

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

**Supporting SmartZone 7.0.0**

© 2024 CommScope, Inc. All rights reserved.

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

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

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

## Patent Marking Notice

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

# Contents

---

<b>Contact Information, Resources, and Conventions.....</b>	<b>5</b>
Contacting RUCKUS Customer Services and Support.....	5
What Support Do I Need?.....	5
Open a Case.....	5
Self-Service Resources.....	6
Document Feedback.....	6
RUCKUS Product Documentation Resources.....	6
Online Training Resources.....	6
Document Conventions.....	7
Notes, Cautions, and Safety Warnings.....	7
Command Syntax Conventions.....	7
<b>About This Guide.....</b>	<b>9</b>
New in This Document.....	9
<b>Wired.....</b>	<b>11</b>
Wired Clients.....	11
Deauthorizing a Wired Client.....	11
Viewing a Summary of Wired Clients.....	11
<b>Wireless.....</b>	<b>13</b>
Wireless Clients.....	13
Traffic Analysis.....	13
Deauthorizing a Wireless Client.....	15
Blocking a Wireless Client.....	15
Unblocking a Wireless Client.....	15
Disconnecting a Wireless Client.....	16
Viewing a Summary of Wireless Clients.....	16
Viewing Wireless Client Information.....	17
<b>Switch Clients.....</b>	<b>19</b>
Switch Clients.....	19



# Contact Information, Resources, and Conventions

---

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

## Contacting RUCKUS Customer Services and Support

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

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

### What Support Do I Need?

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

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

### Open a Case

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

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

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

## Self-Service Resources

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

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

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

## Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

## RUCKUS Product Documentation Resources

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

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

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

## Online Training Resources

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

# Document Conventions

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

**TABLE 1** Text Conventions

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

## Notes, Cautions, and Safety Warnings

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

### NOTE

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

### ATTENTION

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



### CAUTION

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



### DANGER

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

## Command Syntax Conventions

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

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





# About This Guide

---

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

## New in This Document

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

Feature	Description	Reference
Minor Editorial Updates.	Through the Guide.	February 2024



# Wired

- [Wired Clients.....](#) 11
- [Viewing a Summary of Wired Clients.....](#) 11

## Wired Clients

Wired clients are client devices that are connected to the Ethernet ports of access points (APs) managed by the controllers and, thereby, are connected to the wired network services that your managed APs provide.

### Deauthorizing a Wired Client

You can force wired clients that joined the wired network through an authentication portal to reauthenticate themselves by deauthorizing them. Deauthorized wired clients remain connected to the wired network, but are redirected to the authentication portal whenever they attempt to access network resources.

To deauthorize a wired client, complete the following steps.

1. From the dashboard, go to **Monitor > Clients > AP Wired Clients**.

The **AP Wired Clients** tab is displayed.

2. Locate the client that you want to deauthorize.

If you have a large number of wired clients, and you know the MAC address of the client, enter the MAC address in the search field. Press **Enter** to search for the client.

3. Select the client and click the **Deauthorize** button.

The table refreshes, and the client that you deauthorized is removed from the list.

## Viewing a Summary of Wired Clients

You can view a summary of wired clients that are currently associated with all of your managed APs.

From the dashboard, go to **Monitor > Clients > AP Wired Clients**.

The **AP Wired Clients** tab displays a table that lists all clients currently associated with your managed APs.

#### NOTE

To view wired clients that belong to a specific zone, click the zone name in the zone tree. The table refreshes, displaying only the clients that belong to the zone you selected.

#### NOTE

For more information about how the 802.1X configuration works for the port refer to the "Creating an Ethernet Port Profile" section of the *RUCKUS SmartZone (LT-GA) Traffic Management Guide (SZ300/vSZ-H)*.

**TABLE 3** Wired Client Details

Column Name	Description
MAC Address	Displays the MAC address of the wired client
Username	Displays the name of the user logged in to the wired client

## Wired

Viewing a Summary of Wired Clients

**TABLE 3** Wired Client Details (continued)

Column Name	Description
IP Address	Displays the IP address assigned to the wired client
AP MAC	Displays the MAC address of the access point
AP Name	Displays the name assigned to the access point
LAN	Displays the LAN ID assigned to the wired client
VLAN	Displays the VLAN ID assigned to the wired client
Auth Status	Indicates whether the wired client is authorized to access the WLAN service

# Wireless

---

- [Wireless Clients.....](#) 13
- [Viewing a Summary of Wireless Clients.....](#) 16
- [Viewing Wireless Client Information.....](#) 17

## Wireless Clients

Wireless clients are client devices that are connected to the wireless network services that your managed APs provide. Wireless clients can include smart phones, tablets, and notebook computers equipped with wireless network adapters.

## Traffic Analysis

Traffic Analysis provides network traffic information for APs, WLANs and clients.

To view information of the network traffic, select a **Zone > WLAN** and click **Configure**. This displays **Edit WLAN Configuration** of the selected WLAN.

Scroll down to **Firewall Options** category and enable **Application Recognition and Control** toggle button to **On**.

Use below filters to view information of the selected WLAN and different applications connected.

- **Channel Range**
  - **Total**
  - **2.4GHz**
  - **5GHz**
- **Throughput**
  - **TX+RX**—Number of bytes sent and received
  - **TX**—Number of bytes sent
  - **RX**—Number of bytes received
- **Group**

The parameters are displayed as graphs and bar charts. When you hover over the graph you can view the date and time, median, likely range, min-max range of the parameters. To view specific information on the graph, click and drag the portion. The selected portion would zoom in. To restore to normal view, click the **Reset zoom** button.

## Configuring Traffic Analysis Display for Top Clients

Using traffic analysis you can measure the total volume of traffic sent or received by clients.

Using traffic analysis you can measure the total volume of traffic sent or received by clients. You must configure the **Client settings** to view the traffic analysis. You can view historical and real-time data of the clients. The chart displays:

- **Bytes**—Frequency and number of clients connected to the AP
- **OS Type**—Types of OS the associated clients are using
- **Application**—Throughput the applications use

To configure the client settings:

1. From the WLAN area, click settings



The Settings - Clients form displays.

2. In the **Show top** box, enter the number of clients for which the traffic must be analyzed. Range: 5 through 20.
3. Select the **Type** radio button for the type of display you want to view. The choices are **Chart** or **Table**.
4. Select the **WLAN** identification option to be displayed. The choices are **Name**, **MAC**, or **IP**.
5. Click **OK**.

### SmartCell Insight Report on Actual Traffic Rate for APs and Client

The controller reports the total traffic statistics at an interval of every three minutes or 15 minutes to SmartCell Insight (SCI).

For traffic rate calculation, SCI divides the total traffic by time. But, this is not sufficient to accurately calculate airtime efficiency, as APs may not be sending or receiving the traffic all the time in the 15 minute interval. In other words, the SCI reporting of *traffic rate* needs to be across two dimensions:

1. **Traffic Over Time:** This is the current metric, and effectively captures how much traffic was sent or received over a period of time. The goal of this metric is to capture traffic, so that network operators can identify how much the network is being used in a time period.
2. **Traffic Efficiency:** This is the new metric, and effectively captures how much airtime was required to send receive traffic over time. The goal of this metric is to capture traffic efficiency, so that network operators can identify network performance in a time period.

To accomplish the efficiency calculation, information about both traffic and airtime usage (Tx,Rx, and busy), are measured as counters in a reporting interval. For SCI to do this, the controller will send the following information to SCI at the AP level.

- **Total traffic** Uplink and downlink time
- **Total Tx Time:** How much time did the AP spend transmitting traffic
- **Total Rx Time:** How much time did the AP spend receiving traffic for the AP's basic service set identifier (BSSIDs)
- **Other Rx Time:** How much time did the AP spend receiving broadcast traffic and traffic for other BSSIDs

#### NOTE

The reason for this metric is to distinguish between AP traffic and environmental traffic, where environmental traffic does affect airtime availability, but is not incorporated into the traffic efficiency calculation.

- **Total Tx/Rx Time:** How much time did the AP spend receiving and sending traffic in total for its BSSIDs
- **Idle Time:** How much time did the AP spend idle

The controller will send the following information to SCI at the Client level.

- **Total traffic** Uplink and downlink time
- **Total Tx Time:** How much time did the client spend transmitting traffic
- **Total Rx Time:** How much time did the client spend receiving traffic for the AP's basic service set identifier (BSSIDs)
- **Total Tx/Rx Time:** How much time did the client spend receiving and sending traffic in total for its BSSIDs

## Deauthorizing a Wireless Client

You can force wireless clients that joined the wireless network through an authentication portal (for example, a hotspot, guest access, or web authentication portal) to reauthenticate themselves by deauthorizing them. Deauthorized wireless clients remain connected to the wireless network, but are redirected to the authentication portal whenever they attempt to access network resources.

To deauthorize a wireless client, complete the following steps.

1. From the dashboard, click **Monitor > Wireless Clients > Clients**  
The **Wireless Clients** tab is displayed.
2. Locate the client that you want to deauthorize.  
If you have a large number of wireless clients, and you know the MAC address of the client, enter the MAC address in the search field. Press **Enter** to search for the client.
3. Select the client and click the **Deauthorize** button.  
The table refreshes, and the client that you deauthorized is removed from the list.

## Blocking a Wireless Client

When a user associates a wireless client device with an AP that the controller is managing, the client device is recorded and tracked. If, for any reason, you need to block a client device from accessing the network, you can do so from the web interface.

You might consider blocking a wireless client device for the following reasons:

- Network abuse
- Violation of acceptable use policy
- Theft
- Security compromise

To block a wireless client from accessing the SmartZone network, complete the following steps.

1. From the dashboard, click **Monitor > Clients > Wireless Clients**.  
The **Wireless Clients** tab is displayed.
2. Locate the client that you want to block.  
If you have a large number of wireless clients, and you know the MAC address of the client, enter the MAC address in the search field. Press **Enter** to search for the client.
3. Select the client and click the **Block** button.

## Unblocking a Wireless Client

If you want to allow a previously-blocked client to access the SmartZone network, you can unblock their access.

To unblock a wireless client, complete the following steps.

1. From the dashboard, click **Security > Access Control > Blocked Client**.
2. From the list of blocked clients, locate the client that you want to unblock.  
If you have a large number of blocked clients, and you know the MAC address of the client, enter the MAC address in the search field. Press **Enter** to search for the client.
3. Select the client and click the **Delete** button.

## Wireless

Viewing a Summary of Wireless Clients

# Disconnecting a Wireless Client

Wireless clients can be temporarily disconnected from the wireless network through the web interface. For example, when troubleshooting problematic network connections, wireless clients may need to be manually disconnected as part of the troubleshooting process.

To disconnect a wireless client from the WLAN to which it is connected, complete the following steps.

1. From the dashboard, click **Monitor > Clients > Wireless Clients**.
2. Locate the client that you want to disconnect.

If you have a large number of wireless clients, and you know the MAC address of the client, enter the MAC address in the search field. Press **Enter** to search for the client.

3. Select the client and click the **Disconnect** button.

The table refreshes, and the client that you disconnected is removed from the list.

# Viewing a Summary of Wireless Clients

You can view a summary of wireless clients that are currently associated with all of your managed APs.

You can view a summary of wireless clients associated with all of your managed APs. From the dashboard, go to **Monitor > Clients > Wireless Clients**.

The **Wireless Clients** tab displays a table that lists all clients currently associated with your managed APs.


### NOTE

To view wireless clients that belong to a particular zone, click the zone name in the zone tree. The table refreshes, displaying only the clients that belong to the zone you selected.

The following table lists details for the wireless client.

### NOTE

Not all the columns listed in the following table are displayed by default. To display columns that are currently hidden, click the gear icon in the upper-right corner of the table, and select the check boxes for the columns that you want to display.

Click the  icon to export the data into a CSV file.

### NOTE

For 802.1X (WPA2, WPA3) and MAC-auth, WLAN Advanced Option has the Session Timeout configuration. If the Access-Accept of AAA does not include the session timeout, the Session Timeout configuration value is used as the default value. The range is from 120 to 864000 seconds (10 days.) The default value is 172800 seconds (2 days).

**TABLE 4** Wireless Client Details

Column Name	Description
Hostname	Displays the hostname of the wireless client
OS Type	Displays the operating system that the wireless client is using
IP Address	Displays the IP address assigned to the wireless client
MAC Address	Displays the MAC address of the wireless client
WLAN	Displays the name of the WLAN with which the client is associated
AP Name	Displays the name assigned to the access point
AP MAC	Displays the MAC address of the access point



**TABLE 4** Wireless Client Details (continued)

Column Name	Description
Traffic (Session)	Displays the total traffic (in KB, MB, GB, or TB) for this client in this session
Traffic (Uplink)	Displays the total uplink traffic (in KB, MB, GB, or TB) for this client in this session
Traffic (Downlink)	Displays the total downlink traffic (in KB, MB, GB, or TB) for this client in this session
RSSI	Displays the Received Signal Strength Indicator (RSSI), which indicates how well a wireless client can receive a signal from an AP. The RSSI value is shown in decibels (dB) and displayed as either the real-time value or the average value over the past 90 seconds.
SNR	Displays the Signal-to-Noise Ratio (SNR), which indicates the signal strength relative to background noise. The SNR value is shown in decibels (dB) and displayed as either the real-time value or the average value over the past 90 seconds.
Radio Type	Displays the type of wireless radio that the client supports. Possible values include 11b, 11g, 11g/n, 11a, 11a/g/n, 11ac, and 11ax.
VLAN	Displays the VLAN ID assigned to the wireless client
Channel	Displays the wireless channel (and channel width) that the wireless client is using
CPE MAC	Displays the WLAN MAC address of the customer premises equipment
User Name	Displays the name of the user logged in to the wireless client
MCS Rate (Tx) (Rx)	Displays the median Tx and Rx Modulation and Coding Scheme rates for both client and APs on their respective pages. These values are updated every 180 seconds (High Scale) and 90 seconds (Essentials).
Effective Data Rate	Displays the real traffic transmit rate of the wireless client
Auth Method	Displays the authentication method used by the AP to authenticate the wireless client
Auth Status	Indicates whether the wireless client is authorized to access the WLAN service
Encryption	Displays the encryption method used by the access point
Control Plane	Displays the name of the SmartZone node to which the AP's control plane is connected
Packets to	Displays the downlink packet count for this session
Packets from	Displays the uplink packet count for this session
Packets dropped	Displays the downlink packet count that has been dropped for this client
Session start time	Indicates the session creation time

## Viewing Wireless Client Information

You can view more information about a wireless client, including its IP address, MAC address, operating system, and recent events that have occurred on it.

To view information about a wireless client, complete the following steps.

1. From the dashboard, go to **Monitor > Clients > Wireless Clients**.
2. From the list of wireless clients, locate the client whose details you want to view.

## Wireless

### Viewing Wireless Client Information

3. Under the **MAC Address** column, click the MAC address of the wireless client.

The **Associated Client** page displays general information about the wireless client:

- **General:** Displays general client information.
- **Health:** Displays information about the real-time health of the client, displaying graphical trends based on the signal-to-noise ratio (SNR) and data rate. You can use the **Start** and **Stop** options to review client health in real time.
- **Traffic:** Displays historical and real-time traffic information.
- **Event:** Displays information about events associated with the client.

# Switch Clients

- Switch Clients..... 19

## Switch Clients

The Switch Clients tab presents a summary of both wireless and wired switch clients.

From the dashboard, go to **Monitor > Clients > Switch Clients**. The **Switch Clients** page is displayed.

To view the switch clients associated with a particular switch group, select a switch group. The details of the switch client are shown on the right pane.

**TABLE 5** Details of the Switch Client

Column Name	Description
Status	Indicates whether the client is online or offline.
Device MAC	Displays the MAC address of the device.
Device Type	Displays the type of device used by the client.
Last Seen	Displays the last login information.
Authentication Type	Displays the authentication flow used by the client.
User	Displays the user details.
Port	Displays the port number.
Switch	Displays the switch details.
VLAN	Displays the assigned VLAN ID.
Description	Displays the description of the client.
Past 24 Hour Auth	Displays if the client was authorized in the last 24 hours.



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