on a single node. If 500 switches are currently managed, there is room for 1,500 more switches, or 7,500 APs (1500 multiplied by 5).



**VIDEO**

**Onboarding ICX Switches to SmartZone.** Using CLI commands to establish and verify switch connectivity to SmartZone.  
[Click to play video in full screen mode.](#)

## ICX Switch Behavior with SmartZone

**NOTE**

The full range of ICX-Management capabilities (including configuration support in SmartZone 5.1.1 or later) is available only when ICX devices have been upgraded to FastIron 08.0.90a or later using a Unified Forwarding Image (UFI). Beginning with FastIron 08.0.90, RUCKUS ICX devices support unified images that require custom upgrades from prior releases. Any ICX switch that is running a FastIron 08.0.80 non-UFI image on the ICX switch must follow a two-step image upgrade process to FastIron 08.0.90a through SmartZone controller image updates. If an ICX switch from the factory has a FastIron 08.0.80 non-UFI image, it must first be upgraded with a FastIron 08.0.90 UFI, followed by a FastIron 08.0.90a UFI, to avoid any boot configuration issues. Refer to the *RUCKUS FastIron Software Upgrade Guide* for more information.

## Managing ICX Switches from SmartZone

### Enabling an ICX Device to Be Managed by SmartZone

When an ICX switch is managed by SmartZone, the following considerations apply:

- All local configuration methods continue to be available to the local administrator, which means the switch can be configured through the console, Telnet, SSH, SNMP, or the web.
- It is recommended that the ICX switch be configured with the same NTP server as SmartZone.
- In an ICX stack, if a stack switchover or failover occurs, the original connection to SmartZone is closed, and the new active switch initiates a connection with SmartZone.

## Enabling an ICX Device to Be Managed by SmartZone

There are several ways to make an ICX device aware of the SmartZone IP address:

- Use switch registrar discovery.
- Use DHCP option 43.
- Configure the ICX device manually using FastIron commands.

All of these methods are supported for new ICX switches with no configuration as well as for ICX switches with existing configuration.

Beginning with 09.0.10h, access to the ICX device through web management may change when the device is connected to SmartZone.

- When **WebAuth** is not configured on the ICX switch and then is connected to SmartZone, web management is disabled and the CLI command **web-management disable** is then added to the running configuration. To enable web-management, enter **no web-management disable** on the ICX device.
- When an ICX device is configured with **WebAuth** on any VLAN and then is connected to SmartZone there is no change in the web management behavior. If **WebAuth** is disabled later, access to web management will stay enabled until the next time the device is connected to SmartZone.
- When an ICX device is connected to SmartZone and then **WebAuth** is enabled on any VLAN, enter **no web-management disable** on the ICX device to enable web management.
- When a device has web management disabled, if a user enabled the **WebAuth** configuration, it will not work until **no web-management disable** is entered on the device.

## Configuring the ICX Source Address to Be Used by SmartZone

By default, the IP address of the management port is included in the manager query as the ICX source address for an ICX-Management connection. Use the **management source-interface protocol manager** command to specify a different ICX source address.

### NOTE

Only ICX devices with a router image support the **management source-interface protocol manager** command.

The **management source-interface protocol manager** command can specify an Ethernet, LAG, loopback, or virtual Ethernet (VE) interface. The IP address with the lowest number for the specified interface is used for the connection.

The following example configures an Ethernet port as the ICX source address for an ICX-Management connection.

```
ICX# configure terminal
ICX(config)# management source-interface ethernet 1/1/3 protocol manager
```

Refer to the *RUCKUS FastIron Command Reference* for more information.



# Configuring a Custom Port Number for Connection to SmartZone

By default, ICX switches use TCP destination port 22 to connect with SmartZone. Use the **manager ssh-port** command to configure a different port number for connecting with SmartZone.

The following example configures an ICX switch to connect to SmartZone over SSH port 25. A warning message is displayed as shown if a session is already established. You must confirm the configuration update when prompted before the new connection is established. Check configuration status with the **show manager status** command.

```
device# configure terminal
device(config)# manager ssh-port
  DECIMAL  Enter a decimal value (Default 22)
device(config)# manager ssh-port 25

device(config)# manager ssh-port 25 <-- Warning message -->
Current session if established will be dropped to establish a new session with port 25.
Are you sure? (enter 'y' or 'n'): y <-- You must confirm the configuration.
!
!
device(config)# exit

device# show manager status

=====      MGMT Agent State Info      =====

Config Status:Enabled Operation Status:Enabled
State:SSH CONNECTED      Prev State:SSH CONNECTING      Event:SZ_SSH_CONNECT_EVENT

SWR List      : None
DNS List      :
Active List   : 10.176.160.115
Active List IPV6 : None
DHCP Option 43 : No
DHCP Opt 43 List : None
Backup List   : None
Backup List IPV6 : None
Merged List   : 10.176.160.115

SZ IP Used    : 10.176.160.115
Port List     : 987
Server Port Used : 443
Query Status  : APPROVED

SSH Tunnel Status -:
Tunnel Status    : Established
SSH Port         : 25 <-- configuration confirmed
CLI IP/Port      : 127.255.255.253/22866
SNMP IP/Port     : 127.255.255.254/63989
Syslog IP/Port   : 127.0.0.1/20514
HTTP CLIENT IP/Port : 127.0.0.1/5080
HTTP SERVER IP/Port : 127.255.255.252/40042
Timer Status     : Not Running
```

## NOTE

If you configure a custom port on an ICX switch, the SmartZone controller settings must also be updated. Refer to the appropriate version of the RUCKUS SmartZone administration guide for details.

## Setting Up Switch Registrar Discovery

The switch registrar is a RUCKUS-hosted cloud service that enables SmartZone discovery from ICX devices.

You can configure the ICX device to retrieve the correct SmartZone management IP address, IP address set, or fully qualified domain name (FQDN) from the switch registrar. The switch registrar must be set up in advance through Managed Service Provider (MSP) with SmartZone IP addresses or an FQDN and the ICX serial numbers they can manage.

### NOTE

If SmartZone management is not enabled on the ICX device, switch registrar discovery does not occur.

## How Switch Registrar Discovery Works

The ICX device sends an HTTP GET message to a default server host, `sw-registrar.ruckuswireless.com`, for the list of SmartZone management IP addresses or an FQDN, unless the system administrator configures an alternate host. The SmartZone IP address or FQDN obtained in response to the GET message is used to query the SmartZone device to set up a connection. If the ICX device receives a set of IP addresses from the switch registrar, it stores the information and tries the addresses in turn until a successful connection is established with the SmartZone device. The IP address, set of IP addresses, or FQDN obtained through the switch registrar is given priority above all other addresses in the list of SmartZone IP addresses, including addresses received from other sources such as the DHCP list, the active list, and the backup list. Once the ICX device has obtained a SmartZone IP address from the switch registrar, it no longer attempts switch registrar discovery.

This query is performed only for greenfield deployments and when the ICX device boots up with no startup configuration. ICX switches being upgraded from older releases that already have a configuration in place will not have the registrar-based SmartZone discovery turned on. The HTTPS session used for the database query uses the device certificate installed on the switch for SSL session establishment. For the initial release of the switch registrar, no server certificate validation will be performed.

## Disabling or Enabling Switch Registrar Discovery

The system administrator can disable or enable switch registrar discovery from the command line.

### NOTE

The registrar IP list is removed when you disable the switch registrar.

To disable switch registrar discovery, enter the **no manager registrar** command in global configuration mode, and use the **write memory** command to save the change, as shown in the following example.

```
ICX# configure terminal
ICX(config)# no manager registrar
ICX(config)# write memory
```

To restart the switch registrar discovery process, use one of the following commands in privileged EXEC or global configuration mode:

- **manager registrar-query-restart**
- **manager reset**

To enable switch registrar discovery on an alternate registrar host server and save the entry to the startup configuration, enter the following commands.

```
ICX# configure terminal
ICX(config)# manager registrar sw-alternate.ruckuswireless.com
ICX(config)# write memory
```

**NOTE**

The **manager registrar hostname** command is for test purposes only. The **manager registrar-query-restart** command by itself is sufficient to initiate registrar-based SmartZone discovery.

## Confirming Successful Switch Registrar Discovery

To display log entries specific to registrar queries, use the **show manager log** command.

When the switch registrar database has been successfully queried, a syslog message similar to the following is displayed.

```
Aug 8 21:47:17:I:MGMT Agent: SZ Switch Registrar Query to 54.186.143.194 Success
```

When the ICX device requires a restart to connect to the SmartZone address because a new registrar list has been received, a syslog message similar to the following is displayed.

```
Aug 8 21:47:17:I:MGMT Agent: Disconnect to SZ: 54.16.143.194, Got SZ ip via registrar
```

You can use the **show running-config** command to check for the name of the registrar host and the registrar list of SmartZone IP addresses.

The following example indicates that the ICX device uses the default switch registrar host and has obtained one SmartZone IP address (of a possible set of two addresses).

```
ICX# show running-config
!
!
manager registrar
manager registrar-list 23.251.150.119
!
!
```

You can also enter the **show manager status** command to obtain information on the switch registrar, as shown in the following example.

```
ICX# show manager status

===== MGMT Agent State Info =====

Config Status:Enabled Operation Status:Enabled
State:SSH CONNECTED Prev State:SSH CONNECTING Event:SZ_SSH_CONNECT_EVENT

SWR List : None
DNS List :
Active List : 10.176.160.116
Active List IPV6 : 2620:107:90d0:ab40::116
DHCP Option 43 : No
DHCP Opt 43 List : None
Backup List : None
Backup List IPV6 : None
Merged List : 2620:107:90d0:ab40::116 10.176.160.116

SZ IP Used : 2620:107:90d0:ab40::116
Port List : 987
Server Port Used : 443
Query Status : APPROVED

SSH Tunnel Status -:
Tunnel Status : Established
CLI IP/Port : 127.255.255.253/59449
SNMP IP/Port : 127.255.255.254/8253
Syslog IP/Port : 127.0.0.1/20514
HTTP CLIENT IP/Port : 127.0.0.1/5080
HTTP SERVER IP/Port : 127.255.255.252/63098
Timer Status : Not Running
```

## Troubleshooting Switch Registrar Discovery

In the event that switch registrar discovery fails, check for the following conditions:

- The running configuration contains "manager disable".
- The switch registrar is not configured on the ICX device.
- The DNS configuration needed to resolve the switch registrar address is not present on the ICX device.
- The ICX device could not reach the switch registrar due to routing issues.

### NOTE

If the switch registrar is enabled and you enter the **no manager disable** command, switch registrar discovery is still started when the registrar IP list is empty.

### NOTE

The switch registrar discovery process continues to run until the configuration issues are fixed, a successful query result is obtained, or you enter a command to disable the switch registrar.

## Preparing Stacking Devices to Connect to SmartZone

Consider the following guidelines when preparing ICX stacking devices to be discovered and managed by SmartZone:

- Define the stack configuration on the SmartZone device before connecting cables between the SmartZone and ICX devices.
- The devices to be managed in the stack must be part of a "firmware version" switch group configured on the SmartZone device.

If only the ICX device intended to be the stack active controller is an active switch under SmartZone control and is part of a configured "firmware version" switch group, perform the following steps to establish a stack:

- Connect all cables between ICX devices to form the desired stack configuration.
- On the active controller, enter the following commands in privileged EXEC mode:
  - **stack enable** (enables stacking on the active controller)
  - **stack zero-touch-enable** (triggers automatic discovery of the stack units and connections)
  - **write memory** (saves the running configuration to startup flash)

No commands need to be entered on the other stack units in this case.

If all switches intended to be members of a stack have already joined and have been approved by SmartZone and are already part of a "firmware version" switch group, enter the following commands on the ICX devices to form a stack:

- On the active controller, enter the following commands in privileged EXEC mode:
  - **stack enable** (enables stacking on the active controller)
  - **stack zero-touch-enable** (triggers automatic discovery of the stack units and connections)
  - **write memory** (saves the running configuration to startup flash)
- On all other prospective stack members, configure the following commands in global configuration mode:
  - **stack suggested-id**
  - **stack ztp-force**
  - **write memory**

## Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch

A DHCP server can be configured to send SmartZone IP addresses to ICX devices using DHCP Option 43.

Configure DHCP Option 43 on the DHCP server, using **RKUS.scg-address** to identify the SmartZone IP addresses.

A single SmartZone IP address or a comma-separated list can be configured. SmartZone IP addresses are sent with a sub-option value of 6. The ICX device ignores all other data in DHCP Option 43 if SmartZone IP addresses are present.

The following example shows a DHCP Option 43 configuration on a DHCP server. The IP addresses listed are examples only.

```
subnet 192.168.12.0 netmask 255.255.255.0 {
    range 192.168.12.100 192.168.12.199;
    option routers 192.168.12.1;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.12.255;
    option ntp-servers 192.168.11.22;
    class "Ruckus AP" {
        match if option vendor-class-identifier = "Ruckus CPE";
        option vendor-class-identifier "Ruckus CPE";
        default-lease-time 86400;
        vendor-option-space RKUS;
        option RKUS.scg-address "192.168.11.200, 192.168.11.201, 192.168.11.202";
    }
}
```

## Manually Configuring the SmartZone IP Address on an ICX Switch

Complete the following steps to configure a list of SmartZone IP addresses on the ICX device.

1. Enter the **manager active-list** command followed by one or more priority IP addresses for the SmartZone device, as shown in the following example.

The IP addresses listed are examples only.

```
ICX# configure terminal
ICX(config)# manager active-list 192.168.11.200 192.168.11.201 192.168.11.202
```

2. Use the **sz passive-list ip-address** command to configure the SmartZone IP addresses to be used for redundancy.

```
ICX(config)# sz passive-list 10.176.160.118
```

## Displaying the SmartZone Connection Status

Use the **show manager status** command to display the SmartZone IP address lists and information about the status of the connection.

```
ICX# show manager status

===== MGMT Agent State Info =====

Config Status:Enabled Operation Status:Enabled
State:SSH CONNECTED Prev State:SSH CONNECTING Event:SZ_SSH_CONNECT_EVENT

SWR List : None
```

## Managing ICX Switches from SmartZone

### Disconnecting the ICX Switch from SmartZone

```
DNS List           :  
Active List       : 10.176.160.116  
Active List IPV6  : 2620:107:90d0:ab40::116  
DHCP Option 43   : No  
DHCP Opt 43 List : None  
Backup List      : None  
Backup List IPV6 : None  
Merged List      : 2620:107:90d0:ab40::116 10.176.160.116  
  
SZ IP Used        : 2620:107:90d0:ab40::116  
Port List        : 987  
Server Port Used : 443  
Query Status     : APPROVED  
  
SSH Tunnel Status -:  
Tunnel Status    : Established  
CLI IP/Port      : 127.255.255.253/59449  
SNMP IP/Port     : 127.255.255.254/8253  
Syslog IP/Port   : 127.0.0.1/20514  
HTTP CLIENT IP/Port : 127.0.0.1/5080  
HTTP SERVER IP/Port : 127.255.255.252/63098  
Timer Status     : Not Running
```

## Disconnecting the ICX Switch from SmartZone

Use the **manager disconnect** command in privileged exec or global configuration mode to disconnect the ICX switch from SmartZone and initiate a new connection based on the currently available list of SmartZone IP addresses.

Enter the **manager disconnect** command in privileged exec or global configuration mode.

This command can be executed on the local terminal.

```
ICX# manager disconnect  
SZ Disconnect initiated...  
  
ICX# configure terminal  
ICX(config)# manager disconnect  
SZ Disconnect initiated...
```

## Disabling SmartZone Management on the ICX Switch

When SmartZone management is disabled on the switch, the switch will not initiate a connection with SmartZone even if a SmartZone IP address is available.

Enter the **manager disable** command to disable SmartZone management on the ICX switch.

```
ICX(config)# manager disable
```

# Working with Switches

---

- [SmartZone Switch Management](#)..... 23
- [Troubleshooting Switch Issues](#)..... 137
- [Viewing Switches on the Dashboard](#)..... 146

## SmartZone Switch Management

### Using Controller Settings to Manage Switch Groups

Controller allows you to create switch groups, similar to AP zones. Switches connecting to controller can be placed in one of these logical groups for better manageability. A Staging or Default Group is created by the controller automatically. All switches are placed in this group when they initially joining the controller. You have the option to create additional groups.

**NOTE**

In SZ300 and vSZ-H platforms, a warning message is displayed to move the switches from the Staging Group to another group for controller to monitor.

Using registration rules, you can specify which group the switch should be placed into. Refer to [Creating Switch Groups](#) on page 23 and [Creating Switch Registration Rules](#) on page 27 for additional information.

### Creating Switch Groups

You can group switches based on your need, for example, you can group switches based on their size or their location.

You can only create a maximum of two levels within the group hierarchy. By default, all the switches are placed under the default switch group. You can create a group or sub-group and then move the switch under it. You can also modify or delete a group at any time.

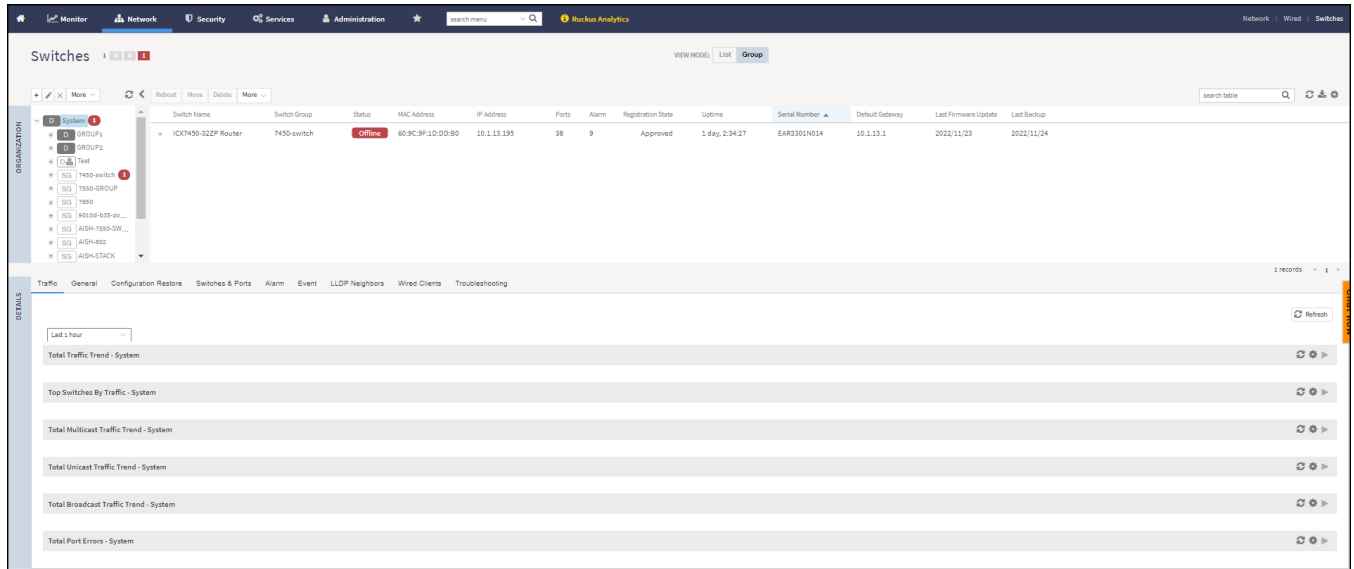
## Working with Switches

### SmartZone Switch Management

After the switch is registered with the controller interface, you can monitor, view status or usage, and perform some basic management, including configuration backups and firmware management.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.

**FIGURE 2** Switches



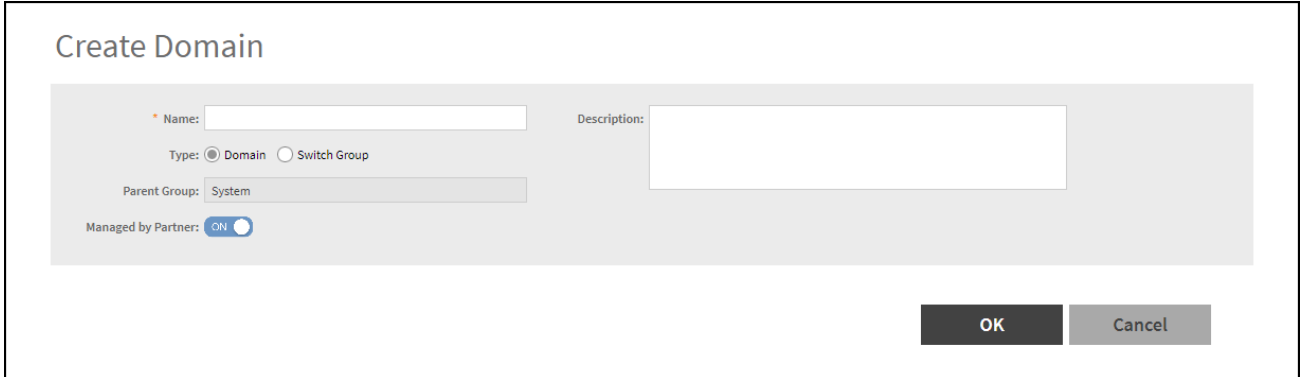
You can create a switch group or you can create a domain and add the switch group to that domain.



2. Complete the following steps to create a domain.

- a) In the **Organization** tab, click  to display the **Create Domain** dialog box.

**FIGURE 3** Create Domain



b) Complete the following fields:

- **Name:** Enter the domain name.
- **Description:** Enter a brief description for the domain.
- **Type:** Domain
- **Parent Group:** Displays the parent group under which the switch group resides. By default **System** is selected.
- **Managed by Partner:** This option is available if you select the group type as **Domain**. You can slide the radio button to ON or OFF to enable or disable partners from managing the switches.

c) Click **OK**.

The domain is created under the selected parent group in the **Organization** tab. The domain is identified with "D" symbol.

3. To create a individual switch group, in the **Organization** tab select the **System** and follow from the [Step 5](#).
4. To create a switch group within a domain, in the **Organization** tab select the **Domain** from the list and follow from the [Step 5](#).

5. In the **Organization** tab, click  icon to display the **Create Switch Group** dialog box. You can also edit or configure the switch group by clicking  icon.

FIGURE 4 Creating Switch Group

Complete the following fields:

- **Name:** Type the name of the switch group that you want to create.
- **Description:** Enter a brief description for the switch group.
- **Firmware Version:** Select the Firmware version (optional) which will automatically upgrade the switches (running an older version) joining the group.
- **Type:** Select **Switch Group**. For enterprise devices such as SZ-300 and vSZ-H.
- **Parent Group:** Displays the parent group under which the switch group resides
- **Two Factor Authentication:** Switch **ON** to use the **Console CLI** or **Remote CLI** to access the **Switches**.

**NOTE**

Turning ON this feature will disable the SSH access to the switches.

**NOTE**

Beginning with the SZ 7.0 release, when **Two Factor Authentication** is enabled on the controller, the ICX System log displays the SZ administrator name associated with the configuration activity performed on the controller. In the earlier releases, the ICX System log showed a generic message indicating that the network controller made the change.

A **message** dialog box is displayed, click **OK**.

- **Backup Schedule:** Allows you to schedule the backup. From the **Interval** drop-down list, select the type of backup such as **Daily**, **Weekly**, or **Monthly**. If the backup selected is **Daily**, you can configure **@Hour** , and **Minute** fields. If the backup selected is **Weekly**, you can configure the **Every** (day of the week), **@Hour** , and **Minute** fields. If the backup selected is **Monthly**, you can configure **Every** (date), **@Hour** , and **Minute** fields.

**NOTE**

The default backup time for scheduling a **Daily** backup is 3:30 a.m. The backup schedule is configured on the level one switch group.

- **SSH/TLS Key Enhance Mode:** Allows you to enable or disable ECDSA Certificate.

**NOTE**

If the administrator wants to turn on **SSH/TLS Key Enhance Mode** of the Switch Group, the **Firmware Version** setting must be configured first, and it must be the following.

- 10.0.10c and later versions
- 9010j and 9010j patch

6. Click **OK**.

The switch group is created under the selected parent group in the **Organization** tab. The switch group is identified with "SG" symbol.

## Creating Switch Registration Rules


You can create registration rules for switch groups, which are identified and approved by the controller to establish connections. Typically, the switch is registered with the controller using an IP address, subnet, or model number.

Complete the following steps to create a registration rule.

1. On the menu, click **Network > Wired > Switch Registration** to display the **Switch Registration** window.

**FIGURE 5** Switch Registration

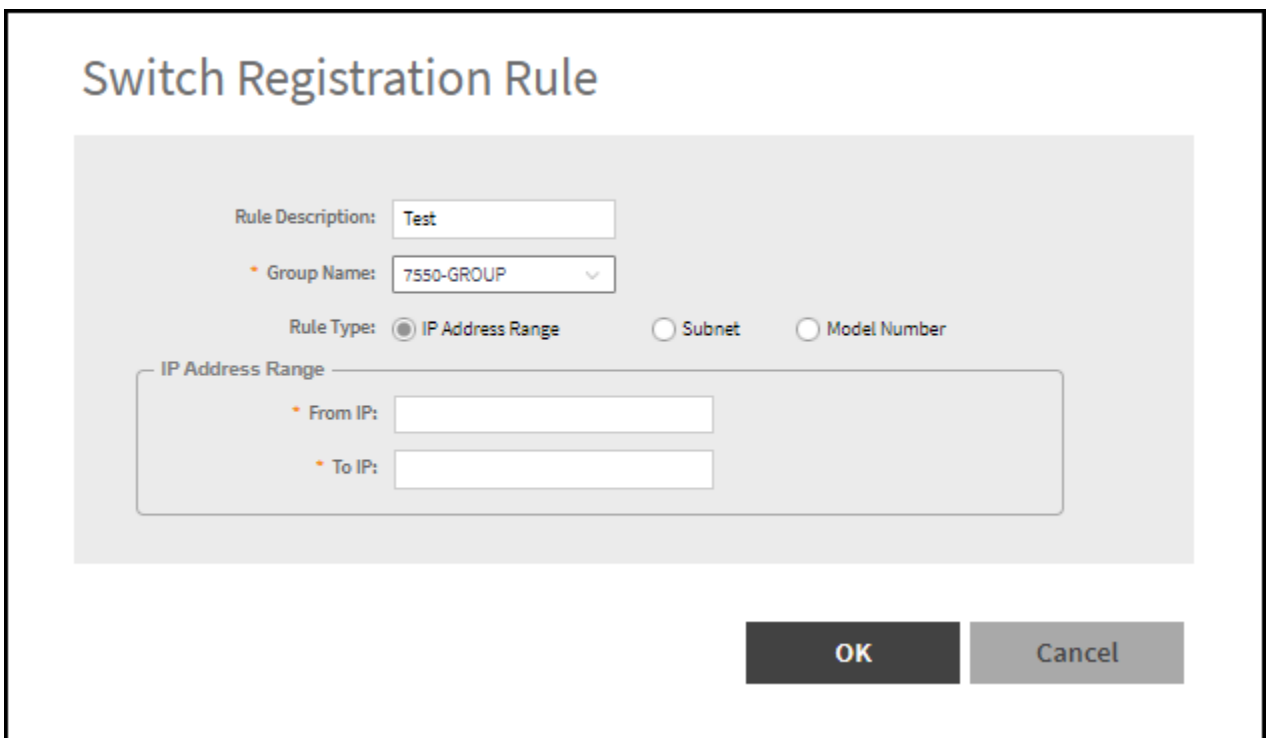
Priority	Rule Type	Rule Description	Rule Parameters	Group Name
1	Model Number	N/A	Model Number: ICX7350-48P	7355-GROUP
2	Model Number	N/A	Model Number: ICX7450-322P	7450-switch

2. Click  icon to display the **Switch Registration Rule** dialog box.

Complete the following fields:

- **Rule Description:** Provide a brief description of the registration rule you are creating to put the switches into specific groups.
- **Group Name:** Select the switch group to which you want to apply this rule from the list.
- **Rule Type:** Select **IP Address Range**, **Subnet**, or **Model Number** to apply the rule to the switch based on the rule type.
  - If you select **IP Address Range**, you must provide the range of the IP addresses for which this rule will apply.
  - If you select **Subnet**, you must provide the network address and subnet mask that will apply to the rule.
  - If you select **Model Number**, you must provide the model number of the device from the drop down list.

**FIGURE 6** Creating Switch Registration Rules - IP Address Range



Switch Registration Rule

Rule Description:

Group Name:

Rule Type:  IP Address Range  Subnet  Model Number

IP Address Range

From IP:

To IP:

OK Cancel

FIGURE 7 Creating Switch Registration Rules - Subnet

The screenshot shows the 'Switch Registration Rule' configuration interface. The 'Rule Description' field contains the text 'Test'. The 'Group Name' dropdown menu is set to '7550-GROUP'. Under the 'Rule Type' section, the 'Subnet' radio button is selected, while 'IP Address Range' and 'Model Number' are unselected. A sub-section titled 'Subnet' contains two input fields: 'Network Address' and 'Subnet Mask', both of which are currently empty. At the bottom of the form, there are two buttons: 'OK' and 'Cancel'.

FIGURE 8 Creating Switch Registration Rules - Model Number

The figure consists of two side-by-side screenshots of the 'Switch Registration Rule' configuration page. Both screenshots show the 'Rule Description' as 'Model Number' and the 'Group Name' as 'AutoConfig'. The 'Rule Type' section has the 'Model Number' radio button selected. The 'Model Number' dropdown menu is open, displaying a list of switch model numbers. In the left screenshot, the dropdown shows 'No data available' at the top, followed by a scrollable list of models including ICX8200-24, ICX8200-24F, ICX8200-24FX, ICX8200-24P, ICX8200-24ZP, ICX8200-48, ICX8200-48F, ICX8200-48P, ICX8200-48PF, ICX8200-48PF2, ICX8200-48ZP2, and ICX8200-C08P. The 'OK' and 'Cancel' buttons are visible below the dropdown. The right screenshot shows the same interface but with the dropdown list scrolled down to show models like ICX8200-24ZP, ICX8200-48, ICX8200-48F, ICX8200-48P, ICX8200-48PF, ICX8200-48PF2, ICX8200-48ZP2, ICX8200-C08P, ICX8200-C08PDC, ICX8200-C08PF, ICX8200-C08PT, and ICX8200-C08ZP. Only the 'OK' button is visible in this view.

3. Click **OK**.

You can edit, copy and delete the rule by selecting the rule and clicking **Configure**, **Clone**, and **Delete**, respectively.

After the registration rules are created, they can be rearranged using the **Up** and **Down** options. They can be arranged in an order of priority. After the order of priority for the list of rules is finalized, click **Update Priority** to confirm.

## Approving Switches

The switch must be approved so that it can be discovered and monitored by the controller.

- Switches that do not match any registration rule are automatically in the default group.
- At this point, a switch is not managed and the status is shown as offline.
- To actively manage a switch in this predicament, you must move it from the staging group to any other switch group or domain in SZ300 and vSZ-H platforms. In SZ100 and vSZ-E platforms, the default group behavior is similar to any other group. Refer to [Moving the Switches between Groups](#) on page 30 for more information.

### NOTE

A switch capacity license (CAPACITY-SWITCH-DEFAULT) is available for controllers and switches managed by the controllers. The license is activated for devices running SmartZone 5.1 or later. Upgrading to SmartZone 5.1 from an earlier version activates the license by default. A 90-day license version is then available for trial or purchase. The controller manages switches only as defined in the Switch Capacity license and rejects individual switches or stacks when license capacity is reached. Any switch that exceeds license limits is moved to the service group, where it cannot be configured. When license capacity is again available, the controller accepts the switch for management. For the controllers (SZ100 or SZ300), a trial license will allow adding the maximum number of switches supported. In the case of vSZ-E or vSZ-H, a trial license will allow the addition of 5 switches.

### NOTE

Based on the switch capacity license (CAPACITY-SWITCH-HA), you can approve a failover switch on a standby cluster to switch over to the original cluster.

The recommendation is to always use switch registration rules so that the switches are placed in the correct switch group and avoid manual intervention.

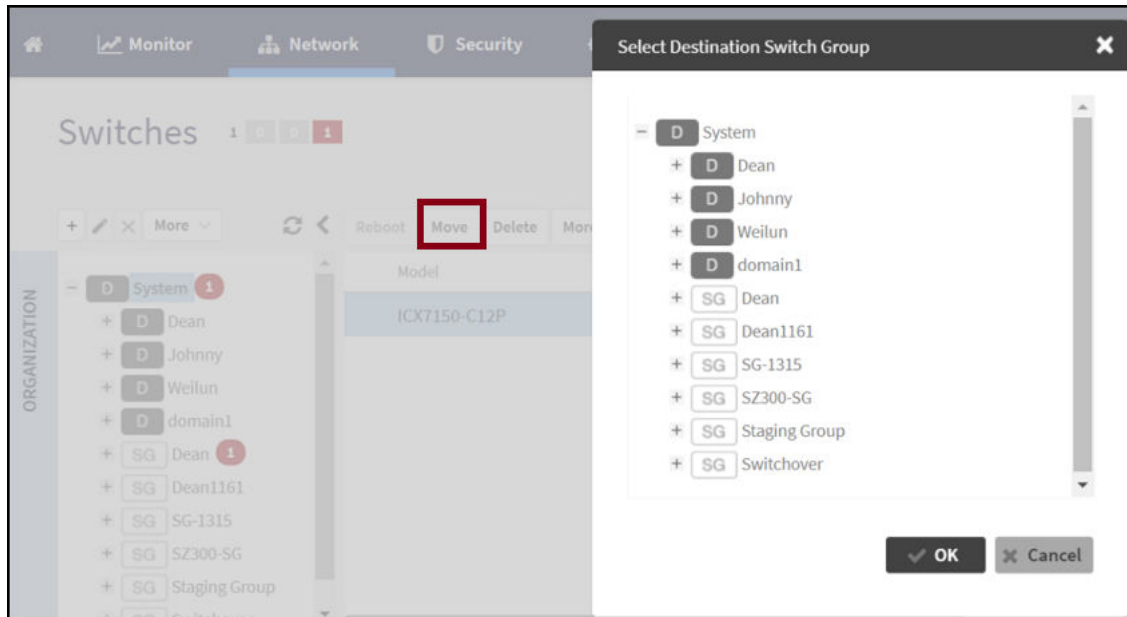
## Moving the Switches between Groups

You can move the switch to any group or sub-group within the system tree hierarchy.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. From the system tree, select a **Domain > Switch Group** or **Switch Group** and select the **Switch** that you want to move.

3. Click the **Move** tab.

**FIGURE 9** Moving the switch



The **Select Destination Switch Group** dialog box is displayed showing the system tree hierarchy.

4. Select a **Domain > Switch Group** or **Switch Group** to which you want to move the selected switch.
5. Click **OK**.

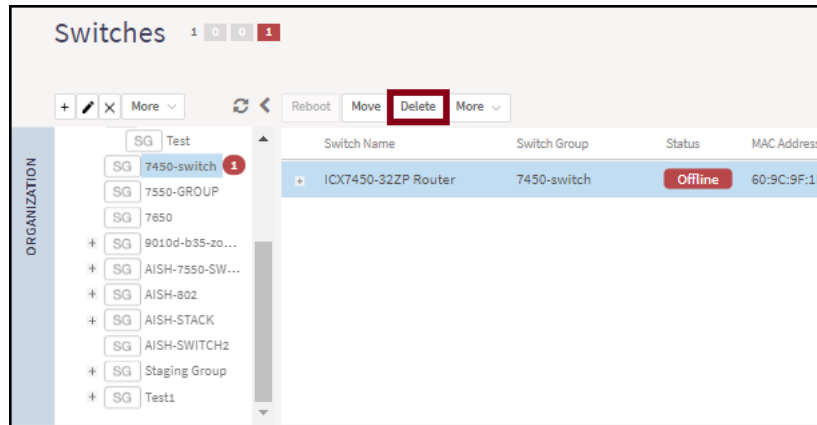
## Deleting Switches

The **Delete** enables you to remove the switches that are no longer needed.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.

- From the system tree, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** that you want to delete.

**FIGURE 10** Clicking the Delete Tab



- Click the **Delete** tab.

After deletion, the selected switch will no longer be managed by the controller interface.

## Backing up and Restoring Switch Configuration

The controller can back up the switch's running configuration. By default, controller makes a backup of switch configuration on a daily basis. The configuration is only stored if there is a change between the last configuration backup and the current backup. Otherwise, it is discarded. Controller saves the last seven configuration backups. When needed, these backups can be restored to the switch. While performing network maintenance, you can initiate a backup without having to wait for the daily backup.

**Prerequisites:** Ensure the controller is synced to the NTP server.

Complete the following steps to configure the switch backup.

- On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.



- From the system tree, select a **Domain > Switch Group** or **Switch Group** to perform switch group configuration backup or select a **Switch** to perform a switch configuration backup.

FIGURE 11 Switch Group Configuration Backup

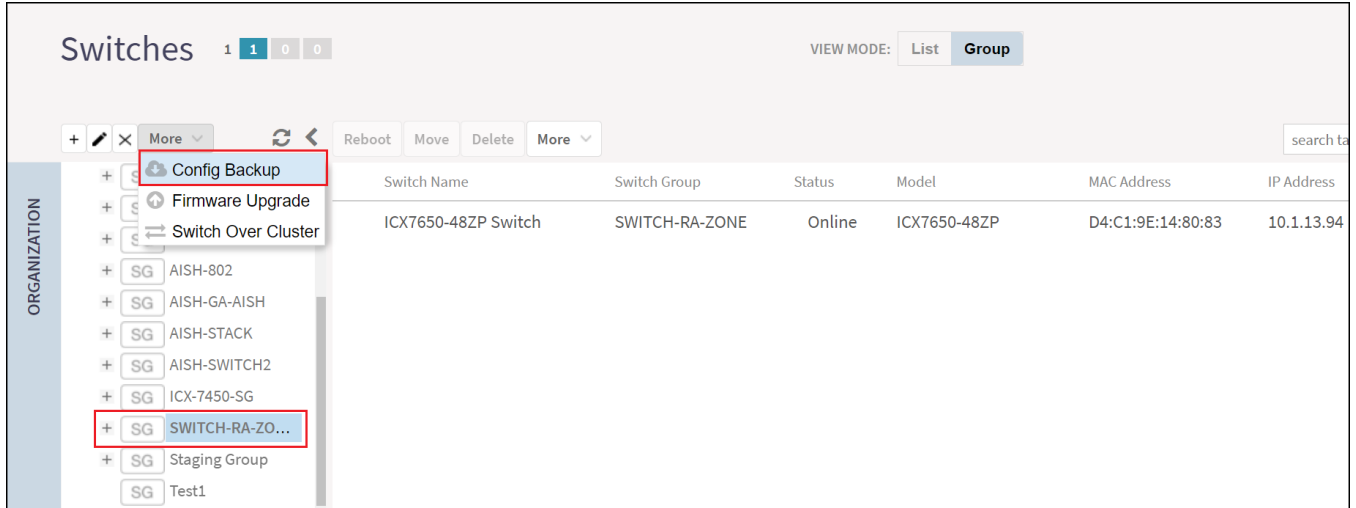
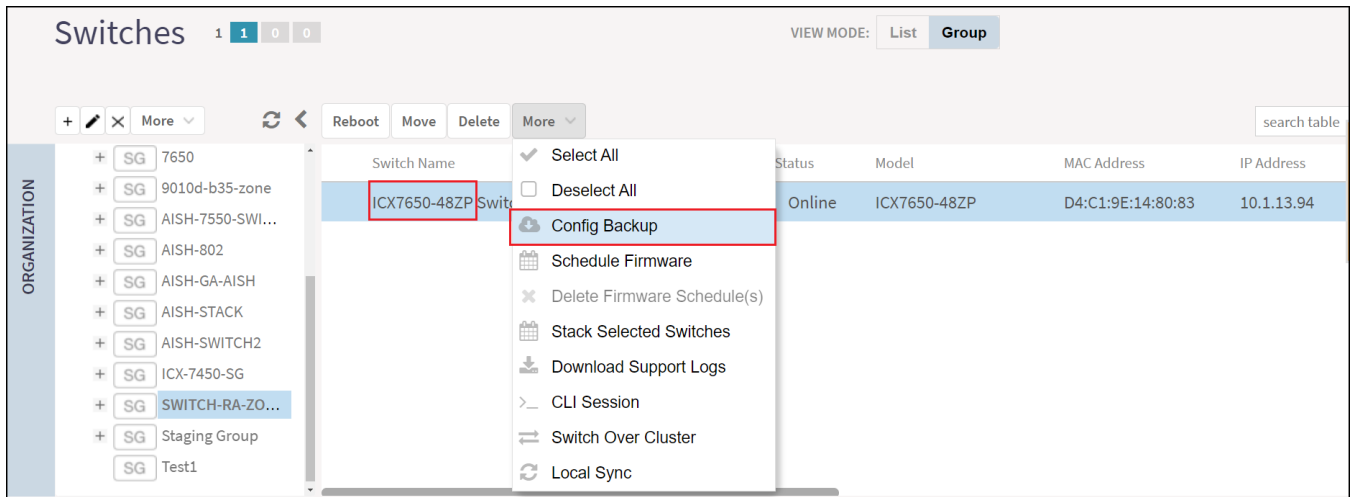
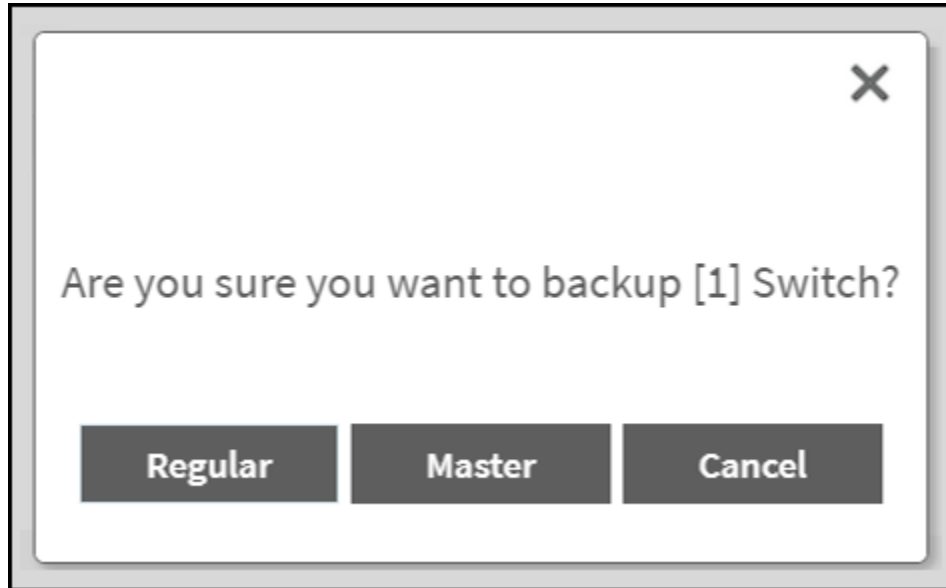


FIGURE 12 Switch Configuration Backup



3. Click **More > Config Backup** to display the **Configuration Backup** dialog box.

**FIGURE 13** Configuring Backup



A confirmation message is displayed asking the type of backup that must be carried such as **Regular** or **Master**.

The master configuration backup is for the configuration change alert feature. It allows you to select a switch configuration backup to serve as the master configuration backup. If the latest regular configuration backup differs from the master configuration backup, the controller will automatically display an alert indicating a configuration change. The regular configuration backup are the scheduled configuration backup that can be triggered by the user at any time.

**NOTE**

It is recommended to use master configuration backup, as the regular configuration backup will be removed if there are more than seven different configuration backups. The master configuration backup will not be removed in this case.

4. Click **Master**. A message is displayed confirming that the backup process has been initiated. Click **OK**.  
After the backup is completed, the status is recorded in the **Configuration Restore** tab.

**NOTE**

- As soon as the switch connects to the controller, and when it is online, the controller retrieves all the information about the switch.
- The controller maintains seven of the latest configuration backups for each switch.
- The controller automatically backs up the configuration of each switch, once, every 24 hours.
- If a previous switch configuration matches the current configuration, the latest configuration is saved and the old configuration is removed.

Complete the below steps to restore an individual switch configuration.

- a. From the system tree, select a **Domain > Switch Group** or **Switch Group** and select the **Switch** for which you want to perform configuration restore.
- b. In the **Details** tab, click the **Configuration Restore** tab to display the listed configurations in the table.
- c. Select a **Configuration** and click **Config Restore**. A message is displayed stating "Are you sure you want to restore this backup configuration to the Switch?"
- d. Click **Yes** to display the message "Switch Configuration restore operation has started and it will take up to two minutes to complete. Refer to the configuration table to know the status."
- e. Click **OK**.

Complete the below steps to view the switch configuration differences.

- a. On the **Configuration Restore** tab, select the configurations for which you want to view the differences. Press **Ctrl** key to select more than one configuration.
- b. Click the **Config Diff** tab. The **Configuration Details** table is displayed showing the configurations of the selected switches.

On the **Configuration Restore** tab, select the configuration to perform the following actions.

- Click the **Config View** tab to display the **Switch Config View** dialog box to see the configuration details.
- Click the **Config Download** tab to download the copy of the configuration file.
- Click the **Master Backup** tab to backup the switch configuration.
- Click the **Delete** tab to delete the configuration file.

## Improving Switch Configuration Change Management

Starting with the 7.0 release, the controller automatically verifies the switch with a Master backup every hour for any configuration changes. If there is a configuration change from the controller GUI or the switch, the controller triggers a configuration backup for the switch. Subsequently, the controller displays a warning on the **Switches** page, notifying that the latest running configuration backup of the switch differs from the Master backup.

**NOTE**

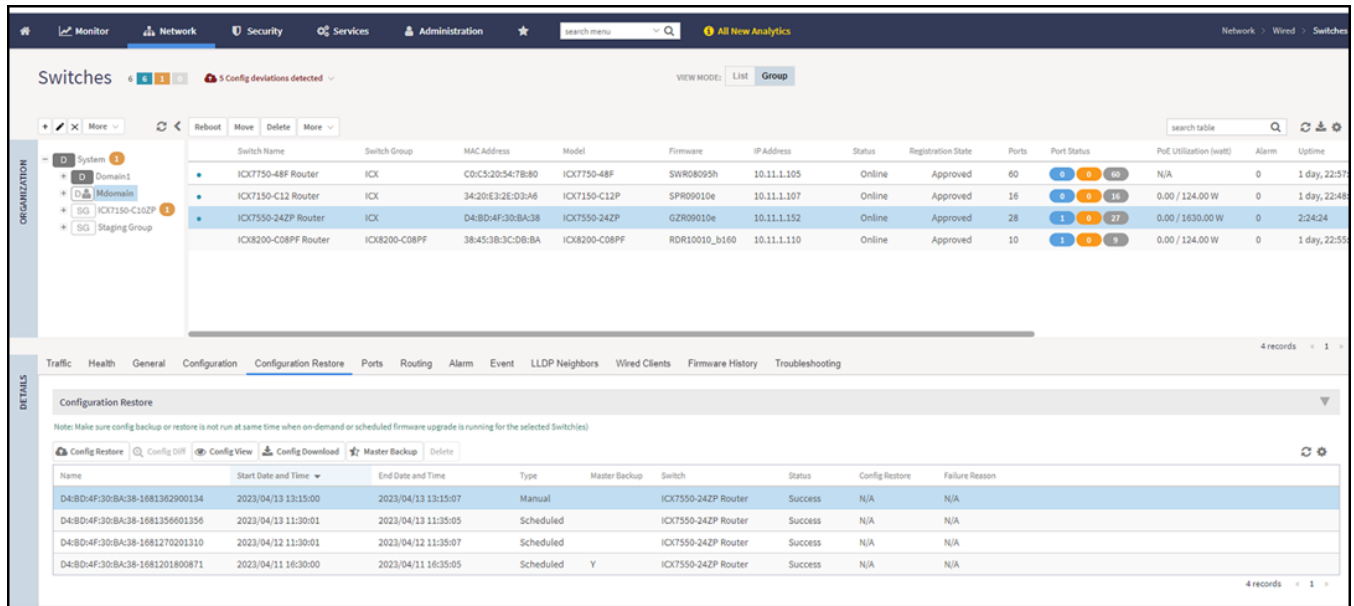
In earlier releases, warnings for differing backups were issued after a day, which was inconvenient.

Perform the below steps to view the switch with Master backup for configuration changes.

1. From the main menu, go to **Network > Wired > Switches**.  
The **Switches** page is displayed.

2. Select a Switch. Click the **Configuration Restore** tab.  
A list of backup configurations is displayed.
3. Set a specific configuration to be the Master by selecting a specific backup configuration and clicking the **Master Backup** button. A confirmation dialog box appears. Click **Yes**. The page refreshes, displaying a **Y** in the Master Backup column.

FIGURE 14 Viewing the Switch Master Backup Configuration



After a configuration has been selected as the Master Backup, any subsequent switch configuration changes will trigger the controller to automatically initiate a switch configuration backup.

## Rehoming Switches

Rehoming is the process of returning the switches that have failed over to the standby cluster back to their original cluster (once it becomes available). Rehoming must be done manually. Switches that have failed over continue to be managed by the failover cluster until you rehome them.

### NOTE

You can rehome switches only in a cluster redundancy environment. When switches of a certain active cluster fail over to a standby cluster, you must manually restore them to the original cluster after the active cluster is fixed and back to service.

Complete the following steps on the standby cluster to rehome switches to the original cluster:.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. From the system tree, select a **Domain > Switch Group** or **Switch Group** and select the **Switch** to rehome.
3. In the **System Domain**, click **More > Rehome Active Cluster** to display the **Confirmation** dialog box.
4. Click **Yes**.

## Switching Over Clusters

Switchover helps move individual switches or switches in a switch groups across clusters.

### NOTE

Ensure that a switch registration rule is created on the target cluster before switching over to another cluster. For more information, refer to [Creating Switch Registration Rules](#) on page 27.

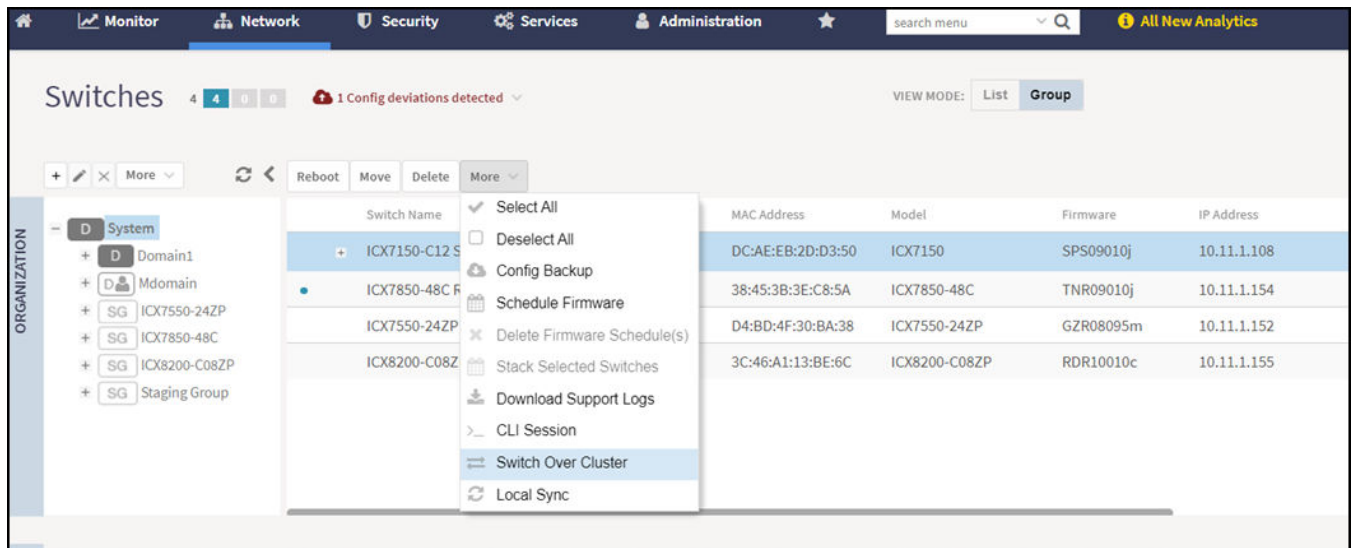
### NOTE

Depending on the switch High Availability license on the standby cluster switches must be approved so that it can be discovered and monitored by the controller. For more information, refer to [Approving Switches](#) on page 30.

Complete the following steps to switch over from one cluster to another.

1. On the menu, click **Network > Switches > Switches** to display the **Switches** window.
2. From the system tree, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**.

FIGURE 15 Switch Over Cluster



3. Click **More**. Select **Switch Over Cluster** from the list.  
The **Switch Over Cluster** dialog box is displayed.
4. In the **Control IP** field, enter the control IP address of the switchover target cluster.
5. Click **OK**. A **Confirmation** dialog box is displayed.
6. Click **YES** to confirm.

## Scheduling a Firmware Upgrade for Switch Group

You can upgrade a switch group on a Level 1 group that has no default firmware setting. The forced upgrade allows the device to remain in the same firmware type (Layer 2 still Layer 2, Layer 3 still Layer 3) with only a change to the version type.

### NOTE

If the switch group has a default firmware selected the **Firmware Upgrade** option is unavailable.

**NOTE**

Beginning with FastIron release 10.0.0, a switch ("Layer 2") image will no longer be provided for ICX devices. Only the router ("Layer 3") image will be available. On Upgradeto FastIron 10.0.00, the configuration of any ICX devices operating with the switch image will automatically be translated to the equivalent router image configuration. The target upgrade to 10.0.0 supports only router code.

The following features are deprecated as a result of this change:

- The IP default gateway
- The management VLAN
- Global configuration of the IP address (Going forward, the IP address must be configured at the interface level for each port.)

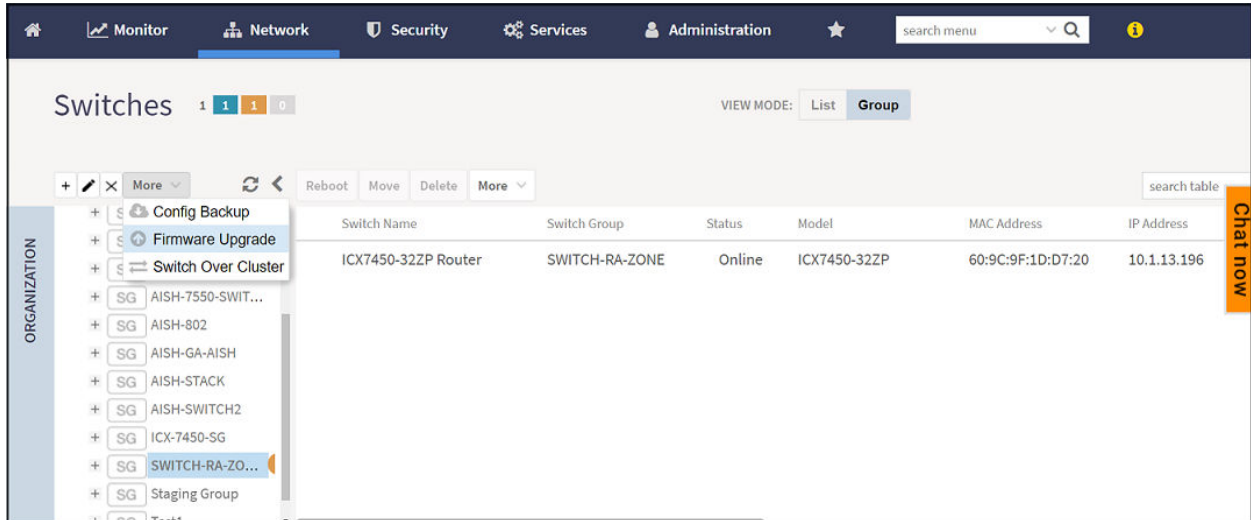
Refer to the RUCKUS FastIron Software Upgrade Guide for additional details.

Complete the following steps to perform a firmware upgrade on the switch group.

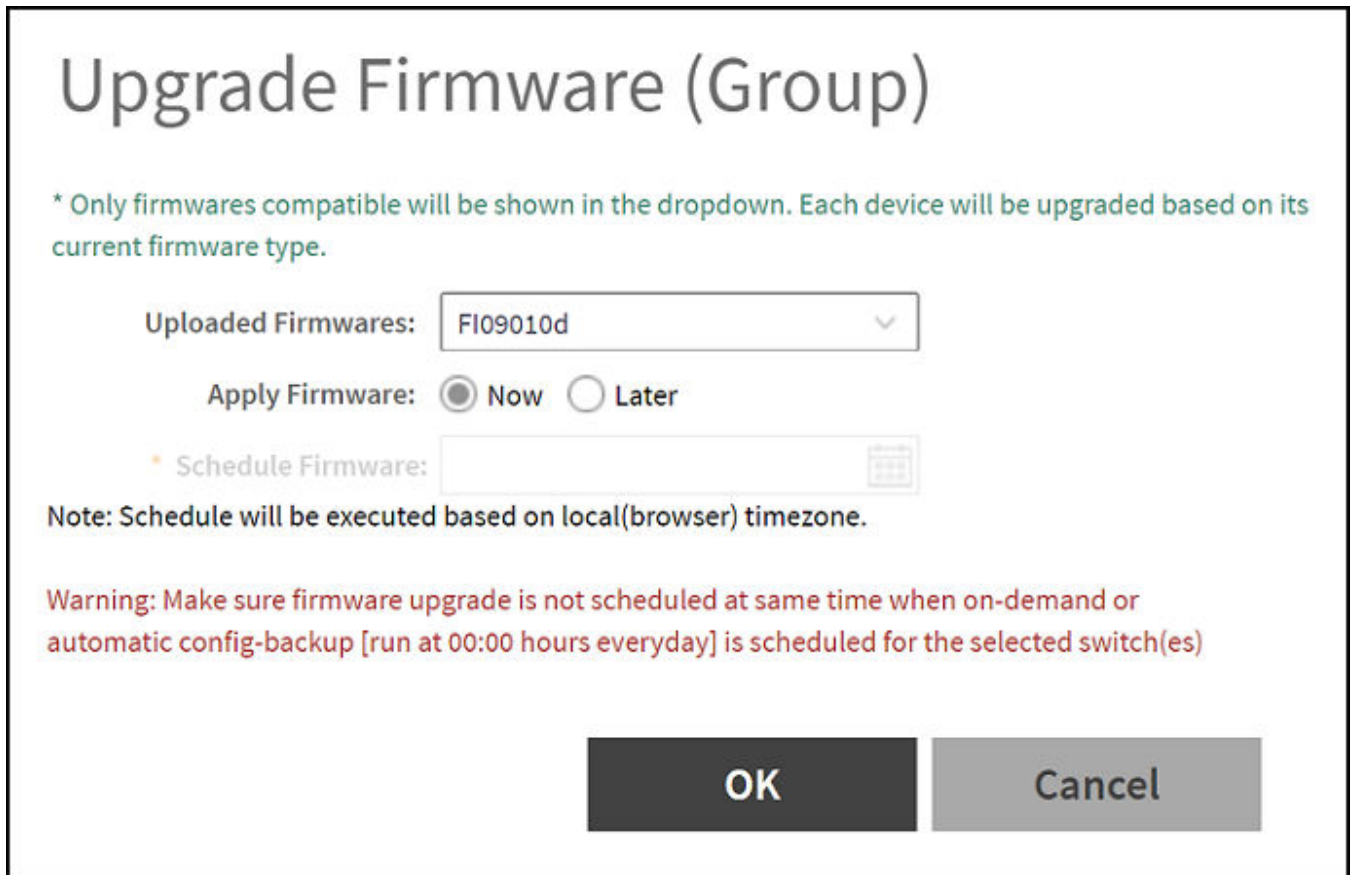
1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group**.

- Click **More > Firmware Upgrade** to display the **Upgrade Firmware (Group)** dialog box.

**FIGURE 16** Selecting Firmware Upgrade for a Switch Group



**FIGURE 17** Scheduling the Upgrade for a Switch Group



4. Complete the following fields:
  - **Uploaded Firmwares:** Select firmware from the list.
  - **Apply Firmware:** Select Now or Later to set the new firmware version to the switch group.
  - **Schedule Firmware:** If you select Later for **Apply Firmware**, you must select the date to schedule the upload.
5. Click **OK**.

## Scheduling a Firmware Upgrade for Selected Switches

You can upgrade or downgrade the firmware version of a switch or multiple switches that you are monitoring. You can upgrade the firmware on demand or schedule a firmware update for a list of selected switches.

### Prerequisites

- Upload a valid FastIron firmware version (newer than version 8.0.80) to the controller.
- Sync the controller with the NTP server. On the controller user interface, navigate to **Administration > System > Time** then click **Sync Server**.

### Scheduling Firmware Upgrade

1. From the main menu, click **Network > Wired > Switches**.  
The **Switches** page is displayed.
2. Select a **Domain > Switch Group** or specific **Switch Group** and select the **Switch** that you want to upgrade.

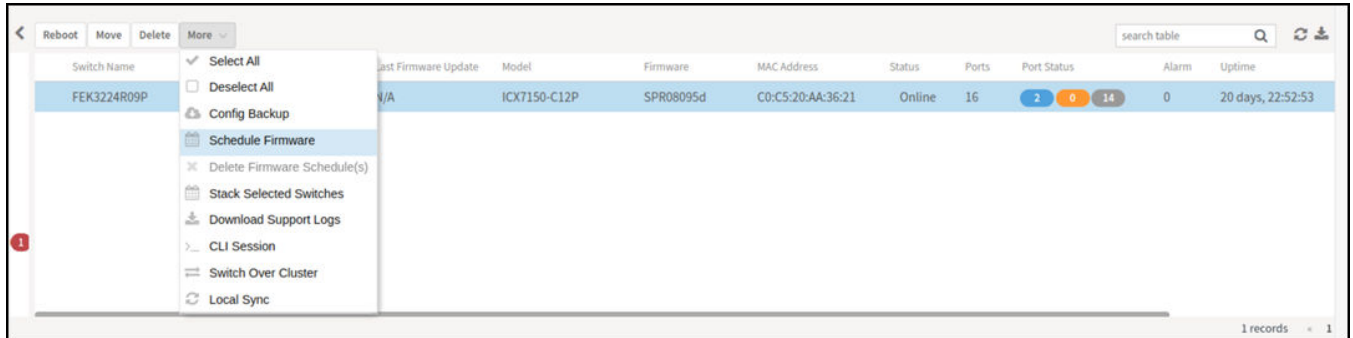
#### NOTE

To upgrade the firmware for multiple switches simultaneously, hold down the **Ctrl** key as you select the desired switches.



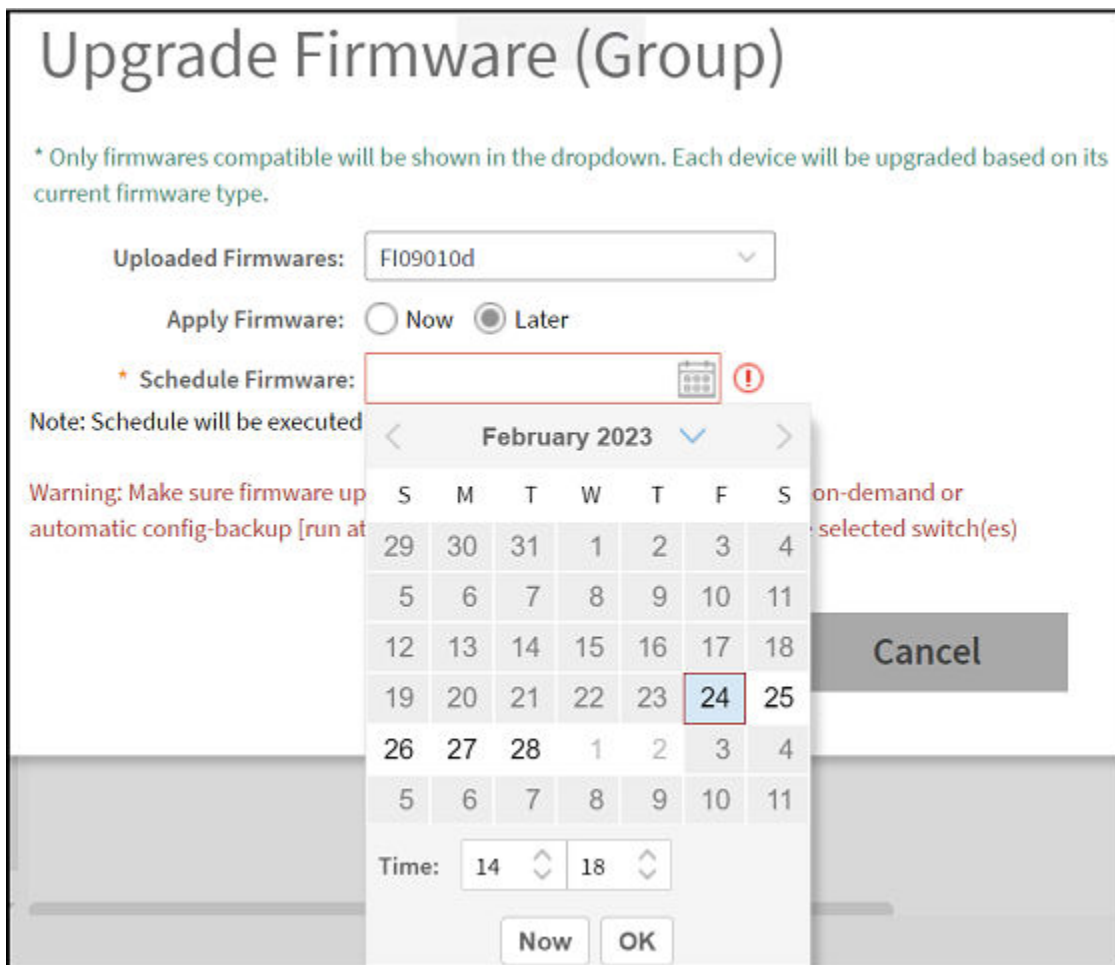
3. Click **More > Schedule Firmware**.

**FIGURE 18** Selecting Schedule Firmware



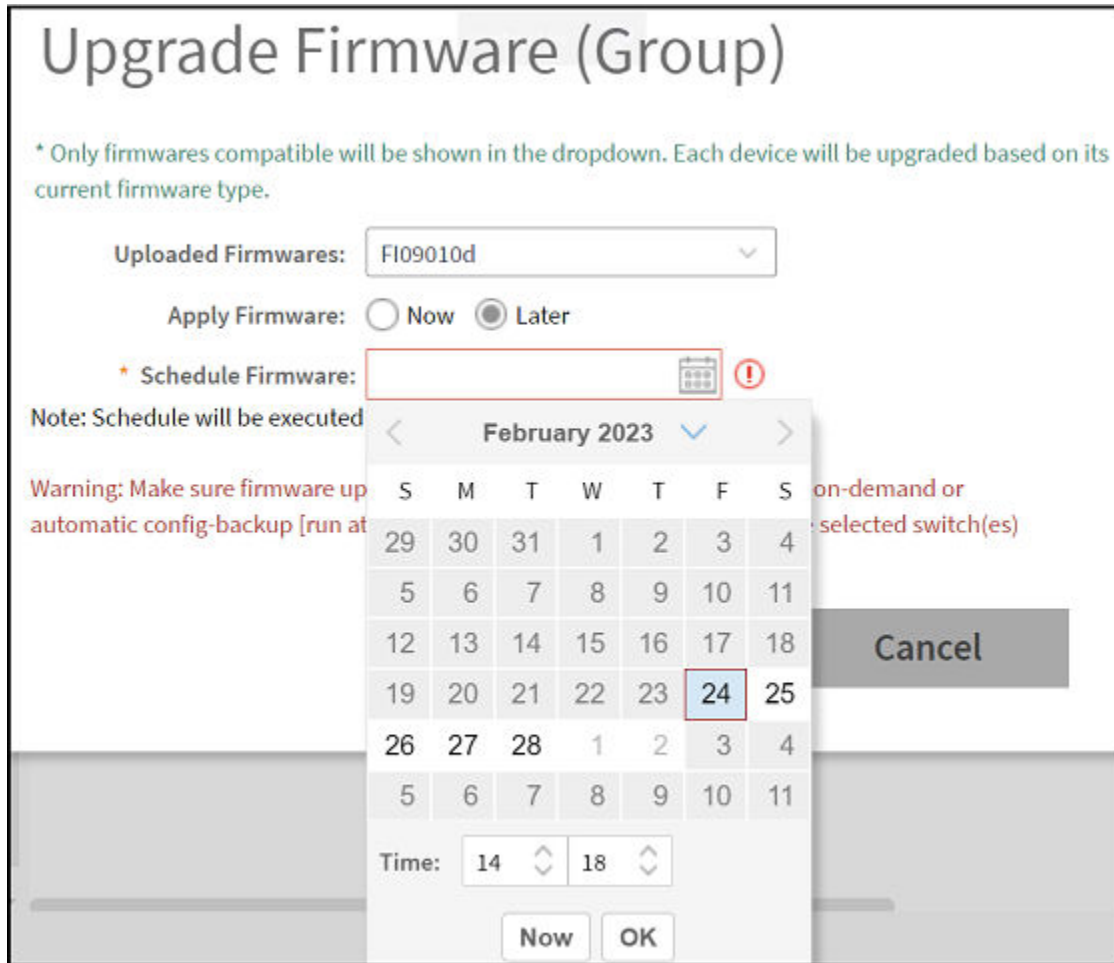
The **Upgrade Firmware** dialog box is displayed.

**FIGURE 19** Scheduling Firmware Upgrade



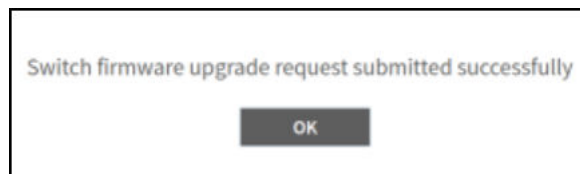
4. Complete the following fields:
  - **Uploaded Firmwares:** Select the firmware version that you want the switch to be upgraded to.
  - **Firmware Type:** Select type of firmware you want to upload to the switch. Options include **Switch** and **Router** images.
  - **Apply Firmware:** Set when you want to apply the new firmware version to the switch. You can select **Now** or **Later** to schedule your upgrade. If you select **Later**, then you must select the date and time from the **Schedule Firmware** field.

FIGURE 20 Scheduling Firmware Upgrade



The switch upgrade request success message is displayed.

FIGURE 21 Switch Upgrade Request Success



5. Click **OK**.

- To monitor the firmware upgrade progress, select the target switch and click the **Firmware History** tab. Hover your cursor over any message in the **Status** field for a tooltip providing additional information regarding that stage of the upgrade process.

The images of six stages of completion along with their tooltips are shown below.

**FIGURE 22** Preparing Phase with Tooltip

The screenshot shows the 'Firmware History' tab in the SmartZone management interface. A table lists the upgrade progress for switch FI08095d. The status is 'Preparing Phase' and the failure reason is 'N/A'. A tooltip is displayed over the status field, stating: 'Switch is providing necessary data to SZ for firmware upgrade'.

Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Preparing Phase	N/A

**FIGURE 23** Backup Image Start with Tooltip

The screenshot shows the 'Firmware History' tab. The status has updated to 'Backup image start'. A tooltip is displayed over the status field, stating: 'Switch starts to backup bootable image'.

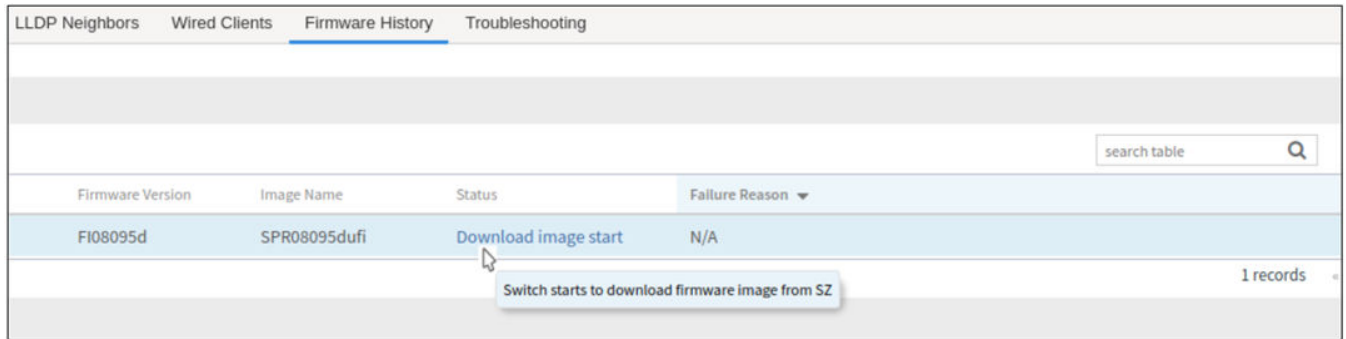
Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Backup image start	N/A

**FIGURE 24** Backup Image Complete with Tooltip

The screenshot shows the 'Firmware History' tab. The status has updated to 'Backup image complete'. A tooltip is displayed over the status field, stating: 'Switch has finished backup image'.

Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Backup image complete	N/A

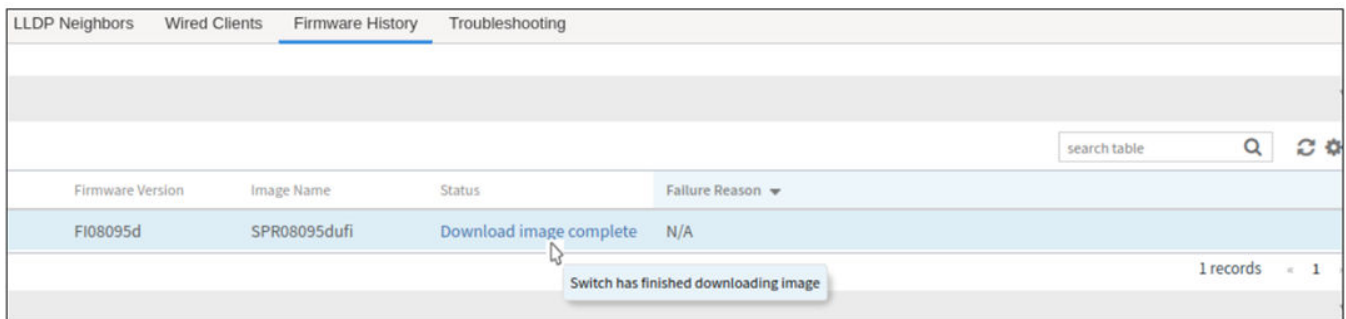
**FIGURE 25** Download Image Start with Tooltip



The screenshot shows a web interface with a navigation menu at the top containing 'LLDP Neighbors', 'Wired Clients', 'Firmware History' (which is selected), and 'Troubleshooting'. Below the menu is a search bar labeled 'search table' with a magnifying glass icon. The main content is a table with the following columns: 'Firmware Version', 'Image Name', 'Status', and 'Failure Reason'. A single row is visible with the following data: 'FI08095d' in the Firmware Version column, 'SPR08095dufi' in the Image Name column, 'Download image start' in the Status column, and 'N/A' in the Failure Reason column. A mouse cursor is hovering over the 'Download image start' status, and a tooltip box appears below it with the text 'Switch starts to download firmware image from SZ'. In the bottom right corner of the table area, it says '1 records'.

Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Download image start	N/A

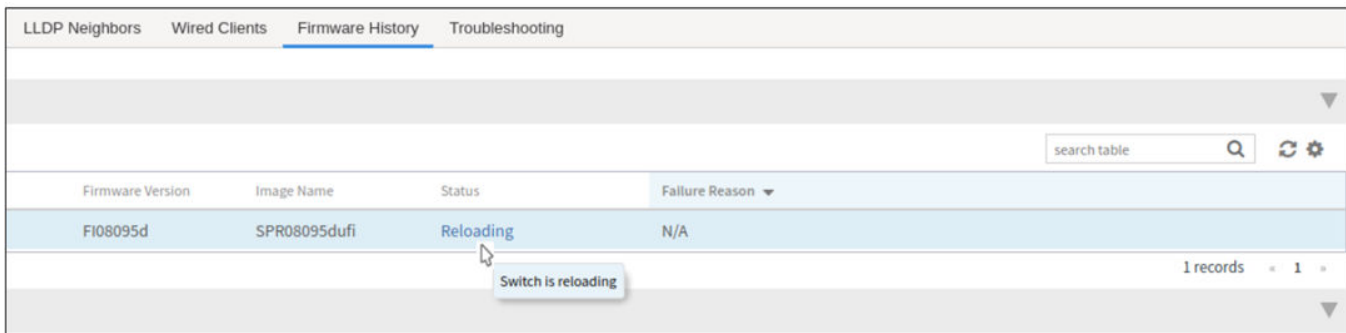
FIGURE 26 Download Image Complete with Tooltip



The screenshot shows the same web interface as Figure 26. The table now shows the status 'Download image complete' for the same row. A mouse cursor is hovering over 'Download image complete', and a tooltip box appears with the text 'Switch has finished downloading image'. The bottom right corner of the table area now says '1 records' with a small '1' next to it.

Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Download image complete	N/A

FIGURE 27 Reloading phase with tooltip



The screenshot shows the same web interface. The table now shows the status 'Reloading' for the same row. A mouse cursor is hovering over 'Reloading', and a tooltip box appears with the text 'Switch is reloading'. The bottom right corner of the table area now says '1 records' with a small '1' next to it.

Firmware Version	Image Name	Status	Failure Reason
FI08095d	SPR08095dufi	Reloading	N/A

## Viewing Switch Information

Details such as switch status, firmware version, and IP address are available for individual switches, stacks, and switch groups.

To view information on a switch, a stack, or a switch group, perform these steps.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.

2. In the **Organization** tab, Select the **Domain > Switch Group** or **Switch Group** and select the **Switch** to display information specific to it. In the **Details** tab, click **General** tab to display the switch information.

FIGURE 28 Switch Stack and General Information

	Traffic	Health	General	Configuration	Configuration Restore
DETAILS	<b>Info</b>				
	Switch Name	ICX7450-32ZP Router			
	MAC Address	60:9C:9F:1D:D7:20			
	Serial Number	EAR3301N001			
	IP Address	10.1.13.196			
	Gateway	10.1.13.1			
	Model	ICX7450-32ZP			
	Switch/Stack	Switch			
	Number of Switch Units	1			
	Firmware Version	SPR09010d			
<b>Status Summary</b>					
Status	Online				
Registration State	Approved				
# of Alarms	7				
Uptime	32 days, 4:03:41.00				
Last Configuration Backup	2023/02/24 09:00:07				
Switch Group	SWITCH-RA-ZONE				

The following information about the selected switch is displayed in the **General** tab:

- **Switch Name:** The name of the switch or group.
- **MAC Address:** The MAC address of the switch.
- **Serial Number:** The serial number assigned to the switch.
- **IP Address:** The IP of the controller that monitors the switch.
- **Gateway:** The gateway IP address through which the switch, group, or stack forwards data.
- **Model:** The model number of the switch.
- **Switch/Stack:** Whether the selected system is a standalone switch or a stack of switches.
- **Number of Switch Units:** The number of switches in a group or stack.
- **Firmware Version:** The firmware version uploaded to the selected switch.
- **Status:** The status of the switch, such as Online, Offline, or Flagged.

**NOTE**

Flagged status indicates that one or more switches have an outstanding alarms and/or Port errors are seen on the switch ports. Click **Flagged** to view the flagged switches.

- **Registration State:** The status of the switch, such as Approved, Offline, Online, or Flagged (when an event or alarm is triggered).
- **# of Alarms:** The number of alarms generated for the selected switch or stack.
- **Uptime:** The time that has elapsed since reboot.
- **Last Configuration Backup:** The time the switch or stack configuration was last backed up.
- **Switch Group:** The name of the group to which the switch belongs.
- **PoE Utilization (watts):** The total switch PoE utilization. For example, if the total PoE allocation for the switch is 520 Watts, and 300 Watts are used, the column displays 300/520 W.

## Configuring the Switch

SmartZone 5.1.1 introduces the switch configuration capabilities. The following features are added:

- **Zero Touch Provisioning:** Simplifies the initial deployment of switches. Allows you to define switch configuration at a switch group level. If a new switch joins the group automatically, it gets provisioned.
- **Ongoing Configuration Changes:** You can modify the switch configuration as a part of network maintenance. This includes modifying switch group level settings, port settings, and routing interfaces.
- **Stack formation:** You can configure individual switches to be formed into a stack directly from the controller.
- **Configuration copy:** You can copy configuration from a working switch to one or multiple new switches seamlessly.

You can view and modify various configuration parameters of switches from the controller web interface. You can create switch configuration profiles at the group level, individual switch level, and at the port level.

The **Configuration** page displays common configurations based on DNS, allows setting configuration values for a family of switches and also provides a summary of the switch configuration history.

You can update the configuration profile for new and existing switches, switches that join the controller after being offline, switches that may or may not have local feature changes through CLI/Telnet/SSH or other web interfaces.

After the switch configuration is updated successfully, you can continue to monitor the configuration deployed on the switch. If the switch configuration is not updated successfully, a message is displayed on the controller interface.

## Zero Touch Provisioning using Group level Configuration

You can create and view configurations that are defined at the switch group level. Within the switch group, there is an option to define common configuration that is applicable to all the switch models in the group and another option to select configuration based on switch family, for example ICX 7150, ICX 7250, and so on. When a new switch without any existing configuration running FastIron version 8.0.90a or later version joins the controller, the group level configuration is automatically applied to the switch. This includes the global AAA settings, common configuration, and model-specific settings. If the switch joining the group already has an existing configuration, then the group level configuration is not applied during the initial join. Only the subsequent changes done at the group level are applied.

### NOTE

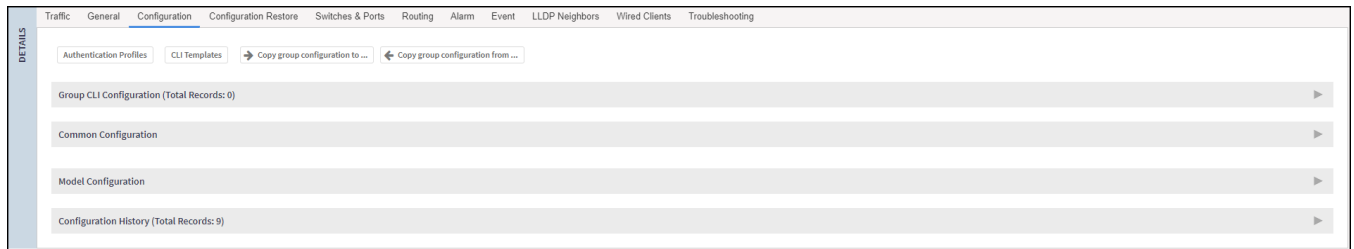
ICX switches must run FastIron 08.0.90a or later release to take advantage of the switch configuration capabilities of the controller.

## Creating a Common Configuration

You can create, view, and edit the configuration settings for a group of switches.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. From the system tree, select a **Domain > Switch Group** or **Switch Group** and in the **Details** tab, click the **Configuration** tab.

FIGURE 29 Configuration



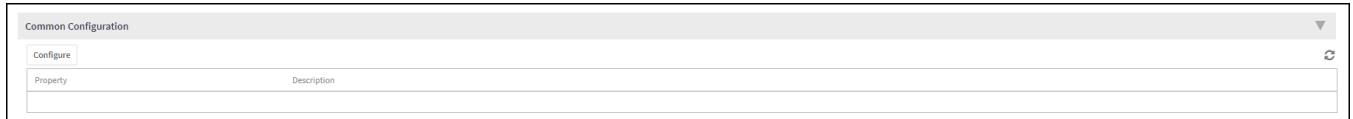


3. In the **Common Configuration** tab, click **Configure** to display the **Common Configuration** dialog box.

**NOTE**

In the following example, the Switch Group is the Default Group.

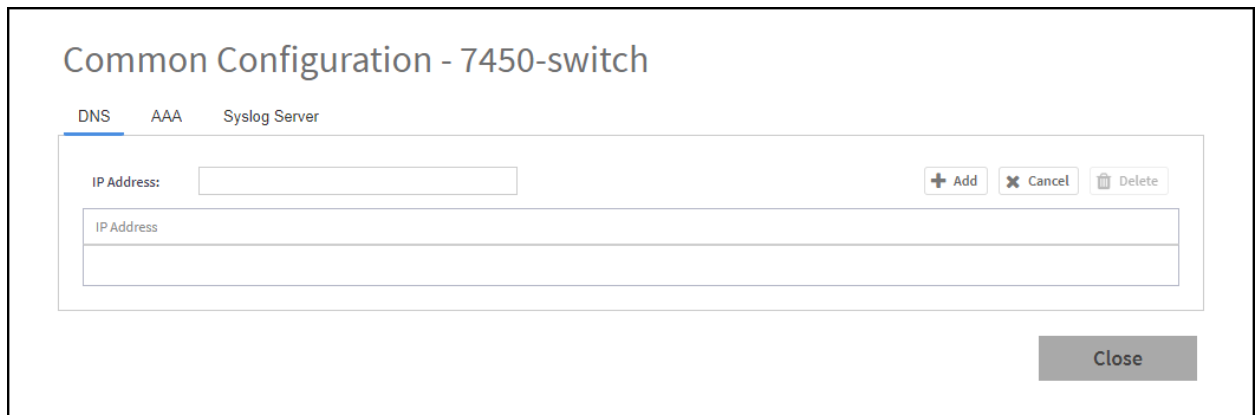
**FIGURE 30** Common Configuration



- a) Configure the **DNS** settings.

1. Click the **DNS** tab.

**FIGURE 31** DNS Settings



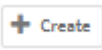
2. Enter the **IP address** and click **Add**.

The IP address is added to the **Common Configuration** page under **Property** and any new (factory default) switch joining this group will have the DNS configuration applied. If you want to edit the configuration, select it and click **Configure** to edit the settings.

- b) Configure the **AAA** settings.

1. Click the **AAA** tab.

2. Expand the **AAA Servers** section and configure one or more AAA servers.

- a. Click the  icon to display the **Create AAA Server** dialog box and complete the AAA server configuration, refer to *Configuring Switch AAA Servers* in the *RUCKUS SmartZone Management Guide*.

**FIGURE 32** Creating AAA Server

**Create AAA Server**

\* Name:

\* Type:  Radius  TACACS+  Local User

\* IP Address:

\* Auth. Port:

\* Acct. Port:

\* Shared Secret:

\* Confirm Shared Secret:

\* Purpose:    
Default   
Authentication   
Accounting

- b. Click **OK**.

**NOTE**

You can subsequently edit or delete a AAA server by selecting the server from the list in the **AAA Servers** section and selecting **Configure** or **Delete**, respectively.

- 3. Configure the **AAA Setting**.

FIGURE 33 AAA Setting

AAA Setting

Login Authentication

SSH Authentication:  ON      Telnet Authentication:  ON

First Pref: Local User      Second Pref: Please select data      Third Pref: Please select data

Authorization

Command Authorization:  OFF      Exec Authorization:  OFF

Level: Read Write      Server 1: Radius

Server 1: Radius      Server 2: Please select data

Server 2: Please select data

Accounting

Command Accounting:  OFF      Exec Accounting:  OFF

Level: Read Write      Server 1: Radius

Server 1: Radius      Server 2: Please select data

Server 2: Please select data

OK      Cancel

- a. Complete the **AAA Settings**. For more information on configuring and managing AAA servers for user authentication, refer to Configuring Switch AAA Server Settings in the *RUCKUS SmartZone Management Guide*.
- b. Click **OK**.
- c) Configure the **Syslog Server** settings.
  1. Click the **Syslog Server** tab.

**NOTE**

This feature is supported on FastIron 08.0.95 and later releases.



2. Complete the following fields:
  - **IP address:** Enter the **IP address** of the remote syslog server. Click **Cancel** to erase the entry in the field.
  - **Port:** Enter the port number in the **Port** field.

**NOTE**

The default setting is UDP port 514, but this can be changed as per your network requirements.

3. Click the  icon.

**NOTE**

Select the IP Address and click the **Delete** icon to delete the syslog server **IP Address**.

- d) Click **Close**.

### Creating Switch Model-Based Configurations

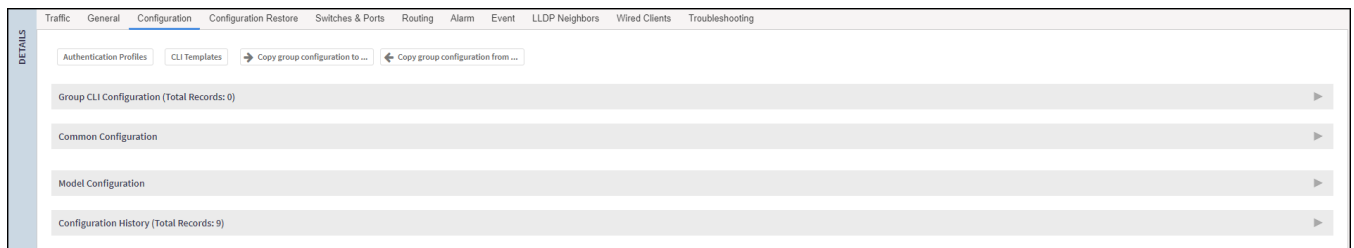
You can create and edit ACL, Layer 2, and Layer 3 configuration settings for a family of switches. You can also create or update the ACL to configure QoS profiles that prioritize VOIP and VIDEO VLAN traffic.

**NOTE**

Configuring the QoS Profiles requires ICX Firmware version 08.0.95.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. Select **Domain > Switch Group** or **Switch Group** and click the **Configuration** tab.

**FIGURE 34** Configuration



3. In the **Model Configuration**, select the **Switch Model** from the drop down list and click **Configure** to display the **Feature Configuration** dialog box.

FIGURE 35 Model Configuration

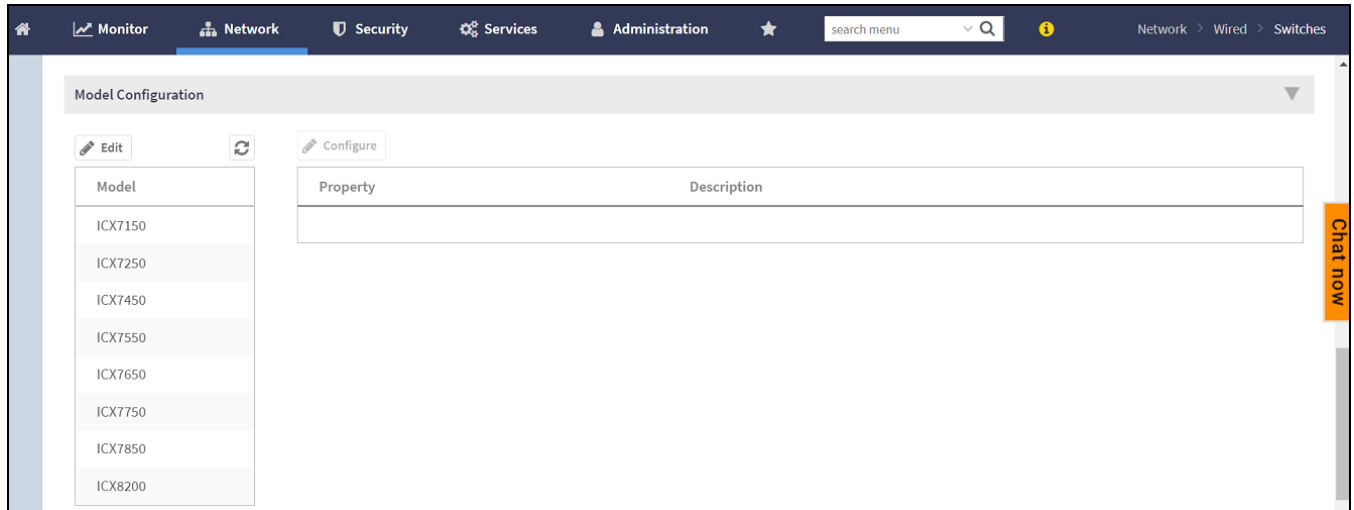
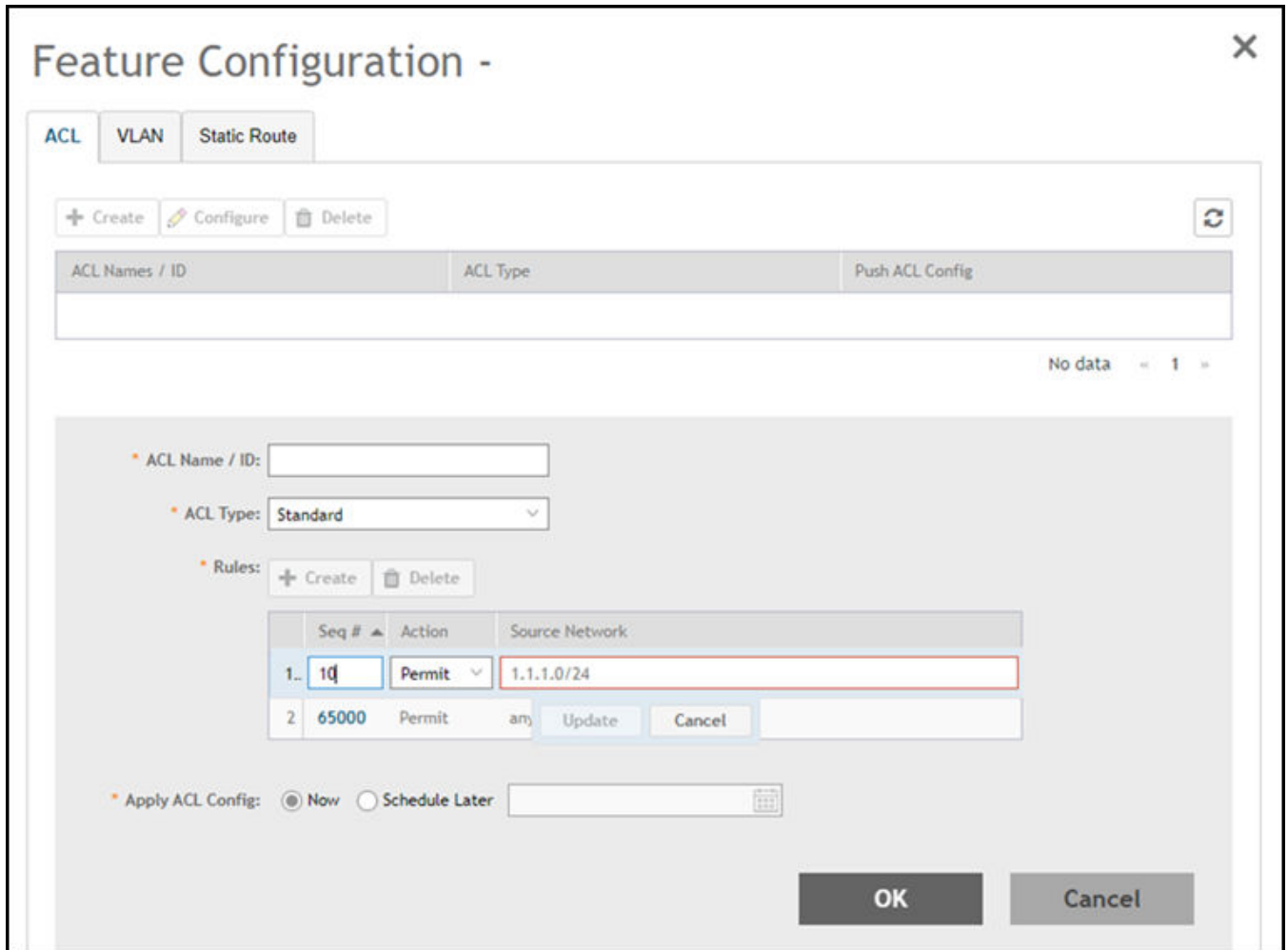


FIGURE 36 Feature Configuration



**NOTE**

The **Feature Configuration** page displays details about the ACL, VLAN, and static route. You can create, edit, and delete these configurations as necessary.


- a) Configure the **ACL** settings.
  - 1. Click the **ACL** tab.
  - 2. Click the  icon to display the **ACL** fields.

FIGURE 37 ACL Configuration with ICX Firmware version 08.0.95 - Extended ACL Type

The screenshot displays the ACL configuration page. At the top, there are tabs for 'Switch', 'ACL', and 'VLAN'. Below the tabs are buttons for '+ Create', 'Configure', and 'Delete'. A table lists ACL configurations with columns for 'ACL Names / ID', 'ACL Type', and 'Push ACL Config'. Below this is a form for creating a new ACL rule. The 'ACL Name / ID' field is empty. The 'ACL Type' is set to 'Extended'. Under 'Rules', there is a '+ Create' button and a 'Delete' button. A table shows the rule configuration with columns: Action, Source Network, Source Port, Destination Network, Destination Port, DSCP Matching, DSCP Marking, and Internal Priority Marking. The DSCP Matching, DSCP Marking, and Internal Priority Marking columns are highlighted with red boxes and labeled (1), (2), and (3) respectively. Below the table, there is an 'Apply ACL Config' section with radio buttons for 'Now' (selected) and 'Schedule Later'. At the bottom right, there are 'OK' and 'Cancel' buttons, and a 'Close' button at the very bottom right.

3. Complete the following fields:

- **ACL Name/ID:** Enter the name of the access control list or provide the list identifier.
- **ACL Type:** Select Standard or Extended from the drop down list.
- **Rules:** Click **Create** to create an ACL rule.

- Complete the following fields to configure the following ACL rule for the Standard ACL type:

You must provide the list sequence (**Seq#**), **Action** (Permit or Deny) and **Source Network** information to create the rule.

**NOTE**

Controller supports the "equal to" operator only.

**NOTE**

The Controller release 5.2.1 adds three new fields adds three fields (**DSCP Matching**, **DSCP Marking** and **Internal Priority Marking**) to configure QoS. After creating or updating the three fields, apply the ACL on a port or a VE to prioritize/de-prioritize traffic.

- Complete the following fields to configure the following ACL rule for the Extended ACL type:

- › **Seq#:** Enter the sequence.
- › **Action:** Select Permit or Deny.


- › **Source Network:** Enter the source network.
- › **Destination Network:** Enter the destination network.
- › **Source Port:** By default port 22 is selected.
- › **Destination Port:** By default port 22 is selected.
- › **DSCP Matching:** Enter the DSCP matching.
- › **DSCP Marking:** Enter the DSCP marking.
- › **Internal Priority Marking:** Enter the internal priority marking.
- **Apply ACL Config:** Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
- Click **OK** to add the newly created ACL configuration to the **ACL** page. You can edit the configuration by selecting **Configure**.

**NOTE**

You can also edit and delete the ACL configuration by selecting the options **Configure** and **Delete** respectively, from the **ACL** tab.

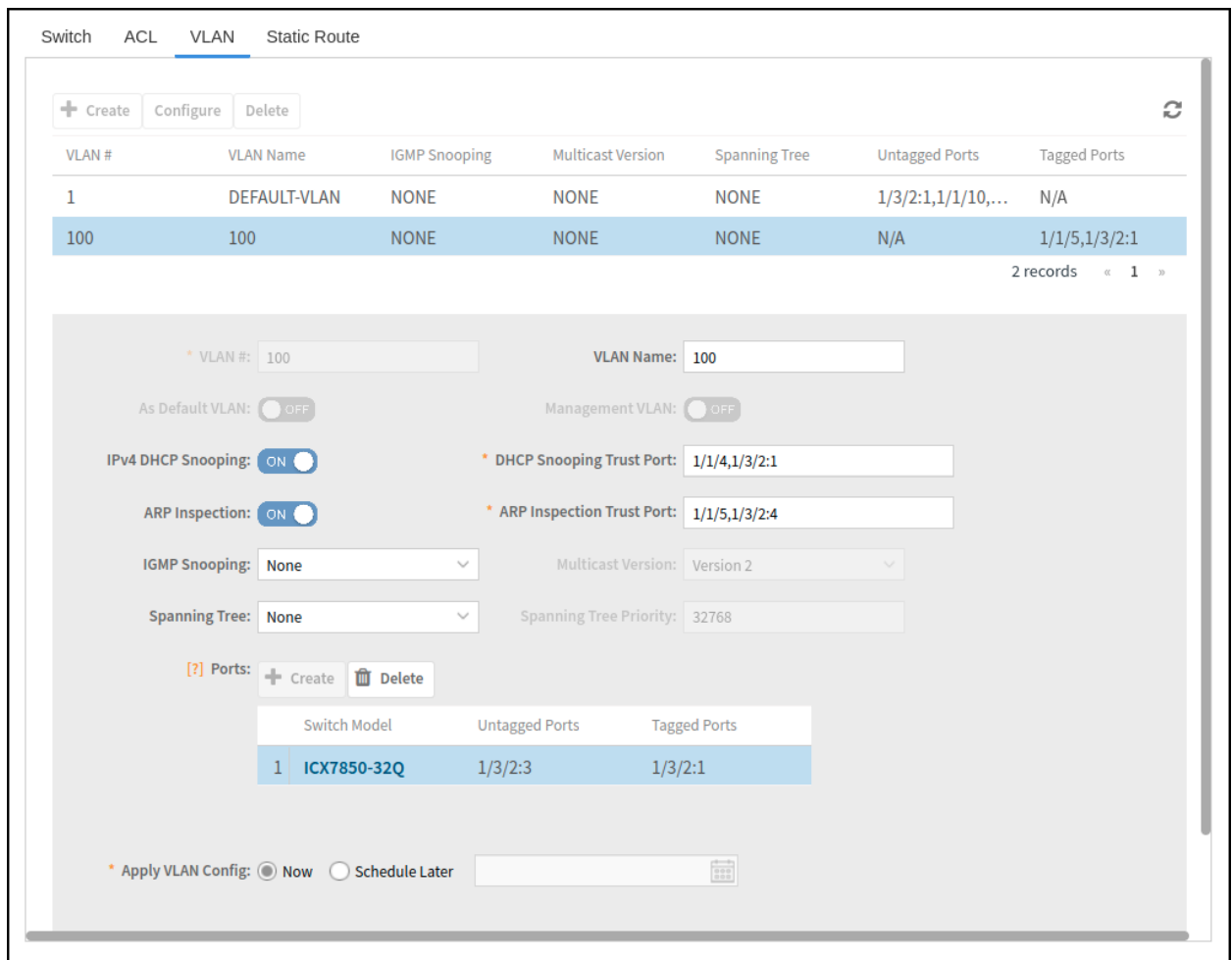
**NOTE**

Beginning with the 7.0 release, when you **Delete** an ACL, the ICX System log displays the SZ Administrator name associated with this activity. In the earlier releases, the ICX System log showed a generic message indicating that the network controller made the change.

- b) Configure the **VLAN** settings.
1. Click the **VLAN** tab.
  2. Click the  icon to display the **VLAN** fields.

**FIGURE 38** VLAN Configuration






3. Complete the following VLAN fields:

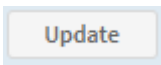
- **VLAN #:** Enter the number of the VLAN.
- **VLAN Name:** Enter the name of the Layer 2 VLAN.
- **As Default VLAN:** If you enable the **As Default VLAN** the **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.
- **Management VLAN:** By enabling this, you can configure Management VLAN for the switches or switch groups.
- **IPv4 DHCP Snooping:** Enable or disable IPv4 DHCP Snooping. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the breakout port for this option in the **DHCP Snooping Trust Port** field.
- **APR Inspection:** Enable or disable ARP Inspection. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the breakout port for this option in the **ARP Inspection Trust Port** field.
- **IGMP Snooping:** Select **None**, **Active**, or **Passive** from the list. The Internet Group Management Protocol (IGMP) allows the switch to track the communication between hosts and routers based on which the switch maintains a map of which links need which IP multicast streams. If you select **Active** or **Passive**, you are required to select the **Multicast Version** as well.
- **Spanning Tree:** Select **None**, **STP (802.1d)**, or **RSTP (802.1w)** from the list. Both Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) prevent creation of bridge loops when you have redundant paths in your network, and the

broadcast radiation that results from them. If you select **STP 802.1d** or **RSTP 802.1w**, you are required to select the **Spanning Tree Priority** as well.

- **Ports:** Click the  icon and complete the following fields:

**NOTE**

Different set of ports can be entered for each switch model.

- **Switch Model:** Select the switch model from the drop down list.
  - **Untagged Ports:** Enter the breakout port.
  - **Tagged Ports:** Enter the breakout port.
  - Click the  icon.
- **Apply VLAN Config:** Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
  - Click **OK** to add the newly created VLAN configuration to the **VLAN** page.

**NOTE**

You can also edit and delete the VLAN configuration by selecting the options **Configure** and **Delete** respectively, from the **VLAN** tab.

**NOTE**

Beginning with the 7.0 release, when you modify the **VLAN #** and **VLAN Name**, the ICX System log displays the SZ Administrator name associated with this configuration activity. In the earlier releases, the ICX System log showed a generic message indicating that the network controller made the change.


- c) Configure the **Static Route** settings.
1. Click the **Static Route** tab.
  2. Click the  icon to display the **Static Route** fields.

FIGURE 39 Static Route Configuration

The screenshot shows the 'Feature Configuration' interface for 'Static Route'. At the top, there are tabs for 'ACL', 'VLAN', and 'Static Route'. Below the tabs are buttons for '+ Create', 'Configure', and 'Delete', along with a refresh icon. A table with columns 'Destination IP', 'Next Hop', 'Admin Distance', and 'Apply Static Route Config' is shown, currently containing 'No data' and a page indicator '1'. Below the table is a configuration form with fields for 'Destination IP', 'Next Hop', 'Admin Distance', and 'Apply Static Route Config' (with radio buttons for 'Now' and 'Schedule Later'). At the bottom right of the form are 'OK' and 'Cancel' buttons. A 'Close' button is located at the bottom right of the entire configuration window.

3. Complete the following Static Route fields:

- **Destination IP:** Enter the destination IP address.
- **Next Hop:** Enter the next-hop IP address. Multicast and broadcast IP addresses are not allowed.
- **Admin Distance:** Enter a value from 1 through 255.
- **Apply Static Route Config:** Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
- Click **OK** to add the newly created static route configuration to the **Static Route** page.

**NOTE**

You can also edit and delete the Static Route configuration by selecting the options **Configure** and **Delete** respectively, from the **Static Route** tab.

d) Click **Close**.

The IP address is added to the **Model Configuration** page under **Property**. If you want to edit the configuration, select it and click **Edit** to edit the settings.

**NOTE**

Any changes made to the group level configuration including common configuration and switch model-based configuration will be applied to all the switches belonging to the group.

Configuration defined at group level can be chosen to be applied instantaneously by selecting the **Now** option or schedule for a later time using **Schedule later** option. The scheduling option is only applicable if you are trying to make changes to existing switches in the group. For any new switches that are joining the group, this configuration gets applied instantaneously.

## Copying Switch Group Configuration

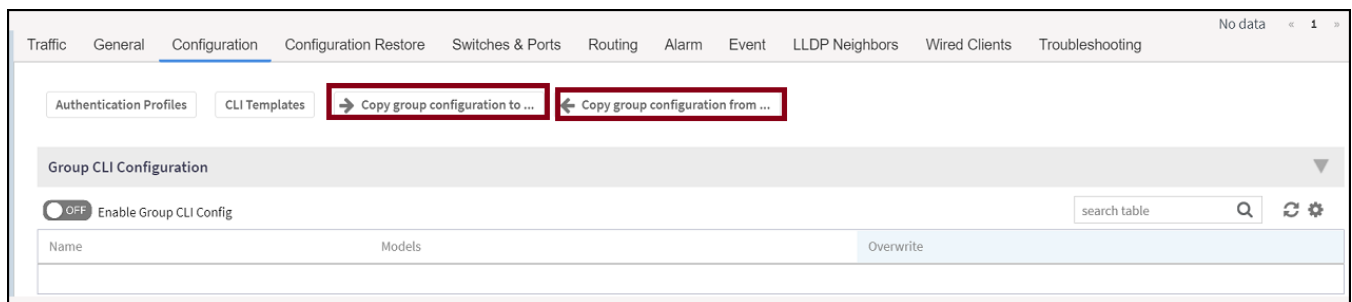
You can copy the configuration settings from a working switch to one or multiple new switches.

### NOTE

It is recommended to exercise caution when using the copy configuration option as it replaces the entire configuration of the destination switch.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and in the **Details** tab click **Configuration** tab.

FIGURE 40 Switch Group Configuration Tab



3. Click **Copy group configuration to** icon to display the **Copy config To Other Switches** dialog box.
4. Select a **Domain > Switch Group** or **Switch Group** to which you want to copy the configuration profile, and click **OK**.
5. Click **Copy group configuration from** icon to to display the **Copy config From Another Switch** dialog box.
6. Select a **Domain > Switch Group** or **Switch Group** from which you want to get the configuration profile, and click **OK**.

## Accessing AAA Settings for Switch Configuration

You can create, view, and edit the configuration settings for a group of switches.

Configure the switch AAA settings, refer to *Configure the AAA settings* in the [Creating a Common Configuration](#) on page 48.

## Viewing the Configuration History of Switches

Starting with the 7.0 release, you can view the configuration status of a selected switch or a switch group in the **Configuration History**. You can select a particular record in the **Configuration History** to view the details such as Switch Name, Switch Serial Number, Start Time, End Time, Status and the command lines that were sent to the switch in the **Configuration Details** table. In the earlier releases, when you configured a CLI template for multiple switches, only the configuration status for the switch group was displayed in the **Configuration** tab; the configuration status of the affected switch was not seen.

### NOTE

The **Configuration History** table displays a maximum of 250 records. The command lines in the **Configuration Details** displays a maximum of 1000 characters. Sensitive data such as the passwords are replaced with '\*\*\*\*\*'.

Complete the following steps to view the **Configuration History** in the **Configuration** tab.

1. From the main menu, go to **Network > Wired > Switches**.  
The **Switches** page is displayed.
2. Select a Switch. In the **Details** pane, click the **Configuration** tab, and locate the section titled **Configuration History**.

**FIGURE 41** Viewing the Configuration History

The screenshot displays the 'Configuration History' section within the 'Configuration' tab of the SmartZone Switch Management interface. The interface includes a top navigation bar with tabs: Traffic, Health, General, Configuration, Configuration Restore, Ports, Alarm, Event, LLDP Neighbors, Wired Clients, Firmware History, and Troubleshooting. Below the Configuration tab, there are buttons for 'Copy Config To Other Switches' and 'Get Config From Another Switch'. A 'Configuration' dropdown menu is visible. Below it, a 'Configure' button and a table with columns 'Property' and 'Description' are shown. The 'Configuration History' section is highlighted with a red border and contains a table with columns 'Date & Time', 'Node', 'Type', and 'Message'. The table lists several configuration events for node 'ca-vszh-test-02'.

Date & Time	Node	Type	Message
2023-02-08 15:45:37	ca-vszh-test-02	PROVISIONING	Success (1) / Failed (0) / Applied (0) / Failed No Response (0) / Failed Save to Flash (0)
2023-02-08 15:45:37	ca-vszh-test-02	SWITCH_GROUP_CONFIGS	Success (1) / Failed (0) / Applied (0) / Failed No Response (0) / Failed Save to Flash (0)
2023-02-08 16:09:43	ca-vszh-test-02	PROVISIONING	Success (1) / Failed (0) / Applied (0) / Failed No Response (0) / Failed Save to Flash (0)
2023-02-08 16:09:44	ca-vszh-test-02	SWITCH_GROUP_CONFIGS	Success (1) / Failed (0) / Applied (0) / Failed No Response (0) / Failed Save to Flash (0)
2023-02-09 21:06:45	ca-vszh-test-02	SWITCH_GROUP_CONFIGS	Success (1) / Failed (0) / Applied (0) / Failed No Response (0) / Failed Save to Flash (0)
2023-02-12 17:43:39	ca-vszh-test-02	SWITCH_GROUP_CONFIGS	Success (1) / Failed (0) / Applied (0) / Failed No Response (0) / Failed Save to Flash (0)
2023-02-17 14:43:01	ca-vszh-test-02	MODEL	Success (0) / Failed (1) / Applied (0) / Failed No Response (0) / Failed Save to Flash (0)
2023-02-17 14:43:59	ca-vszh-test-02	MODEL	Success (1) / Failed (0) / Applied (0) / Failed No Response (0) / Failed Save to Flash (0)

18 records

3. Select a specific configuration history that you want to explore, and click on it.

The **Configuration Details** page is displayed, showing information associated with that particular entry.

FIGURE 42 Viewing Configuration Details

The screenshot displays the SmartZone Switch Management interface. At the top, there are navigation tabs: Traffic, Health, General, Configuration (selected), Configuration Restore, Ports, Alarm, Event, LLDP Neighbors, Wired Clients, Firmware History, and Troubleshooting. Below the tabs are two buttons: 'Copy Config To Other Switches' and 'Get Config From Another Switch'. A 'Configuration' dropdown menu is visible, with a 'Configure' button below it. A table lists configuration categories: Switch Specific (Switch setting), ACL (Access control list), and VLAN (VLAN setting). Below this is the 'Configuration History' section, which includes a search table and a table with columns: Date & Time, Node, Type, and Message. The table contains several entries, with the last one highlighted in blue. Below the history table is the 'Configuration Details' section, which has checkboxes for 'Success' and 'Failure'. It features a table with columns: Switch Name, Serial Number, Start Time, End Time, and Status. One entry is shown: ICK7150-C12 Router, FEK323050A0, 2023-02-17 14:43:59, 2023-02-17 14:44:17, SUCCESS. To the right of this table is a code block showing configuration snippets: 'ip access-list STANDARD \*acl1\*' and 'sequence 65000 PERMIT any'. The bottom of the details section shows '1 records' and a pagination control.

## Data Syncing on the Switch Table

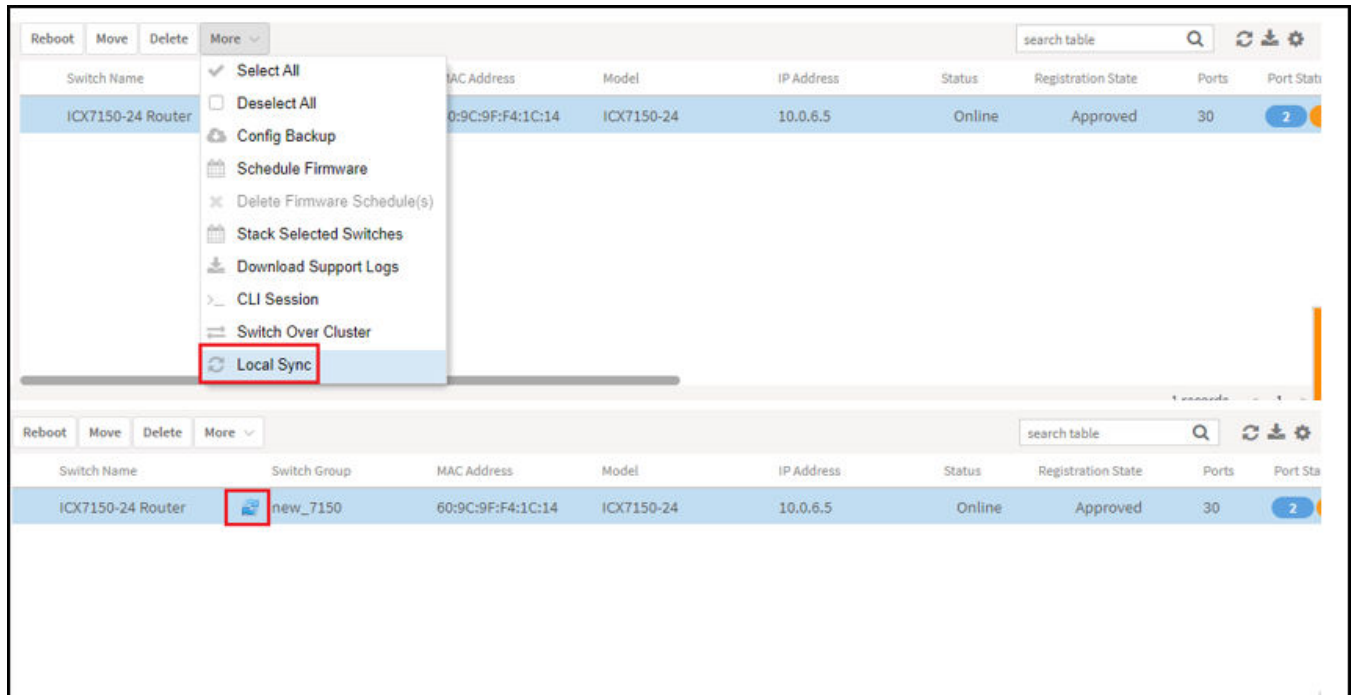
When a switch running FastIron 08.0.90 or later joins the controller, the controller runs the Local Sync operation every 5 minutes. If the changes are made on the switch console or any configuration changes are deployed on the controller, the controller syncs those corresponding changes to the switch or port table five minutes later, which causes a delay. Therefore, beginning with SmartZone 6.1.1, the Local Sync time is reduced from 5 minutes to 3 minutes to speed up the process.

When a CLI session is closed, Local Sync is triggered automatically to update the changes on the controller. Similarly, the controller can trigger Local Sync manually for a selected switch.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.

- In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**. Click **More > Local Sync**.

FIGURE 43 Selecting LocalSync on the Controller UI



## Switch Level Configuration

In addition to the group level configuration, individual switch-level configuration can be edited by selecting the switch from the Switch table.

Switch-specific settings include **Hostname**, **Jumbo Mode**, **IGMP Snooping**, and **DHCP Server**. In addition, the switch configuration defined at the group level is available for editing at the switch level.

### Creating Switch Level Configuration

You can configure switch, ACL, VLAN, and static route settings for each switch.

- On the menu, click **Network > Wired > Switches** to display the **Switches** window.
- In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

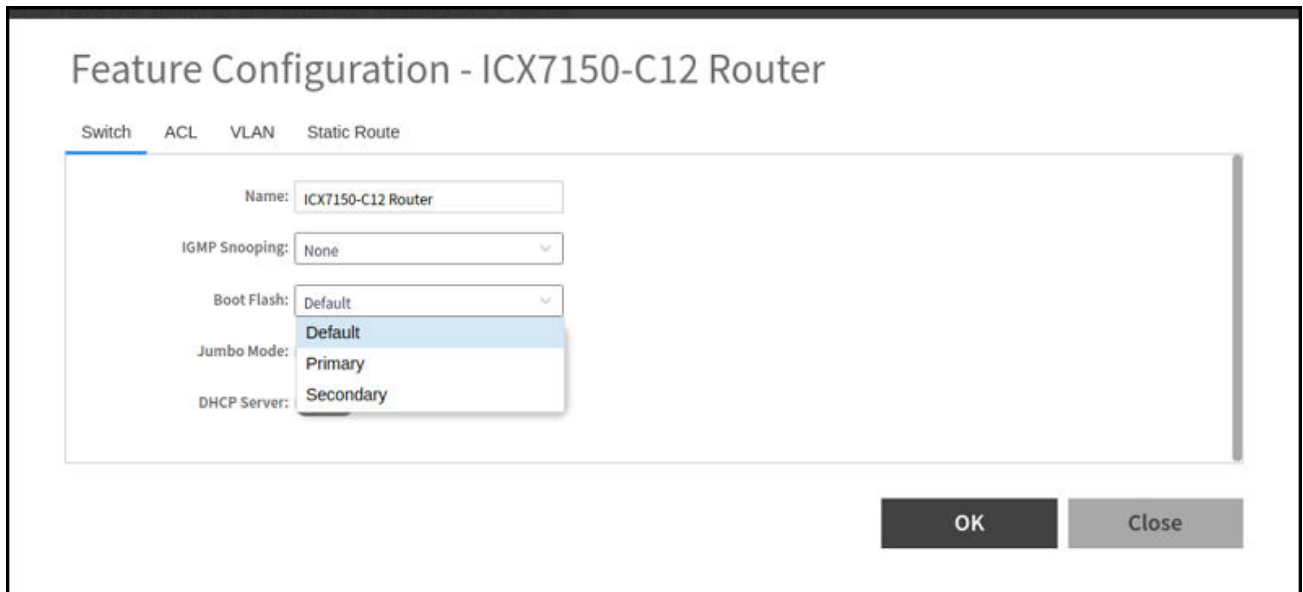
- In the **Model Configuration** tab, select the **Switch Model** and click



icon to display the **Feature Configuration** dialog box.

4. Configure the Switch settings.
  - a) Click **Switch** tab.

**FIGURE 44** Switch Configuration



- b) Complete the following fields:
  - **Name:** Enter the name of the switch.
  - **IGMP Snooping:** Select the profile from the list.
  - **Boot Flash:** Select the **Default**, **Primary** or **Secondary** option to configure boot preference.
  - **Jumbo Mode:** Enable this option to reboot the switch.
  - **DHCP Server:** Enable this option and click **Create** to configure the following DHCP server settings:

**NOTE**

You must disable the DHCP client before enabling the DHCP server.

- **Pool Name:** Enter a name.
- **Network/Mask:** Enter the network address and network mask.
- **Excluded Range:** Enter the network range to be excluded.
- **Lease Time:** Enter the lease time duration.
- **Default Router IP:** Enter the default router IP address.
- **Options:** Click **Create** and enter the option number, , select a type, and enter a value for the option.

Click **Update** to apply the option.


5. Configure the switch ACL settings, refer to *Configure the ACL settings* in the [Creating Switch Model-Based Configurations](#) on page 52.



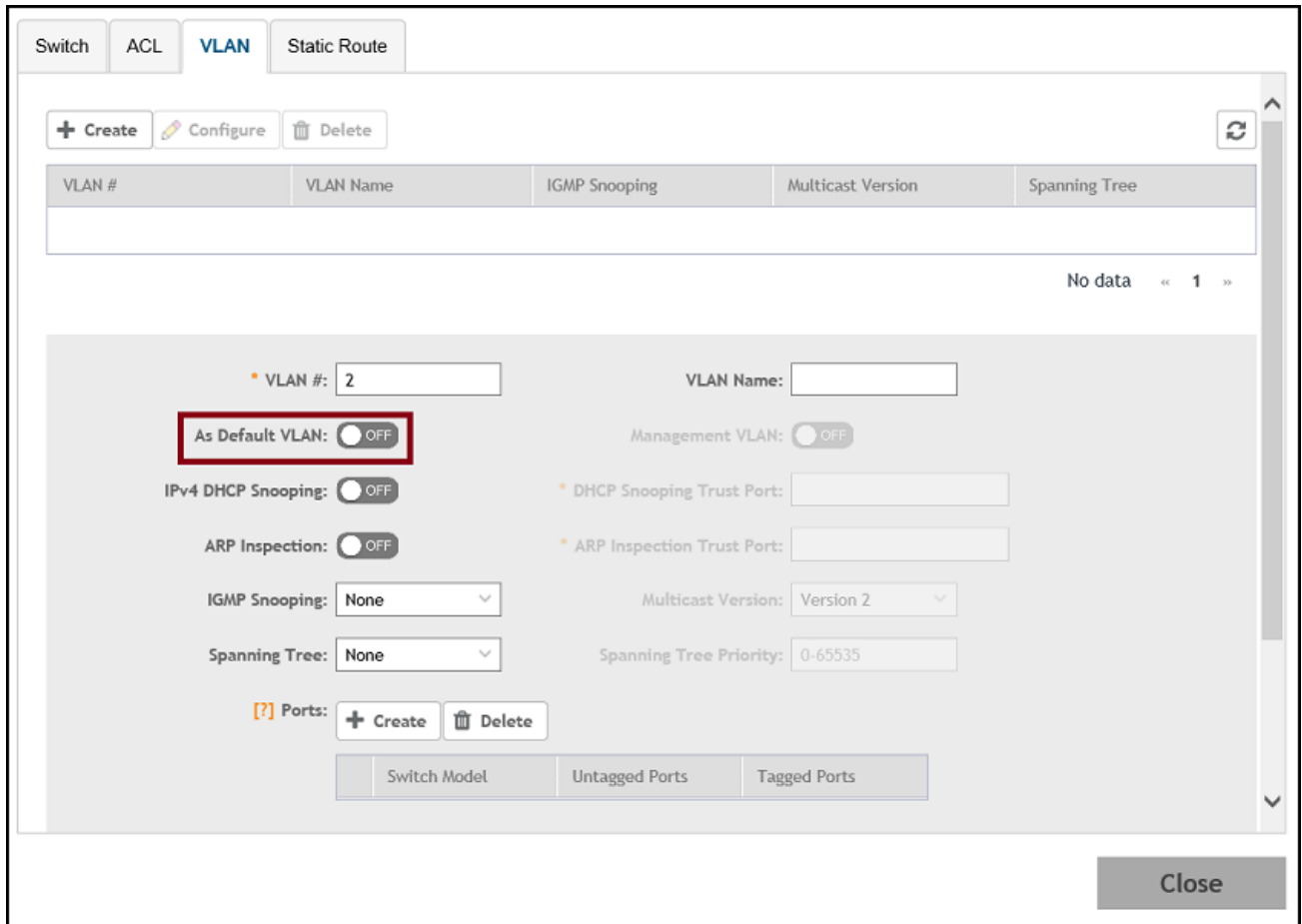
- Configure the switch VLAN settings.

**NOTE**

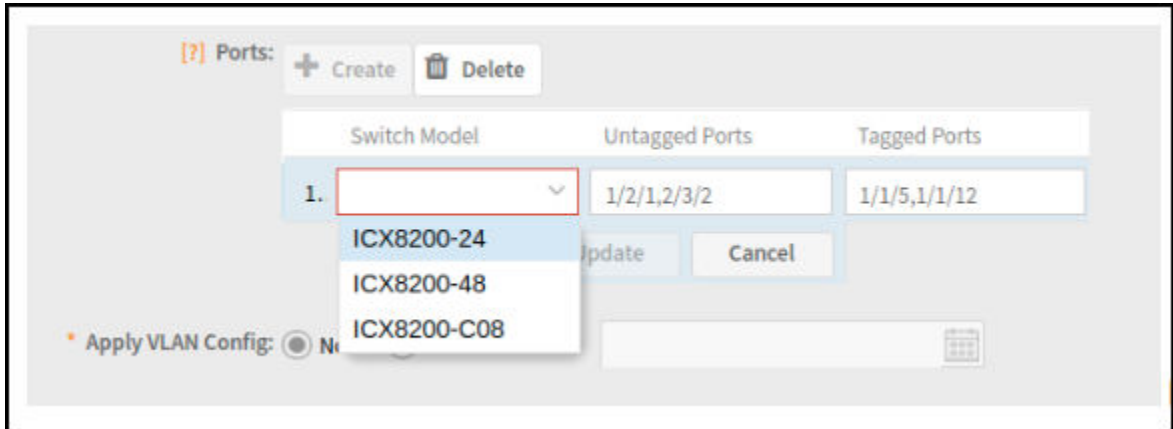
You can create a new VLAN and set it as the default VLAN.

- Click **VLAN** tab.
- Click  icon to display the **VLAN** fields.

**FIGURE 45** VLAN Configuration



**FIGURE 46** Creating Port and Adding Port Details



c) Complete the following fields:

- **VLAN#:** Enter a unique number for VLAN.
- **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.

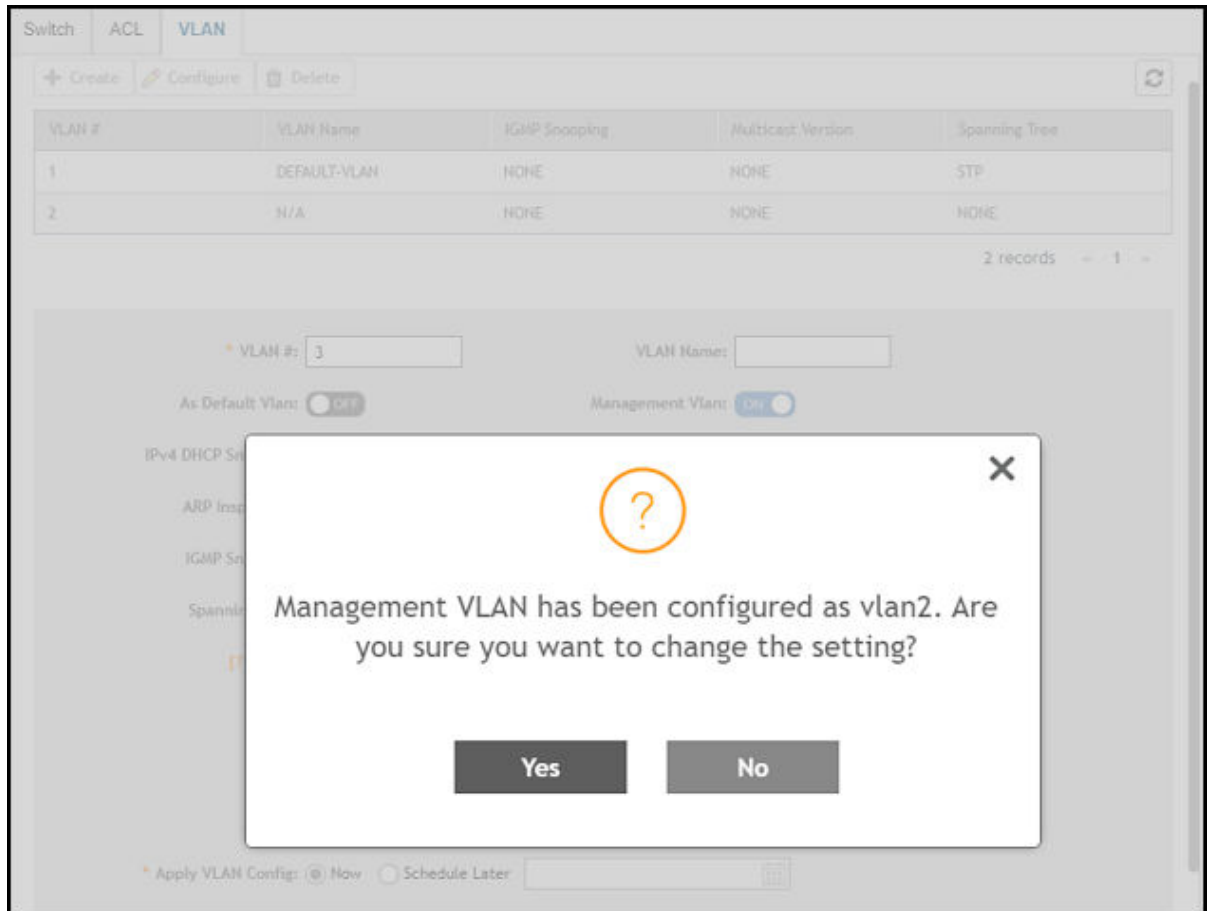
**NOTE**

If you enable the **As Default VLAN**, the **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.

- **Management VLAN:** You can configure the Management VLAN for the switches or switch groups in the following ways:
  - Enable **Management VLAN**, and click **OK**.

If the VLAN is configured as the default VLAN, enable or disable **Management VLAN** on the default VLAN, and click **OK**. A dialogue box is displayed, as shown in the following.

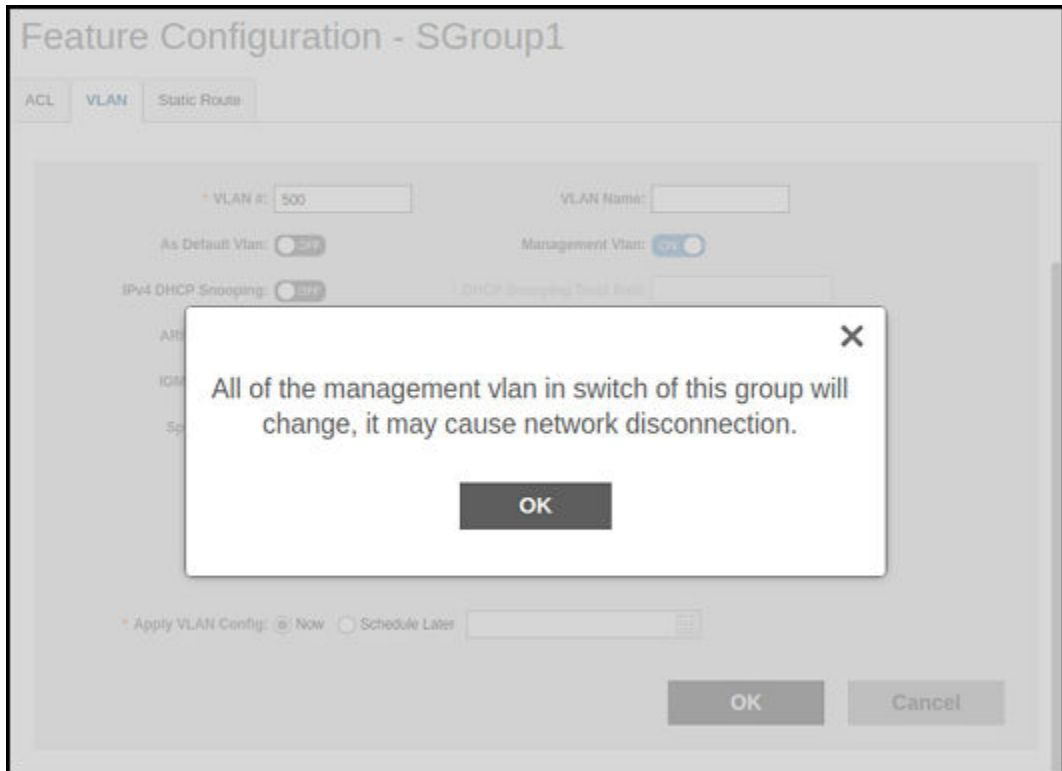
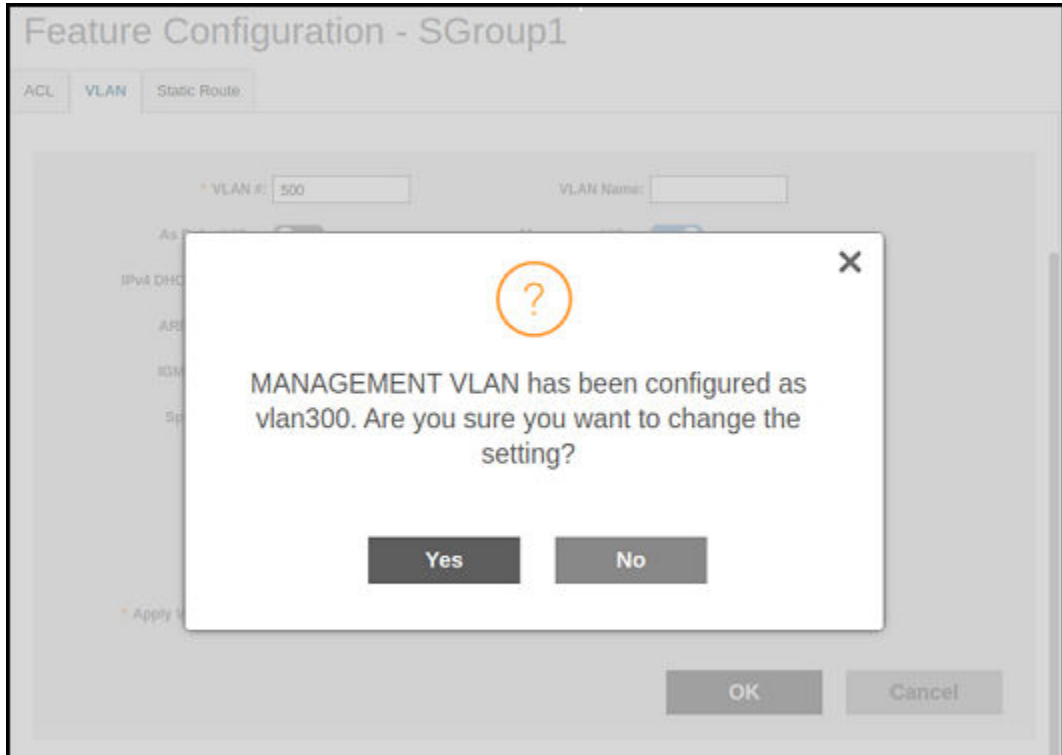
FIGURE 47 Management VLAN Confirmation



If **Management VLAN** is enabled on a VLAN and you try to enable it on another VLAN, the controller displays a dialogue box showing the VLAN ID that has been configured as the Management VLAN. If you click **Yes**, the controller overwrites the settings.

- For a switch group, the controller displays a dialogue box, as shown in the following figure.

FIGURE 48 Management VLAN Confirmation Dialogue Box



- **IPv4 DHCP Snooping:** Enable or disable IPv4 DHCP Snooping. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **DHCP Snooping Trust Port** field.
- **APR Inspection:** enable or disable ARP Inspection. Enabling this option allows the controller to send the ACL-per-port-per-vlan message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **ARP Inspection Trust Port** field.
- **IGMP Snooping:** Select **None**, **Active**, or **Passive** from the list. The Internet Group Management Protocol (IGMP) allows the switch to track the communication between hosts and routers based on which the switch maintains a map of which links need which IP multicast streams. If you select **Active** or **Passive**, you are required to select the **Multicast Version** as well.
- **Spanning Tree:** Select **None**, **STP (802.1d)**, or **RSTP (802.1w)** from the list. Both Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) prevent creation of bridge loops when you have redundant paths in your network, and the broadcast radiation that results from them. If you select **STP** or **RSTP**, you are required to select the **Spanning Tree Priority** as well.
- **Ports:** Click **Create** to assign the ports to the switch model. Enter values for **Switch Model**, **Untagged Ports**, and **Tagged Ports**.
- **Apply VLAN Config:** Select **Now** or **Schedule Later**. If you choose to schedule the configuration deployment for later, provide the time and date.
- Click **OK** to add the newly created VLAN configuration to the **VLAN** tab.

#### NOTE

You can also edit and delete the VLAN configuration by selecting the options **Configure** and **Delete** respectively, from the **VLAN** tab.

7. Configure the switch Static Route settings, refer to *Configure the Static Route settings* in the [Creating Switch Model-Based Configurations](#) on page 52.
8. Click **Close**.

The configurations are updated under **Property**. If you want to edit the configuration, select it and click **Edit** to edit the settings.

#### NOTE

Use the switch-level option to add additional ACLs, VLANs, or static routes other than those already defined at the switch group level. Use the group-level configuration to make changes to existing settings at the group level.

## Copying Configuration

If you already have a switch with the desired set of features configured, controller provides an option to load the current configuration of the switch, remove unique settings like hostname, IP addresses, and so on, and copy it to one or more target switches. This procedure is applicable only if the target switches have no existing configuration.

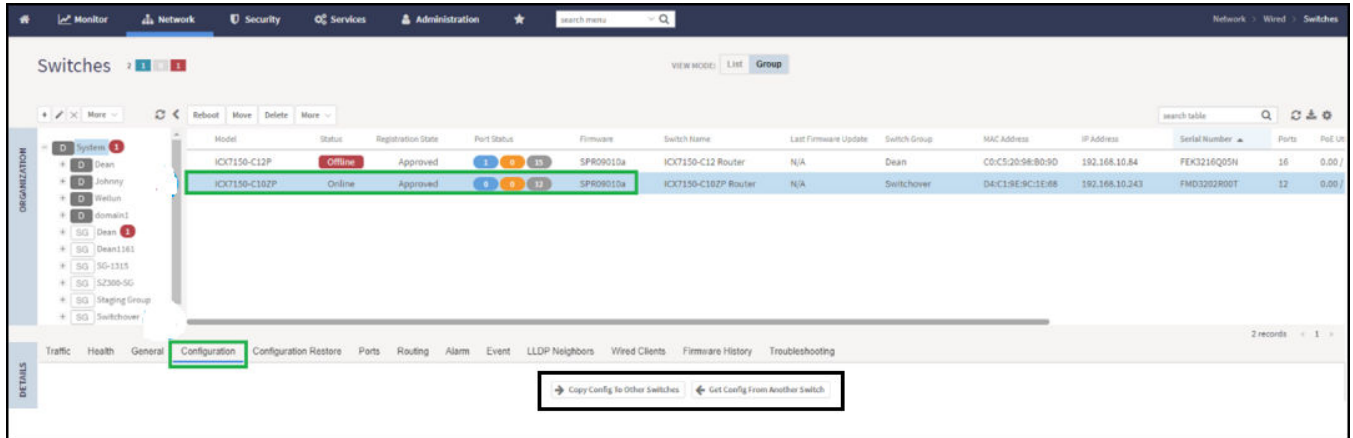
Complete the following steps to copy configuration to one or more target switches.

1. From the main menu, go to **Network > Wired > Switches**.

The **Switches** page appears.

2. Select the switch and then the **Configuration** tab.

FIGURE 49 Switch Group Configuration Tab



3. Click **Copy Configuration To**. This option lets you replace the entire configuration (startup-config) of the selected switch with that of a source switch.
4. Click **Get Configuration From** and select the switch or group from which you want to get the configuration profile, and click **OK**. This option lets you replace the entire configuration of destination switches (one or more) with the configuration of the selected switch.



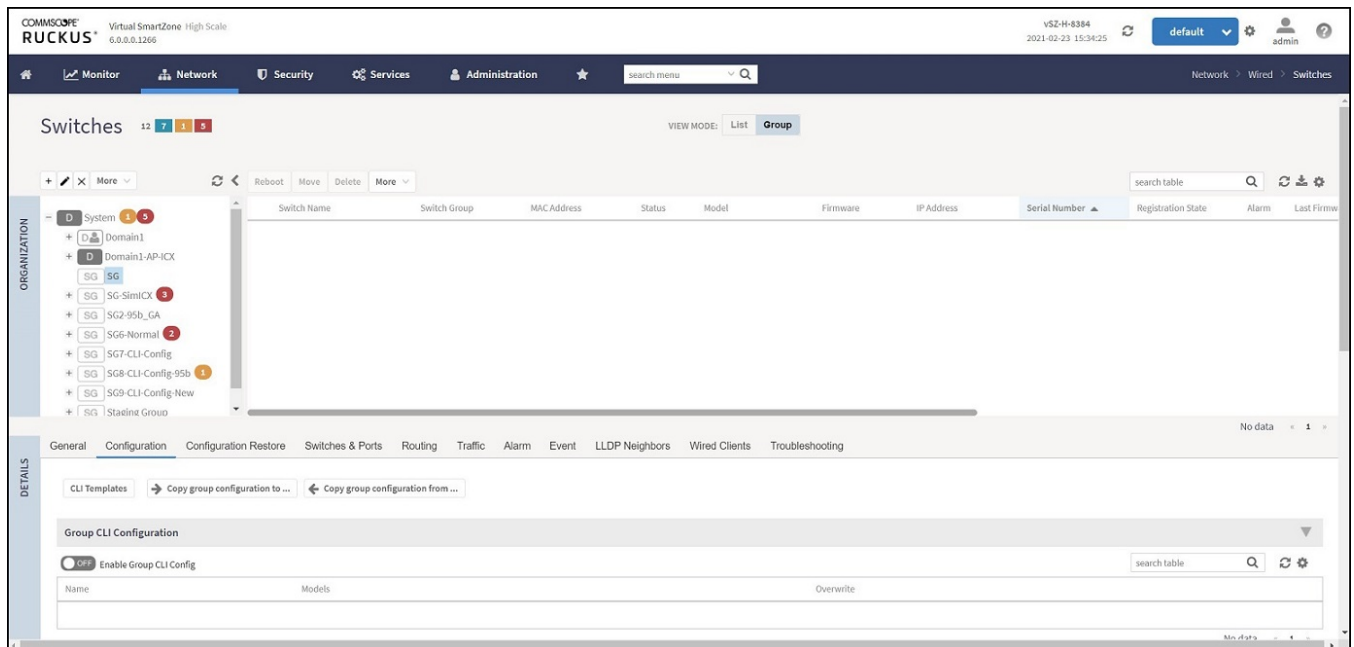
- You cannot return to GUI mode to define the Switch group configuration unless the switch group is deleted and re-created.

## Enabling the Group CLI Configuration

An administrator can create a new template or modify an existing Group CLI configuration for the switch group before enabling the template.

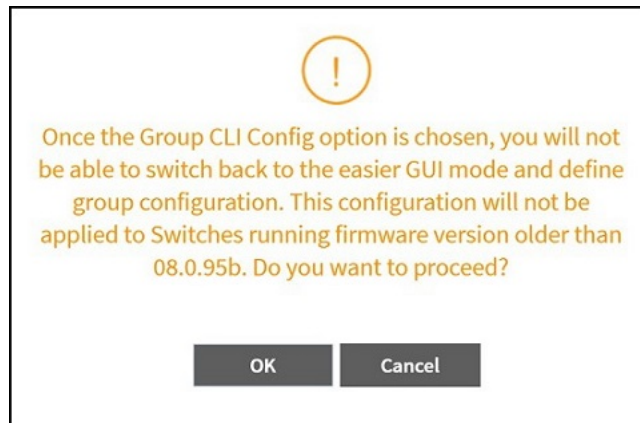
1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

FIGURE 51 Enabling Group CLI Config setup



3. In the **Group CLI Configuration** tab, switch ON **Enable Group CLI Config** to display the **Confirming Group CLI Configuration Setup** dialog box.

FIGURE 52 Confirming Group CLI Configuration Setup



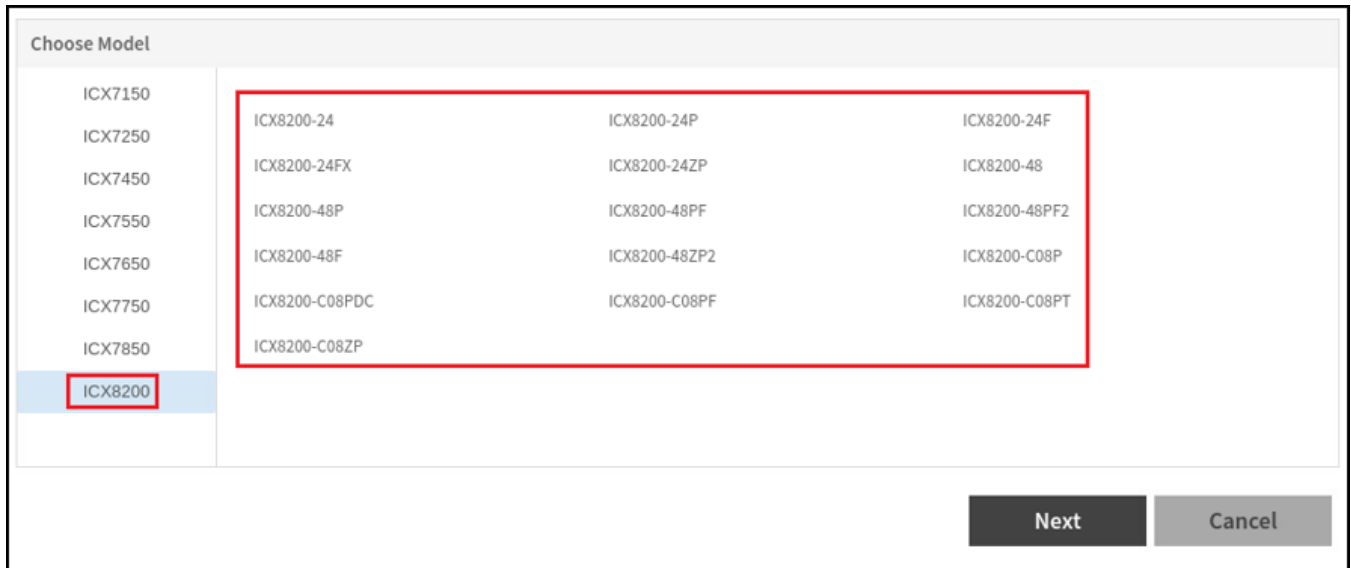


4. Click **OK** to display the **Group CLI Configuration** dialog box.
5. In the **Choose Model**, select one or more ICX models to create a new Group CLI Configuration template and click **Next** to display the **CLI Configuration** tab. You can also select an existing ICX model and click **Next** to modify the Group CLI configuration.

**NOTE**

The RUCKUS ICX devices that have already been selected in the Group CLI Configuration will not be available.

**FIGURE 53** Choosing ICX Models



6. Enter the name of the Group CLI Configuration in the **Name** field. Insert the command lines in the space provided. Users can choose the CLI commands under the 'Examples' pane to build configuration. Alternatively, CLI commands can be typed directly or copied from a notepad and pasted into the 'CLI Configuration' box.

**NOTE**

It is recommended that users get familiarized with FastIron commands and their ordering to avoid any issues with applying the configuration.

**FIGURE 54** Entering the Name in the new Group CLI Configuration

The screenshot shows the 'Group CLI Configuration' interface. On the left is an 'Examples [?]' pane with a scrollable list of CLI command categories: (Required) manager active-list, ARP inspection, CLI banner, Clock, DHCP snooping, IP config (on VE), IP config (on loopback), ND inspection, OSPF, PIM, and Port level. The main area is titled 'CLI Configuration' and contains a 'Name:' field with the placeholder text 'Enter a name for this configuration'. Below the name field is a large text area for entering CLI commands, with a warning message: 'It is user responsibility to ensure the validity and ordering of CLI commands are accurate. The recommendation is to get familiarized with ICX FastIron CLI commands to avoid configuration failures.' Below the text area is an 'Edit Variable' section with a '+ Add' button and a table with columns: Name, Type, Value 1, Value 2, and Value 3. At the bottom left, there is a checkbox labeled 'Overwrite existing configuration on the Switches'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

FIGURE 55 Inserting Command Lines in the New Group CLI Configuration

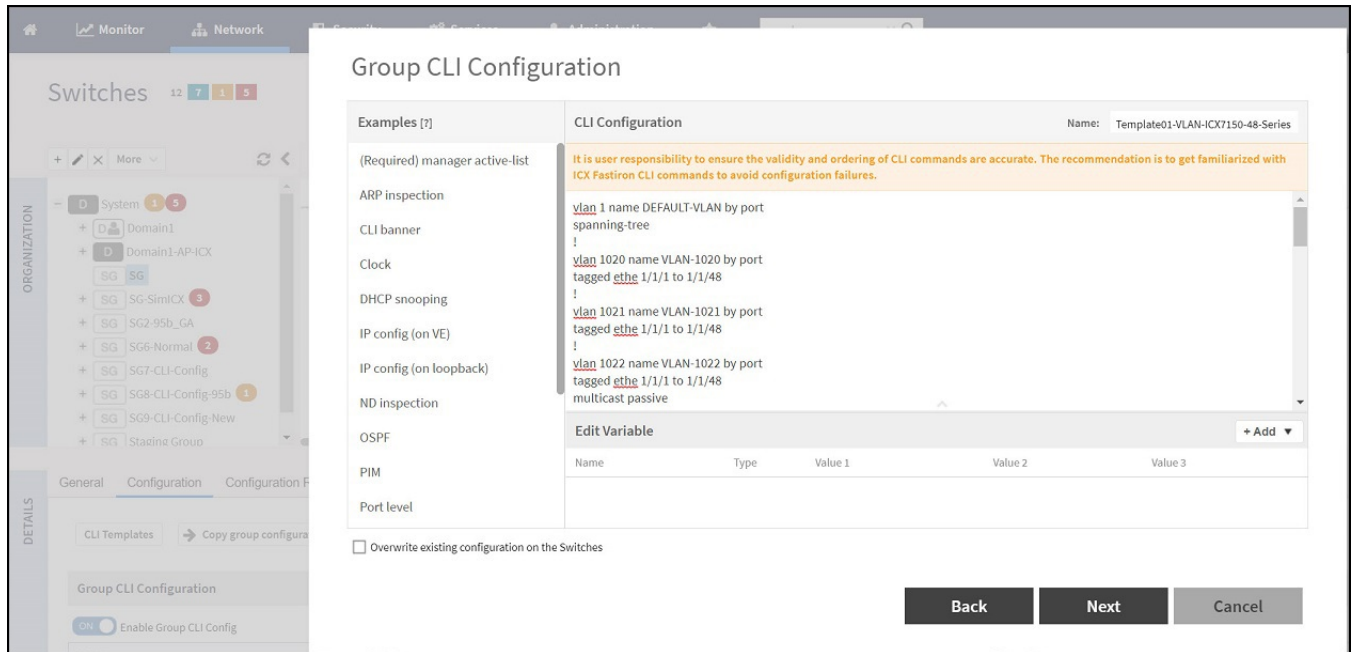


FIGURE 56 Support for space in variable string

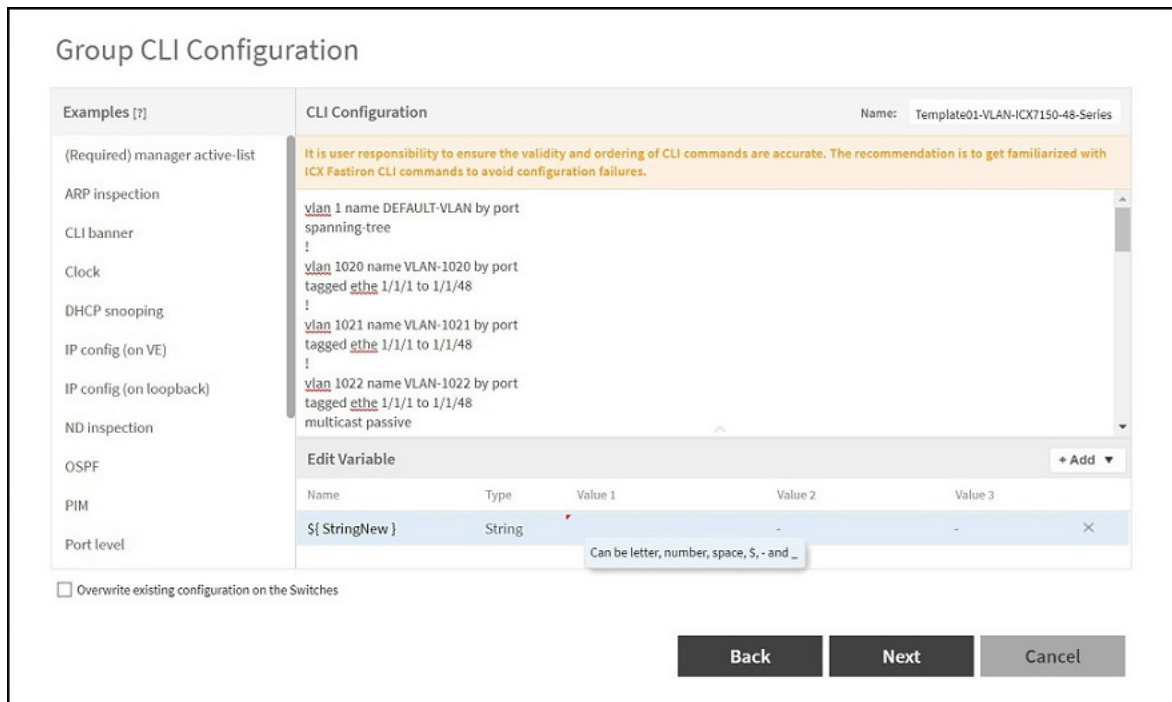


FIGURE 57 Support for dollar sign in variable string

### Group CLI Configuration

Examples [?]

CLI Configuration

Name: Template01-VLAN-ICX7150-48-Series

(Required) manager active-list

ARP inspection

CLI banner

Clock

DHCP snooping

IP config (on VE)

IP config (on loopback)

ND inspection

OSPF

PIM

Port level

It is user responsibility to ensure the validity and ordering of CLI commands are accurate. The recommendation is to get familiarized with ICX Fastiron CLI commands to avoid configuration failures.

```

vlan 1 name DEFAULT-VLAN by port
spanning-tree
!
vlan 1020 name VLAN-1020 by port
tagged ethe 1/1/1 to 1/1/48
!
vlan 1021 name VLAN-1021 by port
tagged ethe 1/1/1 to 1/1/48
!
vlan 1022 name VLAN-1022 by port
tagged ethe 1/1/1 to 1/1/48
multicast passive
                    
```

+ Add ▾

Name	Type	Value 1	Value 2	Value 3	
#{ StringNew }	String	AB 123 - 456 _ \$\$\$	-	-	×

Overwrite existing configuration on the Switches

Back
Next
Cancel

FIGURE 58 Example Template

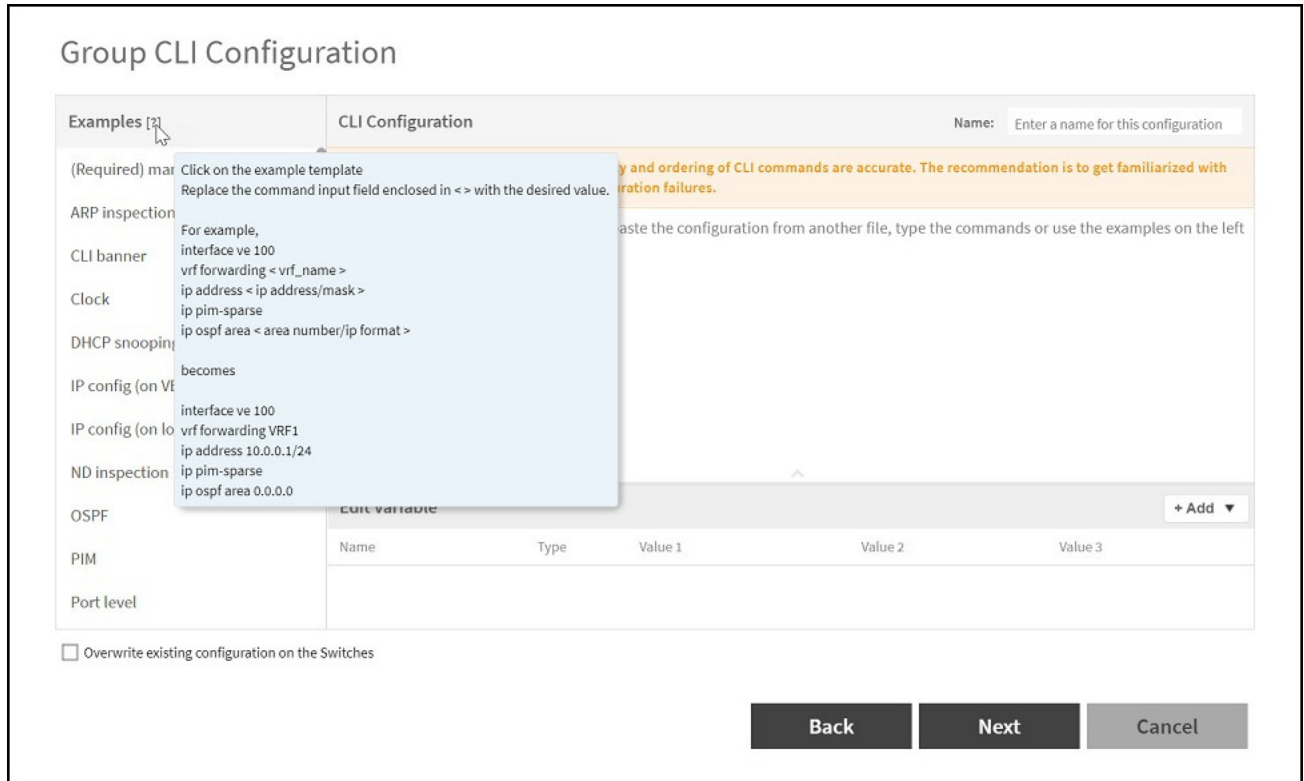


FIGURE 59 Support for IP address in Variable

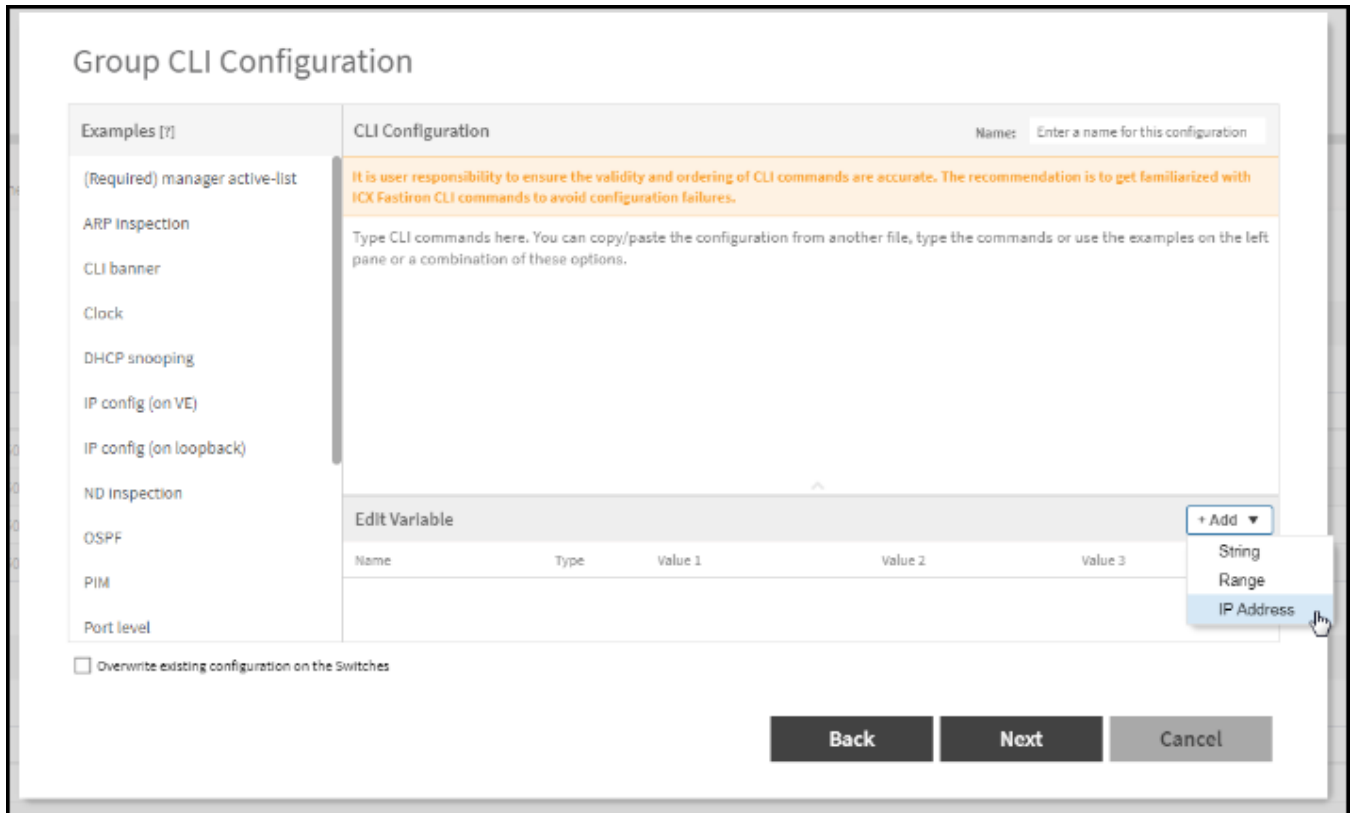


FIGURE 60 Details of fields in IP address in Variable

### Group CLI Configuration

Examples [?]	CLI Configuration												
<ul style="list-style-type: none"> <li>(Required) manager active-list</li> <li>ARP inspection</li> <li>CLI banner</li> <li>Clock</li> <li>DHCP snooping</li> <li>IP config (on VE)</li> <li>IP config (on loopback)</li> <li>ND inspection</li> <li>OSPF</li> <li>PIM</li> <li>Port level</li> </ul>	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px; background-color: #fff9c4;"> <p style="font-size: 0.9em; margin: 0;">It is user responsibility to ensure the validity and ordering of CLI commands are accurate. The recommendation is to get familiarized with ICX Fastiron CLI commands to avoid configuration failures.</p> </div> <p style="font-size: 0.8em; margin: 0;">Type CLI commands here. You can copy/paste the configuration from another file, type the commands or use the examples on the left pane or a combination of these options.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center; border-bottom: 1px solid #ccc;"> <span>Edit Variable</span> <span>+ Add ▼</span> </div> <table border="1" style="width: 100%; border-collapse: collapse; font-size: 0.8em;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="width: 15%;">Name</th> <th style="width: 15%;">Type</th> <th style="width: 20%;">Value 1</th> <th style="width: 20%;">Value 2</th> <th style="width: 20%;">Value 3</th> <th style="width: 10%;"></th> </tr> </thead> <tbody> <tr> <td>\${} </td> <td>IP Address</td> <td>Starting IP Address</td> <td>~ Ending IP Address</td> <td>Netmask</td> <td style="text-align: center;">×</td> </tr> </tbody> </table> </div>	Name	Type	Value 1	Value 2	Value 3		\${}	IP Address	Starting IP Address	~ Ending IP Address	Netmask	×
Name	Type	Value 1	Value 2	Value 3									
\${}	IP Address	Starting IP Address	~ Ending IP Address	Netmask	×								

Overwrite existing configuration on the Switches

Back
Next
Cancel

FIGURE 61 Example for IP address in variable

The screenshot shows the 'Group CLI Configuration' interface. On the left is a sidebar with categories like 'Examples [?]', 'ARP inspection', 'CLI banner', etc. The main area is titled 'CLI Configuration' and shows a configuration snippet: 'interface ethernet 1/1/1' followed by 'ip address \${IP1}'. Below this is an 'Edit Variable' table with columns for Name, Type, Value 1, Value 2, and Value 3. The table contains one entry for the variable \${IP1} with Type 'IP Address', Value 1 '10.0.0.101', Value 2 '~ 10.0.1.254', and Value 3 '255.255.254.0'. At the bottom, there is a checkbox for 'Overwrite existing configuration on the Switches' and three buttons: 'Back', 'Next', and 'Cancel'.

- Variables assist in applying unique configuration to the switches. For example, IP address can be defined as a variable so that each switch gets assigned a unique IP address. In the **Edit Variable** field, enter the **Name**, **Type**, **Value 1**, **Value 2** and **Value 3** of the variables, where **Value 1** denotes the “Starting IP Address”, **Value 2** denotes the “Ending IP Address”, and **Value 3** is the “Netmask”.

**NOTE**

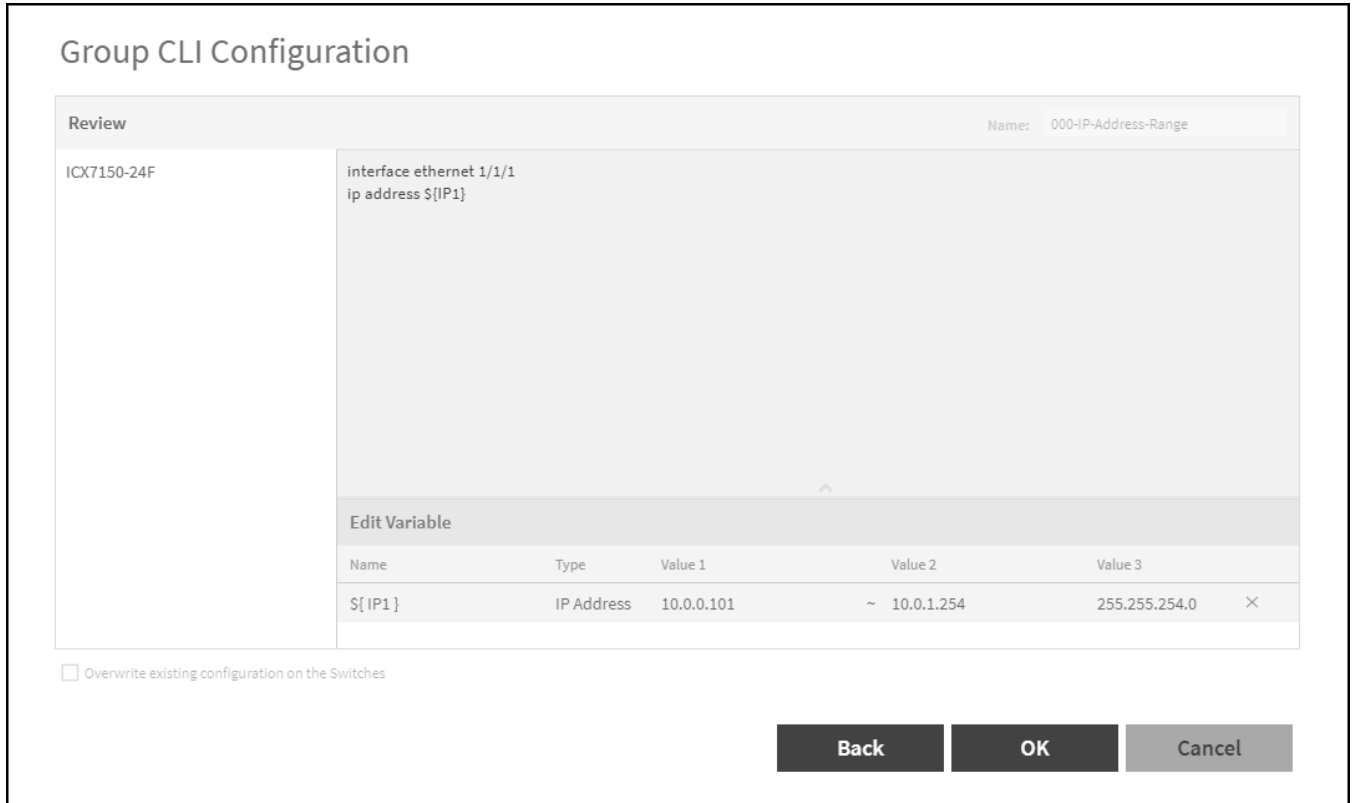
The **Edit Variable** field is optional.

By default, the **Overwrite existing configuration on the Switches** option is not selected and only the factory-default switches (no start-up config) will inherit the group level configuration. If this option is selected, the controller will replace the existing configuration of the switch with the configuration defined for the group.



- After reviewing the Group CLI Configuration, click **OK**.

**FIGURE 62** Reviewing the Group CLI Configuration



- A confirmation dialog box is displayed, click **OK**.

10. The switch group is now Group CLI Configuration enabled and is available for provisioning.

FIGURE 63 Provisioning the Group CLI Configuration Setup

The screenshot displays the SmartZone Switch Management interface. The top navigation bar includes 'Monitor', 'Network', 'Security', 'Services', and 'Administration'. A search menu is located on the right. The main content area is divided into two sections: a log table and a configuration details panel.

**Provisioning Log Table:**

Date & Time	Node	Type	Model Family	Status	Message
2021-02-04 15:53:00	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )
2021-02-04 15:52:59	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )
2021-02-04 15:52:59	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )
2021-02-04 15:52:58	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )
2021-02-04 15:52:57	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )
2021-02-04 15:52:52	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )
2021-02-04 15:52:49	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )
2021-02-04 15:52:47	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )
2021-02-04 15:52:47	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )
2021-02-04 15:52:43	vsZ-H-83	CLI_PROVISIONING	ICX7150	SUCCESS	Success ( 1 ) / Failed ( 0 ) / Applied ( 0 ) / Failed No Response ( 0 ) / Failed Save to Flash ( 0 )

**Configuration Details Panel:**

Switch Name: N/A  
Serial Number: PC071-71005  
Start Time: 2021-02-04 15:52:57  
End Time: 2021-02-04 15:53:57  
Status: SUCCESS

Configuration commands shown on the right:

```

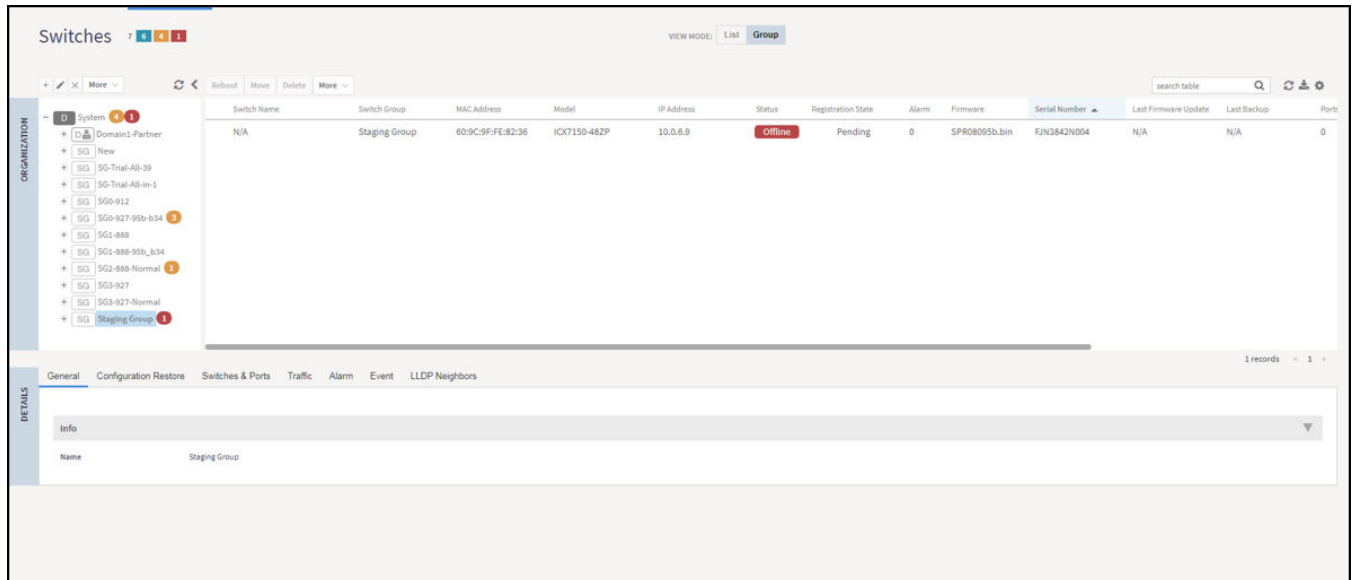
1 interface ethernet 1/1/1
2 ip address 10.0.0.110 255.255.254.0
    
```

1 records < 1 >

11. After the configuration is setup, any factory default switch joining the group will have the configuration applied and will be rebooted for the changes to take effect.

- In the **Organization** tab, select a **Domain** or **Switch Group** and select the **Switches**.

**FIGURE 64** Discovering a New switch



## CLI Templates

CLI templates enable users to make incremental configuration changes on the fly to the selected switches. CLI templates are not tied to any switch or switch group. Once defined, they can be applied to any selected switch(es) or Switch Groups.

### NOTE

Only an administrator with Full Access permission can update CLI configurations. The validity of CLI commands and their ordering rests solely with the administrator.

### Using CLI templates

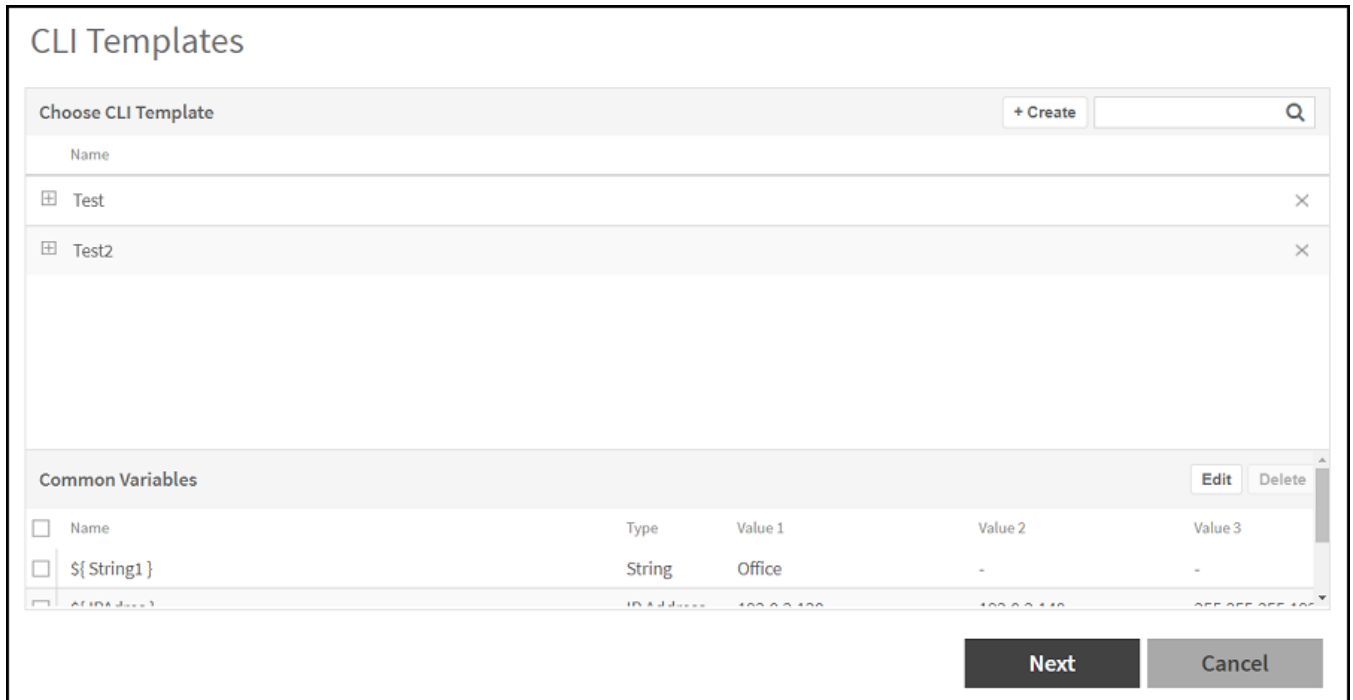
- On the menu, click **Network > Wired > Switches** to display the **Switches** window.
- In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

3. Click **CLI template** icon to display the **CLI Templates** dialog box. You can select an existing CLI template with an existing common variables or create a new CLI template with a new common variables.

**NOTE**

To edit existing common variables or add common variables. Click **Edit** icon, modify the common variables or add common variables and then click **Save**. For more information, see *Step 4 b Edit Variable*.

**FIGURE 65** CLI Template



4. Complete the following steps to create a new CLI template.

- a) Click  icon to display the **CLI Templates** dialog box.



**FIGURE 66** CLI Templates Dialog Box

b) Complete the following fields:

- **Name:** Enter the name of the CLI template.
- **Command Lines:** Insert or edit the command lines in the space provided. Users can choose the CLI commands under the 'Examples' pane to build configuration. Alternatively, CLI commands can be typed directly or copied from a notepad and pasted into the 'CLI Configuration' box.

**NOTE**

It is recommended that users get familiarized with FastIron commands and their ordering to avoid any issues with applying the configuration.

- **Edit Variable:** Click  icon and select the **String** or **Range** or **IP Address** variable to add the **String** or **Range** or **IP Address** variable to the table. Variables helps to apply unique configuration to the switches. For example, IP address can be defined as a variable so that each switch gets assigned a unique IP address. In the **Edit Variable** field, enter the **Name**, **Type**, **Value 1**, **Value 2**, and **Value 3** for IP address variables, where Value1 denotes the “Starting IP Address”, Value 2 denotes the “Ending IP Address”, and Value 3 is the “Netmask”. Click  icon to add a new variables setting to the Common Variables.

**NOTE**

The **Edit Variable** field is optional.

FIGURE 67 Adding Common Variables

**CLI Templates**

Examples [?]

(Required) manager active-list

ARP inspection

CLI banner

Clock

DHCP snooping

**IP config (on VE)**

IP config (on loopback)

ND inspection

OSPF

PIM

**CLI Configuration** Name: Test2

It is user responsibility to ensure the validity and ordering of CLI commands are accurate. The recommendation is to get familiarized with ICX Fastiron CLI commands to avoid configuration failures.

```
interface ve 100
vrf forwarding <vrf_name>
ip address <ip address/mask>
ip pim-sparse
ip ospf area <area number/ip format>
```

**Edit Variable** + Add ▼

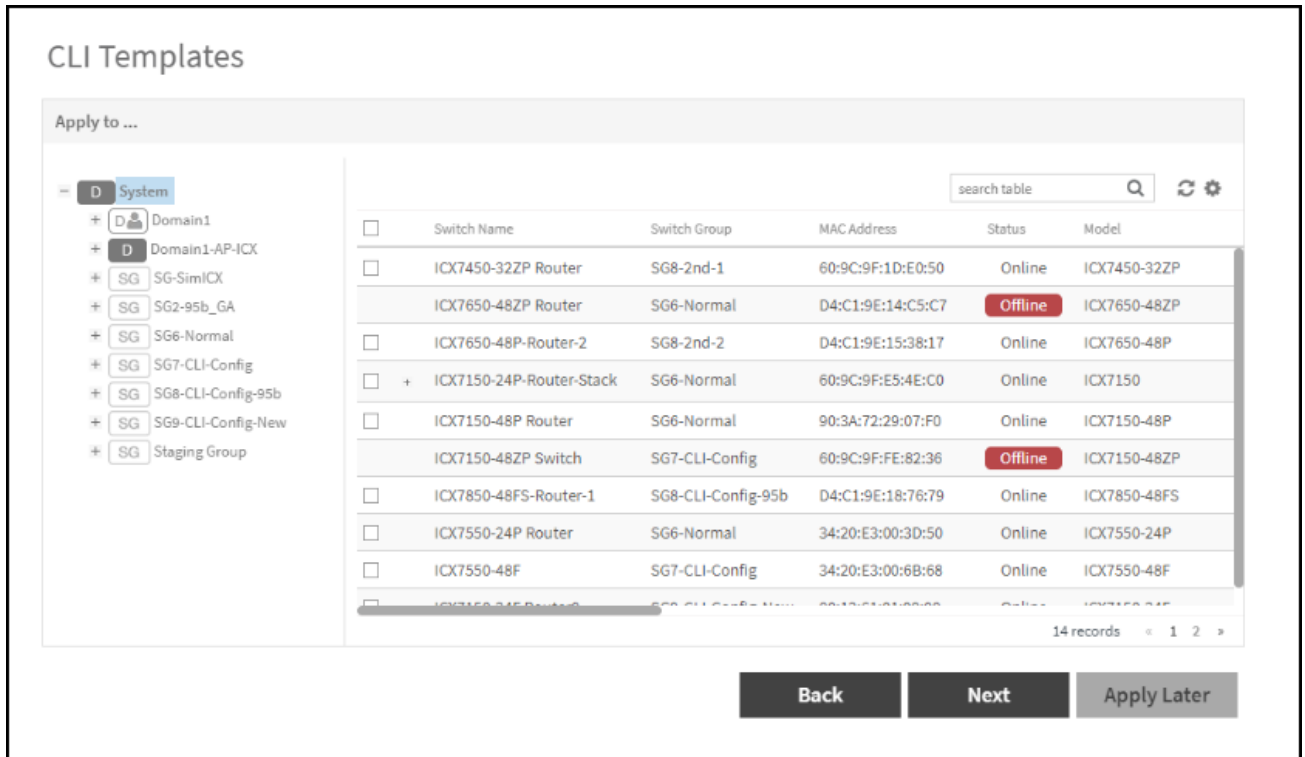
Name	Type	Value 1	Value 2	Value 3	
#{ IPAdres }	IP Address	192.0.2.130	~ 192.0.2.140	255.255.255.192	★ ×
#{ R1 }	Range	1	: 10	-	×
#{ String1 }	String	Office	-	-	×

Reboot the Switches after applying config

Back Save & Next Cancel

- c) Select **Reboot Switches after applying config** check box if you want the switch to reload after the configuration update. If you do not select this option, the switch will not reload after the configuration update.
- d) Click **Save & Next**.
- e) Select the target switches check box and click **Next** to display the **Review** dialog box.

FIGURE 68 Selecting Switches

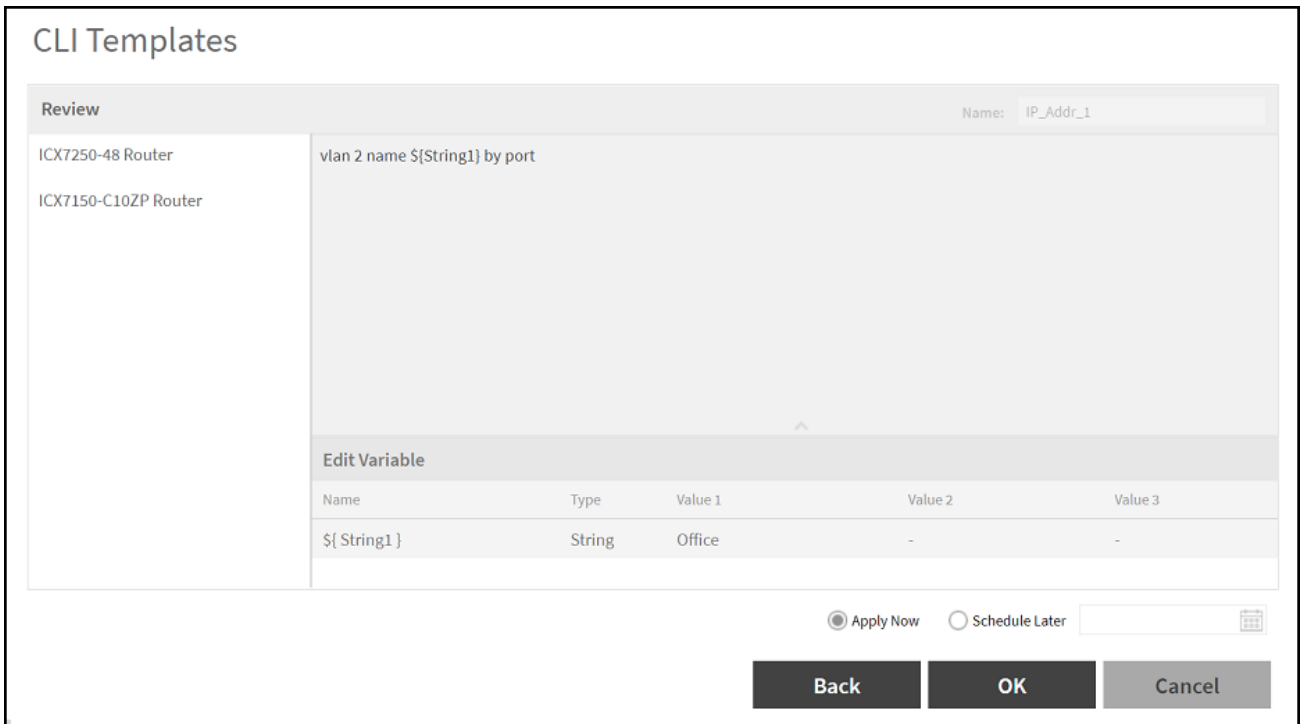


**NOTE**

Configuration will be applied only to the switches that are online. Users need to re-apply configuration for switches that are offline at a later time when they come back online.

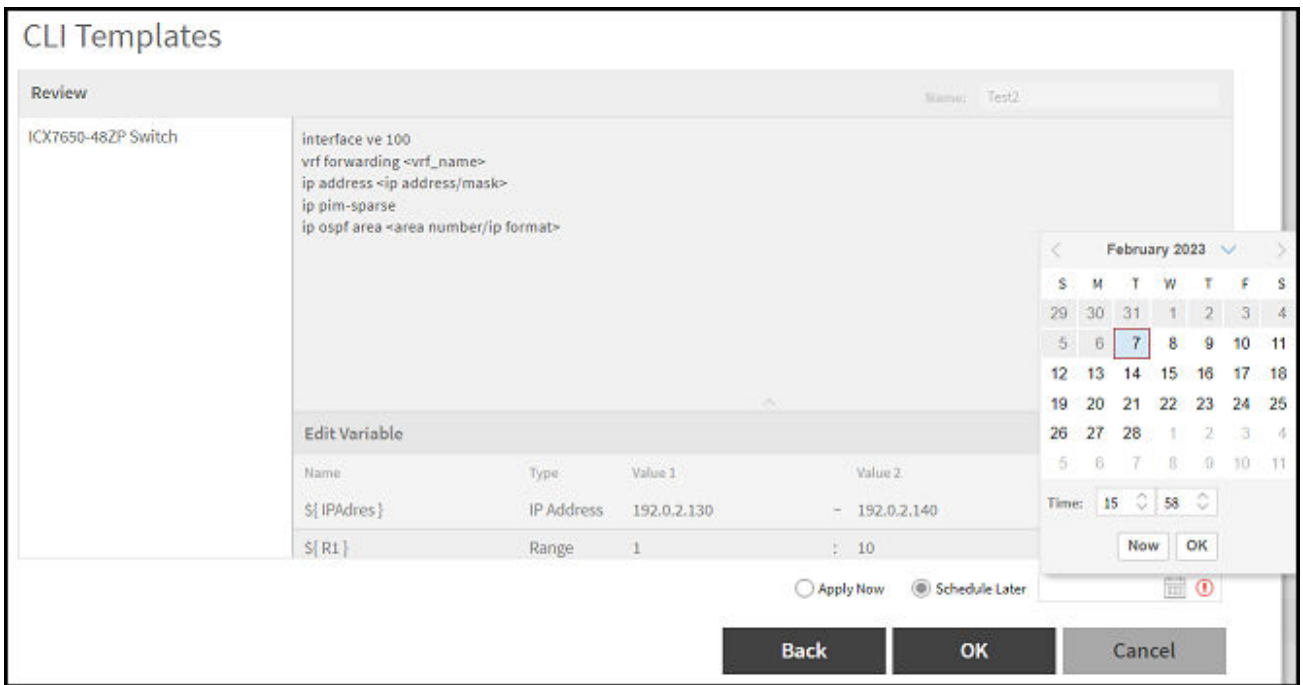
- f) Review the CLI template.

FIGURE 69 Reviewing the CLI Template



- g) Select **Apply now** or **Schedule Later** to save the created template and apply to the selected switches. If you select the **Schedule Later** then select the **Date** and **Time** to apply the configuration.

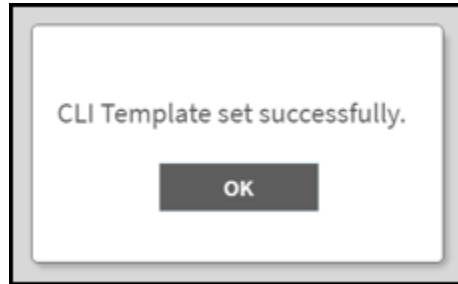
**FIGURE 70** Schedule Later Dialog Box





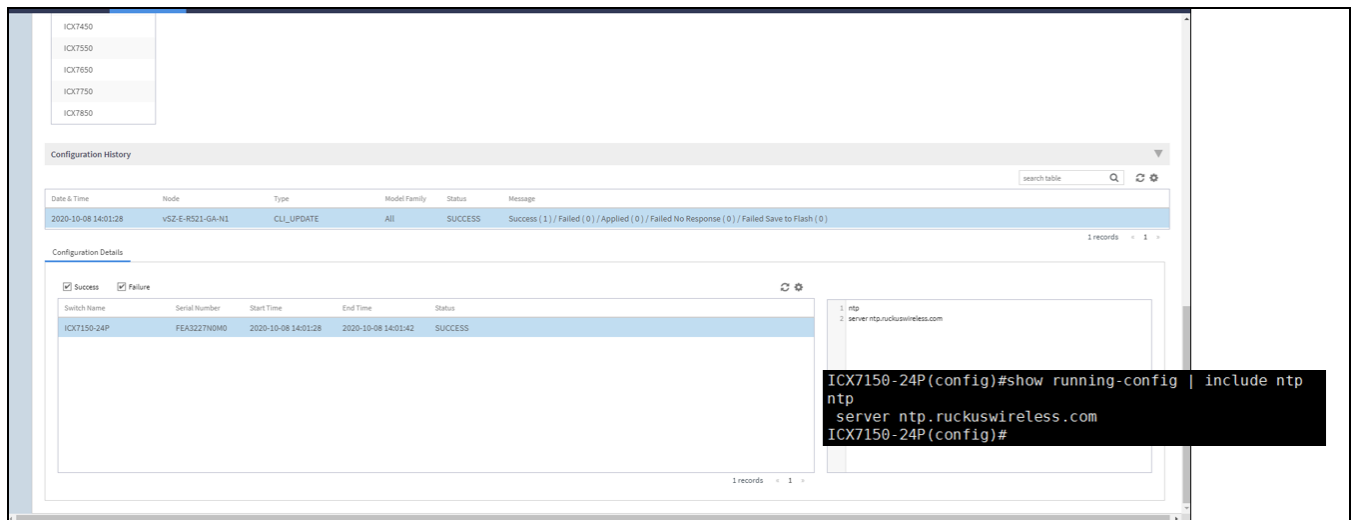
- h) Click **OK** to display the **CLI Template Set Successfully** message.

**FIGURE 71** Applying the CLI Template



- i) Click **OK**.
- In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.
  - In the **Configuration History** tab, select the **Switch** to display the **Configuration Details** tab. Make sure that the CLI template is successfully added to the switch.

**FIGURE 72** Updating the Command Lines to Switch



The following status messages are displayed on the **Status** tab.

- **Success** if the configuration is applied successfully.
- **Failed** if there is a failure in configuring a switch.
- **Applied** if the configuration is partially successful with one or more informational messages or warnings returned by the switch.

## Creating Config Backup for Switch Group

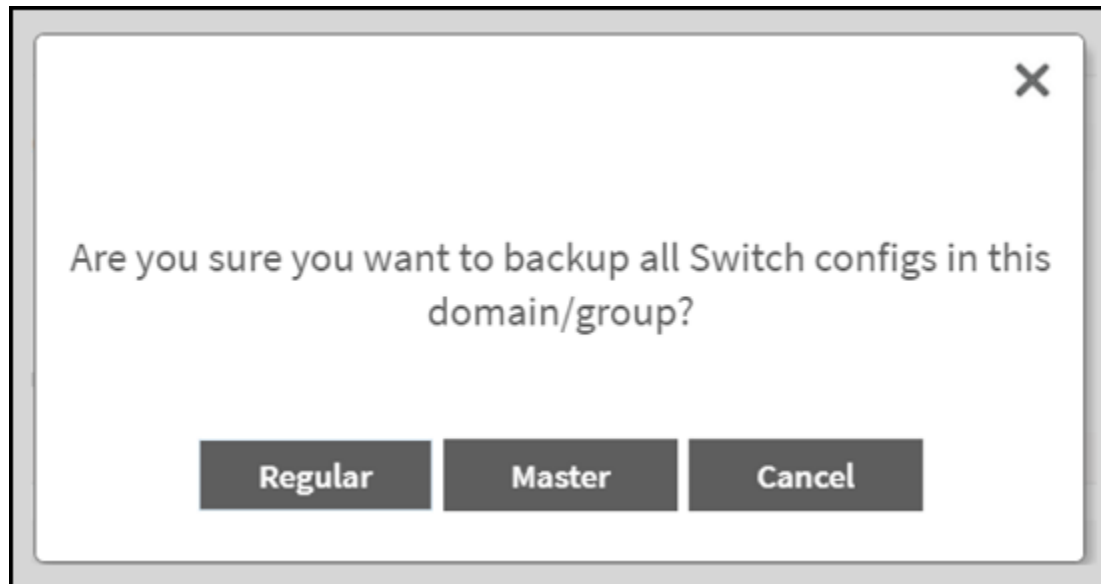
The Master configuration backup allows you to initiate a backup of a switch group or domain.

- On the menu, click **Network > Wired > Switches** to display the **Switches** window.
- From the system tree, select the **Domain > Switch Group** or **Switch Group**.

3. Click **More > Config Backup**.

A dialog box is displayed asking the type of backup to be performed such as **Regular** or **Master**.

**FIGURE 73** Backing up Switch group or Domain



4. Click **Master** to create master backup for switch groups.

The **Switch config backup operation is triggered successfully** dialog box is displayed ensuring the backup operation is completed.

5. Click **OK**.

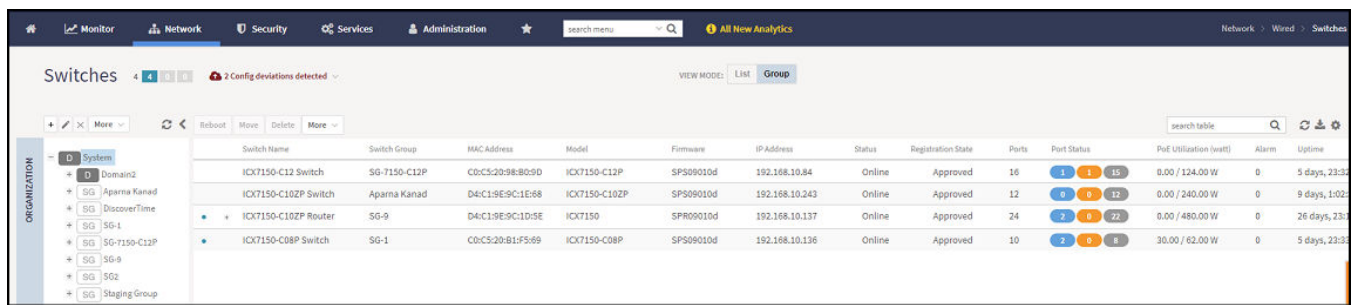
## Viewing Configuration Alerts

If you select a config backup as a master config backup, then you will receive an alert if there are any changes in the later backups containing different content. For more information on config backup settings, refer the topics [Backing up and Restoring Switch Configuration](#) on page 32 and [Creating Config Backup for Switch Group](#) on page 89.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.

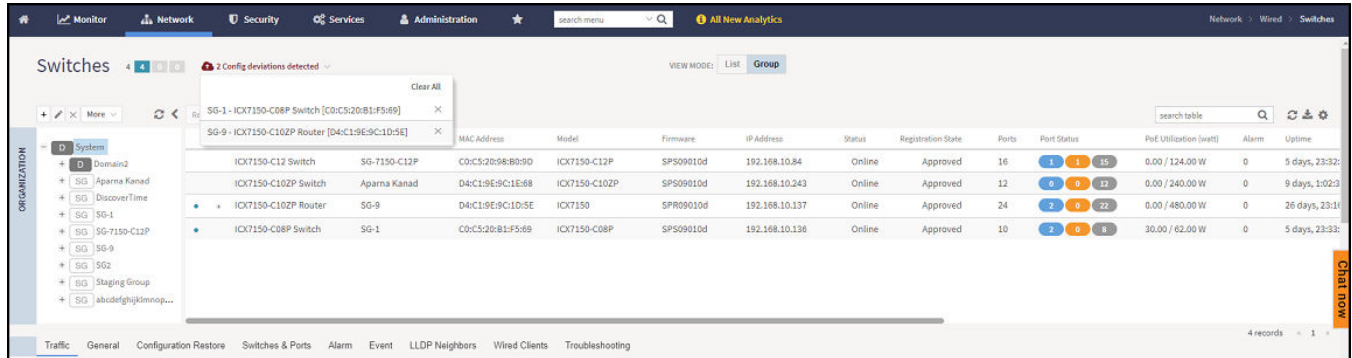
The alert is displayed at the top of the switch page.



**FIGURE 74** Master Backup Alert





- You can select switch or switch groups from the alert list to view the last updated backup configurations.

FIGURE 75 Expanding the drop-down list of Alert



- You can click  to clear all of the alerts from the list, or you can individually remove each switch by clicking .

**NOTE**

The  icon in the switch table announces that the backup in the switch configuration is changed. The  icon and the alert are cleared automatically when the latest config is same as master backup config.

## Port Settings

Port level configuration can be viewed and edited from the **Switch Port** page. You can select ports belonging to a single switch or from different switches within a switch group. The search box can be used to filter ports based on port numbers, names, or VLANs. Once the desired list of ports are filtered, you can select the ports and make changes to their existing settings by performing the procedure [Creating Switch Level Configuration](#) on page 63.

### Creating and Managing Port Templates

The controller allows you to configure switch port settings. However, there are many advanced port settings that are not supported by the controller. You must configure these advanced port settings on the switch console.

The controller introduced with a port template facilitates the deployment of advanced port settings.

You can apply a port template to joined (or online) switch ports for which the firmware version is FastIron 08.0.95b or later. If the switch port is newly added, you must apply the port template again.

**NOTE**

You cannot apply a port template to ports that belong to offline switches.

**NOTE**

Apply the new untag VLAN to selected ports. Make sure to untag the default VLAN from these ports before applying the Port Template.

### Creating a Port Template and Assigning Target Ports

Complete the following steps to create a port template and assign ports to the template.





- On the menu, click **Network > Wired > Switches** to display the **Switches** window.

## Working with Switches

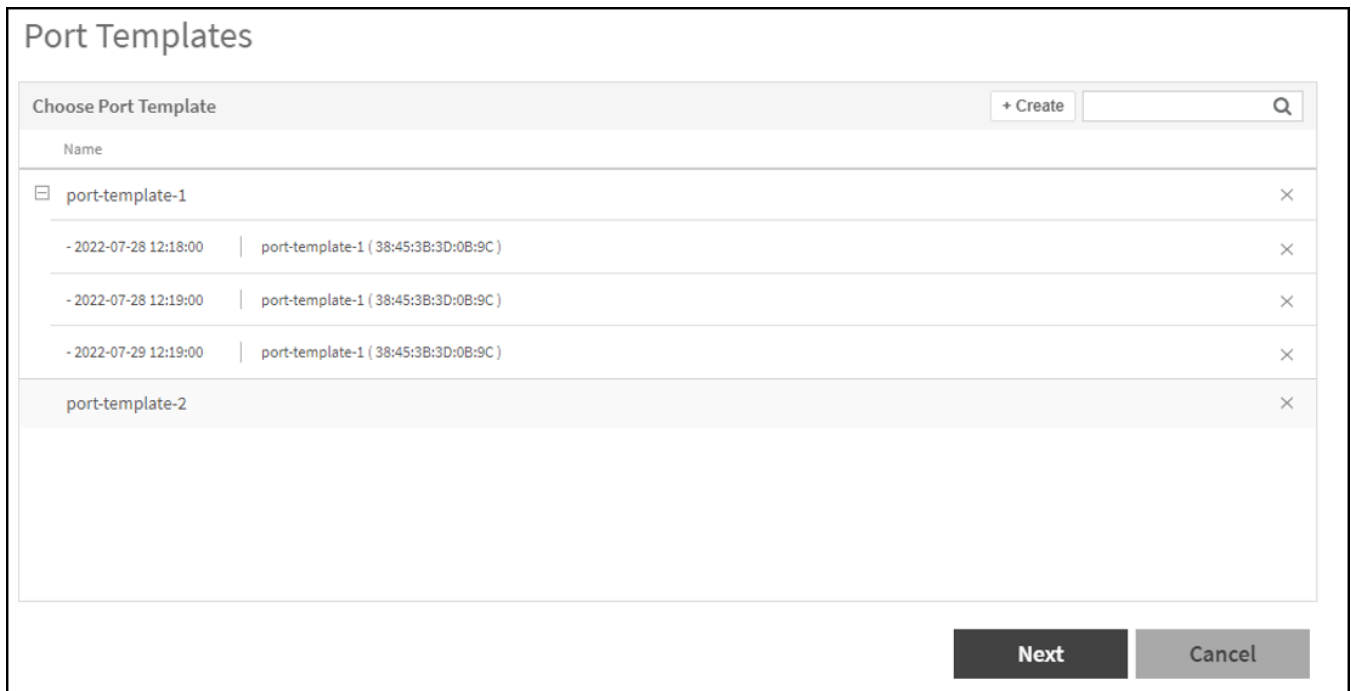
### SmartZone Switch Management

2. Either select a switch group and click the **Switches & Ports** tab, or select a switch and click the **Ports** tab.
3. In the **Port Details** tab, click **Port Templates** to display the **Port Templates** dialog box.

4. In the **Port Templates** following actions are available to create new and manage existing port templates:

- Expand the list of existing port templates. Click "+".
- Create a new port template. Click .
- Delete an existing port template. Click .
- Close the dialog box without applying any changes. Click .
- Update the selected port template. Click .

**FIGURE 76** Port Templates Dialog Box Showing all the Actions



**FIGURE 77** Creating a Port Template

Port Templates

Examples [?]

CLI Configuration

Name: Demd

It is user responsibility to ensure the validity and ordering of CLI commands are accurate. The recommendation is to get familiarized with ICX FastIron CLI commands to avoid configuration failures.

protected-port

Tagged VLANs: Untagged VLAN

Edit Variable + Add ▼

Name	Type	Value 1	Value 2	Value 3
------	------	---------	---------	---------

Back Save & Next Cancel

5. To create a port template, complete the following steps:

- a) In the **Name** field, enter the name of the port template.
- b) Enter VLAN IDs in the **Tagged VLANs** field, separating multiple IDs with commas and no spaces. When you apply the port template to selected ports, the controller will automatically add the needed VLAN CLI commands to the template.

**NOTE**

If the **Tagged VLANs** field is empty, the controller will not add any tagged VLAN CLI commands.

- c) Enter a VLAN ID in the **Untagged VLAN** field. When the port template is applied to the selected ports, the controller will automatically add the necessary VLAN CLI commands to the template.

**NOTE**

If the **Untagged VLANs** field is empty, the controller will not add any untagged VLAN CLI commands.

- d) In the **Edit Variable** field, enter the **Name**, **Type**, **Value 1**, **Value 2**, and **Value 3** for IP address variables. Value1 denotes the “Starting IP Address”, Value 2 denotes the “Ending IP Address”, and Value 3 denotes the “Netmask”. Variables help to apply unique configurations to the switches. If you want to use a variable in the **CLI Configuration** editor, it must begin with a dollar sign (\$) and use a pair of curly braces, for example, \${VARIABLE\_NAME}. An IP address can be defined as a variable so that each switch gets assigned a unique IP address.
- e) In the **CLI Configuration** field, enter command types for the template, including variables.

6. After creating, click **Save & Next** to save the port template. You can click **Back** to view the previous step, or click **Cancel** to close the page.

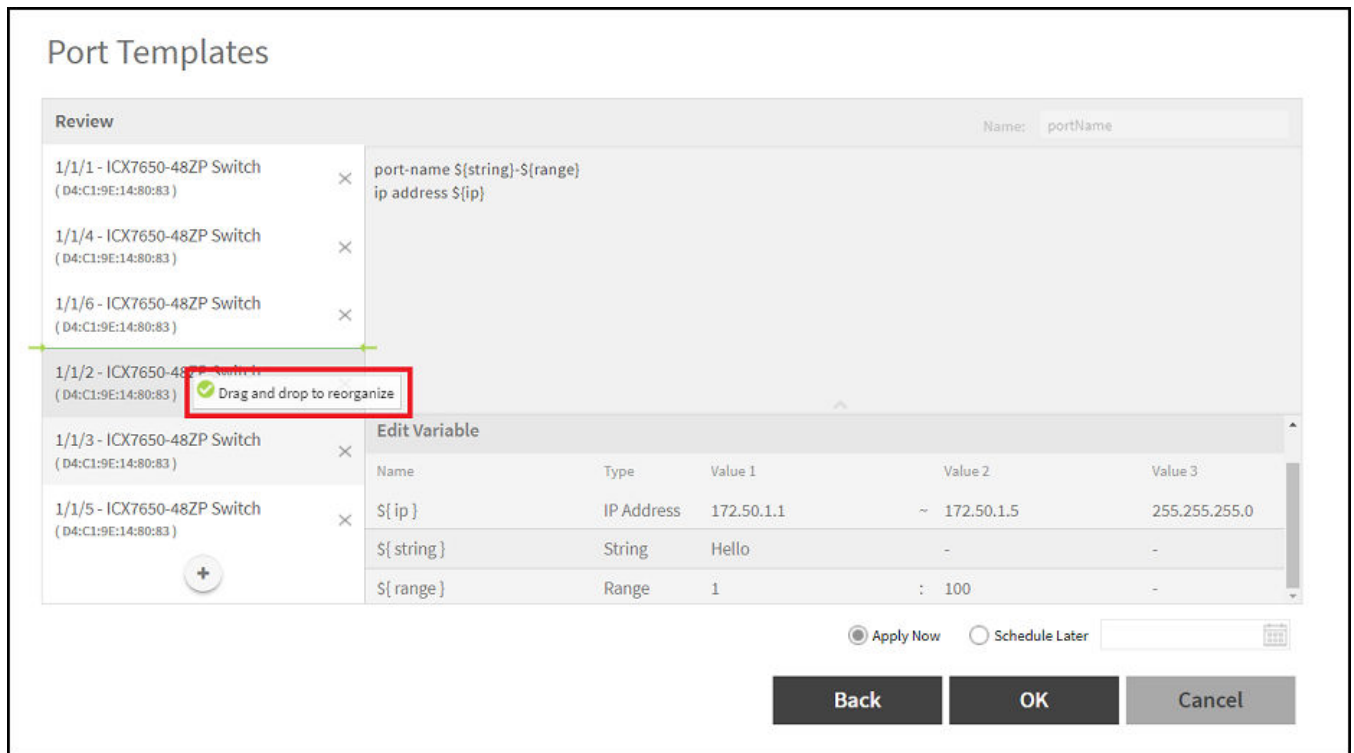
- Click "+" on the left pane of the **Review** page to add more ports to the list. Select **Apply Now** to apply the port template. Select **Schedule Later** to apply the port template at the date and time specified by clicking the calendar icon. After selecting either **Apply Now** or **Schedule Later**, click **OK**.

**NOTE**

Before the SZ 7.0 release, as a preliminary step, you must select a port and then apply the port template. With the 7.0 release, you can apply a port template without initially selecting a port.

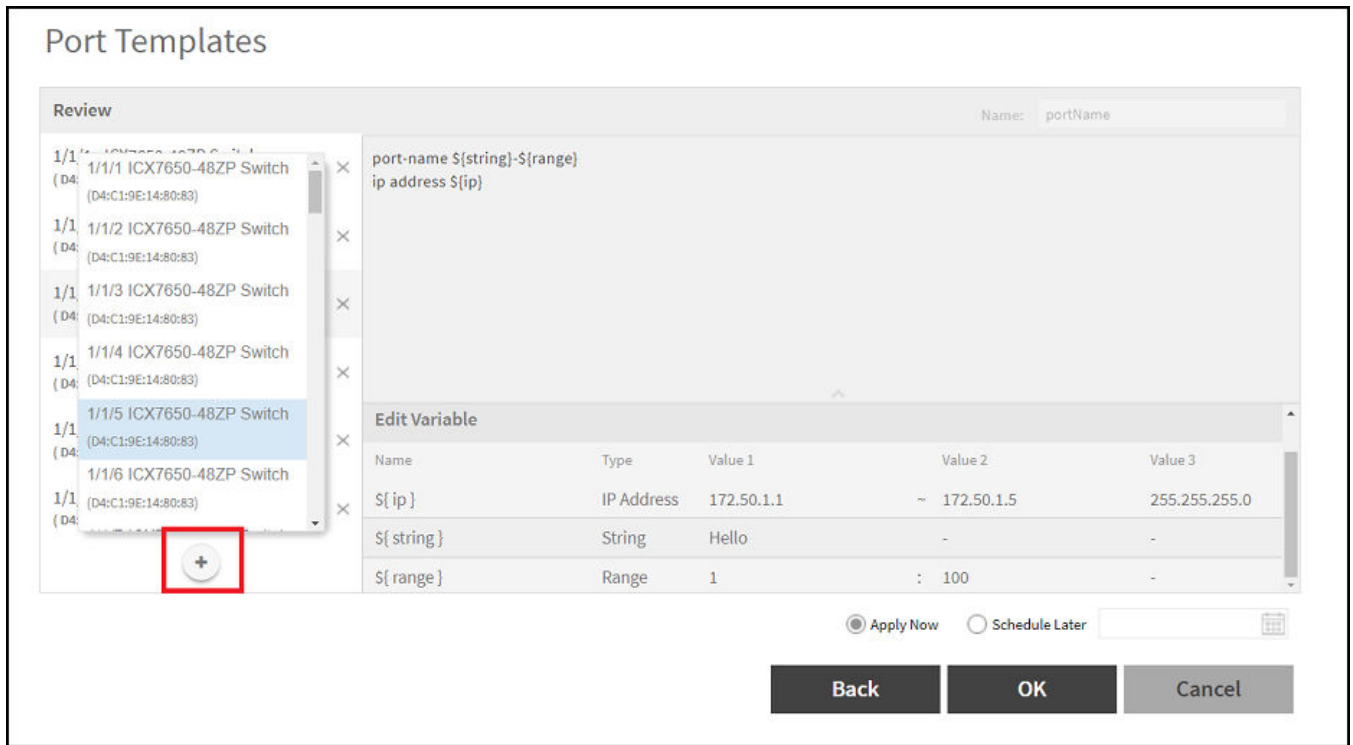
You can also organize the port list by selecting a port and dragging it above or below.

**FIGURE 78** Organizing the Port List



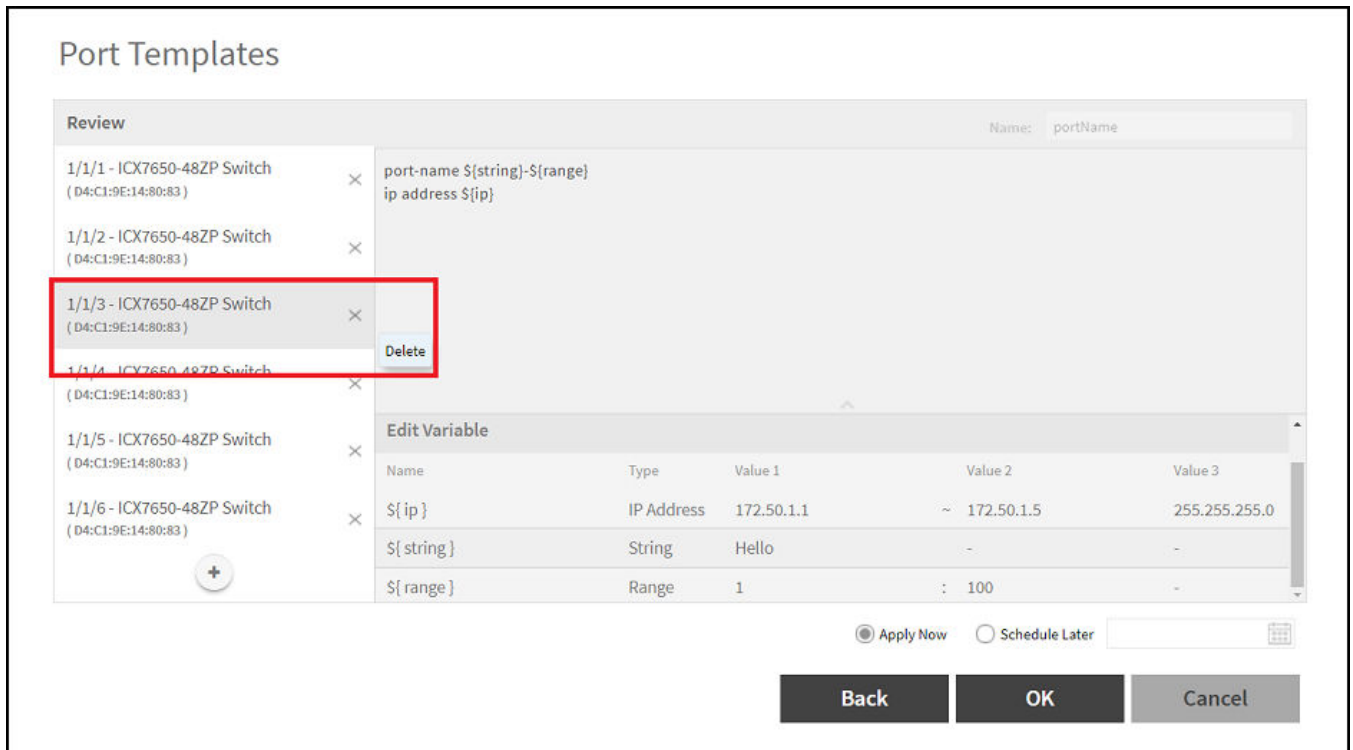
You can also add port to the list.

**FIGURE 79** Adding Ports to the List



You can also delete a port from the list.

**FIGURE 80** Deleting Port from the List





- After applying the port template to the selected ports, a dialog box with the message **Port Template applied successfully** is displayed, click **OK**.

### Configuring Port Settings for a Switch

Port settings enable you to configure ports for a switch, stack, or switch group. You can also invoke the ACL in port configuration for applying the Quality of Service (QoS) settings to prioritize VOIP and VIDEO VLAN traffic.

#### NOTE

Port settings for QoS can only be configured for switches that are executing firmware version 08.0.95 and above.

- On the menu, click **Network > Wired > Switches** to display the **Switches** window.
- In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and in the **Details** tab, click the **Switches and Ports** tab.

FIGURE 81 Switch Port Page

The screenshot shows the SmartZone Switch Management interface. On the left, there is a navigation tree with a 'System' icon and several 'SG' (Switch Group) and 'D' (Domain) items. The main area displays a table of switches:

Switch Name	Switch Group	MAC Address	Model	IP Address
ICX7150-48P Router	7150	90:3A:72:29:07:F0	ICX7150-48P	10.0.6.10

Below the table, there are tabs for 'Traffic', 'General', 'Configuration', 'Configuration Restore', 'Switches & Ports', 'Routing', 'Alarm', 'Event', 'LLDP Neighbors', 'Wired Clients', and 'Troubleshooting'. The 'Switches & Ports' tab is active, showing 'Top Switches' and 'Port Details' sections. The 'Port Details' section has a 'Configure' button and a table of port settings:

Port Name	Port Number	Switch Name	Switch Group	Status	Admin Status	Speed
GigabitEthernet1/1/1	1/1/1	ICX7150-48P R...	7150	Down	Up	link down or no traffic
GigabitEthernet1/1/2	1/1/2	ICX7150-48P R...	7150	Down	Up	link down or no traffic
GigabitEthernet1/1/3	1/1/3	ICX7150-48P R...	7150	Down	Up	link down or no traffic
GigabitEthernet1/1/4	1/1/4	ICX7150-48P R...	7150	Down	Up	link down or no traffic
GigabitEthernet1/1/5	1/1/5	ICX7150-48P R...	7150	Down	Up	link down or no traffic
GigabitEthernet1/1/6	1/1/6	ICX7150-48P R...	7150	Down	Up	link down or no traffic
GigabitEthernet1/1/7	1/1/7	ICX7150-48P R...	7150	Down	Up	link down or no traffic
GigabitEthernet1/1/8	1/1/8	ICX7150-48P R...	7150	Down	Up	link down or no traffic

3. In the **Port Details** tab, select the port that must be updated and click **Configure** to display the **Port Settings** window.

**FIGURE 82** Port Settings Showing Single Update

The screenshot displays the 'Port Settings' window for a single port (1/1/1). The interface includes the following elements:

- Selected Port(s):** 1/1/1
- Port Name:** An empty text input field.
- Port Enabled:** A toggle switch set to 'ON'.
- Port Protected:** A toggle switch set to 'ON'.
- Port VLANs:** A section with two tabs: 'Customize' (active) and 'Use Group Settings'.
  - Tagged VLANs:** A text input field containing '77,15,5,27,28,70,83'.
  - Untagged VLAN:** A text input field containing '1'.
- POE Enable:** A toggle switch set to 'ON'.
- POE Priority:** A text input field containing '3'.
- POE Class:** A dropdown menu showing '0'.
- POE Budget:** An empty text input field.
- Ingress ACL:** A dropdown menu showing 'Please select data' with '+' and edit icons.
- Egress ACL:** A dropdown menu showing 'Please select data' with '+' and edit icons.
- Port Speed:** A dropdown menu showing 'AUTO'.
- Storm Control:** A section with a 'Broadcast Limit' field and radio buttons for 'kbps' and 'Pkts/sec'.

At the bottom right, there are two buttons: 'OK' and 'Cancel'.

FIGURE 83 Port Settings Showing Multiple Update

**Port Settings**

Ingress ACL: Please select data [v] [+] [pencil]

Egress ACL: Please select data [v] [+] [pencil]

Port Speed: Please select data [v]

**Storm Control**

Broadcast Limit: [input] kbps Pkts/sec

Multicast Limit: [input] kbps Pkts/sec

Unknown-Unicast Limit: [input] kbps Pkts/sec

**Flexible Authentication**

[?] Enable:  OFF

RSTP Admin Edge Port:  ON

STP BPDU Guard:  ON

STP Root Guard:  ON

DHCP Snooping Trust Port:  ON

IPSG:  OFF

LLDP:  ON

FIGURE 84 Port Settings for QoS

Voice VLAN:

LLDP QoS:

Application Type	QoS VLAN Type	VLAN ID	Priority	DSCP
GUEST_VOICE	TAGGED	2	0	0

4. Complete the following fields:

- **Port Name:** Enter the port name.
- **Port Enabled:** Click to enable the port.
- **Port Protected:** Click to enable the protected port.

**NOTE**

Port Protected field is displayed only for the switches using SmartZone 5.2.1 and above.

- **Port VLANs:** If you configure VLAN on both group model configuration and port settings, port level changes takes precedence.
- **Customize:** Click customize to identify the ports that need to stay customized.
- **Use Group Settings:** Click user group settings to rebind the identified ports back to the group level.
- **Tagged VLANs:** Enter the tagged VLAN ID or VLAN ID range.
- **Untagged VLAN:** Enter an untagged VLAN ID.
- **POE Enable:** Click to enable PoE.
- **POE Class:** Select the PoE class. You can configure the PoE budget on ports by setting the PoE class to 0 through 4.
- **POE Priority:** Enter the PoE priority.
- **POE Budget:** Allows users to manually set the PoE power limit.
- **Ingress ACL:** Select the ingress ACL from the list.
- **Egress ACL:** Select the egress ACL from the list.
- **Port Speed:** Select the required Port Speed from the list.
- **Storm Control:** If you set Storm Control configuration on a switch, and if this switch joins the controller, you must ensure that the Storm Control configuration on the controller is also set. The Storm Control includes the following fields - Broadcast, Multicast, and Unicast.

**NOTE**

The value 0 pkts/sec and 0 kbps indicates storm control is disabled.

- **Broadcast Limit:** Enter the Broadcast Limit value in this field. The maximum value in **Pkts/sec** is 8388607 and the minimum value is 1; when the port speed is set to **Auto** or **Optic**, the maximum value in **kbps** is 1000000 and the minimum value is 1; when the port speed is other than auto or optic the minimum value in **kbps** is 1 and the maximum value is equivalent to the selected port speed .
- **Multicast Limit:** Enter the Multicast Limit value in this field. The maximum value in **Pkts/sec** is 8388607 and the minimum value is 1; when the port speed is set to **Auto** or **Optic**, the maximum value in **kbps** is 1000000 and the minimum value is 1; when the port speed is other than auto or optic the minimum value in **kbps** is 1 and the maximum value is equivalent to the selected port speed .
- **Unicast Limit:** Enter the Unicast Limit value in this field. The maximum value in **Pkts/sec** is 8388607 and the minimum value is 1; when the port speed is set to **Auto** or **Optic**, the maximum value in **kbps** is 1000000 and the minimum value is 1; when the port speed is other than auto or optic the minimum value in **kbps** is 1 and the maximum value is equivalent to the selected port speed .
- **RSTP Admin Edge Port:** Click to enable the RSTP Admin Edge Port.
- **STP BPDU Guard:** Click to enable the STP BPDU Guard.
- **STP Root Guard:** Click to enable the STP Root Guard.
- **DHCP Snooping Trust Port:** Click to enable the DHCP Snooping Trust Port.
- **IPSG:** Click to enable IPSG.
- **ILLDP:** Click to enable ILLDP.
- **Voice VLAN:** Select the VLAN (tagged or untagged).
- **LLDP QoS:** Click to enable LLDP-MED settings.

- **Application type:** Enter one of the application types : **Guest\_Voice**, **Guest\_Voice\_Signaling**, **Softphone\_Voice**, **Streaming\_Video**, **Video\_Conferencing**, **Video\_Signaling**, **Voice**, and **Voice\_Signaling**.
  - **VLAN type:** The VLAN type can be priority-tagged, tagged, or untagged.
  - **VLAN ID:** Enter the **VLAN ID** of the VLAN type.
  - **Priority:** Enter the priority for the QoS setting.
  - **DSCP:** Enter the DSCP value for the LLDP setting.
5. Click **OK**.



**VIDEO**

**PoE per port settings.** The below video displays the tasks to be performed to configure PoE on a port.

[Click to play video in full screen mode.](#)

### Editing Ports Across Multiple Switches

Before the 5.2.1 release, you could edit ports for one switch at a time. After the 5.2.1 release, you can edit ports for multiple switches in the same switch group.

For instance, if you need to disable ports 1/1/11 and 1/1/12 on multiple switches, the controller lets you filter the ports list by typing your search criteria.

The search criteria is based on the following:

- Switch Name
- Port Numbers - comma separated values (1/1/1,1/1/11,1/1/24), (or) Range of ports (1/1/1 to 1/1/20)
- VLAN Membership
- PoE Detected Ports
- Port Status
- Admin Status

Complete the following steps to edit ports across multiple switches.


1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. From the system tree, select a **Domain > Switch Group** or **Switch Group**.

- In the **Details** pane, click the **Switches and Ports** tab.

**FIGURE 85** Viewing the Switches and Ports Page

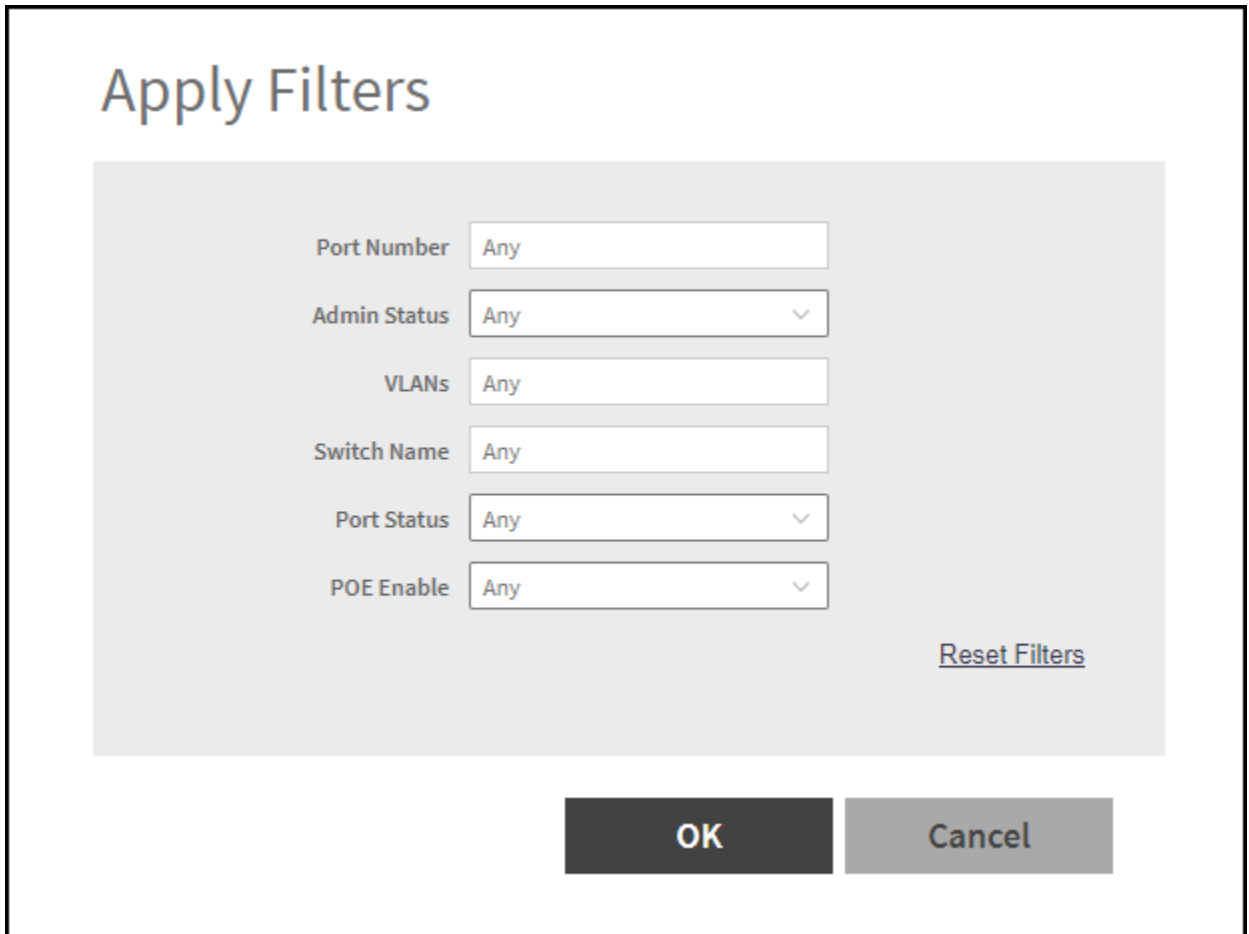
The screenshot displays the 'Switches & Ports' management page. At the top, a navigation bar contains several tabs: 'General', 'Backup & Restore', 'Switches & Ports' (which is selected), 'Traffic', 'Alarm', 'Event', 'LLDP Neighbors', 'Wired Clients', and 'Troubleshooting'. Below this, there are two main sections: 'Top Switches' and 'Port Details'. The 'Port Details' section features a table with the following columns: Port Name, Port Number, Switch Name, Switch Group, Status, Admin Status, Speed, PoE Usage (used/total), VLANs, and Neighbor Name. A hand cursor is pointing to a 'Filter Off' button located above the table. The table contains five rows of data, with the second row highlighted in blue. The status of the ports is indicated by red 'Down' labels or 'Up' labels.

Port Name	Port Number	Switch Name	Switch Group	Status	Admin Status	Speed	PoE Usage (used/total)	VLANs	Neighbor Name
GigabitEthernet1/...	1/1/1	ICX7150-C12 Rou...	SG1	Down	Up	link down or no tr...		1	
GigabitEthernet1/...	1/1/1	ICX7450-24P Swi...	SG1	Up	Up	1 Gb/sec		1	RA_App6_10.2.0.2...
GigabitEthernet1/...	1/1/2	ICX7150-C12 Rou...	SG1	Down	Up	link down or no tr...		1	
GigabitEthernet1/...	1/1/2	ICX7450-24P Swi...	SG1	Down	Up	link down or no tr...		1	
GigabitEthernet1/...	1/1/3	ICX7150-C12 Rou...	SG1	Down	Up	link down or no tr...		1	

4. In the **Port Details** section, click the  icon.

A dialogue box is displayed. The controller provides the following filters to combine several query conditions to filter-out the ports which you want to edit.

**FIGURE 86** Applying Filter to Edit the Ports



**Apply Filters**

Port Number

Admin Status

VLANs

Switch Name

Port Status

POE Enable

[Reset Filters](#)

**OK** **Cancel**

**NOTE**

The **Reset Filters** allows you to clear the search conditions.

5. Click **OK**.
- The controller applies the above filters to return ports that meet the search criteria.

## Creating Routing Configurations

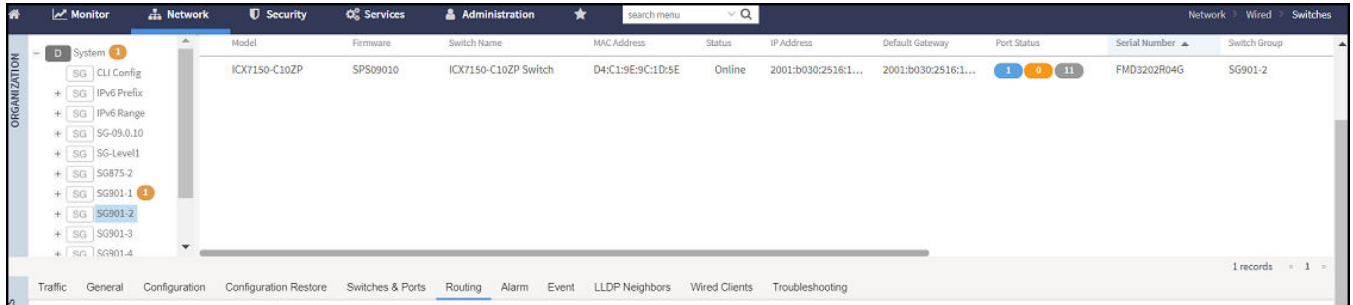
You can create, edit, and delete routing configurations for a switch.


1. From the main menu, go to **Network > Wired > Switches** to display the window.  
The **Switches** page is displayed.
2. Select the **Domain > Switch Group** or specific **Switch Group**, and then choose the switch.



3. In the **Details** pane, click the **Routing** tab.

**FIGURE 87** Switch Routing Tab



4. In the **IP Ports** section, click the  icon.

- The **IP Ports** page is displayed.

**FIGURE 88** IP Ports Page

Switch	Name	Port	DHCP Relay Agent	IP Address
ICX7850-32Q Router	port7	1/1/7	192.112.2.1	10.111.2.1

Switch: ICX7850-32Q Router [D4:C1:9E:18:30:D1]

Name:

Port:

- 1/2/10
- 1/2/11
- 1/2/12
- 1/3/1
- 1/3/2:1
- 1/3/2:2
- 1/3/2:3

OSPF Area:

DHCP Relay Agent:


\* IP Subnet Mask:

Egress ACL:

Complete the following fields:

- **Switch:** Select the switch from the drop down list.
- **Name:** Enter a name.
- **OSPF Area:** Enter the OSPF area IPv4 address.
- **Port:** Select the breakout port number from the list.
- **DHCP Relay Agent:** Enter the DHCP relay agent IP address.
- **IP Address:** Configure the IP address on the selected breakout port.
- **IP Subnet Mask:** Enter an IP subnet mask.
- **Ingress ACL:** Select the ACL for the ingress network interface.
- **Egress ACL:** Select the ACL for the egress network interface.

- Click **OK**.

- In the **VE Ports** section, click the  icon.

**FIGURE 89** VE Ports Page

Complete the following fields:

- **Switch:** Select the switch from the list.
  - **VE#:** Enter the VE number. Range: 1 through 4095.
  - **Name:** Enter a name.
  - **OSPF Area:** Enter the OSPF area IPv4 address.
  - **VLAN#:** Select the VLAN from the list.
  - **DHCP Relay Agent:** Enter the DHCP relay agent IP address.
  - **IP Address:** Enter a unicast IP address.
  - **IP Subnet Mask:** Enter an IP subnet mask.
  - **Ingress ACL:** Select the ACL for the ingress network interface.
  - **Egress ACL:** Select the ACL for the egress network interface.
- The **VE Ports** ports page is displayed.
  - Click **OK**.

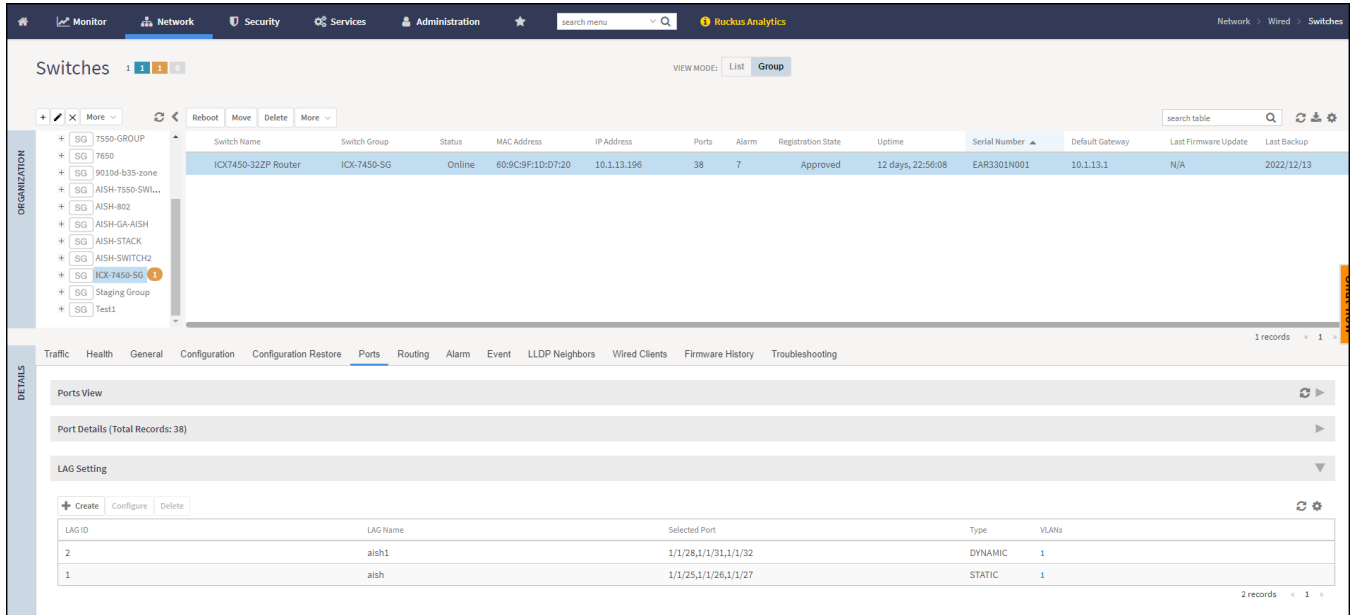
## Managing Link Aggregation Groups (LAGs)

Controller provides an option to define LAGs at an individual switch level.

- From the main the menu, go to **Network > Wired > Switches**.  
The **Switches** page is displayed.
- Select a **Domain > Switch Group** or specific **Switch Group**, and then choose the **Switch**.

3. In the **Details** pane, click the **Ports** tab.

FIGURE 90 Ports




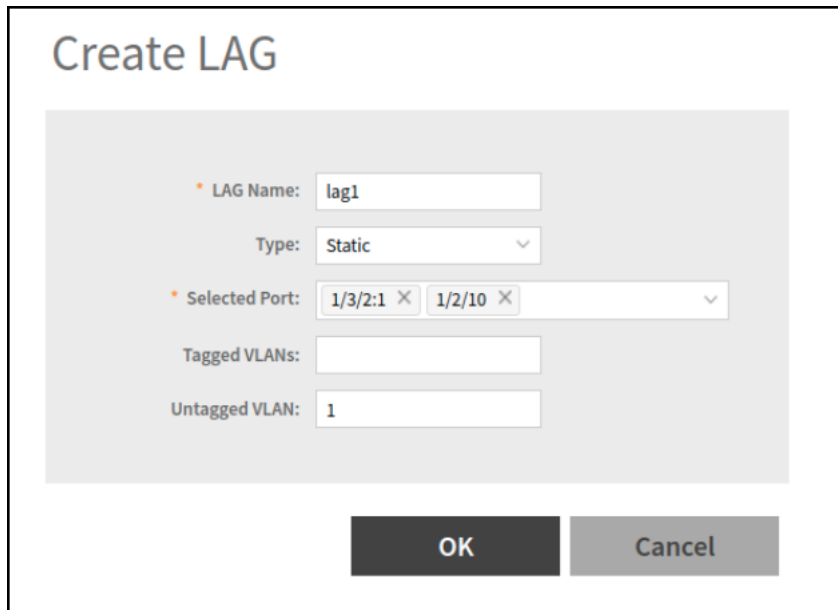
4. In the **LAG Setting** section, click the  icon to display the **Create LAG** dialog box.

FIGURE 91 Creating LAG



5. Complete the following fields:
  - a) **LAG Name:** Enter a name.
  - b) **Type:** Select either **Static** or **Dynamic** from the list.
  - c) **Selected Port:** Add a breakout port to the selected port.

**NOTE**

You are required to manually configure breakout ports on the switches.

- d) **Tagged VLANs:** Enter the tagged VLAN ID or VLAN ID range.
  - e) **Untagged VLANs:** Enter an untagged VLAN ID.
6. Click **OK**.

## Creating a Switch Stack

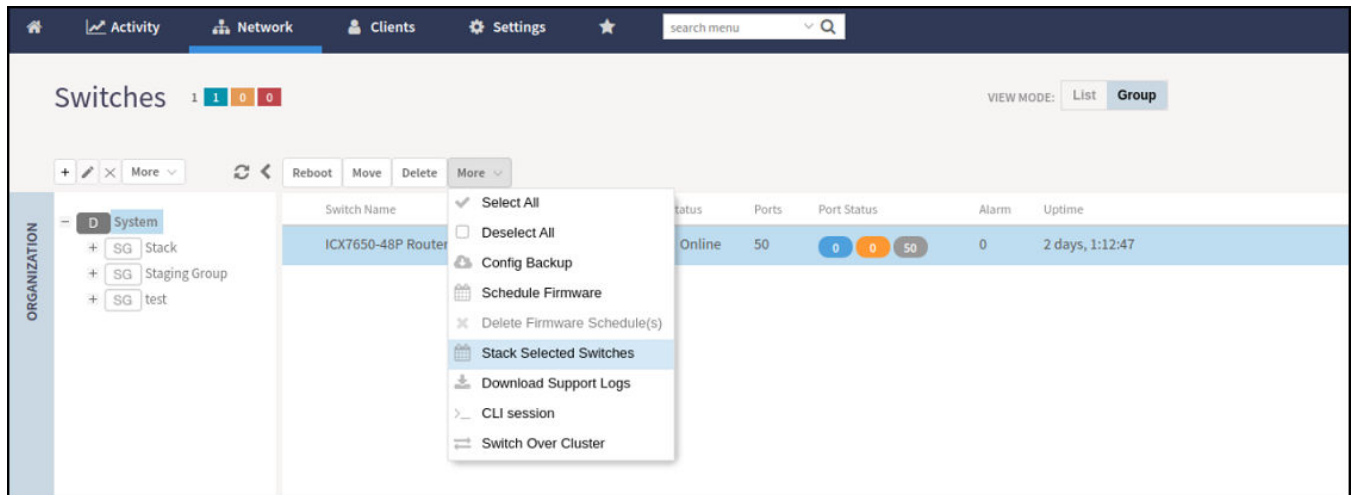
You can create a stack by selecting individual switches that are connected to the controller.

As a prerequisite, before you connect the switch cables ensure to configure switch stacking from the controller.

Complete the following steps to create a stack of switches.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch** that are to be stacked. Click **More > Stack Selected Switches** to display the **Create Stack** page.

**FIGURE 92** Creating a Stack



3. Enable **Active Role** and click **OK** to create the stack.

**NOTE**

The stack creation process takes 15 minutes.

4. To view a switch in the created stack, from the system tree, click **Domain > Switch Group** or **Switch Group** and select the stacked **Switch**.

## Viewing Port Details

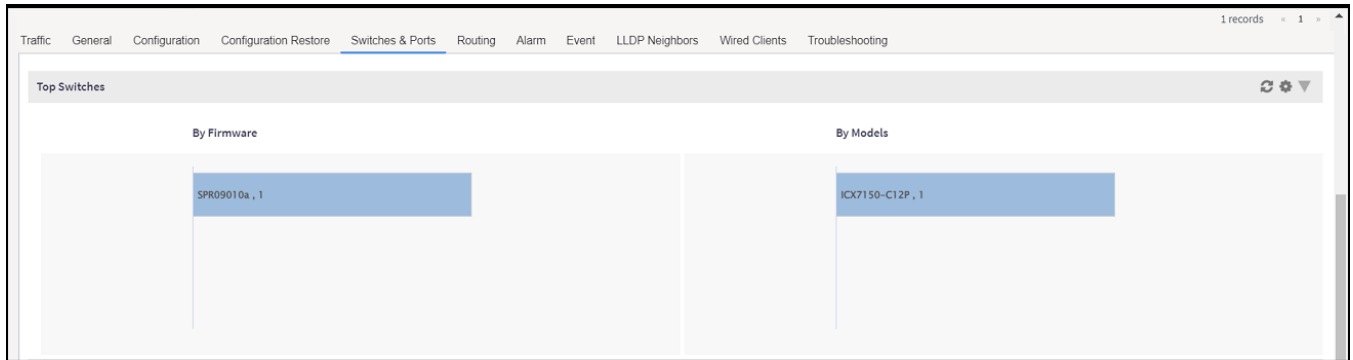
Details on port use are available for individual switches, stacks, and switch groups.

Perform these steps to display information on ports for a switch, stack, or switch group.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. From the system tree, select the **Domain > Switch Group** or **Switch Group** and in the **Details** tab, click **Switches and Ports** tab.

For a switch group, a **Top Switches** tab similar to the following figure is displayed. The graphs provide information on top switches based on firmware and model.

**FIGURE 93** Top Switches Page

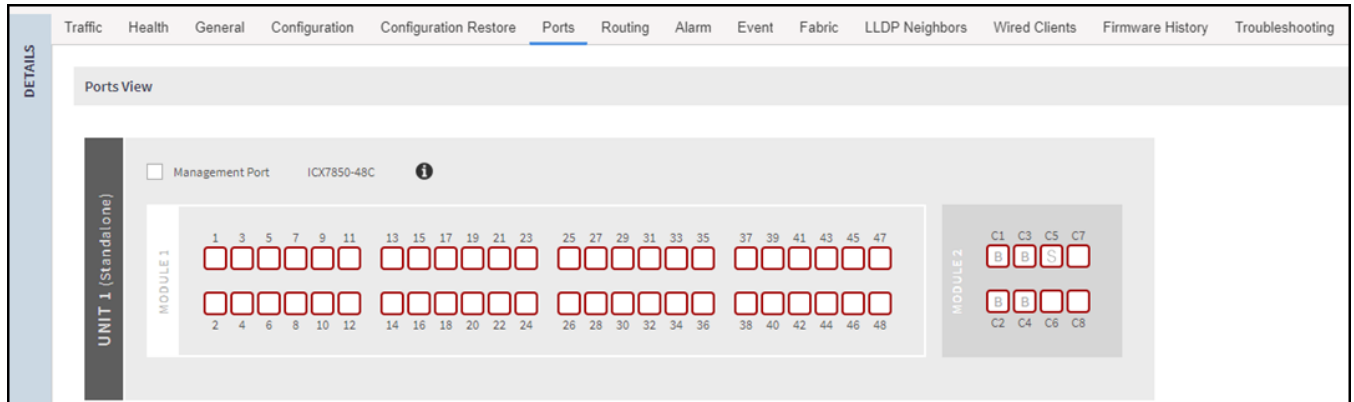


- In the **Switch Group**, select the **Switch** and click **Ports** tab to view the **Front Panel View** in the **Ports View** tab for additional port information as shown in the following figure.

The **Front Panel View** provides information on the state of all ports in each switch module, for example port Up, Down, or Administratively Down.

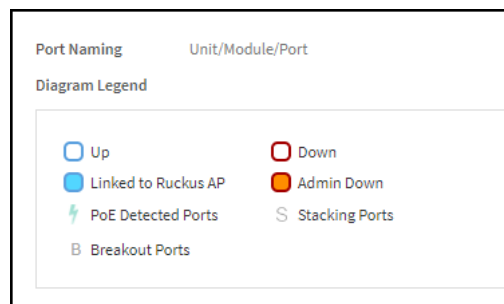
When you hover over the breakout port, a popup window will appear, stating, The 40Gbps port breaks out into four 10Gbps sub-ports respectively

**FIGURE 94** Front Panel View



The following figure shows the diagram legend used in the Front Panel View page.

**FIGURE 95** Diagram Legend



**FIGURE 96** Viewing the Breakout Ports

<input checked="" type="checkbox"/>	1/2/1:1	Port Name:	P2
		Up/Down Status:	Down
		VLAN Untagged:	1
		VLAN Tagged:	N/A
		PoE Utilization:	N/A
<input type="checkbox"/>	1/2/1:2	Port Name:	100GigabitEthernet1/2/1:2
		Up/Down Status:	Down
		VLAN Untagged:	1
		VLAN Tagged:	N/A
		PoE Utilization:	N/A
<input type="checkbox"/>	1/2/1:3	Port Name:	100GigabitEthernet1/2/1:3
		Up/Down Status:	Down
		VLAN Untagged:	1
		VLAN Tagged:	N/A
		PoE Utilization:	N/A
<input type="checkbox"/>	1/2/1:4	Port Name:	100GigabitEthernet1/2/1:4
		Up/Down Status:	Down
		VLAN Untagged:	1
		VLAN Tagged:	N/A
		PoE Utilization:	N/A

The following list further describes items in the Front Panel View legend.

- Up: Ports that are up or active.
- Warning: Ports that have packet errors.
- Down: Ports that are down or inactive.
- Linked to Ruckus AP: Ports that are linked to RUCKUS AP.
- Admin Down: Ports that have been manually disabled by the network administrator.
- PoE Detected Ports: Ports that are PoE detected.
- Stacking Ports: Ports that are stacked.
- Breakout Ports: The 40G/100G port can be divided into 4x10G or 4x25G .



- Click the switch name to view the **Port Details** page as shown in the following figure.

**FIGURE 97** Port Details


Port Details																						
Port Name	Port Number	Switch Name	Switch Group	Status	Admin Status	Speed	PoE Device Type	PoE Usage (used/total wats)	VLANs	Bandwidth IN (%)	Bandwidth OUT (%)	Neighbor Name	LAG Name (Type)	Optics	Incoming Multicast Packets	Outgoing Multicast Packets	Incoming Broadcast Packets	Outgoing Broadcast Packets	In Errors	Out Errors	CRC Errors	In Discard
digbit...	1/21	ICK7650-48EP...	SWITCH-RA-Z...	Up	Up	1 Gb/sec	n/a		1	0.00	0.00			1 Gbit/s...	680543	1480375	4045232	102234	0	0	0	0

The **Port Details** page provides the following information on each port:

**NOTE**

Ports for switch stacks are not configurable from the **Port Details** page.

- **Port Name:** Displays the port name.
- **Port Number:** Displays the breakout port number
- **Status:** Whether the port is operationally up or down.
- **Admin Status:** Whether the port has been set to Up or Down by the network administrator.
- **Speed:** The speed of the port.
- **PoE Device Type:** Inline power device type, such as 802.3af, 802.3at, or Legacy device.
- **PoE Usage (used/total watts):** The PoE power usage compared to the allocated power.
- **VLANs:** The VLANs to which the port is connected.
- **Bandwidth IN (%):** The bandwidth utilization for incoming traffic.
- **Bandwidth OUT (%):** The bandwidth utilization of the port for outgoing traffic.
- **LAG Name (Type):** The name of the Link Aggregation Group (LAG).
- **Optics:** The type of optic.
- **Neighbor Name:** When LLDP is enabled, the name of the neighboring device, such as an AP or another switch or router.
- **Incoming Multicast Packets:** The total number of incoming multicast data packets.
- **Outgoing Multicast Packets:** The total number of outgoing multicast data packets.
- **Incoming Broadcast Packets:** The total number of incoming broadcast data packets.
- **Outgoing Broadcast Packets:** The total number of outgoing broadcast data packets.
- **In Errors:** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- **Out Errors:** The number of outbound packets that could not be transmitted because of errors.
- **CRC Errors:** Indicates that the checksum calculated does not match between the data sender side and the received side. A CRC error usually indicates network transmission problems.
- **In Discard:** The number of inbound packets that were chosen to be discarded (even though no errors are detected) to prevent their being deliverable to a higher-layer protocol. One reason for discarding such a packet could be to free up buffer space.
- **Switch Name:** The name of the switch connected to the port.
- **Switch Group:** The name of the switch group connected to the port.

You can also filter the list of ports by the VLANs associated with them. Click  to set the filters.

**NOTE**

The system does not support configuring LAG interface detail through the controller web user interface. To configure detail settings for LAG after form it, you need to configure it through Switch console directly.



**VIDEO**

**PoE Ports View.** View PoE Information from SmartZone.

[Click to play video in full screen mode.](#)

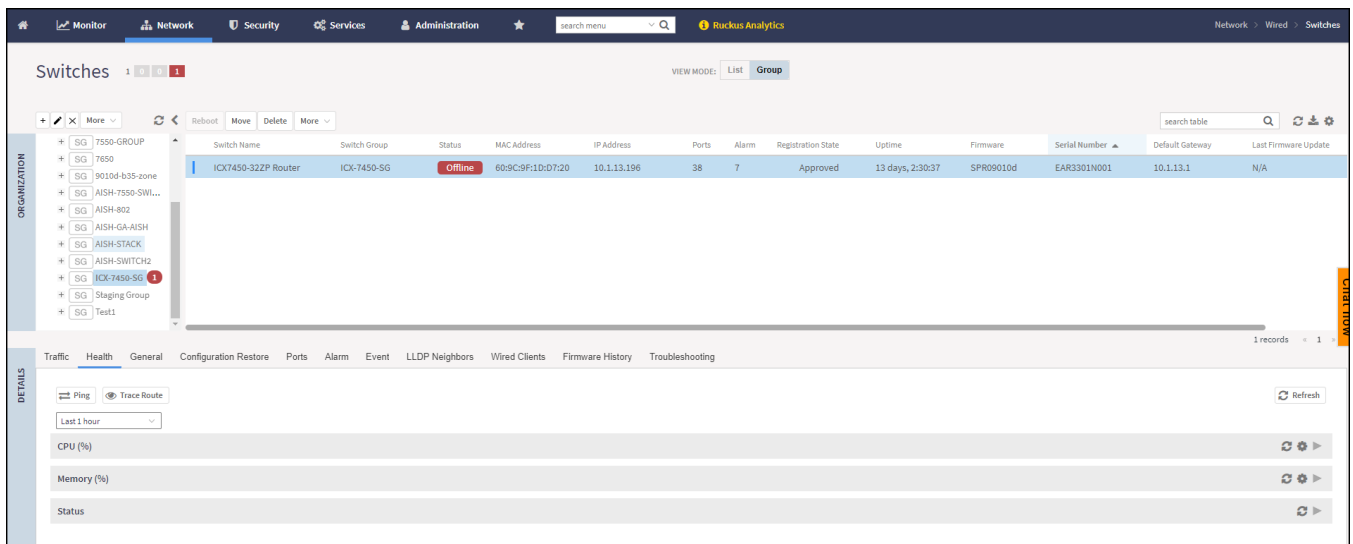
## Viewing Switch Health


Health information displayed for a switch is based on memory usage and CPU usage statistics.

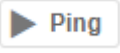
To view information on the health of a switch or the active controller of a stack, perform the following steps.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** tab, click **Health** tab.

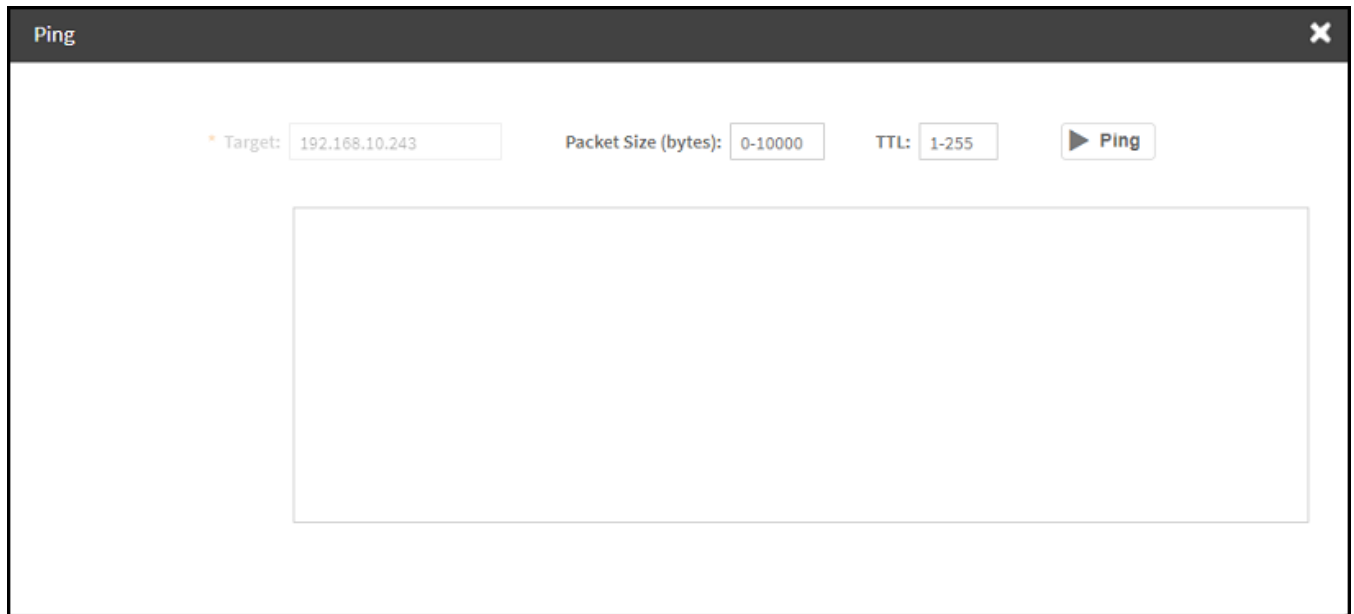
**FIGURE 98** Health

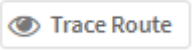


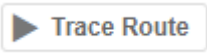
4. Click  icon to display the **Ping** dialog box.

- In the **Ping** dialog box, enter the IP address of the target switch, packet size, and TTL (Time to Live) value. Click  icon. In the below display window you can view that a packet is discarded from the network. As shown in the following example, after the ping, the page displays the number of data packets transmitted, received, and lost and the time required following the ping from the controller to the switch to establish communication.

**FIGURE 99** Pinging the switch

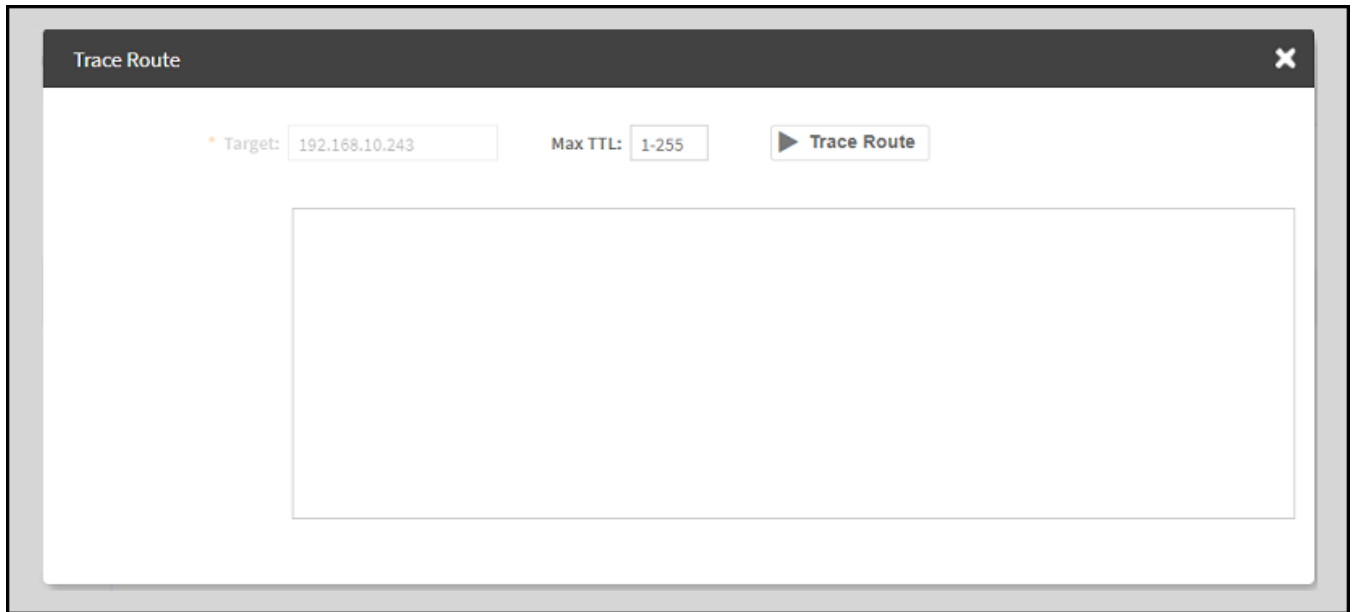



- Click  icon to display the **Trace Route** dialog box.

7. On the **Trace Route** dialog box, enter the TTL (Time to Live) value. Click  icon. In the below display window you can view that a packet is discarded from the network.

As shown in the following example, the page displays the IP address of the hops the packet takes as it traverses the network between the switch and the controller.

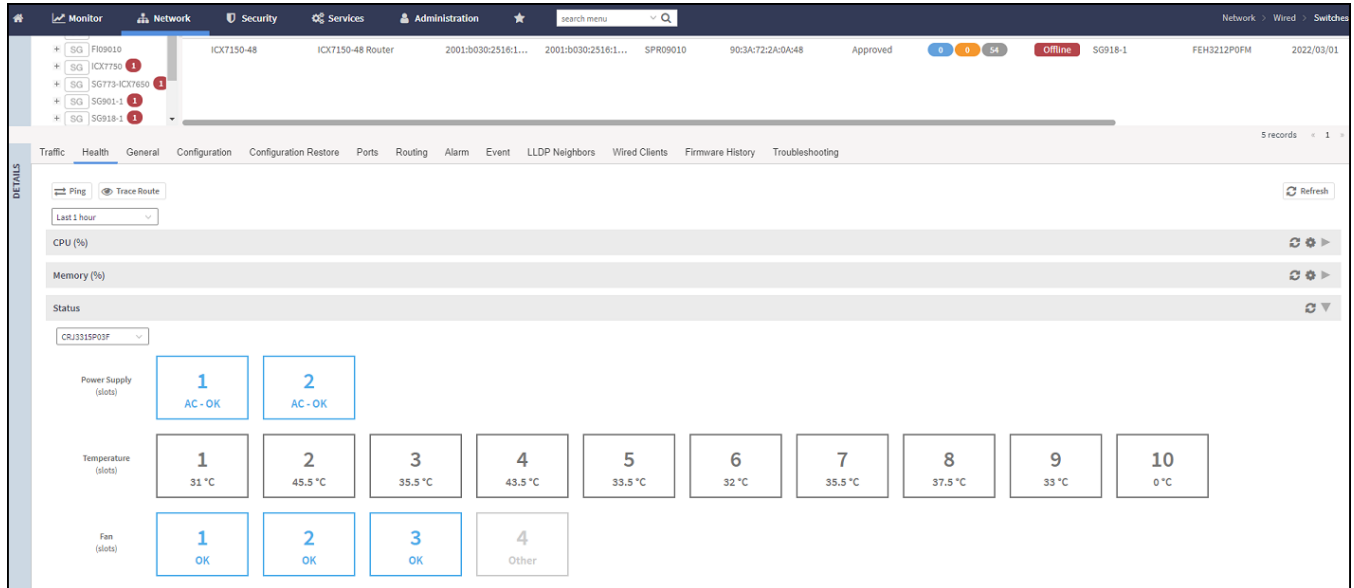
**FIGURE 100** Tracing the packet route through the network



8. In the **Health** tab, from the drop-down menu  select the duration for which you want to view the switch health.


As shown in the following example, information on switch health is displayed on the **Health** Tab, based on your selections.

**FIGURE 101** Health Tab



The following information is displayed based on the duration selected:

- **CPU (%):** The CPU usage of the switch, including the minimum, maximum, average, and current CPU usage trends of the switch.
- **Memory (%):** The memory usage of the switch, including the minimum, maximum, average, and current memory usage trends of the switch.
- **Status:** The health status of the power supply, temperature, and the fans for up to four switch modules are displayed. OK indicates the parameter and components are in good health.

You can click  to modify the display settings. You can view the trend as a graph or a table. You can also modify the display to reflect the switch name, MAC address, or IP address.

## Viewing Alarms

Syslog messages from the switch are sent to the controller to periodically communicate switch health and status. It also brings your attention to issues that may need resolution at the switch level. You can view these details from the **Alarms** tab for individual switches, stacks and switch groups.

Syslog messages from the switch are categorized as **Major** and **Critical**, and are displayed as **events** in the controller. From these events, the following messages are displayed as **alarms** in the controller interface:

- Power Supply failure
- Fan failure
- Module Insertion or removal
- Temperature above the threshold warning

## Working with Switches

### SmartZone Switch Management

- Stack member unit failure
- PoE power allocation failure
- DHCP offer dropped message
- Port put into error disable state

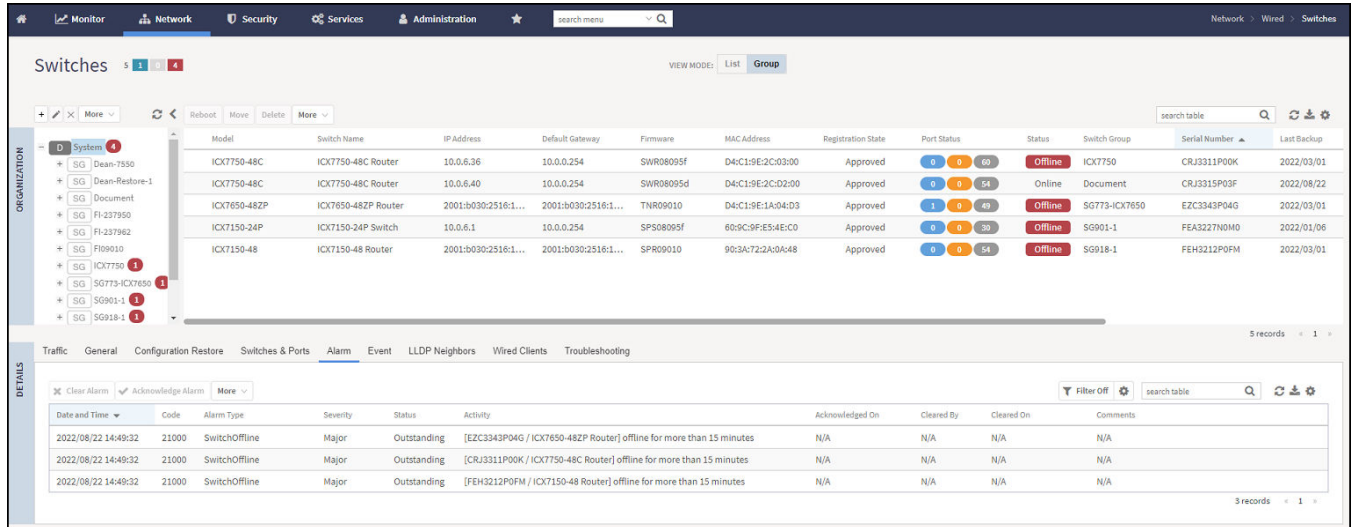
The remaining syslog messages which are categorized by other severity levels are listed in the `switchevent.log` file available in **Diagnostics > Application Logs**.

The alarms generate for the switch also reflect in the **Monitor > Events and Alarms > Events** page.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.

- In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **Alarm** tab.


FIGURE 102 Switches Alarms Tab



The following information is displayed in the **Alarms** tab:

- **Date and Time:** Displays the date and time when the alarm was triggered.
- **Code:** Displays the alarm code (see the Alarm and Reference Guide for your controller platform for more information).
- **Alarm Type:** Displays the type of alarm event that occurred (for example, switch reset to factory settings).
- **Severity:** Displays the severity level assigned to the events such as Critical, Major, Minor and Warning.
- **Status:** Indicates whether the alarm has already been cleared or still outstanding.
- **Activity:** Displays additional details about the alarm, such as how long was the switch offline for.
- **Acknowledged On:** Displays the date and time when the administrator acknowledge the alarm.
- **Cleared By:** Displays information about who cleared the alarm.
- **Cleared On:** Displays the date and time when the alarm was cleared.
- **Comments:** Displays administrator notes recorded during alarm management.




Click  to export the alarms details to a CSV file. Check the default download folder of your web browser and look for a file named *alarms.csv* and view it using a spreadsheet application

Clearing an alarm removes the alarm from the list but keeps it on the controller's database. Select the alarm from the list and click **Clear Alarm**. The **Clear Alarm** page appears. Type your comments and select **Apply**.

Acknowledging an alarm lets other administrators know that you have examined the alarm. Click **Acknowledge Alarm** to acknowledge an alarm. After you acknowledge an alarm, it will remain on the list of alarms and will show the date and time that you acknowledged it.



You can also view alarms by their severity, status, date and time stamp. Click  to apply filters.

## Viewing the Events



Events are triggered by an occurrence or the detection of certain conditions in the switch. For example, when the temperature of the device reaches warning levels, or when the fan speed changes, an event is triggered. You can find these details in the **Events** tab, accessible for individual switches, stacks, and switch groups.

The alarms generate for the switch also reflect in the **Monitor > Events and Alarms > Events** page.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. From the system tree, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** pane, click the **Events** tab.

**FIGURE 103** Events Tab

Date and Time	Code	Type	Severity	Activity
2022/08/18 15:20:07	22091	Switch Discover	Informational	[FMD3202R00T / D4:C1:9E:9C:1E:68] Switch discovered by the controller.
2022/08/18 15:20:07	22082	Switch Connection	Informational	[FMD3202R00T / D4:C1:9E:9C:1E:68] Switch is connected to the controller.

4. The following information is displayed in the **Events** tab.
  - a) **Date and Time:** Displays the date and time when the event occurred.
  - b) **Code:** Displays the event code (see the Alarm and Event Reference Guide for your controller platform more information).
  - c) **Type:** Displays the type of event that occurred (for example, Switch configuration updated).
  - d) **Severity:** Displays the severity level assigned to the events such as Critical, Debug, Informational, Warning, Major etc.
  - e) **Activity:** Displays additional details about the event.
5. Click  to export the events details to a CSV file. Check the default download folder of your web browser and look for a file named *events.csv* and view it using a spreadsheet application.
6. Click  to filter the alarms by their severity, date and time.

## Viewing LLDP Neighbor Information

You can view information about the LLDP neighbors such as printers, VOIP devices, or other user equipment connected to the switch, in addition to the LLDP AP neighbors connected to the switch. Link layer discovery protocol or LLDP is used to discover and identify the clients.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.



2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **LLDP Neighbors** tab.

FIGURE 104 LLDP Neighbors Connected to the Switch

Device Name	Switch Group	Switch Name	Device Type	Remote Port	Local Port	Local MAC	Remote Device Description	Chassis Id
RuckusAP	SWITCH-RA-Z...	ICX7450-32ZP ...	Bridge, WlanA...	eth1	GigabitEthernet1/1/7	60:9c:9f:1d:d7:26	Ruckus R850 Multimedia Hotzo...	28:b3:71:e:ef:fo
RuckusAP	SWITCH-RA-Z...	ICX7450-32ZP ...	Bridge, WlanA...	eth0	GigabitEthernet1/1/14	60:9c:9f:1d:d7:2d	Ruckus R710 Multimedia Hotzo...	38:ff:36:15:bb:fo
RuckusAP	SWITCH-RA-Z...	ICX7450-32ZP ...	Bridge, WlanA...	eth1	GigabitEthernet1/1/10	60:9c:9f:1d:d7:29	Ruckus R650 Multimedia Hotzo...	20:58:69:3b:b9:90
RuckusAP	SWITCH-RA-Z...	ICX7450-32ZP ...	Bridge, WlanA...	eth0	GigabitEthernet1/1/13	60:9c:9f:1d:d7:2c	Ruckus R510 Multimedia Hotzo...	b4:79:c8:2f:7e:90
RuckusAP	SWITCH-RA-Z...	ICX7450-32ZP ...	Bridge, WlanA...	ent3	GigabitEthernet1/1/16	60:9c:9f:1d:d7:2f	Ruckus R720 Multimedia Hotzo...	0c:f4:d5:13:34:a0
RuckusAP	SWITCH-RA-Z...	ICX7450-32ZP ...	Bridge, WlanA...	eth1	GigabitEthernet1/1/9	60:9c:9f:1d:d7:28	Ruckus R550 Multimedia Hotzo...	b4:79:c8:3e:83:b0

Device Name	Switch Group	Switch Name	Chassis Id	Device Type	Remote Port	Local Port	Local MAC	Remote Device Description
N/A	SWITCH-RA-Z...	ICX7450-32ZP ...	10:65:30:0e:f1:d3	Other	N/A	GigabitEthernet1/1/23	60:9c:9f:1d:d7:36	N/A
N/A	SWITCH-RA-Z...	ICX7450-32ZP ...	a0:29:19:21:3d:20	Other	N/A	GigabitEthernet1/1/24	60:9c:9f:1d:d7:37	N/A

The following LLDP Neighbors information for switch is displayed in the **LLDP AP Neighbors** tab and **LLDP Neighbors** tab:

- **Device Name:** Displays the name of the LLDP neighbor or AP neighbor connected to the switch.
- **Switch Group:** The name of the group to which the switch belongs.
- **Switch Name:** The name of the switch or group.
- **Device Type:** Displays the name of the device type (for example, Router).
- **Remote Port:** Displays the remote port to which the device is connected.
- **Local Port:** Displays the local port the device is connected to.
- **Local MAC:** Displays the local MAC address of the device.
- **Remote Device Description:** displays the name of the remote device.
- **Chassis Id:** Display the chassis id information.

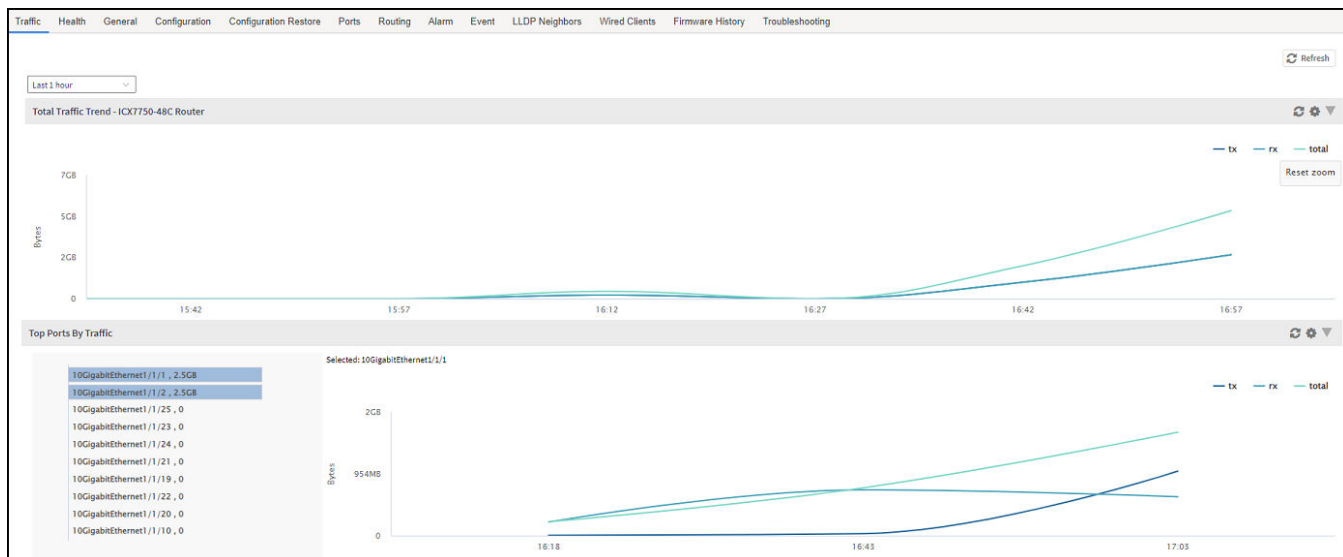
## Viewing Traffic Trends in the Switch

You can view statistical information about how traffic is handled at the switch level. These details are available for individual switches, stacks and switch groups.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.

2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **Traffic** tab.

FIGURE 105 Traffic Trend for a Switch



The following information is displayed in the **Traffic** tab. You can view the traffic trend for the last 1 hour or 24 hours:

- **Total Traffic Trend:** Provides a graphical representation of the network traffic usage over a period of time in the switch or switch group. It also indicates the amount of traffic or data transmitted (tx) and received (rx) by the group in MB, at a certain time and date.
- **Top Switch by Traffic:** Provides a graphical representation of the top switches that handled maximum network traffic over a period of time, in the switch group. You can click on the switch address to view the traffic trend. This trend is only available for switch groups.
- **Top Ports by Traffic:** Provides a graphical representation of the top ports that handled maximum network traffic over a period of time, for a switch. You can click on the port address to view the traffic trend. This trend is only available for individual switches.
- **Total Multicast Traffic Trend:** Provides a graphical representation of the multicast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming multicast data packets (multicastIn) and total number of outgoing multicast packets (multicastOut) by the group in MB, at a certain time and date.
- **Total Unicast Traffic Trend:** Provides a graphical representation of the unicast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming unicast data packet (unicastIn) and total number of outgoing unicast packet (unicastOut) by the group in MB, at a certain time and date.
- **Total Broadcast Traffic Trend:** Provides a graphical representation of the broadcast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming broadcast data packets (broadcastIn) and total number of outgoing broadcast packets (broadcastOut) by the group in MB, at a certain time and date.
- **Total Port Errors:** Provides a graphical representation of the port errors over a period of time in the switch or switch group. It also indicates the total number of inbound packets that contained errors (inErr) and total number of outbound packets that could not be transmitted because of errors (outErr) by the group in MB, at a certain time and date.

## Viewing Firmware History of the Switch

The **Firmware History** allows you to view the detailed status and results of the firmware updates for a switch, as well as view the history of past firmware upgrades on the switch.

You must upgrade the switch firmware as described in [Scheduling a Firmware Upgrade for Selected Switches](#) on page 40

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. From the system tree, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** pane, click the **Firmware History** tab.

**FIGURE 106** Viewing Firmware History

Upgrade Job Status - ICX7650-48ZP Router					
Time	Switch Id	Firmware Version	Image Name	Status	Failure Reason
2021/12/14 13:53:50	D4:C1:9E:1A:04:D3	F109010	TNR09010ufl	Completed	N/A
2021/12/02 11:05:04	D4:C1:9E:1A:04:D3	F109010	TNR09010ufl	Completed	N/A

Firmware Upgrade History - ICX7650-48ZP Router	
Time	Firmware Version
2021/12/14 13:53:50	TNR09010
2021/12/02 11:05:04	TNR09010_b152 -> TNR09010

4. In the **Upgrade Job Status** section, you can verify the upgrade status including the time, switch ID, firmware version, image name, status and any failure reasons (if applicable).
5. In the **Firmware Upgrade History** section, you can see the times of previous upgrades and the firmware versions used.

## Deleting the Firmware Upgrade Schedules

If you schedule a firmware upgrade, and if the firmware upgrade is not executed or is in progress then this feature allows you to cancel the firmware upgrade. However, it must be noted that if the switch is copying or downloading the firmware, the controller will not be able to cancel the process.

To delete the firmware upgrade process, perform the following steps.

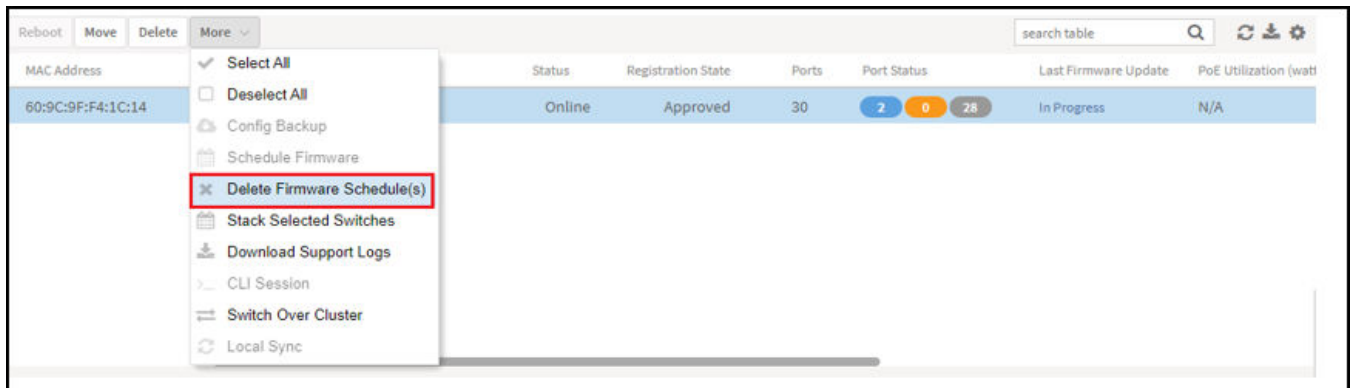
1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.

2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **More > Delete Firmware Schedules**.

FIGURE 107 Upgrade in Progress

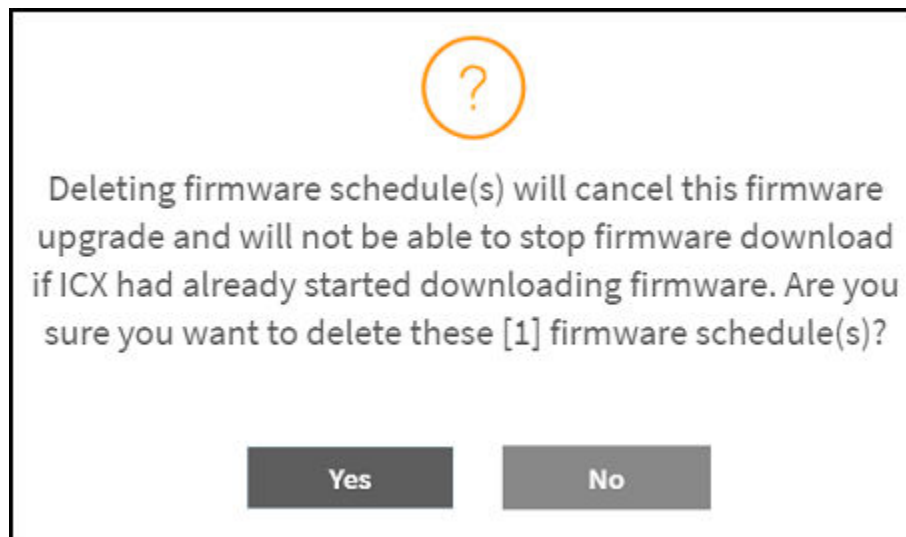
MAC Address	Model	IP Address	Status	Registration State	Ports	Port Status	Last Firmware Update	PoE Utilization (watt)
60:9C:9F:F4:1C:14	ICX7150-24	10.0.0.6.5	Online	Approved	30	2 0 28	In Progress	N/A

FIGURE 108 Deleting Firmware Upgrade Schedule(s)



A warning message is displayed before you cancel the upgrade.

FIGURE 109 Warning Message before deleting



3. Click **Yes** to delete the firmware schedule.
4. A **Switch firmware schedule(s) deleted successfully** message dialog box is displayed, click **OK**.

- In the **Organization** tab, select the **Switch** and in the **Details** tab, select the **Firmware History** tab. In the **Upgrade Job Status** tab confirm that the schedule is canceled.

FIGURE 110 Confirming the deletion

Time	Switch Id	Firmware Version	Image Name	Status	Failure Reason
2022/07/04 10:24:14	60:9C:9F:F4:1C:14	FI09010a	SPR09010aufi	Cancel	Job had been canceled
2022/07/01 16:42:33	60:9C:9F:F4:1C:14	FI09010c	SPR09010cufi	Cancel	Job had been canceled

## Configuring the Group Firmware Settings

The Group Firmware Settings allows you to select default firmware for the switch group.

### NOTE

The default firmware selection at group level does not trigger upgrade for the existing switches in the switch group, it only triggers upgrade for newly joined switches. The newly joined switches are upgraded to the selected firmware in the switch group.

Complete the following steps to perform the firmware upgrade of newly added switch in the switch group to the default firmware version.



- On the menu, click **Network > Wired > Switches** to display the **Switches** window.
- From the system tree, select a **Domain > Switch Group** or **Switch Group** that you want to configure, and click  icon to display the **Configure Switch Group** page.

FIGURE 111 Configuring the Switch with Default Version

**Configure Switch Group**

Name:  Description:

Firmware Version:  

Changing firmware version will cause Switches running older firmware to get upgraded and rebooted.

Type:  Domain  Switch Group

Parent Group:

3. Complete the following details:
  - **Name:** Enter the name for the switch group.
  - **Description:** Enter a brief description about the switch group .
  - **Firmware version:** Select a firmware version from the list or retain the default firmware version.

**FIGURE 112** Configuring the Switch Group with Firmware Version

The screenshot shows a 'Configure Switch Group' dialog box. The 'Name' field is filled with 'Dean'. The 'Description' field is empty. The 'Firmware Version' dropdown is set to 'F108095'. A red warning message states: 'Changing firmware version will cause Switches running older firmware to get upgraded and rebooted.' The 'Type' section has 'Switch Group' selected. The 'Parent Group' is set to 'System'. 'OK' and 'Cancel' buttons are at the bottom right.

**NOTE**

The Group Firmware Settings requires switches to be running on SmartZone 5.2.1 or later.

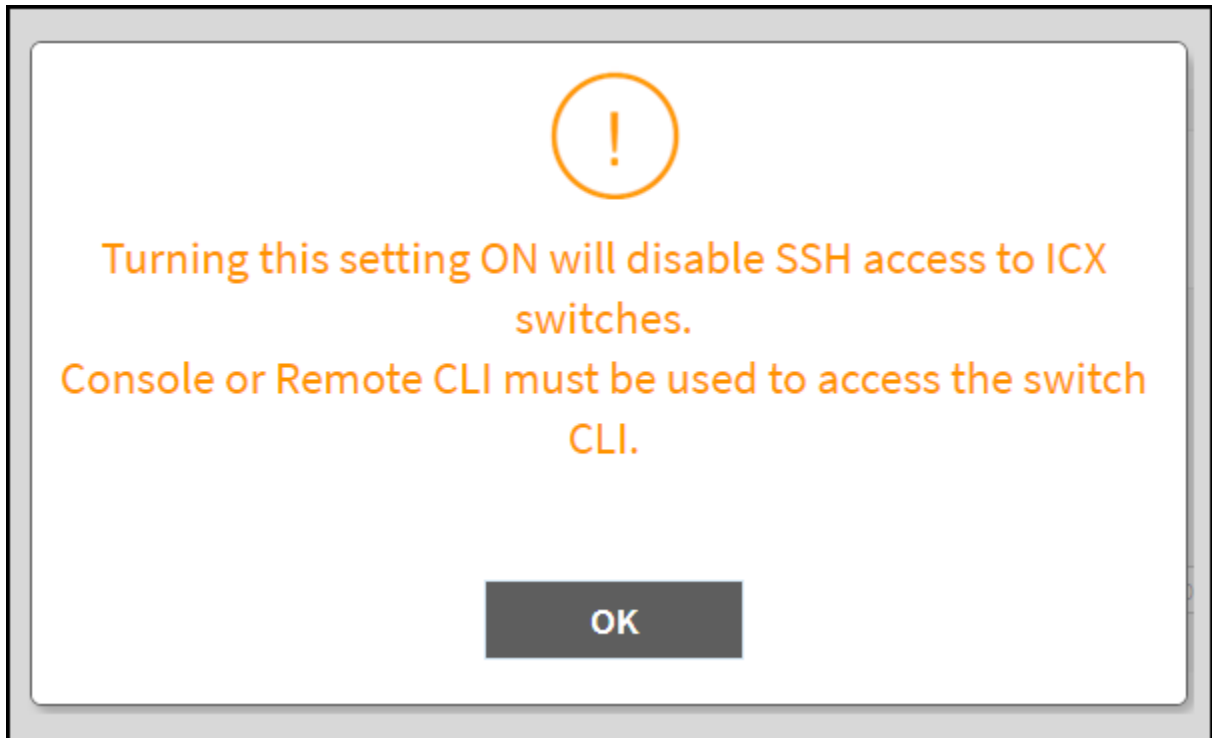
- **Type:** Choose **Switch Group**.
- **Parent Group:** Displays the parent group under which the switch group resides.
- **Two Factor Authentication:** Switch **ON** to use the **Console CLI** or **Remote CLI** to access the **Switches**.

**NOTE**

Turning ON this feature will disable the SSH access to the switches.

A **Message** dialog box is displayed, click **OK**.

FIGURE 113 Two Factor Authentication Message



- **Backup Schedule:** Allows you to schedule the backup. From the **Interval** drop-down list, select the type of backup such as **Daily**, **Weekly**, or **Monthly**. If the backup selected is **Daily**, you can configure **@Hour**, and **Minute** fields. If the backup selected is **Weekly**, you can configure the **Every** (day of the week), **@Hour**, and **Minute** fields. If the backup selected is **Monthly**, you can configure **Every** (date), **@Hour**, and **Minute** fields.

**NOTE**

The default backup time for scheduling a **Daily** backup is 3:30 a.m. The backup schedule is configured on the level one switch group.

4. Click **OK**.

## Accessing the Switch CLI through Controller (Remote CLI)

SmartZone 5.2.1 introduces this essential feature that allows you to directly access the Switch CLI prompt from the controller web interface. The Remote CLI allows you to establish a secured connection between controller and switch that can span over Internet, and eliminate the need to open VPN connection to switch's network when trying to access CLI through SSH or Telnet.

**NOTE**

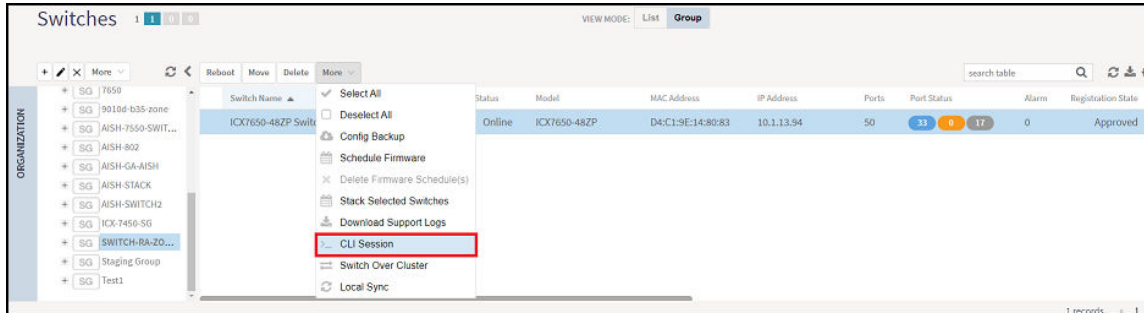
This feature can be accessed by only the System Super-Admin in 5.2.1 release and later releases.

The administrator must complete the following steps to access a CLI session.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**.

3. Click **More > CLI session** to display the CLI command window.

FIGURE 114 Selecting CLI Session





4. Enter the administrator password.

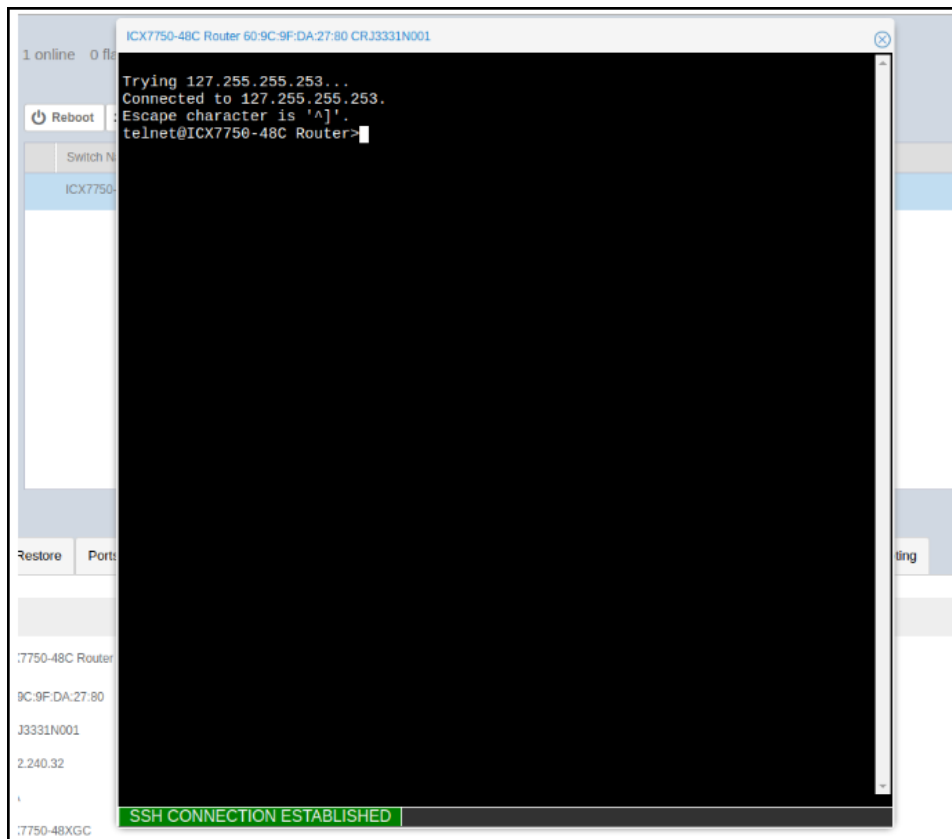
After login, it takes approximately five seconds to set up a secure session within the secure tunnel established between switch and controller to access switch.

**NOTE**

You do not need to enable telnet server on ICX switches to use Remote CLI.

However, if telnet authentication is enabled on the switch, you will be prompted to enter the credentials when opening CLI session via SmartZone. The credentials depend on the type of authentication defined on the switch (local user, RADIUS etc.).

**FIGURE 115** Accessing Switch Through the CLI Sesion

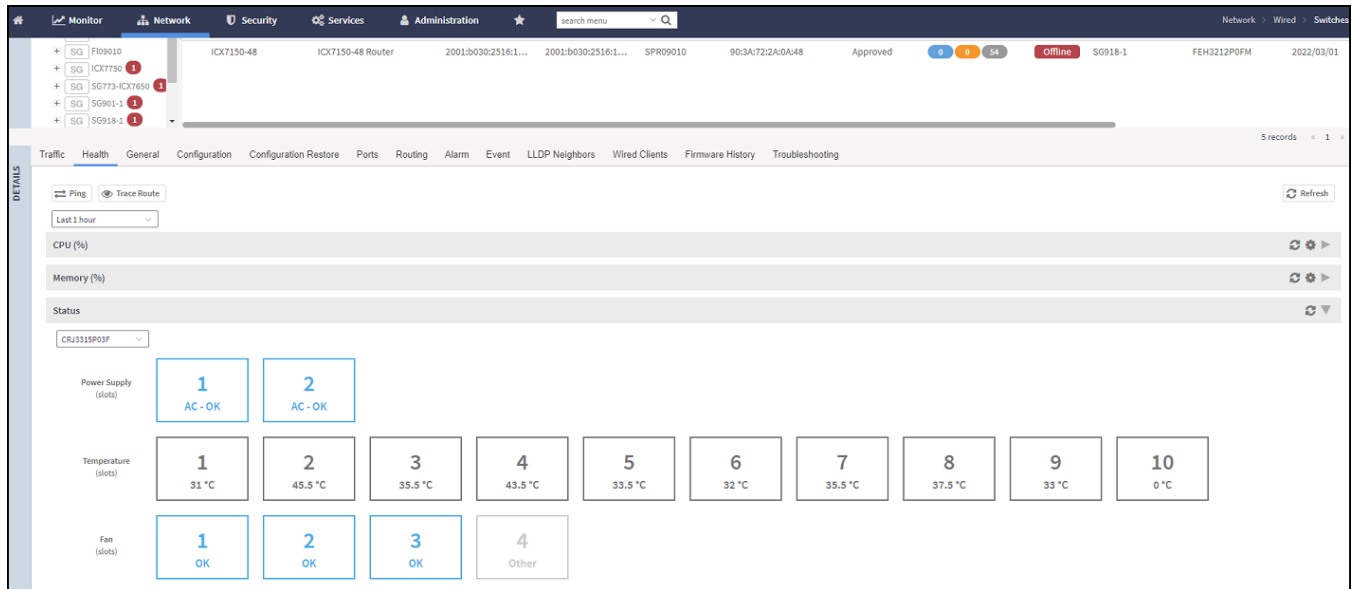




Complete the following steps to view the health status of each member in the stack unit.

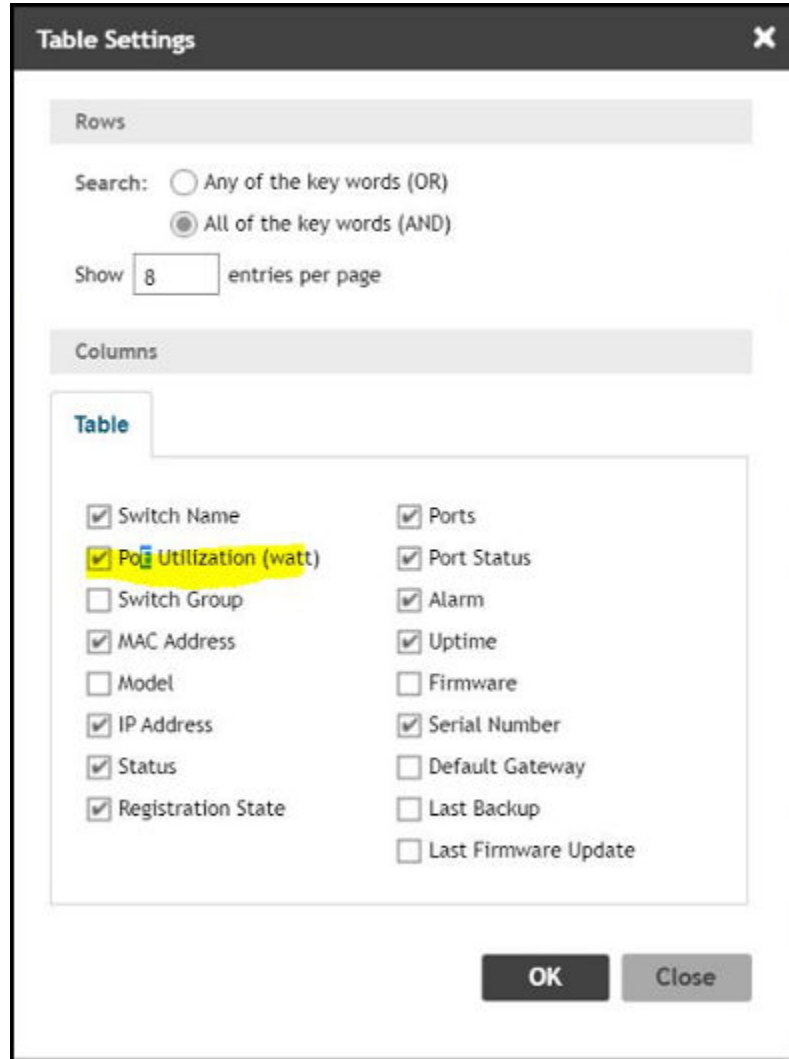
1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** tab, click **Health** tab. In the **Status** tab you can view the health status, such as the power supply, temperature, and fan status of the stack switch.

**FIGURE 117** Viewing the Health Status of Stack Switch



- To enable the PoE Utilization, In the **Organization** tab, click  icon at the top right to display the **Table Settings** dialog box.

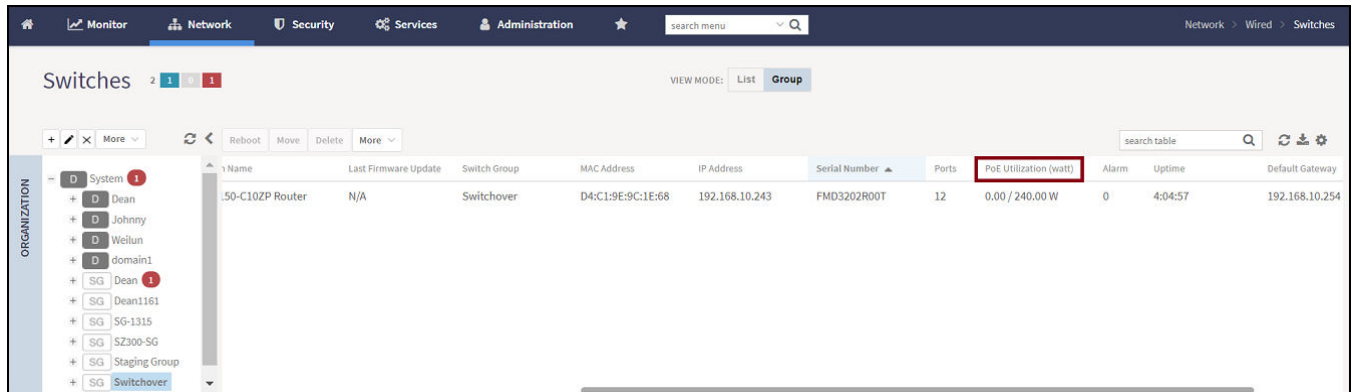
**FIGURE 118** Enabling the PoE Utilization



- Select the **PoE Utilization (watt)** from the table.
- Click **OK**.

7. In the **Organization** tab, select the **Switch**, to view the **PoE Utilization (watt)** field listed in the table.

**FIGURE 119** Viewing the PoE Utilization Field



## Ability to Convert Standalone Switch to Stack

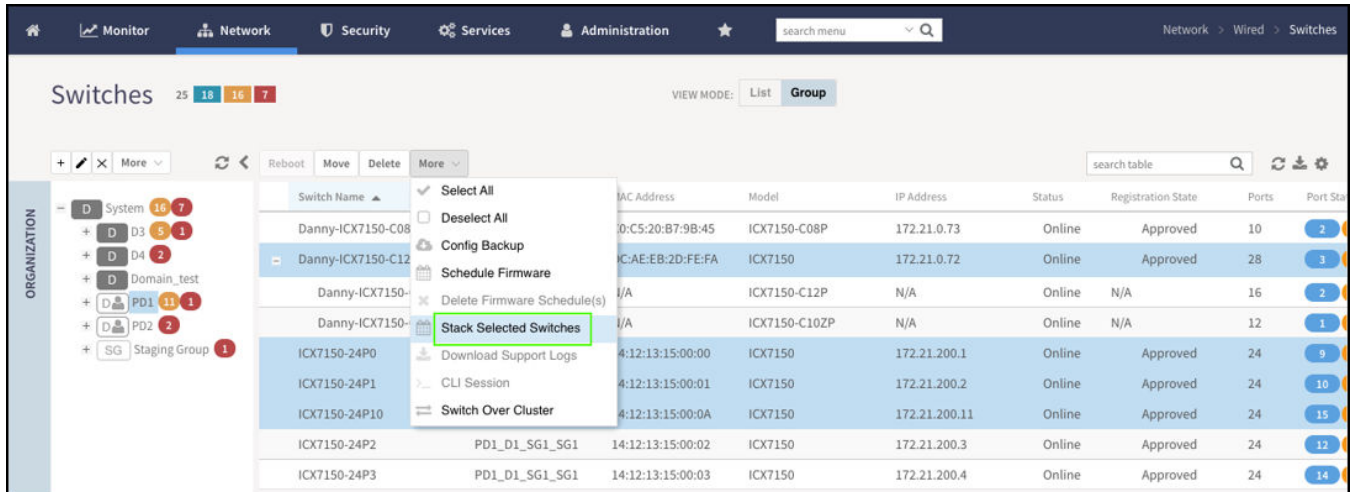
This feature allows the Standalone switch to convert into a stack by adding member switches.

Complete the following steps to convert standalone switch into stack.

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. In the **Organization** tab, click a **Domain > Switch Group** or **Switch Group** and select the **Switch**.

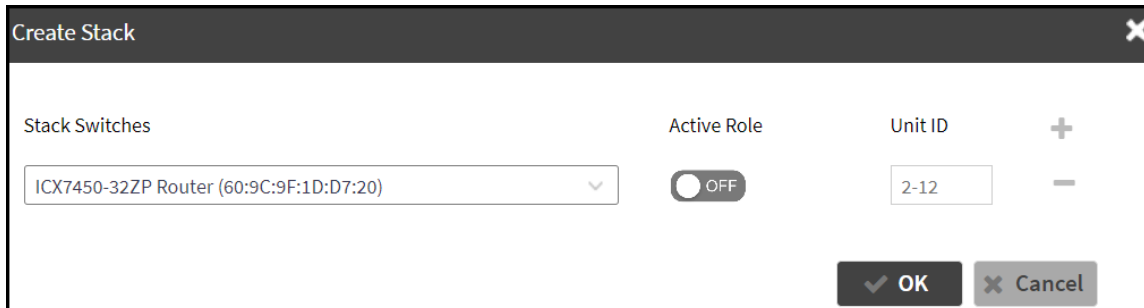
3. To add standalone switch to the stack, click **More > Stack Selected Switches**

FIGURE 120 Stack Selected Switches



The **Create Stack** dialog box is displayed. Turn **Active Role** ON.

FIGURE 121 Create Stack Dialog Box



4. In the **Edit Stack Member** page, click + or - to add or remove the stack entry. A RUCKUS stack contains from two 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, an ICX 7250 stack, an ICX 7450 stack, an ICX 7650 stack, or an ICX 7850 stack.

**NOTE**

From FI 09.0.00, the maximum stack size for ICX 7150 and ICX 7250 devices are limited to eight units in a stack.

Stack Switches	Active Role	Unit ID	
Danny-ICX7150-C12P (DC:AE:EB:2D:FE:FA) - ICX7150-C12P	<input checked="" type="checkbox"/> ON	2-12	<input type="button" value="+"/>
Danny-ICX7150-C12P (DC:AE:EB:2D:FE:FA) - ICX7150-C102P	<input type="checkbox"/> OFF	2	
ICX7150-24P0 (14:12:13:15:00:00)	<input checked="" type="checkbox"/> OFF	2-12	<input type="button" value="-"/>
ICX7150-24P1 (14:12:13:15:00:01)	<input type="checkbox"/> OFF	2-12	<input type="button" value="-"/>
ICX7150-24P2 (14:12:13:15:00:02)	<input type="checkbox"/> OFF	2-12	<input type="button" value="-"/>

Working with Switches  
SmartZone Switch Management

The screenshot shows the 'Edit Stack Member' dialog box. It contains a table of stack switches with columns for 'Stack Switches', 'Active Role', and 'Unit ID'. A dropdown menu is open, showing a 'Reload...' option and a list of switch models and MAC addresses. The dialog also has 'OK' and 'Cancel' buttons at the bottom right.

Stack Switches	Active Role	Unit ID	
Danny-ICX7150-C12P (DC:AE:EB:2D:FE:FA) - ICX7150-C12P	on	2-12	
Danny-ICX7150-C12P (DC:AE:EB:2D:FE:FA) - ICX7150-C102P	off	2	
ICX7150-24P0 (14:12:13:15:00:00)	off	2-12	-
ICX7150-24P1 (14:12:13:15:00:01)	off	2-12	-
ICX7150-24P2 (14:12:13:15:00:02)	off	2-12	-
No data available	off	2-12	-

Reload...

- Danny-ICX7150-C08P (C0:C5:20:B7:9B:45)
- ICX7150-24P10 (14:12:13:15:00:0A)
- ICX7150-24P2 (14:12:13:15:00:02)
- ICX7150-24P3 (14:12:13:15:00:03)
- ICX7150-24P4 (14:12:13:15:00:04)
- ICX7150-24P5 (14:12:13:15:00:05)
- ICX7150-24P6 (14:12:13:15:00:06)
- ICX7150-24P7 (14:12:13:15:00:07)
- ICX7150-24P8 (14:12:13:15:00:08)
- ICX7150-24P9 (14:12:13:15:00:09)

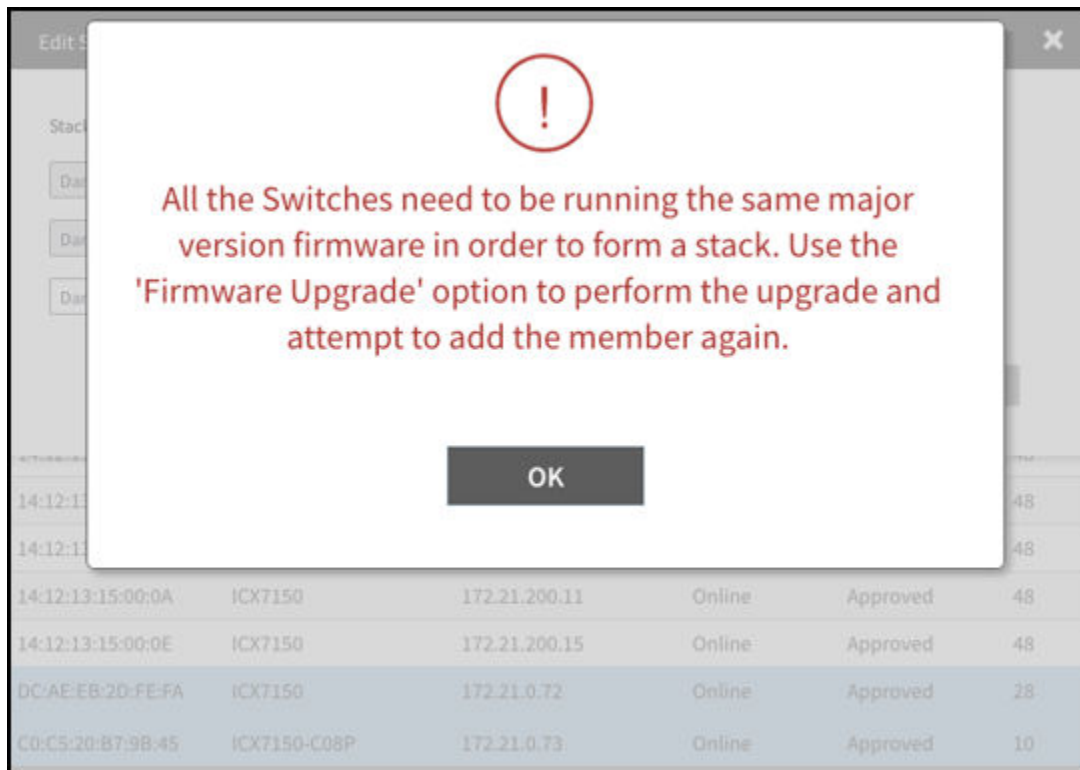
Page 1 of 2



5. Click **OK**.

**NOTE**

If stack and switch are running different version of an image, an error message is displayed.



## Troubleshooting Switch Issues

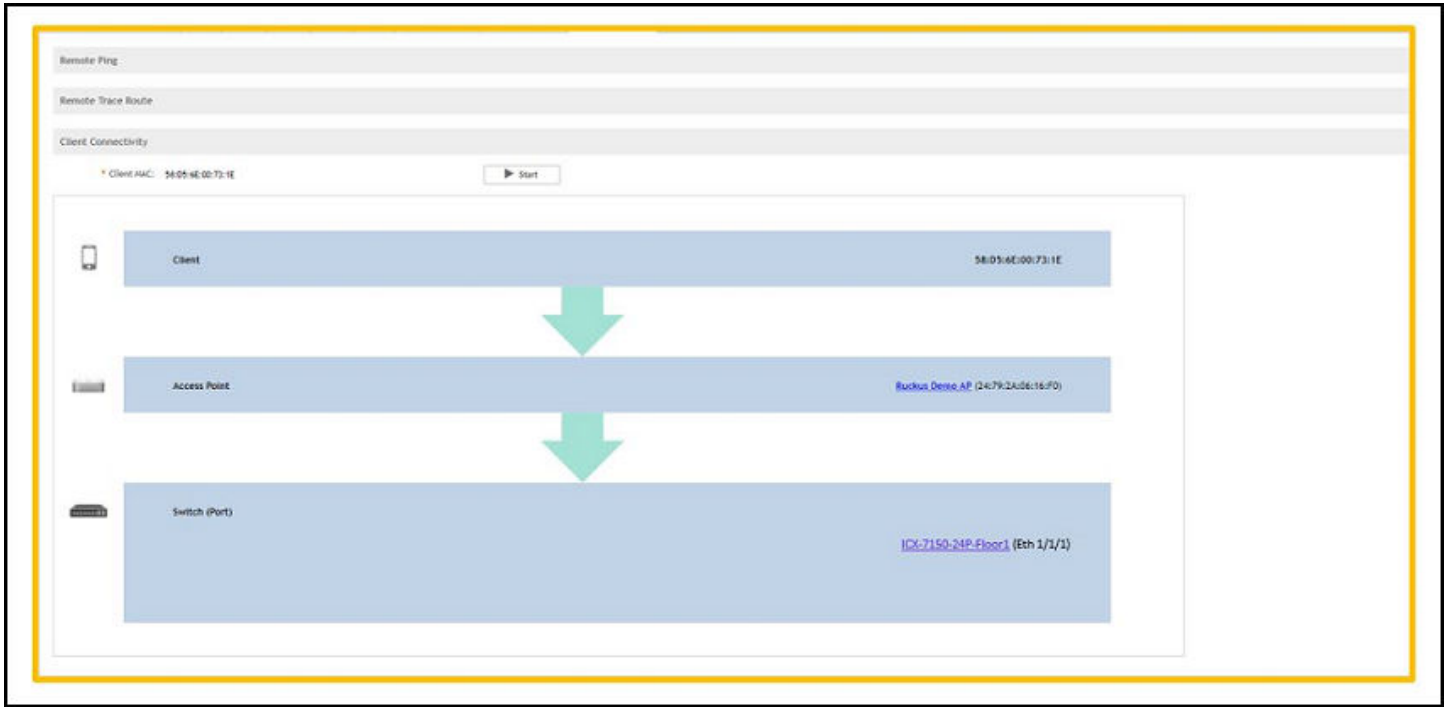
You can troubleshoot issues related to wired and wireless clients connected to the switch at the system level from the **Troubleshooting** tab. You can use Remote operations, Client Connectivity and Custom Events to troubleshoot issues with switches or switch groups.

To access the **Troubleshooting** tab do the following:

1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. In the **Organization** tab, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**.
3. Click **Troubleshooting** tab.

To troubleshoot issues with an AP client, use the MAC address of the client on the **Troubleshooting** tab of a switch or switch group. Once you enter the MAC address of the client, SmartZone displays how the client is connected to the network, including the AP, the switch, and the switch port on which the client MAC is learned. As an example, if a printer is connected to an AP, which in turn is connected to a switch that is managed by a SmartZone controller, you can troubleshoot any connectivity issues between the devices from the **Troubleshooting** tab by providing the MAC address of the printer.

FIGURE 122 Client MAC Search



## Troubleshooting Using Custom Events

You can create custom events to define failure scenario and use them to generate troubleshoot switch issues.

To access the **Switch Custom Events** window do the following:

1. On the menu, click **Monitor > Events and Alarms > Events > Switch Custom Events** to display the **Switch Custom Events** window.

FIGURE 123 Switch Custom Events

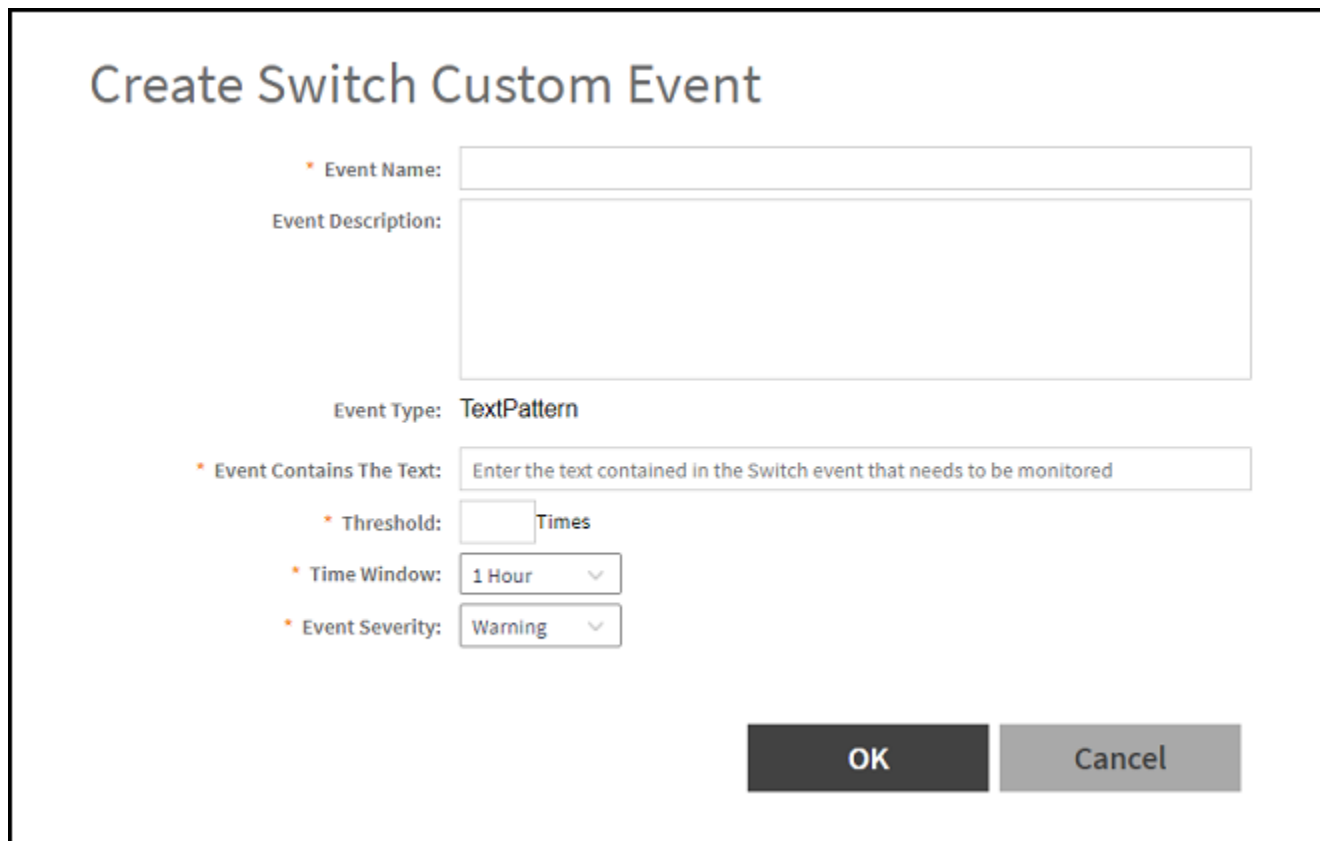
The screenshot shows the Ruckus SmartZone interface for configuring custom events. The top navigation bar includes Monitor, Network, Security, Services, and Administration. The main content area is titled "Switch Custom Events" and contains a table of custom events. The table has the following columns: Event Name, Event Type, Event Severity, Threshold, Event Description, Text Pattern, and Time Window. The table lists several events related to CPU and memory usage thresholds.

Event Name	Event Type	Event Severity	Threshold	Event Description	Text Pattern	Time Window
Warning CPU Usage	CPU	Warning	20	Switch CPU usage is over Warning threshold, 20%	N/A	N/A
Major CPU Usage	CPU	Major	30	Switch CPU usage is over Major threshold, 30%	N/A	N/A
Critical CPU Usage	CPU	Critical	50	Switch CPU usage is over Critical threshold, 50%	N/A	N/A
Warning Memory Usage	Memory	Warning	88	Switch Memory usage is over Warning threshold, 88%	N/A	N/A
Major Memory Usage	Memory	Major	92	Switch Memory usage is over Major threshold, 92%	N/A	N/A
Critical Memory Usage	Memory	Critical	95	Switch Memory usage is over Critical threshold, 95%	N/A	N/A
AISH CPU Usage	TextPattern	Warning	2	CPU USAGE THRESHOLD EXCEEDED	cpu usage threshold exceeded	1 Hour

7 records

2. Click  icon to display the **Create Switch Custom Event** dialog box.

**FIGURE 124** Creating Switch Custom Event



**Create Switch Custom Event**

\* **Event Name:**

**Event Description:**

**Event Type:** TextPattern

\* **Event Contains The Text:**

\* **Threshold:**  Times

\* **Time Window:** 1 Hour ▾

\* **Event Severity:** Warning ▾

**OK** **Cancel**

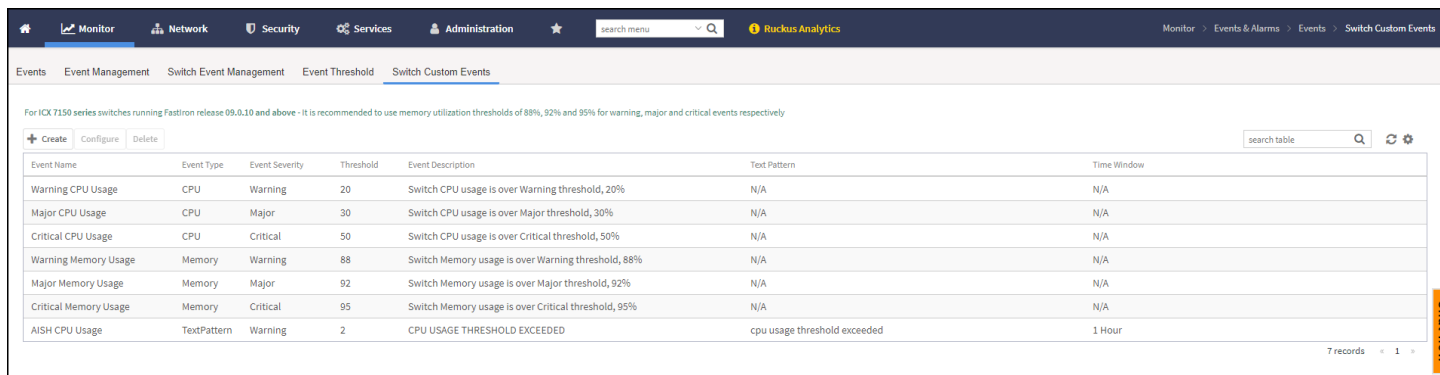
3. Complete the following fields:
  - **Event Name:** Enter the name.
  - **Event Description:** Enter a brief description.
  - **Event Type:** By default, **TextPattern** is selected.
  - **Event Contains The Text:** Enter the text contained in the switch event that needs to be monitored.
  - **Threshold:** Enter the threshold value between 0 to 255.
  - **Time Window:** Select the time from the list.
  - **Event Severity:** Select **Major**, **Critical** or **Warning** status from the list.
4. Click **OK**.

## Working with Switches

### Troubleshooting Switch Issues

For example, you can create a "system is unusable" event with the following settings. Based on this event definition and configuration, if any switch sends this message thrice in one hour, the controller triggers a Custom Event. You can view the "system unavailable" event from the **Switch Custom Events** page. For more information on custom events, refer the topic **Creating Custom Events for ICX Switches** in the *SmartZone Management Guide*.

FIGURE 125 Troubleshooting switch issues through custom events



Event Name	Event Type	Event Severity	Threshold	Event Description	Text Pattern	Time Window
Warning CPU Usage	CPU	Warning	20	Switch CPU usage is over Warning threshold, 20%	N/A	N/A
Major CPU Usage	CPU	Major	30	Switch CPU usage is over Major threshold, 30%	N/A	N/A
Critical CPU Usage	CPU	Critical	50	Switch CPU usage is over Critical threshold, 50%	N/A	N/A
Warning Memory Usage	Memory	Warning	88	Switch Memory usage is over Warning threshold, 88%	N/A	N/A
Major Memory Usage	Memory	Major	92	Switch Memory usage is over Major threshold, 92%	N/A	N/A
Critical Memory Usage	Memory	Critical	95	Switch Memory usage is over Critical threshold, 95%	N/A	N/A
AISH CPU Usage	TextPattern	Warning	2	CPU USAGE THRESHOLD EXCEEDED	cpu usage threshold exceeded	1 Hour

#### NOTE

It is quite common that entry level switches use upto 70-80% of the available memory. You can modify the thresholds for memory usage custom events to a higher limit in such cases.



#### VIDEO


**Switch Custom Troubleshooting Demo** Verify client to WLAN to switch assignment (Switch Client Troubleshooting).

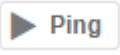
[Click to play video in full screen mode.](#)

## Troubleshooting Using Remote Operations


You can use the **Remote Ping** and **Remote Trace Route** options to identify issues with individual switches.


Follow these steps to troubleshoot switch issues using remote ping and traceroute.


1. On the menu, click **Network > Wired > Switches** to display the **Switches** window.
2. From the system tree, select a **Domain > Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** pane, click the **Troubleshooting** tab.
4. In the **Remote Ping** section, click  to display the **Remote Ping** fields.
5. Complete the following fields:
  - **Target:** Enter the IP address of the destination (target) you are checking.
  - **Packet Size:** Enter the packet size from 0-10000.
  - **TTL (Time to Live):** Enter the Time to Live from 1-255.

- Click the  icon. In the below display window you can view that a packet is discarded from the network.  
The controller pings the switch at the destination IP address provided. As shown in the following example, the results displayed include the number of data packets transmitted, received, and lost and the time required for the controller to ping the switch to establish communication.

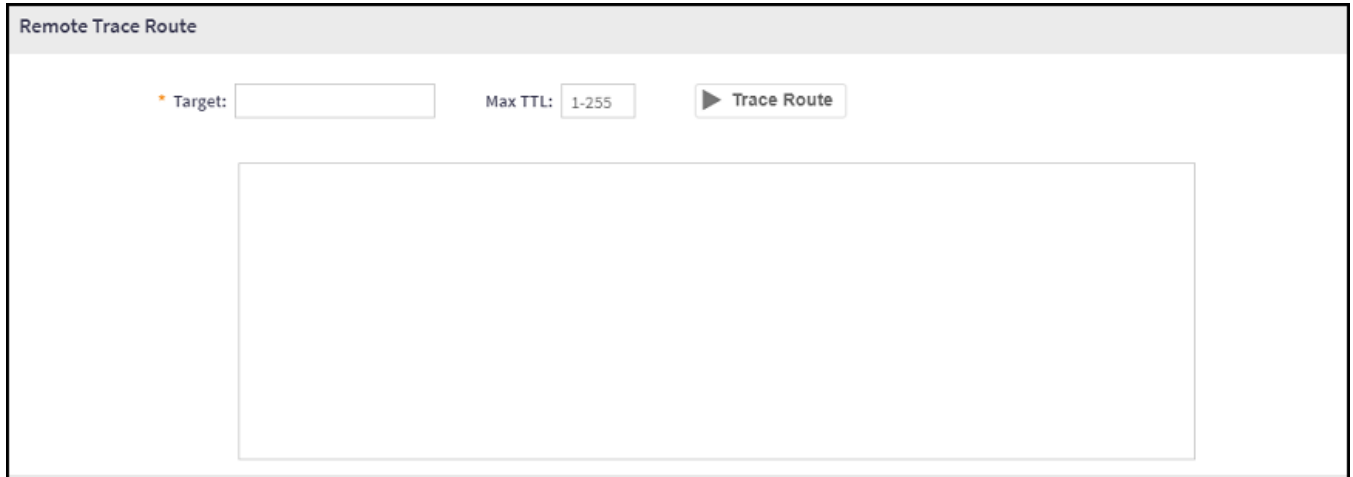
**FIGURE 126** Pinging the switch



- In the **Remote Trace Route** tab, click  to display the **Remote Trace Route** fields.
- Complete the following fields:
  - **Target:** Enter the IP address of the destination (target) you are checking.
  - **Max TTL:** Enter the Maximum Time to Live from 1-255.

9. Click the  icon. In the below display window you can view that a packet is discarded from the network. As shown in the following example, the **Remote Trace Route** page displays the IP address of the hops the packet traverses through the network between the switch and the controller.

**FIGURE 127** Tracing the packet route through the network



10. In the **Blink LED** tab, click  to display the **Blink LED** fields.

**NOTE**

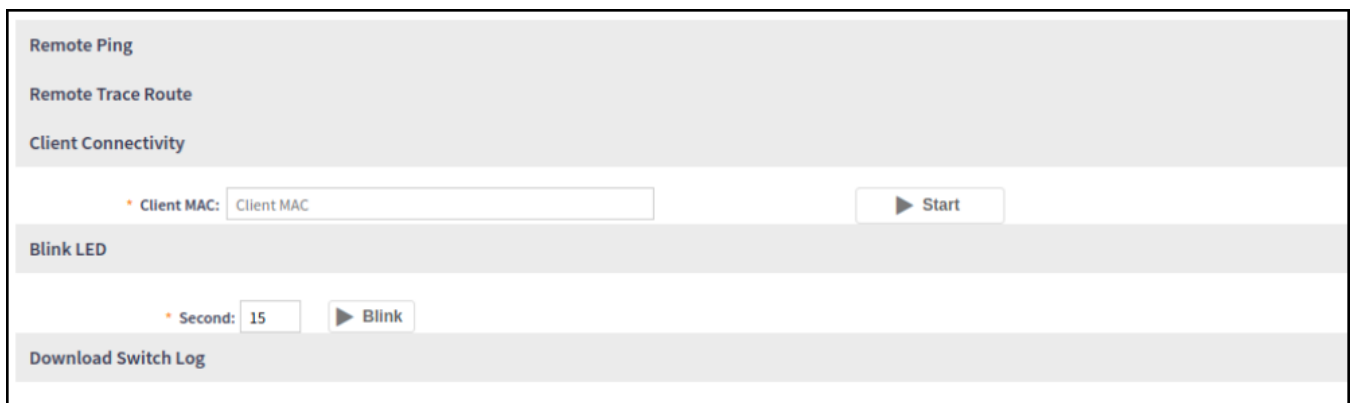
The Blink LED can be applied to either a single switch, or to switch in the stack by selecting an option **All**, or selecting a particular unit-id from the list.

- In the **Seconds** field, enter the time in seconds and click  icon to enable blinking of port LEDs on switches.

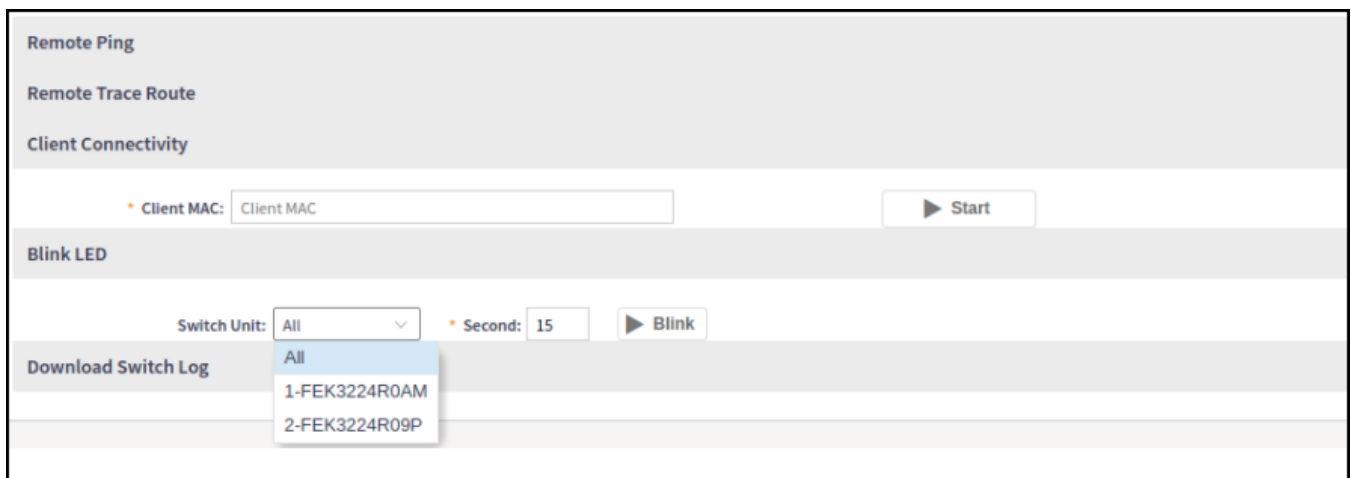
**NOTE**

The value in seconds ranges from 15-120. By default, it is 15.

**FIGURE 128** Applying Blink LED to Single Switch



**FIGURE 129** Applying Blink LED to Switch on Stack




## Cable Testing on ICX Ports

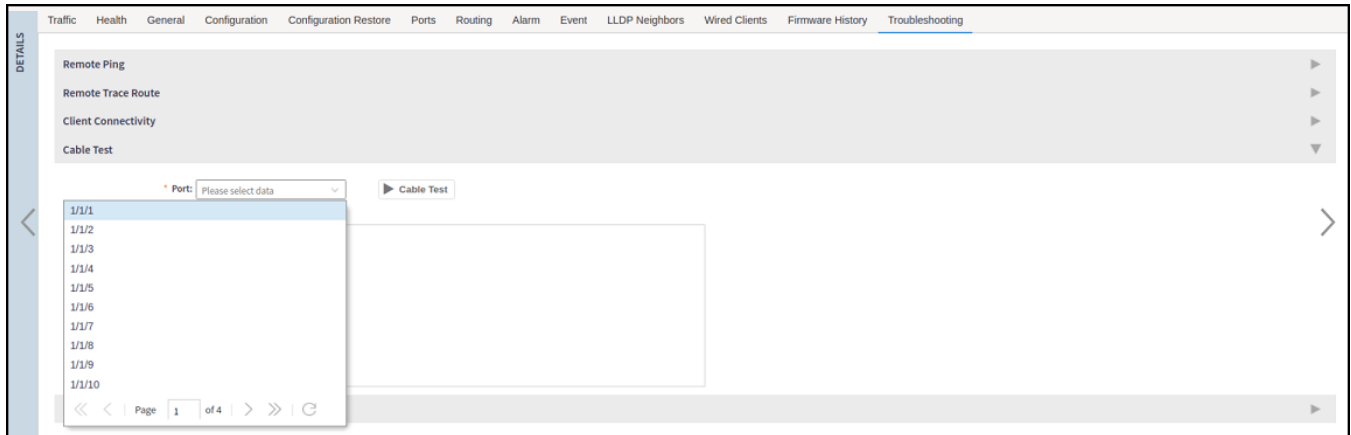
1. From the main menu, click **Network > Wired > Switches** to display the **Switches** window.

## Working with Switches

### Troubleshooting Switch Issues

2. From the system tree, select a **Domain > Switch Group or Switch Group** and select the **Switch**.
3. In the **Details** pane, click the **Troubleshooting** tab.
4. Navigate to the **Cable Test** section, click the  icon to view the **Cable Test** fields.

**FIGURE 130** Clicking Troubleshooting Tab



5. Select a port from the **Port** list.

#### **NOTE**

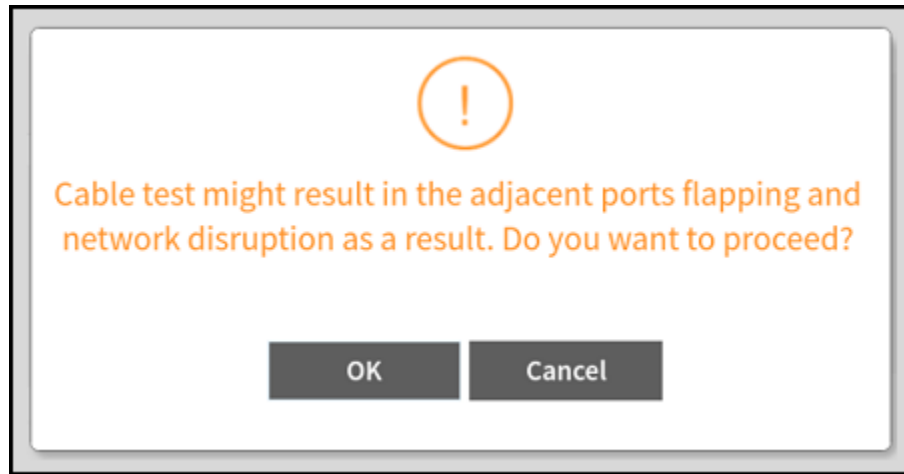
Ensure the port speed is set to **Auto** to execute cable test.

6. Click the  icon.

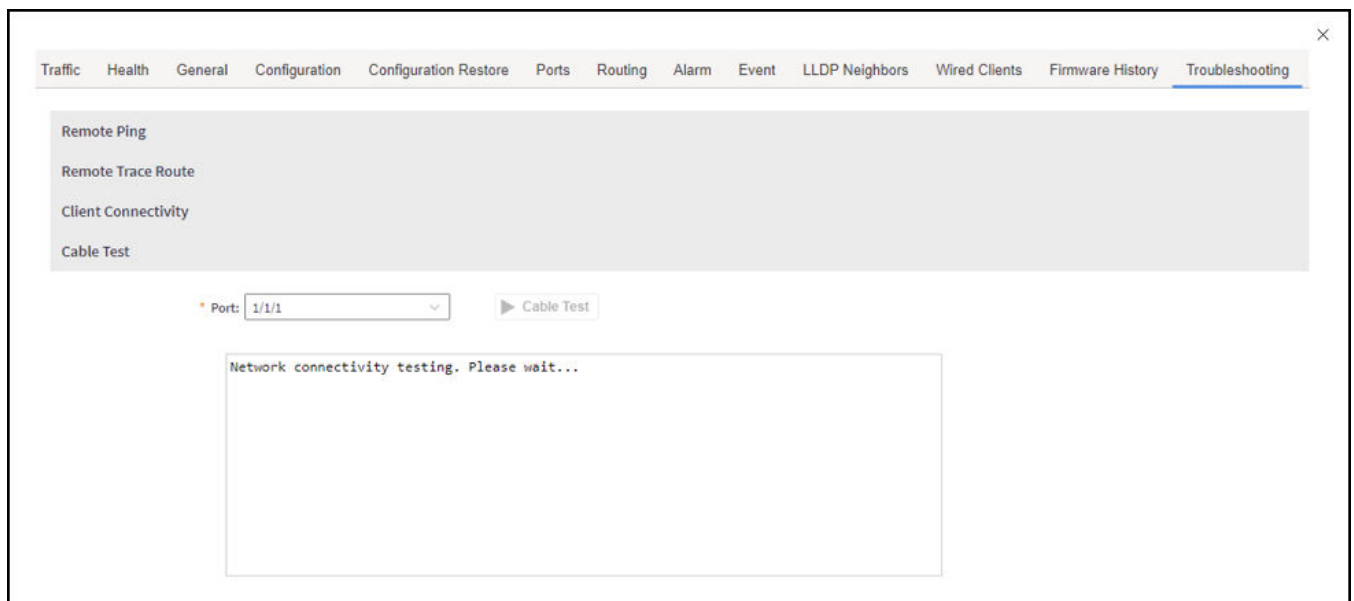


7. A **Cable Test Message** dialog box is displayed, click **OK**.

**FIGURE 131** Warning Message for Confirmation

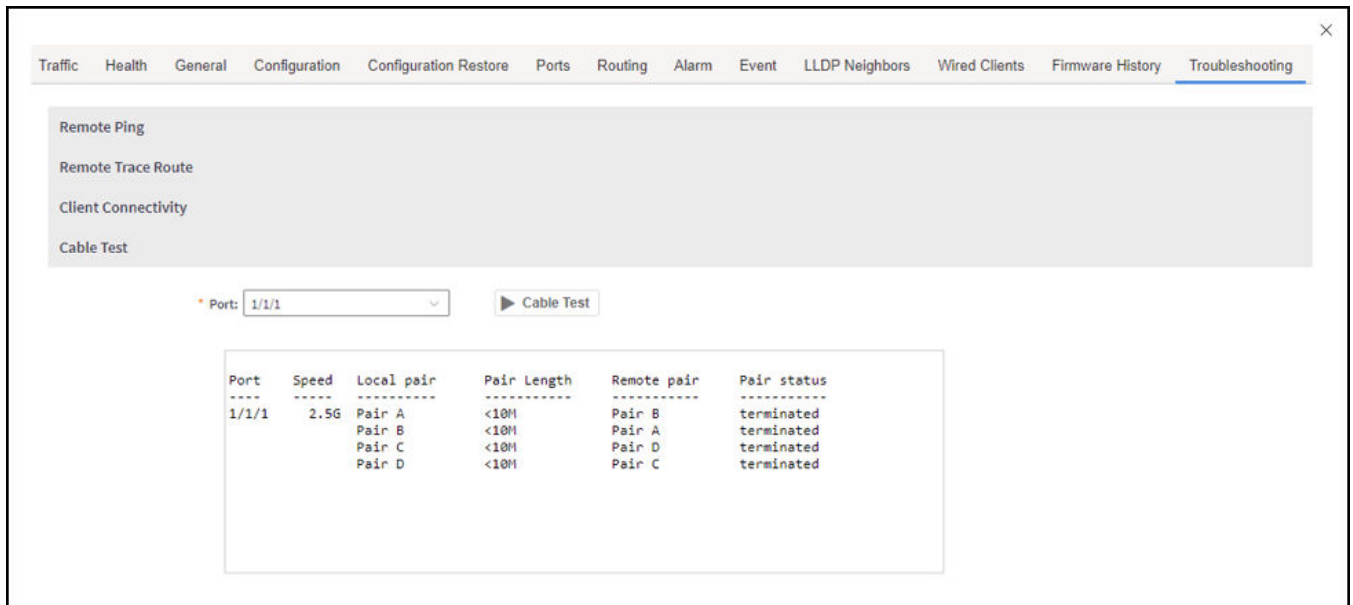


**FIGURE 132** Testing Network Connectivity



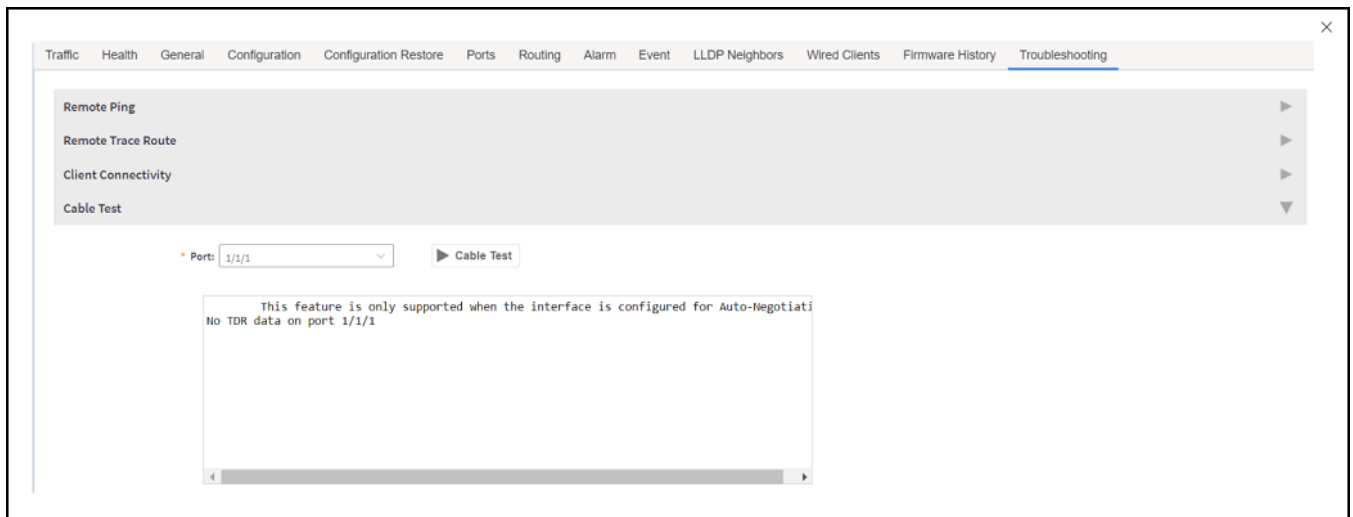
**FIGURE 133** Viewing the Cable Test Report

**Working with Switches**  
Viewing Switches on the Dashboard



- If the selected port has the port speed set to **Fixed**, then an error message is shown as below.

**FIGURE 134** Displaying Error Message



## Viewing Switches on the Dashboard

The wired dashboard displays detailed information about the health of the switch and displays charts illustrating traffic trends.

- On the menu, click **Monitor > Dashboard > Wired** to display the **Dashboard** window.
- In the **Health** tab, click System icon to display the connected switches.

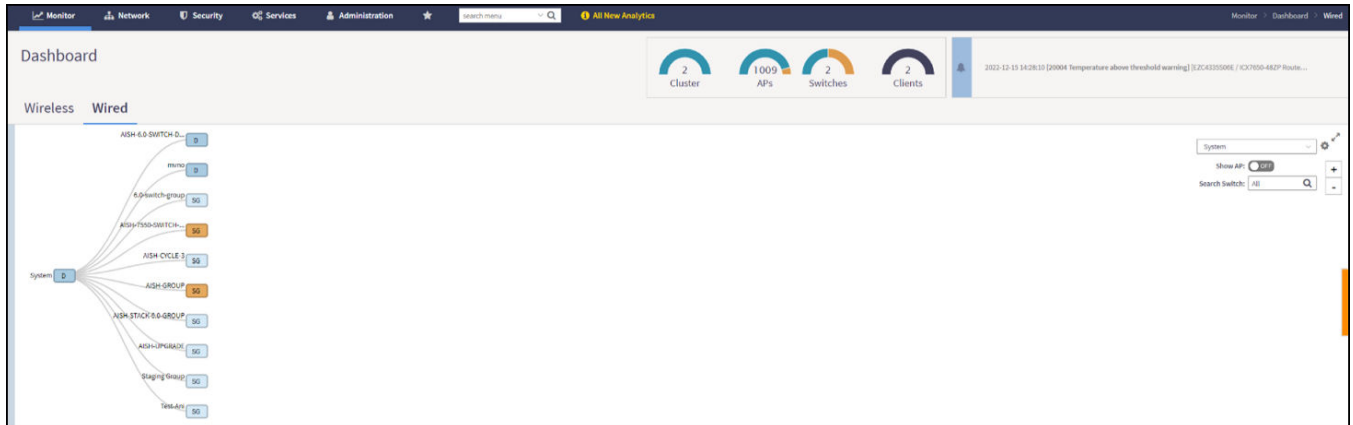
The **Settings-Health Dashboard** page is displayed.

- From the **View Mode** , select either **Topology** or **Ball** view to be displayed on the dashboard.

**FIGURE 135** Viewing Wired Dashboard - Ball



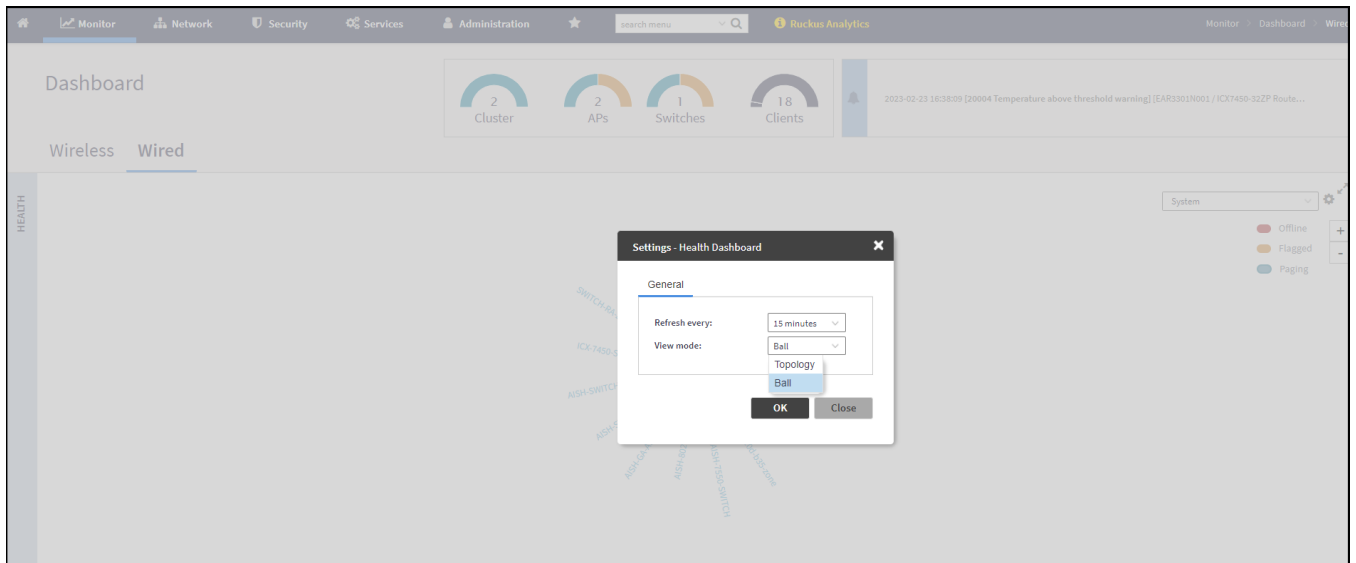
**FIGURE 136** Viewing Wired Dashboard - Topology



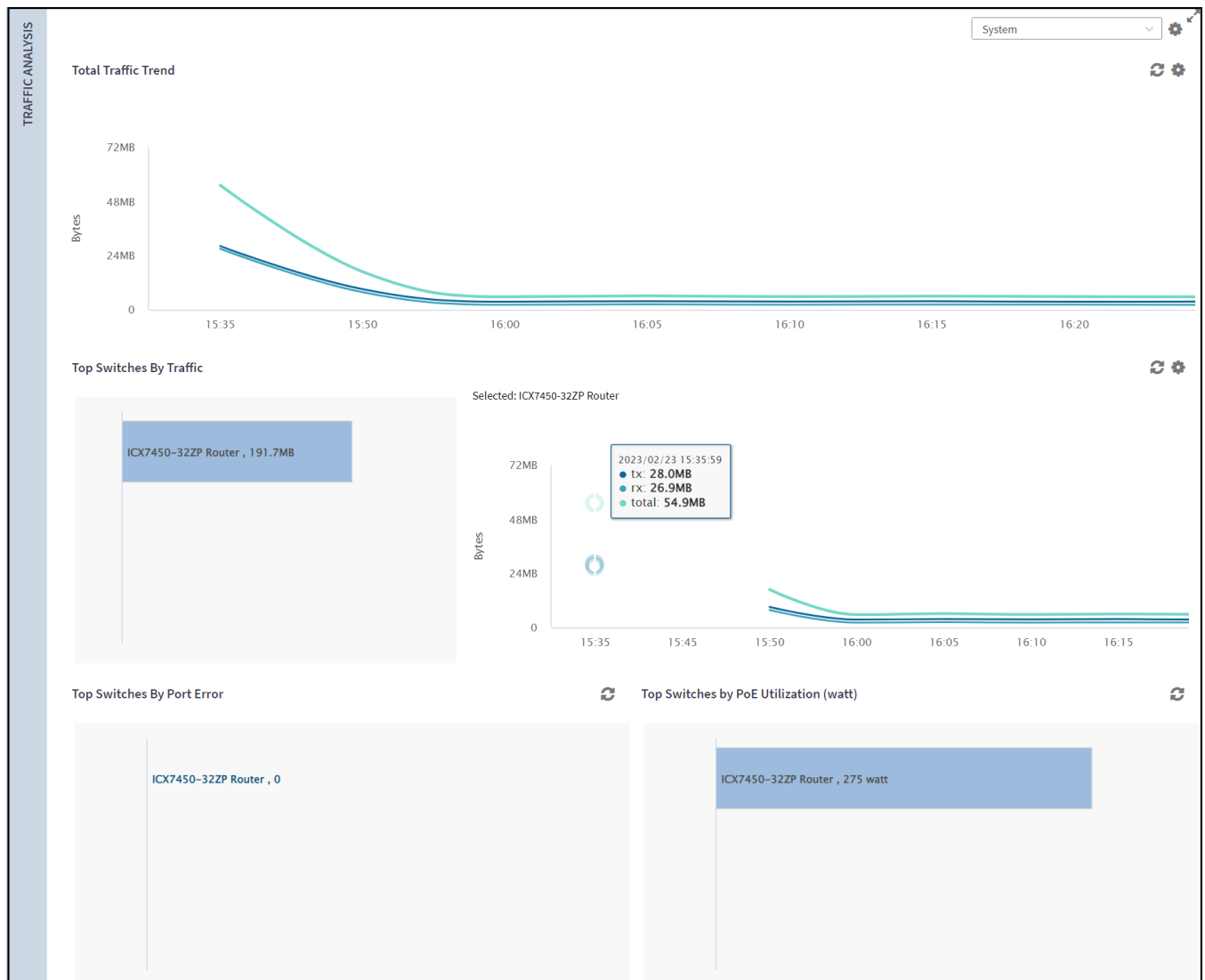
**FIGURE 137** Showing Wired Devices Using Topology View Mode

## Working with Switches

### Viewing Switches on the Dashboard



**FIGURE 138** Viewing Traffic Analysis



The **Health** tab displays the number of switches that are online, offline, and flagged.

The **Traffic Analysis** tab displays the following information:

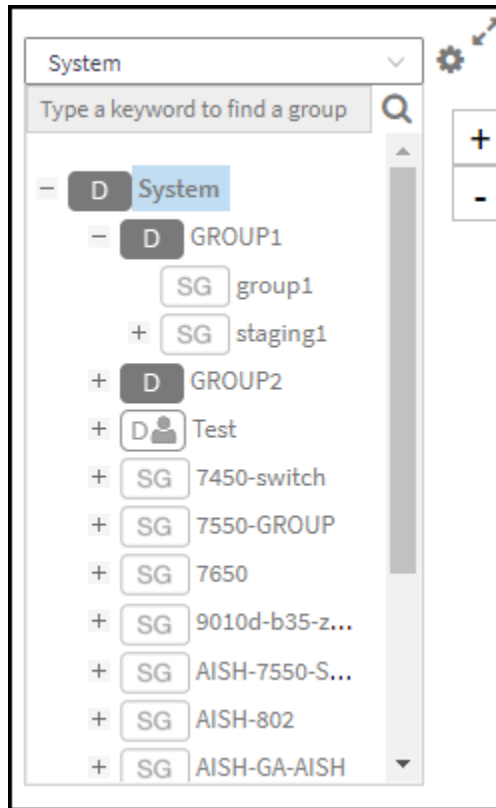
- Total Traffic Trend
- Top Switches By Traffic
- Top Switches By Port Error
- Top Switches by PoE Utilization (watt)

In the topology view mode, the **Health** pane consists of a filter combo box to display domain, sub-domain and switch group in the topology view. If you pause the pointer on a link in the topology view, the highlighted link shows the port and LAG information. If you pause the pointer on a device, the highlighted device shows device information such as name, model, MAC address, and IP address (for the switch only).

**NOTE**

The **Health** dashboard refreshes automatically every 15 minutes to show the latest topology view.

FIGURE 139 Showing Elements on the Health Dashboard





© 2024 CommScope, Inc. All rights reserved.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
<https://www.commscope.com>