

# RUCKUS AP R350 Release Notes

**Supported on SmartZone 6.0.0**

## Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

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

### Export Restrictions

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

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

### Disclaimer

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

### Limitation of Liability

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

### Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

---

- Document History..... 4
- AP R350 ..... 4
  - Power Modes..... 4
- Release Information ..... 4
- Known Issues ..... 5
- Resolved Issues..... 5
- Adding AP R350 to the Controller..... 7

## Document History

Revision Number	Summary of changes	Publication date
B	<ol style="list-style-type: none"><li>1. Support on RUCKUS Analytics Service Validation with virtual wireless clients.</li><li>2. Added to Resolved Issue section:<ol style="list-style-type: none"><li>a. SCG-126454</li><li>b. AP-15044</li><li>c. MLRD-424</li><li>d. SCG-128275</li></ol></li></ol>	25, August 2021
A	Initial release.	16, August 2021

## AP R350

R350 is an 802.11ax Dual-Band Concurrent 2x2:2 802.11ax (5GHz) with 2x2:2 802.11ax (2.4GHz) for indoor applications, which comes with a single port Ethernet (1000/100/10M) with PoE input. It also has an USB port.

**RUCKUS Analytics Service Validation with virtual wireless clients** : AP now has the ability to perform Service Validation tests over the air with virtual wireless client. The trigger for this procedure comes from RUCKUS Analytics.

## Power Modes

Power Mode	2.4G Radio	5G Radio	1Gbps Ethernet port	USB
DC	2x2(20dBm)	2x2(20dBm)	Enabled	Enabled
AF class switch	2x2(20dBm)	2x2(20dBm)	Enabled	Enabled

## Release Information

SmartZone (SZ) and AP's are based on the following release versions:

- Controller Version: **6.0.0.0.1331**
- Control Plane Software Version: **6.0.0.0.1213**
- AP Firmware Version: **6.0.0.0.3073**

## Known Issues

The following are the Caveats, Limitations, and Known issues in this release.

Component/s	AP
Issue	SCG-130972
Description	If the Ethernet link is enabled in APs H550 or R350 and configured as MAP, wireless clients will not be able to connect or browse the Internet.
Workaround	Disable the Ethernet link for APs H550 or R350 acting as MAP.

Component/s	AP
Issue	SCG-130326
Description	The option, <i>Configure.Me</i> fails when the channel changes from static to auto mode on 2.4GHz in set factory mode.

Component/s	AP
Issue	SCG-129613
Description	After AP joins the AP Zone and the configuration is successfully pushed and synchronized from the controller, the GUI (i.e. Web interface) of the controller displays R350 AP's POE port as not working; namely not applicable (N/A).
Workaround	Check the accurate interface status on the controller GUI by navigating to <b>General &gt; LAN Port Setting</b> .

Component/s	AP
Issue	SCG-130030
Description	Randomly, the Ethernet port negotiates 100Mbps when connected to ICX7150 2.5G port.
Workaround	Configure the interface with the following CLI on Switch in exec mode:  <code>speed 1000-full-slave</code>

Component/s	AP
Issue	SCG-129787
Description	Clients connected to the second hop mesh has data path issues.

## Resolved Issues

The following are the resolved issues related to this release.

Component/s	AP
Issue	SCG-126454
Description	Appended GPB for event code 111 to capture proper failure reason when configuration update fails at AP.

## Resolved Issues

<b>Component/s</b>	AP
<b>Issue</b>	AP-15044
<b>Description</b>	Appended AP status GPB with additional information related to counter of beacon queued and beacon reaped.

<b>Component/s</b>	AP
<b>Issue</b>	MLRD-424
<b>Description</b>	Modified <i>State Machine Logic</i> for RUCKUS Analytics Service Valuation. <i>Now ping and trace route</i> procedures will be skipped if the DNS resolution fails.

<b>Component/s</b>	AP
<b>Issue</b>	SCG-128275
<b>Description</b>	Resolved an issue where AP failed to send POE underpower notification when AP was configured with POE-AUTO and Switch/Router was configured with POE-AT.

<b>Component/s</b>	AP
<b>Issue</b>	ER-8562
<b>Description</b>	Resolved an troubleshooting tool issue when UE roamed.

<b>Component/s</b>	AP
<b>Issue</b>	ER-9486
<b>Description</b>	Resolved an issue where Android devices failed to connect with E-DPSK WLAN.

<b>Component/s</b>	AP
<b>Issue</b>	ER-9545
<b>Description</b>	Resolved an issue of 802.11ax AP using multiple MAC addresses was blocked by Switch feature.

<b>Component/s</b>	AP
<b>Issue</b>	ER-9637
<b>Description</b>	Resolved an issue of 802.11ax APs where clients under same WLAN interface with WPA/WPA2 encryption enabled failed to communicate with each other under certain conditions.

<b>Component/s</b>	AP
<b>Issue</b>	ER-9939
<b>Description</b>	Resolved an issue where the message, <i>read lock not preceded by unlock</i> was not categorized with the correct priority level.

<b>Component/s</b>	AP
<b>Issue</b>	ER-9965
<b>Description</b>	Resolved an issue by removing verbose neighbor AP related logs from the AP support information.

Component/s	AP
Issue	ER-9976
Description	Resolved an issue where Mesh failed to work when management VLAN and LACP are both enabled.

Component/s	AP
Issue	ER-10057
Description	Resolved an issue where the message <i>user.warn kernel: Reached buffer limit</i> in the log affected debugging.

Component/s	AP
Issue	ER-10090
Description	Resolved an issue where portal redirection for Web authentication WLAN failed due to large certificate file.

Component/s	AP
Issue	ER-10169
Description	Enhanced AP to support 2048 bits DH Group for SSL services.

Component/s	AP
Issue	ER-10241
Description	Resolved an issue where a ghost MAC address can be sent an on Ekahau app.

Component/s	AP
Issue	ER-10284
Description	Resolved an issue where SSH traffic for wired client was dropped when the port was configured as Trunk Port with VLAN1 untagged.

Component/s	AP
Issue	ER-10340
Description	Resolved an issue where client was unable to reconnect to a different radio on the same AP.

## Adding AP R350 to the Controller

Before you begin this procedure, copy the AP patch file that you want to apply to a location that you can access from your computer.

### IMPORTANT

This patch only needs to be applied to a single node. After you apply this patch to a node, it will be propagated automatically to other nodes in the cluster.

Follow these steps to apply an AP patch:

1. Download the patch file `ap_116.0_R350_patch_pkg-6.0.0.0-3073.noarch.patch` and move the patch file to a location that you can access from the computer that you are using to access the controller's web interface.

## Adding AP R350 to the Controller

2. Apply this patch to release 6.0 GA refresh (build number 6.0.0.0.1331).
3. Log on to the SmartZone web interface.
4. Go to the page for uploading AP patches.
  - On the 6.0.0 web interface, go to **Administration > Upload AP Patch**, and then click the **AP Patch** tab.
5. In **Patch File Upload**, click **Browse** go to the location where you saved the AP patch file (ap\_116.0\_R350\_patch\_pkg-6.0.0.0-3073.noarch.patch).
6. Click **Open**.
7. On the **AP Patch** tab, click **Upload**. After the patch file is uploaded, the section is populated with the Start time, AP firmware version number and AP model number.
8. Click **Apply Patch**.
9. After the firmware file is applied, the AP firmware information is populated with the following information:
  - Name of the patch file
  - Size of the patch file
  - AP firmware version number
  - AP model number
10. Go to **Configuration > AP Zone**
11. Click **Change AP Firmware**.
12. In the **Change AP Firmware** manually change the AP firmware to the latest AP image (6.0.0.0.3073) in default zone or a specific zone in case of High Scale.
13. Click **Yes**
14. When the controller completes updating the AP firmware of the zone, a message appears and notifies you that the zone's AP firmware was updated successfully.
15. Go to **Configuration > Access Points** to verify that the new AP model you added to the controller are listed on AP list page.
16. Also, verify that all AP's in the default or specific zone is upgraded to 6.0.0.0.3073.
17. Under the **Registration State** column, verify that all new AP models have been approved.

You have completed adding the new AP model to the controller.





© 2021 CommScope, Inc. All rights reserved.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
<https://www.commscope.com>