COMMSCOPE®
RUCKUS ®

RUCKUS Unleashed 200.10 GA Refresh 2 Release Notes

Supporting Unleashed 200.10 GA Refresh 2

Copyright, Trademark and Proprietary Rights Information

Contents

Document History

Revision Number	Summary of changes	Publication date
A	Initial release notes	October 2021

Introduction

This document provides release information on RUCKUS Unleashed release 200.10, 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-200.10-onlinehelp/.

New in This Release

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

New Features

- Change in success message status from red to green

  When a test is successful, the status message is displayed in green. When a test fails, the status message is displayed in red.

- Remote Packet Capture

  Captures wireless packets during normal operation and the packets are saved in local files or streamed to Wireshark.

- Simplify the Installation

  During quick installation, a new API is loaded by the UI and WLAN template data is fetched from and sent to the backend. WLAN data such as SSID is displayed in the UI and used as a default value and the data is sent to backend when creating the default WLAN.

- Provide option to change Master AP, based on network intelligence

  This feature gives an option to change the master AP. Under Primary Preferred Master, the UI lists all the APs that accord with a master role on the network. The AP is sorted and listed by a special algorithm (master elect) where the best master is placed at the top of the list. The user can choose the best master as the Primary Preferred Master.

- Election Replay Attack

  This feature aims to avoid DDOS attack as a result of not encrypting the election heartbeat or control packet. When the master AP sends election packet to a member AP, the election packet will include the member AP's MAC address into the packet content. When the member AP receives message from master AP, the MAC address is verified with that of the member AP and if there is a match, then the member AP performs the action specified or else the member AP ignores the election packet.

Following are the messages that include the member AP's MAC address: Reboot, set factory, set debug level, set AP role, and set AP delay elect.

- WPA3 R2: 11r 11w. etc...

  Adds SAE FT and AKM PSK SHA256 support to "Open + WPA2/WPA3-Mixed" WLAN, and adds new WLAN type "802.1X EAP WPA2/WPA3-Mixed".

- QR Code Support

  Unleashed system generates standard QR code so that mobile devices can access Wi-Fi automatically, depending on mobile device version and support.

- Web UI Enhancement - UI Generates Alarm Notification List from backend API

  The UI provides alarm definition list that is fetched from the backend.

- Management VLAN

  This release provides management VLAN support.

- Management ACL

  This release provides management ACL support.

- 2.4G Mesh Support

  This release provides 2.4G mesh support.

- Save AP core dump from master web UI

  This release introduces the option of saving AP core dump files from the web UI. When an AP core dump occurs, a log file is created and stored on Unleashed, and the AP Diagnostic Information section lists the AP's MAC address, IP address, device name, description, and AP model.

- Open VPN Support

  In this release, Unleashed system will provide CLI commands to bring up the openVPN daemon, maintain the openVPN tunnel, and debug the openVPN status and statistics.

- Status/Statistic Report

  Customizing different intervals of different data types, like **wlan-report-interval**, **ap-report-interval**, and **client-report-interval**.

- Remove RUCKUS infomation in web UI

  The Unleashed system will not provide any RUCKUS information in the web UI when **no-ruckus-information** is enabled in the master AP.

- A special portal for local database user to change password

  This feature allows users to modify password of their accounts without the need for an administrator. Also, syslog will have a record of the users who change their passwords. This reduces the workload of the administrator effectively.

- Import multiple users into Local database by CSV file

  This feature helps to import multiple user accounts into local database using a CSV file.

- LACP support for 11ax and wave2 AP in CLI

  This feature provides LACP support for 11ax and wave2 AP in CLI.

Changed Behavior

- None

Hardware and Software Support

Supported Platforms

Unleashed version **200.10.10.5.253** 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	
R850	

Upgrade Information

Supported Upgrade Paths

The following release builds can be directly upgraded to Unleashed version **200.10.10.5.253**:

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)

   NOTE

   To upgrade to 200.10 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 200.10.

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)

Known Issues

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

Issue	UN-5291
Description	Master bonjour gateway is not working if the same VLAN is enabled for management interface.

Issue	UN-5000
Description	iOS devices that support 802.11r and WPA3 cannot associate to open-WPA23-mixed+802.11r WLAN.

Issue	UN-5279
Description	After prov.apk is installed, Android 10 phone is unable to connect to corresponding WLAN by way of "WiFiAutoConf" application.

Issue	UN-5083
Description	Multiple entries are generated for the same iOS or Android device if random MAC addresses are used by the iOS device.

Issue	UN-5070
Description	iphone with iOS 14.0.1 or later version is unable to connect to hotspot 2.0 WLAN.

Issue	UN-4130
Description	Error 403 appears for iOS devices when it tries to connect with a guest WLAN profile using a social login.

Resolved Issues

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

Resolved Issues in Build 200.10.10.5.253

- Resolved an issue where the client is unable to access the internet sometimes. [ER-9521]
- Resolved an issue where AP rebooted due to kernel panic after enabling LACP. [ER-10577]
- Resolved an issue where multicast traffic is allowed when client isolation is enabled. [ER-10555]
- Resolved one MU-MIMO related performance issue for 11ax APs. [ER-9517]

Resolved Issues in Build 200.10.10.5.246

- Resolved an issue where channels 132 and 136 were disabled for 80 Mhz and Auto, Japan country code. [ER-10500]
- Resolved an issue where WLAN passphrase locked up the system. [ER-10223]
- Resolved an issue where Apple clients were getting disconnected from the WLAN due to inactivity. [ER-9831]
- Resolved an issue where the UE loses network connectivity when roaming between radios on same AP, in WPA2 WLAN. [ER-10340]
- Resolved an issue where the client with Sonos app were failing to detect Sonos speakers over the WLAN. GTK Key Index missing. [ER-9637]

Resolved Issues in Build 200.10.10.5.229

- Resolved an issue where Unleashed cannot add ICX switch to the dashboard sometimes. [ER-9968]
- Resolved an issue on AP where Mesh would not function properly when management VLAN and LACP are both enabled. [ER-9976]
- Resolved an issue related to vulnerabilities on Unleashed Master after disabling older TLS versions. [ER-9983]

- Resolved an issue where "mcast-airtime" value was not correct on Unleashed AP. [ER-10202]

COMMSCOPE®

RUCKUS®