

## Digi TX/LR Firmware Release Notes Version 21.2.39.67 (March 2021)

### INTRODUCTION

---

Digi Accelerated Linux is an advanced, high-performance operating system for cellular routers. These are the release notes for the initial Digi Accelerated Linux (DAL) firmware release which supports the Digi TX and LR family of products listed below.

### SUPPORTED PRODUCTS

---

- Digi TX54
- Digi TX64
- Digi TX54 Primary Responder
- Digi TX64 Primary Responder
- Digi LR54

### KNOWN ISSUES

---

- Cellular metrics are not shown under the **Settings** → **Status** → **Communications** section of Digi Remote Manager, but are shown under the **Data Streams** for the device. [DALP-768]
- Health metrics are uploaded to Digi Remote Manager unless the **Monitoring > Device Health > Enable** option is de-selected and either the **Central Management > Enable** option is de-selected or the **Central Management > Service** option is set to something other than Digi Remote Manager. [DAL-3291]
- Wired Internet connectivity is interrupted during cellular modem firmware updates [DAL-4647]
- The cellular Access technology configuration option is ignored if carrier PLMN locking is enabled [DAL-4693]
- VRRP does not always react when its LAN interface goes up or down. [DAL-3794]

### UPDATE CONSIDERATIONS

---

This release does not support migration of WR54 and WR64 devices running xOS firmware.

### UPDATE BEST PRACTICES

---

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you deploy production devices.
2. Unless otherwise noted, apply updates in the following order:

- a. Device firmware
- b. Modem firmware
- c. Configuration
- d. Application

Digi recommends Digi Remote Manager for automated device updates. For more information, see the [Digi Remote Manager User Guide](#).

If you prefer manually updating one device at a time, follow these steps:

1. Download the **21.2.39.67** firmware update image from the [Digi support website](#) to your PC
  - TX54
    - TX54-Single-Cellular-21.2.39.67.bin
    - TX54-Dual-Cellular-21.2.39.67.bin
    - TX54-Dual-Wi-Fi-21.2.39.67.bin
  - TX54 Primary Responder
    - TX54-Single-Cellular-PR-21.2.39.67.bin
    - TX54-Dual-Cellular-PR-21.2.39.67.bin
  - TX64
    - TX64-21.2.39.67.bin
  - TX64 Primary Responder
    - TX64-PR-21.2.39.67.bin
  - LR54
    - LR54-21.2.39.67.bin
    - LR54W-21.2.39.67.bin
2. Log into the Web UI.
3. Navigate to the **System > Firmware Update** page.
4. Click **Choose File** and select the appropriate firmware update image.
5. Click **UPDATE FIRMWARE**.
6. The device will automatically reboot once the firmware update is complete.

## TECHNICAL SUPPORT

---

Get the help you need via our Technical Support team and online resources. Digi offers multiple support levels and professional services to meet your needs. All Digi customers have access to product documentation, firmware, drivers, knowledgebase, and peer-to-peer support forums. Visit us at <https://www.digi.com/support> to find out more.

## CHANGE LOG

---

**Mandatory release** - A firmware release with a critical or high security fix rated by CVSS score. For devices complying with ERC/CIP and PCIDSS, their guidance states that updates are to be deployed onto devices within 30 days of release

**Recommended release** - A firmware release with medium or lower security fixes, or no security fixes

Note that while Digi categorizes firmware releases as mandatory or recommended, the decision if and when to apply the firmware update must be made by the customer after appropriate review

and validation.

## **VERSION 21.2.39.67 (March 2021)**

---

This is a **mandatory** release.

### **NEW FEATURES**

1. Geofence support has been added. The user can configure multiple different circular or polygonal geofences and have the device take a configurable action when it leaves or enters a geofence.
2. A new **modem scan** CLI command has been added to allow the user to scan for available carriers. Configuration has also been added to lock the device to a particular carrier.
3. A REST API has been added that allows the user to get and set configuration.

### **ENHANCEMENTS**

1. The Wi-Fi support has been updated to support DFS channels in client mode. A DFS-Client mode must be set on the Wi-Fi module in order to access DFS channels 149, 153, 157, 161 and 165.  
When in the DFS-Client mode, any Access Points configured on the Wi-Fi module will be disabled.
2. The Wi-Fi 5GHz channels 36, 40, 44 and 48 have been added to the Wi-Fi background scanning support. Also the default settings for the Wi-Fi background settings to be update to be
  - o Scan Threshold : -75
  - o Short Interval : 5
  - o Long Interval : 300
3. The default bandwidth for Wi-Fi 2.4GHz channels has been set to 20MHz.
4. The SureLink recovery of Wi-Fi connections was updated to restart the Wi-Fi module if restarting the network connections fails to recover the connection.
5. The IPsec support has been updated to support asymmetric pre-shared keys with IKEv2.
6. The location support has been updated to allow a user-defined latitude, longitude and altitude to be configured for the device's location.
7. The location forwarding support has been updated to support sending data over a TCP connection and to have a separate interval configuration.
8. The location support has been updated to send the device's location to Digi Remote Manager as soon as it gets a valid GNSS fix.
9. The IPsec connection uptimes are now being uploaded to Digi Remote Manager as part of the metrics.
10. The IPsec support has been updated so that Aggressive/Main mode or Xauth configuration is not displayed if IKEv2 is selected. The iptables TRACE command has been added to for enhanced firewall debugging.
11. Support for running remote CLI commands from Digi Remote Manager have been added.
12. The TX54 reboot functionality has been enhanced to power cycle the USB peripherals.
13. The OpenVPN client and server public key and private key configuration have been changed to Client\_certificate, Server\_certificate and Server\_key to make clearer of their use.
14. The accuracy of the modem status has been improved during a firmware update.

## SECURITY FIXES

For this release, the highest rated security patch has a CVSS score of **8.1 High**.

1. The Python version has been updated to 3.6.12. [DAL-4364]  
[CVE-2020-14422](#) CVSS Score: 5.9 Medium [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H](#)
2. The OpenSSL package has been updated to version 1.1.1i. [DAL-4326]  
[CVE-2020-1971](#) CVSS Score: 5.9 Medium [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H](#)
3. The DNSMasq package has been updated to version 2.83. [DAL-3950]  
[CVE-2019-14834](#) CVSS Score: 3.7 Low [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L](#)  
[CVE-2020-25681](#) CVSS Score: 8.1 High [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H](#)  
[CVE-2020-25682](#) CVSS Score: 8.1 High [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H](#)  
[CVE-2020-25683](#) CVSS Score: 5.9 Medium [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H](#)  
[CVE-2020-25684](#) CVSS Score: 3.7 Low [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N](#)  
[CVE-2020-25685](#) CVSS Score: 3.7 Low [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N](#)  
[CVE-2020-25686](#) CVSS Score: 3.7 Low [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N](#)  
[CVE-2020-25687](#) CVSS Score: 5.9 Medium [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H](#)
4. The hostapd package has been updated to resolve critical issues. [DAL-4232]  
[CVE-2019-16275](#) CVSS Score: 6.5 Medium [CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H](#)  
[CVE-2019-13377](#) CVSS Score: 5.9 Medium [CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N](#)
5. The WPA supplicant package has been updated to resolve critical issues. [DAL-4233]  
[CVE-2019-16275](#) CVSS Score: 6.5 Medium [CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H](#)
6. The libcurl package has been updated to version 7.74.0. [DAL-4234, DAL-4366]  
[CVE-2020-8169](#) CVSS Score: 7.5 High [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N](#)  
[CVE-2020-8177](#) CVSS Score: 7.1 High [CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H](#)
7. The Web server security has been updated with the following headers:
  - Pragma: no-cache
  - Content-Security-Policy
  - X-Content-Type-Options: nosniff
  - X-XSS-Protection: 1; mode=block
  - X-Frame-Options: SAMEORIGIN set to uppercase[DAL-4192]
8. Automatically deactivate active user logins/sessions if the password for that user changes. [DAL-4362]
9. Removed support for HTTPS CBC ciphers. [DAL-4408]
10. Removed debug configuration options for PR firmware for changing HTTPS ciphers. [DAL-4417]
11. An XSS vulnerability on the serial page in the Web UI has been resolved. [DAL-4646]

## BUG FIXES

1. An issue has been resolved where the non-primary DNS servers were queried through the wrong interface when the **use\_dns** configuration option was set to **primary**. [DAL-3156]
2. An issue where a Wi-Fi Access Point would not make a client connection on 2.4GHz has been

resolved. [DAL-3943]

3. An issue on the TX54 where the cellular module disconnects with a “modem not available” error has been resolved. [DAL-4423]
4. An issue that prevented Web UI access when two-factor authentication was enabled has been resolved. [DAL-4509]
5. An issue where an incorrect format of ICCID and IMEI metrics were being sent to Digi Remote Manager has been resolved. Also the phone number of the SIM is now included in the metrics. [DAL-4440]
6. An issue with an aView initiated speed test reporting the same upstream/downstream values has been resolved. [DAL-4420]
7. An issue that prevented the LM940 cellular module from reconnecting after a module firmware update has been resolved. [DAL-2933]
8. An issue when using IPsec configured to use the default route for the local endpoint has been resolved. [DAL-4433]
9. An issue where a cellular module firmware update on dual cellular platforms which could result in the wrong module being updated has been resolved. [DAL-4189]
10. An issue with Wi-Fi LEDs on the TX54 Dual Wi-Fi variants has been resolved. [DAL-4185]
11. An issue where a hotspot would stop responding to DHCP requests if the hotspot was started many times has been resolved. [DAL-4298]
12. An issue with the syslog configuration when updating from the DAL 20.5 release to DAL 20.8 or DAL 20.11 release has been resolved. [DAL-4426]
13. An issue preventing configuration updates via Digi Remote Manager if SCEP settings were enabled on the device have been resolved. [DAL-4445]
14. An issue with the **show wifi ap name <name>** and **show wifi client name <name>** CLI commands has been resolved. [DAL-1615, DAL-1616]
15. An issue where an incorrect system uptime is displayed in the Web UI and **show system** CLI command has been resolved. [DAL-4350]
16. An issue where CLI sessions showing stale configuration settings if the device was updated in a different session has been resolved. [DAL-2284, DAL-2671, DAL-4446, DAL-4530]
17. The message displayed in the Web UI after factory defaulting a device has been updated to direct the user to refresh the page. [DAL-2326]
18. An issue where dynamic DHCP leases were not been displayed in the Web UI or CLI has been resolved. [DAL-4557]
19. An incorrect Ethernet interface status when the device is in passthrough mode has been fixed. [DAL-4543]
20. An issue that prevented use of the Python digidevice.config module in PR firmware images has been resolved. [DAL-4378]
21. An issue with software flow control on serial ports configured in remote access mode has been resolved. [DAL-3630]
22. A timing issue with the LM940 modem that prevented the modem from reconnecting after a firmware update has been resolved. [DAL-4614]
23. A SureLink issue that could prevent a second APN connection if the interface was configured with just an **Interface Up** test has been resolved. [DAL-4629]

24. A rare issue where the Digi RM client could crash when making a configuration change has been resolved. [DAL-4593]

## **VERSION 20.11.32.138 (December 2020)**

---

This is a **mandatory** release.

### **NEW FEATURES**

1. Support for the following Primary Responder (PR) platforms has been added
  - TX54-Single-Cellular-PR (TX54-A146)
  - TX54-Dual-Cellular-PR (TX54-A246)
  - TX64-PR (TX64-A141)
2. The IPsec support has been updated to use XFRM interfaces which allows IPsec tunnels to be treated like network interfaces which allows them to be used for static routes, policy-based routes, access control lists, routing based on metrics, etc.
3. Support for IPv6 IPsec tunnels, IPv6-over-IPv4 and IPv4-over-IPv6 tunneling has been added.
4. Support for Python PIP module for installing external libraries and modules has been added.
5. A new **modem firmware** CLI command for performing local and over-the-air remote firmware updates on the cellular modem(s) on the device.
6. Ethernet configuration for duplex and speed has been added.
7. An option to starting, stopping and viewing serial port activity logs via the CLI, Web UI and Digi RM has been added.

### **ENHANCEMENTS**

1. The **m2m.telus.iot** Telus APN has been added to the APN fallback list.
2. The **890103** and **890141** ICCID prefixes and **31030** PMND ID matchers to the AT&T APN fallback list.
3. The **psmtneorm** and **edneopate010.dpa** APNs have been added to the AT&T APN fallback list.
4. The **reseller** and **tracfone.vzwentp** APNs have been added to the Verizon APN fallback list.
5. The IPsec support has been updated so that the device will wait for Surelink tests (if configured) to pass before initiating outbound IPsec tunnels.
6. The QXDM support has been updated to support encrypted QXDM access to the cellular modem on the device. Note that this is always enabled on the PR platforms.
7. **SSH** and **telnet** CLI commands have been added. Note that the telnet command is not available on the PR platforms.
8. The VRRP support has been updated to use virtual MAC addresses on the LAN interface.
9. A **defaultroute** option has been added for matching policy based router to the device's active default route.
10. A **DSCP** option has been added to policy based routes to allow users to match the routing rule to the type of DSCP field in the packet.
11. A **Services > Ping Responder** configuration has been added for controlling what interfaces and firewall zones the device will respond to ICMP requests on.
12. A **Modbus Gateway** status CLI command and Web UI page have been added,
13. The IPsec support has been updated to hide to the Main / Aggressive Mode configuration if

IKEv2 has been selected. [DAL-4142]

14. A **scripts** status CLI command and Web UI page have been added that allow the user to manage scripts that running on the device.
15. The **show modem** CLI command has been updated to display if the modem is switching firmware.
16. The **Monitoring > Device Health** configuration will now be hidden if the Digi RM management has been disabled.
17. The network bridge support has been updated to use the MAC address of the first configured device in the bridge for the bridge interface.
18. The following modem firmware and SIM details are uploaded to Digi RM as part of the health metrics:
  - SIM PLMN
  - SIM IMSI
  - SIM Provider
  - Modem IMEI
  - Modem Manufacturer
  - Modem Model
  - Modem Revision
  - Modem CNTI
  - Modem Connection Status
19. A system log entry is added if the Surelink DNS tests are skipped if the interface does not have any DNS servers.
20. The Web UI has been updated with several enhancements:
  - The Ethernet interface speed configuration has been updated with correct notation.
  - The dashboard will now display the cellular technology icon for the service being used.
  - The dashboard will now display the Digi RM connection time in a finer granularity.
  - The dashboard has been updated with some formatting changes.
  - Help button added to File System page which links to the relevant User Guide section.
  - The Modem Firmware Update page now has a link to the scheduled maintenance page.

## SECURITY FIXES

For this release, the highest rated security patch has a CVSS score of **9.1 Critical**.

1. A tcpdump memory allocation issue have been resolved. [DAL-4226]  
[CVE-2020-8037](#) CVSS Score: 7.5 High [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H](#)
2. The jQuery package has been updated to 3.5.0.  
[CVE-2020-11022](#) CVSS Score: 6.1 Medium [3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N](#)  
[CVE-2020-11023](#) CVSS Score: 6.1 Medium [3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N](#)
3. The OpenVPN package has been updated to 2.4.9  
[CVE-2018-7544](#) CVSS Score: 9.1 Critical [3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H](#)
4. The Bash package has been updated to 5.0

5. The OpenSSH package has been updated to 8.3p1
6. The OpenSSL package had been updated to 1.1.1h
7. Updates have been made to prevent command injection through modem firmware update web pages. [DAL-4046, DAL-4093, DAL-4104]
8. An issue where some file could be downloaded from the device without authentication has been fixed. [DAL-3835]
9. An issue where it was possible to add files to the encrypted file system on the TX64 if you had physical access has been fixed. [DAL-4149]
10. The Web UI has been updated to prevent authentication in HTTP GET requests. [DAL-3834]
11. The Web UI has been updated to set the Content-Security-Policy header. [DAL-3629]
12. The firmware update process has been updated to further firmware validation. [DAL-3511]
13. TCP forwarding from incoming SSH connections have been disabled. [DAL-3938]

## BUG FIXES

1. An issue that resulted in the delayed sending of health metrics to Digi RM has been resolved. [DAL-3908]
2. An issue with IPsec and OpenVPN Surelink recovery actions failing if the tunnel name is longer than 7 characters have been resolved.
3. An issue with policy based routing not working in conjunction with multiple IPsec tunnels has been fixed. [DAL-3515]
4. The format of user passwords when displayed in Digi RM has been fixed. [DAL-3889]
5. An issue that prevented firewall rules from being setup for OSPFv2 entries has been fixed. [DAL-3869]
6. An issue that prevented multicast traffic from being sent through a GRE tunnel has been fixed. [DAL-3879]
7. An issue that prevented OpenVPN clients using auto-generated configuration files from a TAP-bridge OpenVPN server has been fixed. [DAL-3881]
8. An issue that prevented OpenVPN server managed certificates from being re-generated if the process was interrupted has been fixed. [DAL-3803]
9. An issue with VRRP+, where the device could become the VRRP Master before any of the monitored interfaces come up has been resolved. [DAL-4274]
10. An issue with the Wi-Fi Scanner that prevented the scanner logs from being listed on the **System > Logs** page unless static filtering was enabled has been fixed. [DAL-3817]
11. An issue with Digi RM configuration profiles missing an option for setting the **SIM Slot Preference** has been fixed. [DAL-3912]
12. An issue where not all default configuration values were being uploaded to Digi RM which lead to problems with the Configuration Manager has been fixed. [DAL-3789]
13. The **system disable-cryptography** command has been fixed. [DAL-4169]
14. An issue where the /opt file system space being incorrectly displayed in the **show system verbose** command has been fixed. Other formatting change has also been made. [DAL-3702, DAL-3805]
15. An issue with the factory default second stage erase not working has been fixed. [DAL-3944]
16. Duplicate modem signal information on the Web UI **Modem > Status** page has been removed.



## **VERSION 20.08.22.32 (September 2020)**

---

This is a **mandatory** release.

### **NEW FEATURES**

1. Verizon DNMR support has been added.
2. Serial Modbus gateway support has been added.
3. VRRP+ support to allow a VRRP backup to monitor the VRRP master has been added.
4. Python support sending and receiving SMS messages has been added.
5. MQTT client support has been added via the Python Paho module.
6. Ethernet network bonding to allow the same MAC address and IP configuration to be shared for multiple physical Ethernet ports in either active/backup or round robin mode.
7. Support for custom factory configuration has been added.
8. Support for the Digi aView cloud service has been added.

### **ENHANCEMENTS**

1. The device health metrics support has been updated as follows:
  - Only upload health metrics to DRM that have changed since it was last uploaded.  
Note that all health metrics are uploaded at least once an hour.
  - Allow the user to configure which health metrics are uploaded to DRM
  - The format of the health metrics have been updated to reduce the bandwidth used when being uploaded to DRM.
2. The cellular firmware update on the TX54 and TX64 platforms has been updated as follows:
  - Allow the cellular module not being updated to continue to operate as normal
  - Prevent both cellular modules being updated at the same time
3. The number of maximum Wi-Fi connections supported by the TX64 Wi-Fi 2 module has been increased to 128.
4. The Wi-Fi support has been updated to support multiple RADIUS servers for WPA2 Enterprise security.
5. The Wi-Fi support has been updated to allow the transmit power to be configured. By default, the Wi-Fi module transmit at 100%.
6. A new Authoritative option has been added under TACACS+, RADIUS and LDAP user authentication configuration to prevent other authentication methods from being used if the given user credentials are invalid.
7. The Syslog support has been updated to allow UDP/TCP and port to be configured.
8. The Serial TCP connection support has been updated to allow encrypted/non-encrypted connections to be configured.
9. The Serial TCP/Telnet/SSH connection support has been updated to allow TCP keepalive messages and nodelay to be configured.
10. The NTP support has been updated to use a random unprivileged port for NTP time syncs if standard port 123 fails.

11. The location support on been updated to favor an external GNSS device over the internal GNSS module if both have valid fixes.
12. The ability to copy the running firmware image into the secondary firmware partition has been added. This can be done via the Web UI **Firmware Update** page or and **system duplicate-firmware** CLI command.
13. A new Web UI **Status > VRRP** status page and **show vrrp** CLI command has been added.
14. A new Web UI **Status > Scripts** page and **show scripts** and **system script stop <script name>** CLI commands have been added to show and manually stop any custom scripts or applications.
15. The Web UI Hotspot status page and **show hotspot** CLI command have been updated to include the current hotspot status.
16. The Web UI support has been updated to fade out the **Configuration saved** message to fade out.
17. The **update firmware** CLI command has been moved to be under **system**.

## SECURITY FIXES

For this release, the highest rated security patch has a CVSS score of 6.7 Medium.

1. The Linux kernel has been updated to 5.7 [DAL-3322] [CVE-2020-10732](#) CVSS Score: 4.4 Medium [CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L](#)
2. Admin user login rate limiting has been added to prevent additional login attempts for 15 minutes by default after 5 failed attempts. [DAL-3390] CVSS Score: 6.7 Medium [CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N](#)
3. /etc/config/start has been prevented from running when the shell is disabled. [DAL-2846] CVSS Score: 5.2 Medium [CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:L](#)
4. The Web UI has been updated to prevent file path extension on the Firmware Update and File System pages. [DAL-3471, DAL-3513, DAL-3518] CVSS Score: 3.2 Low [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N](#)
5. The Web UI has been updated to prevent cross-site scripting on the Wi-Fi and Bluetooth scanning pages. [DAL-3628] CVSS Score: 3.8 Low [CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L](#)
6. The boot process for the TX54 and LR54 has been updated to prevent it from being interrupted. [DAL-3590] CVSS Score: 4.2 Medium [CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N](#)
7. The SIM PIN configuration has been updated so that it can no longer be displayed in cleartext. [DAL-3462] CVSS Score: 3.2 Low [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N](#)
8. The Web UI HTTP authentication cookie has been set as secure. [DAL-3393] CVSS Score: 3.1 Low [CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N](#)
9. File descriptor leaks on Serial connections has been fixed. [DAL-3202]

## BUG FIXES

1. An issue which prevented RADIUS or TACACS+ authentication from working if local authentication was not enabled has been resolved. [DAL-3701]
2. An issue where IPsec tunnels with multiple policies configured would only properly route traffic for the last policy has been resolved. [DAL-3448]
3. An issue preventing a network interface from initializing if the interface name was longer than 96000472\_D

- 7 characters has been resolved. [DAL-2327]
4. An issue preventing WAN passthrough mode from working if the WAN interface is configured with a static IP address has been resolved. [DAL-3097]
  5. An issue preventing VLANs from being assigned to Wi-Fi SSIDs has been resolved. [DAL-3113]
  6. An issue causing errors to be displayed on the CLI when configuring a USB serial port in remote access mode has been resolved. [DAL-3207]
  7. An issue preventing users from configuring an IP address as a remote syslog server has been resolved. [DAL-3433]
  8. An issue preventing cellular connectivity if a custom gateway/subnet is configured and the device is not in passthrough mode has been resolved. [DAL-3585]
  9. An issue where an incorrect **Age of Data Indicator** value was being reported in TAIP messages has been resolved. [DAL-3249]
  10. The **show system** CLI command has been updated to correctly display the CPU usage statistics. [DAL-2540]
  11. The **show manufacture** CLI command has been updated to correctly display the MCU version. [DAL-3655]
  12. The **modem sim-slot show** CLI command has been updated to correctly display the active SIM slot when SIM slot is in use. [DAL-3569]
  13. An issue where the **mmcli** shell command would report an invalid SIM slot has been resolved. [DAL-3481]

## **VERSION 20.5.38.58 (July 2020)**

---

This is a **recommended** release.

### **NEW FEATURES**

There are no new features in this release.

### **ENHANCEMENTS**

1. The minimum requirements for a local user password has been changed to require the following:
  - a. A minimum of 10 characters.
  - b. At least one uppercase letter.
  - c. At least one lowercase letter.
  - d. At least one number.
  - e. At least one symbol.

### **SECURITY FIXES**

1. Failed login attempts have been added to the event log and will sent to a remote syslog server if enabled. [DAL-3492]

### **BUG FIXES**

14. An issue that caused a delay in connecting with FirstNet SIMs has been resolved. [DAL-3236]
15. An issue that prevented dual APN connectivity with AT&T when using Sierra Wireless modules has been resolved. [DAL-3586]

16. An issue using QXDM with Sierra Wireless cellular modules has been resolved. [DAL-3469]

## **VERSION 20.5.38.39 (April 2020)**

---

This is a **mandatory** release.

### **NEW FEATURES**

1. LDAP user authentication has been added.
2. An option has been added to the **System > Firmware Update** page to allow the user to update the device from the Digi firmware server.
3. Support for Wi-Fi client isolation has been added. This prevents communication between clients connected to the device's Wi-Fi AP.
4. Support for Digi RM proxy connections has been added.
5. A new **Application** mode has been added for serial ports to allow full control of the serial port by custom Python and Shell scripts. This also allows USB-to-Serial adapters to be access via the `/dev/serial/<config-key-name>`.
6. Support for the Python HID module has been added.
7. A Digi RM connection watchdog has been added.

### **ENHANCEMENTS**

1. When factory-defaulted, the device will have 2 Wi-Fi Access Points running on 2.4GHz and 5GHz with a SSID of `<model>-<serial number>` and with the device's default password. The SSIDs and passwords must be configured or the Access Points disabled when configuring the device.
2. The cellular support has been updated to modem PDP context 1 when an AT&T SIM is detected to support new requirements from AT&T.
3. Support for DHCP address pools larger than `/24` subnets has been added.
4. Support for AES GCM encryption ciphers has been to IPsec.
5. A new **locally authenticate CLI** option has been added to force a user to login when using the device's CLI via Digi RM.
6. A number of enhancements to the Health Metrics has been made.
  - A new health metric to report the interface being used for an IPsec tunnel has been added.
  - A new health metric to report the LTE SNR has been added.
  - The health metrics have been updated to upload no more than 2 reports per minute if there is a backlog due the connection being down.
  - A debug configuration option to provide a delay window/jitter when uploading the health metrics to Digi RM has been added. The default is 2 minutes.
  - Prevent invalid health metrics data being re-uploaded if Digi RM sends a response that the contents of the health metrics are invalid.
7. The Web UI has been updated so that the **Apply** button on the Device Configuration page is always visible when scrolling down the page.
8. IPv6 support has been added to the **traceroute** command.
9. The Rx and Tx byte count has been added to the **show network interface <name>** command.

10. The OpenVPN server device type connection options have been added to make it easier to select the connection type.
11. A 5 second delay has been added when configuring the LTE band on a Telit modem and rebooting the modem.
12. Support for AT&T LWM2M on the TX54-A146 and TX54-A246 has been added.
13. The network analyzer support has been updated to allow any network interface to be monitored.
14. The idle timeout configuration for remote access serial ports has been updated to be consistent with the user admin idle timeout configuration.
15. The **show system** command has been updated to display the firmware version in the alternate firmware bank.
16. A **broadcast** option has been added to the **ping** command.
17. A **statusall** option has been added to the **show ipsec** command has been added.
18. The Support Report generation has been improved to only run modem AT commands once.
19. Cellular modem firmware files are now retained in the event of the firmware update is interrupted.
20. The device SKU has been added to the RCI response to Digi RM.
21. The wldata APN has been added to the APN list.

## SECURITY FIXES

1. Updated to openssl-8.2p1 [DAL-2860] [CVE-2019-6111](#) – CVSS Score: 5.8
2. Fixed user escalation exploit through **cloud.drm.sms** configuration option [DAL-2887]  
CVSS Score:6.0 Severity:Medium Matrix: [AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N](#)
3. Fixed user escalation exploit through **Label** configuration setting for serial ports [DAL-3011]  
CVSS Score: 6.0 Severity: Medium Matrix: [AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N](#)
4. Fixed password exploit through web token [DAL-3069]  
CVSS Score: 5.6 Severity: Medium Matrix: [AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:N](#)
5. Updated StrongSwan to 5.8.3 [DAL-2866]
6. Updated iputils to s20190709 and traceroute to version 2.1.0 [DAL-2338]
7. Updated Linux kernel to version 5.6 [DAL-2873]
8. Updated ipset to version 7.6 [DAL-2853]
9. Updated OpenSSL to 1.1.1g [DAL-2977] [CVE-2020-1967](#) - CVSS Score – 7.5 HIGH
10. Prevent DOM XSS (cross-site scripting) exploit on **Terminal** page in the web UI [DAL-3068]  
CVSS Score: 4.2 Severity: Medium Matrix: [AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N](#)
11. Prevent user escalation exploit through netflash options in web UI [DAL-3129]  
CVSS Score: 4.1 Severity: Medium Matrix: [AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N](#)
12. Prevent use-after-free exploit in CLI configuration of OpenVPN [DAL-2963]  
CVSS Score: 5.7 Severity: Medium Matrix: [AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N](#)
13. Prevent XSS vulnerability on the **Filesystem** page in the web UI where a directory name with HTML embedded in it would be rendered as HTML rather than plain text [DAL-3200]  
CVSS Score: 4.6 Severity: Medium Matrix: [AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:N](#)
14. Prevent unauthenticated users from downloading the ovpn client configuration file from the web UI [DAL-3133]

## BUG FIXES

1. An issue with VRRP crashing on the TX54 has been resolved. [DAL-3181]
2. An IPsec tunnel will now be prevented from being setup if the local network/interface is down. [DAL-2336]
3. Stability issues with the TX64 wifi2 radio have been resolved. [DAL-2359]
4. A Wi-Fi as WAN issue that prevented stale contrack entries from being flushed when there are network changes. [DAL-2775]
5. An IPsec issue where an IPsec tunnel configured to use a specific interface would not be brought down properly if the interface went down has been resolved. [DAL-3023]
6. An IPsec failover issue which prevent the backup IPsec tunnel found coming up when the primary IPsec tunnel went down has been resolved. [DAL-3024]
7. The analyzer support has been fixed so that it does not stop when the user's SSH connection ends. [DAL-2154]
8. An issue with applying policy based routes to incoming packets from WAN interfaces has been resolved. [DAL-2589]
9. An intermittent reporting issue where the Web UI and CLI would display a modem as registered when it was actually connected has been resolved. [DAL-2329]
10. An issue that prevented IP passthrough mode from working if multicast was also enabled has been resolved. [DAL-2709]
11. An issue with the IPv6 Surelink ping test has been resolved. [DAL-2488]
12. An issue with custom DHCP options not working has been resolved. [DAL-3071]
13. An issue with the **config revert** CLI command has been resolved. [DAL-3194]
14. An issue where a certificate is not received from a SCEP server due to a timing issue between requesting the certificate with a private key and when that certificate can be downloaded has been resolved. [DAL-2850]
15. The Telit module recovery has been improved if a firmware update is interrupted. [DAL-2983, DAL-2984]
16. An issue with the Python **digidevice.led release** function not working correctly has been resolved. [DAL-2566]
17. An issue with inconsistent LED names in the Python **digidevice.led** module has been resolved. [DAL-2569]
18. Issues with TX54 and TX64 WWAN LEDs not behaving correctly have been resolved. [DAL-1045, DAL-2239]
19. An issue with Sierra Wireless RM7511 modem firmware update via the Web UI or shell has been resolved. [DAL-2772, DAL-2773]
20. An issue with the modem firmware on the TX64-A141 which crashed the modem has been resolved. [DAL-2982]
21. An issue with the cellular modem not initializing after the resetting the modem has been resolved. [DAL-1409]
22. An issue preventing the current firmware displayed on the Status > Modems Web UI page for Telit LM940 modems has been resolved. [DAL-2375]

23. An intermittent SIM switching issues with the Telit LM960 modem have been resolved. [DAL-2379, DAL-2495]
24. An error with the **show modem** CLI command when the modem was not connected has been resolved. [DAL-2959]
25. An issue with configuration backups not working if the configuration directory contained files or directory paths longer than 100 characters has been resolved. [DAL-3137]

## **VERSION 20.2.162.162 (April 2020)**

---

This is a **recommended** release.

### **NEW FEATURES**

There are no new features in this release.

### **ENHANCEMENTS**

There are no enhancements in this release.

### **SECURITY FIXES**

There are no security fixes in this release.

### **BUG FIXES**

1. An issue with the switching firmware when switching between SIMs on the Telit LM940 module has been resolved. [DAL-2986]

## **VERSION 20.2.162.157 (April 2020)**

---

This is a **recommended** release.

### **NEW FEATURES**

There are no new features in this release.

### **ENHANCEMENTS**

1. The firstnet-broadband APN has been added for AT&T FirstNet SIMs.
2. The Rx and Tx byte counts have been added to the **show modem name <name>** command.
3. The MAC address has been added to the support report filename.

### **SECURITY FIXES**

1. Cross-site scripting (XSS) vulnerabilities on the Web UI configuration, status, terminal and file system pages has been resolved. (DAL-2818, DAL-2819, DAL-2823)
2. A script injection exploit on the Web UI Configuration Maintenance has been resolved. (DAL-2797)
3. A fix to prevent unauthorized read/write access to /op/config and /opt/boot when the interactive shell is disabled. (DAL-2865)
4. An issue where the output of the Analyzer could be written out of the /etc/config/analyzer directory has been resolved. (DAL-2672)

### **BUG FIXES**

1. An issue with the Sierra Wireless EM7511 module firmware update has been resolved. (DAL-2794)
2. An issue with the automatic cellular firmware selection on the Telit LM960 modules for T-Mobile and Sprint SIMs has been resolved. (DAL-2376)
3. An issue that was preventing multicast packets from being sent through a network bridge interface has been resolved. (DAL-2774)
4. An issue with the Digi Remote Manager health metrics reporting the /opt directory as full when it wasn't has been resolved. (DAL-2769)
5. An issue where the device would not automatically reboot after restoring configuration using the Web UI has been resolved. (DAL-2862)
6. An issue with the scheduled reboot always using UTC time rather than the configured timezone has been resolved. (DAL-2859)
7. An issue with stopping the analyzer in the CLI has been resolved. (DAL-2892)
8. An issue with the **show system** command on the TX64 when no Bluetooth module has been fitted has been resolved. (DAL-2871)
9. An issue in reading the status of the accelerometer has been resolved. (DAL-2266)

## **VERSION 20.2.162.90 (March 2020)**

---

This is a **recommended** release.

### **NEW FEATURES**

1. The Connection Monitoring and Active Recovery support has been rebranded as Surelink.
15. The default Surelink settings for WAN interfaces has been changed so that the interface will do DNS tests against its DNS server to determine if the interface is working.
16. Read only admin access has been added.
17. A new shell access parameter has been added to allow you to prevent shell access from being enabled for a group. When disabled, script access to the shell and custom firewall rules are also restricted. If this parameter is subsequently re-enabled, the device will factory-default.
18. Support for TX64 user partition encryption has been added.
19. Support for USB GNSS devices has been added.

### **ENHANCEMENTS**

1. The default setting for 'SIM failover alternative' on Modem interfaces has been changed to 'reset'.
2. Hotspot performance has been improved by reducing the amount of log entries being produced.
3. IPsec status and Tx/Rx byte deltas have been added to the health metrics.
4. HTTPS support has been enabled from the initial boot up.
5. The Web UI has been updated to display devices connected to a hotspot.
6. The IPsec performance on the TX64 has been improved.

### **SECURITY FIXES**

1. The libpcap library has been updated to 1.9.1 (CVE-2017-16808, CVE-2019-15163)



2. The tcpdump application has been updated to 4.9.3 (CVE-2018-14465, CVE-2018-14467 CVE-2018-14470 CVE-2018-14879 CVE-2018-16227 CVE-2018-16452 CVE-2019-15167)
3. The libxml2 library has been update to v2.9.10. (CVE-2018-14567, CVE-2018-9251)
4. The OpenVPN support has been updated to v2.4.4 (CVE-2017-12166)
5. The libldns library has been updated to v1.7.1 (CVE-2017-1000231, CVE-2017-1000232)

## BUG FIXES

1. An issue with poor TX54 Wi-Fi client receive speed in bridged configuration has been fixed. (DAL-2353)
2. An issue with the hotspot starting from bootup is has been fixed. (DAL-2446)
3. The health metrics for the TX54 platforms has been fixed. (DAL-2703)
4. The MAC address assignment has been fixed for TX54 and TX64. (DAL-2290)
5. An issue where only the last SSH key configured for a user would work has been fixed. (DAL-2506)
6. An issue with the TX54 (Single Cellular) cellular LEDs has been fixed. (DAL-2659)
7. An issue with the SCEP client handling extra bytes has been fixed. (DAL-2212)
8. An issue with the ping and traceroute commands not routing out of specific interface has been fixed. (DAL-2605)
9. An issue with the TX54 power settings (ignition sense, input voltage, power button behavior) not taking affect has been resolved. (DAL-2734)

## VERSION 19.11.72.85 (January 2020)

---

This is a **recommended** release.

## NEW FEATURES

There are no new features in this release.

## ENHANCEMENTS

1. The performance for TX54 Wi-Fi client interfaces configured as a bridge has been improved.
2. The MTU is now being displayed with the **show route verbose** CLI command.
3. The Python acl.led module has been moved to the digidevice module.

## SECURITY FIXES

There are no security fixes in this release.

## BUG FIXES

1. An issue with the Dual APN configuration on the TX54 and TX64 has been resolved. (DAL-2311)
2. An issue with the Active Recovery support on cellular interfaces has been resolved. (DAL-2000)
3. An issue with VLAN support on the TX54 has been resolved. (DAL-2264)
4. An IPsec routing issue when configuring a remote network of 0.0.0.0/0 has been resolved. (DAL-2253)

5. The missing Wi-Fi configuration for the TX54 Dual Wi-Fi variant has been added to support 2.4GHz band. (DAL-2451)
6. An issues enabling the location support for the TX54 platforms has been resolved. (DAL-2226)
7. The MAC address assignment for the TX54 and TX64 Wi-Fi interfaces has been corrected. (DAL-2290)
8. An issue were N/A would be displayed for Network Activity counters on the Web UI dashboard has been resolved. (DAL-2295)

## **VERSION 19.11.72.53 (December 2019)**

---

The TX54 and TX64 firmware supports the following key features:

- Cellular
  - 4G LTE and 3G support
  - Dual cellular connections
  - SIM prioritization
- Wi-Fi
  - Access Point support
  - Client support
  - Wi-Fi scanner support
  - Wi-Fi hotspot
- Digi Remote Manager
  - Remote Management
  - Device Health Metrics
- VPN
  - IPsec with certificate and pre-shared key authentication
  - HW encryption for IPsec
  - OpenVPN
  - GRE
- SCEP Client support
- Web Filtering / Cisco Umbrella
- Location support
  - On-board GNSS module
  - 3<sup>rd</sup> party source
  - Forwarding to remote hosts
- IPv4/IPv6
- Routing
  - Static Routes
  - Policy based Routing
  - Routing services (BGP, OSPF, RIP, IS-IS)
  - Multicast
- Port Forwarding
- Packet Filtering
- Packet Analyzer
- IntelliFlow

- Bluetooth scanner support

The following features from earlier Digi xOS firmware are not yet supported in this DAL beta firmware. They will be supported before in the production release later this year:

- VRRP+
- SNMP v1/v2c
- SNMP Enterprise MIB
- SSH Certificates
- DMNR
- DHCP Option User Classes