

RUCKUS SmartZone (ST-GA) Upgrade 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.

Contents

Contact Information, Resources, and Conventions.....	5
Contacting RUCKUS Customer Services and Support.....	5
What Support Do I Need?.....	5
Open a Case.....	5
Self-Service Resources.....	6
Document Feedback.....	6
RUCKUS Product Documentation Resources.....	6
Online Training Resources.....	6
Document Conventions.....	7
Notes, Cautions, and Safety Warnings.....	7
Command Syntax Conventions.....	7
New In This Document.....	9
Before Upgrading to This Release	11
Upgrade overview.....	11
Upgrade Considerations.....	12
Secure Boot.....	12
Overview.....	12
Requirements.....	13
Considerations.....	13
Virtual SmartZone Minimum Requirements.....	14
Virtual SmartZone Minimum Requirements.....	14
Capacity and Licenses.....	19
Supported Platforms.....	20
Hypervisor CPU/IO Requirements - Self Own Hypervisor.....	21
Maximum Supported AP and Switch Management.....	21
Data Migration Recommendations.....	22
Release Compatibility.....	23
Upgrade Tasks.....	25
Controller Upgrade.....	25
Performing the Upgrade.....	25
Verifying the Upgrade.....	26
Rolling Back to a Previous Software Version.....	26
Creating a Cluster Backup.....	26
SigPack Upgrade.....	27
Upgrading Application Signature Package.....	27
Verifying the SigPack Upgrade.....	27
Rolling Back SigPack Upgrade to the Previous Version.....	28
AP Upgrade.....	28
Upgrading the APs.....	28
Verifying the AP Upgrade.....	31
Rolling Back the AP Upgrade.....	32
AP Bundle Upgrade.....	32
Uploading an AP Firmware Bundle.....	32
Data Plane Upgrade.....	33

Upgrading the Data Plane.....	33
Verifying the DP Upgrade.....	34
Rolling Back the DP Upgrade.....	34
Switch Upgrade.....	35
Uploading the Switch Firmware to the Controller.....	35
Upgrading Switches.....	35
Viewing Firmware History of the Switch.....	42
Ports to Open Between Various RUCKUS Devices, Servers, and Controllers.....	45
Geo Redundancy Upgrade Operation Flow.....	51
Upgrade Path and Cluster Redundancy Deployment.....	51
Active-Standby Mode.....	51
Active-Active Mode.....	52
SOP A.....	52
SOP B.....	54
SOP C.....	55
SOP Z.....	56
Is My Access Point Supported by the Firmware Upgrade?.....	59
Supported Matrix and Unsupported Models.....	59
Supported AP Models.....	59
Unsupported AP Models.....	60
Upgrade FAQs.....	61
Do I Need a Valid Support Contract to Upgrade Firmware?.....	61
Is My Controller Supported by the Firmware Upgrade?.....	61
How Do I Get Support?.....	61

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
- Security Bulletins—<https://support.ruckuswireless.com/security>

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

Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

RUCKUS Product Documentation Resources

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

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

White papers, data sheets, and other product documentation are available at <https://www.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>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<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
bold text	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.

New In This Document

TABLE 2 Key Features and Enhancements in *SmartZone 7.0.0 Rev A (February 2024)*

Feature	Description	Reference
Compatibility Matrix	Updated: Updated 7.0.0 release compatibility.	Release Compatibility on page 23
SigPack Upgrade	Updated: RUCKUS support site link to download regular and non-regular SigPack.	Upgrading Application Signature Package on page 27
Capacity and Licenses	New: Provides license available and their usage across the cluster.	Capacity and Licenses on page 19
Secure Boot	New: The feature allows the implementation of secured boot process.	Secure Boot on page 12
Access Point Models and Switch Management Matrix	Updated: Supported, Unsupported Access Point Models and Switch Management Support Matrix.	Is My Access Point Supported by the Firmware Upgrade? on page 59

Before Upgrading to This Release

- Upgrade overview..... 11
- Upgrade Considerations..... 12
- Secure Boot..... 12
- Virtual SmartZone Minimum Requirements..... 14
- Maximum Supported AP and Switch Management..... 21
- Data Migration Recommendations..... 22

Upgrade overview

NOTE

RUCKUS recommends SmartZone R7.0.0 release for users utilizing Wi-Fi7 APs. For those with legacy APs, RUCKUS suggests using SmartZone R6.1.2 release.

One complete controller release includes software for several components in this architecture, such as:

- Control Plane
- Data Plane
- Access Points

Each one may have its own version number, but all of them are grouped in a single controller version.

Apart from this, you can have other software components also managed from the controller.

Software upgrades for these components might be done separately as it will be covered in 'Upgrade tasks' section. This is a summary:

- Controllers: Control and management plane that will be the first devices to upgrade
- Access Points: They are grouped in Zones inside the controller. Once the controllers are upgraded to a new version or a new AP bundle release is uploaded to the controller, the corresponding AP software release will be available. Then, they can be upgraded per zone.
- Data plane: For this component there are two possible scenarios:
 - Contoller physical appliances: This component is inside the appliance, and it gets upgraded at the same time as the controller.
 - Physical or virtual data planes: This component is an independent device from the controller. It is upgraded from the controller WebUI, after the controllers have been upgraded, and using its own software file. It should not be upgraded before the controller, because management from controller would be lost.
- Application Signature package: This is used by AP Packet inspection features, and it is updated independently from Access Point firmware using its own software file. This update is done from controller WebUI.
- ICX Switch Management: They are grouped in Groups inside the controller. When a new ICX switch management software release is uploaded to the controller, the corresponding software release will be available. Then, they can be upgraded individually or per group.

IMPORTANT

The controller upgrades are only done to update the current cluster from the current version to a later one if the path is supported, and not to an older one. For that reason, a cluster or data plane backup is strongly recommended as the rollback point.

There are other devices or components that will interact or are included in some of the previous devices like IOT, Cloudpath or SCI. But they have their own management system, so they are out of the scope of this guide.

Upgrade Considerations



CAUTION

Beginning with SmartZone 6.1, when using three interfaces, the SZ300 and vSZ-H platforms do not support network configuration with the Control, Cluster, and Management interfaces in the same subnet or VLAN. As a workaround, separate the controller Control, Cluster, and Management interfaces to different subnets or VLANs before upgrading.



CAUTION

Data migration is not supported if system upgrades from release 3.6.x. Existing system and network configuration is preserved, but data such as status and statistics, alarms or events, administrator logs, and mesh uplink history is not migrated to the new release. Contact RUCKUS support for concerns or additional clarifications. [SCG-73771]



CAUTION

When the controller meets the following conditions before upgrading:

- Access & core separation feature is enabled
- UDI interface exists
- There are static routes for UDI interface

Then, after upgrading to release 6.1.0, static routes for the UDI interface will be placed in an incorrect routing table so these destinations will not be reachable. [ER-9597]

For assistance, contact RUCKUS support team using <https://support.ruckuswireless.com>.

NOTE

- Due to change in EAP supplicant timeout from default 12 seconds to 60 seconds (SCG-124967), client fails to get IP when RADIUS proxy switch to secondary server.

It is recommended to change the Radius Option values in WLAN before upgrading the controller or AP to SZ6.1.

Following are values recommended under Radius option in WLAN configuration:

- NAS Request Timeout = 5
- NAS Max Number of Retries Retry = 6
- DP Zone Affinity is renamed to DP Group and DP Group is renamed as Internal DP Group. Please refer to the Admin Guide for DP Group details on this feature.
- It is recommended to upgrade the controller Virtual SmartZone (vSZ) before updating the data plane version because if the data plane version is higher than controller vSZ version then data plane cannot be managed by vSZ platform.

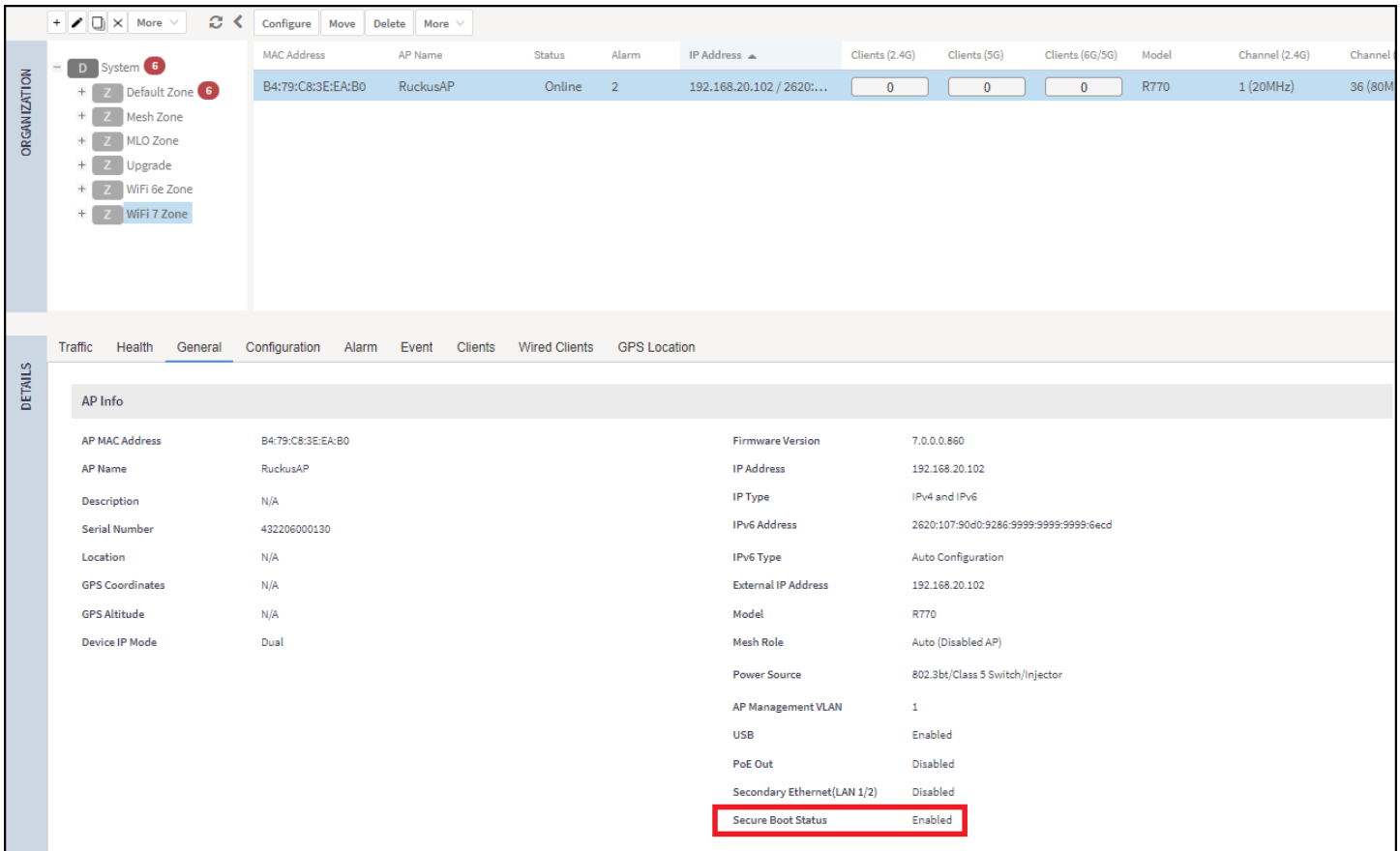
When upgrading vSZ-E/vSZ-H, if the memory/CPU allocation of the current VM instance does not match the lowest resource level of the new VM instance to which the new vSZ-E/vSZ-H version will be installed, you will lose the capacity for APs. On the other hand, if the new VM instance has insufficient hard disk space, a warning message is displayed after you upload the upgrade image, but you will still be able to perform the upgrade.

Secure Boot

Overview

The Secure Boot is a security technology that safeguards against the unauthorized modification of software binaries. The objective of this feature is to implement a secure boot process that includes digital signatures and verification for all bootloader images, up to and including u-boot. This process is designed to prevent unauthorized or corrupted bootloader software from being loaded onto RUCKUS APs during the boot-up sequence.

FIGURE 1 Viewing Secure Boot Status



Requirements

The SmartZone 7.0 and later releases support Secure Boot.

Considerations

NOTE

RUCKUS currently has an Image signing feature, but it's important to note that this feature exclusively signs and verifies the 'rcks_fw.bl7,' which contains the Kernel and Root File System. It does not cover the signing and verification of the bootloader images stored in NOR flash.

Virtual SmartZone Minimum Requirements

Virtual SmartZone Minimum Requirements

NOTE

One or more resources can be higher than the specified requirements. For example, if the instance requires 24Gb RAM, assigning 32Gb RAM is supported.

NOTE

Supported version of the hypervisor may change for every vSZ release. To know the hypervisor version supported for a specific release, refer to the respective release of the Upgrade Guide.

Hypervisor Hardware Performance Requirements

vSZ requires enough hardware resources to sustain the service. vSZ cannot support deployment in low performance hypervisor.

- Sharing hardware server to multiple vSZ instances is not recommended.
- vSZ needs to be deployed on dedicated hardware resource to avoid different VM instance grabbing CPU or IO resources, which can impact vSZ stability in a hypervisor, especially in a scenario where thousands of APs per node are deployed.
- vSZ needs to reach both CPU and IO requirement. Measure the hypervisor hardware performance before deploying vSZ.
- Disks IO is most important in vSZ cluster. Disk IO is the slowest subsystem in a server, which means that write-heavy clusters can easily saturate their disks, which in turn become the bottleneck of the cluster. Avoid network-attached storage (NAS). People routinely claim their NAS solution is faster and more reliable than local drives. NAS is often slower, displays larger latencies with a wider deviation in average latency, and is a single point of failure.

Hypervisor CPU/IO Requirements - Private Hypervisor

CPU Performance Requirement

- CPU single core events per second/per core need > 180 events/sec
- Required CPU level is higher than the Intel Xeon CPU E5-4620 v4 with 2.10 GHz

IO performance requirement detail

vSZ require high IO performance deploy environment. Measure the hypervisor IO performance before deployment. vSZ IO throughput requirements :

- IO requirement per resource level - Refer to the **Disk IO Requirement** column in the resource table.
- Avoid network-attached storage (NAS/SAN). The general claim is that the NAS/SAN solution is faster and more reliable than the local drives. NAS/SAN is often slower, displays larger latencies with a wider deviation in average latency, and is a single point of failure.
- Virtual Disk - Preallocated/Eager Zeroed/Fixed Size is required to provide good performance and low latency for IO. Avoid using "Thick Provision Lazy Zeroed/Dynamic Expanding" to impact IO performance. [*].

How to benchmark vSZ CPU/IO Performance

- The vSZ setup process will detect the IO performance at first setup step.
- Use the SZ CLI in **debug-tools > system > system performance**. The command will run system benchmark on CPU and IO for vSZ.

Network Latency Requirement between vSZ nodes

A fast and reliable network is important for performance in a distributed system. Low latency helps ensure that nodes can communicate easily, while high bandwidth helps shared movement and recovery. Avoid clusters that span multiple data centers, even if the data centers are located in close proximity. It is highly recommended to avoid clusters that span large geographic distances.

vSZ requires low network latency between vSZ nodes on the control & cluster interface network. vSZ cannot support deployment in high network latency environment.

vSZ interface network latency between nodes: Cluster Interface network latency need < 60 ms.

Before upgrading vSZ to this release, verify that the virtual machine on which vSZ is installed has sufficient resources to handle the number of APs, wireless clients and ICX Switches that you plan to manage. See the resource tables below for the **required** virtual machine system resources.

The vCPU, RAM, and Disk Size values are interconnected and must fulfill the minimum requirements within each resource level. When adjusting any of these parameters, all three values must be equal to or greater than the requirements of an existing Resource Level. For instance, considering vSZ-H Resource Level 5, if the number of vCPUs is increased from 4 to 6 or more, the RAM must be adjusted to 22GB or more, and the Disk Size must be adjusted to 300GB or more, ensuring compatibility with or exceeding all the minimum values of Resource Level 6. Failure to meet the minimum requirements of level 6 will result in the vSZ remaining at level 5.

NOTE

The vSZ deployed in the Nutanix Hypervisor introduces more overhead on memory. The 10K AP per node is not sustained on 48GB memory setting. [SCG-113477]

Workaround: When deploying vSZ on Nutanix it is recommended to allocate more memory for vSZ usage. For a 10K AP resource level, setup needs 24 core CPU and 50 GB (+2GB) memory to control. Alternatively decrease to 25% AP deployment in vSZ resource level. For example, 7500 AP in 10K AP resource level.



WARNING

These vSZ required resources may change from release to release. Before upgrading vSZ, always check the required resource tables for the release to which you are upgrading.

NOTE

When initially building up the network it can use a higher Resource Level than needed for the number of APs first deployed, if all the three parameters (vCPU, RAM and Disk Size) **match exactly** with that higher Resource Level.

ATTENTION

It is recommended that there should be only one concurrent CLI connection per cluster when configuring vSZ.

In the following tables the high scale resources are broken into two tables for easy readability. These tables are based on the *AP Count Range*.

TABLE 3 vSZ High Scale required resources

AP Count Range		Max Clients	Nodes per Cluster	AP Count per Node (without Switch)	AP/Switch Capacity Ratio	Maximum Switch (w/o AP)
From	To			Max		Max
10,001	30,000	300,000	4	10,000	5 : 1	6,000
	20,000	200,000	3			4,000
10,001	30,000	300,000	4	10,000	5 : 1	6,000
	20,000	200,000	3			4,000
6,001	10,000	100,000	1-2	10,000	5 : 1	2,000
5,001	6,000	60,000	1-2	6,000	5 : 1	1,200
3,001	5,000	50,000	1-2	5,000	5 : 1	1,000
2,501	3,000	30,000	1-2	3,000	5 : 1	600

Before Upgrading to This Release

Virtual SmartZone Minimum Requirements

TABLE 3 vSZ High Scale required resources (continued)

AP Count Range		Max Clients	Nodes per Cluster	AP Count per Node (without Switch)	AP/Switch Capacity Ratio	Maximum Switch (w/o AP)
From	To			Max		Max
1,001	2,500	25,000	1-2	2,500	5 : 1	500
501	1,000	20,000	1-2	1,000	5 : 1	200
101	500	10,000	1-2	500	5 : 1	100
1	100	2,000	1-2	100	5 : 1	20

TABLE 4 vSZ High Scale required resources

AP Count Range		Nodes per Cluster	Minimum vCPU per node	Minimum RAM per node ^[1]	Minimum Disk Size per node ^[2]	Minimum Disk IO Requirement per node	Preserved Event/ Alarm Days	Concurrent CLI Connection	Resource Level
From	To		Logic Processor	GB	GB	MiB/s	Max	Max (per node not per cluster)	
10,001	30,000	4	24	56	600	45	3/7 Days	4	9 ^[5]
	20,000	3							
10,001	30,000	4	24	48	600	45	3/7 Days	4	8
	20,000	3							
6,001	10,000	1-2	24	48	600	45	3/7 Days	4	7
5,001	6,000	1-2	16	30	300	35	3/7 Days	2	6.6
3,001	5,000	1-2	12	28	300	30	3/7 Days	2	6.5
2,501	3,000	1-2	8	24	300	30	3/7 Days	2	6.1
1,001	2,500	1-2	6	22	300	25	3/7 Days	2	6
501	1,000	1-2	4-6 ^[*4]	18	150	20	3/7 Days	2	5
101	500	1-2	4	16	150	15	3/7 Days	2	4
1	100	1-2	2-4 ^[*3]	13	150	15	3/7 Days	2	3

In the following tables the essential scale resources are broken into two tables for easy readability. These tables are based on the AP Count Range.

TABLE 5 vSZ Essentials required resources

AP Count Range		Maximum Clients	Nodes per Cluster	AP Count per Node	AP/Switch Capacity Ratio	Maximum Switch (w/o AP)
From	To			Max		Max
1025	3,000	60,000	4	1,024	5 : 1	600
	2,000	40,000	3			400
501	1,024	25,000	1-2	1,024	5 : 1	204
101	500	10,000	1-2	500	5 : 1	100
1	100	2,000	1-2	100	5 : 1	20

NOTE

The recommended vCPU core for the vSZ-E with AP Count Range 1 through 100 is 2-4.

TABLE 6 vSZ Essentials required resources

AP Count Range		Nodes per Cluster	Minimum vCPU per node	Minimum RAM per node ^[1]	Minimum Disk Size per node ^[2]	Minimum Disk IO Requirement	Preserved Event/Alarm Days	Concurrent CLI Connection	Resource Level
From	To		Logic Processor	GB	GB	MiB/s	Max	Max (per node not per cluster)	
1025	3,000	4	8	20	250	20	7 Days	2	3
		2,000							
501	1,024	1-2	8	20	250	20	7 Days	2	2
101	500	1-2	4	16	150	15	7 Days	2	1.5
1	100	1-2	2-4 ^[*3]	13	150	15	7 Days	2	1

NOTE

[1] - vSZ-H and vSZ-E have different report interval. For example, AP sends the status to vSZ-E every 90 seconds but to vSZ-H it is sent every 180 seconds, which means that vSZ-E need more RAM in scaling environment based on the resource level.

[2] - NICs assigned to direct IO cannot be shared. Moreover, VMware features such as vMotion, DRS, and HA are unsupported.

Public Cloud Platform - Instance Resource Type

In the following tables the high scale resources are broken into two tables for easy readability. These tables are based on the AP Count Range.

TABLE 7 vSZ High Scale

AP Count Range		Max Clients	Nodes per Cluster	AP Count per Node (without Switch)	Maximum Switch (w/o AP)
From	To			Max	Max
10,001	30,000	300,000	4	10,000	6,000
					20,000
6,001	10,000	100,000	1-2	10,000	2,000
3,001	6,000	60,000	1-2 ^[*4]	6,000	1,200
1,001	3,000	30,000	1-2	3,000	600
501	1,000	20,000	1-2	1,000	200
101	500	10,000	1-2	500	100
1	100	2,000	1-2	100	20

TABLE 8 vSZ High Scale

AP Count Range		Minimum Disk Size	Recommended Machine Type for AWS	Recommended Machine type for Azure	Disk IO Requirement
From	To	GB			
10,001	30,000	600	c5.9xlarge (36 vCPU/72 GB RAM)	F32s_v2 (32 vCPU/64 GB RAM)	45
6,001	10,000	600	c5.9xlarge (36 vCPU/72 GB RAM)	F32s_v2 (32 vCPU/64 GB RAM)	45
3,001	6,000	300	c5.4xlarge (16 vCPU/32 GB RAM)	F16s_v2 (16 vCPU/32 GB RAM)	35

Before Upgrading to This Release

Virtual SmartZone Minimum Requirements

TABLE 8 vSZ High Scale (continued)

AP Count Range		Minimum Disk Size	Recommended Machine Type for AWS	Recommended Machine type for Azure	Disk IO Requirement
From	To	GB			
1,001	3,000	300	m5.2xlarge (8 vCPU/32 GB RAM)	D8s_v3 (8 vCPU/32 GB RAM)	25
501	1,000	150	r5.xlarge (4 vCPU/32GB RAM)	E4s_v3 (4 vCPU/32 GB RAM)	20
101	500	150	m5.xlarge (4 vCPU/16 GB RAM)	D4s_v3 (4 vCPU/16 GB RAM)	15
1	100	150	r5.large (2 vCPU/16 GB RAM)	DS11_v2 (2 vCPU/14 GB RAM) or D4s_v3 (4 vCPU/16 GB RAM)	15

In the following tables the essential scale resources are broken into two tables for easy readability. These tables are based on the *AP Count Range*.

TABLE 9 vSZ Essentials required resources

AP Count Range		Maximum Clients	Nodes per Cluster	AP Count per Node	Maximum Switch (w/o AP)
From	To			Max	Max
1025	3,000	60,000	4	1,024	600
	2,000	40,000	3		400
501	1,024	25,000	1-2	1,024	204
101	500	10,000	1-2	500	100
1	100	2,000	1-2	100	20

NOTE

The recommended vCPU core for the vSZ-E with **AP Count Range** 1 through 100 is 2-4.

TABLE 10 vSZ Essentials required resources

AP Count Range		Minimum Disk Size	Recommended Machine Type for AWS	Recommended Machine type for Azure	Disk IO Requirement
From	To	GB			
1025	3,000	250	m5.2xlarge (8 vCPU/32 GB RAM)	D8s_v3 (8 vCPU/32 GB RAM)	20
	2,000				
501	1,024	250	m5.2xlarge (8 vCPU/32 GB RAM)	D8s_v3 (8 vCPU/32 GB RAM)	20
101	500	150	m5.xlarge (4 vCPU/16 GB RAM)	D4s_v3 (4 vCPU/16 GB RAM)	15
1	100	150	r5.large (2 vCPU/16 GB RAM)	DS11_v2 (2 vCPU/14 GB RAM) or D4s_v3 (4 vCPU/16 GB RAM)	15

NOTE

- [1] - Increase the vSZ total memory 2~4 GB when running on special or extreme deploy environment when vSZ raise a memory exceed (90%) alarm. For example:
 - Deploy 4-node vSZ cluster on Nutanix with full 30K AP capacity.
 - One vSZ node down in 4-node vSZ cluster to long term sustain 30K AP in 3 alive vSZ nodes.

The solution should be recovered the fail vSZ node as soon as possible. But if user need run 3 nodes with 30K AP in long term sustain, it need to increase the vSZ memory to run.
 - All APs with full statistic reports (AVC, HCCD, UE, ...) to the controller on full load stress condition.
- [2] - Required Disk Type
 - AWS: General Purpose SSD (gp2)
 - GCE: SSD
 - Azure: Standard-SSD
- [3] - If deployed hardware CPU computing performance is not good as recommended in 100 AP resource level, the 2 cores CPU setting cannot be supported. Upgrade to 4 cores instead of 2 cores in this case.
- [4] - If deployed hardware CPU computing performance is not good as recommended Hypervisor (like Hyper-V) in 4-CPU setting to support 1000K AP, upgrade to 6 cores instead of 4 cores in this case.
- [5] - Resource level 9 is added for cases that does not sustain the loading with resource level 8.
- The 6000 AP resource profile level could support to 4 nodes cluster. The total supported AP number will be up to 18,000 APs in a 4 node vSZ cluster.
- Workaround if virtualization platform always need Thin Provision/Lazy Zeroed/Dynamic Expanding case.

Change Log of vSZ Resource Plan

- New support for 3000, 6000 APs resource level for more flexible deployment and better cost effectiveness for customer.
- Due to system limitation for the minimum disk requirement, the base disk size requirement is increased from 100 GB to 150 GB on low level resource profile. This has no impact to upgrade from the previous version. For a new vSZ setup, follow the new disk size specified in the resource table. For an existing vSZ setup, shutdown the VM and increase the disk size.
- As the resource level has hit the system limitation in some case, for the vSZ-E 1024 APs resource level memory is increased from 18 GB to 20 GB. No impact for user to upgrade from previous version. User need to change only the memory setting when encountering memory usage alarm exceeding 90%.
- Adding additional notes vSZ memory required in extreme vSZ deployment and cases.
- New session, vSZ-H instance Resource Allocate Instruction, is added.

Capacity and Licenses

Capacity is the maximum information transfer limit of a network at the given point. The Licenses page displays the current count of all licenses and their usage across the cluster.

1. Go to **Administration > System Info > System Summary > Total Capacity**.

Before Upgrading to This Release

Virtual SmartZone Minimum Requirements

- Capacity varies in different conditions as mentioned below.

The tab displays the following options:

- 2 Radio AP:** 2 Radio AP takes 1 capacity.
- 3 Radio AP:** 3 Radio AP takes 2 capacity.
- Switch:** Switch takes 5 capacity.

The AP capacity license refers to the number of approved APs, while the Connected AP represents the total number of APs that are currently connected to the controller. AP capacity is based on system resources (CPU/RAM) and not the AP license count.

For example, a single vSZ-H can support:

10,000 2-radio APs (1x resources) or 5,000 3-radio APs (2x resources) or 2,000 ICX switches (5x resources).

Supported Platforms

This section displays summary of platforms supported by vSZ in this release version.

Hypervisors supported by vSCG/vSZ

TABLE 11 Supported Hypervisors

Vendor	Hypervisor	Version
VMWare	ESXi	5.5 and later (7.0 or later recommended)
Microsoft	Windows Server Hyper-V	Windows Server Hyper-V (2019 and 2022)
KVM	CentOS	7.5 (1804), 7.7 (1908), 8 (1905), 8.2 (2004), 8.3 (2011), 8.4 (2105), and 8.5 (2111)
OpenStack	Ubuntu	Xena and Yoga
Nutanix	Nutanix	Nutanix Community Edition

TABLE 12 Supported Public Cloud Platforms

Vendor
AWS (Amazon Web Service)
Google Cloud
Microsoft Azure

NOTE

RUCKUS only supports usage of vSZ on the above named virtualization platforms.

TABLE 13 Unsupported Platforms

vSZ
Sangfor HCI
VMWare Workstation/Workstation Player
Oracle VM Virtual Box

NOTE

The above mentioned hypervisor platforms are not currently supported by the RUCKUS controller. If vSZ is run on any of the platforms officially not supported or assured by RUCKUS, any errors encountered in vSZ cannot be investigated by RUCKUS support. The above list is not exhaustive, it serves only to clarify the unsupported hypervisors.

Hypervisor CPU/IO Requirements - Self Own Hypervisor

Benchmarking vSZ CPU/IO Performance

System Benchmark Tool included in this release can be used to measure Hypervisor performance. It provides the benchmark result and performance measure to run vSZ on CPU (Central Processing Unit) and IO (Input Output).

Command Location:

```
CLI > debug > debug-tools > system-performance
```

Performance Requirement

CPU	CPU single core events per second/per core need > 180 events/second.
IO	Requirements change per resource level. Refer to resource table for minimum values (column 'Disk IO requirement')

Maximum Supported AP and Switch Management

The tables below list the maximum supported resources between APs and switches.

SmartZone 6.1.x support dynamic (linear) AP/Switch capacity based on capacity ratio. No AP/Switch mode, only mix mode and AP/Switch support number base on total amount connect AP/Switch capacity.

Capacity Ratio

High scale profile with higher switch support capacity to 5:1 from 8:1

vSZ-H L6 ~ L8

5:1 (10000 AP : 2000 switches)

Example: Calculating the Total Capacity

- 200 APs + 100 switches (1:5)
 $(200 \times 1) + (100 \times 5) = 700$ (Total Capacity) This requirement could use L5, since the total capacity is smaller than 1,000.
- 400 APs + 10 switches (1:5)
 $(400 \times 1) + (10 \times 5) = 450$ (Total Capacity) This requirement could use L4, since the total capacity is smaller than 500.

NOTE

These required resources may change from release to release. Before upgrading, always check the required resource tables for the release to which you are upgrading.

TABLE 14 AP and Switch resource table for 1 and 2 nodes

Profile	1 and 2 Nodes				1 or 2 Nodes
Capacity	AP Mode		Switch Mode		AP/Switch Capacity Ratio
SZ100	1,024	0	0	204	5:1
SZ144	2,000	0	0	400	5:1
SZ300	10,000	0	0	2,000	5:1
vSZ-E L1	100	0	0	20	5:1
vSZ-E L1.5	500	0	0	100	5:1
vSZ-E L3	1,024	0	0	204	5:1
vSZ-H L3	100	0	0	20	5:1
vSZ-H L4	500	0	0	100	5:1
vSZ-H L5	1,000	0	0	200	5:1
vSZ-H L6	2,500	0	0	500	5:1
vSZ-H L6.5	5,000	0	0	1,000	5:1
vSZ-H L8	10,000	0	0	2,000	5:1

In the following tables for three and four nodes are broken into two tables for easy readability.

TABLE 15 AP and Switch resource table for 3 and 4 nodes

Profile	3 Nodes					4 Nodes				
Capacity	AP Mode		Switch Mode		AP/Switch Capacity Ratio	AP Mode		Switch Mode		AP/Switch Capacity Ratio
SZ100	2,000	0	0	400	5:1	3,000	0	0	600	5:1
SZ144	4,000	0	0	800	5:1	6,000	0	0	1,200	5:1
SZ300	20,000	0	0	4,000	5:1	30,000	0	0	6,000	5:1
vSZ-E L3	2,000	0	0	400	5:1	3,000	0	0	600	5:1
vSZ-H L8	20,000	0	0	4,000	5:1	30,000	0	0	6,000	5:1

Data Migration Recommendations

If you need to preserve your data or reports, consider the following recommended options before upgrading:

- Leverage an existing SCI platform to send statistics and reports to SCI before the upgrade.

NOTE

SCI comes with a free 90-day evaluation.

- Backup and export existing statistics and reports using Export tools or Streaming API before the upgrade.
- Connect your cluster to RUCKUS AI platform to send multiple data sources to get reporting and other capabilities.

Release Compatibility

The controller provides release compatibility in two forms:

- **Upgradability:** Controller new release can support upgrade from certain previous release trains. This would be limited to software releases (GA, GD or MRs from previous trains) that were already published at the time of new SmartZone release being available.
- **AP zone support:** A new SmartZone release supports AP zone firmware from certain prior releases; different AP zones may use any of the supported firmware releases.

NOTE

The controller data plane devices follow the AP zone compatibility policy as set forth in this section. Data plane devices are compatible with controller in the same way APs are compatible with the controller.

The supported paths for Short Term (ST) and Long Term (LT) releases are the same, and maintain the following compatibilities:

- An ST release is compatible with its current release train and the immediate prior LT GD release train for upgradability and AP Zone support.
- An LT release is compatible with its current release train, the immediate prior ST release, and the latest LT GD (General Deployment) release in immediate prior LT train for upgradability and AP Zone support.
- An LT GD release is compatible with its current release train, the immediate prior ST release, and two immediate prior LT GD releases for upgradability and AP Zone support.

For more information on release definition, refer to RUCKUS Support Portal at <https://support.ruckuswireless.com>.

This SmartZone release is a long-term (LT) release. Refer to the following table for a compatibility matrix for all controller platforms.

TABLE 16 SZ 7.0.0 Compatibility Matrix

Previous releases	7.0.0 (ST GA)
3.6.2.0.78, 3.6.2.0.222, 3.6.2.0.250 (LT GD)	x
5.1.0.0.496, 5.1.1.0.589, 5.1.1.0.598, 5.1.2.0.302 (ST GA)	x
5.2.0.0.699, 5.2.1.0.515 (LT GA)	x
5.2.2.0.317, 5.2.2.0.1161, 5.2.2.0.1562, 5.2.2.0.1563 (LT GD)	x
6.0.0.0.1331 (ST GA)	x
6.1.0.0.935 (LT GA)	√
6.1.1.0.959 (LT GA)	√
6.1.2.0.354, 6.1.2.0.404 (LT GD)	√

NOTE

The AP firmware version that comes in compatible controller releases included in the table, or any later AP firmware patch from those versions can be used.

NOTE

*- Additional support for this path beyond the base policy has been added due to special requirements.

If you are running an earlier version, you must first upgrade to a compatible version, as shown in the table, before upgrading to this release.



CAUTION

To help ensure that the cluster firmware upgrade process can be completed successfully, the cluster interfaces of all nodes must be connected and up.

Release Compatibility

REMEMBER

Before you proceed with upgrading the controller to this release, ensure that all AP zones are running one of the supported firmware versions. Otherwise, the cluster upgrade will be blocked.

Upgrade Tasks

- Controller Upgrade..... 25
- SigPack Upgrade..... 27
- AP Upgrade..... 28
- AP Bundle Upgrade..... 32
- Data Plane Upgrade..... 33
- Switch Upgrade..... 35

Controller Upgrade

Performing the Upgrade

Consult the RUCKUS Support website on a regular basis for updates that can be applied to your RUCKUS network devices.



CAUTION

Although the software upgrade process has been designed to preserve all controller settings, RUCKUS strongly recommends that you back up the controller cluster before performing an upgrade. Having a cluster backup will ensure that you can easily restore the controller system if the upgrade process fails for any reason. Upload the backup files from all the nodes in a cluster to a remote FTP server or download them from SZ WebUI



CAUTION

RUCKUS strongly recommends that you ensure that all interface cables are intact during the upgrade procedure.



CAUTION

RUCKUS strongly recommends that you ensure that the power supply is not disrupted during the upgrade procedure.

Before starting this procedure, you should have already obtained a valid controller software upgrade file from RUCKUS Support or an authorized reseller.

1. Copy the software upgrade file that you received from RUCKUS to the computer where you are accessing the controller web interface or to any location on the network that is accessible from the web interface.
2. Select **Administration > Administration > Upgrade > Upgrade**.

In **Current System Information**, the controller version information is displayed.

NOTE

The **Upgrade History** tab displays information about previous cluster upgrades.

3. From **Upload**, turn on **Run Pre-Upgrade Validations**. It triggers data migration validation during upload process.
4. Click **Browse** to select the patch file.
5. Click **Upload** to upload the new image (.ximg file) to system. The controller uploads the file to its database, and then performs the data migration verification. After the verification is done, the **Patch for Pending Upgrades** section is populated with information about the upgrade file. If verification fails, the following error is displayed:

```
Exception occurred during the validation of data migration. Please apply the system configuration backup and contact system administrator.
```

Upgrade Tasks

Controller Upgrade

6. If the controller configuration upload is successful, click **Backup & Upgrade** to back up the controller cluster and system configuration before performing the upgrade.

When the upgrade (or backup-and-upgrade) process is complete, the controller logs you off the web interface automatically. When the controller login page is displayed again, you have completed upgrading the controller.

Verifying the Upgrade

You can verify the process was successful as follows:

1. Select **Administration > Administration > Upgrade > Upgrade**.
2. In the **Current System Information** section, select the value for **Controller Version**. The upgrade process is successful, if the **Controller Version** displays the latest software version than the software version that the controller was using before you started the upgrade process.

You can also go to Upgrade History section and verify there is a new line with State Successful and System version changed to the latest version.

Rolling Back to a Previous Software Version

If you encounter issues during the software upgrade process and the controller cannot be upgraded successfully, you may want to roll back the controller software to a previous version.

To be able to restore the software to the previous software version, you must perform a cluster backup before upgrading. Refer to [Creating a Cluster Backup](#) on page 26. To roll back to the previous version, perform either Step 1 or Step 2 depending on the outcome of the software upgrade.

1. If the upgrade fails, access all the node's command-line interface (CLI) and run the **restore** command to the local system simultaneously.
2. If the upgrade succeeded, the restore can be run from either the CLI or through the WebUI.

For details about performing a cluster backup, see the “Backing Up and Restoring Clusters” section of the appropriate product *Management Guide*.

Creating a Cluster Backup

Backing up the cluster (includes OS, configuration, database and firmware) periodically enables you to restore it in the event of an emergency. RUCKUS also recommends that you back up the cluster before you upgrade the controller software.

1. Go to **Administration > Administration > Backup and Restore**.
2. Select the **Cluster** tab.
3. In Cluster Backup and Restore, click **Backup Entire Cluster** to backup both nodes in a cluster.

The following confirmation message is displayed: Are you sure you want to back up the cluster?

4. Click **Yes**.

The following message is displayed: The cluster is in maintenance mode. Please wait a few minutes.

When the cluster backup process is complete, a new entry is displayed in the **Cluster Backups History** section with a **Created On** value that is approximate to the time when you started the cluster backup process.

SigPack Upgrade

Upgrading Application Signature Package

AP DPI feature uses an Application Signature Package that in general it can be optionally updated when a new version is available.

NOTE

As R5.1.x to R6.1 release upgrade is not supported, RUCKUS does not have any signature-package upgrade restrictions during zone upgrade.

There are two types of Application Signature Package files available in the Support site:

- Regular Signature package: This package can be used for any scenario but is required if you intend to use the Client Virtual ID Extraction feature available in WLAN configuration. This type of file is not supported by 802.11ac Wave 1 AP running firmware prior to 6.0.
- Non-regular Signature package: This package can be used for any other scenario and is compatible with any supported AP model and firmware version.

This package can be updated to the latest available version that is suggested by the controller or to a file downloaded from RUCKUS download center.

Complete the following steps to update the signature package in all APs in a cluster.

1. Download the following file as required from the RUCKUS support site. In other case, you can skip this step.
 - Regular Signature package only for SZ7.0.0: <https://support.ruckuswireless.com/admin/software/3960-smartzone-7-0-ga-sigpack-1-670-2-regular-application-signature-package>.
 - Non-Regular Signature package for SZ7.0.0 and older releases: <https://support.ruckuswireless.com/admin/software/3961-smartzone-7-0-ga-sigpack-1-670-2-application-signature-package>.
2. From the controller web UI, select **Security > Application Control > Application Signature package**.
 - a. If you choose to install the latest version available in the Support site, go to **Latest available from support site > Check Now > For any latest update > Install**.

NOTE

If Regular and Non-regular Signature package files are available in latest version from support site, SZ will offer to download and install the Regular version. If your AP models do not support it, they will fail to download it and stay in their current Signature package version.

- b. If you choose to install a version downloaded in step 1, go to **Upload Signature Package** section and click **Browse**.
- c. Select the file the version you intend to install and click **Upload** to install that signature package.

After the signature package file is installed or uploaded successfully, the controller will logoff the users.

NOTE

More details can be found in *Security Guide*, in section *Working with Application Signature Package*

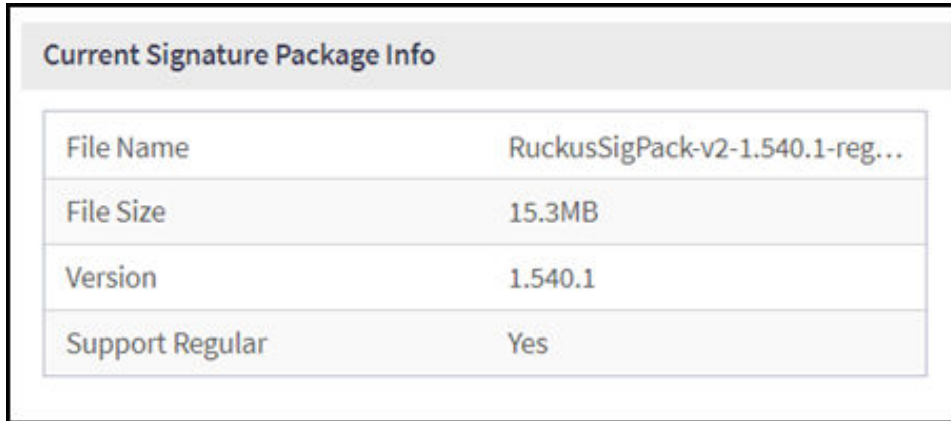
Verifying the SigPack Upgrade

You can verify if the upgrade process was successful as follows:

1. Select **Security > Application Control > Application Signature package**.

- From the **Current Signature Package Info** section, verify if the filename matches with the one that is uploaded and installed.

FIGURE 2 Verifying the SigPack



Current Signature Package Info	
File Name	RuckusSigPack-v2-1.540.1-reg...
File Size	15.3MB
Version	1.540.1
Support Regular	Yes

Rolling Back SigPack Upgrade to the Previous Version

You can roll back to a previous SigPack version with these steps.

- Download the desired Sigpack version from the RUCKUS support site.
- From the controller web UI, select **Security > Application Control > Application Signature package**.
- Go to the **Upload Signature Package** section, click **Browse** and select the file and the version you intend to install.
- Click on **Upload** to install that signature package.

After the signature package file is installed or uploaded successfully, the controller will logoff the users.

AP Upgrade

Upgrading the APs

When the controller is upgraded, a new software version is available for the APs, which is not upgraded automatically along with the controller. Instead, they are upgraded independently per zone (which can have different software versions) following these steps:

- Manual upgrade per zone or group of zones: Refer, [Changing the AP Firmware Version of the Zone](#) on page 28.
- Scheduled upgrade per zone or group of zones: Refer, [Schedule Zone Firmware Upgrade](#) on page 29.

Changing the AP Firmware Version of the Zone

The controller supports multiple firmware versions. You can manually upgrade or downgrade the AP firmware version of the zone.

Complete the following steps to change the AP firmware version of the zone.

- From the **Access Point** page, locate a zone for which you want to upgrade the AP firmware version.

NOTE

To upgrade multiple zones, click the **Zone** view mode and select the zones by holding down the Ctrl key and clicking each of the zones.

2. Click **More** and select **Change AP Firmware**. The **Change AP Firmware** dialog box displays the current AP firmware version.
3. Select the firmware version you need. If you upgrade to a new firmware version, a backup configuration file will be created. You can use this backup file to downgrade to the original firmware version.

NOTE

If the multiple zones do not have the same supported firmware version, the dialog box displays the following message: These Zones do not have same supported AP firmware available for upgrade/downgrade.

4. Click **Yes**, and a confirmation message is displayed stating that the firmware version was updated successfully.

NOTE

If any zone fails to upgrade, a dialog box displays to download an error CSV list.

5. Click **OK**. You have completed changing the AP firmware version of the zone.

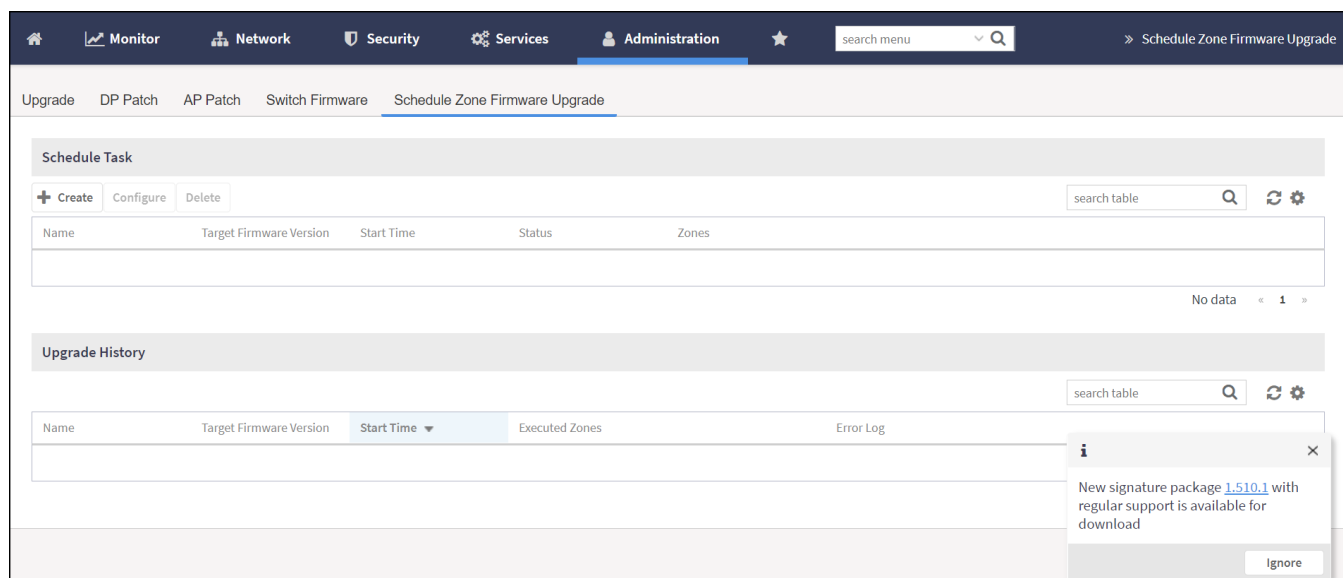
Schedule Zone Firmware Upgrade

Allows user to setup a schedule time to upgrade/downgrade single or multiple zone firmware.

After a zone firmware upgrade/downgrade task is executed, user can see the zone firmware change history.

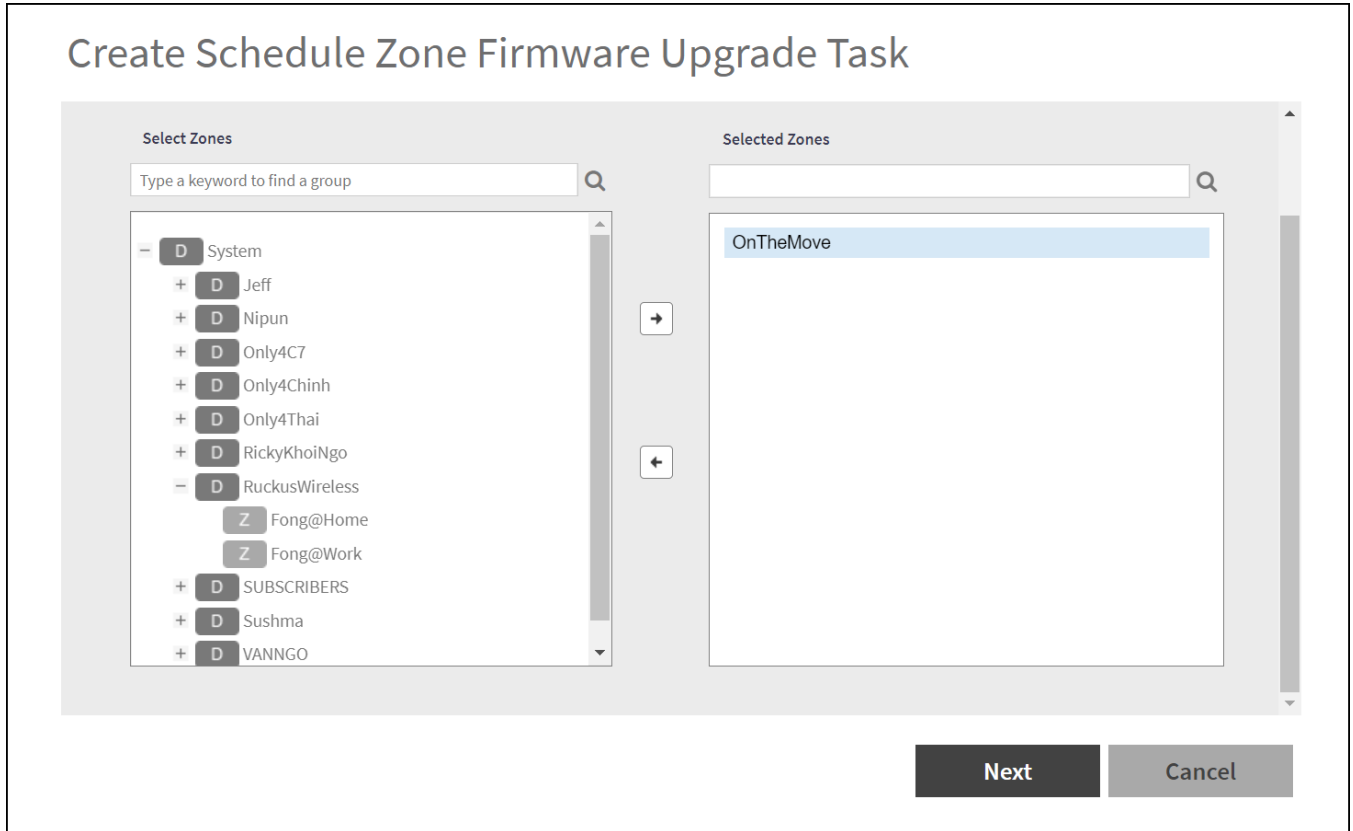
1. Go to **Administration > Upgrade > Schedule Zone Firmware Upgrade**.

FIGURE 3 Schedule Zone Firmware Upgrade



- click **Create**, the **Create Schedule Zone Firmware Upgrade Task** page is displayed.

FIGURE 4 Schedule Zone Firmware Upgrade



- Select the required zone from the **Select Zones** list and move it to the **Selected Zones** list.

- Click **Next**, the **Schedule** tab page is displayed.

FIGURE 5 Configuring the Schedule

Configure Schedule Zone Firmware Upgrade Task

Zone → **Schedule** → Review

It is recommended that AP Firmware version should be same as DP version. The same versions of AP(s) and DP(s) could ensure a consistent agreement on functional communication.

Update to 6.1.0.99.716
Update to 6.1.0.99.721

← Upgrade versions

Please upgrade all DP members of this zone's DP Group. The version that zone can be upgraded is depending on this zone's DP Group version.

* Name:

* Change firmware to:

* Schedule time:

Back Next Cancel

- Enter a **Name**.
- Select the upgrade version from the list. The **Change Firmware to** field will automatically be updated with the selected version.
- Select the **Schedule time**.
- Click **Next**.
- Review the task and click **OK**.

Verifying the AP Upgrade

You can verify if the upgrade process was successful as follows:

- Select **Network > Access Points**.
- Choose the zone you have upgraded, click **More** and select **Change AP Firmware**. The **Change AP Firmware** dialog displays the current AP firmware version.

Rolling Back the AP Upgrade

You can rollback to the previous software version that was running in an AP zone as follows:

NOTE

With this process you will also rollback to the configuration and AP list that this zone had when it was upgraded from the selected version.

1. Select **Network > Access Points**.
2. Choose the zone you have upgraded, click **More** and select **Change AP Firmware**. The **Change AP Firmware** dialog box displays the current AP firmware version and the list of available AP Firmware version to roll back.
3. Select the firmware version you need and click **Yes**.
A confirmation message is displayed stating that the firmware version was updated successfully.
4. Click **OK**. You have completed changing the AP firmware version of the zone.

AP Bundle Upgrade

Uploading an AP Firmware Bundle

An AP Patch is a separate software file only containing a new version for AP component. It can be uploaded into an SZ cluster to add that new version for this component. Main purposes:

- New AP model: Patch is introducing a new AP model not supported into that release version yet.
- Bug fix: Patch containing additional software fixes compared to previous official AP version.

To upload an AP patch in a SmartZone cluster:

1. Select **Administration > Administration > Upgrade > Upgrade**.
2. Select the **AP Patch** tab.
3. In Patch File Upload, click **Browse** to select the patch file (with extension .patch).
4. Click **Open**.
5. Click **Upload**. The upload status bar is displayed, and after the patch file is uploaded, the section is populated with the patch filename, size, firmware version, and supporting AP models.
6. Click **Apply Patch**. The apply patch status bar is displayed.

After the patch file is updated, you will be prompted to log out.

When you login again, the **AP Patch History** section displays information about the patch file such as start time, AP firmware and model.

You have successfully updated the AP models and AP firmware with the patch file, without having to upgrade the controller software.

For upgrading, verifying and rolling back tasks using this AP patch, you can refer to the same steps described in [AP Upgrade](#) on page 28.

Data Plane Upgrade

Upgrading the Data Plane

You can view and upgrade the virtual data plane version using patch files. This feature is only supported on vSZ-H and vSZ-E.



CAUTION

RUCKUS strongly recommends that you back up the data plane before performing an upgrade. Having this backup will ensure that you can easily restore the data plane if the upgrade process fails for any reason. For this you have Backup and Restore options in the same page where Upgrade is performed.

NOTE

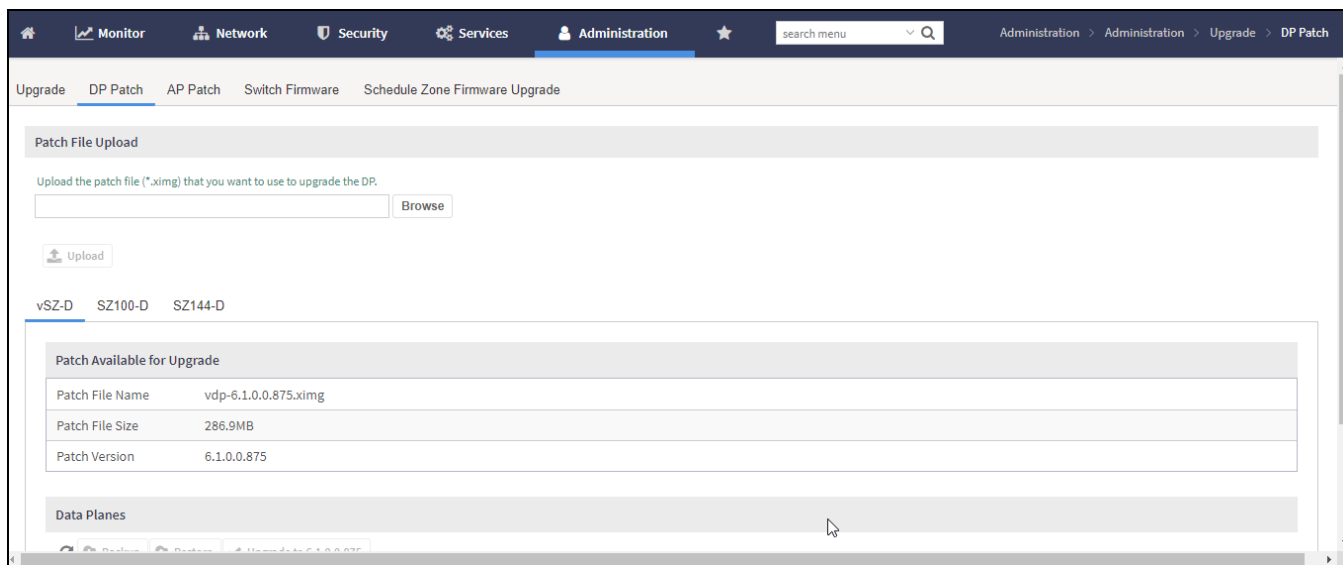
This task is applicable only for external Data planes

To Upgrade the Data Plane:

1. Select **Administration > Administration > Upgrade**.
2. Select the **DP Patch** tab.

The **DP Patch** page is displayed.

FIGURE 6 Upgrading the Data Plane



3. In **Patch File Upload**, click **Browse** to select the patch file (.ximg file).

Upgrade Tasks

Data Plane Upgrade

4. Click **Upload**.

The controller automatically identifies the Type of DP (vSZ-D or SZ-D) and switches to the specific Tab page. Uploads the file to its database, and then performs file verification. After the file is verified, the **Patch for Pending Upgrade** section is populated with information about the upgrade file.

The following upgrade details are displayed:

- Patch File Name—Displays the name of the patch file.
- Patch File Size—Displays the size of the patch file.
- Patch Version—Displays the version of the patch file.

5. In **Data Planes**, choose a patch file version from the **Select upgrade version**.

6. Click **Apply** to apply the patch file version to the virtual data plane.

A pop-up prompting data plane backup is displayed.

7. Click **Upgrade Anyway** to proceed without a data plane backup or click **Backup** to create a backup.

The following information about the virtual data plane is displayed after the patch file upgrade is completed.

- Name—Displays the name of the virtual data plane.
- DP MAC Address—Displays the MAC IP address of the data plane.
- Current Firmware—Displays the current version of the data plane that has been upgraded.
- Backup Firmware—Displays the backup version of the data plane.
- Last Backup Time—Displays the date and time of last backup.
- Process State—Displays the completion state of the patch file upgrade for the virtual data plane.
- DP Status—Displays the DP status.

You have successfully upgraded the virtual data plane.

Verifying the DP Upgrade

You can verify if the upgrade process was successful as follows:

1. Select **Administration > Upgrade > DP Patch**.
2. Select the tab for the upgraded data plane model.
3. Look for the Data plane that is upgraded and verify the **Current Firmware** column if its value corresponds to the software version it has been upgraded to.

Rolling Back the DP Upgrade

To be able to restore the software to the previous software version, you must perform a data plane backup before upgrading. To roll back to the previous version, perform the following steps:

1. Select **Administration > Upgrade > DP Patch**.
2. Select the tab for the data plane model upgraded.
3. Select the Data plane and click on **Restore**.

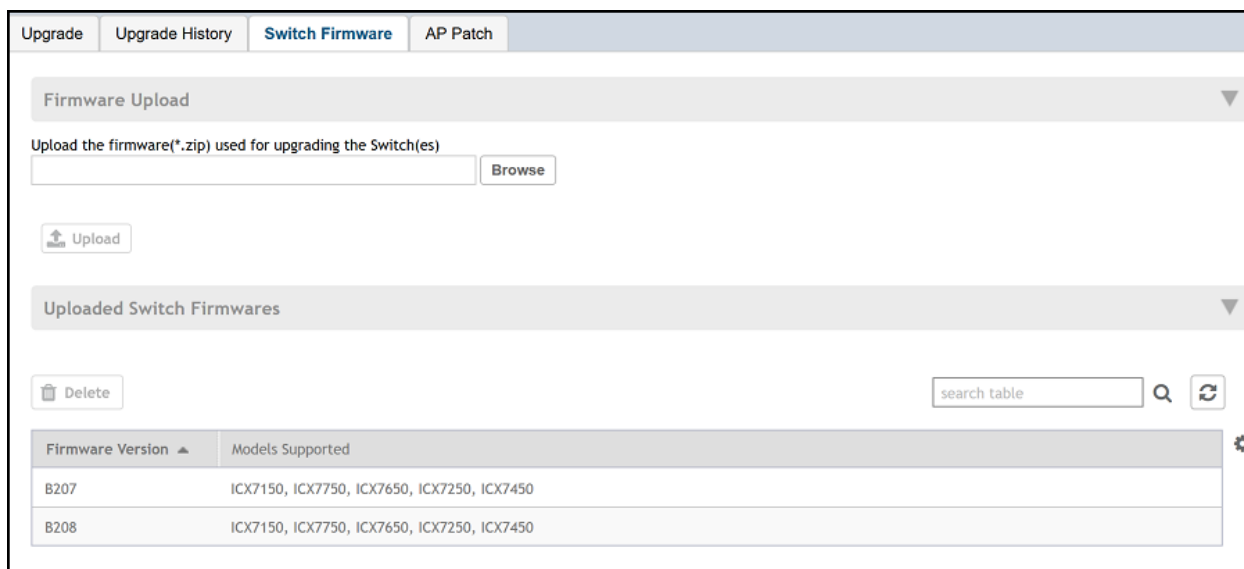
Switch Upgrade

Uploading the Switch Firmware to the Controller

You can upload the latest available firmware to a switch from the controller, thereby upgrading the firmware version of the switch.

1. Select **Administration > Administration > Upgrade**.
2. Select the **Switch Firmware** tab.

FIGURE 7 Upgrading the Switch Firmware



3. In Firmware Upload click **Browse** to select the firmware file for upgrading the switch.
4. Click **Open**.
5. Click **Upload**. The upload status bar is displayed, and after the firmware file is uploaded, the **Uploaded Switch Firmwares** section is populated with the firmware version and switch models it supports.

You have successfully uploaded the switch firmware to the controller.

Upgrading Switches

RUCKUS switches starting from 08.0.90 releases supports unified images which require two step process from prior releases. The two step process is:

1. Step 1 - Upgrade from **08.0.80 (non- Unified FastIron Image (UFI) or UFI) > 08.0.90 UFI**
2. Step 2 - Upgrade from **08.0.90 UFI > 08.0.90a UFI**

NOTE

Refer to RUCKUS FastIron Software Upgrade Guide, 08.0.90 for details.

Ensure that the image version in both primary and secondary partition use 8.0.80 or later version.

You can upgrade switches per switch group or selected switches as explained in the following sections.

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**.

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

FIGURE 8 Selecting Firmware Upgrade for a Switch Group

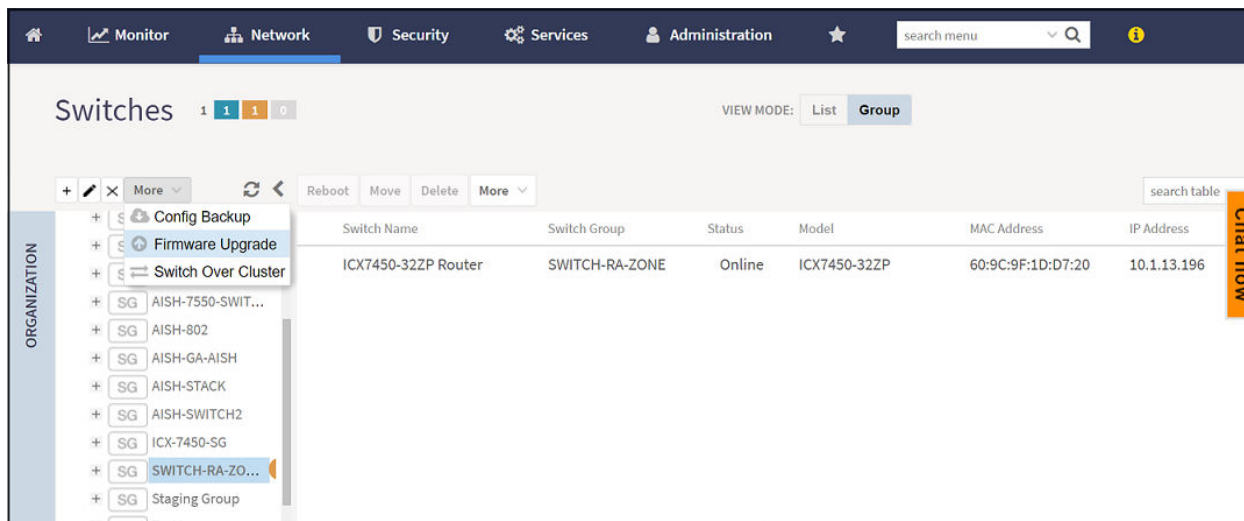
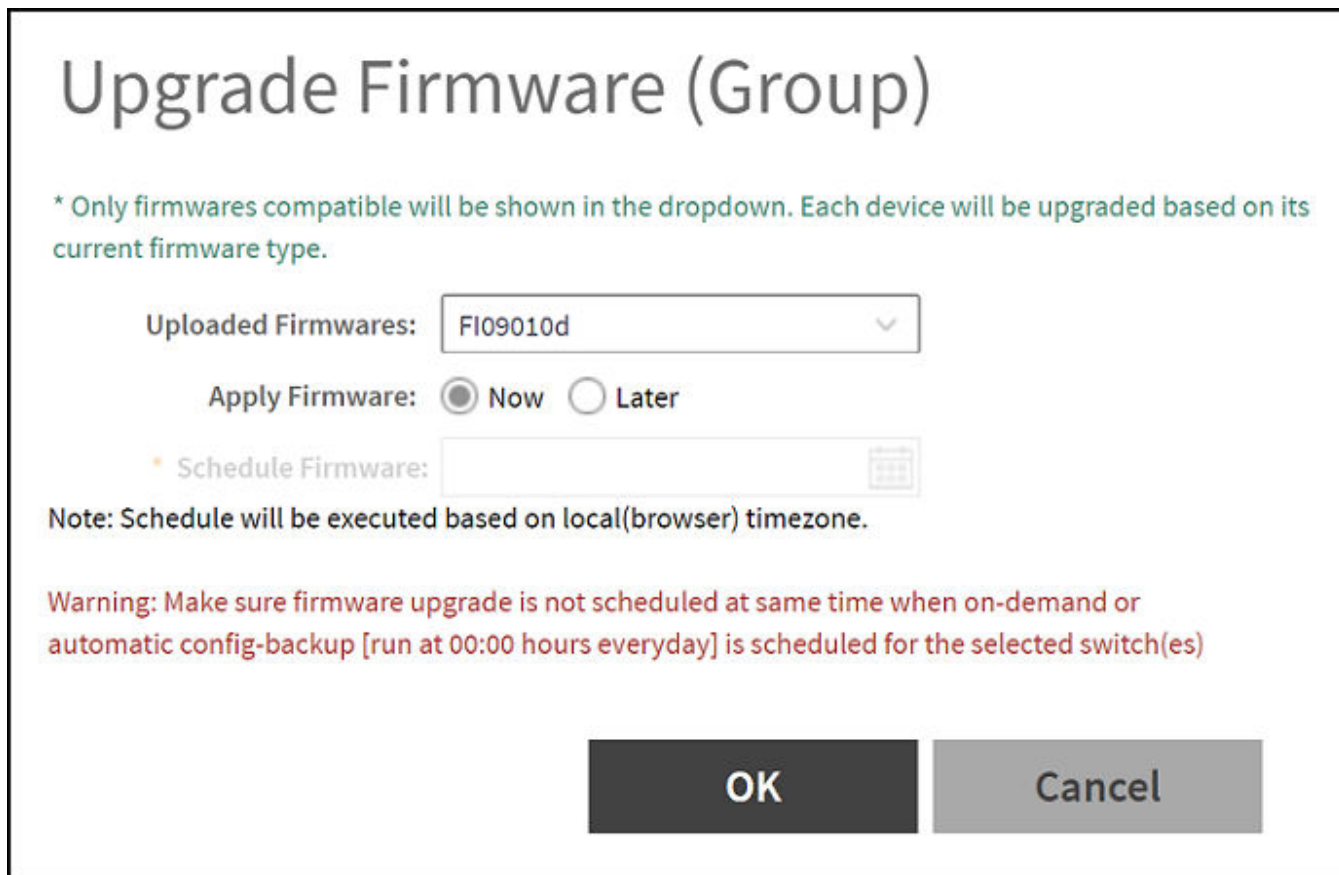


FIGURE 9 Scheduling the Upgrade for a Switch Group



Upgrade Tasks

Switch Upgrade

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

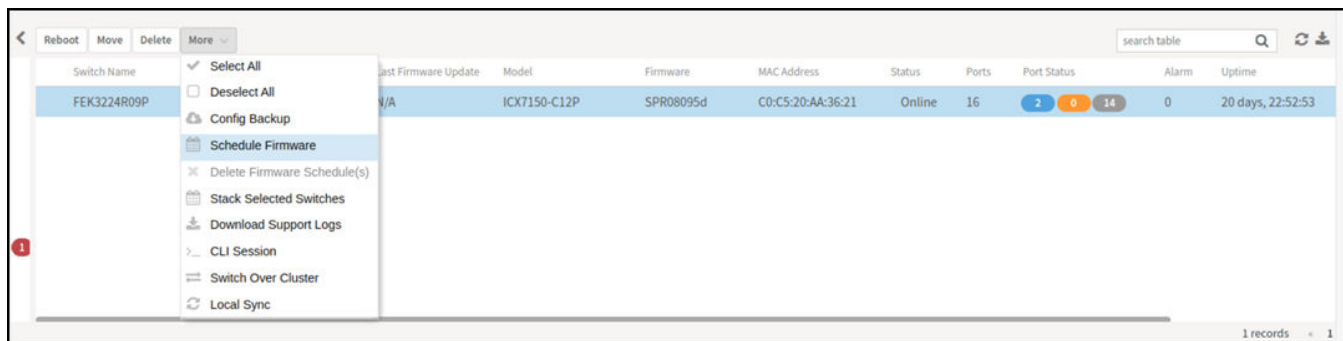
1. From the main menu, click **Network > Wired > Switches**.
The **Switches** page is displayed.
2. Select a **Domain > Switch Group** or specific **Switch Group** and select the **Switch** that you want to upgrade.

NOTE

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

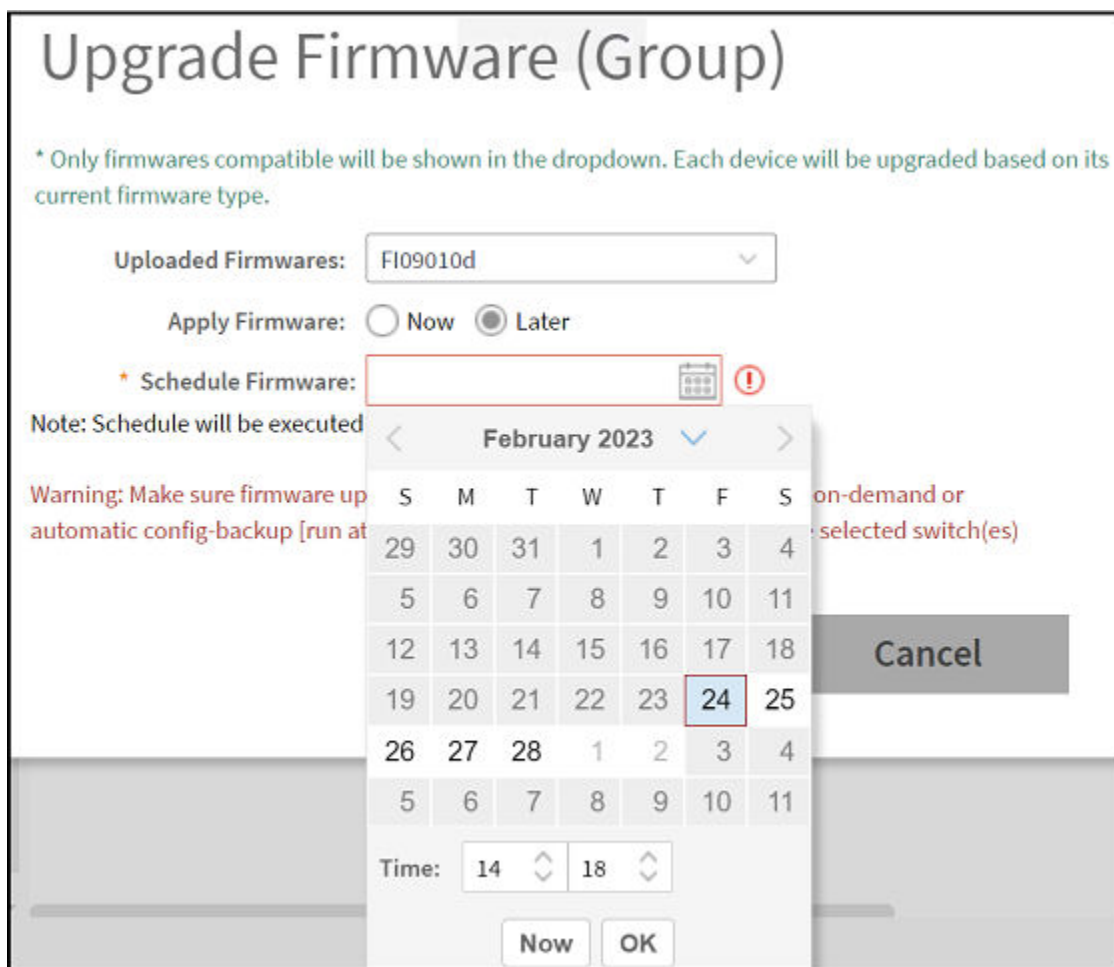
3. Click **More > Schedule Firmware**.

FIGURE 10 Selecting Schedule Firmware



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

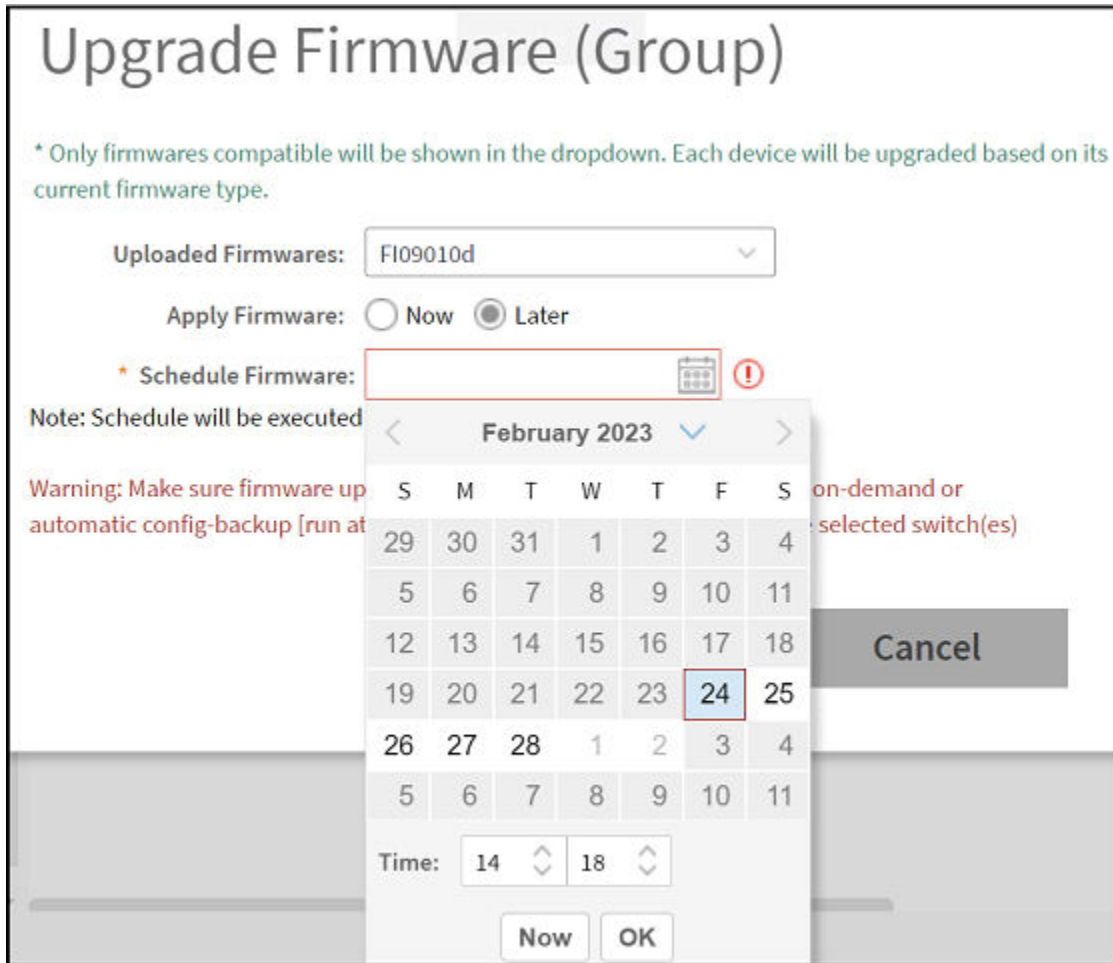
FIGURE 11 Scheduling Firmware Upgrade



Upgrade Tasks
Switch Upgrade

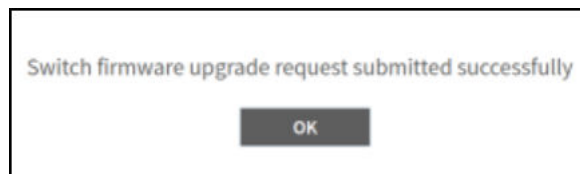
- Complete the following fields:
 - Uploaded Firmwares:** Select the firmware version that you want the switch to be upgraded to.
 - Firmware Type:** Select type of firmware you want to upload to the switch. Options include **Switch** and **Router** images.
 - Apply Firmware:** Set when you want to apply 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 12 Scheduling Firmware Upgrade



The switch upgrade request success message is displayed.

FIGURE 13 Switch Upgrade Request Success



- 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 14 Preparing Phase with Tooltip

The screenshot shows a web interface with a navigation bar containing 'LLDP Neighbors', 'Wired Clients', 'Firmware History' (selected), and 'Troubleshooting'. Below the navigation bar is a search bar labeled 'search table' and a refresh icon. The main content is a table with the following data:

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

A tooltip is displayed over the 'Preparing Phase' status, containing the text: "Switch is providing necessary data to SZ for firmware upgrade". At the bottom right of the table, it indicates "1 records" and a page navigation control.

FIGURE 15 Backup Image Start with Tooltip

The screenshot shows the same web interface as Figure 14. The table now displays the following data:

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

A tooltip is displayed over the 'Backup image start' status, containing the text: "Switch starts to backup bootable image".

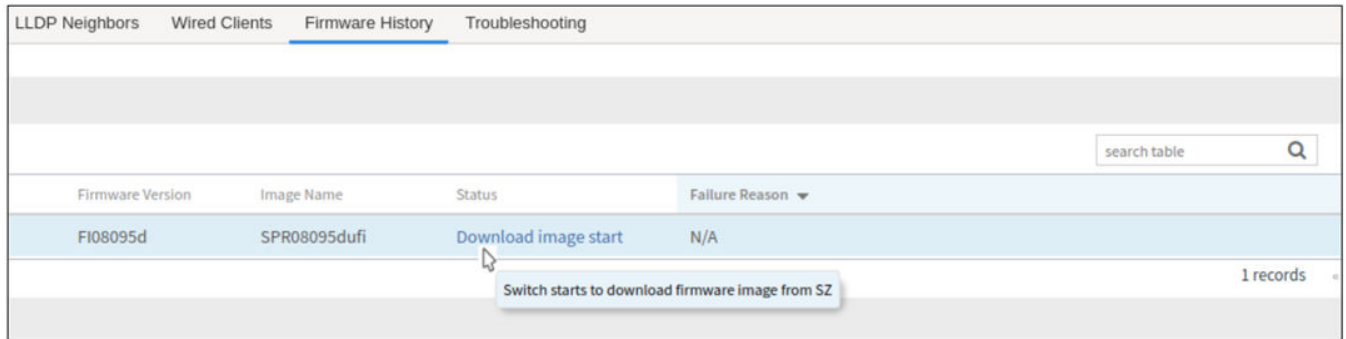
FIGURE 16 Backup Image Complete with Tooltip

The screenshot shows the same web interface as Figure 14. The table now displays the following data:

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

A tooltip is displayed over the 'Backup image complete' status, containing the text: "Switch has finished backup image".

FIGURE 17 Download Image Start with Tooltip

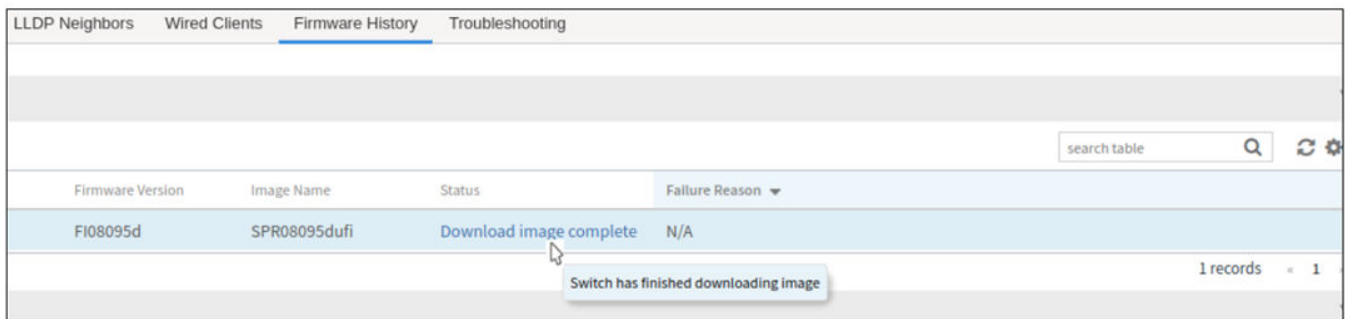


The screenshot shows a web interface with a navigation bar containing 'LLDP Neighbors', 'Wired Clients', 'Firmware History' (selected), and 'Troubleshooting'. Below the navigation bar is a search table input. The main content is a table with the following data:

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

A tooltip is displayed over the 'Download image start' status, containing the text: 'Switch starts to download firmware image from SZ'. The bottom right of the table indicates '1 records'.

FIGURE 18 Download Image Complete with Tooltip

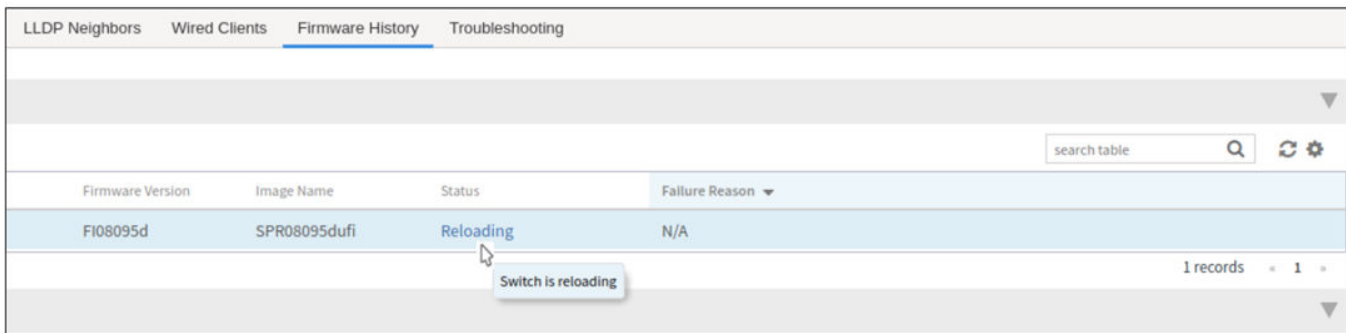


The screenshot shows the same web interface as Figure 18. The table now shows the status 'Download image complete'.

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

A tooltip is displayed over the 'Download image complete' status, containing the text: 'Switch has finished downloading image'. The bottom right of the table indicates '1 records'.

FIGURE 19 Reloading phase with tooltip



The screenshot shows the same web interface as Figure 19. The table now shows the status 'Reloading'.

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

A tooltip is displayed over the 'Reloading' status, containing the text: 'Switch is reloading'. The bottom right of the table indicates '1 records'.

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 38

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**.

- In the **Details** pane, click the **Firmware History** tab.

FIGURE 20 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	FI09010	TNR09010ufl	Completed	N/A
2021/12/02 11:05:04	D4:C1:9E:1A:04:D3	FI09010	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

- 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).
- In the **Firmware Upgrade History** section, you can see the times of previous upgrades and the firmware versions used.

Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

The below table lists ports that must be opened in the network firewall to ensure that the vSZ-D/SZ/vSZ (controller), managed APs, and RADIUS servers can communicate with each other successfully.

TABLE 17 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
AP	Control plane of : SZ-100 SZ-300 vSZ	21	TCP	Control	No	ZD and Solo APs can download SZ AP firmware and convert themselves to SZ APs.
AP	vSZ control plane	22	TCP	Control	No	SSH Tunnel for management
AP ZD	SZ	69	UDP	Control	No	ZD Migration
AP	vSZ control plane	91 (AP firmware version 2.0 to 3.1.x) and 443 (AP firmware version 3.2 and later)	TCP	Control	No	<p>AP firmware upgrade APs need Port 91 to download the Guest Logo and to update the signature package for the ARC.</p> <p>NOTE Starting with SZ 3.2 release, the controller uses an HTTPS connection and an encrypted path for the firmware download. The port used for AP firmware downloads has been changed from port 91 to 443 to distinguish between the two methods. To ensure that all APs can be upgraded successfully to the new firmware, open both ports 91 and 443 in the network firewall.</p>

Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

TABLE 17 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers (continued)

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
AP	RAC (RADIUS Access Controller)	1813	UDP	Management, Cluster, Control NOTE The Management interface is applicable when vSZ-H is in single-interface mode. If in 3-interface mode, Access and Core separation disabled, it depends on the configured Management traffic interface.	No	RADIUS_Auth profile defines both inbound and outbound traffic. Information specified here is for inbound traffic only.
AP	SZ	5353	UDP	Control	No	Resolves hostnames to IP addresses
AP DP	SZ	8200	TCP	Control	No	Captive Portal OAuth service port for HTTP
AP DP	SZ	8222	TCP	Control	No	Captive Portal OAuth service port for HTTPS
AP DP	SZ	8280	TCP	Control	No	Captive Portal Web Proxy service port for HTTPS
AP-MD	SZ-MD	9191	TCP	Cluster	No	Communication between AP-MD and SZ-MD
AP	vSZ control plane	12223	UDP	Control	No	LWAPP discovery sends image upgrade request to ZD-APs via LWAPP (RFC 5412).
AP UE	SZ	18301	UDP	Management, Cluster, Control	No	SpeedFlex tests the network performance between AP, UE, and SZ.
ICX	vSZ control plane	22	TCP	Control	No	SSH Tunnel.
ICX	vSZ control plane	443	TCP	Control	No	Access to the vSZ/SZ control plane over secure HTTPS.
SZ	External FTP server	20-21	TCP	Control, Cluster, Management	No	Transfer data to external FTP servers
Follower SZ nodes	Master SZ node	123	UDP	Cluster	No	Sync system time among SZ nodes
SZ	External Licensing Server	443	TCP	Management	No	Download licensing and support entitlements from the licensing server.
SZ	External Licensing server	443	TCP	Management	No	Download licensing and support entitlements from the licensing server.

TABLE 17 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers (continued)

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
SZ-RAC	External AAA	1812	UDP	Management, Cluster, Control NOTE The Management interface is applicable when vSZ-H is in single-interface mode. If in 3-interface mode, Access and Core separation disabled, it depends on the configured Management traffic interface.	Yes	To Support RADIUS Proxy Authentication
SZ	SZ	5671-5672	TCP	Cluster	No	RabbitMQ inter-node cluster communication
SZ	SZ	6379, 6380	TCP	Cluster	No	Internal communication among SZ nodes
SZ	SZ	7000	TCP/UDP	Cluster	No	Cassandra (database) cluster communication and data replication
SZ	SZ	7500	UDP	Cluster	No	SZ Clustering Operation
SZ	SZ	7800	TCP/UDP	Cluster	No	Cluster node communication for cluster's operations
SZ	SZ	7800-7805	TCP	Cluster	No	A protocol stack using TCP on JGroups library for node to node communication
SZ	SZ	7810	TCP	Cluster	No	A protocol stack using FD_SOCKET on JGroups library for node-to-node communication
SZ	SZ	7811	TCP	Cluster	No	A protocol stack using FD_SOCKET on JGroups library for node-to-node communication
SZ	SZ	7812	TCP	Cluster	No	A protocol stack using FD_SOCKET on JGroups library for node-to-node communication

Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

TABLE 17 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers (continued)

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
SZ	SPoT	8883 NOTE The connection between the controller and vSPoT is an outbound connection, so it depends on the destination IP address. If the destination IP address falls in the subnet of one interface, it is routed to that interface. Otherwise, it is routed via the default route.	TCP	Management, Cluster, Control	No	Communication between SZ and SPoT
SZ	SZ	9300-9400	TCP	Cluster	No	Internal communication between nodes within the cluster (ElasticSearch database)
SZ local modules	SZ memproxy	11211	TCP	Cluster	No	Internal proxy for saving in-memory data to memcached
SZ	SZ	11311	TCP	Cluster	No	Memory cache server
SZ	SZ	33434-33534	UDP	Management, Cluster, Control	No	ICX Troubleshooting (traceroute).
SZ CS	DP	65534, 65535	TCP	Management	No	DP Debug
TACACS+ Server	TACACS+ Server	49	TCP	Management, Cluster, Control	No	TACACS+
DNS Server	DNS	53	TCP/UDP	Management, Cluster, Control	No	DNS
DHCP Server	SZ	67,68	UDP	Management, Cluster, Control	No	DHCP
Walled-Garden Web Server	Captive Portal with HTTP Proxy	80	TCP	Management, Cluster, Control	No	WISPr_WalledGarden
SNMP Client	SZ	161	UDP	Management	No	Simple Network Management Protocol (SNMP)
LDAP Server	RAC	389	TCP/UDP	Management, Cluster, Control	Yes	SZ to LDAP
SZ	rsyslog	514	TCP/UDP	Management, Cluster, Control	No	Remote Syslog
DHCP v6 Server	SZ	546, 547	UDP	Management, Cluster, Control	No	DHCPv6 Protocol
LDAPS Server	RAC	636	TCP	Management, Cluster, Control	Yes	SZ to LDAPS Server
AAA server	SZ	2083 (RadSec)	TCP	Management, Cluster, Control	No	The default destination port number for RADIUS over TLS is TCP/2083 (As per RFC-6614)

TABLE 17 Ports to Open Between Various RUCKUS Devices, Servers, and Controllers (continued)

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
AAA server	SZ	2084 (CoA/DM Over RadSec)	TCP	Management, Cluster, Control	No	SZ as RadSec server listens on port 2084 for incoming TLS connection from client (AAA Client) to process CoA/DM messages over RadSec.
AD Server (MSTF-GC)	RAC	3268	TCP	Management, Cluster, Control	Yes	SZ to AD (MSTF-GC)
External AAA Server (free RADIUS)	SZ-RAC (vSZ control plane)	3799	UDP	Management, Cluster, Control	No	Supports Disconnect Message and CoA (Change of Authorization) which allows dynamic changes to a user session such as disconnecting users and changing authorizations applicable to a user session.
JITC CAC	SZ	4443	TCP	Control	No	Since SZ 5.1.2 release, mainly for JITC CAC login support. This port is opened for NGINX to configure for client certificate authentication.
Legacy Public API Client	SZ	7443	TCP	Management	No	Deprecated Public API
Any	Management interface	8022	No (SSH)	Management	Yes	When the management ACL is enabled, you must use port 8022 (instead of the default port 22) to log on to the CLI or to use SSH.
Any	vSZ control plane	8090	TCP	Control	No	Allows unauthorized UEs to browse to an HTTP website
Any	vSZ control plane	8099	TCP	Control	No	Allows unauthorized UEs to browse to an HTTPS website
Any	vSZ control plane	8100	TCP	Control	No	Allows unauthorized UEs to browse using a proxy UE
Any	vSZ management plane	8443 NOTE The Public API port has changed from 7443 to 8443.	TCP	Management	No	Access to the controller web interface via HTTPS
Any	vSZ control plane	9080	HTTP	Management, Control	No	Northbound Portal Interface for hotspots
Any	vSZ control plane	9443	HTTPS	Management, Control	No	Northbound Portal Interface for hotspots
Client device	SZ control Plane	9997	TCP	Control	No	Internal Subscriber Portal in HTTP
Any	vSZ control plane	9998	TCP	Control	No	Hotspot WISPr subscriber portal login/logout over HTTPS

Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

TABLE 18 vDP/ SZ300 DP/ SZ100 Data Group(PG-2):

From (Sender)	To (Listener)	Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
AP vSZ_D	vSZ control plane	22	TCP	Control, Cluster, Management	No	SSH Tunnel
External DP	Internal DP	23232	TCP	Cluster (SZ100)	No	Create DP-DP Tunnel; Only happen in Port One Group
AP	AP-DP Tunnel	23233	TCP	Cluster (SZ100)	No	Create DP-DP Tunnel; Only happen in Port One Group

NOTE

The destination interfaces are meant for three-interface deployments. In a single-interface deployment, all the destination ports must be forwarded to the combined management and control interface IP address.

NOTE

Communication between APs is not possible across NAT servers.

Geo Redundancy Upgrade Operation Flow

- [Upgrade Path and Cluster Redundancy Deployment.....](#) 51
- [SOP A.....](#) 52
- [SOP B.....](#) 54
- [SOP C.....](#) 55
- [SOP Z.....](#) 56

When there are multiple clusters on the network, you can configure cluster redundancy to enable APs managed by a particular cluster to fail over automatically to another cluster if the parent cluster goes out of service or becomes unavailable.

Upgrade Path and Cluster Redundancy Deployment

There are two cluster redundancy deployment modes:

- Active-Standby mode
- Active-Active mode

Active-Standby Mode

When an active cluster becomes inaccessible for APs, external DPs (vSZ-D and SZ100-D), and ICX switches, a standby cluster restores the latest configuration of the out-of-service (OOS) active cluster, then takes over all external devices (including APs, external DPs, and ICX switches). The AP or ICX switch capacity is limited by the AP or ICX switch High Availability (HA) licenses on the standby cluster and the services license limits from the failed active cluster. When the active cluster returns to the in-service state, the end user can "rehome" all APs, external DPs, and ICX switches back to the active cluster.

The behavior of the standby cluster changes automatically when there is a configuration change in the following deployment types:

- One-to-one (one active cluster to one standby cluster) deployment

The standby cluster restores the configuration from the active cluster after the configuration synchronization is completed. The standby cluster is always in backup mode and ready to receive the APs, external DPs, and ICX switches from the out-of-service active cluster.

- Many-to-one (two or three active clusters to one standby cluster) deployment

The time taken by the standby cluster between detecting the active cluster is out-of-service and being ready to serve APs and external DPs has been enhanced.

TABLE 19 Upgrade Path

Base Version	Upgrade Version	Topology ("Active Cluster #"-"Standby Cluster #")	Upgrade Flow
3.6.x	5.x	1-to-1	SOP C on page 55 Only 1-to-1 deployment in R3.6
5.0.x	5.1.x	1-to-1	SOP B on page 54
		N-to-1 (N ≥ 2)	SOP A on page 52
5.1.x	5.2.x	1-to-1	SOP B on page 54
		N-to-1 (N ≥ 2)	SOP A on page 52
5.2.x	6.0.x	1-to-1	SOP B on page 54
		N-to-1 (N ≥ 2)	SOP A on page 52

TABLE 19 Upgrade Path (continued)

Base Version	Upgrade Version	Topology ("Active Cluster #"-to-"Standby Cluster #")	Upgrade Flow
6.0.x	6.1.x	1-to-1	SOP B on page 54
		N-to-1 ($N \geq 2$)	SOP A on page 52

Active-Active Mode

When there are multiple clusters, one cluster can be the configuration source cluster, and all other active cluster restores its configuration periodically to make sure the configuration between the clusters are synchronized constantly. When the active cluster becomes inaccessible for APs and external DPs (vSZ-D and SZ100-D), they fail over to the target active cluster with priority. Refer to [SOP Z](#) on page 56 for more information.

SOP A

This section provides information on upgrade paths, preconditions, the applicable topology, and the upgrade flow for SOP A.

SZ Upgrade Path

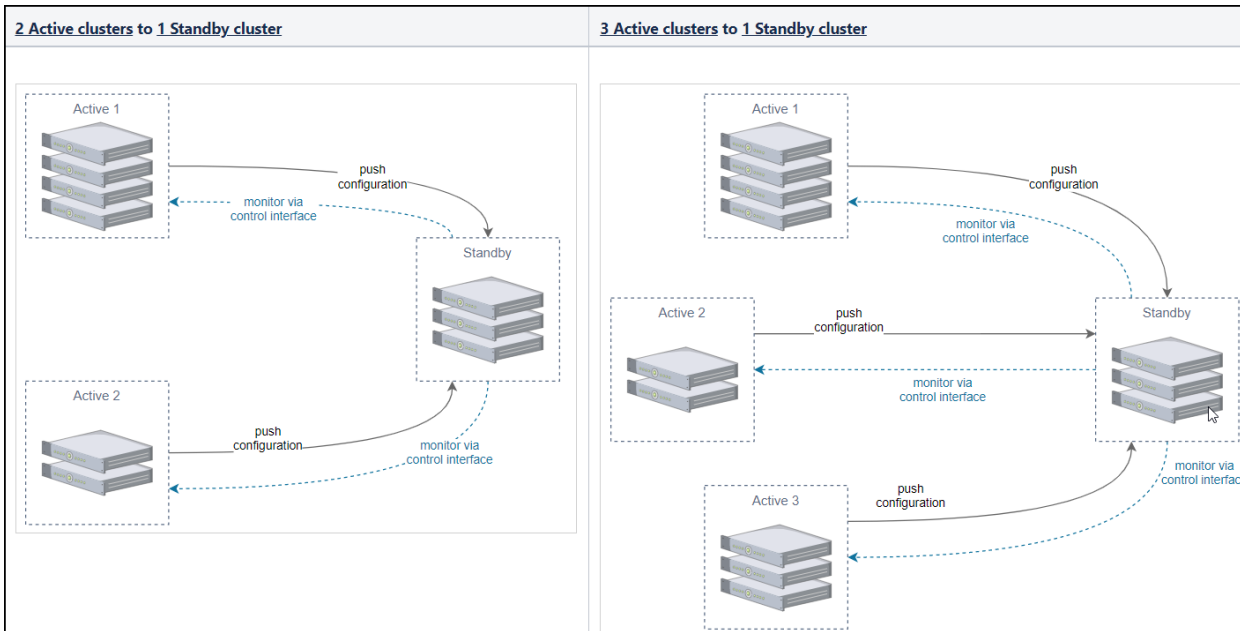
- 5.0.x to 5.1.x
- 5.1.x to 5.2.x
- 5.2.x to 6.0.x

Precondition

The standby cluster must have the following license in order to be upgraded:

- SZ300: **SUP_SZ300_HA_EU** or **SUP_SZ300_HA_PTNR**
- vSZ-H: **SUPPORT_HA_EU** or **SUPPORT_HA_PTNR**

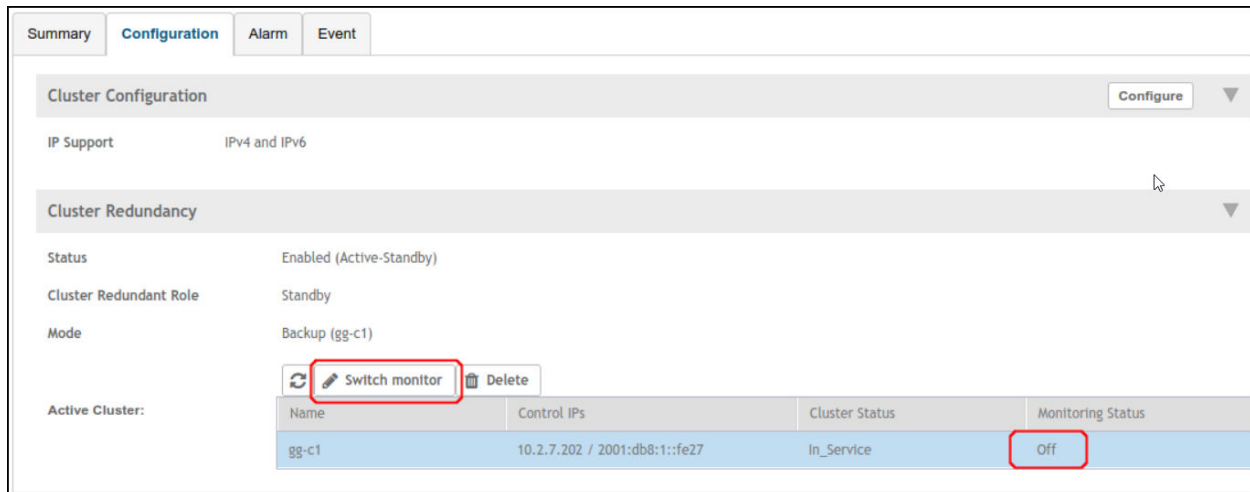
FIGURE 21 SOP A Applicable Topology



Cluster Upgrade Flow

1. Turn off the monitoring status of each active cluster from the standby cluster. In the standby cluster interface, go to **Network > Data and Control Plane > Cluster**.
2. Select the cluster root, and click the **Configuration** tab.
For example, select the active cluster in the table and click **Switch monitor**. Ensure the **Monitoring Status** is set to **Off**.

FIGURE 22 Turning Off Monitoring Status



3. Upgrade the Active 1 cluster and make sure it is successfully upgraded.
4. From the active cluster, go to **Monitor > Events and Alarms > Eventss** and check the details of event code 814. Refer [Performing the Upgrade](#) on page 25.

Geo Redundancy Upgrade Operation Flow

SOP B

5. Repeat [Step 2](#) and [Step 3](#) to upgrade the Active 2 cluster and the Active 3 cluster.
6. Upgrade the standby cluster after all the active clusters are successfully upgraded.
7. Click **Sync Now** in each active cluster after all the active and standby clusters are successfully upgraded.
8. From the active cluster, go to **Monitor > Events and Alarms > Eventss** and check the details of event code 814. Refer [Performing the Upgrade](#) on page 25.
9. Turn on the monitoring status of each active cluster from the standby cluster after the standby cluster is successfully upgraded.
10. If the new SZ version is 5.2.x (including 5.2), and the standby cluster monitors only one active cluster, the standby cluster will automatically switch to Backup mode regardless of the number of nodes of the Active cluster. After cluster redundancy is enabled, the standby cluster will take some time to restore the configuration of the latest active cluster.

SOP B

This section provides information on upgrade paths, preconditions, the applicable topology, and the upgrade for SOP B.

SZ Upgrade Path

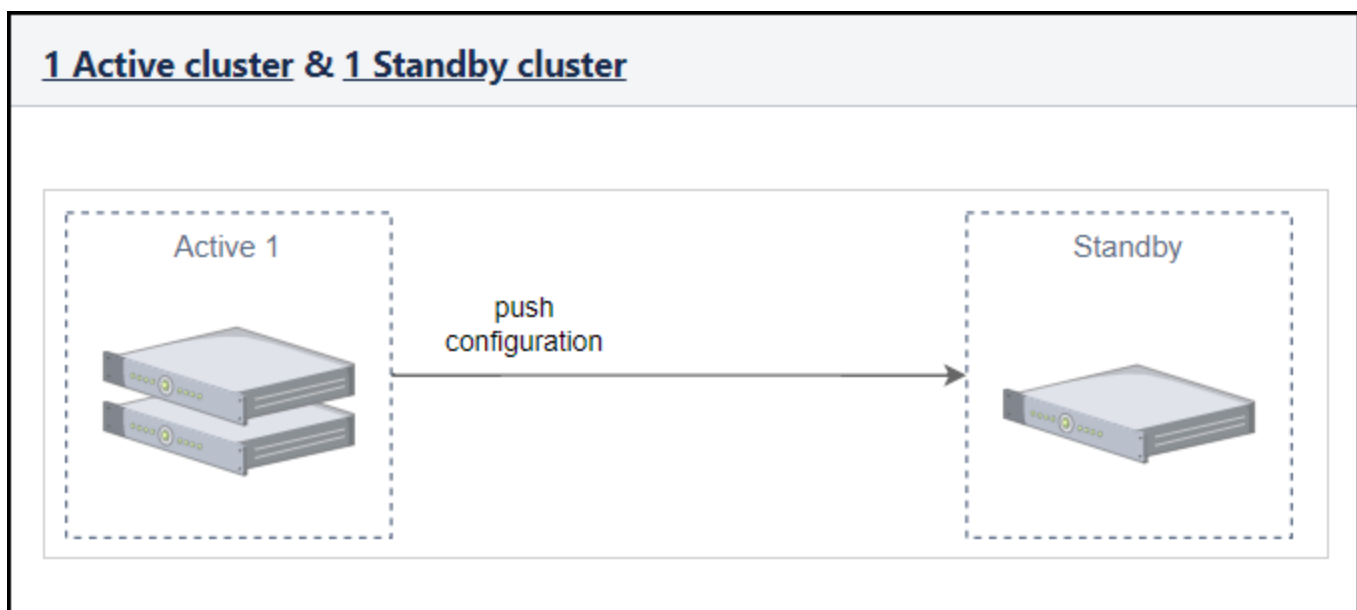
- 5.0.x to 5.1.x
- 5.1.x to 5.2.x
- 5.2.x to 6.0.x

Preconditions

The standby cluster must have the following license in order to be upgraded:

- SZ300: **SUP_SZ300_HA_EU** or **SUP_SZ300_HA_PTNR**
- vSZ-H: **SUPPORT_HA_EU** or **SUPPORT_HA_PTNR**

FIGURE 23 SOP B Applicable Topology



Cluster Upgrade Flow

1. Rehome any AP from the standby cluster and ensure all the APs are on the active cluster.
2. Disable cluster redundancy from the active cluster and check if all APs are online and up-to-date.
3. Upgrade the active cluster and ensure the active SZ is successfully upgraded.
4. From the Active cluster, go to **Events and Alarms > Events** and check the details of event code 814
5. From the active cluster, go to **Administration > Upgrade > Upgrade History** to verify previous cluster upgrades.
6. Ensure all APs are online and up-to-date after the upgrade.
7. Upgrade the standby cluster, and ensure it is successfully upgraded.
8. Repeat [Step 4](#) and [Step 5](#).
9. Enable cluster redundancy on the active cluster.
10. Verify if the active SZ engages the latest cluster redundancy resource-type admin activities.
If the new SZ version is 5.2.x (including 5.2), the standby cluster will automatically switch to Backup mode after cluster redundancy is enabled. The standby cluster will take some time to restore the configuration of the latest active cluster.
11. In the standby cluster interface, go to **Network > Data and Control Plane > Cluster**.
12. Repeat [Step 4](#).
13. Select the cluster root, and click the **Configuration** tab.

SOP C

This section provides information on upgrade paths, preconditions, the applicable topology, and the upgrade flow for SOP C.

SZ Upgrade Path

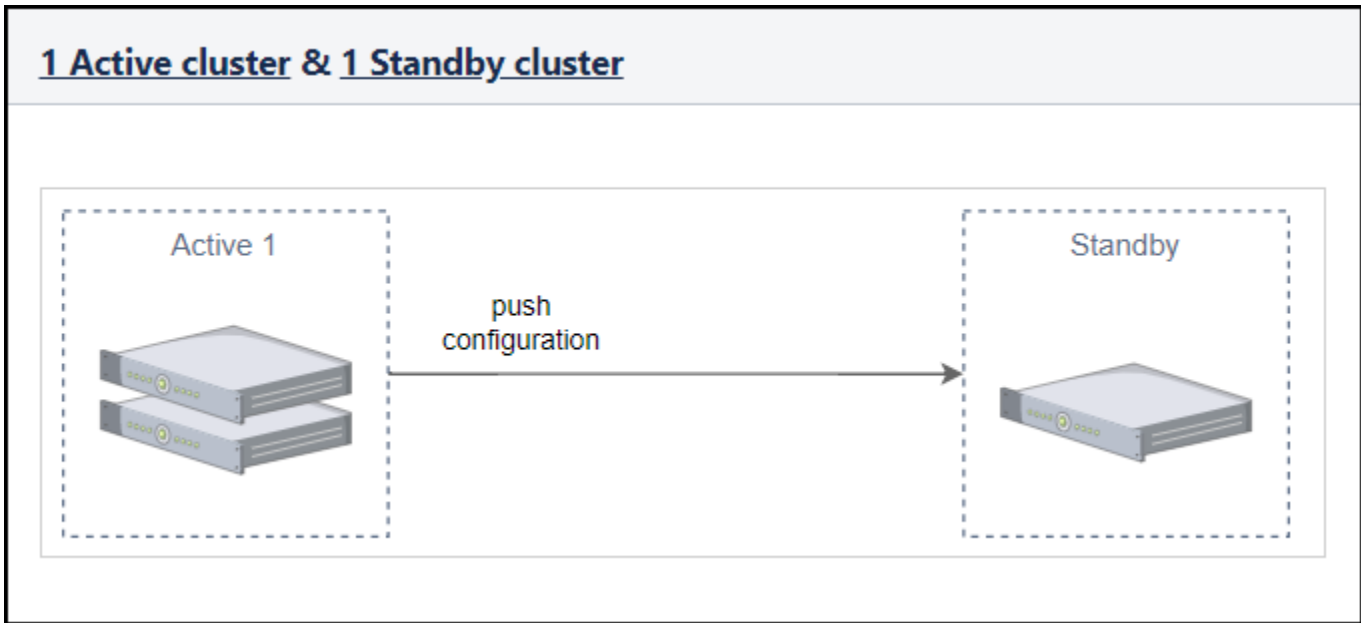
- 3.6.x to 5.x

Preconditions

The standby cluster must have the following license in order to be upgraded:

- SZ300: **SUP_SZ300_HA_EU** or **SUP_SZ300_HA_PTNR**
- vSZ-H: **SUPPORT_HA_EU** or **SUPPORT_HA_PTNR**

FIGURE 24 SOP C Applicable Topology



Cluster Upgrade Flow

1. From the active cluster, go to **Network > Data and Control Plane > Cluster > Configuration** and disable schedule configuration sync. Do not change the cluster redundancy-enabled settings.
2. Upgrade the active cluster and ensure that the active SZ is successfully upgraded.
3. From the active cluster, go to **Monitor > Events and Alarms > Events** and check the details of event code 814.
4. From the active cluster, go to **Administration > Administration > Upgrade > Upgrade History** to verify previous cluster upgrades.
5. Rehome all APs in the standby cluster to the active cluster and ensure there is no AP on the standby cluster.
6. Ensure all APs are on the Active cluster with **Status** online and **Configuration Status** up-to-date after the upgrade.
7. Upgrade the standby cluster, and ensure it is successfully upgraded.
8. Repeat [Step 3](#) and [Step 4](#).
9. In the active cluster interface, go to **Network > Data and Control Plane > Cluster > Configuration** and disable cluster redundancy.
10. In the standby cluster interface, go to **Network > Data and Control Plane > Cluster > Configuration** and ensure that all active data is deleted.
11. Enable cluster redundancy again from the active cluster.
12. From the active cluster, go to **Administration > Administration > Admin Activities** and check if cluster redundancy is set successfully by investigating admin activities.

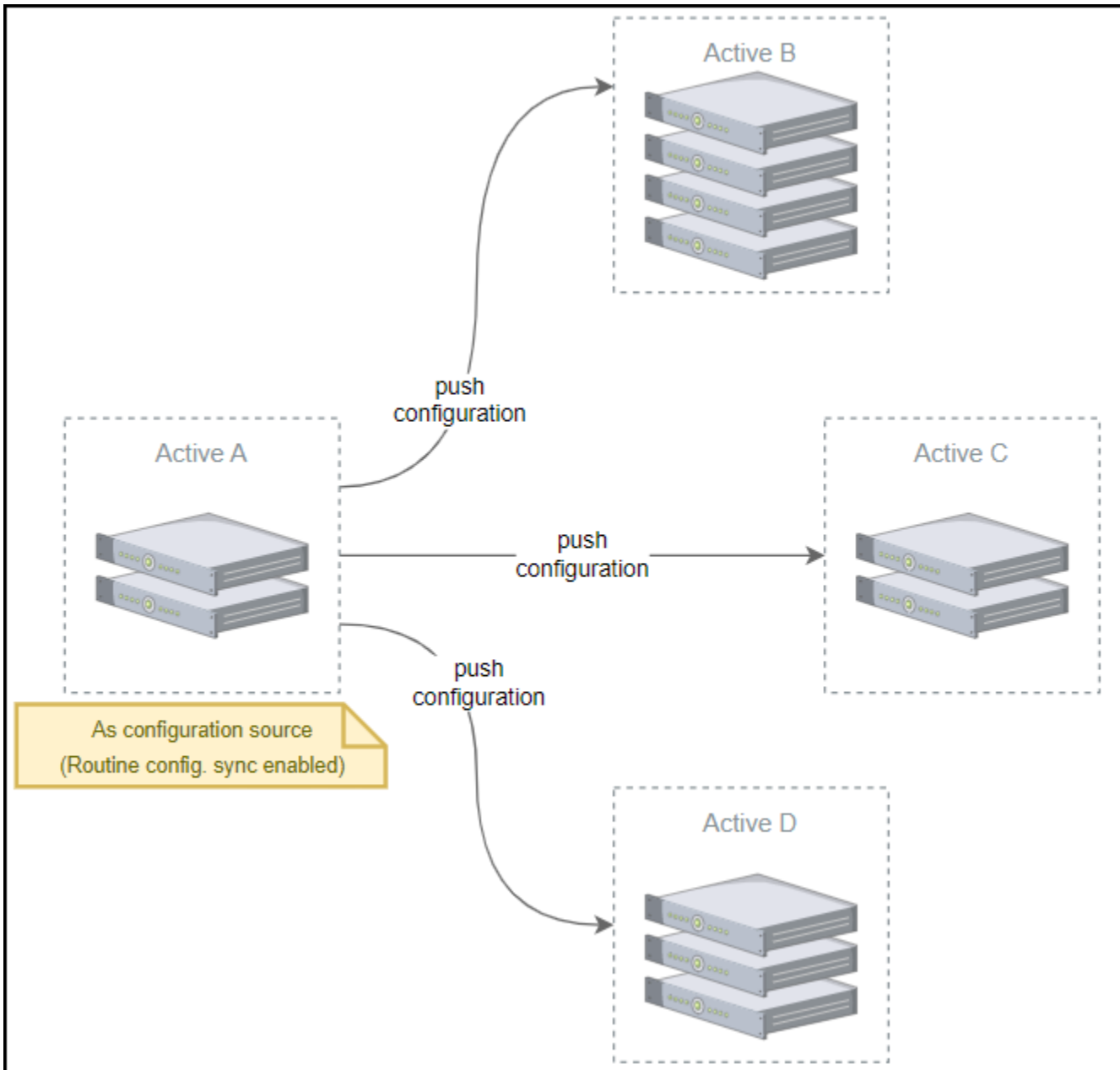
SOP Z

This section provides information on preconditions, the applicable topology, and the upgrade flow for SOP Z.

Preconditions

All active cluster should have valid upgrade license.

FIGURE 25 SOP Z Applicable Topology



Cluster Upgrade Flow

1. Ensure that all the APs, DPs, and switches are at their home clusters before upgrading the active cluster that is selected as the master configuration. The switchover operation can be used to let the APs, DPs, and switches connect to another cluster.
2. From the active cluster, go to **Network > Data and Control Plane > Cluster > Configuration** and disable schedule configuration sync.
3. Upgrade the active cluster A.
4. When the Active A cluster is upgraded, begin to upgrade clusters Active B, Active C, and Active D sequentially.
5. After all the active clusters are upgraded successfully, click **Sync Now** to sync the configuration from the Active A cluster.

6. Select **Configuration Sync** from the scheduler task in the Active A cluster.

Is My Access Point Supported by the Firmware Upgrade?

- Supported Matrix and Unsupported Models..... 59

Supported Matrix and Unsupported Models

Before upgrading to this release, check if the controller is currently managing APs, Switches or IoT devices.

APs preconfigured with the SmartZone AP firmware may be used with SZ300, SZ100, or vSZ in their native default configuration. APs factory-configured with the ZoneFlex-AP firmware may be used with the controller when LWAPP discovery services are enabled.

LWAPP2SCG must be disabled on the controller if Solo APs running 104.x are being moved under controller management. To disable the LWAPP2SCG service on the controller, log on to the CLI, and then go to **enable > mode > config > lwapp2scg > policy deny-all**. Enter **Yes** to save your changes.

NOTE

Solo APs running releases 104.x or higher are capable of connecting to both Zone Director and SmartZone platforms. If an AP is running release 104.x or later and the LWAPP2SCG service is enabled on the controller, a race condition will occur.

IMPORTANT

AP PoE power modes: AP features may be limited depending on power provided via PoE. Refer to AP datasheets for more information.

Supported AP Models

This release supports the following RUCKUS AP models.

TABLE 20 Supported AP Models

11ax	
Indoor	Outdoor
R850	T750SE
R770	T750
R760	T350SE
R750	T350D
R650	T350C
R560	
R550	
R350	
H550	
H350	

The following lists the supported AP models in this SmartZone release when placed in an AP Zone that uses an older AP version.

ATTENTION

The R730 AP must be removed from the AP Zone before upgrading the AP Zone to the AP firmware version 6.1.1 or later.

Is My Access Point Supported by the Firmware Upgrade?

Supported Matrix and Unsupported Models

ATTENTION

For APs that are not compatible with R7.0.0, it is essential to maintain them with AP firmware versions of R6.1, 6.1.1, and 6.1.2. The upgrade of the Zone for APs that are not supported in R6.1, 6.1.1, and 6.1.2 is not feasible.

TABLE 21 Supported AP Models for AP Zones using older AP versions

11ax	11ac-Wave2	
NOTE Supported on R6.1.0, 6.1.1, and 6.1.2.	Indoor	Outdoor
T750SE	R720	T811CM
T750	R710	T710S
T350SE	R610	T710
T350D	R510	T610S
T350C	R320	T610
R850	M510	T310S
R760 (not supported on R6.1.0)	H510	T310N
R750	H320	T310D
R730	C110	T310C
R650		T305I
R560 (not supported on R6.1.0)		T305E
R550		E510
R350		
H550		
H350		

ATTENTION

AP R310 is Wave 1 and supports WPA3 - this is the one exception, the rest of the APs that support WPA3 are 802.11ac Wave2 or 802.11ax.

Unsupported AP Models

The following lists the AP models have reached end-of-life (EoL) status and, therefore, are no longer supported in this release.

TABLE 22 Unsupported AP Models

Unsupported AP Models				
SC8800-S	SC8800-S-AC	ZF2741	ZF2741-EXT	ZF2942
ZF7025	ZF7321	ZF7321-U	ZF7341	ZF7343
ZF7343-U	ZF7351	ZF7351-U	ZF7363	ZF7363-U
ZF7441	ZF7761-CM	ZF7762	ZF7762-AC	ZF7762-S
ZF7762-S-AC	ZF7762-T	ZF7962	ZF7781CM	ZF7982
ZF7782-S	ZF7782-E	ZF7782	ZF7372-E	ZF7372
ZF7352	ZF7055	R300	R310	R700
C500	H500	R600	R500	R310
R500E	T504	T300	T300E	T301N
T301S	FZM300	FZP300		

Upgrade FAQs

- [Do I Need a Valid Support Contract to Upgrade Firmware?](#)
- [Is My Controller Supported by the Firmware Upgrade?](#)
- [How Do I Get Support?](#)

Do I Need a Valid Support Contract to Upgrade Firmware?

You must have a valid support contract to upgrade the SmartZone software. If you do not have a valid support contract, contact your reseller to purchase an appropriate support contract. After downloading and installing the software, select **Administer** > **Support** from the WebUI for information on activating your support contract.

NOTE

By downloading the SmartZone software and subsequently upgrading SmartZone to version 6.1.0, be advised that the software will periodically connect to RUCKUS and RUCKUS will collect the hardware serial number, software version and build number. RUCKUS will transmit a file back to the SmartZone device that will be used to display the current status of your SmartZone support contract. Any information collected from the SmartZone device may be transferred and stored outside of your country of residence where data protection standards may be different.

Is My Controller Supported by the Firmware Upgrade?

This guide supports the following SmartZone models:

- SmartZone 100 (SZ100)
- SmartZone 144 (SZ144)
- SmartZone 300 (SZ300)
- Virtual SmartZone (vSZ)
- Virtual SmartZone Data Plane (vSZ-D)
- SmartZone 100 Data Plane (SZ100-D)
- SmartZone 144 Data Plane (SZ144-D)

For information about the specific models and modules supported in a SmartZone model, refer to the appropriate hardware installation guide.

How Do I Get Support?

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



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