RELEASE NOTES

Unleashed 200.8 Refresh 1 Release Notes

Supporting Unleashed 200.8 Refresh 1

Part Number: 800-72718-001 Rev A
Publication Date: May 2020

Copyright, Trademark and Proprietary Rights Information

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

Revision Number	Summary of changes	Publication date
A	Initial release notes	May 2020

Introduction

This document provides release information on Ruckus Unleashed release 200.8, including new features and enhancements, along with known issues, caveats, workarounds, supported platforms and upgrade information for this release.

Introducing Ruckus Unleashed

Unleashed is a controller-less WLAN solution that allows small businesses to deliver an enterprise-class Wi-Fi user experience in a cost effective, easy to implement, intuitive and yet feature-rich platform.

An Unleashed network can scale up to 128 Access Points and 2,048 concurrent clients in bridge mode (gateway mode supports up to 50 APs and 1,024 clients).

For more information on Unleashed configuration, administration and maintenance, please see the Unleashed Online Help, available at *https://docs.ruckuswireless.com/unleashed/200.8/index.html*.

New in This Release

This section lists the new features and changed behavior in this release.

New Features in GA Release

- Increased Scale to 128 APs

  Unleashed now supports up to 128 APs and 2,048 clients in bridge mode. In gateway mode, a maximum of 50 APs and 1,028 clients is supported.

- ICX Switch Monitoring and Management

  Provides options for monitoring and basic configuration of connected ICX switches.

  The following ICX switch models are supported:

  - ICX7xxx series
  - ICX7xxx series stack

  The following ICX switch firmware versions are supported:

  - SPS08090ufi
  - SPS08091ufi
  - SPS08092ufi
  - SPR08090ufi
  - SPR08091ufi
  - SPR08092ufi

- Easy Deployment Using UMM

Provides an option for automatically configuring and deploying Unleashed networks remotely using an Unleashed Multi-Site Manager template.

- M510 Enhancements

  LTE status information and connectivity check features.

- Local Upgrade Support in Setup Wizard

  Setup Wizard provides an option to upgrade the firmware prior to building the Unleashed network.

- Remove Wave 1 AP Support

  802.11ac Wave 1 APs are no longer supported. Unleashed R310, R500, R600, and T300 series do not support firmware release 200.8 or later and cannot be upgraded to this release.

- URL Filtering

  URL filtering allows administrators to manage internet usage by preventing access to inappropriate websites using a customizable combination of blacklists and whitelists.

- Top 10 ARC Graphs per AP Group/per WLAN

  Application recognition graphs to display in per AP group and per WLAN views.

- New ARC Engine

  The Application Recognition engine has been upgraded to a new system with improved application detection.

- WPA3

  WPA3 encryption and all WPA3-related WLAN types are now supported (WPA3, WPA2/WPA3-mixed, OWE).

- Mark Rogue Devices

  Provides the option to mark rogue APs as "known" so that they do not appear repeatedly in system event and alarm messages.

- Admin Active Directory Authentication

  Allows administrator authentication using a remote authentication server.

- Restructure of Admin & Services Web Interface

  Reorganized several features in the Services and Administration sections of the web UI for improved navigability.

- Additional SMS Service Provider Support

  Additional country code options can now be configured for custom SMS servers.

- Additional Configuration Options from WLAN Edit Page

  Ability to edit WLAN parameters including 802.1X, accounting, etc. from WLAN edit page.

- Remote Syslog Server Support

  Provides options for delivering log messages to a remote syslog server.

- Syslog Client Specific Log Options

  Provides options for limiting syslogs to client-specific subsets.

- Guest Info Exportability

  Allows export of guest information: client connect and disconnect logs.

- GDPR (Phase 1)

  Enables compliance with the EU’s General Data Protection Regulation “right to know” and “right to delete” rules for protection of client data.

- Limit the Allowed Login Domains for Google Authentication

Google authentication can be limited to specific domains for corporate Gmail users.

- PoE Mode Warnings

  Displays a warning icon and a message when an AP is receiving less than full power. Refer to the Online Help for AP-specific details on limitations due to reduced power input.

- UMM Login Enhancement

  Improved handling of remote login from UMM.

- ARC Category Policy Support

  Allows the user to select "all" applications when creating an application recognition rule.

- New CLI Configuration Commands

  Three new Master CLI configuration commands: "HS2.0 support", "Configure restore" and "Location message forwarding."

- Internet Checking Enhancement

  New CLI commands allow configuration of DNS addresses used for Internet status checking.

- WiFi4EU Snippet

  This option allows introduction of a WFi4EU snippet, which allows access to free of charge Wi-Fi for EU citizens and visitors via hotspots in public spaces in municipalities across Europe.

- Changed Election Heartbeat Broadcast Packets to Unicast

  Member APs will send unicast packets rather than broadcast packets to known APs after entering run state.

Enhancements in Release 200.8.10.3.278

- Enhancement of system security
- Removal of product registration in GUI

Changed Behavior

- None

Hardware and Software Support

Supported Platforms

Unleashed version **200.8.10.3.278** supports the following Ruckus AP models:

Indoor AP	Outdoor AP
C110	E510
H320	T310c
H510	T310d
M510	T310n
R320	T310s
R510	T610
R610	T610s

Indoor AP	Outdoor AP
R710	T710
R720	T710s
R750	

NOTE

The following 802.11ac "Wave 1" APs are no longer supported as of this release and cannot be upgraded to Unleashed firmware version 200.8 or later:

- R310
- R500
- R600
- T300
- T300e
- T301n
- T301s

If any unsupported APs are detected during upgrade, a warning message will appear. If you proceed with the upgrade, the APs will be unable to connect.

Upgrade Information

Supported Upgrade Paths

The following release builds can be directly upgraded to Unleashed version **200.8.10.3.278**:

Online Upgrade:

- 200.7.10.2.339 (Unleashed 200.7 GA)
- 200.7.10.102.64 (Unleashed 200.7 MR1)
- 200.7.10.202.94 (Unleashed 200.7 MR2)
- 200.7.10.202.118 (Unleashed 200.7 MR2 refresh1)
- 200.8.10.3.243 (Unleashed 200.8 GA)

NOTE

Beginning with Unleashed 200.8, 802.11ac wave1 APs will not be supported by Unleashed. To upgrade from a release before 200.7 (e.g., 200.6) to 200.8, you must first upgrade to 200.7 before upgrading to a later release (e.g., 200.8).

Local Upgrade:

- 200.2.9.13.186 (Unleashed 200.2 GA)
- 200.3.9.13.228 (Unleashed 200.3 GA)
- 200.4.9.13.47 (Unleashed 200.4 GA)
- 200.5.10.0.235 (Unleashed 200.5 GA refresh 1)
- 200.5.10.0.291 (Unleashed 200.5 GA refresh 3)
- 200.6.10.1.308 (Unleashed 200.6 GA)
- 200.6.10.1.310 (Unleashed 200.6 GA refresh 1)

- 200.6.10.1.312 (Unleashed 200.6 GA refresh 2)
- 200.7.10.2.339 (Unleashed 200.7 GA)
- 200.7.10.102.64 (Unleashed 200.7 MR1)
- 200.7.10.202.94 (Unleashed 200.7 MR2)
- 200.7.10.202.118 (Unleashed 200.7 MR2 refresh 1)
- 200.8.10.3.243 (Unleashed 200.8 GA)

NOTE
Unleashed local upgrade, if destination build across two major release, AP will set factory after upgrade, previous configuration will be lost.

Known Issues

This section lists the caveats, limitations and known issues in this release.

Issue	UN-4149
Description	Online upgrade from a release prior to release 200.7 requires first upgrading to 200.7 and then upgrading to 200.8.

Issue	UN-3891
Description	When performing a local upgrade from a release prior to 200.5 to 200.8, the Unleashed network will be reset to factory default settings.

Issue	UN-3508
Description	Local upgrade will fail if 802.11ac Wave 1 APs exist on the Unleashed network.

Issue	UN-3766
Description	The web UI only shows general and health info for active ICX switches in an ICX stack.

Issue	UN-4043
Description	iOS devices may fail to be redirected to the login page when connecting to a Google social media guest WLAN.

Issue	UN-3861
Description	Support for WeChat guest authentication is no longer supported by Tencent, WeChat's parent company, due to security concerns.

Resolved Issues

- • Resolved two security issues related to UI vulnerabilities. For security incidents and responses, see *www.ruckuswireless.com/security*.
- Resolved a fast roaming issue that could cause Multicast/broadcast packets to get dropped. [ER-6780]
- Resolved an issue where the Directed-Multicast setting would not persist on the WLAN and Ethernet interfaces on APs. [ER-7600]
- Resolved an R730 AP watchdog timeout issue. [ER-7870]

- Resolved an issue that could cause R720 and R730 APs to reboot due to target fail detected error. [ER-7874]
- Resolved an issue that could cause AP reboots due to kernel panic caused by a memory leak. [ER-7896]
- Resolved an issue with throughput performance in WPA/WAP2 WLANs. [ER-7956]
- Resolved an issue where clients in sleep mode were unable to receive multicast/broadcast packets. [ER-8085]
- Resolved an issue where accessing the ZoneDirector GUI would intermittently fail. [ER-8267/ER-8217/ER-8056]
- Changed the log level of one PoE-related syslog message from error to debug. [ER-8439]

COMMSCOPE®
RUCKUS®

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com