RUCKUS Edge Release Notes, 2.2.0

Supporting RUCKUS Edge 2.2.0 Release

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

Document History

TABLE 1 Document History

Revision	Summary of changes	Publication date
A	Key features and enhancements • Active-Active HA support for DMZ cluster • Fallback support for Active / Active Clustering • Personal Identity networks (PIN) For Campus Housing w/ DHCP and NAT support	18th December 2024

New in This Release

The RUCKUS Edge 2.2.0 release supports the following hardware and software features.

Product Information

This RUCKUS Edge 2.2.0 release is a General Availability (GA) release. This section lists each components in this release.

RUCKUS Edge Information

• RUCKUS Edge Firmware Version : 2.2.0.1066

• RUCKUS AP Firmware Version: 7.0.0.400.6554

• RUCKUS Switch Firmware Version: 10.0.10f

New in this Release

This section provides a high-level overview of several key features that are introduced in the RUCKUS Edge software release.

The following are the key features in RUCKUS Edge 2.2.0 release.

TABLE 2 Key Features and Enhancements

Feature	Description
4-Node Clustering with Active-Active High Availability	The Active-Active High Availability mode provides load balancing, scalability and redundancy . There can be minimum 2 or maximum 4 edges in the Cluster operating in Active-Active mode. With SDLAN-Service, these edges can simultaneously manage tunnels from APs
Active-Active HA support for DMZ cluster	Ensures AA HA support for DMZ cluster.
Fallback support for Active-Active Clustering	Allows an AP to reconnect to the preferred primary RUCKUS Edge device according to the user-configured schedule.
Personal Identity networks (PIN) For Campus Housing for DHCP and NAT support (Early Access)	Personal Identity Networks (PIN) use VxLAN tunneling to extend Wi-Fi client and wired client via RUCKUS switch access to the RUCKUS Edge, creating seamless connectivity across the network domain. It enables Wi-Fi and wired clients to securely access their networks and connected devices while also establishing Personal Area Networks (PAN) for secure, individualized connectivity.

TABLE 3 Commands in this Release

Command Name
Updated: show peer-tunnel
Updated: show peer-tunnel ka
New: show pin-info (Early Access)
New: show pin-pan (Early Access)

Product Support

This section provides information on customer service and support team details.

How Do I Get Support?

For product support information and contact details of the RUCKUS Customer Services and Support Team, go to the Support Portal https://support.ruckuswireless.com or https://www.ruckuswireless.com and select **Support**.

Hardware and Software Support

Overview

This section provides release information about the RUCKUS Edge device.

- All configuration changes must be performed in the designated maintenance window
- Switching the **Load Distribution** method between **Random** and **Per AP Group** in the cluster's HA settings will alter the active Edge device to which an AP connects, causing a service disruption.

Known Issues in Release 2.2.0

Known Issues

The following table provides information on the known issues and limitations in the current release.

Issues	Description
ECD-4866	**Symptom**: In Edge2, when the LAN port is reconnected to Edge1, it is observed that the log in Edge2 changes to VRRP_ROLE_BACKUP for a brief period and then reverts to VRRP_ROLE_MASTER. **Condition**: In the ESXi environment using vSwitch, initially, Edge1 is active and Edge2 Backup. When it is disconnected and then reconnected to the LAN port connected to the vSwitch on Edge1, the Edge 2 changes from **Master** to **Backup** for a brief period before reverting back to **Master**. **Workaround**: None

Issues	Description
ECD-5492	**Symptom**: Sometimes modifying the VRRP configuration (virtual IP or HA timeout) or applying or removing SD-LAN service may result in the backup node to go into **Initialize** state (for a 60 seconds) and then return to **Backup** state. **Condition**: Join 2-node Edge Cluster to RUCKUS One and complete the Port General, Cluster IP, Virtual IP settings for the cluster. Changing the VRRP configuration (Virtual IP or HA timeout). Applying / removing SD-LAN service. **Workaround**: None

ECD-5149	**Symptom**: The Cluster role may change when recovering the LAN interface because by default, ICX has fast-span enabled for all the ports in the system. However, this property is lost when port becomes a TAGGED member of any VLAN, for example: fast-span is automatically disabled as soon as a port becomes TAGGED port. As a result, the Cluster role may change when recovering the LAN interface.
	Condition: ICX has fast-span enabled for all the ports in the system. However, this property is lost when port becomes a TAGGED member of any VLAN i.e fast-span is automatically disabled as soon as a port becomes TAGGED port.
	
	Workaround: Work around to configure on ICX Switch.
	
	1. Run 802.1W instead of spanning-tree on the VLAN. For example:
	
	```\nSwitch(config-vlan-1)#spanning-tree 802-1w\nSwitch(config-vlan-10)#spanning-tree 802-1w\n```
	
	2. Configure these ports are rstp/802.1w admin edge ports.
	
	This will ensure interface 1/1/4 is always considered as an edge port & does not go through regular Spanning state transitions. For example:
	
	```\nConfigure the ICX Switch port that is connected to the SmartEdge.\nSwitch(config-if-e2500-1/1/4)#spanning-tree 802-1w admin-edge-port\n```

ACX-66646	**Symptom**: Control packet is not prioritized on the Edge. **Condition**: User can experience slowness when trying to configure RUCKUS One if there are a lot of data traffic. **Workaround**: None
ACX-65424	**Symptom**: When creating an SD-LAN profile, the same Captive Portal network enables the Data Center (DC) tunnel across different venues, but under the **show sdlan config** command, it displays a tunnel-to-peer connection because currently Edge can only identify, and forward traffic based on VLAN ID, not WLAN ID. So networks with same VLAN IDid will all have the same behavior. This caused the RUCKUS One GUI and Edge CLI (**show sdlan config**) display conflicts and it will confuse users. **Condition**: If two different networks configured with same VLAN ID and both tunneled to DMZ at beginning. Then when user turned off one of them from tunneling to DMZ, it does not change the behavior of that network. It will still be tunneled to DMZ since another network with same VLAN ID is still tunneling to DMZ. **Workaround**: None
AP-35820	**Symptom**: Ensure that the **vxlan config** is present on the AP and **rvxlanmgr** is running. Disable **vxlan** via CLI/**R1 GUI** and reboot the AP. This can cause **rvxlanmgr** to crash. **Condition**: **rvxlanmgr** can crash. **Workaround**: None
ACX-68692	**Symptom**: After onboarding, during E144 upgrade to target version of venue, user will see two attempts to upgrade, the first one will be failed. The upgrade will be succeeded eventually. **Condition**: E144 loaded with **2.1.0.852** only. **Workaround**: No workaround, this is design intent.

Issues	Description
AP-38092	**Symptom**: AVPD crash is seen on R670, T670, and R770 APs. **Condition**: Issue is seen when both FQDN and IP address are configured in the same rule in Wi-Ficalling profile. Day-1 issue on the RUCKUS One controller UI. Due to Wi-Fi calling configuration data-structure corruption, during packet-processing, it is going for a crash. **Workaround**: Remove the IP address from the WFC profiles.
ACX-74102	**Symptom**: The PIN for Edge of DHCP - the UE can't get the IP when configuration mix mode internal DHCP + external DHCP. **Condition**: 1. Turn on the PIN and Sub-interface FF on the RUCKUS One. 2. Set up two SmartEdge(SE1 and SE2) with three interfaces (WAN, LAN and Cluster) and onboard to RUCKUS One tenant via the "Add -> Cluster" 3. Completed the enroll progress and waiting for the SmartEdge status in the "Need Ports Config" Test Steps:Now, when the PIN profile configuration is the setup of an external DHCP pool for PIN UE, set up an internal DHCP pool for WebAuth. The UE will not get the IP address. The PIN profile only allows configuration;1. WebAuth - internal DHCP, and PIN-UE internal DHCP2. WebAuth - external DHCP, and PIN-UE external DHCP NOT allows;1. WebAuth - internal DHCP, and PIN-UE external DHCP2. WebAuth - external DHCP, and PIN-UE internal DHCP. **Workaround**:
ACX-74002	**Symptom**: Adding a Single Edge on RUCKUS One, PIN will not work. **Condition**: Customer wants to enable a single Edge for the PIN feature, it does not work. **Workaround**: Add a Cluster as Active-Standby mode and add only one Edge serial number. Run Cluster & RUCKUS Edge configuration wizard to configure port IP (WAN, LAN, Cluster) and assign virtual IP.
ACX-73340	**Symptom**: Edge cannot apply DHCP pool setting. **Condition**: A single node Edge cluster which is created before 2.2 will hit this problem. **Result**: DHCP pool settng is not applied. **Workaround**: Add another Edge into this cluster to form Active-Backup Cluster can solve this problem. **Recovery**: No recovery action is available.
ACX-72843	**Symptom**: The HA mode column display either AA or AS as the default HA mode to a single node Edge. **Condition**: 1. Fresh install RUCKUS Edge. 2. Add RUCKUS Edge on the upper-right conner. 3. Onboard RUCKUS Edge to the RUCKUS One with ZTP, Virtual Edge do SCEP enrollment. 4. Complete the port configuration setup. **Workaround**:
FI-305065	Few APs connected to ICX8200 stack in density network are not getting IP address from the DHCP server. **Customer Symptom for Publication**: ICX8200 drop unicast DHCP offer/ack packets when it is configured as a relay/l2-forwarding device. **Conditions for Publication**: ICX8200 drop unicast DHCP offer/ack packets if DHCP client send request packet with unicast flag set. **Workaround**: Send discover packet from client with broadcast flag set.

Issues	Description
ACX-69471	**Symptom**: Edge may report a **Firmware update failed** status after a successful upgrade to 2.2.0.1066. **Conditions**: This issue might arise in rare instances during the upgrade process. It has been resolved in version 2.2.0.1066. **Workaround**: To address this issue, delete the affected Edge device and re-enroll it. This action will initiate a new upgrade attempt.