RELEASE NOTES

RUCKUS Unleashed 200.7.10.202.145 Refresh 8 Release Notes

Supporting Unleashed 200.7.10.202.145

Part Number: 800-73495-001 Rev A
Publication Date: September 2023

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 Release

This document provides release information on RUCKUS Unleashed release 200.7, 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.

The Unleashed solution scales up to 50 Access Points and 1,024 concurrent clients.

For more information on Unleashed configuration, administration, and maintenance, please see the Unleashed Online Help, available at https://docs.commscope.com/bundle/unleashed-200.7-onlinehelp.

Supported Platforms and Upgrade Information

Supported Platforms

Unleashed version **200.7.10.202.145** supports the following RUCKUS AP models:

Indoor AP	Outdoor AP
C110	E510
H320	T300
H510	T300e
M510	T301n
R310	T301s
R320	T310c
R500	T310d
R510	T310n
R600	T310s
R610	T610
R710	T610s
R720	T710
	T710s

Upgrade Information

The following release builds can be directly upgraded to Unleashed version **200.7.10.202.145**:

Online Upgrade:

- 200.0.9.9.608 (Unleashed 200.0 GA)
- 200.1.9.12.62 (Refresh of Unleashed 200.1 GA)
- 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)
- 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 GA Refresh 1)
- 200.7.10.202.92 (Unleashed 200.7 GA Refresh 2)
- 200.7.10.202.94 (Unleashed 200.7 GA Refresh 3)
- 200.7.10.202.118 (Unleashed 200.7 GA Refresh 4)
- 200.7.10.202.121 (Unleashed 200.7 GA Refresh 5)
- 200.7.10.202.127 (Unleashed 200.7 MR Refresh 6)
- 200.7.10.202.141 (Unleashed 200.7 MR Refresh 7)

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)
- 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 GA Refresh 1)
- 200.7.10.202.92 (Unleashed 200.7 GA Refresh 2)
- 200.7.10.202.94 (Unleashed 200.7 GA Refresh 3)
- 200.7.10.202.118 (Unleashed 200.7 GA Refresh 4)
- 200.7.10.202.121 (Unleashed 200.7 GA Refresh 5)
- 200.7.10.202.127 (Unleashed 200.7 MR Refresh 6)
- 200.7.10.202.141 (Unleashed 200.7 MR Refresh 7)

Enhancements and Resolved Issues

This section lists new features and enhancements that have been added in this release, and any customer-reported issues from previous releases that have been resolved in this release.

Enhancements in Release 200.7.202.141

- Fix for FragAttacks (11ac wave1 AP 5G radio)

Enhancements in Release 200.7.202.127

- Fix for FragAttacks (11ac wave2 AP)

Enhancements in Release 200.7.202.121

- Enhancement of system security

Enhancements in Release 200.7.202.118

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

Enhancements in Release 200.7.10.202.94

- Enhancement of system security

Enhancements in Release 200.7.10.202.92

Release 200.7.10.202.92 (200.7 GA Refresh 2) introduces the following new features and enhancements:

- A new option in the Setup Wizard allows the admin to perform a local firmware upgrade prior to deployment.
- New CLI commands allow the admin to force Unleashed Multi-Site Manager (UMM) management, preventing the disabling of UMM management from the web interface. Use the `Unleashed-Multi-Site-Manager-Force` command to enable the force-umm feature. Use the `no Unleashed-Multi-Site-Manager-Force` command to disable force-umm.

Enhancements in Release 200.7.10.102.64

Release 200.7.10.102.64 (200.7 GA Refresh 1) introduces the following new features and enhancements:

- This release adds support for the Japan version of the Unleashed M510 LTE Access Point.
- Unleashed Admin accounts can now be created with limited monitoring privileges, in addition to full administrative access.
- Enhanced the Hotspot web interface.
- Enhanced PoE Mode settings in AP model-specific controls to provide better control over AP power settings.
- External DPSK: Dynamic PSKs can now be created for clients authenticated via external RADIUS server, in addition to internal database.
- Extended the maximum size of the guest WLAN "Terms and Conditions" to 16,000 bytes.

Enhancements/New Features in the GA Release

Release 200.7 (GA) introduces the following new features and enhancements:

- AP Groups

  AP Groups can now be configured, allowing admins to apply multiple configuration profiles to different groups of APs.

- CLI Setup Wizard

  A new CLI setup wizard provides another way to perform the initial network configuration, in addition to the mobile app and browser-based setup methods.

- Increase Scale to 50 APs and 1,024 Clients

Unleashed now supports up to 50 APs (up from 25), and 1,024 clients (up from 512).

> **NOTE**
> As of this release, this increase applies only to Unleashed 802.11ac Wave 2 APs.

> **NOTE**
> The 50 AP maximum does not apply when the Master AP is in Gateway Mode, regardless of AP model. If the Master AP is deployed in Gateway Mode, the maximum remains 25 APs.

- 802.1X Authentication Caching

  This feature allows the APs to cache 802.1X client credentials at the AP, so that clients will not have to perform additional authentications in case of disconnection from the RADIUS server within a specified time limit.

- WPA2+Hotspot WLANs

  This release adds support for creating an SSID using WPA2-PSK and Hotspot service at the same time.

- Bonjour Fencing

  Bonjour Fencing provides a mechanism to limit the scope of Bonjour service discovery in the physical/spatial domain. This is useful because logical network boundaries (e.g. VLANs) do not always correlate well to physical boundaries within a building/floor.

  This feature can be configured via CLI commands only in this release.

- Ethernet Port VLAN Support

  Allows VLAN configuration of Ethernet ports on wall-plate type APs (H320 and H510).

- Merge Guest and Social Media WLAN Types

  Social Media WLANs are now a subcategory of Guest WLAN, rather than being a separate WLAN type as in previous releases.

- Captive Portal Customization

  Provides several new options for customizing the Captive Portal login page for Guest WLANs.

- Portal Page Multi-Language Support

  This feature is enabled by default for the Guest WLAN login portal page when the web interface language is not English.

- Client Connection Diagnostics Enhancement

  Client connection troubleshooting can now be run on clients connected to Web Auth, Hotspot (WISPr), and Social Media Guest WLANs, in addition to standard usage WLANs.

- Save Debug Info Progress Indication

  A progress indicator is now displayed when the Save Debug Info button is pressed to download a debug log file.

- Display Unleashed Version on First Installation Page

  The firmware version number currently being configured is now displayed on the first installation wizard screen.

- Favorite Client Support

  Mark a client as a "favorite," to receive notifications when the client connects or disconnects.

- L3 Fast Path Performance Enhancement

  This feature improves throughput performance when the AP is gateway mode, increasing efficiency by allowing certain packets to bypass bridge and route processes based on information learned from traffic analysis.

- Event Level Setting in Diagnostics Logs

  Provides a configuration option to set the level of debug logs to display on the Events page.

- Display "Uploading" Progress Bar on Upgrade Page

A progress bar is now displayed to indicate the image file upload progress.

- Increased Max Bind IP Addresses for DHCP Server to 128 from 32.
- Improved speed of Setup Wizard process.
- MAC Auth authentication can now use local database as the auth server.
- Reduce Channel Change Frequency.

Resolved Issues in Build 200.7.10.202.145

- iOS MA unable to login to manage Unleashed network. (Must upgrade MA to the latest version that includes the fix for security DNS issue on MA side). [ER-12577]

Resolved Issues in Build 200.7.10.202.141

- Resolved an issue where WISPr client was not able to access the domain in the walled garden whitelist. [ER-6559]
- Resolved an issue where MacBook client was getting disconnected intermittently. [ER-9831]
- Resolved an issue where ZoneDirector system was becoming unresponsive under certain conditions. [ER-10223]
- Resolved a fingerprints-related issue. [ER-10981]

Resolved Issues in Build 200.7.10.202.127

- Resolved an issue related to FragAttacks. For more details, refer to https://www.commscope.com/fragattacks-commscope-ruckus-resource-center/.
- Resolved an issue where R310 APs would reboot randomly due to "Application reboot". [ER-10050]

Resolved Issues in Build 200.7.10.202.121

- Resolved an issue where the "Directed-Multicast" setting would not persist on the WLAN and Ethernet interfaces on APs. [ER-7600]
- Resolved a security issue related to CLI vulnerabilities. [UN-4624]

  For security incidents and responses, see: http://www.ruckuswireless.com/security

Resolved Issues in Build 200.7.10.202.118

- Resolved an issue where rogue device reporting would not work properly when the SSID name is configured as a non-English name. [ER-6248]
- Resolved an issue on R720 APs where wireless clients could experience low uplink throughput if they had previously associated to a WLAN with rate limiting enabled on the same R720 AP. [ER-6567, ER-6576, ER-6830]
- Resolved a kernel panic issue on APs located in high density environments when associated wireless clients were frequently roaming in and out of range. [ER-6689]
- Resolved a Multicast group issue that could cause multicast/broadcast packets to get dropped. [ER-6748]
- Resolved an issue with delayed response from session manager from controller due to latency between controller and remote APs, which could result in timeout errors during DPSK authentication. [ER-6886]
- Resolved an issue on R310 APs where the 5G radio would not function properly in 20 MHz channelization mode. [ER-6969]
- Resolved an issue on 11ac Wave 1 APs where unsupported data rates were used to send the first data packet to a wireless client over the 5 GHz radio. [ER-7018]

- Resolved an issue where the R700 APs rebooted on detection of target failure. [ER-7073]
- Resolved an issue where the incorrect redirection URL was sent for guest authentication by the controller if the "domain" field was not set in the uploaded certificate. [ER-7156]
- Resolved an issue with mesh APs establishing a connection to an uplink AP when smart uplink selection is enabled. [ER-7204]
- Resolved an issue where configurations saved on an access point might become corrupted randomly. [ER-7225]
- Resolved an AP issue with "Singapore" country code where DFS channels were not listed in the supported channel list for certain AP models. [ER-7247]
- Resolved an issue with T310D APs rebooting with reason "Reset Button". [ER-7419]
- Resolved an issue where the AP CLI command "get scanresults" did not work properly. [ER-7630]
- Resolved an issue where the reported MAC address and other content was inaccurate in packets sent from the AP to the Aeroscout server. [ER-7937/ER-8161]

Resolved Issues in Build 200.7.10.202.94

- Resolved an issue of dropping ARPs in target firmware, due to all GRP Key entries occupied. [ER-6748]

Resolved Issues in Build 200.7.10.202.92

- Resolved a security issue related to vulnerability CVE-2019-11477, CVE-2019-11478 and CVE-2019-11479. [AP-11589]

  For information on security incidents and responses, please visit *https://www.ruckuswireless.com/security*.
- Resolved an issue where, when a CA signed certificate was installed on the Master AP and the Master AP was disconnected, the certificate would not be pushed to the member AP that would become the new Master, resulting in the new Master using its original certificate rather than the signed certificate. [ER-7625]
- Resolved an issue where the authentication portal page would still show up on MacOS clients after successful guest authentication. [ER-7392]
- Resolved an issue on R720 APs where the output of the CLI command `get bond` would incorrectly display LACP disabled when LACP was enabled. [ER-7796]

Resolved Issues in Build 200.7.10.102.64

- Resolved an issue with high CPU utilization caused by bulk login and logoff attempts from the network. [ER-7081]
- Resolved an issue with R310 APs that could cause instability when 5 GHz radio channelization was set to 20. [ER-6969]
- Resolved an issue on R720 APs where wireless clients could experience low uplink throughput if they had previously associated to a WLAN with rate limiting enabled on the same R720 AP. [ER-6567, ER-6830, ER-6576]
- Resolved an issue that could cause R720 APs to reboot due to kernel panic. [ER-6689]

Caveats, Limitations and Known Issues

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

Issue	N/A
Description	None

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