RELEASE NOTES

FastIron 10.0.20 for RUCKUS ICX Switches Release Notes Version 1

Supporting FastIron Software Release 10.0.20

Part Number: 53-1005797-01
Publication Date: 27 March 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

Version	Summary of changes	Publication date
FastIron 10.0.20 for ICX Switches Version 1	• New software features and enhancements • Known and Resolved issues	March 27, 2024

Introduction

About RUCKUS FastIron Release 10.0.20

FastIron release 10.0.20 introduces several new features and manageability enhancements. Key additions include the following:

- BGP EVPN VXLAN
- Enhanced ICX visibility
- RADIUS enhancements
- Flexible authentication enhancements
- IP performance metrics
- Syslog enhancements, including RFC 5424 format
- Layer 2 Trace Route
- IPv6 supportsave support
- OpenFlow support for ICX 7550 devices
- PTP-TC support for ICX 8200 devices
- IPoE-tagged VLANs
- DHCP enhancements
- PPPoE Intermediate Agent

Refer to Software Features on page 11 for a detailed list of features and enhancements in the Fastron 10.0.20 release.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckusnetworks.com.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckusnetworks.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.ruckuswireless.com
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

New in This Release

Hardware

No new switch models were introduced in FastIron release 10.0.20.

Software Features

The following section lists new, modified, and deprecated software features in release 10.0.20.

New Software Features in 10.0.20

The following software features and enhancements are introduced in this release. Refer to the *RUCKUS FastIron Features and Standards Support Matrix*, available at support.ruckuswireless.com, for a detailed listing of feature and platform support.

NOTE

If you are a RUCKUS One user, RUCKUS recommends that you upgrade to the recommended version listed on the version management page.

Feature	Description
BGP EVPN VXLAN	Border Gateway Protocol (BGP) Ethernet Virtual Private Network (EVPN) provides an efficient control plane protocol for a VXLAN. When BGP EVPN is configured for a VXLAN, remote Virtual Tunnel End Points (VTEPs) and Virtual Network Identifiers (VNIs) do not need to be manually configured, and remote MAC addresses can be learned via the control plane. VTEPs in a VXLAN can use BGP EVPN to exchange locally learned Layer 2 and Layer 3 destinations with remote VTEPs. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide* for more information.
Apply an ACL to Multiple Interfaces Simultaneously	You can apply an existing ACL to a range of interfaces simultaneously. Refer to the *RUCKUS FastIron Security Configuration Guide* for more information.
RADIUS Location Attribute	A vendor-specific attribute (VSA) for a RUCKUS location can be configured for RADIUS authentication requests. The RUCKUS location is configured with the new **host-location** command. Refer to the *RUCKUS FastIron Security Configuration Guide* for more information.
Flexible Authentication Accepts a VLAN Group Attribute	If you configure a VLAN group with the **vlan-group** command, it is included in RUCKUS VSA options in RADIUS request messages. The VLAN group is supported by the Tunnel-Private-Group-ID (TPGID) attribute. Refer to the *RUCKUS FastIron Security Configuration Guide* for more information.

Feature	Description
Allow an 'auth-fail' Client to Remain in the Auth-Default VLAN (Flexible Authentication)	In Flexible authentication, the action in response to a failed authentication can be configured as "permit" to place the client in the authentication default VLAN. The failure is logged, but the client is not blocked. The "permit" option can be configured globally or at the interface level. Refer to the *RUCKUS FastIron Security Configuration Guide* for more information.
Enhancements to DHCP Option 82 and DHCP Option 37 Relay Agent Information	Additional security allows a switch to act as the DHCP relay agent to present requests from non-trusted sources. Refer to the *RUCKUS FastIron DHCP Configuration Guide* for more information.
Layer 2 Trace Route Utility	This feature traces the traffic path through a specified device in a VLAN. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide* for more information.
IPoE S-tag and C-Tag VLANs	When configuring selective Q-in-Q tunneling, customer VLANs (CVLANs) can be added or replaced, enhancing traffic management capabilities in environments where complex VLAN handling is required. When Internet Protocol over Ethernet (IPoE) service-tagged (S-tag) and customer-tagged (C-tag) VLANs are enabled, traffic from different clients or tenants can be segregated, ensuring the efficient use of available VLAN IDs and simplifying the network configuration. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide* for more information.
Assigning Different VLAN IDs to Reserved VLANs	The **reserved-vlan-map** command now allows VLAN 4090 to be reassigned in addition to VLANs 4091 and 4092. Refer to the *RUCKUS FastIron Layer 2 Switching Configuration Guide* for more information.
Image Consistent Check Before Stack Reload	This feature prevents the stack from reloading if the user triggers a reload, and an appropriate error message notifies the user of the image version mismatch. Refer to the *RUCKUS FastIron Software Upgrade Guide* and the *RUCKUS FastIron Stacking Configuration Guide* for more information.
Point-to-Point Protocol over Ethernet Intermediate Agent (PPPoE IA)	Point-to-Point Protocol over Ethernet Intermediate Agent (PPPoE IA) acts as another level of security between the host and the broadband remote access server by intercepting all PPPoE Active Discovery (PAD) messages on a per-port basis. Refer to the *RUCKUS FastIron Management Configuration Guide* for more information.
NTP Server Start Delay	The NTP server response from an ICX switch can be delayed until the ICX switch itself has synchronized with an external NTP server. This can be used when an ICX switch is being used as both an NTP server as well as a client. Refer to the *RUCKUS FastIron Management Configuration Guide* for more information.
CLI Banner Support for Unicode Characters	The banner now can include French Unicode characters. Refer to the *RUCKUS FastIron Management Configuration Guide* for more information.
Time Zone Enhancement	Once the start and end day of the month are configured, the recurring summer-time settings are automatically applied each year. Refer to the *RUCKUS FastIron Management Configuration Guide* for more information.
Precision Time Protocol Support on ICX 8200 Devices	Precision Time Protocol (PTP-TC) feature support has been added for ICX 8200 devices. Refer to the *RUCKUS FastIron Management Configuration Guide* for more information.
1-Gbps Support on 10-Gbps Copper GBIC	'1000-full' support is added on 10-Gbps Copper gigabit interface converter (GBIC) optics. Refer to the *RUCKUS FastIron Management Configuration Guide* for more information.

Feature	Description
4 x 10-Gbps Breakout Support	4x10G breakout support is added on RUCKUS ICX 7550 24ZP and ICX 7550 24F devices. Refer to the *RUCKUS FastIron Management Configuration Guide* for more information.
IP Performance Metrics (IPPM)	IP Performance Metrics (IPPM) supports the monitoring of metrics related to IPv4 and IPv6 data. IPPM generates traffic and reports the statistics to the administrator through syslog messages. IPPM is configured through profiles and can monitor statistics such as jitter, round-trip time (RTT), time to live (TTL), and response time. Refer to the *RUCKUS FastIron Monitoring Configuration Guide* for more information.
RFC 5424 Syslog Enhancements	When RFC5424 is enabled, the syslog format includes additional information such as detailed time, structured data, hostname, domain name, and the syslog sequence ID. Refer to the *RUCKUS FastIron Monitoring Configuration Guide* for more information.
Syslog Output Enhancements	Information is added to the output of Telnet and SSH messages, including the address of the specified port, the specified destination IP address, and the destination port. Refer to the *RUCKUS FastIron Monitoring Configuration Guide* for more information.
Supportsave Support over IPV6 Protocol	IPv6 supports the **supportsave** command. Refer to the *RUCKUS FastIron Monitoring Configuration Guide* for more information.
OpenFlow Support on ICX 7550 Devices	Software-defined networking (OpenFlow) is supported on ICX 7550 devices beginning with this release. Refer to the *RUCKUS FastIron SDN Configuration Guide* for more information.
RESTCONF support for IPPM	RESTCONF support is added for the IPPM profile configurations. Refer to the *RUCKUS FastIron RESTCONF Programmers Guide* for more information.
RESTCONF support for Watcher Profile Name	RESTCONF support is added for the watcher profile name. Refer to the *RUCKUS FastIron RESTCONF Programmers Guide* for more information.
RESTCONF support for Slot Profile	RESTCONF support is added to configure the slot 2 module ports to uplink 40-Gbps and 100-Gbps ports on RUCKUS ICX 7550-24ZP and ICX 7550-24F devices. Refer to the *RUCKUS FastIron RESTCONF Programmers Guide* for more information.
RESTCONF support for Breakout Port	RESTCONF support is added for the breakout settings. Refer to the *RUCKUS FastIron RESTCONF Programmers Guide* for more information.

Important Changes in Release 10.0.20

NOTE

Refer to Software Features on page 11 for a list of new features in this release. Refer to the *RUCKUS FastIron Features and Standards Support Matrix*, available at https://support.ruckuswireless.com/, for a detailed listing of feature and platform support.

Enabling SSH Communication Between 10.0.10c Devices and 08.0.95 Devices

Due to the differences in default key exchange and host key algorithms in different FastIron releases, devices running different releases may experience SSH connection issues.

For devices running FastIron release 09.0.10 and later, when trying to establish an SSH connection with a device running FastIron release 08.0.95 or earlier, a mismatch in algorithms prevents the SSH connection from being established. The problem arises during the negotiation phase, where the server offers key exchange and host key algorithms that are not compatible with the default settings of the device running FastIron release 09.0.10 or later.

For devices running FastIron release 10.0.10c and later, RUCKUS recommends configuring specific key exchange and host key algorithms on the devices to resolve this issue and enable SSH communication. Perform the following procedure to enable SSH communication with devices running FastIron release 08.0.95 or earlier:

```
device# configure terminal
device(config)# ip ssh key-ex
  key-exchange-method           SSH key exchange method
device(config)# ip ssh key-exchange-method
  ASCII string   Enter algorithms separated by a space:
                 diffie-hellman-group-exchange-sha256
                 diffie-hellman-group14-sha256
                 diffie-hellman-group16-sha512
                 diffie-hellman-group18-sha512
                 curve25519-sha256@libssh.org
                 diffie-hellman-group14-sha1
                 ecdh-sha2-nistp256
                 ecdh-sha2-nistp384
                 ecdh-sha2-nistp521
                 curve25519-sha256
device(config)# ip ssh key-exchange-method diffie-hellman-group14-sha1
device(config)# ip ssh host
  host-key-method               SSH host key method
device(config)# ip ssh host-key-method
  ASCII string   Enter algorithms separated by a space:
                 ecdsa-sha2-nistp256
                 ecdsa-sha2-nistp384
                 rsa-sha2-512
                 rsa-sha2-256
                 ssh-rsa
device(config)# ip ssh host-key-method ssh-rsa
```

ICX 8200 Multigigabit Support in FastIron 10.0.10b

ICX 8200 switches with multigigabit support that are shipped with FastIron release 10.0.10b can be downgraded, if necessary, to FastIron release 10.0.10a; however, they should not be downgraded to earlier releases due to driver incompatibilities.

In the case of an unintentional downgrade, the switch can be recovered by booting with the golden image using the following steps.

1. Make a console connection to the switch.
2. Continuously enter **b** to stop at the boot prompt.
3. Enter the command **boot_golden_primary** or **boot_golden_secondary**.

AAA authentication Behavior Changes in FastIron Release 10.0.10a

From FastIron release 10.0.10a, there is a behavior change for the AAA authentication method-list TACACS+ option. The **aaa authorization exec default tacacs+** command must be configured before the **aaa authentication login default tacacs+** command or the **aaa authentication enable default tacacs+** command can be configured. If you attempt to configure either of these commands first, the following message is displayed:

```
Warning- Please configure exec authorization using TACACS+ to get user privilege.
```

From FastIron release 10.0.10a, there is also a behavior change for the AAA authentication method-list RADIUS option. The **aaa authorization exec default radius** command must be configured before the **aaa authentication login default radius** command or the **aaa authentication enable default radius** command can be configured. If you attempt to configure either of these commands first, the following message is displayed:

```
Warning- Please configure exec authorization using RADIUS to get user privilege.
```

Strict Password Enforcement Available in FastIron Release 10.0.10

Strict password enforcement, reintroduced in FastIron release 10.0.00a, is also available from FastIron release 10.0.10. When strict password enforcement is enabled, new passwords must be a minimum of 15 characters and must meet other requirements. Refer to the *RUCKUS FastIron Security Configuration Guide* for configuration details.

CLI Commands

The commands listed in this section were introduced, modified, or deprecated in FastIron release 10.0.20.

Reintroduced Commands for FastIron 10.0.20

The following command has been reintroduced in this release.

- **trace-l2**

New Commands for FastIron 10.0.20

The following commands have been added (new for this release):

- **action**
- **address-family l2vpn evpn**
- **arp-suppression**
- **clear pppoe intermediate-agent**
- **delay-server**
- **dhcp-relay information**
- **dhcpv6-relay information**
- **encapsulation vxlan**
- **evpn-instance**
- **evpn-instance range**
- **host-location**
- **host-reachability protocol bgp**
- **inspect**
- **ip evpn prefix-list**
- **ip tcp analytics rate**
- **ippm profile**
- **jitter threshold**
- **l2vpn evpn**

- **mac duplication limit**
- **match evpn-route-type**
- **match evpn-vni**
- **match ip address evpn-prefix-list**
- **my-mac advertise**
- **pppoe intermediate-agent**
- **rd** (VNI)
- **rfc-8365-compat-disable**
- **route-target export**
- **route-target import**
- **rtt**
- **schedule start**
- **show access tcam group**
- **show dhcpv4-relay information**
- **show dhcpv6-relay information**
- **show ip bgp evpn attribute-entries**
- **show ip bgp evpn neighbors**
- **show ip bgp evpn routes**
- **show ip bgp evpn summary**
- **show ippm profile**
- **show l2vpn evpn**
- **show pppoe intermediate-agent**
- **show watcher**
- **slot 2 uplink-40g**
- **trace-l2**
- **ttl_threshold**
- **type layer2-extension evpn**
- **watcher name**
- **watch ippm**
- **type layer2-extension evpn**
- **unknown-ucast-suppress**
- **vni**

Modified Commands for FastIron 10.0.20

The following commands have been modified (updated for this release).

- **arp**
- **auth-fail-action**
- **authentication fail-action**
- **banner**

- **client-to-client-reflection**
- **clock summer-time**
- **graceful-restart** (BGP)
- **ip access-group**
- **ip access-group frag deny**
- **ipv6 access-group**
- **neighbor activate**
- **neighbor route-map**
- **neighbor route-reflector-client**
- **neighbor send-community**
- **neighbor weight**
- **poe enable**
- **reserved-vlan map**
- **qinq-tunnel cvlan**
- **show access-list tcam**
- **show qinq-tunnel**
- **show reserved-vlan map**
- **show running-config**
- **supportsave**

Deprecated Commands for FastIron 10.0.20

No commands have been deprecated for this release.

RFCs and Standards

There are no newly supported RFCs or standards in FastIron release 10.0.20.

MIBs

The following MIBs were updated in FastIron release 10.0.20:

- BGP EVPN
- Stacking (Slot Profile)
- Ethernet Port Breakout

Hardware Support

Supported Devices

The following devices are supported in FastIron release 10.0.20.

- ICX 7550 Series (ICX7550-24, ICX7550-48, ICX7550-24P, ICX7550-48P, ICX7550-24ZP, ICX7550-48ZP, ICX7550-24F, ICX7550-48F)
- ICX 7650 Series (ICX7650-48P, ICX7650-48ZP, ICX7650-48F)
- ICX 7850 Series (ICX7850-32Q, ICX7850-48FS, ICX7850-48F, ICX7850-48C)
- ICX 8200 Series (ICX8200-24, ICX8200-24P, ICX8200-24F, ICX8200-24FX, ICX8200-24ZP, ICX8200-48, ICX8200-48F, ICX8200-48P, ICX8200-48ZP2, ICX8200-48PF, ICX8200-48PF2, ICX8200-C08PF, ICX8200-C08ZP)

Hardware Scaling

FastIron release 10.0.20 supports the following scaling numbers, which will be revised to higher limits in upcoming releases.

- ICX 7550, ICX 7650, and ICX 7850 devices: up to 8-unit stack and up to 800 VLANs
- ICX 8200 devices managed by CLI or SmartZone: up to 8-unit stack and up to 800 VLANs
- ICX 8200 devices managed by RUCKUS One: up to 4-unit stack and up to 400 VLANs

Default Username and Password

New ICX switches that are initially deployed using 08.0.90 or later releases must be accessed using the following default local username and password:

- Default local username: super
- Default password: sp-admin

The default username and password apply to all forms of access including Console, SSH, and Web. The administrator will be prompted to create a new password after logging in. ICX devices that are already deployed with a previous release and upgraded to 08.0.90 will not be affected by this change.

Supported Power Supplies

For a list of supported power supplies, refer to either the *RUCKUS ICX Switch Product Line Data Sheet* or the model-specific Data Sheets available online at https://www.ruckusnetworks.com/products/ethernet-switches.

Supported Optics

For a list of supported fiber-optic transceivers that are available from RUCKUS, refer to the latest version of the *RUCKUS Ethernet Optics Family Data Sheet* available online at https://www.commscope.com/globalassets/digizuite/61722-ds-ethernet-optics-family.pdf.

Upgrade Information

Image File Names

Download the following FastIron images from www.ruckuswireless.com.

The UFI (which was introduced in 08.0.80) consists of the application image, the boot code image, and the signature file and can be downloaded in a single file.

Beginning with FastIron 08.0.90, any new ICX hardware platform (starting with the ICX 7850) will use only UFI images. Any systems upgraded from 08.0.70 or earlier releases directly to 08.0.90 manually or using the manifest file must be upgraded a second time using the UFI image. If the upgrade is from 08.0.80, then use the UFI image.

For detailed instructions on how to upgrade to a new FastIron release, see the *RUCKUS FastIron Software Upgrade Guide*.

Device	UFI file name (boot, image)
ICX 7550	GZR10020ufi.bin
ICX 7650	TNR10020ufi.bin
ICX 7850	TNR10020ufi.bin
ICX 8200	RDR10020ufi.bin

PoE Firmware Files

The following table lists the PoE firmware file types supported in this release.

Device	Firmware version	File name
ICX 7550	01.64.07.b001.fw	icx7xxx_poe_01.64.20.b001.fw
ICX 7650	02.1.8 fw	icx7xxx_poe_02.2.4.b002 (PD69220) or icx7xxx_poe_02.1.8.b004.fw (PD69200)
ICX 7850	N/A	Not supported
ICX 8200	01.64.07.b001.fw	icx7xxx_poe_01.64.20.b001.fw

The firmware files are generally specific to their devices and are not interchangeable. For example, you cannot load ICX 7550 firmware on an ICX 7650 device.

NOTE

Please note the following recommendations and notices:

- Inline power is enabled by default as of FastIron release 08.0.70.
- As of FastIron release 08.0.70 **legacy-inline-power** configuration is disabled by default.
- Data link operation is decoupled from inline power by default as of FastIron release 08.0.70.
- Use the **[no] inline power** command to enable and disable POE on one or a range of ports.
- Data link operation is coupled with inline power using the command **inline power ethernet** *x/x/x* **couple-datalink** in Privileged EXEC mode or in interface configuration mode using the command **inline power couple-datalink**. The PoE behavior remains the same as in releases prior to 08.0.70 (08.0.30, 08.0.40, 08.0.50, 08.0.61).
- Do not downgrade PoE firmware from the factory-installed version. When changing the PoE firmware, always check the current firmware version with the **show inline power detail** command, and make sure the firmware version you are installing is higher than the version currently running.
- PoE firmware will auto-upgrade to version 2.1.0 during the loading of FastIron release 08.0.80. This auto-upgrade of the PoE firmware will add approximately 10 minutes to the loading of FastIron release 08.0.80 on ICX 7650 devices.

Open Source and Third-Party Code

RUCKUS FastIron software contains or references the following third-party or open source software.

Third Party Software	Open source (Yes/No)
Abduco - Console	Yes
Aquantia - PHY Drivers	No
avl	Yes
Bind9	Yes
Broadcom - Linux	Yes
Broadcom - PHY Drivers	No
Broadcom - SDK	No
Broadcom / Marvell - sysroot	Yes
Broadcom - Uboot	Yes
Busybox - Telnet	Yes
curl	Yes
diffios - conf_archive	Yes
Dynamic (.so) and static(.a) libraries	Yes
FCGI2 - RESTConf	Yes
FCGIWrap - RESTConf	Yes
Ingy dot Net - YAML Parser, libyaml-0.2.5	Yes
IP Infusion - MVRP	No
iptables	Yes
ISC - DHCPv6 Server ISC - DHCPv4 server client	Yes
Libtelnet - RConsole	Yes
libunwind	Yes
libxml	Yes

Third Party Software	Open source (Yes/No)
Linux-Pam - PAM authentication	Yes
Marvell - MSA (SDK)	No
Nettle - Cryptographic library for radsecproxy	Yes
Network Security Services (NSS)	Yes
Nginx - RESTConf/Web	Yes
OpenSSH - SSH client / server	Yes
OpenSSL	Yes
Pyrad - RADIUS	Yes
Python	Yes
Python 3	Yes
Python-PAM - Python based PAM authentication module	Yes
Radsecproxy - Proxy RADIUS server	Yes
rootfs Source (Part of Linux)	Yes
SZ agent: Nginx - szagent Uwsgi - szagent curl - szagent zlib - szagent libxml - szagent	Yes
TACACS Plus (TACACS+)	Yes
Trusted Computing Group - TPM	Yes
Ulogd - Management access	Yes
Web UI: flask_package - webui node_module - webui openssl - webui	Yes
WindRiver - IPSec	No
WindRiver - OSPFv3	No
WindRiver - PKI	No
WindRiver - SNMP	No
ZeroMQ – Library for Inter Process Communication	Yes
zlib	Yes

Known Behavior

This section describes known behaviors for certain RUCKUS ICX devices and recommended workarounds where they exist.

UniFi HD WiFi Access Point Power Up

UniFi AP-HD APs may not be powered on at the IEEE 802.3bt ports, use the **dm poe enable legacy extended ethernet <x/y/z> ethernet <a/b/c> to <m/n/o>** command to resolve the issue. The **legacy-inline-power** command should be configured at the interface configuration level before executing this command and the interfaces should be in disabled state. If the switch reboots or if the PD is unplugged and then plugged in, the **dm poe enable legacy extended** command has to be executed again.

ICX 8200 PoE Status LED

If the power level you configure for an ICX 8200 port is less than the power consumed by an attached power device (PD), the PoE status for the port alternates between "overload" and "powered state" until the allocated or configured power level is higher than the power consumed by the PD.

ICX 8200-24FX and ICX 8200-48F Units as Stack Active Controller

When an ICX 8200-24FX or an ICX 8200-48F unit is operating as the active controller of a stack, MAC address table size is limited to 8,000.

ICX 8200-24F and ICX 8200-48F Default Port Setting

On ICX 8200-24F and ICX 8200-48F devices, 100Base-FX is enabled by default.

ICX 8200-C08ZP

ICX 8200-C08ZP devices connect only through auto-negotiation. RUCKUS recommends that you use the default speed setting (speed auto) on 10G Multi-gig ports rather than configuring a specific speed.

MACsec Traffic

Beginning with FastIron release 09.0.10c, MACsec is no longer backward compatible with previous software versions. All connected devices must have FastIron release 09.0.10c or later for MACsec traffic to flow correctly.

ICX 7550 Port LED in PoE Mode

When a RUCKUS ICX 7550-24ZP or a RUCKUS ICX 7550-48ZP device is operating in PoE mode and the user connects a powered device to a 10-Gbps port, the port LED comes up green but immediately goes to amber, although the expected LED color is green.

When the powered device is connected while the ICX device is not in PoE mode and is then placed in PoE mode, the port LED remains green as expected.

Workaround: If you encounter the issue, change the device to any other mode, or rotate to the PoE mode again. The LED will then work as expected.

Known Issues in Release 10.0.20

Issue	FI-288925
Symptom	On ICX8200, Device may not bootup in secondary partition due to MSA initialization failure instead it will bootup in primary partition.
Condition	On ICX8200, Device may not bootup in secondary partition due to MSA initialization failure instead it will bootup in primary partition.
Workaround	User needs to login to the device and try booting to secondary partition again.
Recovery	No recovery.
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-288347
Symptom	Unconfiguring of reserved vlan-map vlan 4091 returns error when tried before reload.
Condition	Configuration to map reserved vlan 4091 to new-vlan
Workaround	Reloading the device and then unconfiguring the reserved-vlan-map
Recovery	Device will be recovered once reload is done
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-286815
Symptom	In ICX7850 sometime observed reload got stuck on ICX7850.
Condition	
Workaround	Power cycle need for that stuck condition for the ICX7850 box.
Recovery	Power cycle need for that stuck condition for the ICX7850 box.
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-287326
Symptom	Error message - "RESTCONF: Configuration sync failed for module ip/ipv6 interfaces" is seen during bootup and RuckusOne will not show ipv6 address for down interfaces
Condition	Error message - "RESTCONF: Configuration sync failed for module ip/ipv6 interfaces" is seen during bootup and RuckusOne will not show ipv6 address for down interfaces
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-287998
Symptom	On ICX8200, sometimes the device will not boot up with secondary partition even though "boot system flash secondary" is entered. Instead, it boots up with primary partition.
Condition	On ICX8200, sometimes the device will not boot up with secondary partition even though "boot system flash secondary" is entered. Instead, it boots up with primary partition.
Workaround	User can enter "boot system flash secondary" once again from primary partition.
Recovery	Recovery not required.
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-287919
Symptom	The cfg_sync process memory will get increased continuously in Active unit in stack and due to this, system memory will get increased.
Condition	This will happen when there are lot of dynamic syslogs generated in Active unit in rapid rate, and due to this cfg_sync processing this lot of syslogs and syncing to standby, during this time cfg_sync memory increase will happen.
Workaround	We need to set the rate limit on syslogs processed per second, we can configure 'logging-rate-limit' with very low value once the system booted up for that.
Recovery	
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-287594
Symptom	Syslog will not be generated when user logs in with incorrect credentials
Condition	When SSH/Telnet/Console Connection is established,
Workaround	NA
Recovery	NA
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-287531
Symptom	Even after unplugging LRM external optics "show optic" would display external optics data.
Condition	
Workaround	Executing "dm optic eeprom" on the respective port would recover.
Recovery	Executing "dm optic eeprom" on the respective port would recover.
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-287522
Symptom	Index number is not incrementing properly in output of show ip ospf border-routers
Condition	Index number is not incrementing properly in output of show ip ospf border-routers
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-287486
Symptom	With scaled clients dhcp client renew is failing sometimes when dynamic arp inspection is also enabled.
Condition	With scaled clients dhcp client renew is failing sometimes when dynamic arp inspection is also enabled.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-287030
Symptom	DHCP packets ingress on protected port in vlan is flooded to other ports in vlan if dhcp relay is configured on interface.
Condition	DHCP packets ingress on protected port in vlan is flooded to other ports in vlan if dhcp relay is configured on interface.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-286911
Symptom	Duplicate dhcp packets are received by dhcp clients when relay is configured.
Condition	Duplicate dhcp packets are received by dhcp clients when relay is configured.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-286858
Symptom	Option 82/option37 is not removed for packets forwarded to client when dhcp L2 relay is configured on lag interface.
Condition	Option 82/option37 is not removed for packets forwarded to client when dhcp L2 relay is configured on lag interface.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-286846
Symptom	PPPoE packets from client is not reaching server when PPPoE intermediate-agent are configured on LAG interface.
Condition	PPPoE packets from client is not reaching server when PPPoE intermediate-agent are configured on LAG interface.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-286119
Symptom	DHCP server lease entries on RuckusOne shows both stale and new entries.
Condition	ICX connected to RuckusOne and DHCP lease entries get renewed from ICX
Workaround	Use CLI commands to check the lease entries
Recovery	
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-284326
Symptom	ping/traffic forwarding stops working once vrf forwarding is removed from ve interface and ip is assigned to physical port part of same vlan.
Condition	ping/traffic forwarding stops working once vrf forwarding is removed from ve interface and ip is assigned to physical port part of same vlan.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-283913
Symptom	Link does not come up between ICX7850-48F 25G port configured as 1G and ICX8200-24FX 10G port (configured as 1G or default config).
Condition	always
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-283722
Symptom	Openflow flows attached to the interface are not removed when no interface ethernet x/x/x is configured.
Condition	Openflow flows attached to the interface are not removed when no interface ethernet x/x/x is configured.
Workaround	None
Recovery	clear openflow flow can be used to clear the flows.
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-283658
Symptom	PBR is not forwarding traffic when precedence is used permit match criteria.
Condition	PBR is not forwarding traffic when precedence is used permit match criteria.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-283576
Symptom	when openflow is enabled on more than one interface and with flows created, if we do "clear openflow all", it is not clearing hardware entries for flow.
Condition	when openflow is enabled on more than one interface and with flows created, if we do "clear openflow all", it is not clearing hardware entries for flow.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-283518
Symptom	rx power,txpower, TxBiasCurrent and Voltage MIBs are not seen during snmpwalk on snIfOpticalLaneMonitoringTable table.
Condition	rx power,txpower, TxBiasCurrent and Voltage MIBs are not seen during snmpwalk on snIfOpticalLaneMonitoringTable table.
Workaround	NA
Recovery	
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-282927
Symptom	Snmpget/snmpwalk on ruckusWiredClientsTable is not showing ruckusWiredClientV4Addr and ruckusWiredClientV6Addr.
Condition	Snmpget/snmpwalk on ruckusWiredClientsTable is not showing ruckusWiredClientV4Addr and ruckusWiredClientV6Addr.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-282653
Symptom	During powercycle of ICX 8200-48F platform an unexpected reload of plugin proc application might happen sometimes.
Condition	This happens when there are multiple power cycles happened in this system, that is if around 1000 power cycles is performed in the system.
Workaround	
Recovery	The plugin-proc application after it stopped, would be restarted again by hmon application after few seconds automatically.
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-280784
Symptom	Directed broadcast packet is not getting forwarded.
Condition	Directed broadcast packet is not getting forwarded.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-280326
Symptom	Customer may not able to use DEVICE_PROFILE for radius/tacacs/syslog servers for SSL connection
Condition	If user wants to use tpm certificate for radius/tacacs/syslog servers for SSL connection, user may not be use as DEVICE_PROFILE is not available on the system
Workaround	Customer can use User created SSL profiles for radius/tacacs/syslog servers for SSL connection
Recovery	
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-280294
Symptom	Mac address not learnt on static lag.
Condition	Only if static lag has one port and that one port fron standby unit
Workaround	Removal and readding the port in the lag solves it
Recovery	
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-279930
Symptom	clock time shown in 'show cpu-utilization histogram trace' will be wrong.
Condition	This happens on issuing this command 'show cpu-utilization histogram trace'
Workaround	
Recovery	
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-278693
Symptom	" Config Parsing Failed " error is seen when trying to copy tftp running-config
Condition	ICX running-config is applied, with the value "manager port-list 987" in the config file.
Workaround	No
Recovery	No
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-278226
Symptom	"show who" command does not show the user who logged from R1 cloud
Condition	login using CLI from R1 cloud
Workaround	No
Recovery	No
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Issue	FI-275597
Symptom	Jumbo traffic counters are not updating in snSwIfStatsInJumboFrames MIB during snmpwalk/ snmpget on the MIB
Condition	Jumbo traffic counters are not updating in snSwIfStatsInJumboFrames MIB during snmpwalk/ snmpget on the MIB
Workaround	NA
Recovery	
Probability	
Found In	FI 10.0.20
Technology / Technology Group	

Closed Issues with Code Changes in Release 10.0.20

Issue	FI-288388
Symptom	IGMP/MLD receiver receive multicast traffic after 10 sec delay when IGMP/MLD snooping is configured in stack
Condition	ICX when deployed in stacking mode and multicast snooping enabled, would then result in 10 sec delay for the receiver to receive multicast traffic.
Workaround	NA
Recovery	NA
Probability	
Found In	FI 10.0.10
Technology / Technology Group	IP Multicast - IGMP - Internet Group Management Protocol

Issue	FI-288538
Symptom	IGMP/MLD receiver receive multicast traffic after 10 sec delay when IGMP/MLD snooping is configured in stack
Condition	ICX when deployed in stacking mode along with multicast snooping enabled would result in 10 sec delay for the receiver to receive multicast traffic.
Workaround	NA
Recovery	NA
Probability	
Found In	FI 10.0.10
Technology / Technology Group	IP Multicast - IGMP - Internet Group Management Protocol

Issue	FI-284020
Symptom	"Manual configuration is not allowed for this option" is shown during bootup for dhcp ip and static route pushed by dhcp
Condition	"Manual configuration is not allowed for this option" is shown during bootup for dhcp ip and static route pushed by dhcp
Workaround	None
Recovery	None
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Management - Web Management

Closed Issues with Code Changes in Release 10.0.20

Issue	FI-287885
Symptom	The PING cli when used with option source IP, the last decimal is getting lost in the source IP. As intended source IP changes, it results in a PING failure.
Condition	In ICX when the user tries a ping command along with the source option.
Workaround	NA
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	Other - Other

Issue	FI-285629
Symptom	Typo in the help string of command "license set" .
Condition	Execution of command "license set"
Workaround	
Recovery	
Probability	
Found In	FI 08.0.95
Technology / Technology Group	System - CLI

Issue	FI-287724
Symptom	When a local or radius authentication is tried with password length beyond 32 characters, the authentication fails.
Condition	The ICX device with user having password length greater than 32 characters results in authentication failure.
Workaround	NA
Recovery	NA
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Security - AAA - Authentication, Authorization, and Accounting

Issue	FI-287481
Symptom	Command "debug ip aaa" shows credentials as clear text
Condition	Execution of command "debug ip aaa"
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10 FI 09.0.10
Technology / Technology Group	Security - AAA - Authentication, Authorization, and Accounting

Issue	FI-282710
Symptom	ICX acting as DHCP client not sending hostname option to server
Condition	When ICX acting as DHCP client
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	

Issue	FI-287152
Symptom	DHCPACK syslog message is generated very frequently as an Informational message after configuring the lease time value as 5 mins.
Condition	configure the DHCP lease time value to less value.
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	

Issue	FI-286970
Symptom	Unable to access ICX console , SSH , Telnet session
Condition	Using Unimus tool to access switch via SSH and providing invalid user credentials
Workaround	No workaround
Recovery	Reload of the device
Probability	
Found In	FI 10.0.10
Technology / Technology Group	

Issue	FI-286789
Symptom	Increase in memory usage of ICX device
Condition	ICX device configured with multiple syslog server and dot1x radius authentication.
Workaround	None
Recovery	None
Probability	
Found In	FI 10.0.10
Technology / Technology Group	Traffic Management - Buffer Queue Management

Closed Issues with Code Changes in Release 10.0.20

Issue	FI-284496
Symptom	user can see 1Hr time difference in "show clock" and "show log" time stamps
Condition	Issue will be seen if system configured with Day Light Saving time zones and the current time is not in Day Light Saving time.
Workaround	No workaround
Recovery	NA
Probability	
Found In	FI 10.0.10
Technology / Technology Group	

Issue	FI-284802
Symptom	Memory leak in ICX device
Condition	Multicast configuration in ICX
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	IP Multicast - IGMP - Internet Group Management Protocol

Issue	FI-284910
Symptom	VLAN memberships are inadvertently deleted when the ports associated with the port-profile transition to a down state. This results in the removal of member interfaces from the VLAN, affecting both configurations applied through port-profile and standard configurations.
Condition	When a port, to which a port-profile with VLAN configurations is attached, goes down, this situation can occur.
Workaround	Reconfigure the vlan member interfaces
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	Layer 2

Issue	FI-283164
Symptom	No commands accepted after login at enable prompt
Condition	Remote server authentication providing unsupported privilege level
Workaround	
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	

Issue	FI-281125
Symptom	UniFi_UAP-AC-HD wifi access point would not get powered on ICX8200 and ICX7550
Condition	UniFi_UAP-AC-HD wifi access point not getting powered.
Workaround	No workaround
Recovery	no recovery.
Probability	
Found In	FI 10.0.10 FI 10.0.20
Technology / Technology Group	Other - Other

Issue	FI-283720
Symptom	Dynamic VLAN assignment will fail when Tunnel-Private-Group-ID attribute contains VLAN name
Condition	Radius server configured Tunnel-Private-Group-ID attribute with VLAN names
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	Security - RADIUS

Issue	FI-279766
Symptom	Unable to start SSH/TELNET sessions.
Condition	Automated tool like AUVIK is running and causing abrupt closure of CLI sessions.
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10 FI 10.0.00
Technology / Technology Group	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-282625
Symptom	Dot1x authentication will fail
Condition	Microsoft NP radius server used as authentication server
Workaround	
Recovery	
Probability	
Found In	FI 09.0.00
Technology / Technology Group	Security - RADIUS

Closed Issues with Code Changes in Release 10.0.20

Issue	FI-281075
Symptom	High CPU is observed on the ICX
Condition	On paged mode display, if user doesn't provide any option while CLI is expecting an input from the user.
Workaround	Once the paged display prompts options for continue or quit, provide the necessary input to continue.
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	System - CLI

Issue	FI-280867
Symptom	VLAN name is getting removed from the config
Condition	VLAN name is deleted when a port is added to a port-profile
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	

Issue	FI-280617
Symptom	Same port can be configured, in multiple port profiles
Condition	When user tries to configure same port to multiple port profiles, configuration doesn;t error out
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	

Issue	FI-274280
Symptom	ASCII characters are missing in running and startup configuration for DHCP option string
Condition	Configuration of DHCP option string with ASCII characters
Workaround	
Recovery	
Probability	
Found In	FI 10.0.00
Technology / Technology Group	Management - DHCP (IPv4)

Issue	FI-279275
Symptom	Unexpected reload while configuring broadcast/multicast/unknown-unicast rate limiting
Condition	When configuring broadcast/multicast/unknown-unicast rate limiting
Workaround	None
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	Traffic Management - Rate Limiting and Shaping

Issue	FI-279006
Symptom	ICX8200 can sometime fail in 802.1x authentication
Condition	If radius server sends a packet with more than 1534 length , ICX8200 can fail in 801.1x authentication
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	Security - 802.1x Port-based Authentication

Issue	FI-279628
Symptom	Write Exception seen when adding logging/syslog host server
Condition	When trying to configure logging/syslog host server
Workaround	None
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Management - IPv4/IPv6 Host Management

Issue	FI-277683
Symptom	Unexpected reload of ICX-7550 under rare conditions
Condition	Some timing issue can cause unexpected reload of ICX-7550
Workaround	
Recovery	
Probability	
Found In	FI 08.0.95
Technology / Technology Group	Other - Other

Closed Issues with Code Changes in Release 10.0.20

Issue	FI-274081
Symptom	SSH to ICX will fail
Condition	ICX act as VRRP-e master
Workaround	
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Management - SSH2 and SCP - Secure Shell and Copy

Issue	FI-276546
Symptom	Crash is removed when same network ip is removed from virtual interface and configured on loopback interface in quick succession.
Condition	Crash is removed when same network ip is removed from virtual interface and configured on loopback interface in quick succession.
Workaround	Adding few seconds of delay between the configs will prevent the crash.
Recovery	None
Probability	
Found In	FI 10.0.10
Technology / Technology Group	

Issue	FI-277687
Symptom	PDs on few continuous ports might not get powered and can show up the status as Overload condition in "show inline power" output.
Condition	The may be seen after switch reload or after disabling and enabling of poe on the ports.
Workaround	
Recovery	disabling and re-enabling PoE on the affected ports can recover from the issue.
Probability	
Found In	FI 10.0.00
Technology / Technology Group	

Issue	FI-278378
Symptom	ICX-8200 can go for an unexpected reload under rare condition
Condition	ICX-8200 under certain timing condition can access wrong memory resulting in unexpected reload
Workaround	
Recovery	
Probability	
Found In	FI 10.0.00
Technology / Technology Group	System - System

Issue	FI-277887
Symptom	port-name doesn?t allow spaces while adding using int e x/x/x to x/x/x
Condition	port-name allow spaces while adding using int e x/x/x to x/x/x
Workaround	
Recovery	
Probability	
Found In	FI 10.0.10
Technology / Technology Group	

Issue	FI-277752
Symptom	Not able to configure SNMP Location/Contact object with input as multiple string values.
Condition	When configuring SNMP Location/Contact object with input as multiple string values.
Workaround	Configure SNMP Location/Contact object with input as single string value.
Recovery	NA
Probability	
Found In	FI 10.0.10
Technology / Technology Group	Management - SNMP - Simple Network Management Protocol

Issue	FI-277464
Symptom	ICX will go for reload when executing "show ip ospf border routers" command.
Condition	when the switch has number of OSPF border router entries more than 65.
Workaround	NA
Recovery	NA
Probability	
Found In	FI 09.0.00
Technology / Technology Group	Layer 3 Routing/Network Layer - OSPF - IPv4 Open Shortest Path First

Issue	FI-276656
Symptom	"show reload" command can provide incorrect detail of scheduled reload
Condition	When a reload is scheduled, icx might report incorrect time in the "show reload" command output
Workaround	
Recovery	
Probability	
Found In	FI 09.0.10
Technology / Technology Group	Management

Issue	FI-276767
Symptom	DHCP Snoop config is not applied on the ports
Condition	When an older release with port security and dhcp snoop on the same port is upgraded to a later release
Workaround	Configuration should be redone in new released version
Recovery	Configuration should be redone in new released version
Probability	
Found In	FI 10.0.10 FI 09.0.10
Technology / Technology Group	Layer 3 Routing/Network Layer - DHCP - Dynamic Host Configuration Protocol

Issue	FI-272984
Symptom	Unexpected Reload might occur when we execute "dm ipv4-unicast vrf 20 hw-route"
Condition	Unexpected Reload might occur when we execute "dm ipv4-unicast vrf 20 hw-route"
Workaround	None
Recovery	NA
Probability	
Found In	FI 08.0.95
Technology / Technology Group	

Issue	FI-275536
Symptom	The active member in a 2 member ICX7750 stack experienced unexpected reload.
Condition	Active unit of 2 member ICX7750 stack experienced unexpected reload, when generating log message in case of hardware route programming failure.
Workaround	NA
Recovery	None
Probability	Low
Found In	FI 08.0.80
Technology / Technology Group	System - System

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