RELEASE NOTES

RUCKUS Edge Release Notes, 2.1.0

Supporting RUCKUS Edge 2.1.0 Release

Part Number: 800-73359-001 Rev A

Publication Date: October 2024

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	Added new Hardware appliance support - E144 and other new features of RUCKUS Edge build 2.1.0.xxx.	16th October 2024

New in This Release

The RUCKUS Edge 2.1.0 release supports the following hardware and software features.

Product Information

This RUCKUS Edge 2.1.0 release is a General Availability (GA) release. This section lists each components in this release.

RUCKUS Edge Information

- RUCKUS Edge Firmware Version : 2.1.0.971
- RUCKUS AP Firmware Version: 7.0.0.200.6407

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 for Early Access release.

TABLE 2 Key Features and Enhancements

Feature	Description
Link Aggregation Group	The link aggregation is a mechanism to bundle or aggregate one or more physical interfaces into a single logical interface.
Software Defined Local Area Network (SD-LAN)	Software defined local area network provides centralized forwarding for RUCKUS Access Points.
High Availability	The High Availability (HA) for Edge enables the network to operate continously without failing.
New Hardware Platform Support - E144	Support of new hardware platform - RUCKUS Edge 144
Graceful Shutdown	This is to have an option for an end user to perform a graceful shutdown of the RUCKUS Edge in RUCKUS One.
Zero Touch Onboarding for RUCKUS Edge 144	RUCKUS Edge appliances will have a similar Zero touch onboarding process. User will take the Serial number from the appliance box and enter that into RUCKUS one. The customer can also scan the serial number from the phone app, if prefered. Once that is entered, the customer can plug the device into any single port on the appliance. If the device can get a DHCP address and has access to the internet it will automatically connect with RUCKUS One.
KVM Hypervisor support	Supports for the KVM Hypervisor.
Multiple Venue Support for Edge - SDLAN	Supports multiple venues talking to a single Edge.

TABLE 2 Key Features and Enhancements (continued)

Feature	Description
VXLAN-GPE Extensions	Supports VXLAN-GPE Extensions. GPE extensions are required to add information such as WLAN ID No., VLAN Information, etc... that allows to extend standard based VXLAN to have more information.
Vxlan tunnel keepalive between AP and Edge needed	VxLAN tunnel keepalive between AP and RUCKUS Edge.

TABLE 3 Commands Introduced in this Release

Command Name
cfgmgr
cluster
connect-agent
enroll-device
featureflag
logging
network
packet-capture
ping
reboot
reset
resource-manager
rproxy
set default gateway
set dns server
set interface
set internal-network
set log level
show default gateway
show dns server
show interface address
show internal network
show lacp
show lacp details
show lag
show lag details
show log level
show peer-tunnel
show peer-tunnel ka
show pin-info
show pin-pan
show resource manager
show route
show sdlan config
show sdlan counters

TABLE 3 Commands Introduced in this Release (continued)

Command Name
show sdlan info
show sdlan mac
show sdlan peer
show sdlan summary
show status
show tunnel profile
show version
show vxlan config
show vxlan dstats
show vxlan pmtu table
show vxlan tunnel
show vxlan tunnel profile
show vxlan-gpe config
show vxlan-gpe dstats
show vxlan-gpe pmtu table
show vxlan-gpe tunnel
show vxlan-gpe tunnel keepalive session
start dhcp client
stats
stop dhcp client
support-core
support-export
support-log
switch-over
system
traceroute

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**.

Known Issues in Release 2.1.0

Known Issues

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

Issues	Description
ECD-5347	**Symptom**: The HA vrrp event of VRRP IPv4 Instance ID 250 transitioned from INITIALIZE to BACKUP does not show up after Active Node Failure Failure Recovery (this is a random probability issue). **Condition**: Turn on the R1 HA and SD-LAN FF on the RUCKUS Edge:R1 HA FF: edge-ha-toggleR1 SD-LAN FF: edge-sdlan-ha-toggle **Set up two Edge(SE1 and SE2) with two interfaces** > **Go to the Edge list, click Add > Cluster, then use the Cluster name, the Venue-name, and the SE1 and SE2 Serial Number** > **Complete the enrollment process for SE1/SE2** > **Set up the SE1/SE2 core-lan port and cluster port configuration, waiting for the Cluster status Ready2/2, and the SE1 is Standby-node, SE2 is the Active-node Create the SD-LAN profile use the vxlan-vlan and apply to the WLAN-vlan60** Test Steps **UE connects to the WLAN and starts ping 8.8.8.8 and ping 192.168.60.254(GW)** > **Check the Active-node cluster status and vrrp status, then shut down the (SE2)Active-node** > **Check the SE1 correct become to Active-node and UE traffic correct ping out** > **Bootup the SE2, after the SE2 bootup check the event of "VRRP IPv4 Instance ID 250 transitioned from INITIALIZE to BACKUP" on the seinfra-events-55dbf9b6d5-tgvgz** **Workaround**: None
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
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 R1 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:
	`Switch(config-vlan-1)#spanning-tree 802-1w`
	`Switch(config-vlan-10)#spanning-tree 802-1w`
	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:
	`Configure the ICX Switch port that is connected to the SmartEdge.`
	`Switch(config-if-e2500-1/1/4)#spanning-tree 802-1w admin-edge-port`

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

Issues	Description
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
ACX-65315	**Symptom**: When the client traffic is to be tunneled between AP and the Edge device, an unexpected incident **VLAN mismatch found in Venue:** <*Venue Name*> is generated by RA. **Condition**: Clients should be connected on user VLANs to the tunneled Wireless networks. **Workaround**: None
ACX-64828	**Symptom**: After disabling the DMZ tunnel in an existing SD-LAN profile, the **Uplink-Conn-Types** information does not update in the Data Center (DC) cluster when running the **Network# show sdlan config** command. Because currently Edge can only identify, and forward traffic based on VLAN ID, not WLAN ID. So networks with same VLAN ID 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
ACX-64022	**Symptom**: After deleteing RUCKUS Edge 144 from RUCKUS One, the interface MAC address may change. RUCKUS Edge 144 may not connect back to RUCKUS One after user delete the Edge device. **Condition**: After deleting RUCKUS Edge 144 from RUCKUS One, there is a very little chance that the interface MAC address may change. In normal case, it does not impact the Edge 144 boot up with manufacturing firmware and connect back to RUCKUS One. **Workaround**: Do not bundle the Edge MAC address in the DHCP server. To recover RUCKUS Edge 144, reboot the device.
ACX-68709	**Symptom**: After onboarding, there are chances that Edge might display configuration update failed. UI displays incorrect status. **Condition**: Randomly happens after onboarding before setup wizard, or device trigger golden reset locally on device itself. **Workaround**: Apply any new configuration to retrigger configuration, update process will fix it. This is a status display issue, no need to recover.
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.
ACX-68520	**Symptom**: The number of Active APs is displayed as 0 on the R1 Web UI if the RUCKUS Edge is a single-node cluster. UI displays incorrect number. **Condition**: RUCKUS Edge is a single-node cluster. **Workaround**: No workaround.

Issues	Description
ACX-68794	**Symptom**: Network configuration fails when setting up interfaces via RUCKUS One. The configuration fails due to a network domain conflict. Multiple interfaces have IP addresses in the same subnet, leading to conflicts. **Condition**: Multiple network cables are connected to the same broadcast domain. That are able to receive IP addresses from a DHCP server. One interface is changed from DHCP to a static IP configuration within the same network domain as the DHCP server. For example, the DHCP server provides addresses in the 10.10.10.0/24 subnet, and the interface is manually configured with the static IP 10.10.10.200/24. **Workaround**: The device can still be managed via R1. The following steps are recommended: 1. Disconnect Unnecessary Cables Remove any redundant cables connected to the same broadcast domain before configuring network settings to prevent IP address conflicts. 2. Ensure Unique Network Domains for Interfaces Avoid assigning IP addresses from the same network domain to different interfaces. Each interface should be on a separate subnet to prevent network conflicts.

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com