RELEASE NOTES

Unleashed 200.6 Refresh 1 Release Notes

Supporting Unleashed 200.6 Refresh 1

Part Number: 800-71973-001 Rev A
Publication Date: June 2018

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, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS 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, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

About This Release

This document provides release information on Ruckus Unleashed release 200.6, 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 25 Access Points and 512 concurrent clients.

For more information on Unleashed configuration, administration and maintenance, please see the Unleashed Online Help, available at *https://docs.ruckuswireless.com/unleashed/200.6/index.html*.

Supported Platforms and Upgrade Information

Supported Platforms

Unleashed version **200.6.10.1.310** supports the following Ruckus AP models:

Indoor AP	Outdoor AP
C110	T300
E510	T300e
H320	T301n
H510	T301s
R310	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 **200.6.10.1.310**:

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)
- 200.5.10.0.283 (Unleashed 200.5 GA Refresh 2)
- 200.5.10.0.291 (Unleashed 200.5 GA Refresh 3)
- 200.6.10.1.308 (Unleashed 200.6 GA)

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)
- 200.5.10.0.283 (Unleashed 200.5 GA Refresh 2)
- 200.5.10.0.291 (Unleashed 200.5 GA Refresh 3)
- 200.6.10.1.308 (Unleashed 200.6 GA)

Enhancements and Resolved Issues

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

New Access Points

- New Access Point: C110

  This release adds Unleashed support for the C110 802.11ac Wall Plate AP with DOCSIS 3.0 backhaul support. Designed to be installed in an outlet box with a coaxial cable termination, the C110 features a DOCSIS/EuroDOCSIS 3.0 cable modem for backhaul, a USB port for uses such as a BLE dongle or other IoT applications, and two RJ-45 LAN ports for in-room wired Ethernet access.

- New Access Point: E510

  This release adds Unleashed support for the E510 Modular Access Point. The E510 is a modular outdoor AP designed for installation in scenarios where the Wi-Fi intelligence and the antenna modules must be physically separated, such as light poles, light fixtures, street furniture, railway carriages and track side installations.

- New Access Point: T310 Series

  This release adds Unleashed support for the T310 series of outdoor dual-band 802.11ac Wave 2 APs.

  The T310 series (T310c, T310d, T310n, T310s) is an outdoor dual-band 802.11ac Wave 2 AP designed for flexible installation in a wide variety of outdoor environments.

  The T310d has an omni antenna, an extended temperature range (-40C to 65C), one 10/100/1000 Ethernet port that supports 802.3af PoE in, optional DC power input, and a USB port for IoT devices, such as a BLE or Zigbee dongle, Z-Wave, etc.

  The T310c has an omni antenna, with narrower operating temperature range, and no USB port or DC power supply option.

  The T310s is the sector antenna variant of the T310 series, and the T310n is the narrow sector antenna variant.

Enhancements

Release 200.6 introduces the following new features/enhancements:

- Same-WLAN Support for Multiple Social Media Logins

  Existing Social Media login methods (Facebook, Google, LinkedIn and Microsoft) can now be used simultaneously on the same WLAN.
- WeChat WLANs

  A new social media WLAN type – WeChat – is now available.
- Zero Touch Mesh

  Zero Touch Mesh allows customers to skip the mesh configuration priming process, enabling Mesh APs already installed in their permanent locations to auto-discover, auto-provision and auto-form a mesh network without priming.
- Application Recognition and Control Enhancements

  Application rate limiting and QoS traffic shaping rules can now be created, in addition to application denial rules.
- Client Connection Troubleshooting

  Client connection troubleshooting allows customers to diagnose wireless client connection issues to determine why a client fails to connect to the wireless network.
- Unleashed Multi-Site Manager (UMM) Connectivity Enhancements

  Allows connectivity from UMM to an Unleashed Master AP behind a NAT firewall. Unleashed will initiate an SSH tunnel when the "Enable management by Unleashed Multi-Site Manager" option is selected, allowing TR-069 protocol traffic to traverse the firewall.
- Internet Status Enhancement

  The Internet component on the Dashboard now provides details on the Unleashed Master AP's upstream connection to the internet, including public IP address, DNS servers, Gateway address, and the Ethernet port being used as the WAN port.
- Dashboard Refresh Performance Enhancement

  Improved UI performance when refreshing Dashboard elements.
- Local Upgrade Enhancement

  Allows the user to upgrade a single AP at a time using an image file from a local PC. A new Local Upgrade button is displayed when the AP is blocked or disconnected due to version mismatch, and clicking this button launches an upgrade page with the option to upgrade each AP individually.
- AP Ethernet Port Status

  The web UI now provides information on AP Ethernet port status, including link status and link speed.
- Uniform Recovery SSID

  Enhanced the AP configure and recovery SSIDs to allow remote wireless configuration of newly installed APs and recovery of isolated mesh APs.
- Support Entitlement Enforcement

  Unleashed remote management will now check for a valid Support Entitlement file. If none is found, a license expired message will be displayed to remind customers to update the license file when the support license has expired.
- Password Recovery

  The Unleashed Setup Wizard now provides an option to enter a Security Email, Security Question and Security Answer to allow you to reset your password in the event that your username or password are forgotten.

- Client Rename Feature

  Connected wireless clients can now be renamed in the Unleashed web UI for easier identification. Manually renaming a client changes its display name in any locations where the client Host Name is displayed.
- AP Reboot Cause Reporting

  Additional reboot causes are provided when a member AP reboots after rejoining an Unleashed Master.
- 2014/53/EU (RED) Compliance

  With this release, Ruckus Access Points are in compliance with the new European Radio Equipment Directive (EU directive 2014/53/EU). Please refer to the Declaration of Conformity insert in the AP box for more information.

Resolved Issues in Build 310

- Resolved an issue that could cause Mesh APs to disconnect when an ACL rule was changed for a WLAN. [ZF-19038]
- Resolved an issue that could prevent users from accessing the Unleashed Setup Wizard via wired Ethernet connection to the AP's default IP address 192.168.0.1 when the AP is in factory default state and there is no DHCP server on the network to assign an IP address to the Unleashed AP. [UN-2503]
- Resolved incorrect UI text description of E510 external antenna settings. [UN-2505]

Resolved Issues in Build 308

- Resolved an issue that could cause R610 traffic graphs to display regular traffic spikes at double the normal rate. [ER-6236]
- Resolved an issue that could cause performance degradation for 802.1X WLANs with certain encryption options enabled. [ER-5956]
- Resolved an issue where guest pass emails would be sent with the default text (in English) for self-service guest passes, even when the text was changed on the *Services* > *Guest Access Service* page. [ER-6142]
- Resolved an issue where guest passes would display an incorrect validity period when users connected to a guest WLAN with *"single shared guest pass among all users"* enabled. [ER-6092]
- Resolved an issue where users connected to a guest WLAN would fail to be redirected to the login page. [ER-5892]
- Resolved an issue where import of guest pass customization file would fail. [ER-5887]
- Resolved a guest pass printout incompatibility issue that could cause guest pass printouts to display incorrectly, if they had been customized in an earlier release before upgrading to release 200.5. [ER-5865]
- Resolved an issue where SMTP server hostnames were limited to 32 characters. [ER-5789]
- Resolved an issue where client fingerprinting would fail to properly identify clients running Windows 10 version 1803. [ER-6414]
- Resolved an issue where ARP packets for internal communications between C110 AP and CM modules could leak out to the cable network. [ER-5985]

Caveats, Limitations and Known Issues

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

- If a Ruckus AP running standalone AP firmware is upgraded to Unleashed 200.6, the "Zero Touch Mesh" feature will not work until another factory reset is performed after upgrade. [UN-2084]

- If a guest pass printout customization was created running Unleashed 200.3 or earlier, the printouts may display incorrect or missing information after upgrading to 200.6. [UN-2383]

  Workaround: Edit and save the existing template after upgrading to 200.6, or create a new one after upgrading and replace the old one.
- The Unleashed Upgrade page allows the user to downgrade a T310 or E510 AP to an unsupported release via local upgrade. As these APs are new in 200.6, they should not be downgradeable to a previous release. Admins should be careful not to accidentally downgrade an AP to an Unleashed build that does not support that AP model. If this does happen, the AP will reboot 5-7 times and then revert to the previous image. [UN-1688]
- The built-in credentials for social media WLANs (other than Facebook) only work when the Master uses the default certificate. If an admin imports a new SSL certificate for the Unleashed Master, he/she will need use his/her own client ID for social media WLAN login. [UN-2374]
- All C110 APs under the same CMTS are isolated by default. [UN-1851]
- Google Pixel and Nexus 6P are not correctly identified by the client fingerprinting feature. [UN-2203]
- Libratone wireless speaker clients fail to properly renew IP addresses from DHCP. [UN-2134]
- Uploading a logo from the mobile app may fail without an error message if the upload is too large. [UN-2251]
- Some clients (including Huawei Honor 8) running certain versions of Chrome browser (including Chrome version 65.0.3325.109) may fail to be redirected to the AAA server login page after connecting to a web auth WLAN due to a compatibility issue with Chrome and HTTPS redirect. [UN-2132, UN-2475]

  Workaround: By default, web auth portal redirection is in forced HTTPS mode. To disable forced HTTPS redirection for web auth WLANs, enter the Master AP CLI and enter the following commands:

  ```
  ruckus# config
  You have all rights in this mode.
  ruckus(config)# no web-portal-force-https-redirection
  The command was executed successfully.
  ruckus(config)#
  ruckus(config)#
  ruckus(config)# show portal-auth-generation
  Force DNS server: Disabled
  Force Web Portal HTTPS Redirection: Disabled
  ruckus(config)#
  ```
- HTTPS redirect for web auth WLANs may fail in Firefox browser (v.59.0.2) due to an SSL certificate error. [UN-2486]

  Workarounds: 1) Click the "Open network login page" button on right top corner of this error page to open the web portal login page in a new tab. 2) Use another browser, such as Chrome v65, Safari 10.1.2, or IE 11.
- Attempting to visit certain websites (e.g., www.google.com) while connected to a "Configure.Me" SSID from an AP in factory default state may fail to launch the Unleashed Setup Wizard. This is due to certain websites' use of HSTS (Hypertext Strict Transport Security), which will cause the browser to refuse to redirect to the Unleashed Setup Wizard page properly without an authenticated third party certificate. [UN-2483]

  Workaround: Try another website that doesn't use HSTS (www.ruckuswireless.com, for example). The browser will redirect to the Setup Wizard.
- Zero-IT profile file fails to download via iOS 11.3 CNA. [UN-2480]

  Workaround: Enable Bypass Apple CNA feature.
- If an Unleashed Master AP is configured with a static IP address, it will retain the static IP address after rebooting and another member AP takes over as Master, rather than switching to DHCP to get a new dynamic IP address. [UN-2159]
- If a Google Social Media WLAN was created prior to upgrading to 200.6 using non-default credentials, it may fail to work after upgrading to 200.6 due to a change in the Google redirection URI. [UN-2501]

Workarounds: 1) Use the default built-in Google account. 2) Change the user's Google account URI settings to add the URI "http://unleashed.ruckuswireless.com/user/auth.jsp " to match with the system.