RELEASE NOTES

Ruckus Wireless Unleashed 200.5 Refresh 2 Release Notes

Supporting Unleashed 200.5

Part Number: 800-71628-001 Rev C
Publication Date: October 2017

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

About This Release

This document provides release information on Ruckus Unleashed release 200.5, including new features, enhancements, known issues, caveats, workarounds, supported platforms and upgrade information for this release.

Introducing Ruckus Unleashed

Unleashed is a controller-less solution from Ruckus Wireless that provides a cost effective, easy to implement, and yet feature-rich solution that is perfect for SMB and home customers. The Unleashed solution scales up to 25 APs and 512 clients. For more information on Unleashed configuration, administration and maintenance, please see the Unleashed Online Help, available at http://docs.ruckuswireless.com/unleashed/200.5/index.html.

Supported Platforms and Upgrade Information

Supported Platforms

Unleashed version **200.5.10.0.283** supports the following Ruckus AP models:

- H320
- H510
- R310
- R500
- R510
- R600
- R610
- R710
- R720
- T300
- T300e
- T301n
- T301s
- T610
- T610s
- T710
- T710s

Upgrade Information

The following release builds can be directly upgraded to Unleashed version **200.5.10.0.283**:

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)
- 200.5.10.0.122 (Unleashed 200.5 Beta)
- 200.5.10.0.179 (Unleashed 200.5 Mobile App Beta)
- 200.5.10.0.235 (Unleashed 200.5 GA Refresh)

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)
- 200.5.10.0.122 (Unleashed 200.5 Beta)
- 200.5.10.0.179 (Unleashed 200.5 Mobile App Beta)
- 200.5.10.0.235 (Unleashed 200.5 GA Refresh)

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: R720

  This release adds Unleashed support for the Ruckus R720 802.11ac Wave 2 Access Point. The R720 is a 4x4:4 dual-band concurrent indoor AP designed for high density indoor applications. The R720 features one 10/100/1000 Ethernet port, and one 100/1000/2500 Ethernet port that supports 802.3af and 802.3at Power Over Ethernet (PoE), and a USB port for IoT applications.

- New Access Point: T610/T610s

  This release adds Unleashed support for the T610 and T610s (sector antenna variant) outdoor 802.11ac Wave 2 Access Points. The T610 is a carrier-grade 802.11ac Wave 2 outdoor AP designed for enterprise and service provider outdoor WLAN applications. The T610 includes dual radios with 4x4:4 spatial streams, two 10/100/1000 Ethernet ports (one port supports PoE input), and 802.1ax Ethernet port aggregation. The T610 also includes a USB port for BLE Smart Beacon, Zigbee or other IoT devices.

  The T610s is the sector antenna version of the T610. It includes all of the same features as the T610.

- New Access Point: H320

  The H320 is an 802.11a/b/g/n/ac "Wave 2" dual band access point with integrated 3-port Ethernet, in a form factor designed for mounting to electrical outlet boxes. The H320 is targeted for hospitality and MDU applications where it will be installed one per room for a typical hotel room. The switch ports can be used for in-room wired applications like IPTV and/or to provide a wired alternative for guest internet access.

  The H320 has one 10/100/1000 Mbps Ethernet port and two 10/100 Mbps Ethernet ports. The Gigabit port on the rear of the unit supports 802.3af PoE input. The PD will identify as a Class 3 device with a max draw of 12.95W.

  NOTE
  The H320 does *Not* support mesh.

Enhancements

Release 200.5 introduces the following new features/enhancements:

- Setup Wizard Enhancement

  The Unleashed Setup Wizard now requires less steps to complete. The "Configuring Unleashed Master" screen is no longer displayed and the reboot is no longer necessary.

- Any URL Redirects to Unleashed Setup Wizard

  When a client connects to the “Configure.Me” setup WLAN, any URL address entered into the browser’s navigation bar will be redirected to the Unleashed setup web interface.

- Enable UPnP and Bonjour service

  This release adds support for Universal Plug & Play (UPnP) for Unleashed AP discovery on Windows networks, and Bonjour, for discovery by Apple/Google devices.

- Enable/disable WLAN per radio

  Users can now manually enable/disable WLAN service per radio. Default is enabled on both radios for any newly created WLANs.

- Guest Access Portal enhancement

  Guest access portal, sponsor login and self service registration pages have been updated.

- SSID Rate Limiting

  Added the option to configure rate limiting on a per-WLAN basis (in addition to the existing per-user rate limiting). If per-SSID rate limiting is enabled, per-user rate limiting is disabled.

- RADIUS Accounting

  AAA server type RADIUS Accounting is now supported.

- Dynamic VLAN

  Dynamic VLAN allows clients to be assigned to VLANs dynamically based on RADIUS group attributes.

- Master CLI Support

  Many controller configuration functions can now be performed via CLI commands issued to the Master AP via SSH or console connection.

- Port Forwarding and WAN Port Protection in Gateway Mode

  Two new features are now available when the Unleashed Master is in Gateway mode. Port forwarding allows the admin to create forwarding rules for forwarding certain types of traffic across the WAN interface. WAN Port Protection allows the admin to configure which types of services are accessible through the WAN port.

- Application Recognition and Control Enhancements

  Enhanced ARC framework to use the same framework as ZoneDirector 10.0.

- Gateway Mode Enhancements
  - ARC support on Master AP
  - Gateway AP Recovery mechanism
  - Merged two DHCP client scripts together
  - Gateway Master now supports Mesh in PPPoE mode
  - The default WAN port for Gateway mode should be a non-PoE port

- Multi-language support:
  - English
  - Brazilian Portuguese
  - Chinese Simplified
  - Chinese Traditional
  - Czech
  - Dutch
  - French
  - German
  - Spanish
  - Swedish
  - Turkish
  - Italian
- Preferred Master

  The "Preferred Master" setting allows customers to select a specific AP to be the Master AP in an Unleashed network, so that if the current Master AP is disconnected, it will have the highest priority to resume the role of Master AP again once it rejoins the Unleashed network. By default, there is no preference as to which AP should become the Master AP; the first (highest capability) AP that is deployed automatically becomes the Master AP.

  Using the Preferred Master setting, users can configure one AP to have priority. Any (non-mesh) AP can become the Master if the preferred Master is offline, but when the Preferred Master comes back online, it will assume the Master role again.

  NOTE
  A Mesh AP cannot be configured as the Preferred Master.

- Ruckus Unleashed Multi-site Manager

  The Unleashed Multi-Site Manager allows customers to manage up to 300 Unleashed networks from a central location, enabling remote administration of multiple Unleashed deployments using a single admin user name and password.

  The Unleashed Multi-Site Manager provides the following critical centralized network management functions:
  - Monitoring - provides the ability to get health status of all Unleashed networks, events & alarms, placement of APs on world map, clients info from dashboard itself.
  - Reporting - Rich reports are available such as Device Inventory, Client association, PCI, Resource Monitoring, Capacity, etc. For more details refer to product documentation.
  - Management - enables to perform several management activities from a central location namely scheduled software upgrade, backup & restore to create cookie cutter configuration to deploy several sites and so on.
- Mobile App Support Remote Management for Multiple Unleashed Networks

  The Unleashed Mobile App version 2.0 now allows customers to perform common monitoring and management functions remotely for up to 10 Unleashed networks. Simply login using a supported Social Media login, add the Unleashed networks to be managed, and start managing them locally as well as remotely.

  Customers do not need to do any complex port forwarding configuration or open firewall ports to enable remote management of Unleashed networks.

  NOTE
  Although not enforced in this release, a Support contract for Unleashed network will be needed for Social Media login-based remote management.

- Mobile App Notification

If enabled, Unleashed will deliver an app notification whenever an alarm is triggered.

Resolved Issues

Resolved Issues in Build 283

- Resolved an issue related to the WPA KRACK vulnerability. For information on security incidents and responses, see https://www.ruckuswireless.com/security. [AP-6463]

  This release fixes multiple vulnerabilities (also known as KRACK vulnerabilities) discovered in the four-way handshake stage of the WPA protocol. The Common Vulnerabilities and Exposures (CVE) IDs that this release addresses include:

  – CVE-2017-13077
  – CVE-2017-13078
  – CVE-2017-13079
  – CVE-2017-13080
  – CVE-2017-13081
  – CVE-2017-13082

  Client devices that have not yet been patched are vulnerable to KRACK attacks. To help protect unpatched client devices from KRACK attacks, Ruckus strongly recommends running the CLI commands below:

  ```
  ruckus# config
  ruckus(config)# system
  ruckus(config-sys)# eapol-no-retry
  ```

  Use the following command to disable:

  ```
  ruckus(config-sys)# no eapol-no-retry
  ```

  Enabling the eapol-no-retry feature (disabled by default) prevents the AP from retrying packets in the key exchange process that have been found to be vulnerable to KRACK attacks. Note that enabling this feature may introduce client connectivity delay in high client density environments.

  For more information about KRACK vulnerabilities, visit the Ruckus Support Resource Center at https://support.ruckuswireless.com/krack-ruckus-wireless-support-resource-center.

- New CLI commands for configuring WLAN QoS settings on the Master AP are now supported. [UN-1593]

Resolved Issues in Build 235

- Resolved an issue that could cause kernel panic in Unleashed APs running release 200.4. [ER-5664]

Caveats, Limitations and Known Issues

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

- The Setup Wizard web page closes automatically after clicking "Finish" when setting up the network using Mac OS. [UN-1180]
- Firefox and Chrome browsers fail to automatically redirect to the Setup Wizard page when the default home page is used. [UN-988]

  Workaround: Users must manually input any URL in the browser to be redirected to the Unleashed Setup Wizard.

- Member AP fails to get an IP address when LAN port is connected to an ICX 6430-C12 switch with STP enabled. [UN-1211]
- Gateway Master recovery limitations: [UN-1205]
  - Per-AP configuration settings will be lost when a member AP becomes the new Master AP.
  - Per-AP settings will be lost when a previous Master AP rejoins the network as a member AP.
  - Any configuration changes made less than one day before a Master recovery occurs will be lost.
- Unleashed fails to redirect clients associating to a Facebook Wi-Fi WLAN to a URL that is longer than 450 characters. [UN-1438]
- The URL displayed in the browser's navigation bar will still include the original domain name after redirecting to the Unleashed setup wizard page. [UN-1435]
- Some 802.11k enabled clients are not sending Neighbor report requests after association. [UN-1390]
- Zero-IT apk file does not properly install after registration for Moto X Style clients running Android version 6.0. [UN-1343]
- Zero-IT provisioning file is not properly downloading for some Android clients running older versions of Chrome browser. [UN-1342]
- Alarm notification and remote management messages have not been translated and remain in English when the system language is other than English. [UN-1319]
- Special characters such as "< > { } ;" are not supported in Hotspot user names and passwords. [UN-1060]
- The pre-launch browser is not appearing when the Bypass Apple CNA feature is disabled for WISPr and Guest Access authentication. This means that users will have to launch a Safari browser window to be able to complete guest authentication. [UN-444]
- The Unleashed web interface does not properly display the OS type for several device categories, including Blackberry, Chrome OS, Playstation, and printers. [UN-316]
- Per-model LED settings and global WLAN service settings may be overridden after upgrading from 200.1 to 200.5. [UN-1511]

  Workaround: Manually reconfigure those settings after upgrading if you encounter this issue.