

# RUCKUS SmartZone 7.0.0 (ST-GA) Monitoring Guide (SZ300/vSZ-H)

## Supporting SmartZone 7.0.0

© 2024 CommScope, Inc. All rights reserved.

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

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

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

## Patent Marking Notice

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

# Contents

---

<b>Contact Information, Resources, and Conventions.....</b>	<b>5</b>
Contacting RUCKUS Customer Services and Support.....	5
What Support Do I Need?.....	5
Open a Case.....	5
Self-Service Resources.....	6
Document Feedback.....	6
RUCKUS Product Documentation Resources.....	6
Online Training Resources.....	6
Document Conventions.....	7
Notes, Cautions, and Safety Warnings.....	7
Command Syntax Conventions.....	7
<b>About This Document.....</b>	<b>9</b>
New in This Document.....	9
<b>Application Monitoring.....</b>	<b>11</b>
SmartZone Web Interface.....	11
Controller Web Interface Features.....	11
<b>Diagnostics.....</b>	<b>15</b>
Support Bundle.....	15
Scripts.....	17
Applying Scripts.....	17
Uploading AP CLI Scripts.....	17
Executing AP CLI Scripts.....	18
Scheduling AP CLI Scripts.....	19
Viewing Scripts.....	20
Viewing the Script Execution Summary.....	21
Application Logs.....	22
Application Logs.....	22
RADIUS Proxy.....	24
Viewing RADIUS Proxy Settings.....	24
<b>Reports.....</b>	<b>27</b>
Creating Reports.....	27
Generating Reports.....	29
<b>Chatbot.....</b>	<b>31</b>
Logging in to Chatbot.....	31
<b>Third Party Service.....</b>	<b>35</b>
Enabling Ekahau and Aer Scout/Stanley RTLS Tags.....	35



# Contact Information, Resources, and Conventions

---

- [Contacting RUCKUS Customer Services and Support](#)..... 5
- [Document Feedback](#)..... 6
- [RUCKUS Product Documentation Resources](#)..... 6
- [Online Training Resources](#)..... 6
- [Document Conventions](#)..... 7
- [Command Syntax Conventions](#)..... 7

## Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

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

### What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

### Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

## Self-Service Resources

The RUCKUS Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://community.ruckuswireless.com>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—[https://support.ruckuswireless.com/#products\\_grid](https://support.ruckuswireless.com/#products_grid)
- Security Bulletins—<https://support.ruckuswireless.com/security>

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

## Document Feedback

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

You can email your comments to RUCKUS at [#Ruckus-Docs@commscope.com](mailto:#Ruckus-Docs@commscope.com).

When contacting us, include the following information:

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

For example:

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

## RUCKUS Product Documentation Resources

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

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

White papers, data sheets, and other product documentation are available at <https://www.ruckusnetworks.com>.

## Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://commscopeuniversity.myabsorb.com/>. The registration is a two-step process described in this [video](#). You create a CommScope account and then register for, and request access for, CommScope University.

# Document Conventions

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

**TABLE 1** Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<code>device(config)# interface ethernet 1/1/6</code>
<b>bold</b>	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information.

## Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

### NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

### ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



### CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



### DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

## Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.  Default responses to system prompts are enclosed in square brackets.
{x  y  z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.





# About This Document

---

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

## New in This Document

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

Feature	Description	Reference
Removal of Legacy UI menu toggle	<b>Removed:</b> The support for this feature is removed.	<a href="#">Chatbot</a> on page 31



# Application Monitoring

- SmartZone Web Interface..... 11

## SmartZone Web Interface

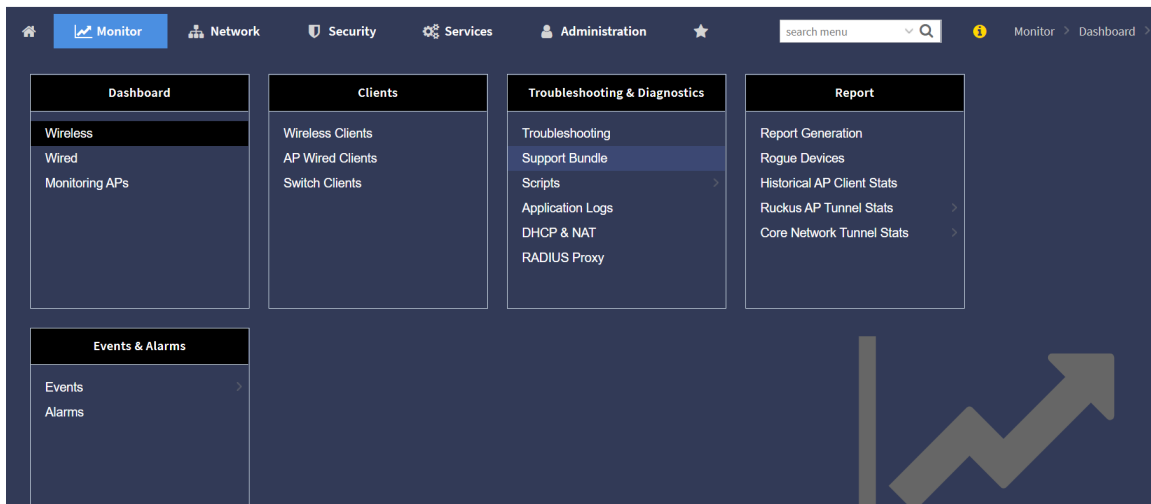
### Controller Web Interface Features

The controller web interface is the primary graphical front end for the controller and is the primary interface.

You can use the controller web interface to take the following actions:

- Manage access points and WLANs
- Create and manage users and roles
- Monitor wireless clients, managed devices, and rogue access points
- View alarms, events, and administrator activity
- Generate reports
- Perform administrative tasks, including backup and restoring system configuration, upgrading the cluster, downloading support, performing system diagnostic tests, viewing the status of controller processes, uploading additional license, and other administrative tasks

FIGURE 1 Controller Web Interface Components



The following table describes the controller web interface components.

TABLE 3 Controller Web Interface Components

Component	Description	Action
Main Menu	Lists the menus for administrative tasks.	Select the required menu and submenu.
Tab Page	Displays the options specific to the selected menu.	Select the required tab page.

**TABLE 3** Controller Web Interface Components (continued)

Component	Description	Action
Content Area	Displays tables, forms, and information specific to the selected menu and tab page.	View the tables, forms, and information specific to the selected menu, submenu, and tab page. Double-click an object or profile in a table, for example, a WLAN, to edit the settings.
Header Bar	Displays information specific to the controller web interface.	Select the required option (from left to right): <ul style="list-style-type: none"> <li>● Warning: Lists the critical issues to be resolved.</li> <li>● System Date and Time: Displays the current system date and time.</li> <li>● Refresh: Refreshes the web page.</li> <li>● Global filter: Allows you to set the preferred system filter.</li> <li>● My Account link: Allows you to: <ul style="list-style-type: none"> <li>- Change password</li> <li>- Set session preference</li> <li>- View account activities such as login information and privilege changes</li> <li>- Log off</li> </ul> </li> <li>● Online Help: Allows access to web help.</li> </ul>

You can use the **Menu** icon to expand and shrink the **Main menu**. Shrinking the main menu increases the size of the content area for better readability and viewing.

### 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.



# Diagnostics

- Support Bundle..... 15
- Scripts..... 17
- Application Logs..... 22
- RADIUS Proxy..... 24

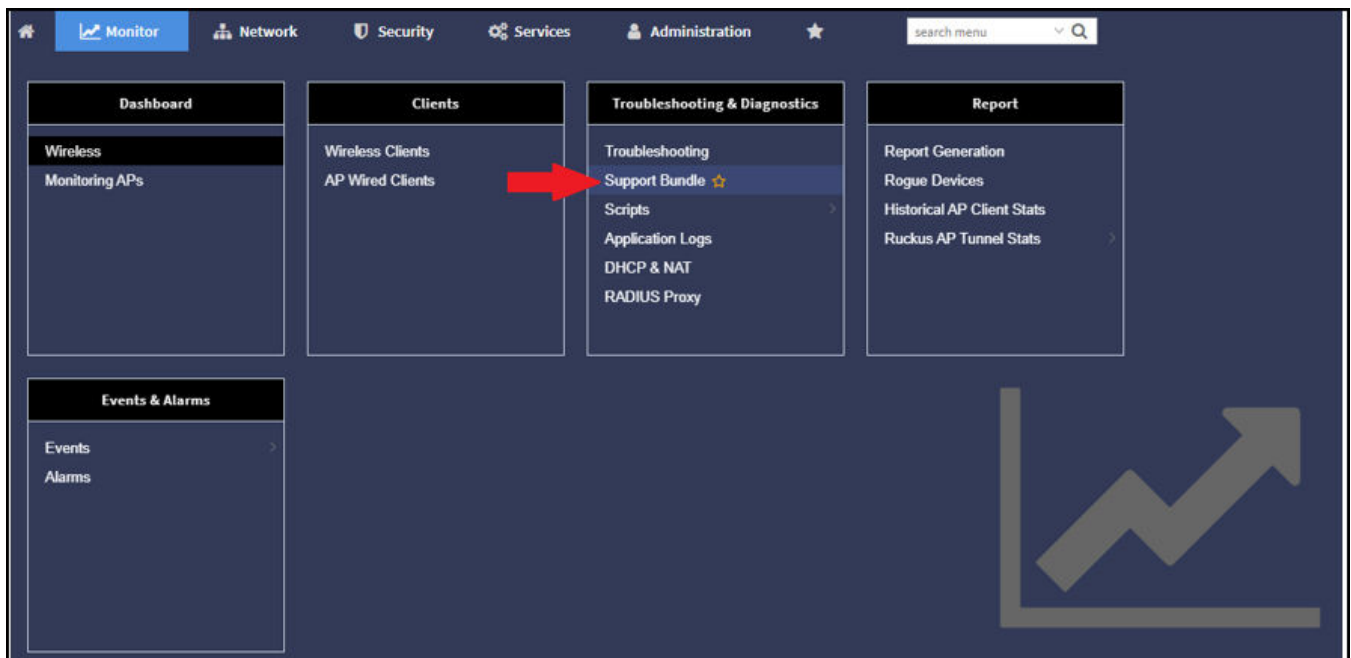
## Support Bundle

Support Bundle allows you to gather the bundle log files from the controller and APs.

Complete the following steps to enable Support Bundle.

1. From the controller web interface, go to **Monitor > Troubleshooting & Diagnostics > Support Bundle**.  
The **Support Bundle** dialog box is displayed.

**FIGURE 2** Accessing the Support Bundle



2. Configure the following options:

FIGURE 3 Support Bundle Dialog Box

- **Category:** Select the type of support bundle from the list.
- **WLAN:** Select the WLAN on which the log collection will be performed from the list.
- **Targeted AP(s):** Select the APs from the list. The list contains the APs that have served the selected WLAN and are limited to the same zone.

**NOTE**

Any APs with a firmware version earlier than SmartZone 6.1 are disabled. A maximum of three APs can be displayed for the selected WLAN.

- The disconnected APs cannot be selected by the user.
- When the support bundle process is running, user cannot change the **Application Log**.

- **Duration:** Enter the time period for log selection (in seconds). The minimum value is 10 seconds, and the maximum value is 300 seconds.
- **Logs Selection:** Set **SZ Key Application Logs** or **SZ Snapshot Logs** to **ON**, this allows the application to collect different types of logs. If you use **SZ Key Application Logs**, a message is displayed to indicate that the application log level changes and this affect the application performance.
- **AP Packet Capture:** Set **AP Packet Capture** to **ON**, and complete the following options:
  - **Capture Interface:** Select **2.4 GHz** or **5 GHz** for the wireless interface.
  - **Client MAC Address Filter:** Enter the MAC address.
  - **Frame Type Filter:** Set the required options (**Management**, **Control**, and **Data**) to **ON**.

3. Click **OK**.



- To download Support Bundle output files, click **File Ready** in the **Key Application Logs** or **AP Support Bundle** columns.

FIGURE 4 Support Bundle Download Options

WLAN	Duration (Seconds)	AP Packet Capture	Start Time	End Time	Key Application Status	Key Application Logs	AP Status	AP Support Bundle	Snapshot Status	Snapshot Logs
TDC-5F-1	300	True	2020/12/15 01:59:10	N/A	Collecting		Collecting		Collecting	
TDC-5F-1	100	True	2020/11/06 20:10:10	2020/11/06 20:11:50	Not Enabled		Send command failed		Terminated	
TDC-5F-1	100	False	2020/11/06 20:30:00	2020/11/06 20:31:40	Completed	<b>File Ready (322MB)</b>	Partial completed	<b>File Ready (50MB)</b>	Completed	<b>File Ready (655MB)</b>

WLAN	Targeted AP(s)	AP Packet Capture	Capture Interface	Mac Address Filter
TDC-5F-1	AP1@AA:BB:CC:DD:EE:FF : Completed AP2@AA:BB:CC:DD:EE:F1 : Completed AP3@AA:BB:CC:DD:EE:F2 : Send Command Failed	False	N/A	N/A

## Scripts

New AP models and firmware updates are supported without the need to upgrade the controller image by using AP patch files and diagnostic scripts.

### Applying Scripts

Complete the following steps to apply scripts.

- From the main menu, click **Monitor**.
- Under **Troubleshooting & Diagnostics**, hover over the **Scripts**, and click **Patch/Diagnostic Scripts**.
- Select the **Upload to current node** check box.
- Click **Browse** to select a script that you want to upload to the controller.
- Click **Upload**.

The script is listed in the **System Uploaded Scripts** area.

If you have uploaded a patch script, it is displayed in the **System Uploaded Patch Scripts** area with the following information:

- Name of the patch file
- Patch file description
- Supported AP firmware version
- AP model number

You can click **Delete** to delete scripts.

- Click **Apply Patch** to apply the patch file to the AP model or firmware as appropriate.

### Uploading AP CLI Scripts

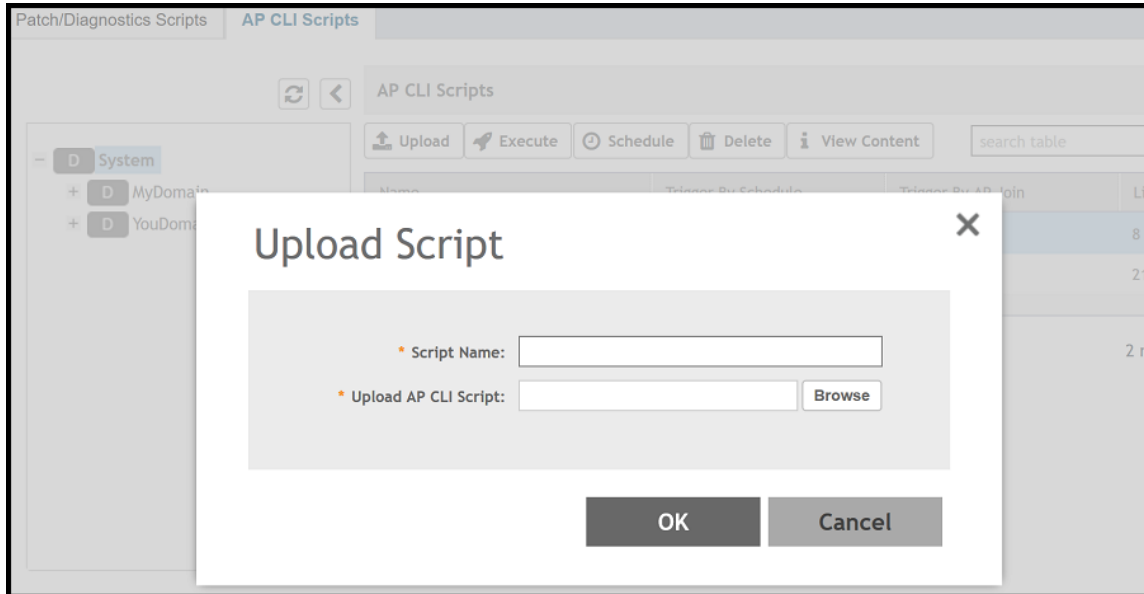
You can upload AP CLI scripts to the controller to make the controller compatible with new AP models and new firmware without the need to upgrade the controller image.

- From the main menu, click **Monitor**.
- Under **Troubleshooting & Diagnostics**, hover over the **Scripts**, and click **Patch/Diagnostic Scripts**.

3. Select the **AP CLI Scripts** tab.
4. From the domain tree, select the AP zone to apply the script.
5. Click **Upload**.

The **Upload Script** dialog box is displayed.

**FIGURE 5** Uploading Scripts



6. For **Script Name**, enter the name of the script you want to upload.
7. For **Upload AP CLI Script**, click **Browse** to select an AP CLI script that you want to upload.
8. Click **OK** to apply the AP CLI script file to the AP zone.

## Executing AP CLI Scripts

You can upload AP CLI scripts to be run on APs within selected zones and execute them immediately or on demand.

1. From the main menu, click **Monitor**.
2. Under **Troubleshooting & Diagnostics**, hover over the **Scripts**, and click **Patch/Diagnostic Scripts**.
3. Select the **AP CLI Scripts** tab.
4. From the domain tree, select the domain in which the AP is present.
5. From the **AP CLI Scripts** tab, select the script from the list of scripts.

6. Click **Execute**.  
The **Execute Script** dialog box is displayed.

**FIGURE 6** Executing a Script



7. Select one or more zones from the domain tree.
8. Click **OK** to run the AP CLI script on the AP zone.

The controller runs the selected script on the specified zone.

## Scheduling AP CLI Scripts

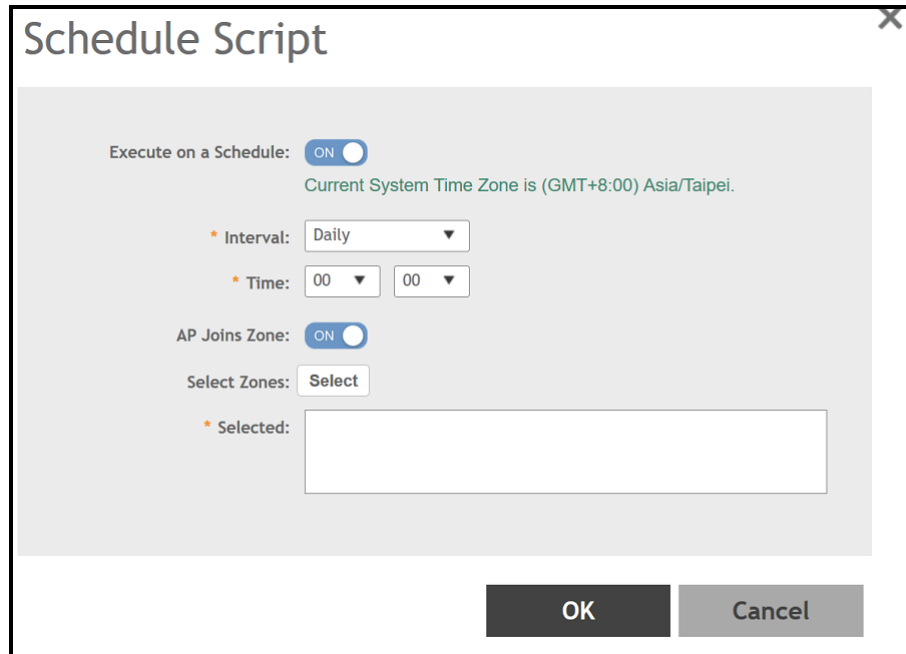
You can upload AP CLI scripts to be run on APs within selected zones. You can also schedule the script to be run on the APs at a particular time or when the AP joins the zone.

1. From the main menu, click **Monitor**.
2. Under **Troubleshooting & Diagnostics**, hover over the **Scripts**, and click **Patch/Diagnostic Scripts**.
3. Select the **AP CLI Scripts** tab.
4. From the domain tree, choose the domain in which the AP is present.

- From the **AP CLI Scripts** tab, select the script from the list of scripts.
- Click **Schedule**.

The **Schedule Script** dialog box is displayed.

**FIGURE 7** Scheduling a Script



- Configure the following options:
  - Execute on a Schedule:** Enable this option to execute the script based on the current system time.
  - Interval:** Schedule the script execution in multiple events. Options are Daily, Weekly and Monthly.
  - Time:** Select the time from the drop-down menu to execute the script.
  - AP Joins Zone:** By default this option is disabled. Enable this option to make sure the script runs on the AP when it joins a particular zone.
- To select the zone, click **Select**.  
This displays the **Select Zone** page . Identify and select the zone. The selected zone is populated in the **Selected** area.
- Click **OK**.

The schedule is configured and the script will run on the AP as planned.

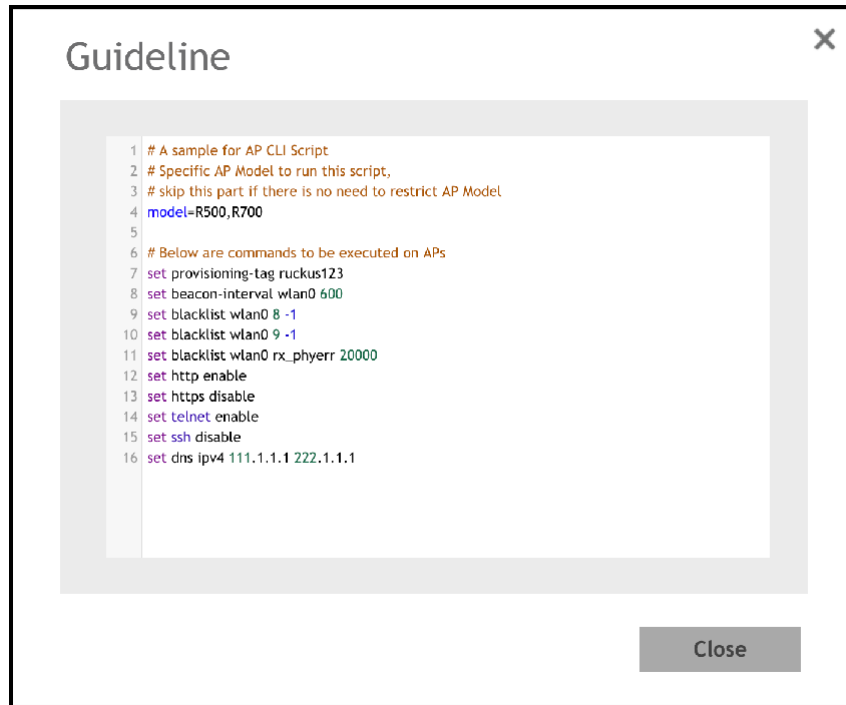
## Viewing Scripts

You can open the AP CLI script and view the script details.

- From the main menu, click **Monitor**.
- Under **Troubleshooting & Diagnostics**, hover over the **Scripts**, and click **Patch/Diagnostic Scripts**.
- Select the **AP CLI Scripts** tab.
- From the domain tree, choose the domain in which the AP is present.

5. From the **AP CLI Scripts** tab, select the script from the list of scripts.
6. Click **View Content**.  
The **Guideline** dialog box is displayed.

**FIGURE 8** Viewing Script Details



7. Click **Close**.

## Viewing the Script Execution Summary

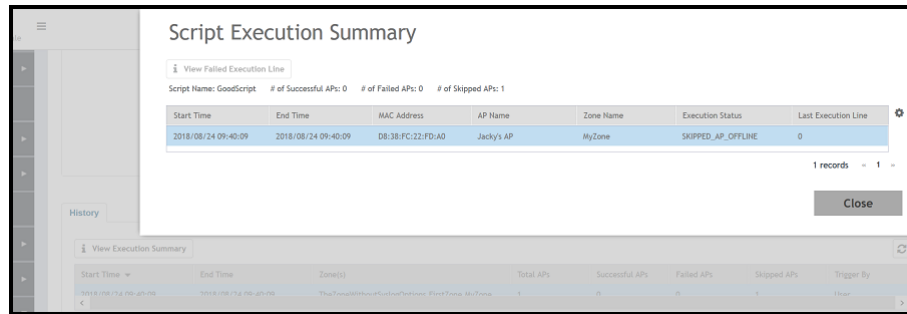
After an AP CLI script is executed on-demand or as scheduled, you can view the details in the **History** tab.

1. From the main menu, click **Monitor**.
2. Under **Troubleshooting & Diagnostics**, hover over the **Scripts**, and click **Patch/Diagnostic Scripts**.
3. Select the **AP CLI Scripts** tab.
4. From the domain tree, choose the domain in which the AP is present.  
The **History** tab displays the list of scripts that were executed.
5. From the **AP CLI Scripts** tab, select the script from the list of scripts.

6. Select a script from the **History** tab, and click **View Execution Summary**.

The **Script Execution Summary** displays the script name, the number of successful, failed, and skipped APs, the start and end times of the execution process, the MAC address of the AP, the AP and zone names, the execution status, and the last execution line.

**FIGURE 9** Script Execution Summary



7. Click **Close**.

## Application Logs

### Application Logs

The controller generates logs for all the applications that are running on the server.

#### Viewing and Downloading Logs

Complete the following steps to view and download logs.

1. From the main menu, click **Monitor**.
2. Under **Troubleshooting & Diagnostics**, click **Application Logs**.  
The **Application Logs** screen is displayed.
3. Select a control plane from the **Select Control Plane** dropdown list to view and download logs.
4. Select the **Log Type** and click **Download**. You can download the logs using the following options.

**TABLE 4** Download Options

Options	Description
<b>Download Logs</b>	Downloads all logs for the selected application.
<b>Download All Logs</b>	Downloads all available logs from the controller. In your web browser's default download location, verify that the TGZ file was downloaded successfully. You must use your preferred compression/decompression program to extract the log files from the TGZ file. When the log files are extracted (for example, adminweb.log, cassandra.log, communicator.log, and so on), use a text editor to open and view the log contents.

**TABLE 4** Download Options (continued)

Options	Description
<b>Download Snapshot Logs</b>	Downloads snapshot logs that contain system and configuration information, such as the AP list, configurations settings, event list, communicator logs, SSH tunnel lists, and so on. If you triggered the controller to generate a snapshot from the CLI, you have the option to download snapshot logs from the web interface. In your web browser's default download folder, verify that the snapshot log file or files have been downloaded successfully. Extract the contents of the .tar file.

## System Logs

The controller generates logs for all the applications that are running on the server.

The following table lists the controller applications that are running.

**TABLE 5** Controller Applications and Log Types for SZ300 and vSZ-H controller platforms

Application	Description
Cassandra	The controller database server that stores most of the run-time information and statistical data
Communicator	Communicates with access points and retrieves statuses, statistics, and configuration updates
Configurer	Performs configuration synchronization and cluster operations (for example, join, remove, upgrade, backup, and restore)
Diagnostics	An interface that can be used to upload RUCKUS scripts (.ksp files) for troubleshooting or applying software patches. This interface displays the diagnostic scripts and system patch scripts that are uploaded to a node.
EventReader	Receives event messages from access points and saves the information to the database
LogMgr	Organizes the application logs into a common format, segregates them, and copies them into the respective application log files
MdProxy	MdProxy on AP and controller connect to AP-MD and controller-MD respectively. MdProxy on controller receives messages and retrieves the message header. It also forwards the response to controller-MD. This message is sent to MdProxy on AP through AP-MD. MdProxy on AP removes the MSL header and responds to the connection on which the request was received.
MemCached	The controller memory cache that stores client authentication information for fast authentication or roaming
MemProxy	Replicates MemCached entries to other cluster nodes
Mosquitto	A lightweight method used to carry out messaging between LBS and APs
MsgDist	The message distributor (MD) maintains a list of communication points for both local applications and remote MDs to perform local and remote routing.
NginX	A web server that is used as a reserve proxy server or an HTTP cache
Northbound	As an interface between SP and AAA, performs UE authentication and handles approval or denial of UEs to APs
RadiusProxy	Sets the RADIUS dispatch rules and synchronizes configuration to each cluster node
Scheduler	Performs task scheduling and aggregates statistical data
SNMP	Provides a framework for the monitoring devices on a network. The SNMP manager is used to control and monitor the activities of network hosts using SNMP. As an agent that responds to queries from the SNMP Manager, SNMP Traps with relevant details are sent to the SNMP Manager when configured.

**TABLE 5** Controller Applications and Log Types for SZ300 and vSZ-H controller platforms (continued)

Application	Description
SubscriberManagement	Maintains local user credentials for WISPr authentication
SubscriberPortal	Internal portal page for WISPr (hotspot)
System	Collects and sends log information from all processes
Web	Runs the controller management web server

**TABLE 6** Controller Applications and Log Types for SZ100 and vSZ-E controller platforms

Application	Description
API	The application program interface (API) provides an interface for customers to configure and monitor the system
CaptivePortal	Performs portal redirect for clients and manages the walled garden and blacklist
Cassandra	The controller database server that stores most of the run-time information and statistical data
Configurer	Performs configuration synchronization and cluster operations (for example, join, remove, upgrade, backup, and restore)
Diagnosics	An interface that customers can use to upload RUCKUS scripts for performing troubleshooting or applying software patches
ElasticSearch	Scalable real-time search engine used in the controller
MemCached	The controller memory cache that stores client authentication information for fast authentication or roaming
MemProxy	Replicates MemCached entries to other cluster nodes
Mosquitto	A lightweight method used to carry out messaging between LBS and APs
Northbound	Performs UE authentication and handles approval or denial of UEs to APs
RadiusProxy	Sets the RADIUS dispatch rules and synchronizes configuration to each cluster node
SNMP	Provides a framework for the monitoring devices on a network. The SNMP manager is used to control and monitor the activities of network hosts using SNMP.
SubscriberManagement	A process for maintaining local user credentials for WISPr authentication
SubscriberPortal	Internal portal page for WISPr (hotspot)
System	Collects and sends log information from all processes
Web	Runs the controller management web server

## RADIUS Proxy

### Viewing RADIUS Proxy Settings

You must be aware of the RADIUS Proxy settings on the controller to monitor the health of the controller.

Go to **Monitor > Troubleshooting and Diagnostics > RADIUS Proxy**. The **Proxy** page appears displaying the RADIUS settings.



FIGURE 10 Diagnostics - RADIUS Proxy

The screenshot shows the 'RADIUS Proxy' diagnostics page. The top navigation bar includes 'Monitor', 'Network', 'Security', 'Services', and 'Administration'. Below the navigation, the 'Proxy' section is active. A table displays the following data:

MVNO Account	Control Plane	AAA IP	Created On	Last Modified On	NAS Type	Auth	Accounting	ACCESS Request	ACCESS Challenge	ACCESS Accept
Super	00:0C:29:F...	192.168.92...	2022/08/24 12:58:30	2022/08/26 10:45:16	Ruckus AP	7/4/0	0/0	20/20	0/0	7/7

At the bottom right of the table, it indicates '1 records'.



# Reports

- [Creating Reports.....](#) 27
- [Generating Reports.....](#) 29

## Creating Reports

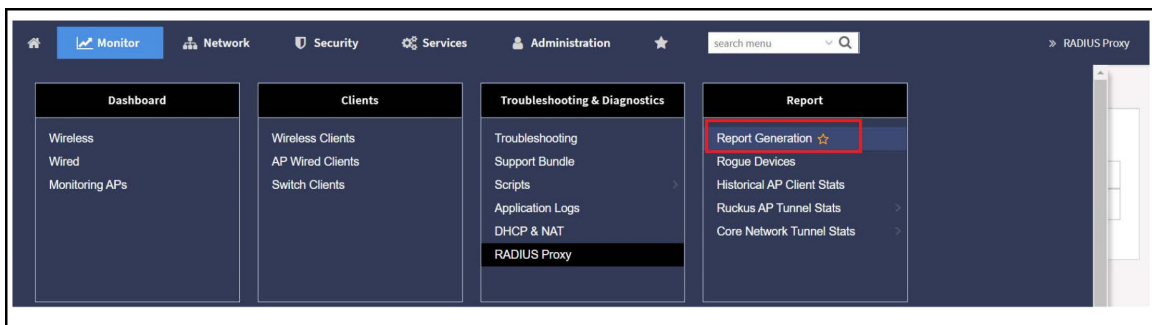
You can create reports to obtain a historical view of the maximum and minimum number of clients connected to the system, the number of clients connected at different time intervals, and the traffic statistics for the switches.

Complete the following steps to create a new report.

1. From the main menu, go to **Monitor>Report >Report Generation**.

The **Report Generation** page is displayed.

**FIGURE 11** Report Generation Screen



2. Click **Create**. The **Create Report** dialog box is displayed.

FIGURE 12 Create Report Dialog Box

3. Enter the required parameters as described in the following table.

TABLE 7 Report Parameters

Field	Description	Your Action
<b>General Information</b>		
<b>Title</b>	Indicates the report name.	Enter a title for the report.
<b>Description</b>	Describes the report type.	Enter a short description.
<b>Report Category</b>	Provides an option to generate reports for system or switch devices in the network.	Select <b>System</b> or <b>Switch</b> as appropriate.
<b>Report Type</b>	Specifies the report type.	Select the required report type.
<b>Output Format</b>	Specifies the report output format.	Select the required report output format.
<b>Resource Filter Criteria</b>		
<b>Device</b>	Indicates the level of resource filtering for which you want to generate the report; for example, Management Domains, AP Zone or Access Point (if you select the System option), and Switch.	Enter the device or switch name or select the device or switch from the list and select the option.
<b>SSID</b>	Indicates the SSID for which you want to generate the report.	Select the check box and select the SSID for which you want the report. You can select <b>All SSIDs</b> to generate reports for all the SSIDs available. This option is convenient because you do not have to update the resource filter criteria periodically.
<b>Radio</b>	Indicates the frequency for which you want to generate the report.	Select the check box and select the required frequency: <ul style="list-style-type: none"> <li>• <b>2.4G</b></li> <li>• <b>5G</b></li> <li>• <b>6GHz/5GHz</b></li> </ul>
<b>Time Filter</b>		
<b>Time Interval</b>	Defines the time interval at which to generate the report.	Select the required time interval.

**TABLE 7** Report Parameters (continued)

Field	Description	Your Action
<b>Time Filter</b>	Defines the time duration for which to generate the report.	Select the required time filter.
<b>Schedules</b>		
<b>Enable/Disable</b>	Specifies the scheduled time when a report must be generated. By default, the current system time zone is also displayed.	By default, this option is disabled. Select <b>Enable</b> and <b>Interval, Hour, and Minute</b> . You can add multiple schedules. You can also click <b>Add New</b> to include more schedules.
<b>Email Notification</b>		
<b>Enable/Disable</b>	Triggers an email notification when the report is generated.	By default, this option is disabled. Select <b>Enable</b> , click <b>Add New</b> , and enter the email address. You can add multiple email addresses.
<b>Export Report Results</b>		
<b>Enable/Disable</b>	Automatically uploads the reports to an FTP server.	By default, this option is disabled. Select <b>Enable</b> , and select the FTP server from the drop-down list and click <b>Test</b> .

4. Click **OK**.

**NOTE**

You can also edit or delete a report by selecting the **Configure** or **Delete** options.

## Generating Reports

Complete the following steps to generate a report.

1. From the main menu, go to **Monitor > Report > Report Generation**.  
The **Report Generation** page is displayed.
2. Select the required report from the list, and click **Generate**. The **Report Generated** form is displayed.
3. Click **OK**. The report is generated and listed in the **Report Results** pane.
4. From the **Result Links** column, select the required format, and click **Open** to view the report.



# Chatbot

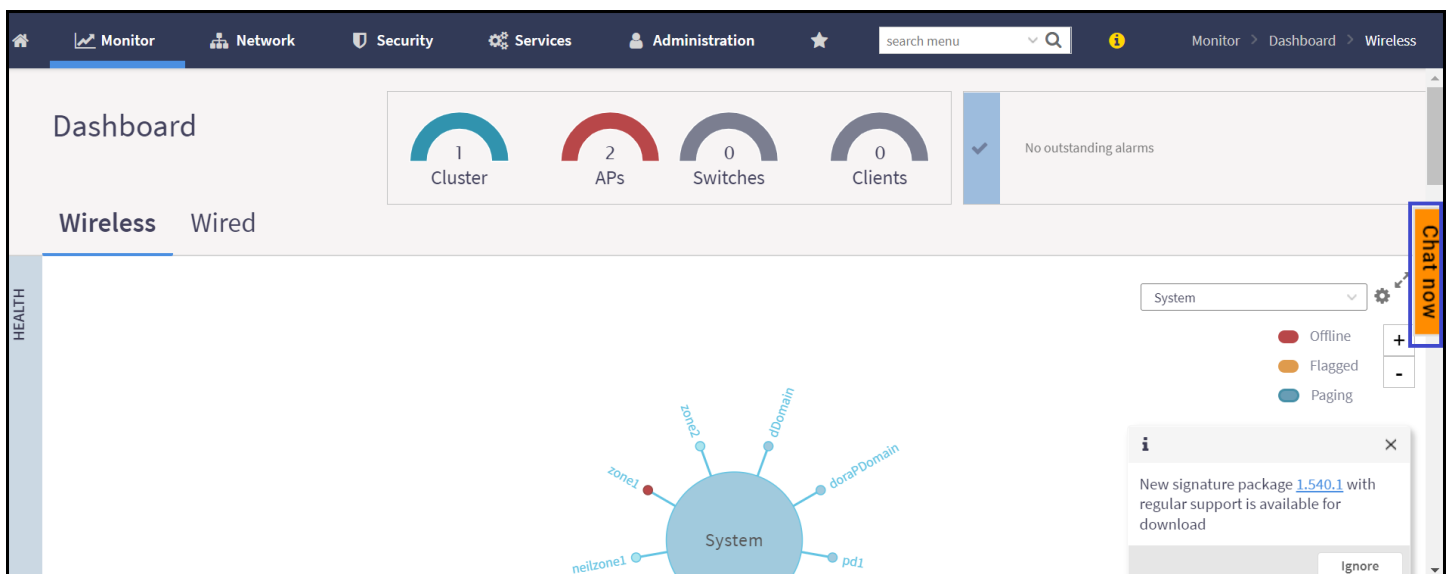
The key task of the Chatbot is to help users by providing answers to their queries. The Chatbot communicates in human like conversation with users through text messages on the chat.

The Chatbot is available in the home page of the controller application.

## NOTE

The Chatbot feature in SmartZone is available only for an account with an **Administrator** permission.

FIGURE 13 Chatbot Menu



The Chatbot helps to create a support ticket in case of any issues with the application.

Any user with a **RUCKUS** account has complete access to the Chatbot. However, a user without a **RUCKUS** account has limited access and can access only the knowledge base.

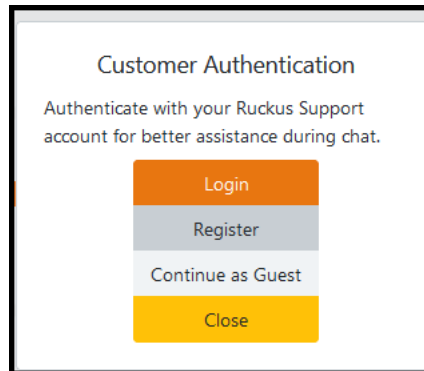
## Logging in to Chatbot

To access the Chatbot, a user must log in to the **RUCKUS** Support account and authenticate the credentials.

## Chatbot

Logging in to Chatbot

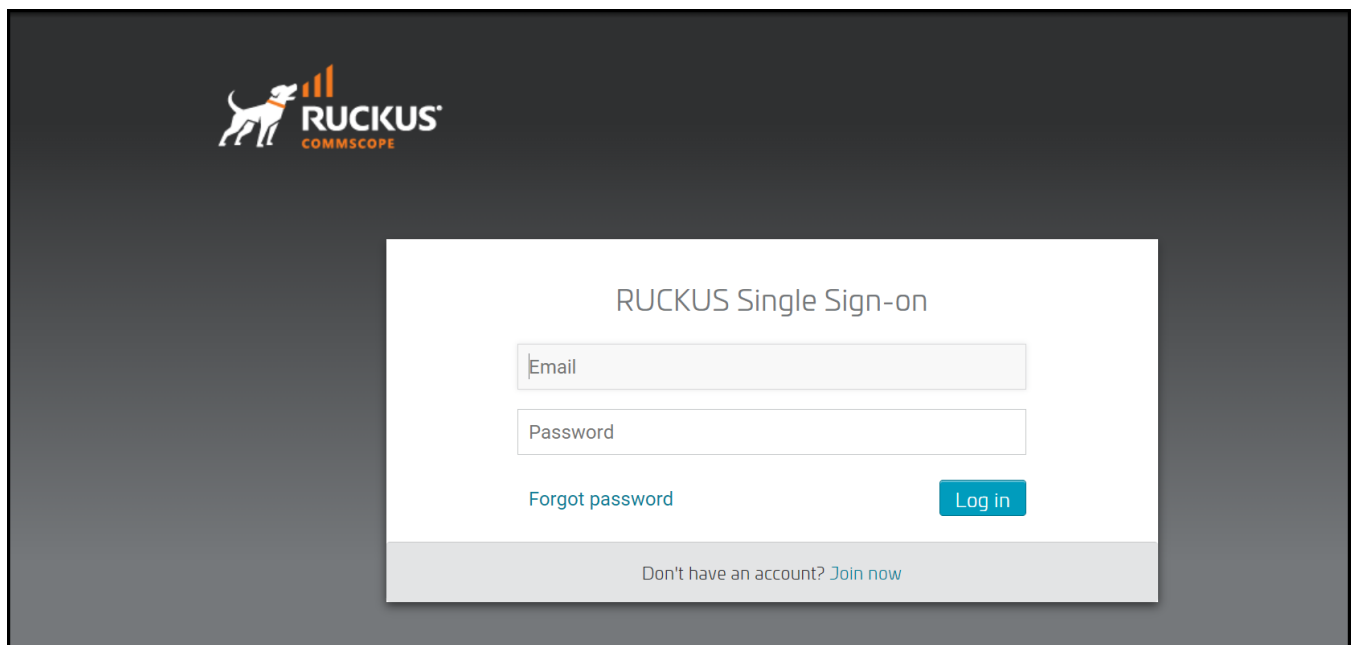
**FIGURE 14** Customer Authentication



Login by RUCKUS account

1. Click **Login**. This displays the RUCKUS authentication page.

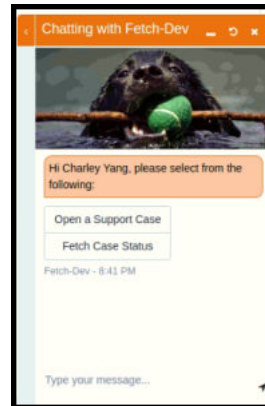
**FIGURE 15** RUCKUS Authentication Screen





2. After authentication, a user can create or track a Support ticket. The Chatbot sends the data with the **RUCKUS** account authorization information.

**FIGURE 16** Chatbot Menu



3. To create a new support ticket, click **Open a Support Case** and provide the following information:
  - a. Serial Number
  - b. Product Information
  - c. Description of the Issue (limited to 255 words)

## Chatbot

### Logging in to Chatbot

- To track a Support ticket, click **Fetch Case Status** and provide the case number.

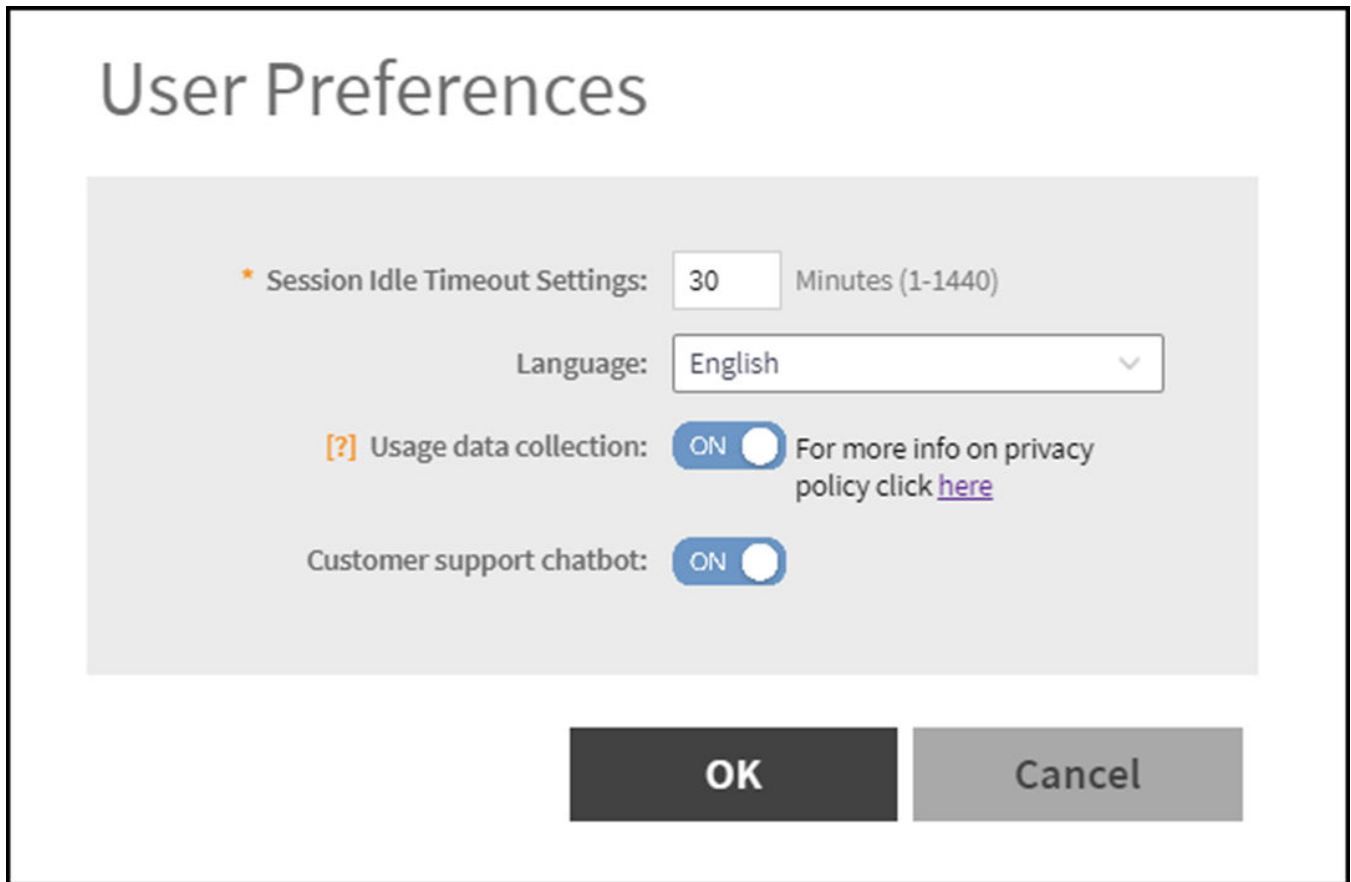
#### NOTE

User can access Chatbot as a **Guest** but cannot create any ticket.

#### NOTE

A user can disable the Chatbot feature in the **Admin > User Preferences** screen by clicking the **Customer support chatbot** toggle switch to **OFF** and then click **OK**.

**FIGURE 17** Enable/Disable Chatbot



The screenshot displays the 'User Preferences' dialog box. It features a title bar at the top with the text 'User Preferences'. Below the title bar, there are four settings:

- Session Idle Timeout Settings:** A text input field containing '30' followed by the text 'Minutes (1-1440)'.
- Language:** A dropdown menu currently showing 'English' with a downward arrow.
- Usage data collection:** A toggle switch labeled 'ON' with a blue circle to its right. To the right of the toggle is the text 'For more info on privacy policy click [here](#)'.
- Customer support chatbot:** A toggle switch labeled 'ON' with a blue circle to its right.

At the bottom of the dialog box, there are two buttons: a dark grey 'OK' button and a light grey 'Cancel' button.

# Third Party Service

- [Enabling Ekahau and Aeroscout/Stanley RTLS Tags.....](#) 35

SmartZone controller supports integration for Ekahau and Aeroscout/Stanley tags, and information is forwarded to the Ekahau and Aeroscout servers. This enhancement provides support for Real-Time Location Service (RTLS) tags without requiring them to be associated to the network.

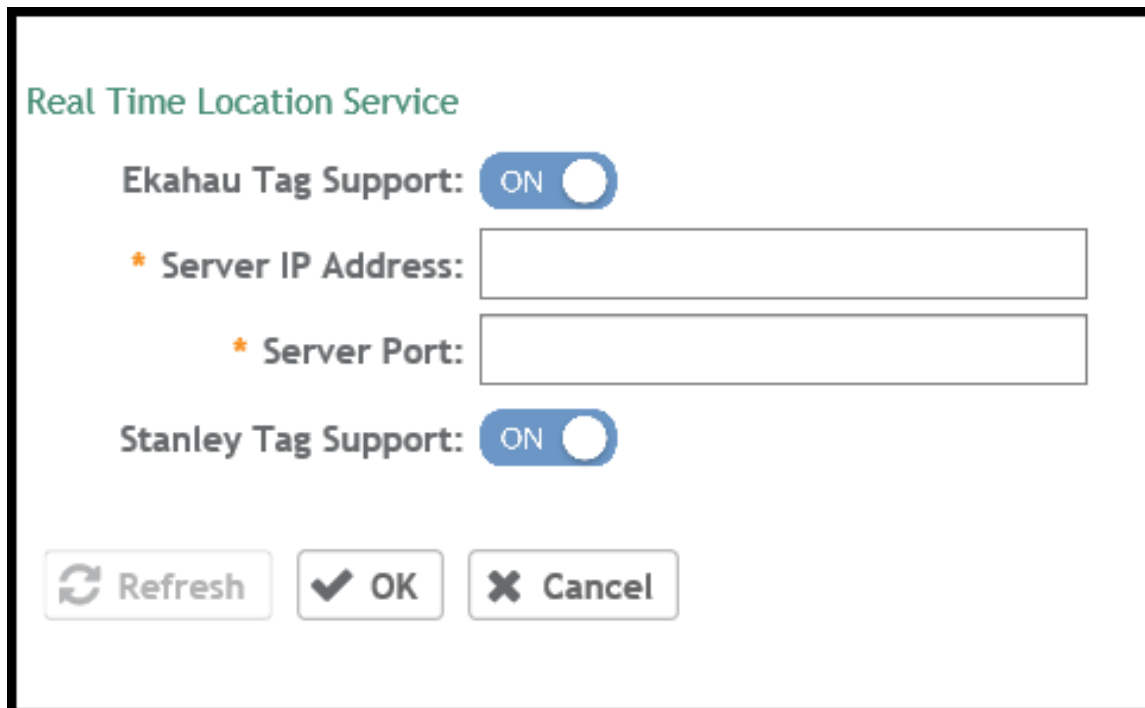
## Enabling Ekahau and Aeroscout/Stanley RTLS Tags

To locate tag positions, SmartZone allows you to enable Ekahau and Aeroscout/Stanley RTLS tags.

1. Select **Services > Others > 3rd Party Service > RTLS**.

The **RTLS** page is displayed.

**FIGURE 18** Enabling Ekahau and Aeroscout/Stanley Tag Support



2. Select a zone to enable the tags.
3. To enable **Ekahau Tag Support**, set **Ekahau Tag Support** to **ON**.
4. In the **Server IP Address** field, enter the IP address of the server to which data is forwarded.
5. In the **Server Port** field, enter the server port to which data is forwarded.
6. To enable **Stanley Tag Support**, set **Stanley Tag Support** to **ON**.
7. Click **OK**.



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