Unleashed 200.7 Release Notes

Supporting Unleashed 200.7

Copyright, Trademark and Proprietary Rights Information

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.ruckuswireless.com/unleashed/200.7/index.html*.

Supported Platforms and Upgrade Information

Supported Platforms

Unleashed version **200.7.10.2.339** 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

> **NOTE**
> The M510 and R320 are new in this release.

Upgrade Information

The following release builds can be directly upgraded to Unleashed version **200.7.10.2.339**:

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)

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)

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

This release adds Unleashed support for two new APs: Unleashed M510 and Unleashed R320.

- Unleashed M510

    This release adds Unleashed support for the M510 Wave 2 802.11ac LTE Wi-Fi access point (AP). The M510 is designed to leverage LTE networks as a backhaul to connect wirelessly back to any network without the need for an Ethernet cable connection.

- Unleashed R320

    The R320 is an entry-level 2x2:2 802.11ac Wave 2 indoor AP designed for medium-density enterprise deployments. It features one GbE port, dual 2.4/5 GHz radios, BeamFlex support, 802.3af/at PoE support and a small form factor for flexible installation.

Enhancements/New Features

Release 200.7 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

Caveats, Limitations and Known Issues

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

Issue	UN-2817
Description	5 GHz SSIDs fail to deploy immediately after completing the CLI setup wizard when DFS channels are used.

Issue	UN-2855
Description	Windows 10 clients running Chrome version 70.0.3538.67 may not properly redirect to the setup wizard screen when attempting to configure an AP in factory default state.

Issue	UN-2936
Description	Guest login pages may display incorrect language after changing the language setting.

Issue	UN-2480
Description	iOS 11.3 devices may fail to download Zero-IT profiles using the onboarding portal. Workaround: Enable Bypass Apple CNA feature in WLAN settings.

Issue	UN-2990
Description	M510 does not support hot-swapping SIM cards. Removing and reinserting a SIM card or replacing a SIM card with another one will require an AP reboot to bring the new SIM card into service.

Issue	UN-2802
Description	Upload progress indicator does not display correctly in Microsoft Internet Explorer and Edge browsers.

Issue	UN-3035
Description	Android clients are unable to download the Zero-IT activation file when connected to a guest network via CNA.

Issue	UN-3034
Description	Mac OS clients are unable to download the Zero-IT activation file when connected to a guest network via CNA.

Issue	UN-3031
Description	801.1X Zero-IT profiles are not created properly for Windows 10 OS version 17134.407 clients. Clients are prompting for username and password when connecting.