DEPLOYMENT GUIDE

Ruckus SmartZone 5.1.2 Deployment Guide — ICX Switch Management

Supporting SmartZone 5.1.2

Part Number: 53-1005646-01
Publication Date: 6 December 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Introduction to SmartZone **4**
SmartZone Overview 4
SmartZone Essentials (SZ100 and vSZ-E) 4
SmartZone High Scale (SZ300 and vSZ-H) 4
Setting Up SmartZone (Physical or Virtual) 5
Displaying SmartZone OS Version Information 6
Downloading the Latest SmartZone OS 7
Upgrading the SmartZone OS 7

Device Bringup on SmartZone **8**
Bringing Up the ICX Switch on SmartZone 8
Configuring SZ IP Address: Automated (DHCP Option 43) 9
Configuring SZ IP Address: Manually 9
Switch Group and Registration Management 10

Use Cases **12**
ICX Switches Using SmartZone 12
Configuration 13
Monitoring 23
Reporting 32
Troubleshooting 40

Syslog **43**

Conclusion **44**

References **45**

Introduction to SmartZone

SmartZone Overview

SmartZone (SZ) provides the flexibility and scalability to meet the management needs of all deployments. SmartZone network controllers provide full Zero Touch Provisioning (ZTP), management, and configuration control of Ruckus access points (APs) and ICX switches. SmartZone is offered as both physical and virtual controllers. The controllers come in different versions based on the scale of the supported network.

TABLE 1 SmartZone Comparison

Audience	Physical Controller	Virtual Controller
Small- to medium-sized deployments	SZ100	Virtual SmartZone Essentials (vSZ-E)
Large-scale deployments	SZ300	Virtual SmartZone High Scale (vSZ-H)

SmartZone Essentials (SZ100 and vSZ-E)

The following table shows the scale limits on the SmartZone Essentials platform.

TABLE 2 SmartZone Essentials Limits

1-2 Nodes		3 Nodes		4 Nodes	
Max. Number of APs	Max. Number of Switches	Max. Number of APs	Max. Number of Switches	Max. Number of APs	Max. Number of Switches
Up to 1,024	Up to 200	Up to 2,048	Up to 400	Up to 3,000	Up to 600

The maximum numbers are applicable for AP-only or ICX switch-only deployments. In a mixed deployment (AP and switch), the maximum number of APs and switches will change.

An AP-to-switch ratio of 5:1 is applicable in mixed deployments.

Example 1: On a single-node SZ100, if 100 switches are added, then the room left for APs is (200–100) x 5 = 500 APs

Example 2: On a 3-node SZ100 cluster, if 1,500 APs are added, then the room left for switches is (2,048–1,500)/5 = 110 switches

SmartZone High Scale (SZ300 and vSZ-H)

The following table shows the scale limits on the SmartZone High Scale platform.

TABLE 3 SmartZone High Scale Limits

1-2 Nodes		3 Nodes		4 Nodes	
Max. Number of APs	Max. Number of Switches	Max. Number of APs	Max. Number of Switches	Max. Number of APs	Max. Number of Switches
Up to 10,000	Up to 2,000	Up to 20,000	Up to 4,000	Up to 30,000	Up to 6,000

The maximum numbers are applicable for AP-only or ICX switch-only deployments. In a mixed deployment (AP and switch), the maximum number of APs and switches will change.

An AP-to-switch ratio of 5:1 is applicable in mixed deployments.

Example 1: On a single-node SZ300, if 1,000 switches are added, then the room left for APs is (2,000–1,000) x 5 = 5,000 APs

Example 2: On a 3-node SZ300 cluster, if 15,000 APs are added, then the room left for switches is (20,000–15,000)/5 = 1,000 switches

Setting Up SmartZone (Physical or Virtual)

Consult the following links for the quick setup guides.

TABLE 4 Quick Setup Guides

SZ100	https://support.ruckuswireless.com/documents/2817-smartzone-100-quick-setup-guide
SZ300	https://support.ruckuswireless.com/documents/2803-smartzone-300-quick-setup-guide
Virtual SmartZone (vSZ)	https://support.ruckuswireless.com/documents/2818-virtual-smartzone-quick-setup-guide-vsz

Consult the following links for the administration guides.

TABLE 5 Administration Guides

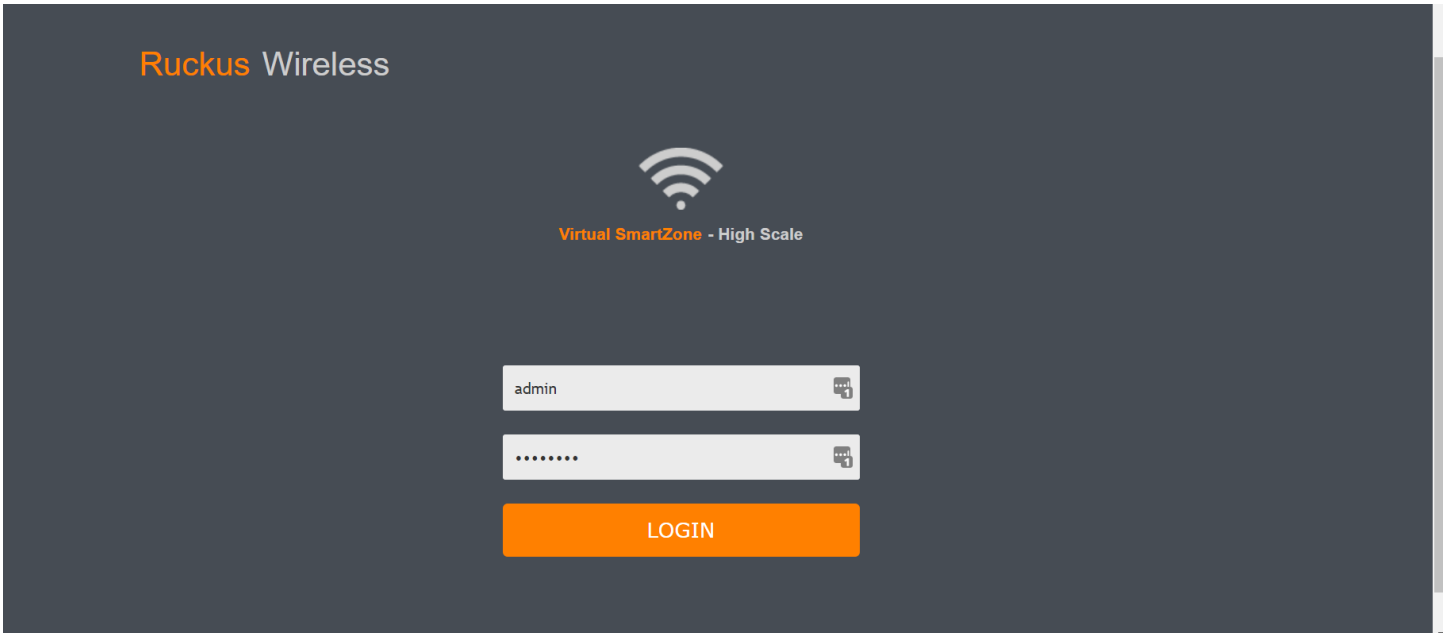
SZ100, SZ300, and vSZ	https://support.ruckuswireless.com/documents/2959-smartzone-5-1-2-software-documentation-sz100-sz300-vsz
Virtual SmartZone (vSZ) and vSZ-D	https://support.ruckuswireless.com/documents/2819-virtual-smartzone-getting-started-guide-vsz-vsz-d

SmartZone port dependencies: https://support.ruckuswireless.com/article_attachments/kA250000000PHSKCA4?attachment_index=0.

> **NOTE**
> To access SmartZone, use a web browser and open an HTTPS connection to the SmartZone controller IP address with port number 8443.

Using the web interface to access SZ: https://10.176.217.100:8443/wsg/

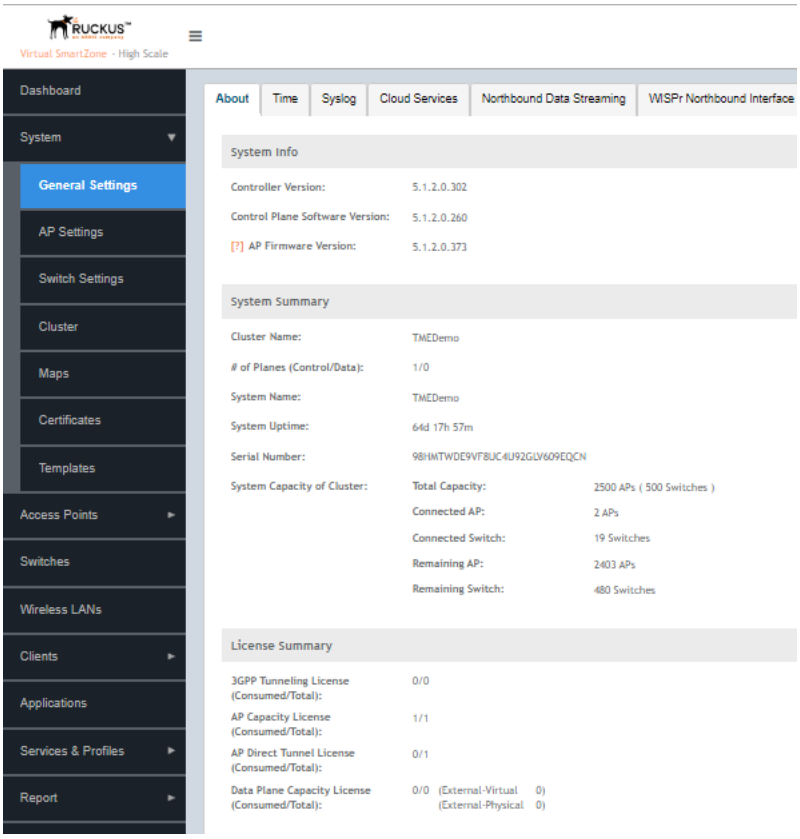
FIGURE 1 SmartZone Login Page



Displaying SmartZone OS Version Information

From the navigation pane, select **Systems** > **General Settings**. On this page, you can see the SmartZone OS version under **System Info**.

FIGURE 2 SmartZone Controller Version



Downloading the Latest SmartZone OS

To get the latest version of the software, visit the Ruckus Support website at https://support.ruckuswireless.com/product_families/11-smartzone-sz. Navigate to your SmartZone model and click **Software Downloads**. Click the link to the XIMG file. You will be prompted to enter a username and password to grant access to the software.

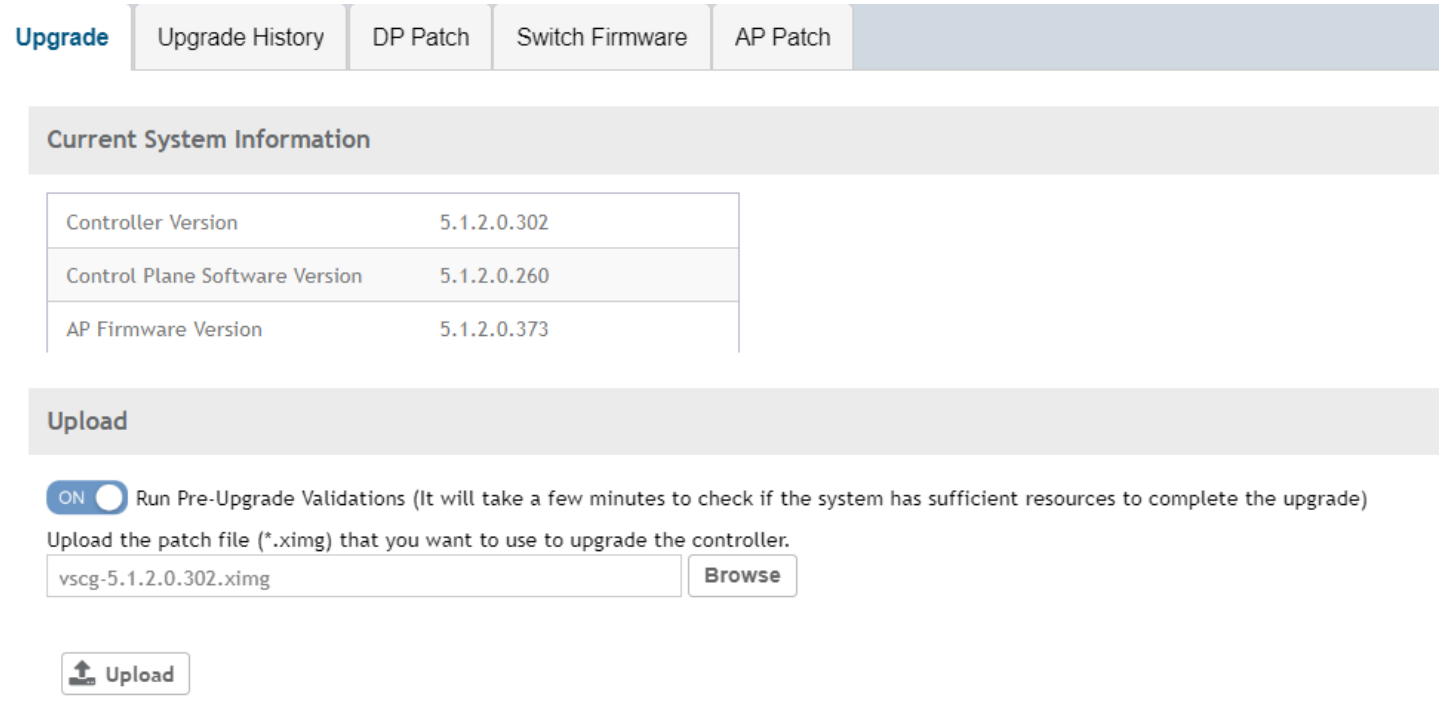
FIGURE 3 Downloading the SmartZone OS

SmartZone 5.1.2.0.302 (GA) Software Release (SZ300)	5.1.2.0.302	XIMG	2019-09-13

Upgrading the SmartZone OS

Once you have the desired XIMG file on your local server, from the SmartZone web interface navigation pane, select **Administration** > **Upgrade**. Use the **Browse** button to locate the XIMG file and click **Upload**. After the pre-upgrade validations are complete, follow the instructions to complete upgrading SmartZone.

FIGURE 4 Upgrading SmartZone



When the upgrade process is complete (about 30 to 40 minutes), you are logged out of SmartZone and a login page is displayed.

Verify whether the upgrade was successful by navigating to **Administration** > **Upgrade** and checking for the **Controller Version** under **Current System Information**.

Device Bringup on SmartZone

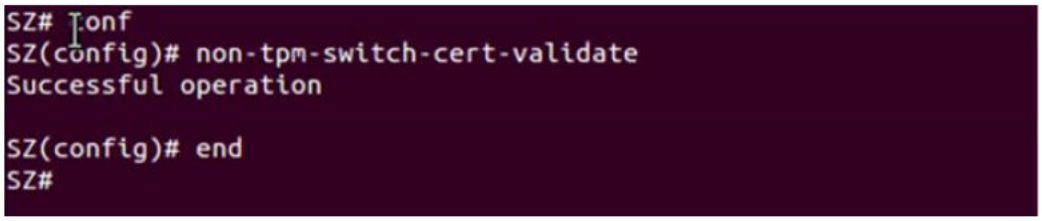
Bringing Up the ICX Switch on SmartZone

The following ICX switch models can be managed from SmartZone:

- ICX 7150
- ICX 7250
- ICX 7450
- ICX 7650
- ICX 7750
- ICX 7850

NOTE
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.

FIGURE 5 Entering non-tpm-switch-cert-validate Command on SmartZone Console



ICX 7150, ICX 7650, and ICX 7850 devices are shipped with embedded certificates that are used for authentication with SmartZone.

To manage the ICX switches using SmartZone, the ICX switches must run the FastIron 08.0.90d Unified Forwarding Image (UFI) or later, and the SmartZone OS version must be 5.1.1 or later. Be sure to download the appropriate software version from https://support.ruckuswireless.com and upgrade the devices.

> **NOTE**
> The recommended software version for ICX switches is the FastIron 08.0.90d UFI or later, and for SmartZone, the version is 5.1.1 or later.

The ICX switches initially look for SmartZone using the controller IP address. Once a switch is able to reach the SmartZone controller, SmartZone begins the process of registering the switch and initiates a secured SSH connection between the two. For this process to take place, there are three basic criteria that must be satisfied:

1. The switch must have a management IP address.
2. The switch must be configured with the SmartZone controller IP address that it must initially contact.
3. There must be proper IP connectivity between the switch and SmartZone.

The switches can be configured with an IP address and the controller IP address either manually or using the recommended automated method (DHCP Option 43).

Configuring SZ IP Address: Automated (DHCP Option 43)

1. Configure the DHCP server to send an **option43** with the SmartZone IP address along with the switch IP address.
2. Configure one of the ICX switches in the network to act as a DHCP server to issue an **option43** with the SmartZone IP address and switch IP address.

> **NOTE**
> To configure the DHCP server with the **option43** option, you must enter the SZ IP address in the hex format. Use the following link to generate the **option43** hex: http://shimi.net/services/opt43/index.php.

Configuring SZ IP Address: Manually

Configure the ICX switch management IP address either manually or using DHCP. Preconfigure the SmartZone IP address on the switch using the **manager active-list x.x.x.x** command. You can do this by way of a console, SSH, or Telnet connection. Also, manually configure a static IP address for the switch.

> **NOTE**
> For ICX switches running a software version prior to FastIron 08.0.92, use the **sz active-list x.x.x.x** command.

Switch Group and Registration Management

Once the switches have contacted the SmartZone controller and SmartZone has registered the switches, they are added to buckets known as the switch group. By default, the SmartZone OS comes with a default switch group. You have the option to create as many switch groups as you want, and you can define rules for each of these switch groups, known as "registration rules." This way of grouping switches to different buckets helps in managing, configuring, and monitoring the switches more efficiently.

The switch groups can be seen listed under the **Switches** tab on the SmartZone interface. There is a slight difference between the default groups based on which SmartZone is being used.

vSZ-E and SZ100

The switch group is called "Default group" under the **Switches** tab. You can add configurations to and manage switches that are placed in this group.

vSZ-H and SZ300

The switch group is called "Staging Group." In this group, the switches cannot be managed or configured. A switch in this group must be manually or automatically moved to a user-defined group; only then will the switch come online on SmartZone and then can be managed and configured as desired. You can manually drag and drop a switch from one group to another, or use the automated way of defining registration rules for different user groups and have the switches automatically placed under those groups during the initial switch registration process.

NOTE
The vSZ-H and SZ300 users must move the switches to a user-defined switch group from the Staging Group, and only then will the SZ connection be established.

Once the switches have successfully registered with SmartZone, you can verify the same on the switch console.

FIGURE 6 Verifying SmartZone Registration

```
7250-U30#show sz status

============    SZ Agent State Info     ===================
Config Status: None     Operation Status: Enabled
State: SZ SSH CONNECTED     Prev State: SZ SSH CONNECTING    Event: NONE
```

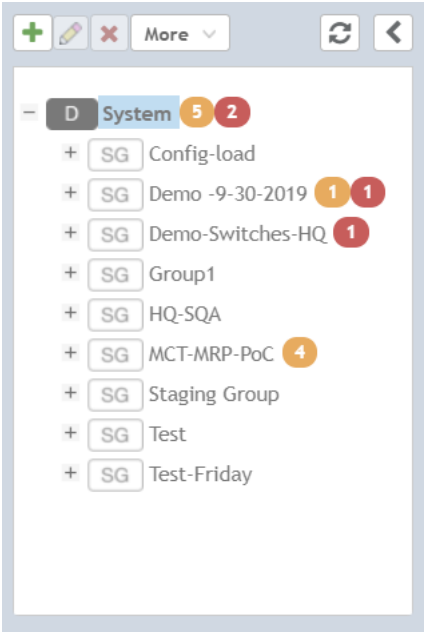
NOTE
The recommended way to manage a switch on any SmartZone controller is to create a user-defined switch group and define registration rules for that group. By doing so, you can control two important things:

- The switches are placed under different groups, which is an efficient way to manage.
- Predefined configurations at the group level are pushed to the switches.

Complete the following steps to define registration rules.

1. Navigate to the **Switches** tab and create a switch group under a domain.

FIGURE 7 Creating a Switch Group



2. Navigate to **System** > **Switch Settings** to access the rules.
3. Under **Switch Registration**, click **Create**, and select the group name from the list and pick the rule type.

   There are multiple ways in which you can define a registration rule.

   a. IP address range: All switches with a management IP address within the defined range will be classified under this rule.
   b. Subnet: All the switches with a management IP address in a particular subnet will be defined by this rule.
   c. Model number: Switch groups can be differentiated based on the switch model numbers.

   You can define as many registration rules as you want, and can assign a priority to each rule that determines the order of precedence.

   For example, there are multiple rules that are defined with both the IP address range and the model number. The priority is set for each of these rules with 1 being the highest precedence. If an ICX7250-48P model switch is detected by SZ and has a management IP address of 10.176.113.142, then this switch is added to the Demo-Switches-HQ group (not the MCT-MRP-PoC group) because of the first rule.

FIGURE 8 Example of Rule Priority



Registration rules help you define the layout of the entire network and easily classify the switches into multiple manageable groups. Once the groups are formed, you can apply a configuration at the group level. But, to upgrade, you must select the required switches in a particular switch group and then schedule a firmware upgrade.

4. If you already have a rule and want to edit it, navigate to **System** > **Switch Settings**, select the rule, and click **Configure**.
5. If you have multiple rules and want to reassign priorities, select a rule and click **Up** or **Down**. Once you have rearranged the rules, click **Update Priorities**.

Use Cases

ICX Switches Using SmartZone

SmartZone is a management platform for both wired and wireless Ruckus devices. The focus here is what can be done with the ICX switches using SmartZone.

What are some of the most popular use cases of configuring, monitoring, reporting, and troubleshooting an ICX switch using SmartZone?

Configuration

In Zero Touch Provisioning (ZTP) of ICX switches, you can bring up a new factory default ICX switch on SmartZone, group it based on registration rules, and configure some popular features such as DNS, VLANs, ACLs, static routes, and so on on the switches automatically. The configuration can be made specific to a series of switches or it can be defined to a particular model in a given series. As of SmartZone release 5.1.2, you can define configuration to a particular model only for tagging or untagging a VLAN port. For example, a configuration can be added to "ICX7150" or it can be made specific to "ICX7150-48P".

Once these switches are on SmartZone and have the group-level configuration, you may want to add some switch-specific configuration, such as adding a VLAN to one particular switch in a switch group. You can also access a particular switch and add port-level configurations, such as enabling or disabling LLDP, configuring a Link Aggregation Group (LAG), and adding specific ports to the LAG. These examples are displayed under the switch-specific use case.

SmartZone offers an option to schedule a particular date and time to make these configurations to minimize any disruption to the service.

If you have multiple devices all running a base configuration plus or minus some features, then you can configure one of the switches with the common configuration and copy it to all the other switches. While copying the configuration to other switches, you have the option to make changes to the configuration file as required and load it to the new switch.

Stack management is critical to ICX switches. You can find use cases to add an existing stack of ICX switches to be managed by SmartZone, and to form a stack from a list of standalone switches that are already registered to SmartZone.

Monitoring

SmartZone provides various ways to monitor the health of ICX switches. Events and alarms are provided by default and you can also add custom events. SmartZone allows you to set threshold limits to three different severity levels and, based on how often the events are triggered in a given period of time, SmartZone can take an action and send a notification in the form of an email message or SNMP trap.

Reporting

SmartZone gives you the ability to create rules that generate a switch traffic report for a single switch or a group of switches. This rule can be customized further to generate the report immediately or schedule it to run at a particular time. The generated report can be handled in three different ways: use the default option to save the report on the local database, send an email message, or send it to an external FTP server.

Troubleshooting

In a multilocation deployment, the ICX switches and the Ruckus APs can be part of multiple different networks. SmartZone provides troubleshooting tools to check network connectivity without actually connecting to each and every network. You can test the connections remotely from a centralized interface. If you see a MAC address in SmartZone and are not sure where that particular device is connected, the client connectivity tool is helpful because it draws a map from the client to the switch with port numbers. In this fashion, you can easily locate a specific device in a large-deployment scenario.

Configuration

The configuration use cases answer some of the following questions:

- How to bring up a factory default switch on SmartZone?
- How to add a configuration that is specific to a switch?
- How to change a port-level configuration?
- How to apply a template configuration on one switch to many switches?
- How to add a stack of ICX switches to SmartZone?
- How to form a stack of ICX switches on SmartZone?

Zero Touch Provisioning (ZTP) of ICX Switches

You can bring up a factory default switch on SmartZone and preconfigure parameters based on network requirements.

The switch must have no configuration on it, and usually a newly unboxed switch has no stored configuration. If the switch has any stored configuration, you must set it back to factory default mode.

Complete the following steps to perform a factory reset using the Reset button.

NOTE
Performing a factory reset with the Reset button is applicable for FastIron 08.0.70 and later.

1. Remove power from the switch.
2. Press and hold the Reset button and apply power to the switch.
3. Release the Reset button after all of the system LEDs flash amber.

Complete the following steps to perform a factory reset using the serial console or SSH connection.

1. Enter the **erase system factory-default** command.
2. Confirm the reset and the switch will reboot.

NOTE
The recommended software version for ICX switches is FastIron 08.0.90d or later and for SmartZone, the version is 5.1.1 or later.

Complete the following steps to bring up a factory default switch.

1. Power on the switch and load the recommended software version code on the ICX switch.
2. The ICX switches must be configured with the SmartZone IP address and the address must be reachable. There is more than one way this can be achieved on an ICX switch.

   Automated:

   a. Configure a DHCP server to send an **option43** with the SZ IP address along with the IP address.
   b. Configure one of the ICX switches in the network to act as a DHCP server to issue an **option43** with the SZ IP address.

   NOTE
   To configure the DHCP server with **option43**, you must enter the SZ IP address in the hex format. Use the following link to generate the **option43** hex: http://shimi.net/services/opt43/index.php.

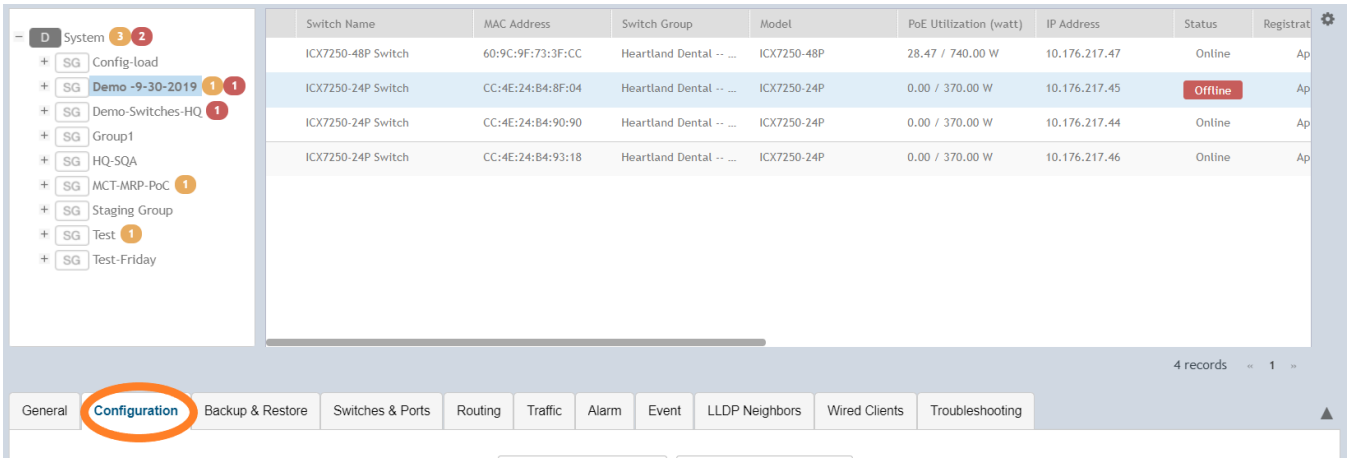
   Manual:

   Preconfigure the SZ IP address on the switch using the **manager active-list x.x.x.x** command. You can do this by way of a console, SSH, or Telnet connection.

   NOTE
   For ICX switches running a software version prior to FastIron 08.0.92, use the **sz active-list x.x.x.x** command.

3. Create a switch group (optional for vSZ-E and SZ100, but recommended). Navigate to **Switches** and create a group under an existing domain.
4. Create a registration rule for this switch group so that when the new switches are registered on SZ, they are automatically placed in this switch group and the group-level configurations are applied to the switches. Refer to vSZ-H and SZ300 on page 10 and follow steps 2 through 5.
5. Select the group created in the previous step and click the **Configuration** tab.

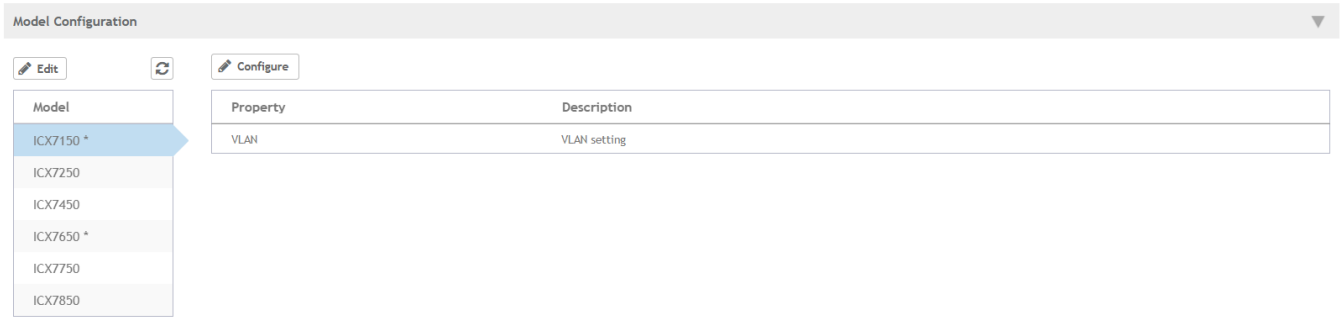
FIGURE 9 Configuration Tab



6. Define a common configuration. As of SmartZone version 5.1.2, DNS configuration is supported, which is provisioned on all the switches that join this particular switch group.
7. To define a model-specific configuration, navigate to **Switches**, select the desired switch group, and click **Configuration**. Under **Model Configuration**, select the model from the list provided, and click **Configure**. At this level, you can configure ACLs, VLANs, and static routes.

   For example, the following figure shows a VLAN configuration for an ICX 7150 switch. When SZ detects and registers an ICX 7150 switch to this particular switch group, a VLAN defined here is programmed automatically. This rule is specific to the ICX 7150. You must define rules for all the desired models.

FIGURE 10 Model Configuration Example



NOTE
The common and model-level configuration takes effect on a switch that has no prior user-defined configuration.

Adding a Switch-Specific Configuration

You can add a configuration that is specific to a switch and change the port-level configuration.

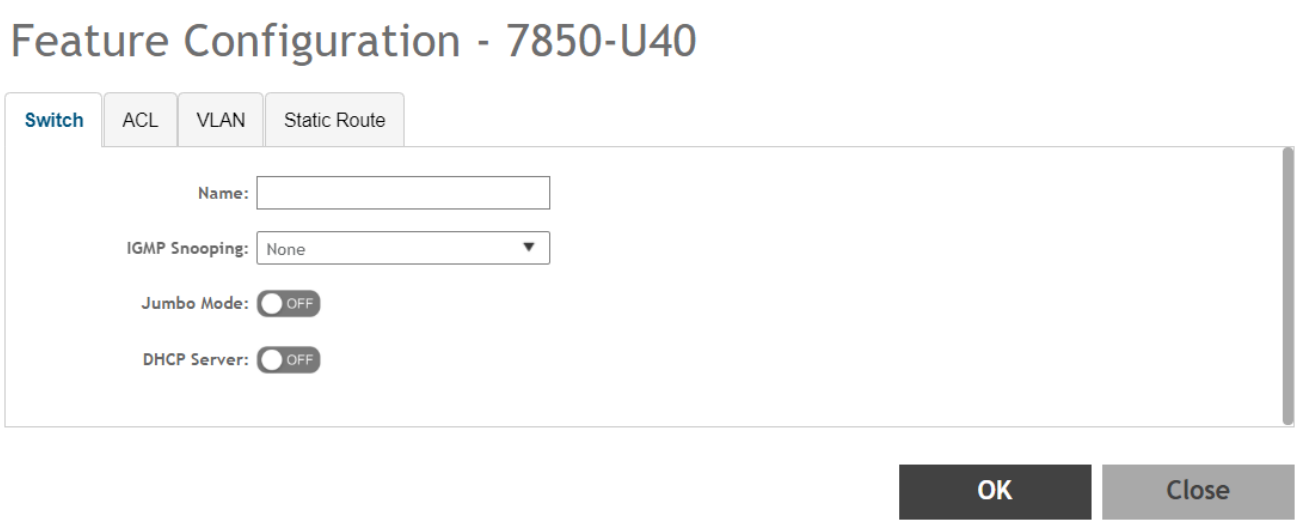
Once the switch is registered with SZ, you can add a switch-specific configuration.

NOTE
Switch-specific configuration is allowed for switches only after they are registered with SZ.

1. Navigate to **Switches** and select the desired switch group, and then the desired switch.
2. In the **Configuration** tab, select the property you want to configure. The options are **Switch Specific**, **ACL**, **VLAN**, and **Static Route**.
3. In **Switch Specific**, you are able to configure the following items:
   - Switch hostname
   - Enable or disable switch global IGMP snooping
   - Enable or disable Jumbo forwarding mode
   - Enable or disable a DHCP server

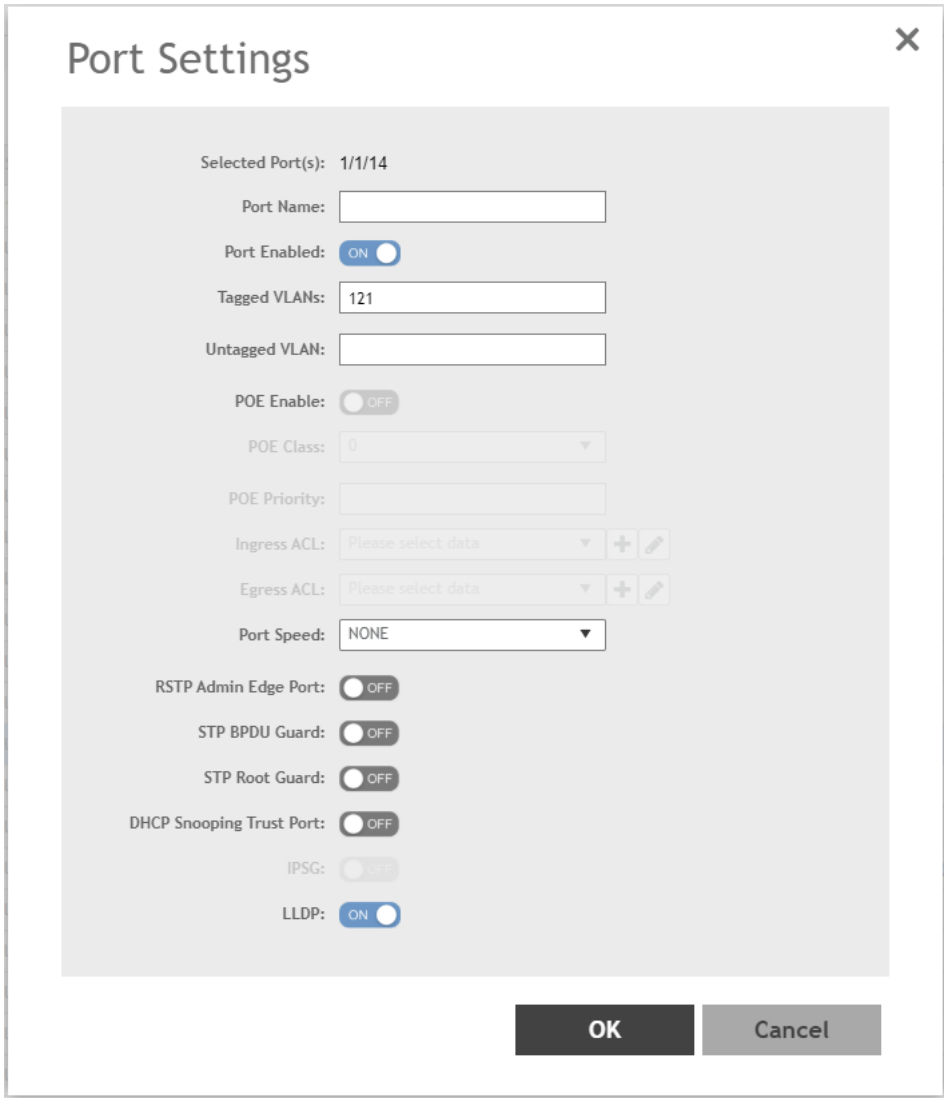
   NOTE
   It is recommended to use the group-level configuration options for adding ACLs, VLANs, and static routes.

FIGURE 11 Switch-Specific Configuration



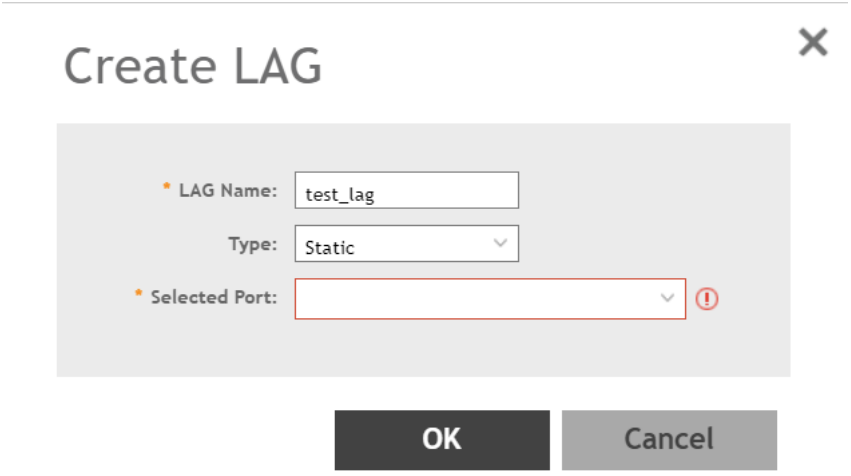
4. You can configure many features at the port level of a particular switch. To do so, navigate to **Switches** and select the desired switch group.
5. From the desired switch group, select the switch, and click **Ports**.
6. In **Port Details**, select the port you are interested in and click **Configure**.
   - If you want to add a new VLAN to the switch apart from the ones defined in the model configuration, then under **Port Settings**, add the required port as a tagged or untagged member of the new VLAN.
   - For an existing VLAN, you can change the membership of a particular port using this dialog box.
   - Enable or disable LLDP at the port level. By default, LLDP is enabled.

FIGURE 12 Port Settings Dialog Box



- Create static or dynamic LAGs on a switch under the port settings.
- If working with a stack, you can form a LAG and select ports from any switch in the stack from the **Selected Port** list.

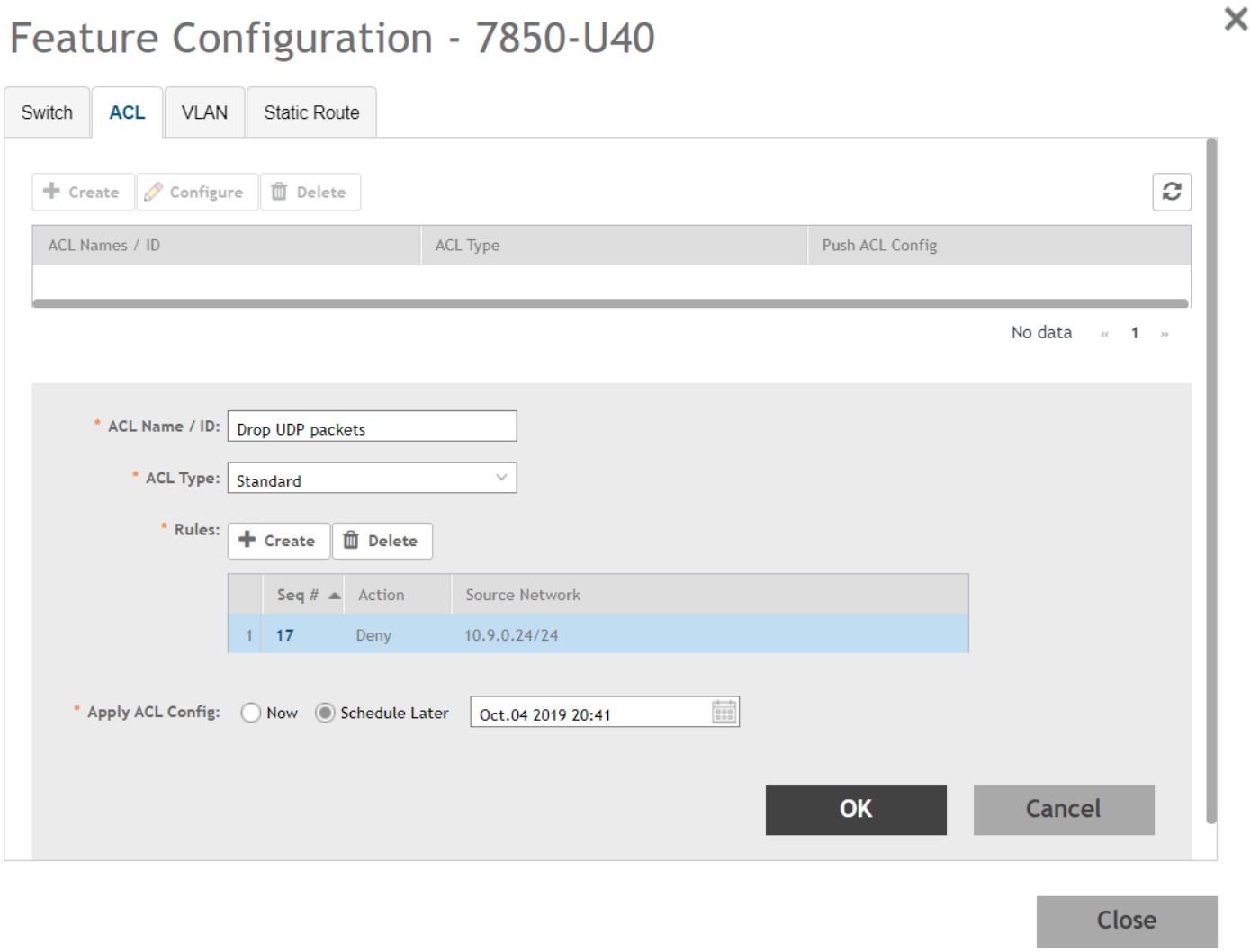
FIGURE 13 Selecting Ports from a Switch



Scheduling a Configuration

Network administrators would like to have control over when the configuration is pushed to the switches. SZ provides an automated way of scheduling the time and date when the configuration is pushed to a switch.

FIGURE 14 Scheduling a Configuration

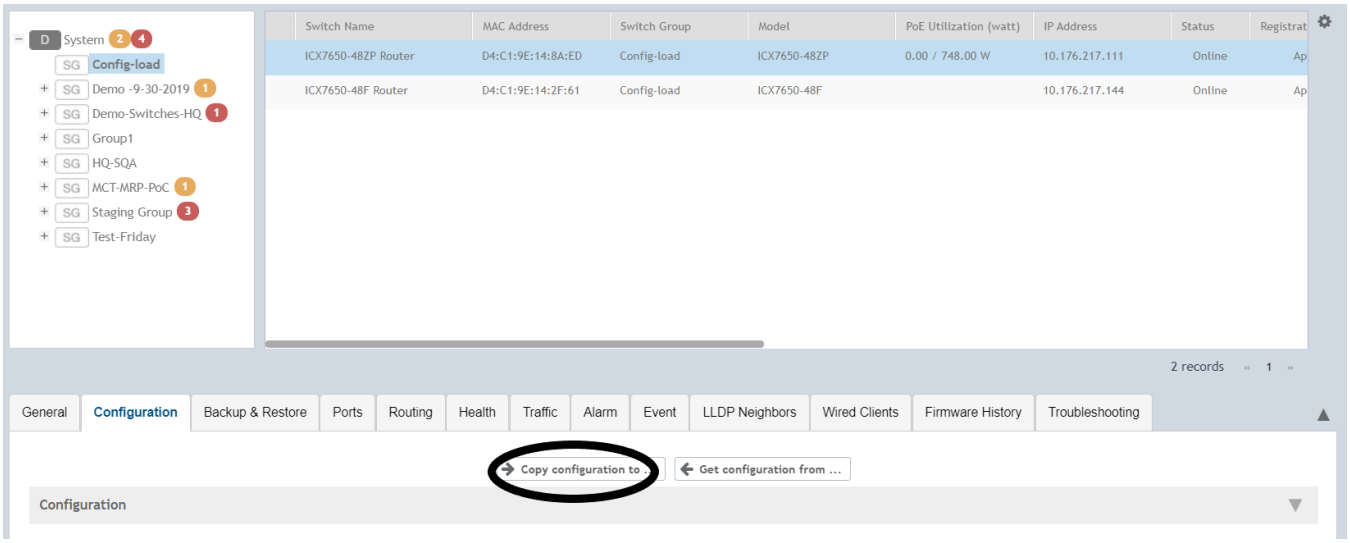


Copying a Working Configuration to Other Switches

SmartZone provides an easy and clean method to copy a configuration from one switch to many other switches. SZ also provides an option to manually enter additional configuration information during this process. This can help a network administrator maintain the network with some baseline configuration on all the switches. With a "golden switch" running the baseline configuration, you can copy the configuration to the new switch during the onboarding process. Complete the following steps to onboard a new switch and port the configuration.

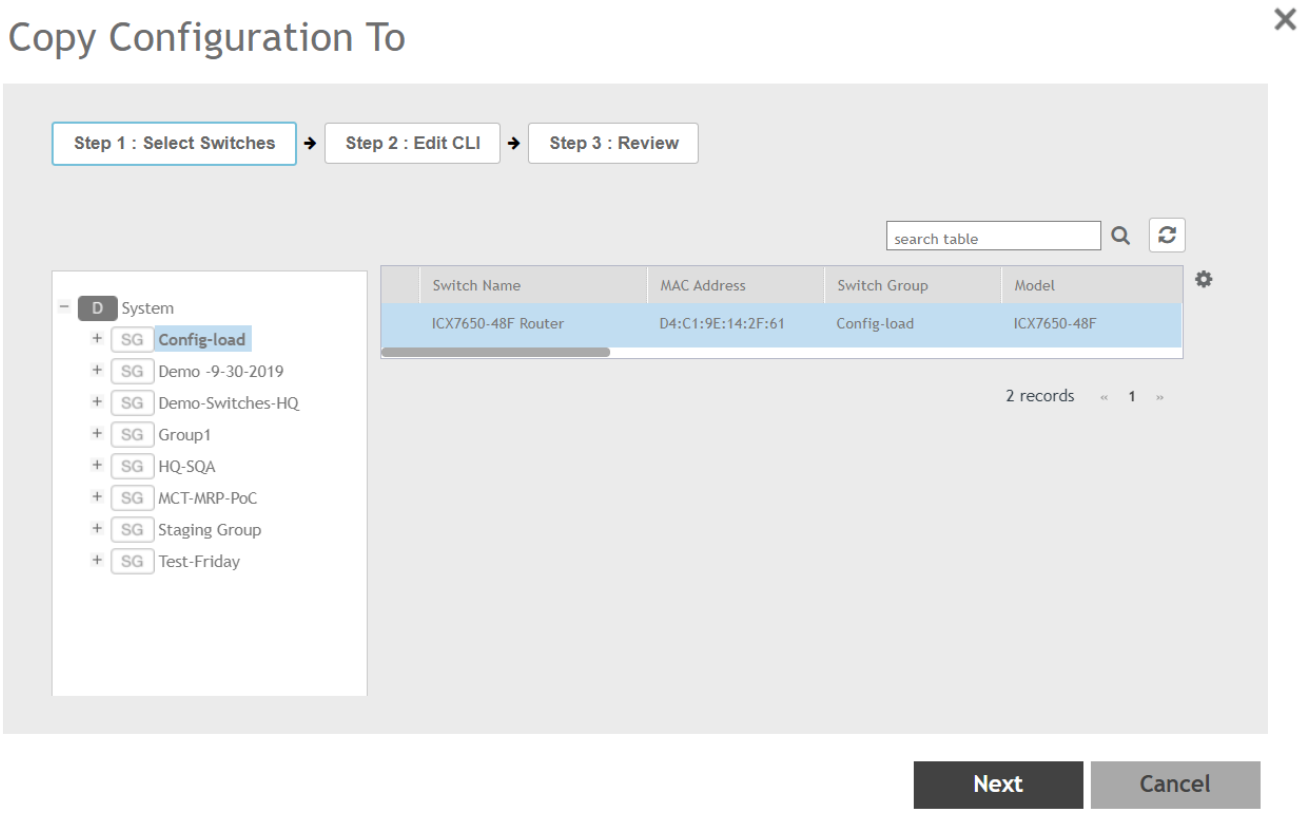
1. Make sure the new switch is registered on SZ. If it is not, complete the steps in Configuration on page 13.
2. On SZ, navigate to **Switches**, select a switch group with the golden switch, and click **Configuration**.
3. Click the **Copy configuration to ...** button.

FIGURE 15 Copying the Configuration



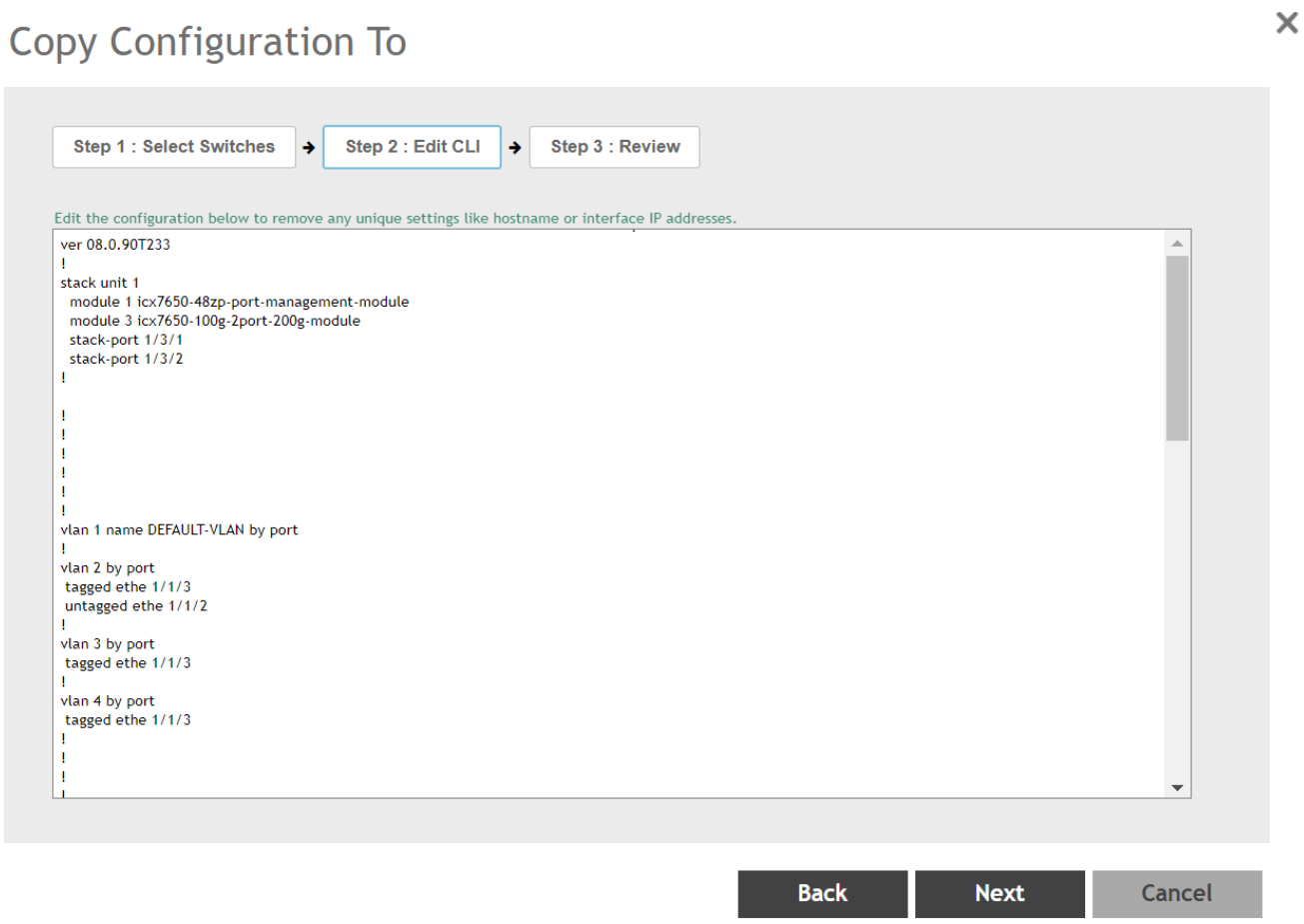
4. In the **Copy Configuration To** dialog box, select the target switch to which you want this configuration to be copied. This new switch can be a member of any switch group, and you can select multiple target switches.

FIGURE 16 Selecting a Target Switch



5. (Optional) Edit the configuration according to your requirements.

FIGURE 17 Editing the Configuration



6. Confirm the configuration update and that the new switch reboots to apply the new configuration. This process completely overwrites any existing configuration on the new switch with this copied configuration, and the configuration takes effect after the reboot.

In similar fashion, you can go to the target switch first and in the **Configuration** tab, click the **Get configuration from ...** button. Select the source switch and follow steps 4 through 6 to achieve a one-to-one switch configuration copy.

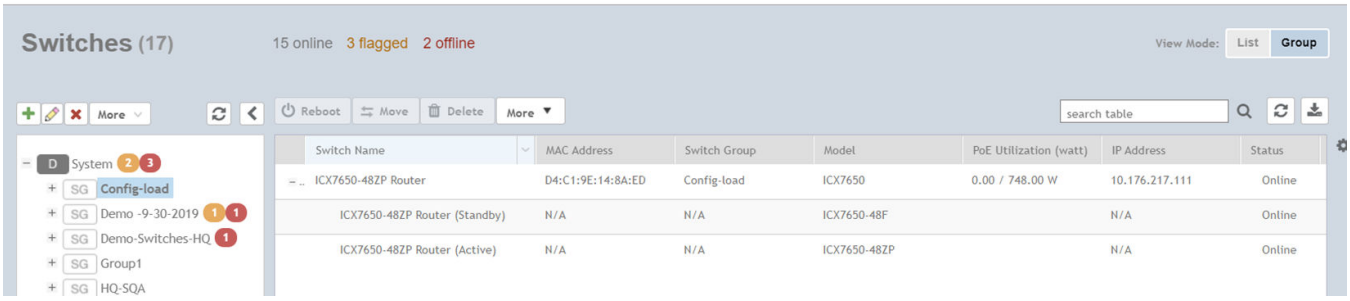
Adding an Existing ICX Switch Stack to SmartZone

You can add a stack of ICX switches to SmartZone.

1. Make sure the stack has an IP address and an SZ IP address is configured either manually or by way of Option 43 through a DHCP server.
2. From the switch, make sure you can reach the SZ IP address.
3. On vSZ or SZ300, the switch should show up in the Staging Group if there are no registration rules. If there are defined registration rules, you can find the switch registered in the proper switch group.

4. Wait for one to two cycles of an SNMP walk by SZ on the ICX switch (which can take between 5 and 10 minutes). If you try to look at the member switches of the stack on SZ during this time, an error message will be displayed. A completely registered stack on SZ is shown in the following figure.

FIGURE 18 Registered Stack on SmartZone



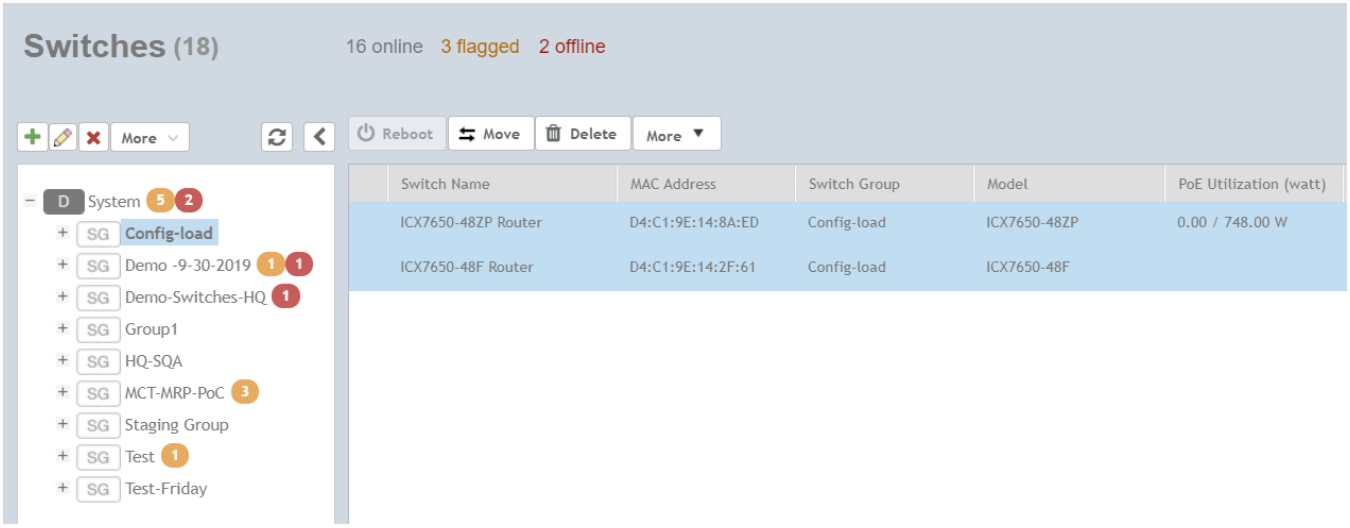
Forming a Stack Using Standalone ICX Switches on SmartZone

1. Move all the switches to a defined switch group either manually or by registering these switches using a registration rule.

NOTE
All the switches that need to be added to a stack must be part of a single switch group.

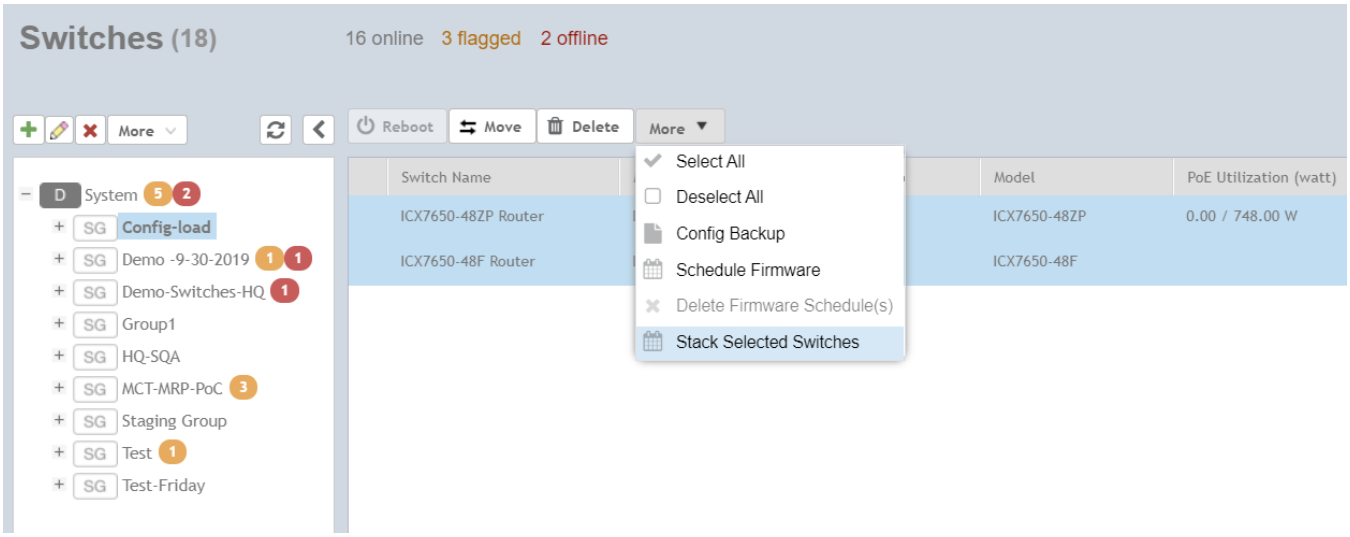
2. Once these switches show up on SmartZone, the standalone switches can have an existing configuration. Select the switches from the list in the switch group and click the **More** menu.

FIGURE 19 Selecting Switches in the Switch Group



3. Click **Stack Selected Switches**.

FIGURE 20 Stacking the Selected Switches



A message is displayed asking you to wait while this configuration is being applied. It takes 15 to 20 minutes before SZ shows a complete stack.

Monitoring

The monitoring use cases answer some of the following questions:

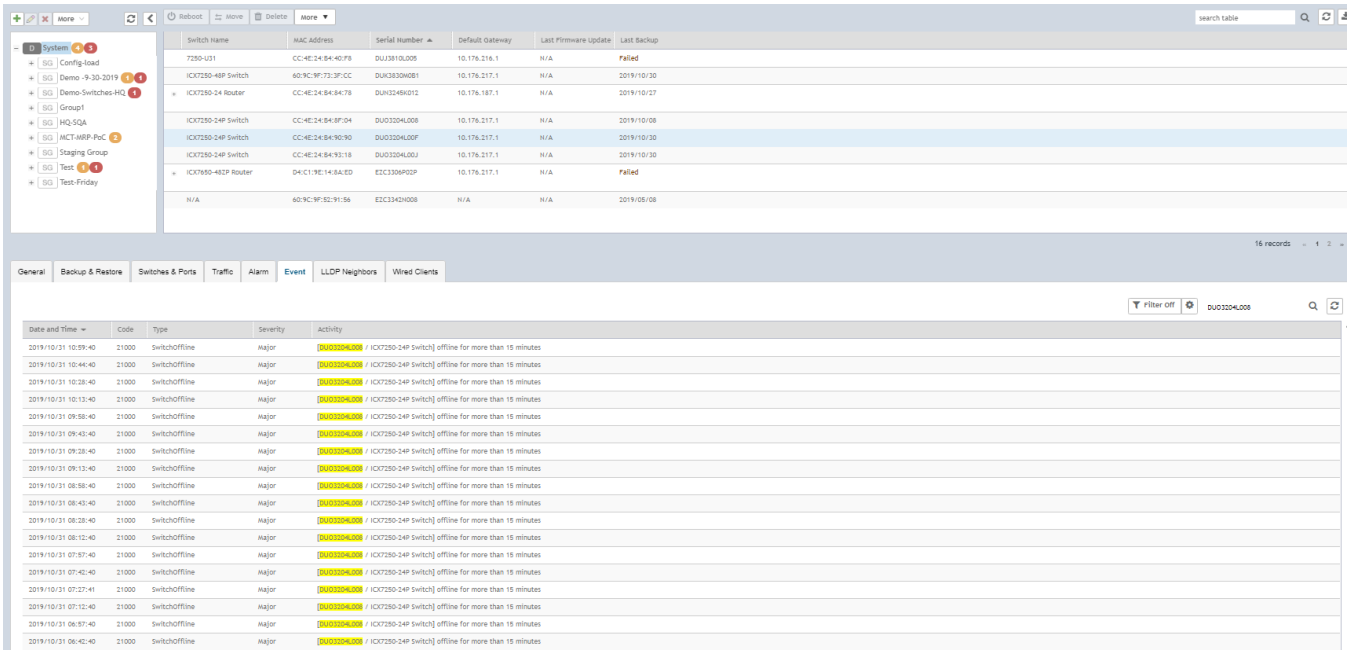
- How to customize an event?
- How to add new events?
- How to send a notification when an event has reached the threshold limit?
- How to back up a switch configuration?
- How to restore a configuration onto the switch?
- How to upgrade an ICX switch using SmartZone?

Events

Syslog messages that are marked Critical, Alert, and Warning are shown under the **Events** tab. The **Events** tab is available at multiple levels. It can be found at the domain, switch group, or specific switch level.

1. Navigate to **Switches** and select the domain, switch group, or switch.
2. Click the **Events** tab to access ICX switch events (including Critical, Alert, and Warning syslog messages). To access the entire set of syslog messages from all the switches, refer to Syslog on page 43.
3. Filter the events using serial numbers to display a list that belongs to a specific switch.

FIGURE 21 Events Listed by Serial Number



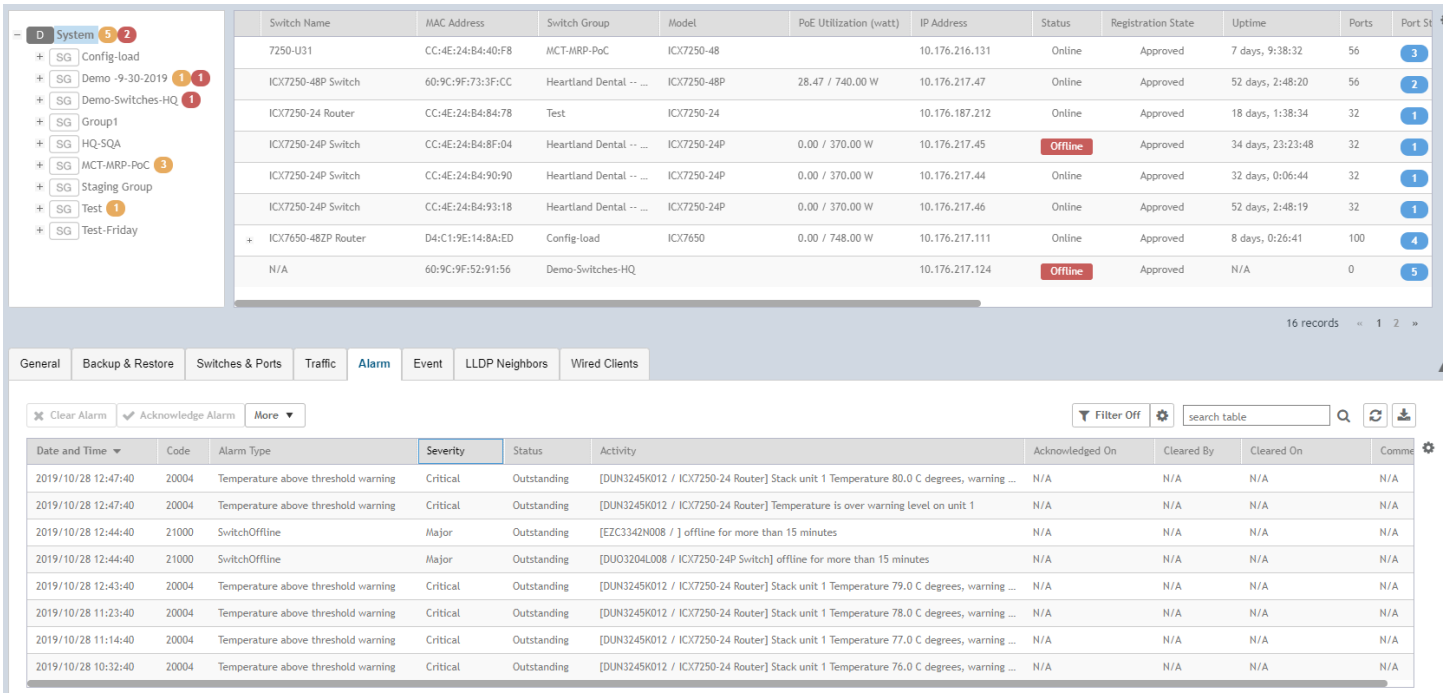
Alarms

To make the system more robust, nine top events have been identified and alarms have been created for these events by default:

- Power supply failure
- Fan failure
- Module insertion or removal
- Temperature above the threshold warning
- Stack member unit failure
- PoE power allocation failure
- Device (switch or stack) offline for more than 15 minutes
- DHCP_Snooping: DHCP offer dropped message
- Port put into error disable state

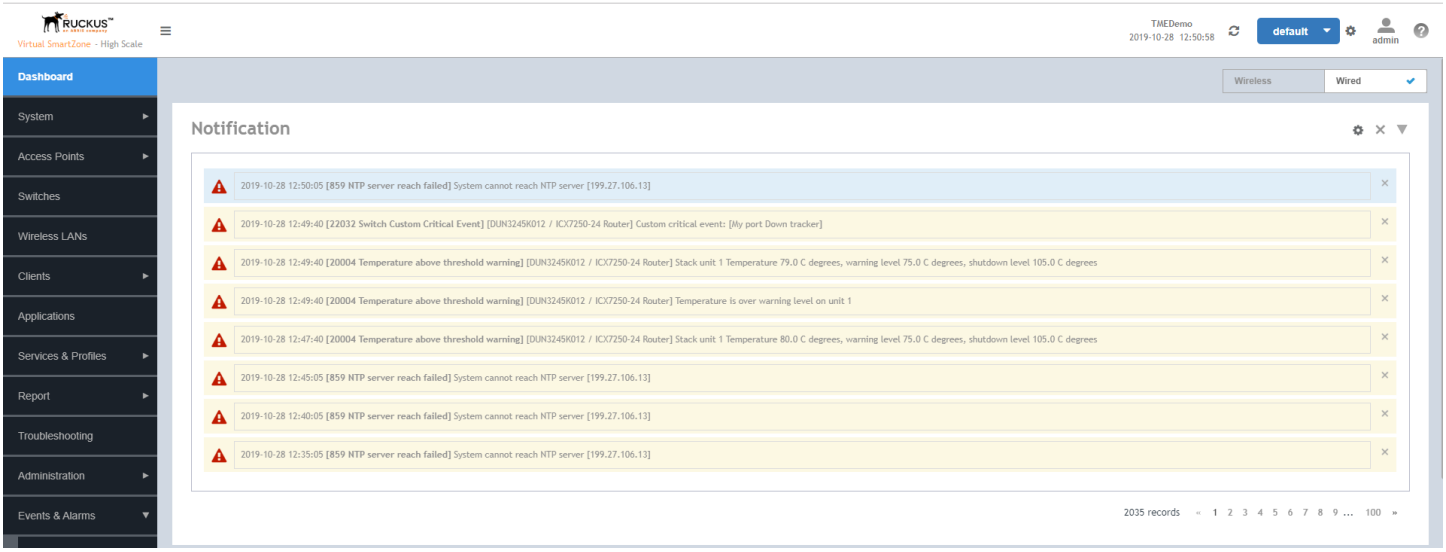
If any of the events are triggered on an ICX switch, SZ will create a corresponding alarm. The alarm can be found on the **Alarms** tab at the domain, switch group, or switch level.

FIGURE 22 Alarms Tab



The alarms also generate notification entry, which can be seen at the top of the SmartZone **Wired** dashboard.

FIGURE 23 Alarm Notifications



Custom Events and Alarms

Six CPU and memory events are provided by default, and these events can be customized.

You can define the threshold levels for the six default events.

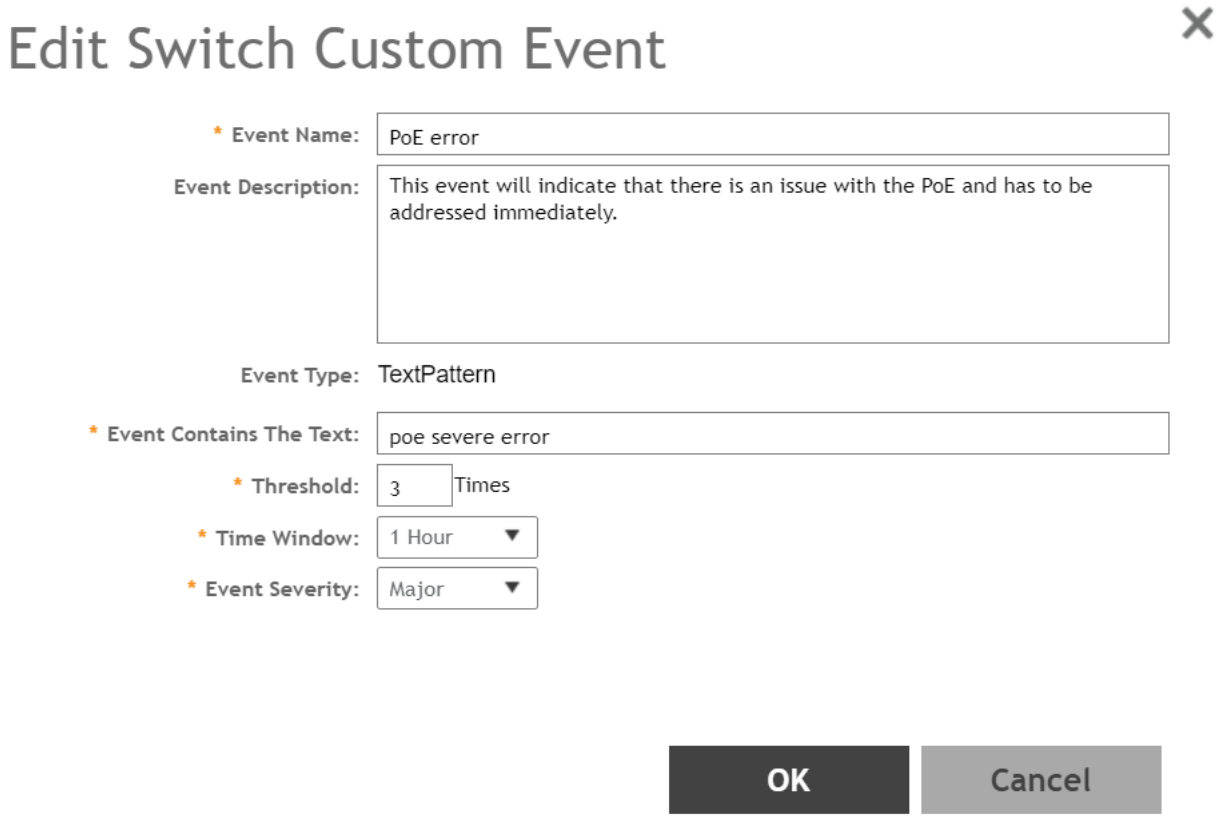
FIGURE 24 Default CPU and Memory Events

Event Name	Event Type	Event Severity	Threshold	Event Description	Text Pattern	Time Window
Warning CPU Usage	CPU	Warning	20	Switch CPU usage is over Warni...	N/A	N/A
Major CPU Usage	CPU	Major	30	Switch CPU usage is over Major ...	N/A	N/A
Critical CPU Usage	CPU	Critical	50	Switch CPU usage is over Critic...	N/A	N/A
Warning Memory Usage	Memory	Warning	60	Switch Memory usage is over W...	N/A	N/A
Major Memory Usage	Memory	Major	80	Switch Memory usage is over Ma...	N/A	N/A
Critical Memory Usage	Memory	Critical	90	Switch Memory usage is over Cr...	N/A	N/A

You can create custom events based on your requirements using SmartZone.

1. On SZ, from the navigation pane, select **Events & Alarms** > **Switch Custom Events**.
2. Click **Create** and fill in the details as needed. The text that you enter in the **Event Contains The Text** field is the string that you are interested in as seen in the ICX switch system log. In the following figure, an event is created that will look for the particular string "poe severe error" in the system log on ICX switches.

   FIGURE 25 Creating a Custom Switch Event



3. When the event is triggered, an entry is created and can be seen on the particular switch under the **Event** tab. Navigate to **Switches** and select the desired switch group and the desired switch. Click the **Event** tab.

Sending a Notification When an Event Reaches the Threshold Limit

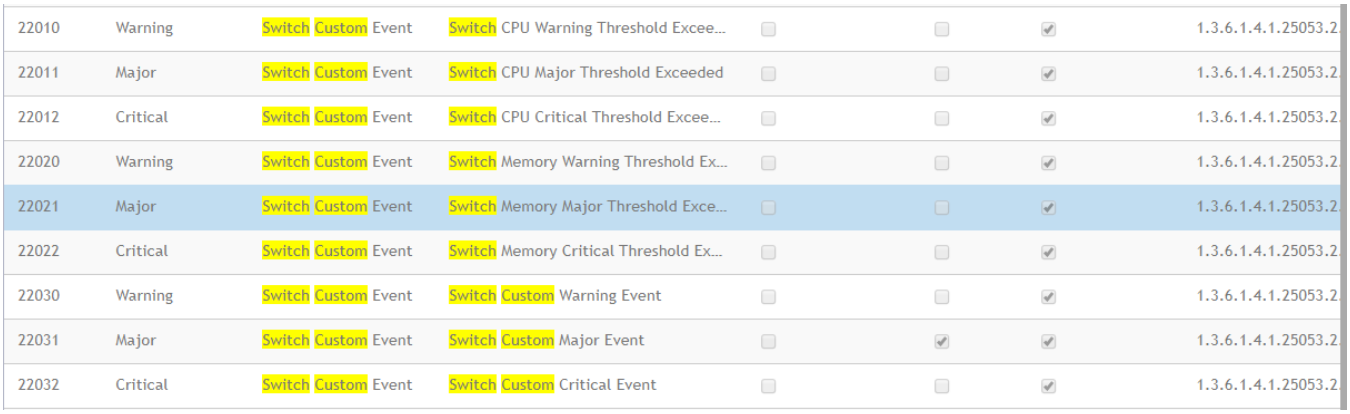
SZ provides multiple ways to notify you in case of an event.

You can configure SZ to send an email notification or to trigger an SNMP trap.

1. Navigate to **Events & Alarms** > **Events** > **Event Management**.
2. In the search bar, look for "switch custom".

   All the events, both default and custom events, will be listed. For the default events, the description will be either CPU Threshold (Warning, Major, or Critical) or Memory (Warning, Major, or Critical). Custom events are not listed separately. Custom events are separated into three categories based on the severity (Warning, Major, and Critical).

   FIGURE 26 Custom Switch Events



22010	Warning	Switch Custom Event	Switch CPU Warning Threshold Excee...	☐	☐	☑	1.3.6.1.4.1.25053.2
22011	Major	Switch Custom Event	Switch CPU Major Threshold Exceeded	☐	☐	☑	1.3.6.1.4.1.25053.2
22012	Critical	Switch Custom Event	Switch CPU Critical Threshold Excee...	☐	☐	☑	1.3.6.1.4.1.25053.2
22020	Warning	Switch Custom Event	Switch Memory Warning Threshold Ex...	☐	☐	☑	1.3.6.1.4.1.25053.2
22021	Major	Switch Custom Event	Switch Memory Major Threshold Exce...	☐	☐	☑	1.3.6.1.4.1.25053.2
22022	Critical	Switch Custom Event	Switch Memory Critical Threshold Ex...	☐	☐	☑	1.3.6.1.4.1.25053.2
22030	Warning	Switch Custom Event	Switch Custom Warning Event	☐	☐	☑	1.3.6.1.4.1.25053.2
22031	Major	Switch Custom Event	Switch Custom Major Event	☐	☑	☑	1.3.6.1.4.1.25053.2
22032	Critical	Switch Custom Event	Switch Custom Critical Event	☐	☐	☑	1.3.6.1.4.1.25053.2

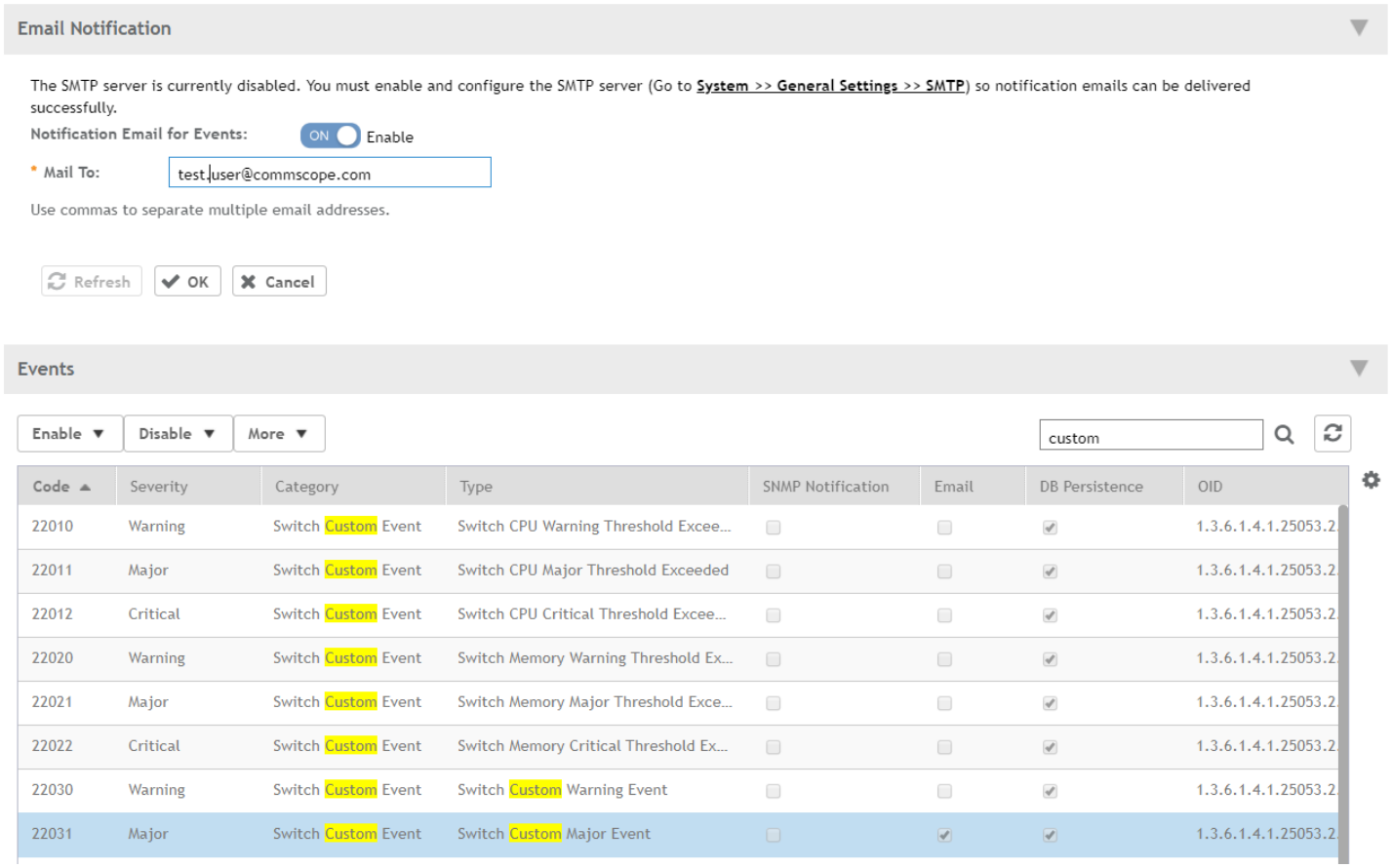
3. Select an event.
4. Using the **Enable** menu, select the options to enable or disable SNMP, Email, or local DataBase store. By default, every event is stored in the local database.

   NOTE
   It is recommended that you keep DB Persistence enabled and choose other notifications according to your requirements.

Setting Up an Email Notification

If you want to send an email notification when an event is triggered, define a recipient email address on the **Event Management** page.

FIGURE 27 Setting Up Email Notification

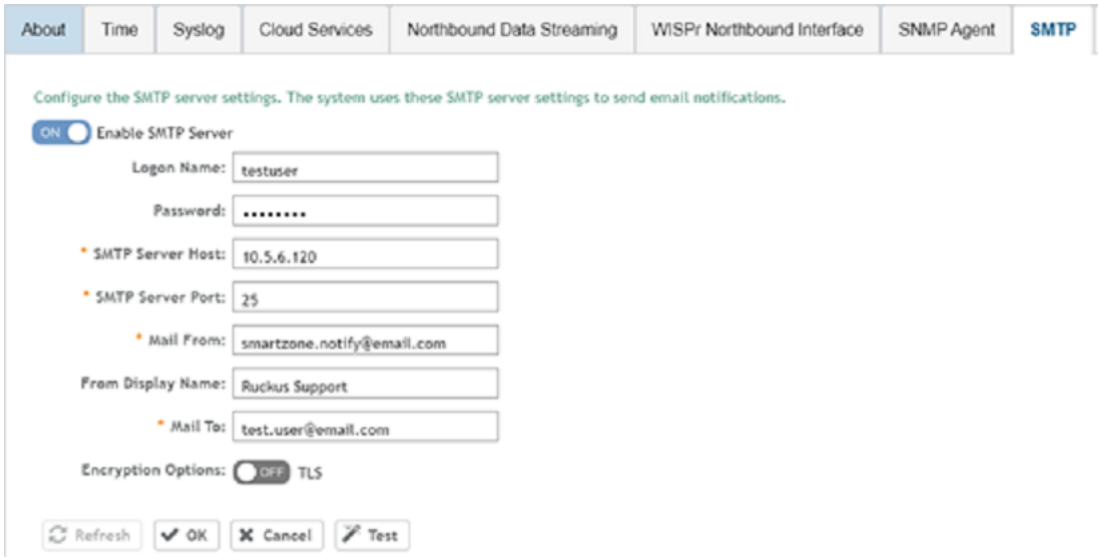


Configuring the SMTP Server Parameters

You must next configure the SMTP server parameters.

1. Navigate to **System** > **General Settings** > **SMTP**.
2. Under the **SMTP** tab, enable the SMTP server and enter all the details.

FIGURE 28 Entering SMTP Server Parameters

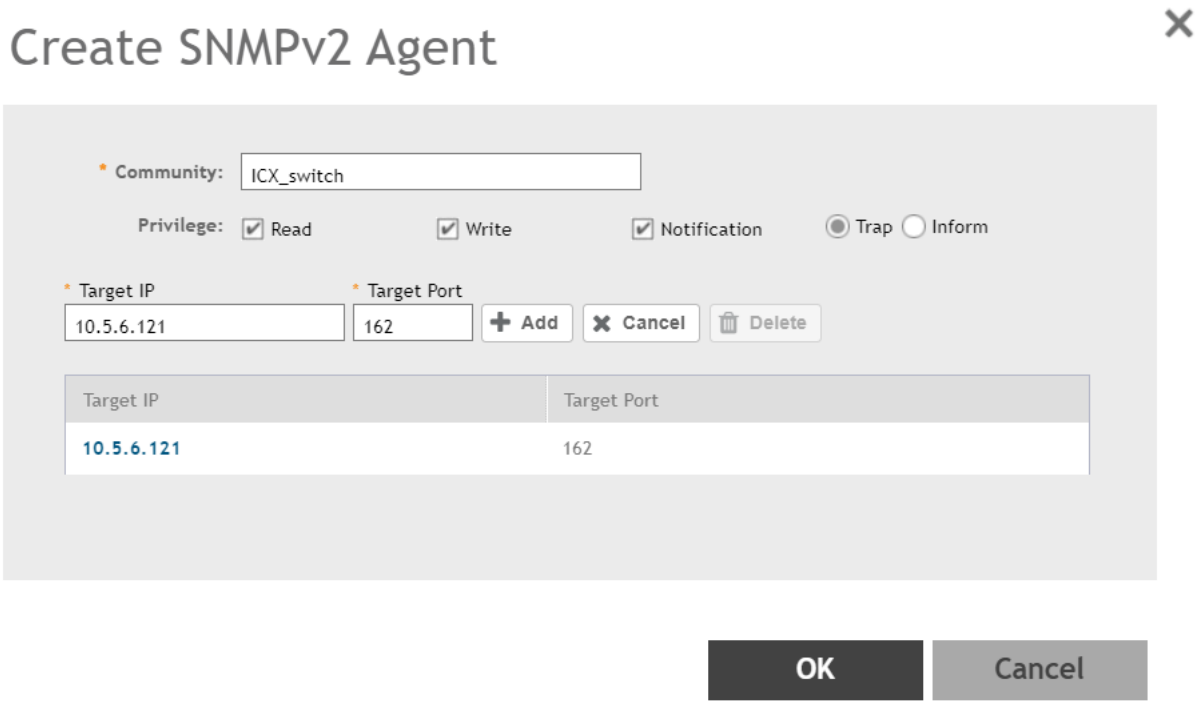


3. Using the **Test** button, test the connection to the SMTP server. Once it is successful, click **OK**.

Setting Up SNMP Notification

1. Navigate to **System** > **General Settings** > **SNMP Agent**.
2. Enable SNMP notifications globally and then add an entry to an SNMPv2 or SNMPv3 Agent.

FIGURE 29 Creating an SNMPv2 Agent



NOTE
Be sure to enable **Notification** and add an entry to point to the SNMP trap server.

Backing Up and Restoring a Switch Configuration

By default, SmartZone backs up all the switch configurations at midnight every day. A copy of the configuration is available for viewing or download to a local server under the **Backup & Restore** tab.

If you want to restore a particular configuration from a previous date, simply select the desired switch, select the configuration to restore, and confirm the process. The selected configuration is loaded on the switch and the switch boots up with the configuration.

1. Navigate to **Switches** > **Domain**.
2. Click the **Backup & Restore** tab to see a list of all backups available for all the switches in that domain.
3. Click any line item and view or download the configuration. The same can be done at the switch group level.
4. Select a particular switch, and use the **More** menu to initiate a manual configuration backup for that particular switch.
5. The configuration restore can be handled at the single switch level. Navigate to **Switches** and select the desired switch group and the desired switch.
6. Select a particular switch configuration that has been backed up in the **Backup & Restore** tab.
7. Click **Configuration Restore** and click **Yes** when prompted.

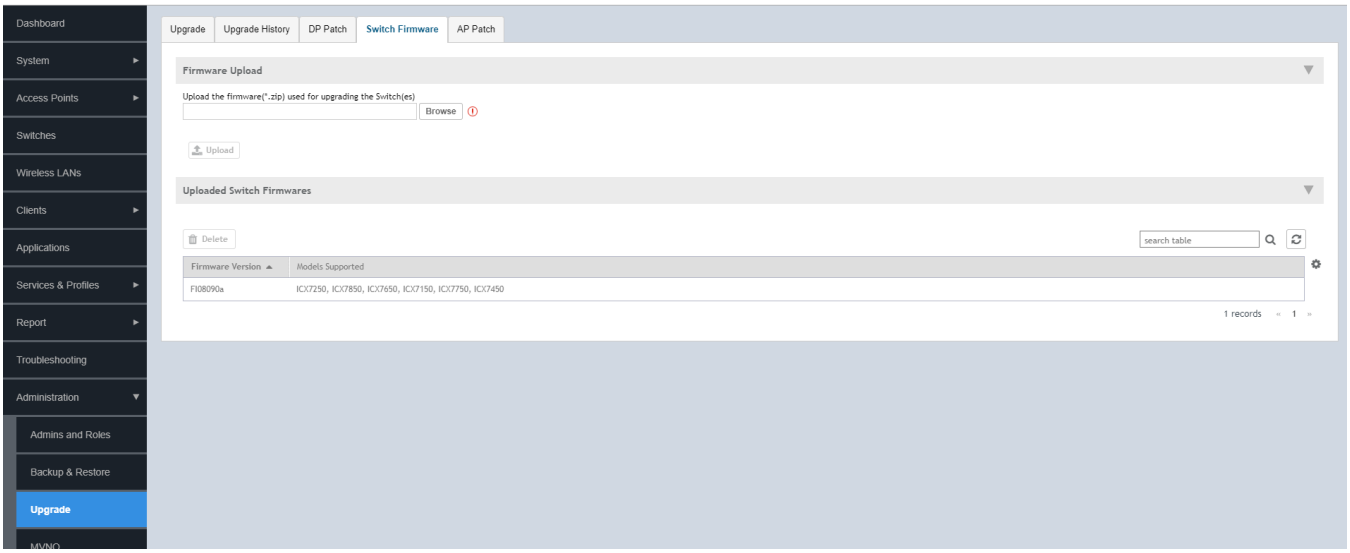
Upgrading an ICX Switch Using SmartZone

SmartZone allows you to upgrade a single or multiple ICX switches using a single pane of glass.

You must upload the ZIP folder that was downloaded from the Ruckus Support website to the SmartZone controller. This folder includes firmware for all the different models of ICX switches. You can select the switches that require an upgrade and schedule the upgrade for now or sometime in future. SmartZone takes care of selecting the image needed for the switch model and rebooting the switch after the upgrade.

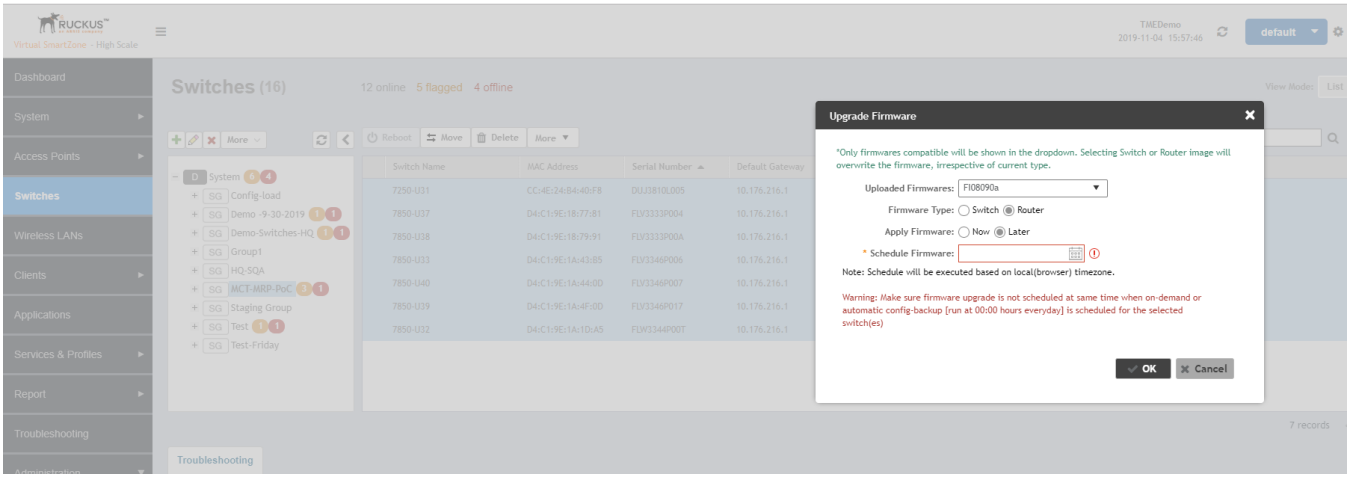
1. Upload the ZIP folder that was downloaded from the support website to the controller. Navigate to **Administrator** > **Upgrade** > **Switch Firmware**. Once the folder is uploaded, an entry is created in the **Uploaded Switch Firmwares** list.

   FIGURE 30 Uploaded Switch Firmware



2. Navigate to **Switches**, from the domain level or the switch group level, and select the switches that you want to upgrade. Click the **More** menu to select all the switches.
3. Click **Schedule Firmware**. You have the option to upgrade now or at a later date and time.

   FIGURE 31 Scheduling the Upgrade



4. (Optional) You can delete a scheduled firmware upgrade using the **More** menu.

Reporting

The reporting use cases offer the following options:

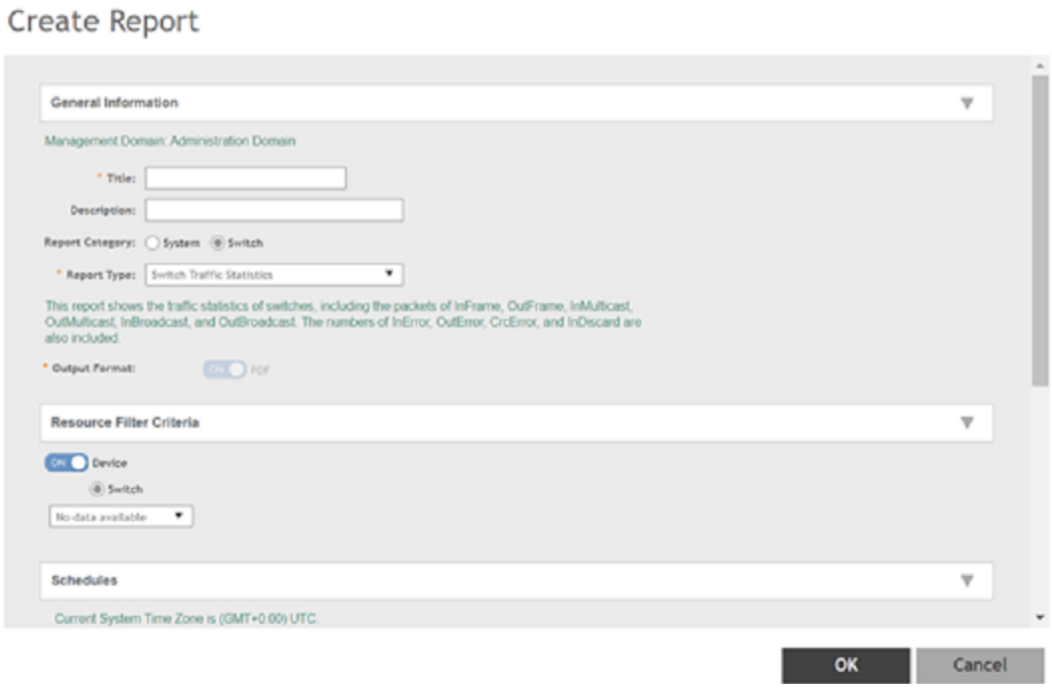
- Generate a report for switch traffic results and store it locally
- Generate a report for switch traffic results and send an email notification
- Generate a report for switch traffic results and export it to an FTP location

Generating a Report for Switch Traffic Results and Storing It Locally

SmartZone allows you to generate reports with switch traffic results. The report can be generated for a single switch or a group of switches.

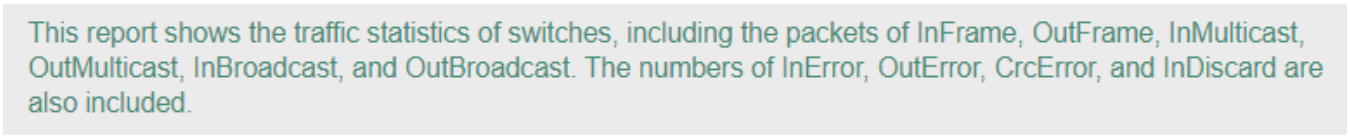
1. Select **Report** on the navigation pane. In **Report Generation**, click **Create**.

FIGURE 32 Creating a Report



2. For **Report Category**, select **Switch**, and fill in the details. The previous figure shows the available **Report Type** is **Switch Traffic Statistics** and a brief description.

FIGURE 33 Switch Traffic Statistics Description



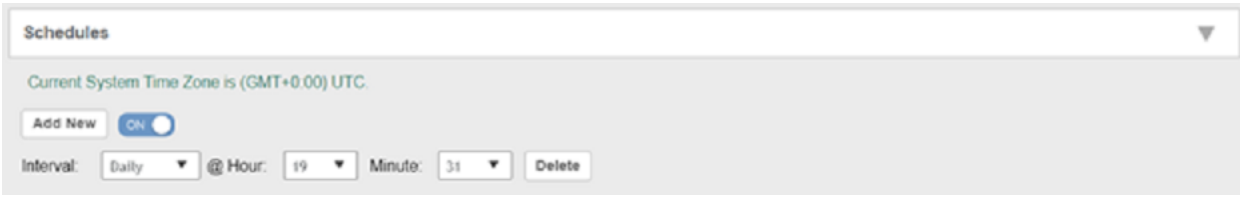
3. For **Resource Filter Criteria**, select the switches for which you want to generate a report.

FIGURE 34 Resource Filter Criteria



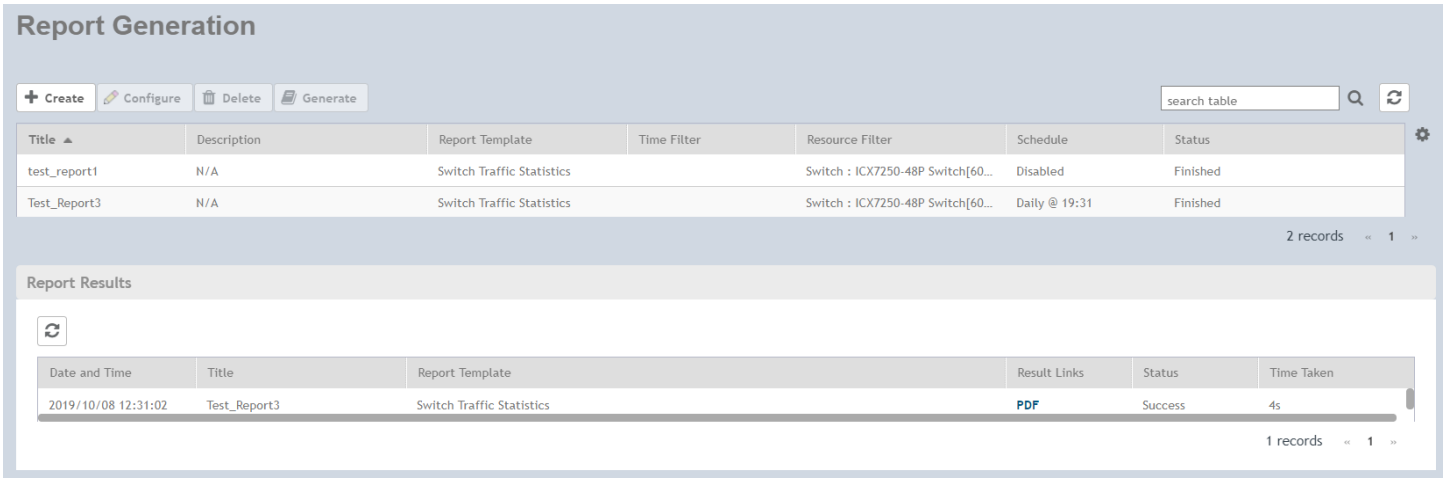
4. For **Schedules**, you have the option to schedule the report generation. If you do not enter a time interval, then the report is generated immediately after you click **OK**.

FIGURE 35 Scheduling Report Generation



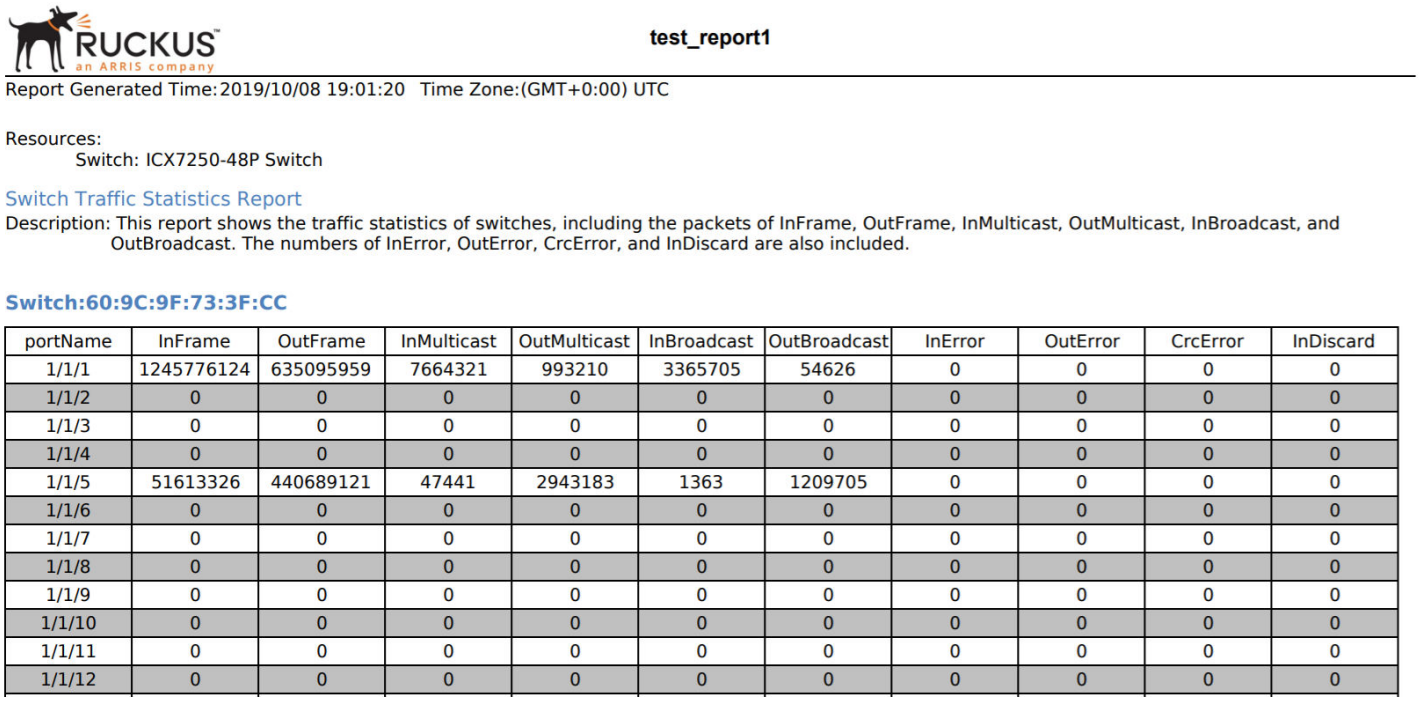
By default, after generating the report, SmartZone stores it on the **Report Generation** page and provides a URL to download the PDF file.

FIGURE 36 Storing the Generated Report



The final report looks like the report shown in the following figure. If there are multiple switches in the same report, they are identified by the MAC address of each switch.

FIGURE 37 Final Report Example



RUCKUS an ARRIS company

test_report1

Report Generated Time:2019/10/08 19:01:20 Time Zone:(GMT+0:00) UTC

Resources:
Switch: ICX7250-48P Switch

Switch Traffic Statistics Report

Description: This report shows the traffic statistics of switches, including the packets of InFrame, OutFrame, InMulticast, OutMulticast, InBroadcast, and OutBroadcast. The numbers of InError, OutError, CrcError, and InDiscard are also included.

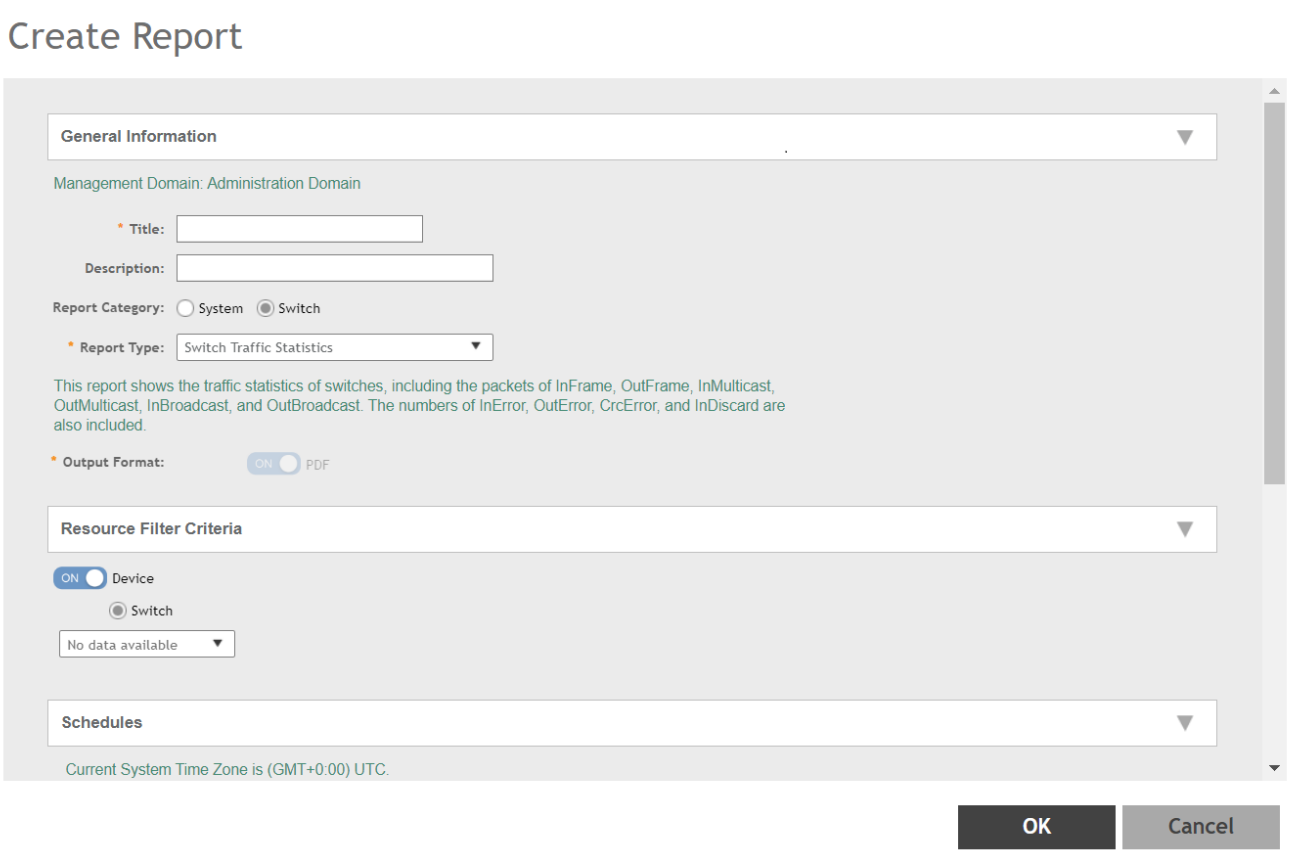
Switch:60:9C:9F:73:3F:CC

portName	InFrame	OutFrame	InMulticast	OutMulticast	InBroadcast	OutBroadcast	InError	OutError	CrcError	InDiscard
1/1/1	1245776124	635095959	7664321	993210	3365705	54626	0	0	0	0
1/1/2	0	0	0	0	0	0	0	0	0	0
1/1/3	0	0	0	0	0	0	0	0	0	0
1/1/4	0	0	0	0	0	0	0	0	0	0
1/1/5	51613326	440689121	47441	2943183	1363	1209705	0	0	0	0
1/1/6	0	0	0	0	0	0	0	0	0	0
1/1/7	0	0	0	0	0	0	0	0	0	0
1/1/8	0	0	0	0	0	0	0	0	0	0
1/1/9	0	0	0	0	0	0	0	0	0	0
1/1/10	0	0	0	0	0	0	0	0	0	0
1/1/11	0	0	0	0	0	0	0	0	0	0
1/1/12	0	0	0	0	0	0	0	0	0	0

Generating a Report for Switch Traffic Results and Sending an Email Notification

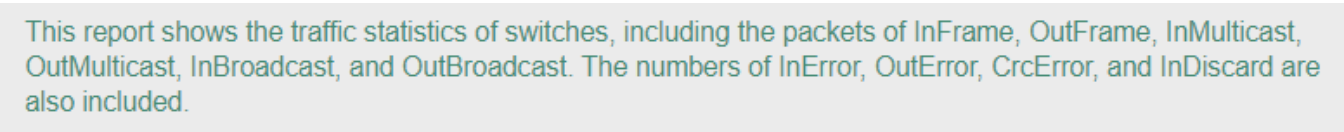
1. Select **Report** on the navigation pane. In **Report Generation**, click **Create**.

FIGURE 38 Creating a Report



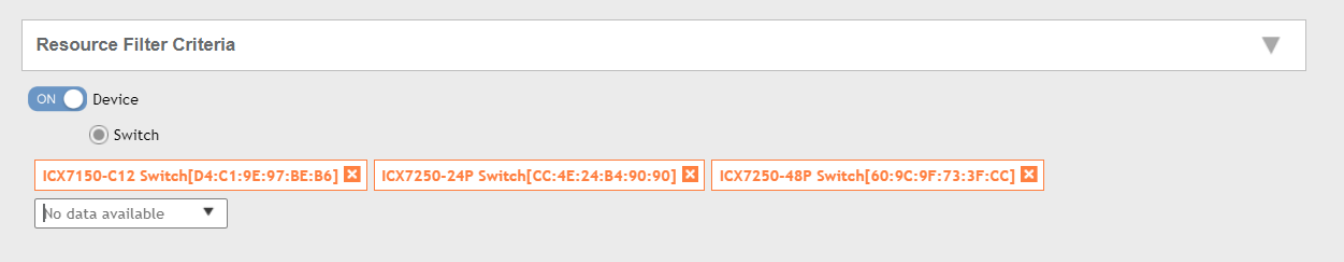
2. For **Report Category**, select **Switch**, and fill in the details. The previous figure shows the available **Report Type** is **Switch Traffic Statistics** and a brief description.

FIGURE 39 Switch Traffic Statistics Description



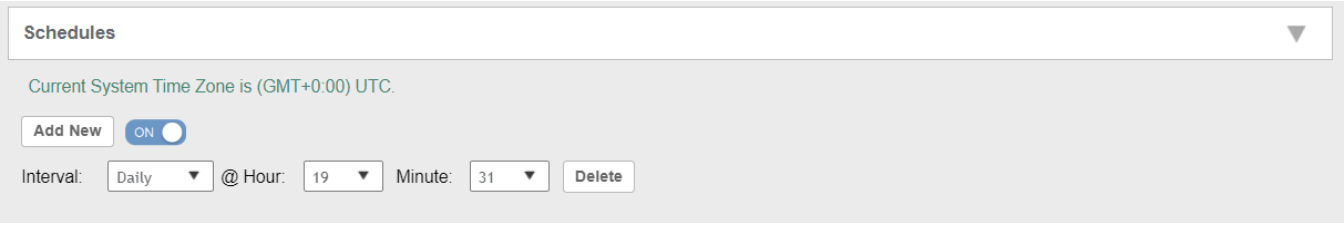
3. For **Resource Filter Criteria**, select the switches for which you want to generate a report.

FIGURE 40 Resource Filter Criteria



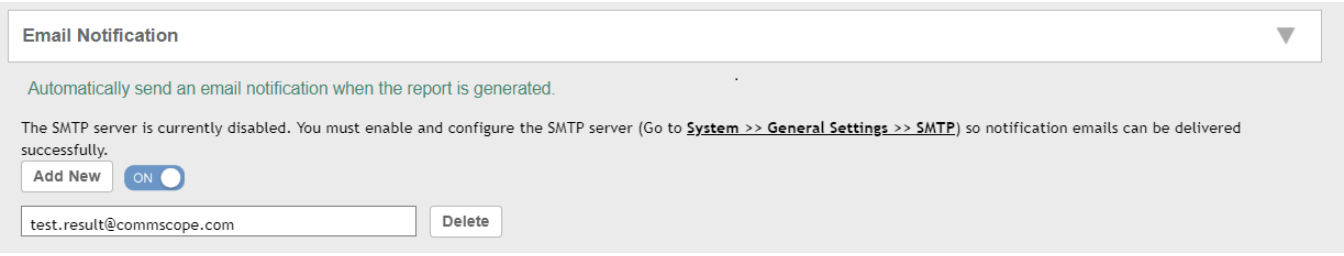
4. For **Schedules**, you have the option to schedule the report generation. If you do not enter a time interval, then the report is generated immediately after you click **OK**.

FIGURE 41 Scheduling Report Generation



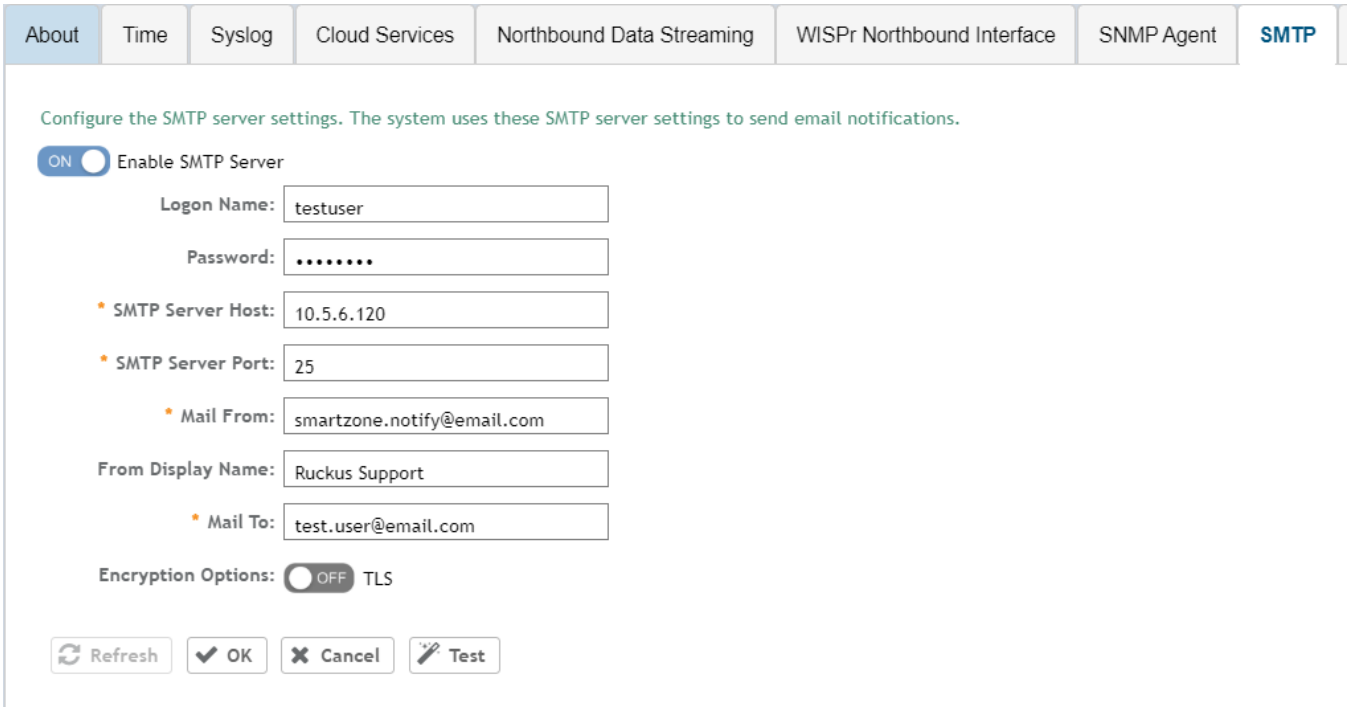
5. For **Email Notification**, enter an email address.

FIGURE 42 Email Notification



6. Navigate to **System** > **General Settings** > **SMTP** to set up the SMTP server.
7. In the **SMTP** tab, enable the SMTP server and enter all the details.

FIGURE 43 SMTP Tab

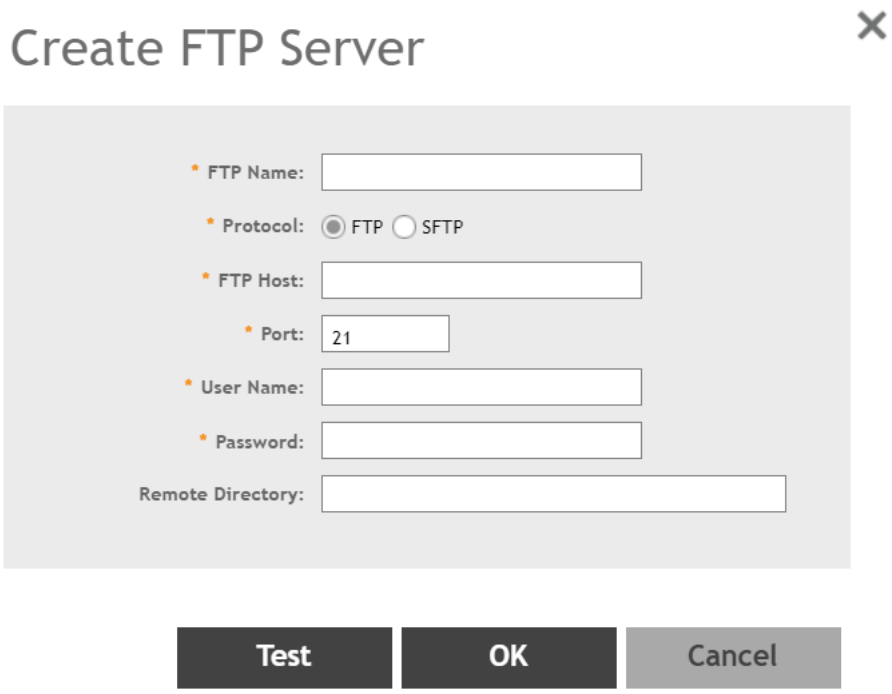


8. Click the **Test** button to test the connection to the SMTP server. Once the test is successful, click **OK**.

Generating a Report for Switch Traffic Results and Exporting It to an FTP Location

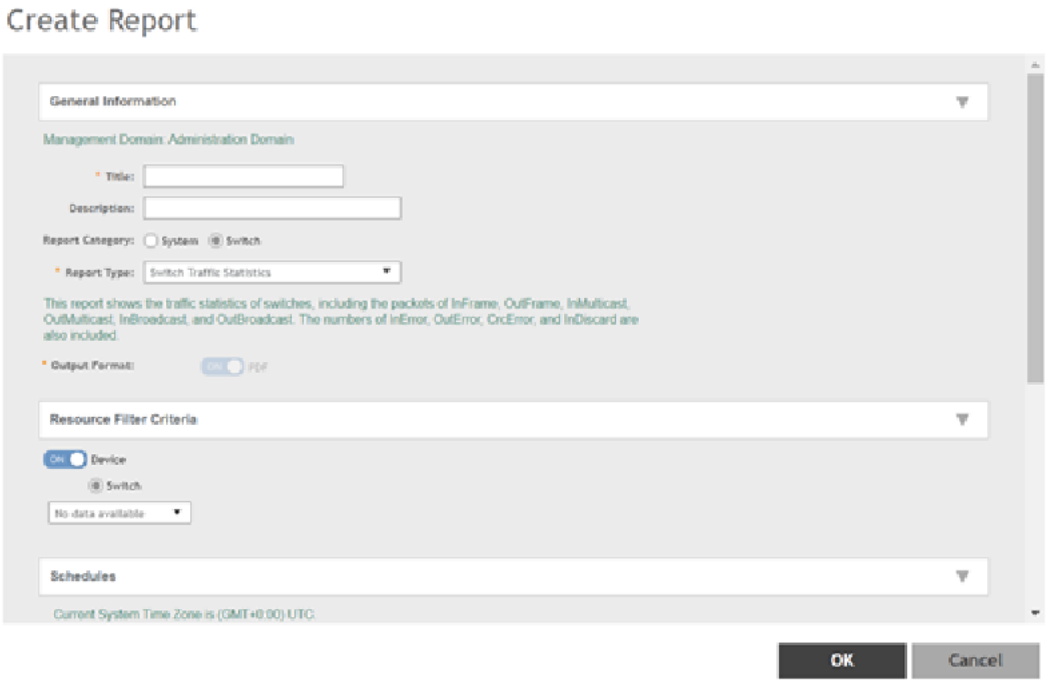
1. Navigate to **System** > **General Settings** > **FTP**.
2. Define a known FTP server location, test the connection, and save it.

FIGURE 44 Defining the FTP Server



3. Select **Report** on the navigation pane. In **Report Generation**, click **Create**.

FIGURE 45 Creating a Report



4. For **Report Category**, select **Switch**, and fill in the details. The previous figure shows the available **Report Type** is **Switch Traffic Statistics** and a brief description.

   FIGURE 46 Switch Traffic Statistics Description

   This report shows the traffic statistics of switches, including the packets of InFrame, OutFrame, InMulticast, OutMulticast, InBroadcast, and OutBroadcast. The numbers of InError, OutError, CrcError, and InDiscard are also included.

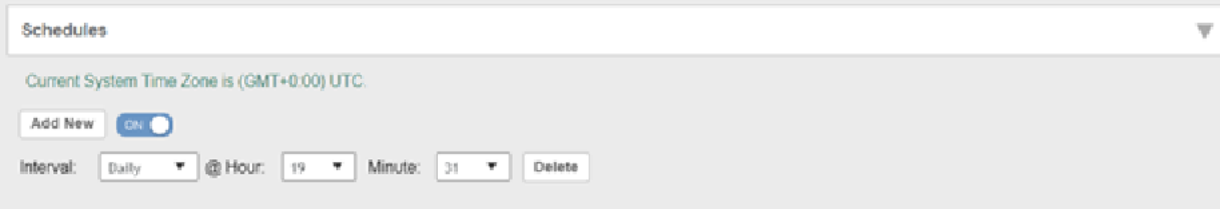
5. For **Resource Filter Criteria**, select the switches for which you want to generate a report.

   FIGURE 47 Resource Filter Criteria



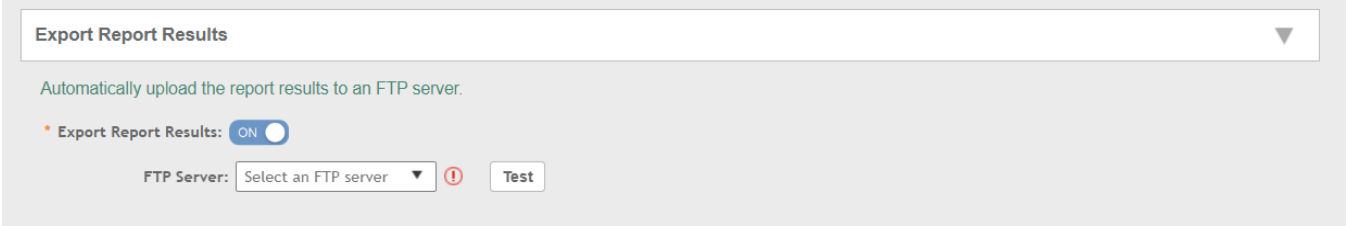
6. For **Schedules**, you have the option to schedule the report generation. If you do not enter a time interval, then the report is generated immediately after you click **OK**.

   FIGURE 48 Scheduling Report Generation



7. Enable **Export Report Results**, select an FTP server from the **FTP Server** menu, and test the connection.

   FIGURE 49 Export Report Results



Troubleshooting

The troubleshooting use cases answer some of the following questions:

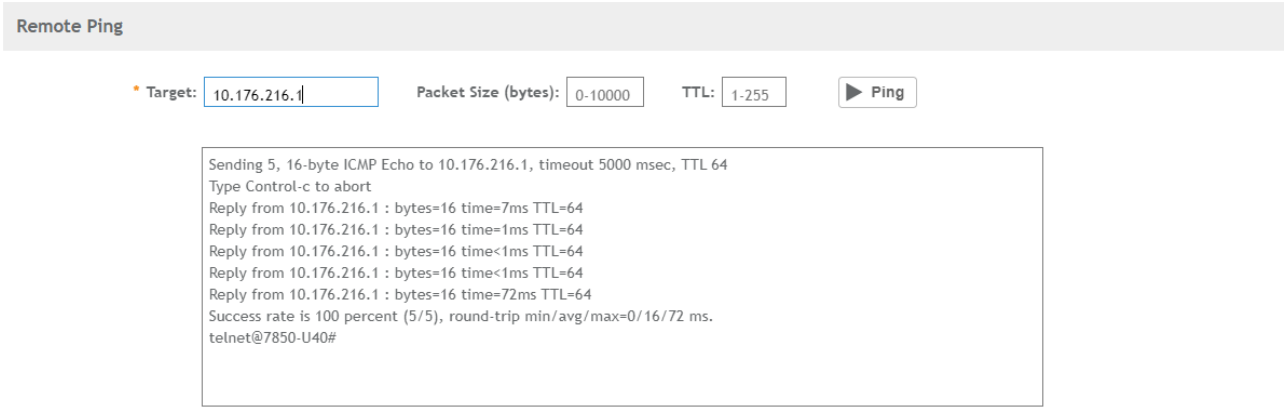
- How to check the switch connectivity to a remote server, printer, or edge device?
- How to narrow down an issue with connectivity to a client?
- How to know where the clients are connected in the network?

Remote Ping

Complete the following steps to check the switch connectivity to a remote server, printer, or edge device.

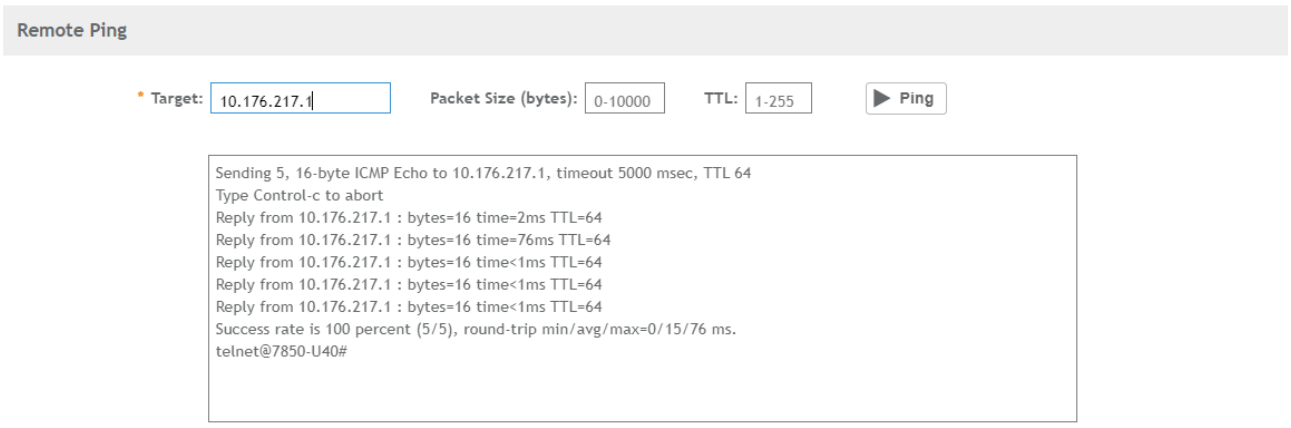
1. Select **Switches** from the navigation pane.
2. Select the required switch group and select the switch under review.
3. Select the **Troubleshooting** tab.
4. Expand the **Remote Ping** page and enter a target IP address. You can also test with a different packet size. For example, in the following scenario, the source IP address is 10.176.216.144 and the target IP address is 10.176.217.140.
   a. Check connectivity to the default gateway at 10.176.216.1.

FIGURE 50 Connectivity to Default Gateway



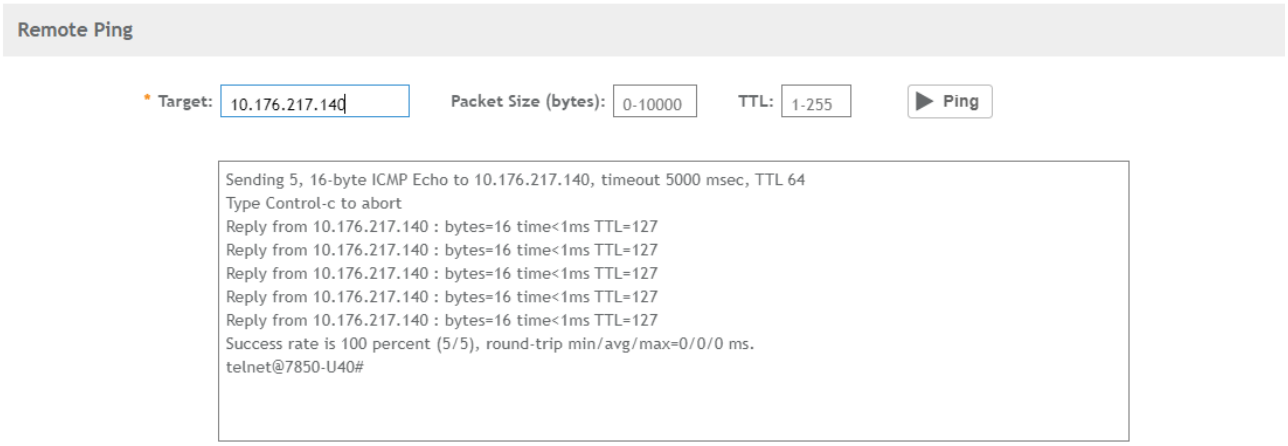
   b. Check connectivity to the TOR switch connected to the server at 10.176.217.1.

FIGURE 51 Connectivity to TOR Switch



c. Check connectivity to the target IP address.

FIGURE 52 Connectivity to Target IP Address



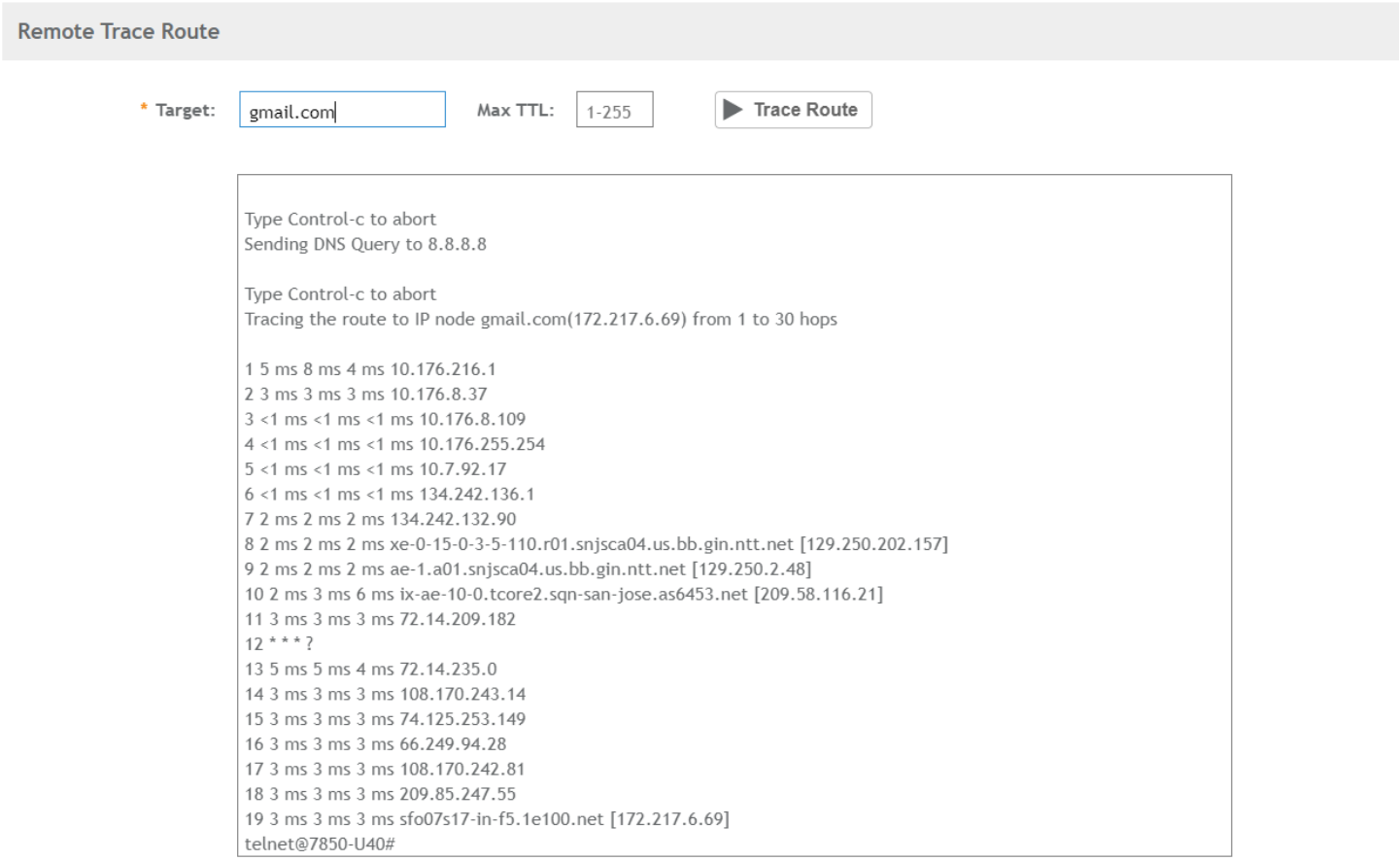
In this fashion, you can debug any connectivity issue, see where the actual problem lies, and take proper action.

Remote Trace Route

1. Select **Switches** from the navigation pane.
2. Select the desired switch group and the desired switch.
3. Select the **Troubleshooting** tab.
4. Expand the **Remote Trace Route** page and enter the target IP address.

   NOTE
   The required **Target** can be an IP address or a URL.

FIGURE 53 Remote Trace Route



Client Connectivity

Suppose you have a Ruckus AP powered by an ICX switch and this AP has active clients connected. In the case of an issue that is local to a particular client, this troubleshooting technique will help narrow down the problem by checking connectivity from the ICX switch to the AP and from the AP to the client.

1. Navigate to **Switches** and select the desired switch group.
2. Select the **Troubleshooting** tab and expand the **Client Connectivity** page.
3. Enter the MAC address of the client in the **Client MAC** field and click **Start**.

FIGURE 54 Connectivity Path



The visual graph shows the connectivity path from the client to the AP and from the AP to the ICX switch port. You can navigate to the AP or the switch itself on SZ by clicking the hyperlink.

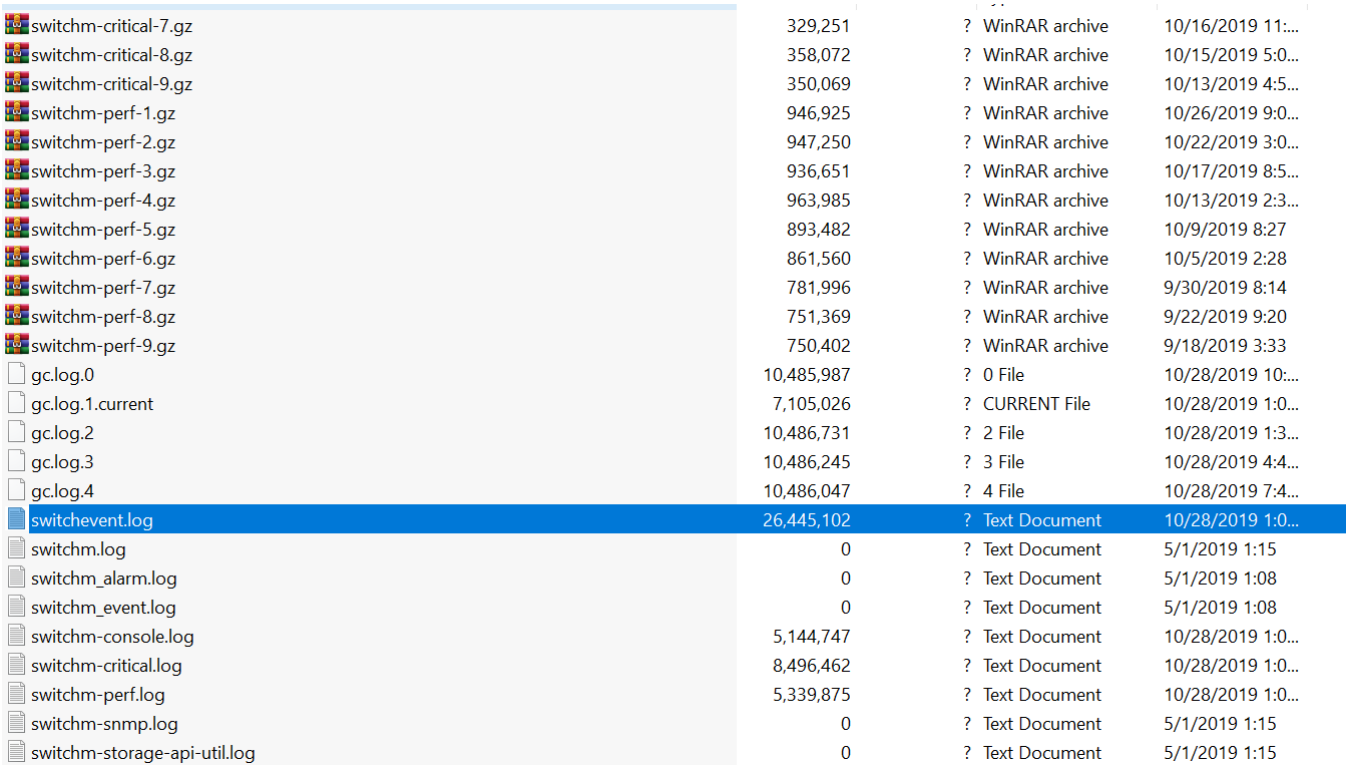
Syslog

All the syslog files from an ICX device are captured by SmartZone. The entire syslog file can be downloaded. To download an entire syslog file, complete the following steps.

1. Navigate to **Diagnostics** > **Application Logs**.
2. Select **switchm** from the list of applications.
3. Click **Download Logs**.

   A ZIP file downloads. Once you extract the files, you can find the switchevent.log file, which contains all the syslog messages for all the switches registered to SmartZone.
4. Search for a specific switch log using the serial number.

FIGURE 55 Finding a Switch Log



switchm-critical-7.gz	329,251	?	WinRAR archive	10/16/2019 11:...
switchm-critical-8.gz	358,072	?	WinRAR archive	10/15/2019 5:0...
switchm-critical-9.gz	350,069	?	WinRAR archive	10/13/2019 4:5...
switchm-perf-1.gz	946,925	?	WinRAR archive	10/26/2019 9:0...
switchm-perf-2.gz	947,250	?	WinRAR archive	10/22/2019 3:0...
switchm-perf-3.gz	936,651	?	WinRAR archive	10/17/2019 8:5...
switchm-perf-4.gz	963,985	?	WinRAR archive	10/13/2019 2:3...
switchm-perf-5.gz	893,482	?	WinRAR archive	10/9/2019 8:27
switchm-perf-6.gz	861,560	?	WinRAR archive	10/5/2019 2:28
switchm-perf-7.gz	781,996	?	WinRAR archive	9/30/2019 8:14
switchm-perf-8.gz	751,369	?	WinRAR archive	9/22/2019 9:20
switchm-perf-9.gz	750,402	?	WinRAR archive	9/18/2019 3:33
gc.log.0	10,485,987	?	0 File	10/28/2019 10:...
gc.log.1.current	7,105,026	?	CURRENT File	10/28/2019 1:0...
gc.log.2	10,486,731	?	2 File	10/28/2019 1:3...
gc.log.3	10,486,245	?	3 File	10/28/2019 4:4...
gc.log.4	10,486,047	?	4 File	10/28/2019 7:4...
switchevent.log	26,445,102	?	Text Document	10/28/2019 1:0...
switchm.log	0	?	Text Document	5/1/2019 1:15
switchm_alarm.log	0	?	Text Document	5/1/2019 1:08
switchm_event.log	0	?	Text Document	5/1/2019 1:08
switchm-console.log	5,144,747	?	Text Document	10/28/2019 1:0...
switchm-critical.log	8,496,462	?	Text Document	10/28/2019 1:0...
switchm-perf.log	5,339,875	?	Text Document	10/28/2019 1:0...
switchm-snmp.log	0	?	Text Document	5/1/2019 1:15
switchm-storage-api-util.log	0	?	Text Document	5/1/2019 1:15

Conclusion

SmartZone is a management platform that helps you manage and configure a large number of ICX switches and Ruckus APs from a single pane of glass. Using Zero Touch Provisioning, you can bring up a new switch on SmartZone, manage switches under different switch groups, and apply predefined configurations onto the switches automatically. You can add a specific configuration using switch- and port-level settings, and copy a configuration from one switch to multiple switches. You can define a base-level configuration on only one switch and replicate the configuration to multiple switches with just a few clicks.

Once your network is up and running, you can monitor performance using one or many graphs provided on the dashboard, look at the events and alarms at multiple levels (domain, switch group, and switch) to know more about one or many switch states. You can create one or more custom events and configure SmartZone to send an email message or SNMP trap when an event triggers an alarm.

You can easily schedule traffic results report generation and choose one of the many methods available to distribute the reports. Also, SmartZone provides multiple troubleshooting tools to help you debug the network in case of a failure. A direct connection to each and every network is not required, but troubleshooting can be handled remotely from a single SmartZone instance.

You can use SmartZone to manage and configure edge devices such as the popular Ruckus APs, access-level gigabit and multigigabit PoE switches, aggregation switches, and the high-scale core switches.

References

SmartZone support: https://support.ruckuswireless.com/product_families/11-smartzone-sz

SmartZone 300 Quick Setup Guide: https://support.ruckuswireless.com/documents/2803-smartzone-300-quick-setup-guide

SmartZone 100 Quick Setup Guide: https://support.ruckuswireless.com/documents/2817-smartzone-100-quick-setup-guide

SmartZone 5.1.2 Software Documentation (SZ100/SZ300/vSZ). Refer to the "Managing ICX Switches from SmartZone", "SmartZone Switch Management", and "Troubleshooting Switch Issues" chapters under Administrator Guide. https://support.ruckuswireless.com/documents/2959-smartzone-5-1-2-software-documentation-sz100-sz300-vsz

Ruckus ICX Switch Quick Start Guide: https://support.ruckuswireless.com/documents/1592-ruckus-icx-switch-quick-start-guide-icx-7150-7250-7450-7650



© 2019 CommScope, Inc. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com