



RUCKUS SmartZone (LT-GD) Basic Controller Settings, 6.1.2

Published from

CommScope Technical Content Portal by

29 January 2025

CommScope Legal Statements

© 2025 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, SUPPLIES, 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

All trademarks identified by ™ or ® are trademarks or registered trademarks in the US and may be registered in other countries. All product names, trademarks, and registered trademarks are property of their respective owners.

Patent marking notice

For applicable patents, see www.cs-pat.com. That website is intended to give notice under 35 U.S.C. § 287(a) of articles that are patented or for use under the identified patents. That website identifies the patents associated with each of the patented articles.

Table of Contents

Contact Information, Resources, and Conventions

Document Conventions.	6
Command Syntax Conventions.	7
Document Feedback.	8
RUCKUS Product Documentation Resources.	8
Online Training Resources.	9
Contacting RUCKUS Customer Services and Support.	9

About This Guide

New in This Document.	11
-------------------------------	----

Controller Setup

Setting Up the Controller for the First Time.	12
---	----

Firewall Ports

Introduction to Firewall Ports.	13
Ports to Open Between Various RUCKUS Devices, Servers, and Controllers.	13

SmartZone Web Interface

Introduction to SmartZone Web Interface.	26
Logging in to the Web Interface.	26
Logging Off the Controller.	27

Changing the Administrator Password.	28
---	----

Controller User Interface (UI)

System Settings

Viewing System Settings.	32
Configuring the System Time.	33
Creating a DNS Server Profile.	35
Creating a DNS Spoofing Profile.	36
Setting User Preferences.	37

Warnings and Notifications

Warnings.	40
Setting Global Notifications.	41

Working with Maps

Importing a Floorplan Map.	42
Viewing RF Signal Strength.	45
Monitoring APs Using the Map View.	46

Health and Maps

Understanding Cluster and AP Health Icons.	49
Customizing Health Status Thresholds.	49
Customizing AP Flagged Status Thresholds.	50

Using the Health Dashboard Map.	52
Configuring the Google Map API Key Behavior.	54

Contact Information, Resources, and Conventions

[Document Conventions](#)

[Command Syntax Conventions](#)

[Document Feedback](#)

[RUCKUS Product Documentation Resources](#)

[Online Training Resources](#)

[Contacting RUCKUS Customer Services and Support](#)

Document Conventions


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


Table 1. Text Conventions


Convention	Description	Example
monospace	Identifies command syntax examples	device(config)# interface ethernet 1/1/6
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the Start menu, click All Programs .
<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.

Parent topic: [Contact Information, Resources, and Conventions](#)

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, member[member...].

Convention	Description
\	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.

Parent topic: [Contact Information, Resources, and Conventions](#)

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

Parent topic: [Contact Information, Resources, and Conventions](#)

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>.

Parent topic: [Contact Information, Resources, and Conventions](#)

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.

Parent topic: [Contact Information, Resources, and Conventions](#)

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.

Parent topic: [Contact Information, Resources, and Conventions](#)

About This Guide

New in This Document

New in This Document

Table 1. Key Features and Enhancements in SmartZone 6.1.2 Rev B (April 2024)

Feature	Description	Reference
Doc-defect SCG - 152431	Updated: Added missing port for AP to AP communications in the firewall port list.	Ports to Open Between Various RUCKUS Devices, Servers, and Controllers

Parent topic: [About This Guide](#)

Controller Setup

Setting Up the Controller for the First Time

Setting Up the Controller for the First Time

RUCKUS SmartZone controllers are next-generation high-performance wireless LAN controllers that run the RUCKUS SmartZone operating system. To deploy the controller, it must first be set up on the network. For information on how to set up the controller for the first time, including instructions for preparing your chosen hypervisor, installing the vSZ image on to hypervisor, and completing the vSZ Setup Wizard, refer to the Getting Started Guide or Quick Setup Guide for your controller platform.

- 🔗 **Note:** While deploying vSZ, block level storage must be used and the hosts must see this as direct-attached storage. For real time database access and synchronization, vSZ requires lower latency and higher numbers of read/write transactions than file level storage solutions such as NAS or network file shares allow.

You can deploy vSZ and vSZ-D via vCenter 6.7 on ESXi. Some of the features (for example, location based services, rogue AP detection, force DHCP, and others) may not be visible on the controller web interface if the AP firmware deployed to the zone you are configuring is earlier than this release.

- 🔗 **Note:** To ensure that you can view and configure all new features that are available in this release, RUCKUS recommends upgrading the AP firmware to the latest version.

Parent topic: [Controller Setup](#)

Firewall Ports

Introduction to Firewall Ports

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

Introduction to Firewall Ports

An important part of a stateful firewall is the ability to track the state of traffic connections.

This is a security measure intended to help prevent intrusions and spoofs. The firewall attempts to make sure any incoming connection is matched with a known active connection that was initiated from inside the firewall. Any packets that do not comply with these rules or are specifically allowed (well-known protocols such as FTP servers and others) are typically dropped. Different ports are necessary to allow various communications for control, data, and management traffic.


Parent topic: [Firewall Ports](#)



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 1. 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	AP	1883	TCP	Control	No	AP-AP communication for neighbor AP information

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
						exchange in FT, Client Load Balance, etc.
AP	Control plane of : SZ-100 SZ-300 vSZ	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</p>


From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
						 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.
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,	No	RADIUS_Auth profile defines both inbound and outbound traffic. Information specified here is for inbound traffic only.

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
				 Access and Core separation disabled, it depends on the configured Management traffic interface.		
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).

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
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.
SZ-RAC	External AAA	1812	UDP	Management, Cluster, Control  Note: The Managem	Yes	To Support RADIUS Proxy Authentication

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
				 ent 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.		
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

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
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
SZ	SPoT	8883	TCP	Management, Cluster, Control	No	Communication between SZ and SPoT

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
		 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.				
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

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
						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_Walled Garden
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

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
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)
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

From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
						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


From (Sender)	To (Listener)	Communication Port Number	Layer 4 Protocol	Interface	Configurable from Web Interface?	Purpose
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

Table 2. vDP/ SZ300 DP 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

- ⓘ **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.

Parent topic: [Firewall Ports](#)

SmartZone Web Interface

[Introduction to SmartZone Web Interface](#)

[Logging in to the Web Interface](#)

[Logging Off the Controller](#)

[Changing the Administrator Password](#)

Introduction to SmartZone Web Interface

RUCKUS SmartZone network controllers simplify the complexity of scaling and managing wired switches and wireless access points (APs) through a common interface to support private cloud Network as a Service (NaaS) offerings in addition to general enterprise networks.

All physical and virtual SmartZone appliances support network configuration, monitoring, provisioning, discovery, planning, troubleshooting, performance management, security, and reporting. The user-friendly SmartZone Web Interface handles network visibility from the wireless edge to the network core and enables IT administrators to perform day-to-day management tasks, troubleshoot user-connectivity problems, and define and monitor user and application policies without requiring advanced network skills and command line interface (CLI) expertise.

Parent topic: [SmartZone Web Interface](#)

Logging in to the Web Interface

Before you can log in to the controller web interface, you must have the IP address that you assigned to the Management (Web) interface when you set up the controller on the network using the Setup Wizard.

Once you have this IP address, you can access the controller web interface on any computer that can reach the Management (Web) interface on the IP network.

Complete the following steps to log in to the controller web interface.

1. Start a web browser on a computer that is on the same subnet as the Management (Web) interface. The following web browsers are supported:
 - Google Chrome
 - Safari
 - Mozilla Firefox
 - Internet Explorer

- Microsoft Edge
2. In the address bar, enter the IP address that you assigned to the Management (Web) interface, and append a colon (:) and 8443 (the management port number of the controller) to the end of the address.

For example, if the IP address that you assigned to the Management (Web) interface is 10.10.101.1, you should enter: <https://10.10.101.1:8443>.

- **Note:** The controller web interface requires an HTTPS connection. You must append "https" (not "http") to the Management (Web) interface IP address to connect to the controller web interface. Because the default SSL certificate (or security certificate) that the controller is using for HTTPS communication is signed by RUCKUS and is not recognized by most web browsers, a browser security warning may be displayed.

The controller web interface logon page is displayed.

3. Log in to the controller web interface using the following credentials:

- **User Name:** admin
- **Password:** Password you set in the Setup Wizard

4. Click **Log On**.

The controller web interface displays the **Dashboard**, which indicates that you have logged on successfully.

Parent topic: [SmartZone Web Interface](#)

Logging Off the Controller

You can log off the controller by using either the web interface or the Command Line Interface (CLI).

Logging off Using the Web Interface

1. On the controller web interface, select **Log off** from the **default** list.

The following message is displayed: Are you sure you want to log off?

2. Click **Yes**.

You have completed logging off the web interface

Logging off Using CLI

1. To schedule a shutdown at the CLI prompt, enter the command **shutdown** and specify the delay in seconds before controller shuts down.
2. To shutdown the controller immediately, enter the command **shutdown now**.

Parent topic: [SmartZone Web Interface](#)


Changing the Administrator Password

Follow these steps to change the administrator password.

1. On the controller web interface, select **Change Password** from the **default** list.

The following window is displayed.

Figure 1. Change Password Form

A screenshot of a web-based 'Change Password' form. The form has a title bar with the text 'Change Password' and a close button (X). Inside the form, there are three input fields, each preceded by an asterisk: 'Old Password:', 'New Password:', and 'Confirm Password:'. Below the input fields are two buttons: 'Change' and 'Cancel'.

2. Enter:
 - **Old Password**—Your current password.
 - **New Password**—Your new password.
 - **Confirm Password**—Your new password.
3. Click **Change**, your new password is updated.

Parent topic: [SmartZone Web Interface](#)

Controller User Interface (UI)

Prior to release 6.0.0, the controller menu had vertical layout that resulted in some menu items not being visible on the screen. So, to make navigation easier, a new menu was introduced in release 6.0.0 release. The new menu has features such as **Category**, **Favorite**, **Search** and **Breadcrumbs**.

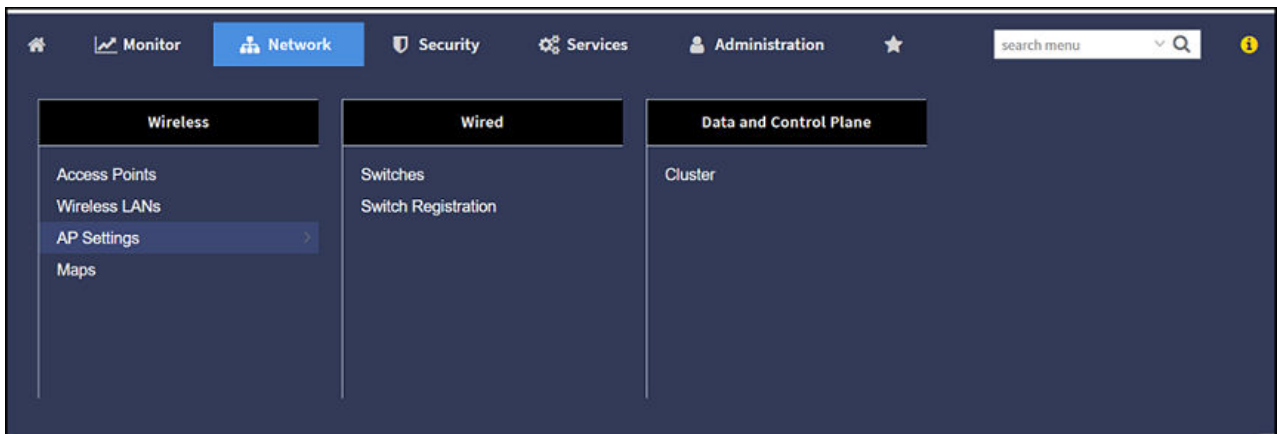
- **Category** - The menu items are organized into distinct categories or groups making it easier to find and access specific functionalities. The various categories are **Monitor**, **Network**, **Security**, **Services** and **Administration**.

Figure 1. Displaying Categories on the Menu Bar



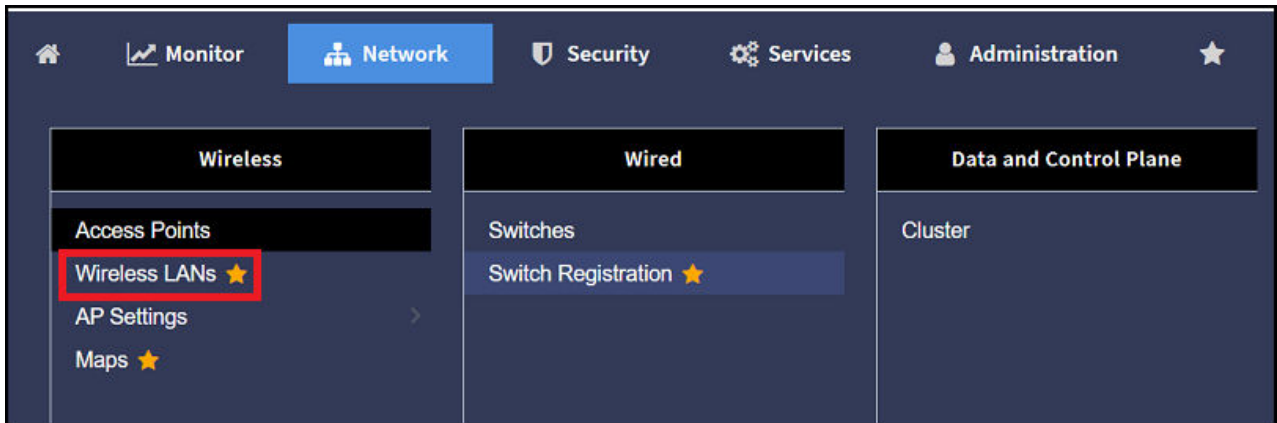
For example, the menu items under the category **Network** are displayed as per the screenshot below.

Figure 2. Displaying Menu Items in the Network Category



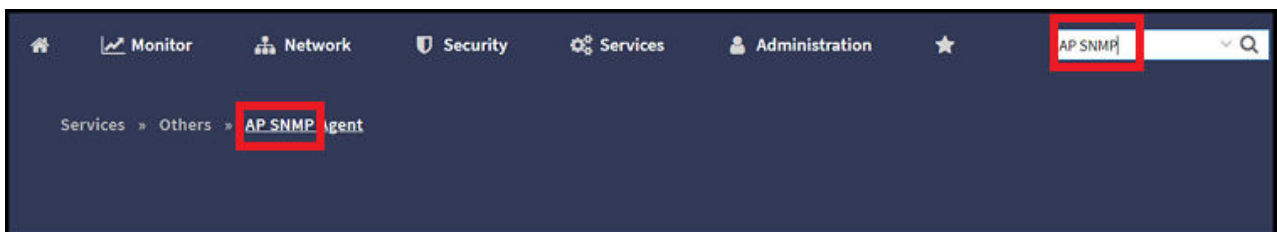
- **Favorite** - The **Star** icon allows you to mark certain menu items as their favorites or frequently accessed options. This feature saves time by providing quick access to the functions you use most often. The star icon acts like a toggle allowing you to add or remove menu item from your favorite list.

Figure 3. Marking Favorites



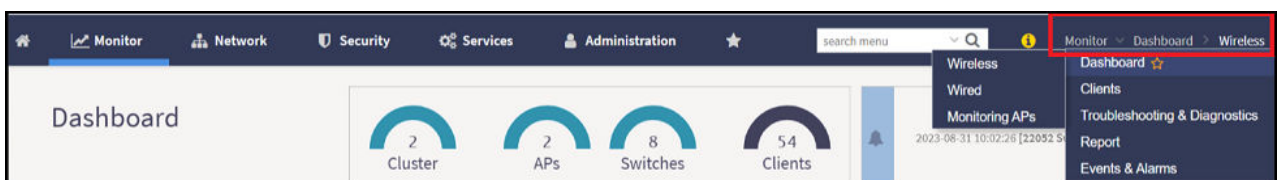
- Search - The **Search** menu increases the usability by allowing you to input keywords specific terms to find relevant information. When you use a search option, it queries the system and returns results that match your input, making it easier to locate specific content or data. It helps you in quickly find what you are looking for.

Figure 4. Using the Search Field



- Breadcrumb - The **Breadcrumb** is a navigation aid that shows your current location within the menu hierarchy. This allows you to see where you are and easily navigate back to previous levels.

Figure 5. Displaying Breadcrumb



- Search History - The **Search History** typically refers to a record of the searches you've conducted. It can include the keywords or phrases you entered when searching for information.

Figure 6. Search History



System Settings

[Viewing System Settings](#)

[Configuring the System Time](#)

[Creating a DNS Server Profile](#)

[Creating a DNS Spoofing Profile](#)

[Setting User Preferences](#)

Viewing System Settings

System settings include options to view system information, configure system time, NTP servers, and DNS servers.

To view the system settings information, select **Administration > System > System Info**. The following system information is displayed:

- Controller Version
- Control Plane Software Version
- Data Plane Software Version
- Default AP Firmware Version (hover over the field to see the firmware type)
- Supported AP Model List with AP firmware and supported AP models
- Cluster Name
- Number of Planes
- System Name
- System Uptime
- Serial Number
- System Capacity of Cluster
- 3GPP Tunneling License

- AP Capacity License
- AP Direct Tunnel License
- Data Plane Capacity License

Figure 1. General Settings for vSZ-H

The screenshot displays the Ruckus SmartZone Administration web interface. At the top, a red banner indicates 'AP certificate is expired'. The navigation bar includes links for Monitor, Network, Security, Services, and Administration. The 'Administration' tab is active, showing a sidebar with 'About', 'Time', and 'Syslog'. The main content area is titled 'System Info' and contains the following details:

- Controller Version: 6.1.2.0.215
- Control Plane Software Version: 6.1.2.0.131
- Default AP Firmware Version: 6.1.2.0.447

Below this, the 'Support AP Model List' is shown as a table with two columns: 'AP Firmware' and 'AP Models'.

AP Firmware	AP Models
6.1.2.0.447	M510,R720,H320,T610S,E510,T305I,T305E,R550,R650,T750,R350,R710,T310S,R510,R610,T710,R310,R750,T610,T750SE,H350,R850,T310N,T710S,H550,H510,T811CM,T310D,C110,T310C,T350SE,R320,R760,R560,T350D,T350C
6.1.0.0.9213	M510,R720,H320,T610S,E510,T305I,T305E,R550,T750,R650,R350,T310S,R710,R510,R730,T710,R610,R750,R310,T750SE,T610,R850,T310N,H350,T710S,H550,T811CM,H510,T310D,T310C,C110,T350SE,R320,R760,T350D,T350C
6.1.0.0.1595	M510,R720,H320,T610S,E510,T305I,T305E,R550,R650,T750,R350,R710,T310S,R510,R730,R610,T710,T750SE,R310,T610,R750,R850,H350,T310N,T710S,H550,H510,T811CM,T310D,T350SE,C110,T310C,R320,T350D,T350C
5.2.2.0.2064	R600,T504,T301S,M510,R720,R500,H320,T610S,E510,F2M300,T305I,T305E,R550,T750,R650,T301N,R500E,T310S,R710,R510,R730,T710,R610,R750,R310,T750SE,T610,R850,T310N,T710S,T811CM,H510,T300E,T310D,T310C,C110,R320,T3...
5.2.2.0.2012	R600,T504,T301S,M510,R720,R500,H320,T610S,E510,F2M300,T305I,T305E,R550,T750,R650,T301N,R500E,T310S,R710,R510,R730,T710,R610,R750,R310,T750SE,T610,R850,T310N,T710S,T811CM,H510,T300E,T310D,T310C,C110,R320,T3...
5.2.2.0.1106	R600,T504,T301S,M510,R720,R500,H320,T610S,E510,F2M300,T305I,T305E,R550,T750,R650,T301N,R500E,T310S,R710,R510,R730,T710,R610,R750,R310,T750SE,T610,R850,T310N,T710S,T811CM,H510,T300E,T310D,T310C,C110,R320,T3...
5.2.2.0.1080	R600,T504,T301S,M510,R720,R500,H320,T610S,E510,F2M300,T305I,T305E,R550,T750,R650,T301N,R500E,T310S,R710,R510,R730,T710,R610,R750,R310,T750SE,T610,R850,T310N,T710S,T811CM,H510,T300E,T310D,T310C,C110,R320,T3...
5.2.2.0.1040	R600,T504,T301S,M510,R720,R500,H320,T610S,E510,F2M300,T305I,T305E,R550,T750,R650,T301N,R500E,T310S,R710,R510,R730,T710,R610,R750,R310,T750SE,T610,R850,T310N,T710S,T811CM,H510,T300E,T310D,T310C,C110,R320,T3...
5.2.2.0.1026	R600,T504,T301S,M510,R720,R500,H320,T610S,E510,F2M300,T305I,T305E,R550,T750,R650,T301N,R500E,T310S,R710,R510,R730,T710,R610,R750,R310,T750SE,T610,R850,T310N,T710S,T811CM,H510,T300E,T310D,T310C,C110,R320,T3...
5.2.2.0.1019	R600,T504,T301S,M510,R720,R500,H320,T610S,E510,F2M300,T305I,T305E,R550,T750,R650,T301N,R500E,T310S,R710,R510,R730,T710,R610,R750,R310,T750SE,T610,R850,T310N,T710S,T811CM,H510,T300E,T310D,T310C,C110,R320,T3...
5.2.2.0.301	R600,T504,T301S,M510,R720,R500,H320,T610S,E510,F2M300,T305I,T305E,R550,T750,R650,T301N,R500E,T310S,R710,R510,R730,T710,R610,R750,R310,T750SE,T610,R850,T310N,T710S,T811CM,H510,T300E,T310D,T310C,C110,R320,T3...

- **Note:** For the SZ300 and vSZ-H platforms, the AP to switch ratio is 5:1. For more details, refer to *SmartZone Upgrade Guide* and *Virtual SmartZone Getting Started Guide*.

Parent topic: [System Settings](#)

Configuring the System Time

The controller has three external Network Time Protocol (NTP) servers that are used to synchronize the time across access points, cluster nodes, and virtual data planes.

- **Note:** The controller supports NTP version 4.2.6p5. The controller and access points do not accept broadcast and multicast NTP packets that would result in a timestamp. These packets are ignored by default.

Perform the following steps to edit the system time:

1. From the main menu, navigate to **Administration > System > Time**.
2. Configure the following options:

- a. **NTP Primary Server:** Enter the primary NTP server address.

Figure 1. Setting the System Time

System Time

System Time: 2020-07-20 10:56:00 UTC

System UTC Time: 2020-07-20 10:56:00 UTC

* NTP Primary Server:

NTP Secondary Server:

NTP Third Server:

* System Time Zone:

NTP Primary Server Authentication

Key Type:

* Key ID:

* Key: The PSK is provided by the NTP server, please fill it accordingly

NTP Secondary Server Authentication

Key Type:

* Key ID:

* Key: The PSK is provided by the NTP server, please fill it accordingly

NTP Third Server Authentication

Key Type:

* Key ID:

* Key: The PSK is provided by the NTP server, please fill it accordingly

- b. **Sync Server:** Click this button to enable the controller to sync with the configured NTP server, and then sync the cluster-follower nodes, APs, and vDPs with the controller time.

- c. **System Time Zone:** Select the time zone from the drop-down. The default time zone is (GMT +0:00) UTC.

- d. You can achieve secured communication with NTP servers after configuring them.

To establish this communication, in the **NTP Server Authentication** field, configure the following:

- **Key Type** as MD5 or SHA1.
- **KEY ID** in the range of 1 to 65534.
- **Key or PSK** as negotiated for each of the NTP servers.


3. Click **OK**.


Parent topic: [System Settings](#)

Creating a DNS Server Profile

A DNS server profile, allows you specify the primary and secondary address of the DNS server for devices to identify the host name within the specified Zone.

1. Go to **Administration > System > DNS Servers**.
The **DNS Servers** page is displayed.
2. Click **Create**.
The **Create DNS Server Profile** page is displayed.
3. Configure the following:
 - a. Name: Type a name for the DNS server profile.
 - b. Description: Type a short description for profile.
 - c. Primary DNS IP: Type the primary DNS IP address.

 **Note:** This feature supports IPv4 address format.
 - d. Secondary DNS IP: Type the secondary DNS IP address.

 **Note:** This feature supports IPv4 address format.
 - e. Click **OK**.

You have created the DNS Server Profile.

- **Note:** You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **DNS Servers** page.

Parent topic: [System Settings](#)

Creating a DNS Spoofing Profile

A DNS spoofing profile allows you to specify individual Fully Qualified Domain Name (FQDN) entries to bypass DNS resolution and provide clients with the result specified in the associated rules.

Follow the steps below to create a DNS Spoofing profile.


1. Go to **Services > Others > DNS Spoofing**
2. Select the zone for which you want to create profile.
3. Click **Create**.
The **Create DNS Spoofing Profile** page is displayed.

Figure 1. Creating DNS Spoofing Profile

The screenshot shows the 'Create DNS Spoofing Profile' dialog box. It features a title bar and two main sections. The 'General Options' section includes a 'Name' field (marked with a red asterisk) and a 'Description' field. The 'Rules' section includes a dropdown menu and three buttons: '+ Create', 'Configure', and 'Delete'. Below these buttons is a table with two columns: 'Domain Name' and 'IP Address'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

4. Configure the following:
 - a. Name: Enter a name for the DNS spoofing profile.
 - b. Description: Enter a short description for the profile.
 - c. Click **Create**, and the **Create Rules** dialog box is displayed.

- d. In the **Domain Name** field, enter the FQDN of an individual host entry.
- e. In the **IP Address** field, enter the IPv4 or IPv6 address to resolve the domain name and click **Add**. If the user sends DNS request with the domain name configured in the DNS Spoofing profile, then the AP responds with the IP address configured in the DNS Spoofing profile for the requested domain name.
- f. Click **OK** to confirm the rules.
- g. Click **OK** to confirm the creation of DNS spoofing profile.

 **Note:** You can also edit, clone or delete the profile by selecting the options **Configure**, **Clone** or **Delete** respectively, from the **DNS Spoofing** tab.

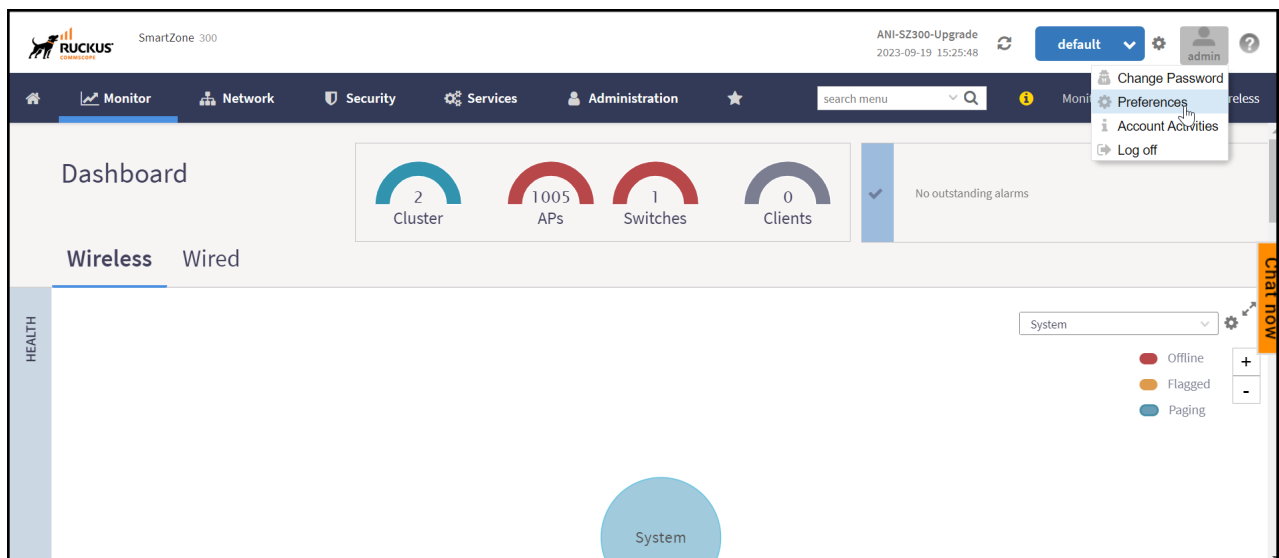
Parent topic: [System Settings](#)

Setting User Preferences

You can configure the language in which the user interface must appear, and also customize the session time for the interface.

1. In the controller web interface, click on the **user profile** and click **Preferences**. This displays **User Preferences** page.

Figure 1. User Profile Menu - Preferences



2. In the **User Preferences** page, enter the following details.
 - **Session Idle Timeout Setting** - Enter the duration in **minutes** for the web interface session to refresh.
 - **Language** - Select the language of your choice from the drop-down list to view the web interface content. The following languages are supported in the application -

- Spanish
- Brazilian Portuguese
- French
- German
- Italian
- Russian
- Simplified Chinese
- Traditional Chinese
- Korean
- Japanese
- **Use Legacy Menu** - By default this button is **Off**, enable this button to view the old menu (prior to release 6.0.0).
- **Usage Data Collection** - By default this button is **Off**, enable this button to collect data for analytics. For more information on data collection, click on the link corresponding to the field.
- **Customer Support Chat Bot** - By default this button is **On**, this button enables the chat support feature which is available in the main screen.

Figure 2. User Preferences

User Preferences

* Session Idle Timeout Settings: Minutes (1-1440)

Language:

Use Legacy Menu: ☐ OFF

[?] Usage data collection: ☒ ON For more info on privacy policy click [here](#)

Customer support chatbot: ☒ ON

OK

Cancel

Parent topic: [System Settings](#)

Warnings and Notifications

Warnings

Setting Global Notifications

Warnings

Warnings are displayed in the Miscellaneous bar. They are issues which are critical in nature. Warnings cannot be removed or acknowledged unless the critical issue is resolved.

Figure 1. Sample Warning Message



A list of warning messages that appear are as follows:

- Default 90-day support expiring soon
- System support expiring soon
- System support has expired
- Default 90-day AP license expiring soon
- Default AP license has expired
- Default 90-day RTU license expiring soon
- RTU has expired
- AP Certificate Expiration
- Node Out of Service
- Cluster Out of Service
- VM Resource Mismatch
- Suggested AP Limit Exceeded
- AP/DP version mismatch

Parent topic: [Warnings and Notifications](#)

Setting Global Notifications

Notifications are integrated with existing alarms and they are displayed only when a notification alarm exists and is not acknowledged by the administrator. Notifications can be viewed from the **Content** area. Administrators can acknowledge the notification by either:

- Clearing the alarm
- Acknowledging the Alarm


For more information, refer to the “Managing Alarms and Events” chapter.

Alarm severity are of three types:

- Minor
- Major
- Critical

The administrator can change the alarm severity shown on the dashboard. To do so:

1. From the Notifications area, Click the **Setting** icon, this displays **Settings - Global Notification** window.
2. From the **Lowest alarm severity** drop-down, select the required severity level.
3. Click **OK**. Notifications corresponding to the selected alarm severity and severity above it are displayed in the Notification area of the Dashboard.

 **Note:** RUCKUS AI is configured on the SmartZone (controller) platform. When the user connects to RUCKUS AI through the controller, a status tag is displayed in the controller header and the browser re-directs the user to RUCKUS AI page. Currently, this feature is dependent on RUCKUS AI.

Parent topic: [Warnings and Notifications](#)

Working with Maps

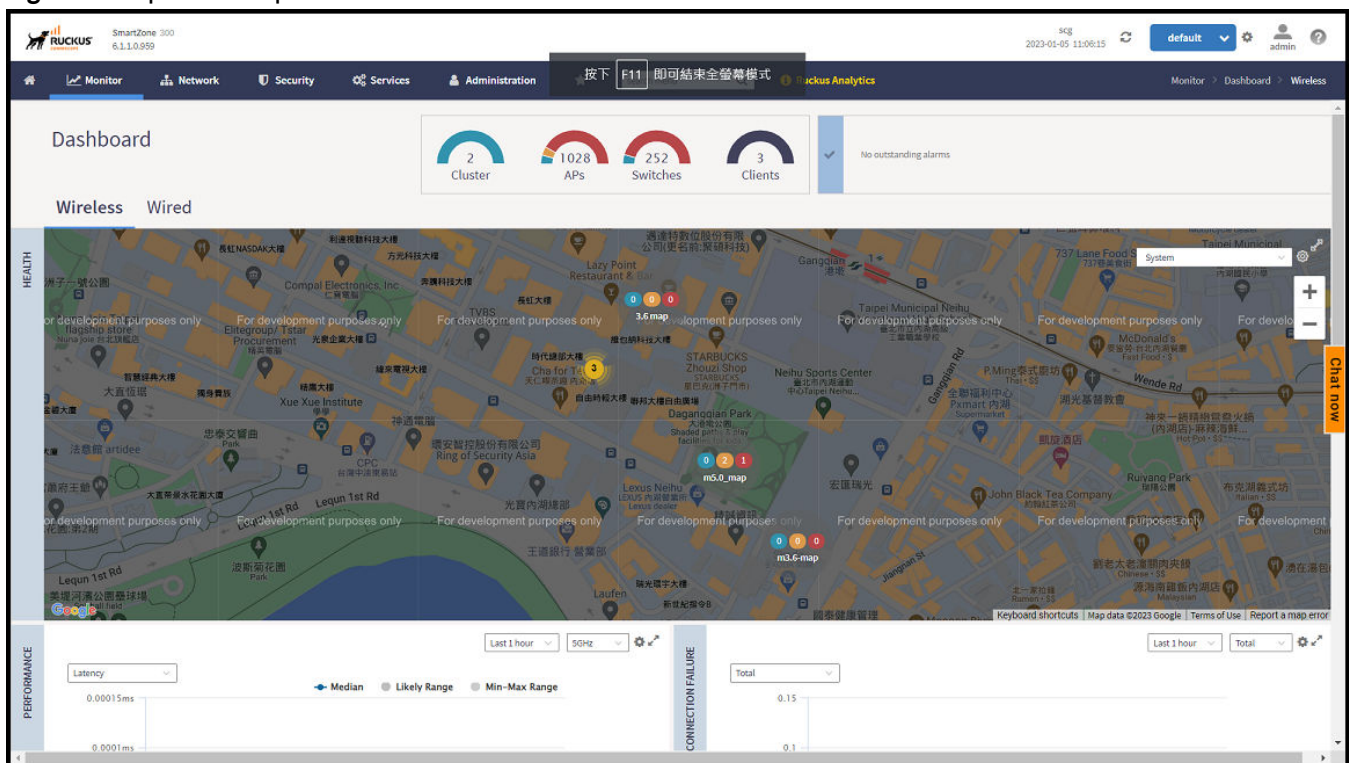
Importing floorplan maps into SmartZone allows you to further customize the information displayed on the Dashboard and Access Points pages, and monitor your APs, zones, groups, clients and traffic statistics all within the world map view on the Dashboard.

Additionally, you can use the maps to quickly locate more specific information on a venue or zone, and drag and drop APs onto the floor plan map to represent their locations in physical space in your venue.

Once a map is imported and GPS coordinates are entered, an icon representing the venue appears on the world map on the Dashboard. The icon displays the current number of APs (Online, Flagged and Offline). You can hover over the icon for more information.

Double-click the map icon or click **Zoom into this map** to view the imported map in the Dashboard.

Figure 1. Imported Maps on the Dashboard



Importing a Floorplan Map

The controller provides a user-friendly workflow for importing a map of your venue floorplan, placing APs in their respective physical locations on the map, and scaling the map to match the actual dimensions of your venue.

Floorplan maps allow you to view site/venue/floor-specific details such as:

- AP status, performance, and health conditions
- Client connections to an AP
- Location-specific trouble spots related to AP or client connectivity

To import a floorplan map:

1. Go to **Network > Wireless > Maps**.
2. From the System tree hierarchy, select the location where you want to create a map and click the **Add** icon button. The **Add Map** form appears.
3. On the **Details** tab, enter a **Name** and optionally a **Description** to identify the map.
4. Enter a **Location** for the map. Alternatively, you can choose the location from the auto-completion options. After you select the location, the GPS Coordinates are automatically updated.
5. For **GPS Coordinates**, you can enter the **Latitude** and **Longitude** values.

Figure 1. Creating the Add Map form

The screenshot shows the 'Add Map' dialog box. It has a title bar with a close button (X). Inside, there are three tabs: 'Details', 'Scale Map', and 'Place APs'. The 'Details' tab is active. Below the tabs, there are several input fields: 'Name' with the value 'My Floorplan 1', 'Description' with 'Office building map', 'Location' with 'Sunnyvale', 'GPS Coordinates: Latitude' with '25.07858', 'Longitude' with '121.57141', and an example '(example: 25.07858, 121.57141)'. There is also a 'Map Image' field with a 'Browse' button. At the bottom right, there are 'Next' and 'Cancel' buttons.

6. To add a **Map Image**, click **Browse** and select a site, venue, or floor map in jpg, jpeg, png, bmp or svg file formats.

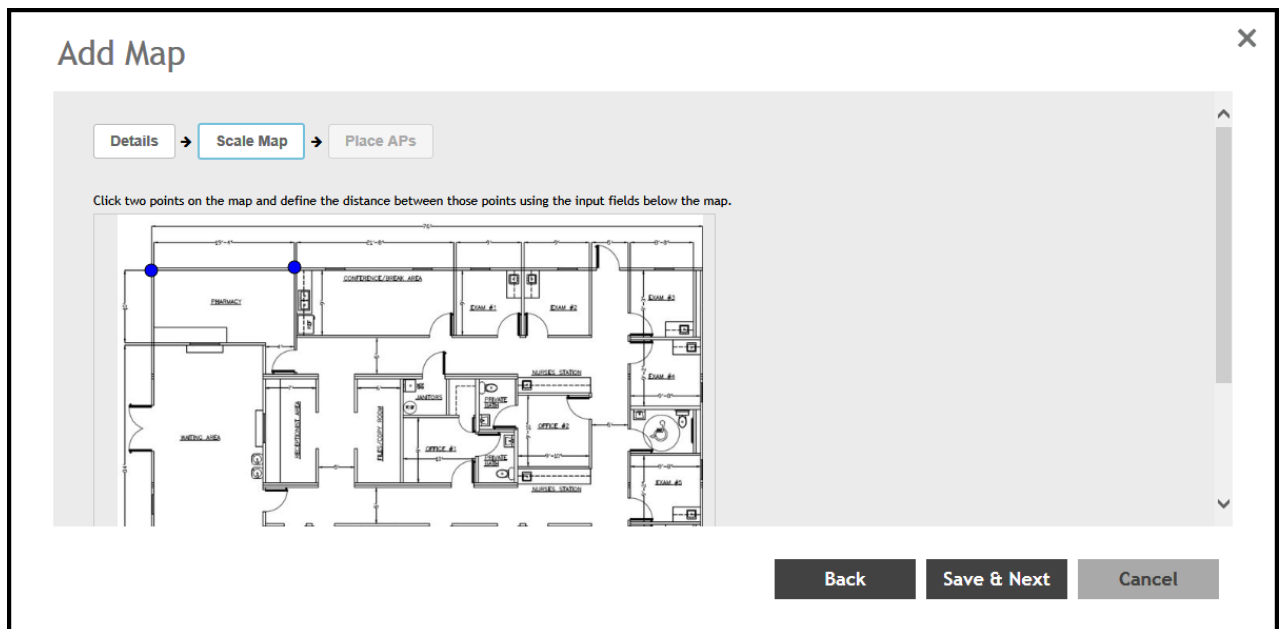
Note:

The maximum file size per indoor map is 5MB.

7. Click **Next**, the **Scale Map** tab is displayed.

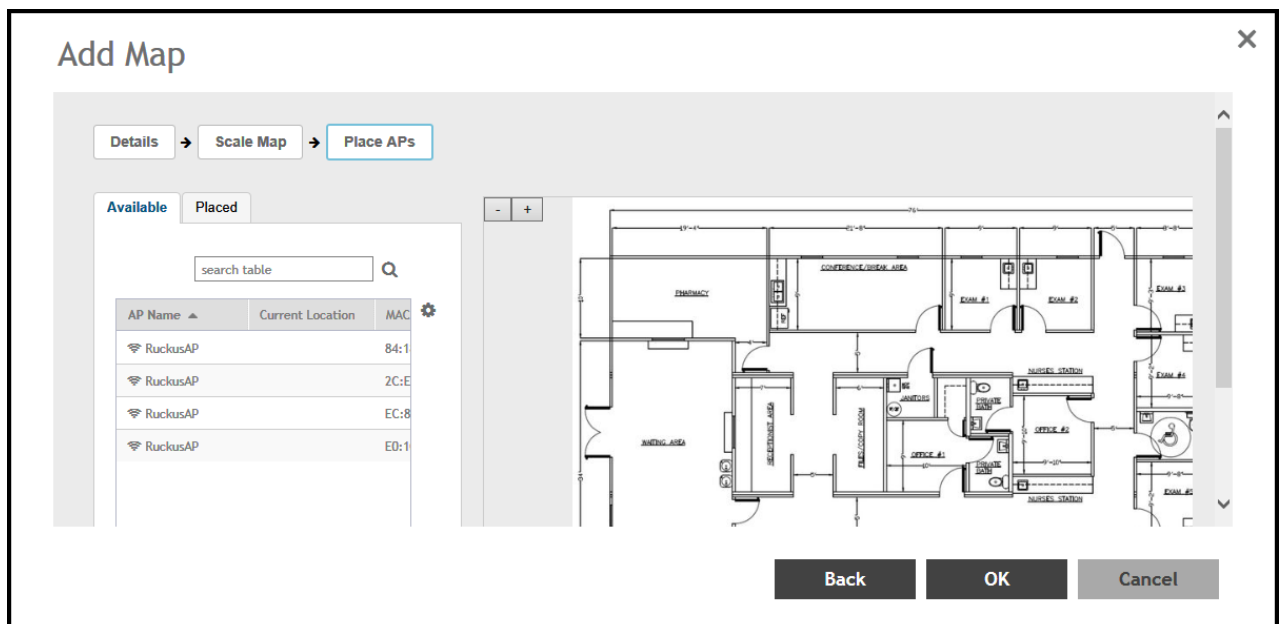
8. Click two points on the map between which you know the distance. Blue dots appear to show the points you selected.

Figure 2. Indicating the Selected Points on the Map



9. Enter the **Physical Distance** between the two points and select the unit of measurement (mm, cm, m, ft, yard).
10. Click **Save & Next**. The **Place APs** tab appears.
11. From the **Available** list, drag the APs and place them in their physical locations on the map. Click the **Placed** tab to see the list of placed APs.

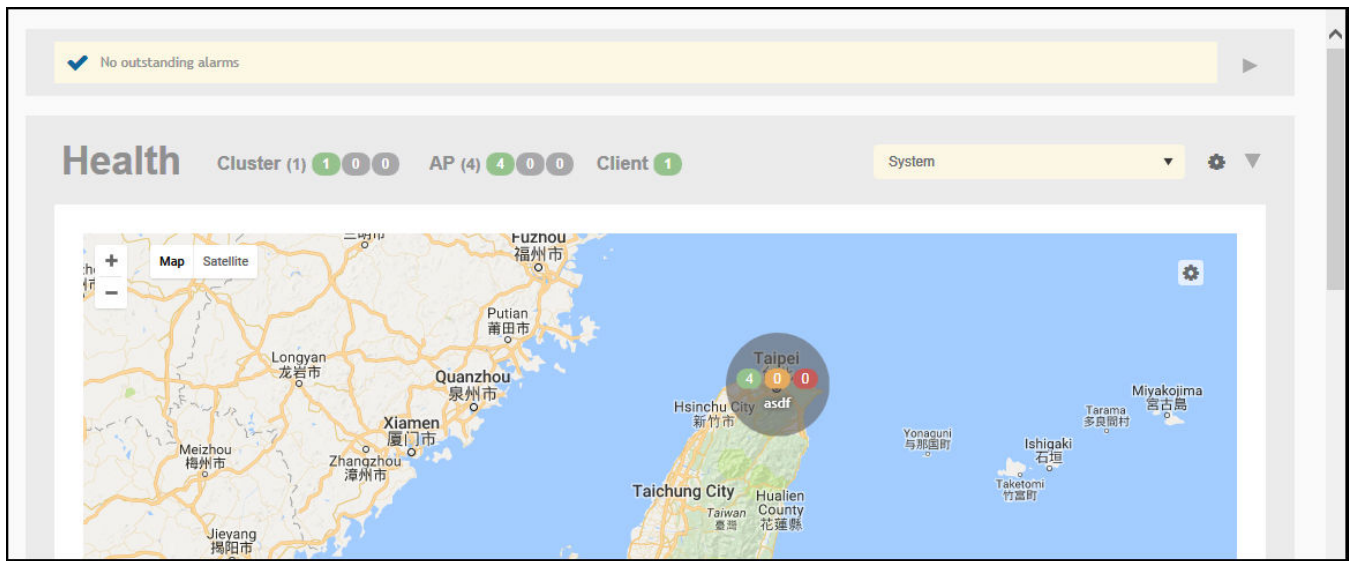
Figure 3. Dragging and dropping to place APs on the Floorplan



- Once you are happy with the placement of your APs on the map, click **OK** to save your map.

Your venue now appears as an icon on the world map on the Dashboard, located at your venue's actual physical location (if you entered the GPS coordinates correctly). The Dashboard icon that represents your venue provides an overview of the number of APs in the venue and their status. Hover over the icon to view more details, or click one of the links to zoom in to the venue floorplan map you imported.

Figure 4. Importing Venue Map Icon



- Note:** You can also edit or delete a map. To do so, select the map from the list and click the **Edit** or **Delete** icons respectively.

Parent topic: [Working with Maps](#)

Viewing RF Signal Strength

Radio Frequency (RF) signal strength can be viewed using a heat map for a specific location.

The heat map helps us identify the RF signal strength in a specific location. It provides heat maps using actual path loss information from the environment. You can view an indoor floor plan map for an AP.

To view the RF signal strength:

- Go to **Network > Wireless > Maps**.
- From the System tree hierarchy, select the location of the map that you want to view.
- Select the **Show Signal Coverage** check box and choose the required RF frequency. For example, 2.4 GHz or 5 GHz. The heat map is displayed with a color-gradient legend. High signal strength appears in red. The color changes as the signal strength reduces.

Figure 1. RF Coverage Heat Map

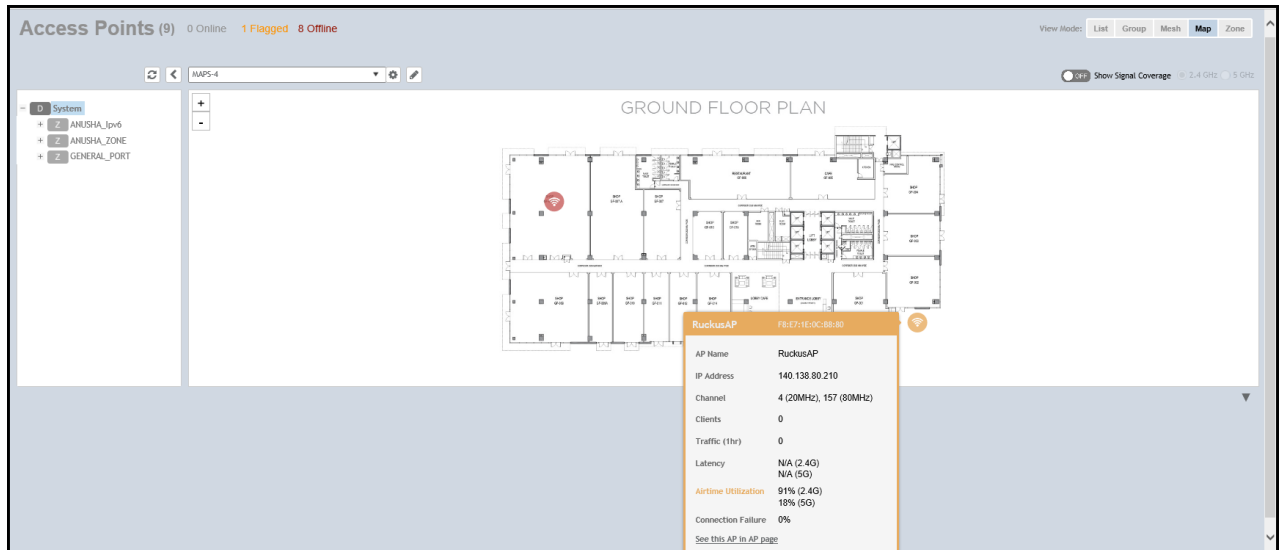
Parent topic: [Working with Maps](#)

Monitoring APs Using the Map View

Use the Map view on the **Access Points** page to monitor APs in relation to your venue's floorplan.

1. Go to **Network > Wireless > Access Points**.
2. In **View Mode**, click the **Map** button. The map view is displayed with your placed APs.
3. Hover over an AP to view the following AP-specific details:
 - **AP Name:** The name of the AP, if configured. If not, the default AP name is "RuckusAP."
 - **IP Address:** The current IPv4 or IPv6 address assigned to the AP.
 - **Channel:** Displays the channel (2.4 GHz / 5 GHz) in use, along with the channel width in parentheses.
 - **Clients:** The number of currently connected wireless clients.
 - **Traffic:** The total traffic volume over the last 1 hour.
 - **Latency:** The average time delay between AP and connected clients.
 - **Airtime Utilization:** Percent of airtime utilized, by radio.
 - **Connection Failure:** Percent of client connection attempt failures.

Figure 1. Hover to AP to view details



- To view more specific details on the AP, click the **See this AP in AP page** link.
- To view the RF signal strength, select the **Show Signal Coverage** check box and choose the required RF frequency. For example, 2.4 GHz or 5 GHz.
The heat map is displayed with a color-gradient legend. High signal strength appears in red. The color changes as the signal strength reduces.

Parent topic: [Working with Maps](#)

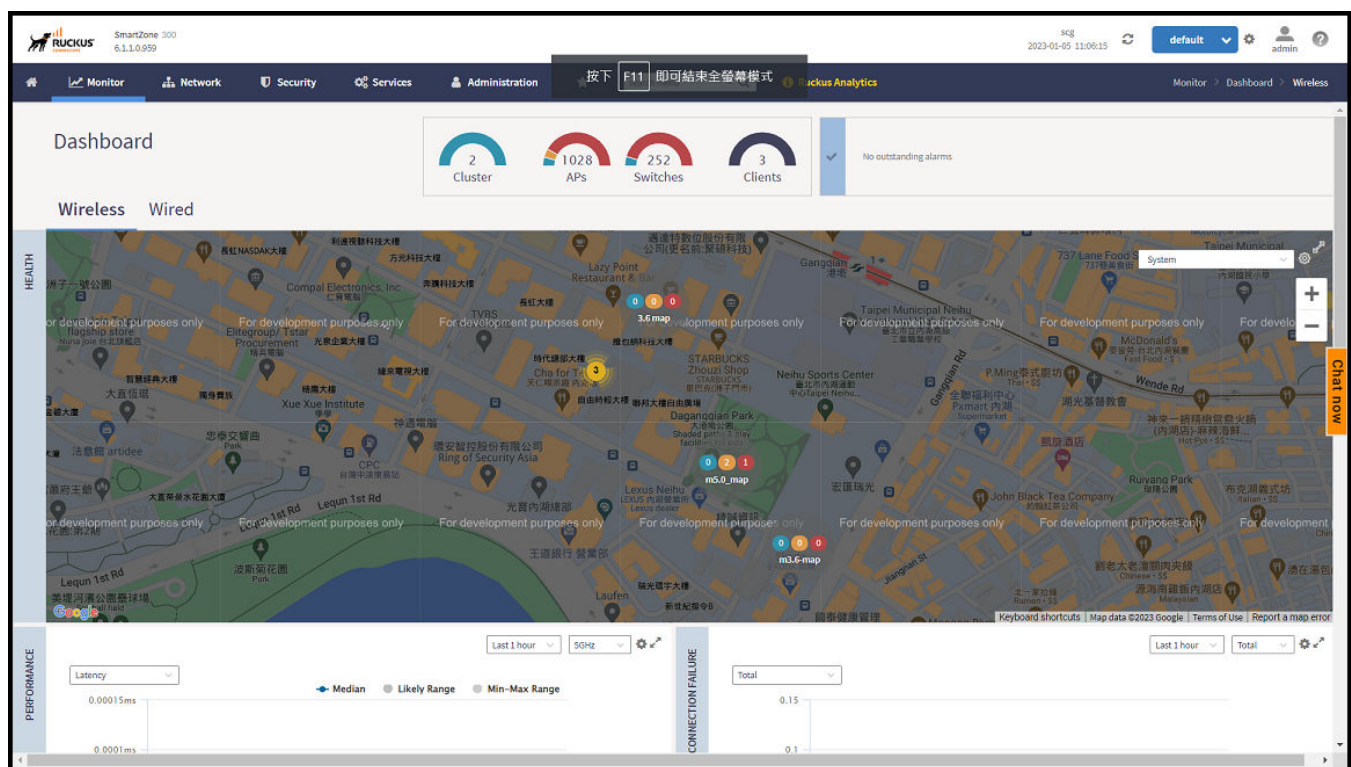
Health and Maps

The Health dashboard gives you a very high-level overview of wireless devices such as cluster, AP and clients, and wired devices such as ICX switches. For wireless devices, it displays a world map view using Google Maps, which provides a global view of your SmartZone-controlled wireless network deployments.

You must click **Wireless** or **Wired** in the dashboard to view the respective devices.

The status bar at the top of the Health dashboard contains an iconic representation of the total Cluster, AP and Client counts for the entire system. This information can be filtered to display a single zone, AP group, or venue using the drop-down filter menu. You can also customize the dashboard layout and threshold settings using the Settings (gear) icon.

Figure 1. Health Workspace Area



The Wired devices section provides information about the health of the switch and the traffic it handles.

For more information on customizing the information displayed on the Health dashboard, see the section [Customizing Health Status Thresholds](#).

Understanding Cluster and AP Health Icons

The Health dashboard status bar displays the following Cluster and AP information using three colored icons to denote the number of APs/clusters currently in that state.

The icons for both Cluster and AP status overviews are represented by the following color coding scheme:

-  (Green): Online
-  (Orange): Flagged
-  (Red): Offline

Online and Offline status are self-explanatory. "Flagged" status is user-defined. You can customize the thresholds at which an AP or cluster enters "flagged" state using the **Settings** (gear) icon in the status bar. For more information, see [Customizing Health Status Thresholds](#).

Parent topic: [Health and Maps](#)

Customizing Health Status Thresholds

You can customize the way the controller categorizes and displays clusters and APs shown in "Flagged Status" in the status bar.

To customize the Health dashboard, click the **Settings** (gear) icon. In the **Settings - Health Dashboard** form, click the **Cluster Status** or **AP Status** tab, and configure the following:

- **Cluster Status:** Configure CPU, hard disk and memory usage percentages above which the cluster will be marked as flagged status.
- **AP Status:** Configure the criteria upon which APs will be flagged. For more information, see the [Customizing Health Status Thresholds](#) section.

Figure 1. Setting Cluster Health Status Thresholds

Settings - Health Dashboard

Display Google Map API Key **Cluster Status** AP Status

Flagged Status

CPU usage exceeds: %

Disk usage exceeds: %

Memory usage exceeds: %

Processor temperature exceeds: °C

OK **Close**

Parent topic: [Health and Maps](#)

Customizing AP Flagged Status Thresholds

Use the following procedure to customize when APs will be marked as "flagged" on the Health dashboard status bar.

1. Click the **Gear** icon on the **Health** dashboard.
2. The **Settings - Health Dashboard** form appears. Click the **AP Status** tab.
3. Select the behavior of flagging policies when applying changes to parent or child groups:
 - Apply the change to all child groups
 - Apply the change if child group settings already match the parent group
4. Configure thresholds above which APs will be marked as "flagged" for the following criteria:
 - Latency
 - Airtime Utilization
 - Connection Failures
 - Total connected clients

- Configure the radio (2.4 / 5 GHz) from the drop-down menu and select the level (system, zone, AP group) at which you want to apply the policy, and configure the **Sensitivity** control for the threshold (Low, Medium, High). Setting the Sensitivity level to Low means that an AP must remain above the threshold for a longer period of time before it will appear in the flagged category, while a High sensitivity means that APs will more quickly alternate between flagged and non-flagged status.
- Click **OK** to save your changes.

Figure 1. Configuring AP Flagged Status Thresholds

Settings - Health Dashboard

Display Google Map API Key Cluster Status **AP Status**

AP status will be "flagged" based on the following criteria.
When changing settings of a parent group, how should it affect child groups?

☒ Apply the change to all child groups
☐ Apply the change if child group settings already match parent group

☒ Latency ▼ Hide Threshold

2.4GHz

	Enable	Threshold	Sensitivity
- [D] System	<input checked="" type="checkbox"/>	150 ms	Medium
+ [D] Domain_3.6	<input checked="" type="checkbox"/>	150 ms	Medium
+ [D] Domain_5.0	<input checked="" type="checkbox"/>	150 ms	Medium
+ [D] Domain_5.1.2	<input checked="" type="checkbox"/>	150 ms	Medium

☒ Airtime Utilization ► Show Threshold

OK **Close**

Parent topic: [Customizing Health Status Thresholds](#)

Using the Health Dashboard Map

Use the Google Maps view just as you would normally use Google Maps - including zoom, satellite view, rotate and even street view icons. You can customize the AP icon information displayed on the map using the tools in the upper-right hand corner.

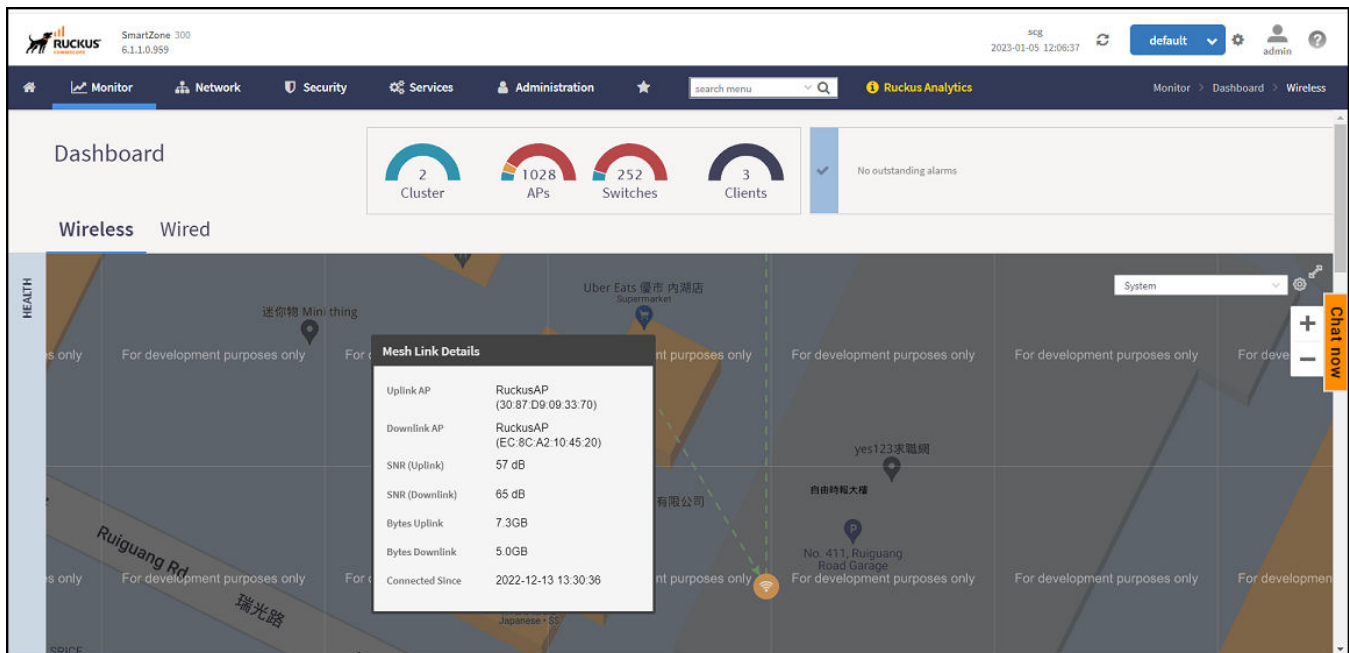
For SZ100 and vSZ-E platforms, use the **AP Status** pull-down menu to configure which AP health parameters will be displayed on the AP icons on the map. Use the Display menu to display the client count or radio channel in use.

Use the **Settings** icon to configure the information displayed in tooltips when hovering over an AP on the map. You can also change the view mode altogether, from map view to Groups, Control Planes or Data Planes view mode using the settings menu. Additionally, you can also select the check-box to show mesh links. These links appear as dotted lines. If you hover over the mesh link on the map, a pop-up appears displaying more information such as the following:

- Uplink AP: displays the IP address of the uplink AP to which the wireless client sends data
- Downlink AP: displays the IP address of the downlink AP from which data is sent back to the wireless client
- SNR (Uplink): displays the signal-to-noise ratio in the uplink path
- SNR (Downlink): displays the signal-to-noise ratio in the downlink path
- Bytes (Uplink): displays the bytes of data transferred from the client to the uplink AP
- Bytes (Downlink): displays the bytes of data transferred from the downlink AP to the client
- Connected Since: displays the date and time when the mesh connection was established

Bytes (Uplink) and *Bytes (Downlink)* are aggregate counters for the mesh connection since the start of that mesh connection. If the mesh link is broken and restarts, the counter restarts. If the mesh AP connects to a different mesh root or uplink, the counter restarts.

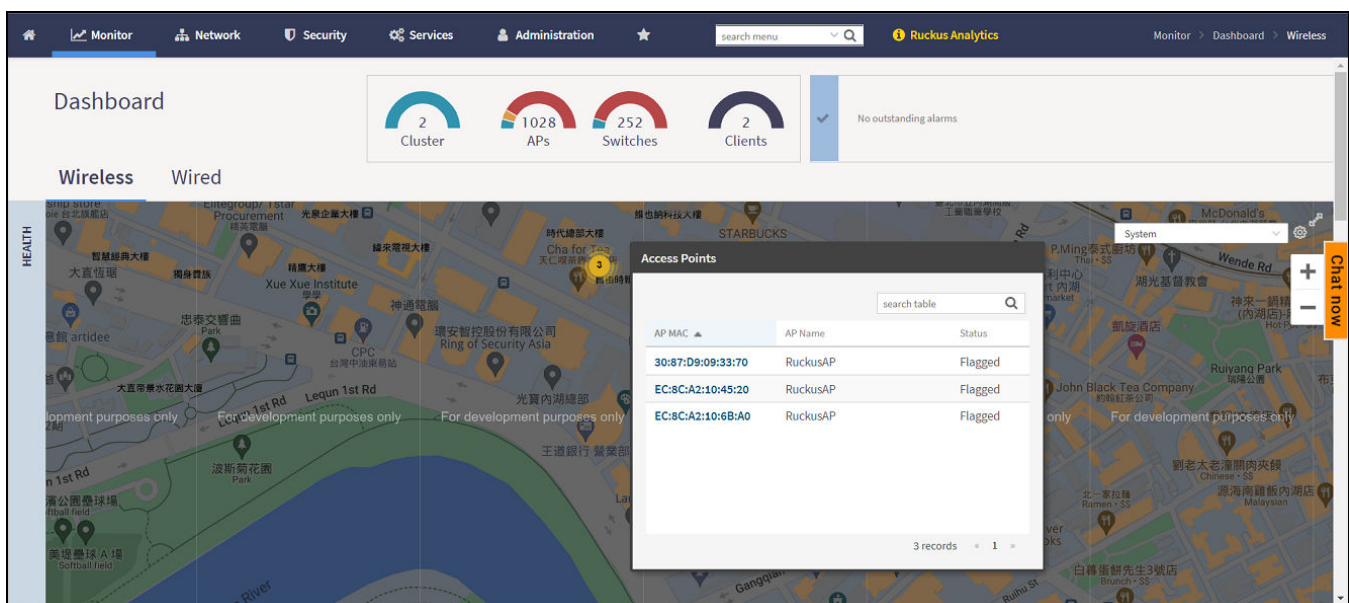
Figure 1. Mesh Link Details



You can view and identify APs with the same GPS. If you hover over and click the clustered marker of AP on the map, a pop-up appears displaying more information such as the following:

- AP MAC: Displays the MAC address of the AP
- AP Name: Displays the name assigned to the access point
- Status: Displays the status of the AP such as Online or Offline

Figure 2. AP Details



You can also select the Google Map API key to use the Maps service with the application.

Figure 3. Configuring Map Settings

The screenshot shows a window titled "Settings - Health Dashboard" with a close button (X) in the top right corner. Below the title bar are four tabs: "Display", "Google Map API Key", "Cluster Status", and "AP Status". The "Display" tab is selected and highlighted with a blue underline. Inside the "Display" tab, there is a form with the following settings:

- Refresh every:** A dropdown menu set to "15 minutes".
- Mouse scroll behavior:** Two radio buttons, "Zoom" (unselected) and "Scroll" (selected).
- View Mode:** A dropdown menu set to "Map".
- Tooltip:** A list of seven items, each with a toggle switch set to "ON":
 - IP Address
 - Channel
 - Clients
 - Traffic (1hr)
 - Latency
 - Airtime Utilization
 - Connection Failure
- Show Mesh Links:** A toggle switch set to "ON".

At the bottom right of the window are two buttons: "OK" and "Close".

Note: In order for your venues to appear on the world map, you must first import a map of your site floorplan.

Parent topic: [Health and Maps](#)

Configuring the Google Map API Key Behavior

The Google Maps feature in the controller application works based on API interaction between the application and the Maps service hosted by Google. By default, these APIs are commonly available without the need for an API key but sometimes, you might have to generate a key.

If Google Maps do not display properly in the absence of an API key, or when the API usage exceeds the daily limit, then an API key needs to be generated to ensure the map displays all the elements properly.

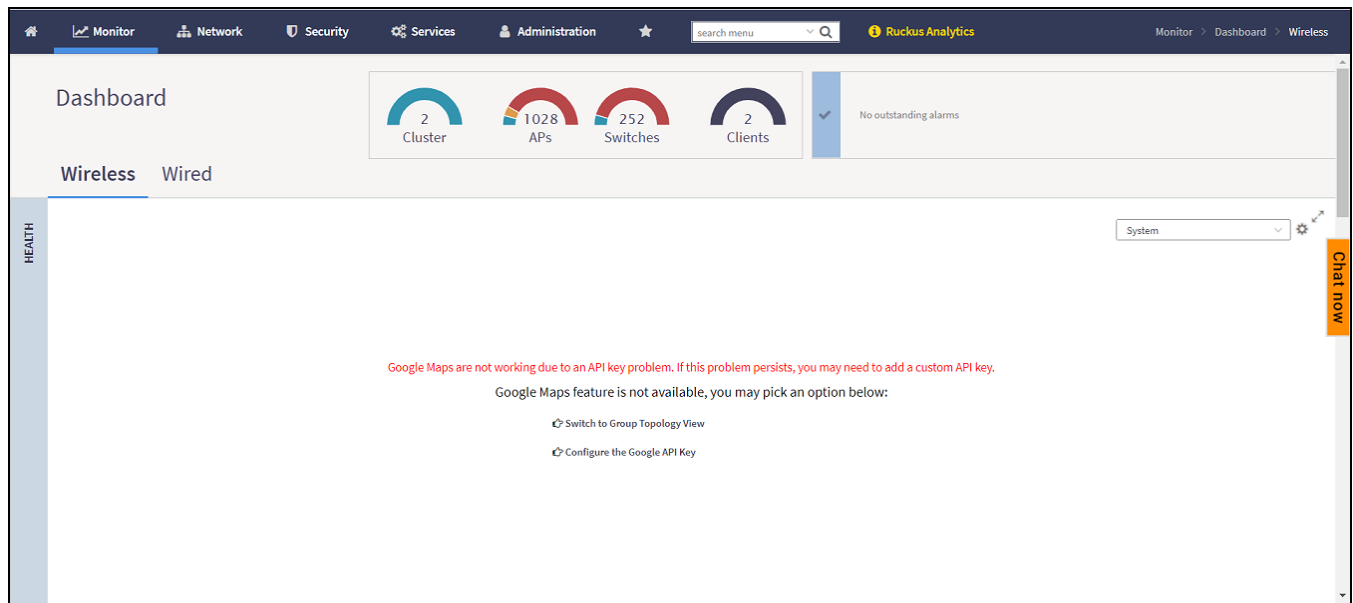
You would also have to generate an API key if you encounter errors such as:

MissingKeyMapError

or

NoApiKeys

Figure 1. Health dashboard view when API key is not available



Clicking **Configure the Google API Key** directs you to the **Google Map API Key** tab, where you can manage the Google Map API Key behavior.

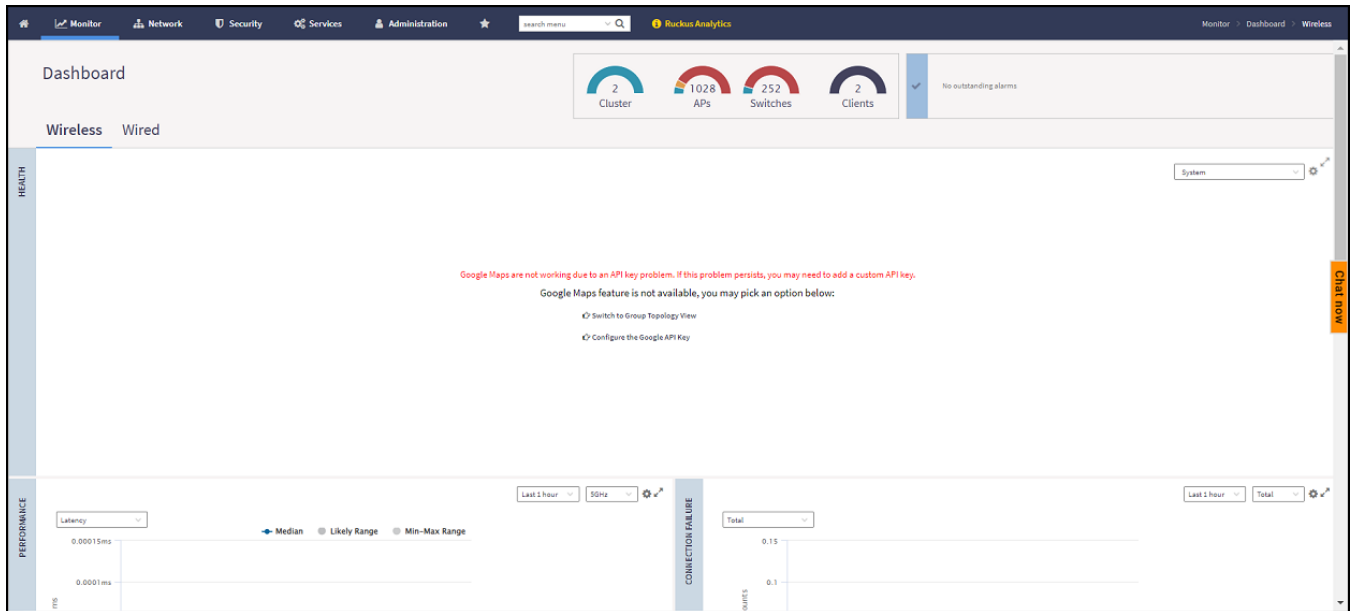
All administrators of the system can use the same API key, or apply a unique API key per administrator. Allowing an API key per administrator enables more flexibility when API usage is high, or in circumstances when each tenant must use their own API key.

Follow these steps to configure the Google Map API Key behavior.

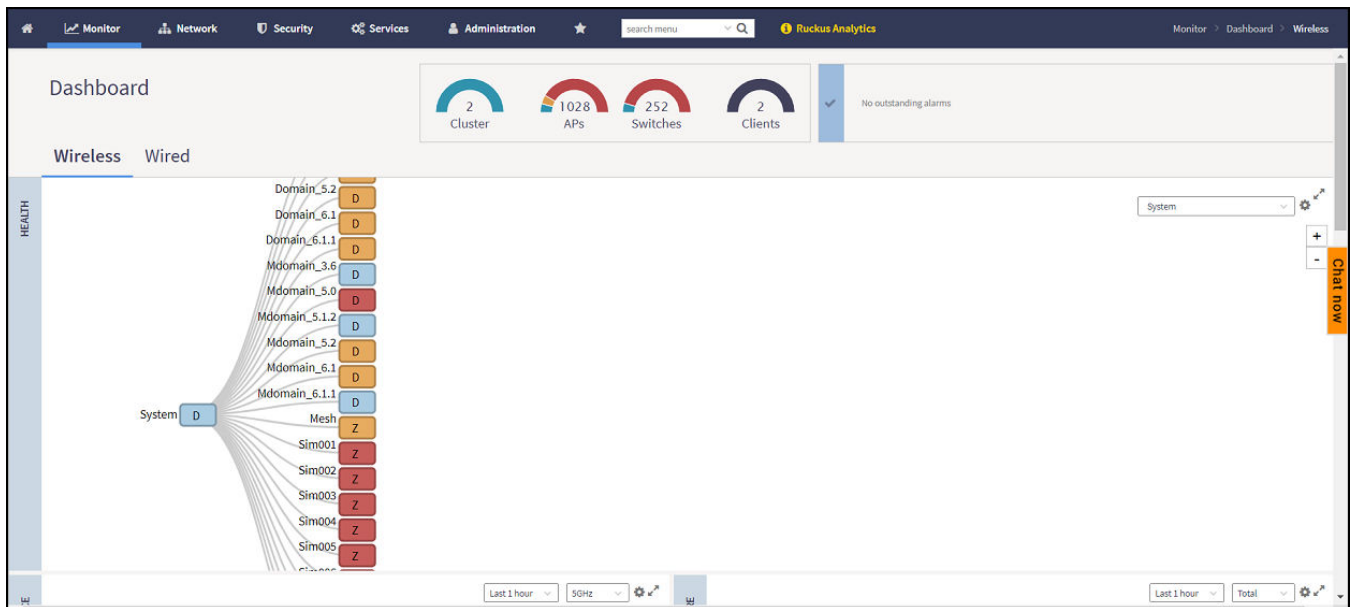
Launching the application displays the **Dashboard** menu, by default.

In **Health**, the map view appears if you are connected to a network. If you are not, then you might see the following screen and would have to view your network deployment as a topology diagram.

Figure 2. No Map View

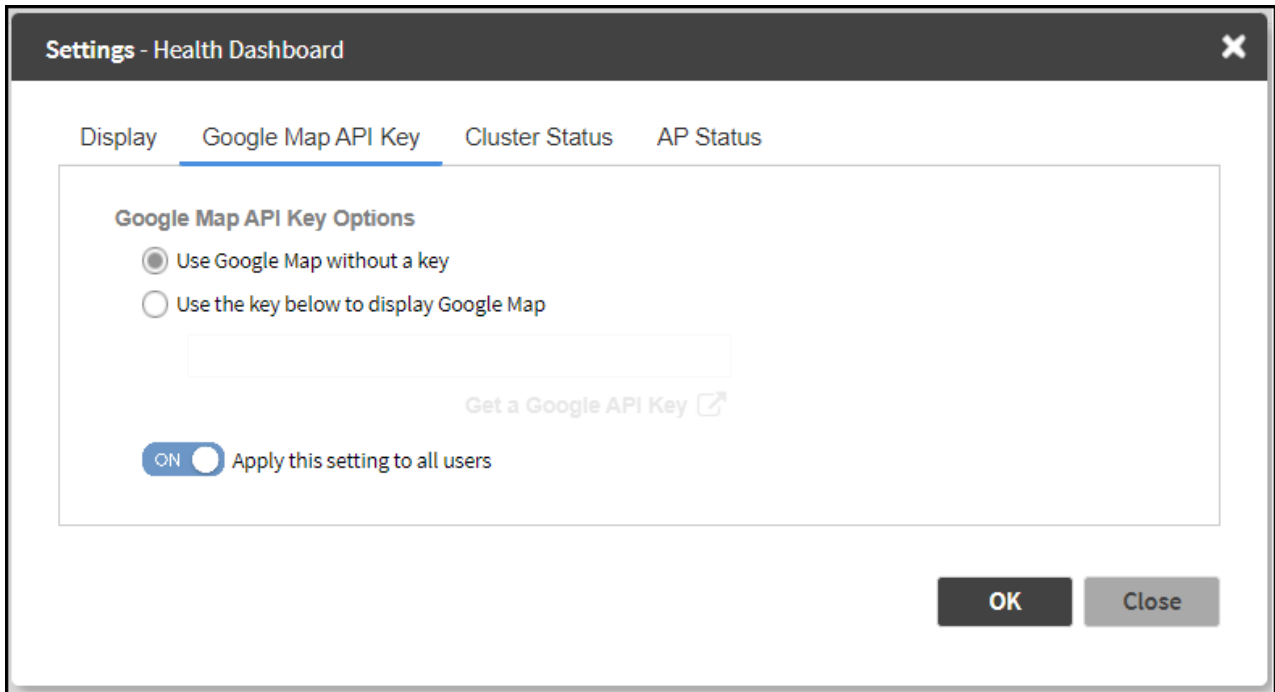


If you click the **Switch to Group Topology View**, a topology diagram similar to the below figure is displayed.
Figure 3. Topology View



1. From the map view in **Health**, click the **Settings** icon.
 The **Settings-Map** page appears.


Figure 4. Google Map API Key Options



From the **Display** tab, you can choose the mode in which you want to view your network deployment.

2. Click the **Google Map API Key** tab.
3. From the **Google Map API Key Options**, select one of the following:

Option	Description
Use Google Map without a key	Allows you to use the Google map feature without an API key.
Use the key below to display Google Map	Allows you to enter an API key which you already have to use the Google map feature. If you do not have a pre-existing API key, you can generate one by following the instructions in the Get a Google API Key link.

 **Note:** The Google API Console is a platform on which you can build, test, and deploy applications. To use Google Maps API, you must register your application on the Google API Console and generate a Google API key which you can add to the application. For more information, see <https://developers.google.com/maps/documentation/javascript/tutorial>

If you already have a Google API Map Key, type the key to establish a connection with Google Maps.

4. Select **Apply this setting to all users** to apply the configuration settings to all users in the network deployment.

5. Click **OK**.

Parent topic: [Using the Health Dashboard Map](#)



Corporate Headquarters

CommScope • Hickory • North Carolina • 28602 • USA

T: 1-828-324-2200

www.commscope.com