RELEASE NOTES

RUCKUS Unleashed 200.12 MR1 Refresh1 Release Notes

Supporting Unleashed 200.12

Part Number: 800-73198-001 Rev A
Publication Date: June 2022

Copyright, Trademark and Proprietary Rights Information

© 2022 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**

Introduction **4**

Introducing RUCKUS Unleashed 4

New in This Release **4**

New Features and Enhancements in 200.12.10.105.100 4

New Access Points in 200.12.10.5.234 4

New Features in GA Release 5

Changed Behavior 5

Hardware and Software Support **5**

Supported Platforms 5

Upgrade Information **6**

Supported Upgrade Paths 6

Known Issues **8**

Resolved Issues **8**

Resolved Issues in Build 200.12.10.105.129 8

Resolved Issues in Build 200.12.10.105.100 8

Resolved Issues in Build 200.12.10.5.234 8

Document History

Revision Number	Summary of changes	Publication date
A	Initial release notes	June 2022

Introduction

This document provides release information on RUCKUS Unleashed release 200.12, 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 25 APs and 512 clients).

For more information on Unleashed configuration, administration, and maintenance, please see the Unleashed Online Help, available at https://docs.commscope.com/bundle/unleashed-200.12-onlinehelp/.

New in This Release

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

New Features and Enhancements in 200.12.10.105.100

- Dual WAN ports are supported

  When gateway mode is enabled, the user can configure two WAN ports, one active WAN port and another standby WAN port that works in failover mode.

  NOTE
  Dual WAN ports support is applicable only for H350/H550 Gateway mode.

- Rouge AP Report

  Support to report rouge AP information in status/statistics report.
- Updating security issues in code, related to vulnerabilities CVE-2018-15504, CVE-2018-15505, and CVE-2019-12953.
- Change default "dn" name into ruckus default domain name for hotspot WLAN.
- Enable SSID command in the master CLI.

New Access Points in 200.12.10.5.234

- H350

  This release adds Unleashed support for the new H350 indoor 802.11ax AP.

H350 is an 802.11ax Dual-Band Concurrent 2x2:2 .11ax(5GHz) + 2x2:2 .11ax(2.4GHz) for indoor applications which comes with a three port Ethernet (10/100/1000) with PoE input. It doesn't have USB port.

- T350se

  This release adds Unleashed support for the new T350se outdoor 802.11ax (Wi-Fi 6) AP.

  T350se is an 802.11ax Dual-Band Concurrent 2x2:2 .11ax(5GHz) + 2x2:2 .11ax(2.4GHz) for outdoor applications which comes with a single port Ethernet (1000/100/10M). It also has an integrated USB port.

New Features in GA Release

- Portal WLAN enhancement for new certificate input

  When a new certificate is imported, unleashed master or controller uses the FQDN as the URL host name for portal server access, and corresponding dns-spoofing is done to resolve the domain name to the IP address of unleashed master or controller.

- Master CLI supports the following:
  - WLAN service for AP group
  - APs from other AP groups can be moved from one AP group to another AP group.
- Friendly-guest key support for guest WLAN

  Introduction of user-friendly guest key that consists of only numbers.

- Channel 144 support

  Channel 144 is supported for country codes "US" and "JP" when DFS is enabled.

- DNSmasq upgrade for security issue

  DNSmasq is upgraded to address a security issue.

- Change of keywords in CLI and web GUI.

  The keywords "blacklist" and "whitelist" is changed to "blocklist" and "allowlist" respectively.

- UMM tunnel to AP for debugging

  UMM web UI can access master AP's CLI by way of using an SSH tunnel between the master AP and UMM.

- Support navigate to AP detail from AP group page

  From the AP group page, navigation to AP detail page is supported.

- Remote access Unleashed and change Unleashed password

  Remote access to the Unleashed system is supported to reset the password for Unleashed.

Changed Behavior

- None

Hardware and Software Support

Supported Platforms

Unleashed version **200.12.10.105.129** supports the following RUCKUS AP models:

Indoor AP	Outdoor AP
C110	E510
H320	T310c
H510	T310d
M510	T310n
R320	T310s
R510	T610
R550	T610s
R610	T710
R650	T710s
R710	T750
R720	T750se
R750	T350c
R850	T350d
R350	T350se*
H550	
H350*	

NOTE
H350 and T350se were introduced in GA release.

Upgrade Information

Supported Upgrade Paths

The following release builds can be directly upgraded to Unleashed version **200.12.10.105.129**:

Online Upgrade:

- 200.7.10.2.339 (Unleashed 200.7 GA)
- 200.7.10.102.64 (Unleashed 200.7 MR1)
- 200.7.10.102.92 (Unleashed 200.7 MR2)
- 200.7.10.102.94 (Unleashed 200.7 MR3)
- 200.7.10.202.118 (Unleashed 200.7 MR4)
- 200.7.10.202.121 (Unleashed 200.7 MR5)
- 200.7.10.202.127 (Unleashed 200.7 MR6)
- 200.8.10.3.243 (Unleashed 200.8 GA)
- 200.8.10.3.278 (Unleashed 200.8 MR1)
- 200.8.10.3.290 (Unleashed 200.8 MR2)
- 200.9.10.4.202 (Unleashed 200.9 GA)
- 200.9.10.4.212 (Unleashed 200.9 GA Refresh 1)
- 200.9.10.4.233 (Unleashed 200.9 GA Refresh 2)
- 200.9.10.4.243 (Unleashed 200.9 GA Refresh 3)

- 200.10.10.5.229 (Unleashed 200.10 GA)
- 200.10.10.5.246 (Unleashed 200.10 GA Refresh 1)
- 200.10.10.5.253 (Unleashed 200.10 GA Refresh 2)
- 200.11.10.5.195 (Unleashed 200.11 GA)
- 200.12.10.5.234 (Unleashed 200.12 GA)
- 200.12.10.105.100 (Unleashed 200.12 MR1)

NOTE
To upgrade to 200.12 using the online upgrade method, your Unleashed network must be running **200.7** or later. If your network is running an earlier release, first upgrade to 200.7, then continue to upgrade to 200.12.

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)
- 200.7.10.202.92 (Unleashed 200.7 MR2)
- 200.7.10.202.94 (Unleashed 200.7 MR3)
- 200.7.10.202.118 (Unleashed 200.7 MR4)
- 2007.10.202.121 (Unleashed 200.7 MR5)
- 200.7.10.202.127 (Unleashed 200.7 MR6)
- 200.8.10.3.243 (Unleashed 200.8 GA)
- 200.8.10.3.278 (Unleashed 200.8 MR1)
- 200.8.10.3.290 (Unleashed 200.8 MR2)
- 200.9.10.4.202 (Unleashed 200.9 GA)
- 200.9.10.4.212 (Unleashed 200.9 GA Refresh 1)
- 200.9.10.4.233 (Unleashed 200.9 GA Refresh 2)
- 200.9.10.4.243 (Unleashed 200.9 GA Refresh 3)
- 200.10.10.5.229 (Unleashed 200.10 GA)
- 200.10.10.5.246 (Unleashed 200.10 GA Refresh 1)
- 200.10.10.5.253 (Unleashed 200.10 GA Refresh 2)
- 200.11.10.5.195 (Unleashed 200.11 GA)
- 200.12.10.5.234 (Unleashed 200.12 GA)
- 200.12.10.105.100 (Unleashed 200.12 MR1)

Known Issues

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

- None

Resolved Issues

This section lists any customer-reported issues from previous releases that have been resolved in this release.

Resolved Issues in Build 200.12.10.105.129

- Resolved a display issue of guest portal page for mobile devices. [ER-11330]
- Resolved an issue where the OS types and host names were not recognized properly for certain devices. [ER-10981]
- Resolved a packet loss issue during background scanning on some particular APs. [ER-10181]
- Enhanced the SMS notification feature to support JSON format in post data. [ER-11148]
- Resolved an issue where certain allowed service got unexpectedly blocked when application policy denial rule was configured as blocking all Tunneling. [ER-11140]

Resolved Issues in Build 200.12.10.105.100

- Uplink throughput is better than downlink throughput in R710 AP with 3x3 clients; performance is well below when compared to that of AP R610. [ER-10474]
- APs R710 and R610 reboot due to kernel panic. [ER-10607]
- T610/T710 APs - Air Time Fairness (ATF) with 8x8 11ax clients; 2 clients receiving nearly zero throughput. [ER-10530]
- R320 AP VoIP silence, wrong sequence number. [ER-10181]
- R710 AP reboots due to kernel panic. [ER-10918]
- AP R750 UE with high idle time are not getting cleared from the host table. [ER-10844]
- All the clients randomly lost network connection on the AP. [ER-10797]
- R850 AP reboots due to kernel panic. [ER-10944]
- Random EAP disconnects on Zebra Scan Guns. [ER-10760]

Resolved Issues in Build 200.12.10.5.234

- Clients dropped out with a session timeout of 60 seconds. [ER-10627]
- Multicast traffic was allowed with client isolation enabled. [ER-10555]
- R850/R720/R730 802.1X UE cannot connect with non-proxy mode. [ER-10422]
- UE loses network connectivity when roaming between radios in the same AP, in WPA2 WLAN. [ER-10340]
- SSH traffic was blocked with "untag vlan 1" in trunk uplink. [ER-10284]
- Non-existing ghost MAC was sent from AP to RTLS server. [ER-10241]
- "get mcast-airtime" returned the value "0". [ER-10202]
- Multicast (mDNS) traffic from the client not egressing out of the AP when "unicast+multicast" client isolation is enabled. [ER-10103]
- Reached buffer limit in syslog or support log. [ER-10057]

- LACP works with Mesh enabled. [ER-9976]
- Read lock is not preceded by unlock. [ER-9939]
- Apple clients disconnecting from WLAN due to inactivity. [ER-9831]
- Clients with Sonos App are failing to detect Sonos speakers over WLAN. GTK Key Index missing. [ER-9637]
- R750 MU-MIMO 2.4GHz has very low throughput and 5GHz uplink has 50% more throughput than downlink. [UN-9517]
- AP reboots due to memory leakage. [UN-9496]

© 2022 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com