

RUCKUS Access Point 118.2 Release Notes

Supporting Release 118.2.0.0.875

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

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

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

About This Document.....4

Supported Devices..... 4

What's New in this Release..... 4

Resolved Issues..... 5

About This Document

This document provides release information on RUCKUS Access Point (AP) release 118.2.

NOTE

By downloading this software and subsequently upgrading RUCKUS APs to base image 118.2 and later, do be advised that:

- The AP may send a query to RUCKUS containing the AP's serial number. This allows your AP to autonomously connect with a wireless LAN controller operated by your choice of cloud service provider. RUCKUS may transmit the Fully Qualified Domain Name (FQDN) or IP address of the controller that the AP will subsequently attempt to join back to the AP.
- Do be advised that this information may be transferred and stored outside of your country of residence where data protection standards may be different.

Supported Devices

RUCKUS Access Point standalone firmware version 118.2 supports the following APs.

TABLE 1 Supported AP Models

11ax		11ac-Wave2		11ac-Wave1
Indoor	Outdoor	Indoor	Outdoor	Indoor
R850	T750SE	R720	T811CM	R310
R760	T750	R710	T710S	
R750	T350SE	R610	T710	
R650	T350D	R510	T610S	
R560	T350C	R320	T610	
R550		M510	T310S	
R350		H510	T310N	
H550		H320	T310D	
H350		C110	T310C	
			T305I	
			T305E	
			E510	

What's New in this Release

The following is the *Cross-site scripting (XSS)* vulnerability that is fixed for this release.

- AP Web GUI vulnerability: XSS.

Security fix for the web GUI component. For more information, refer to <https://support.ruckuswireless.com/security>.

Resolved Issues

The following is the resolved issue in this release.

- Security fix for the Cross-site scripting (XSS) vulnerability in the web management interface (GUI) component. For more information, refer to <https://support.ruckuswireless.com/security>.

Cross-site scripting (XSS) vulnerability is fixed in the Solo build and is available for download from <https://support.ruckuswireless.com>.

Usually, the AP Solo functionality is expected to be used only for onboarding to the controller. Probability of hitting this vulnerability is low. If there is a possibility of any party access to the devices in the network, RUCKUS recommends to upgrade the new APs which are not onboarded to controller to this new solo build available on the support site. Also, note that the issue has been fixed in SmartZone R6.1.2.



© 2023 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>