DIGI INTERNATIONAL
9350 Excelsior Blvd, Suite 700
Hopkins, MN 55343, USA
+1 (952) 912-3444 | +1 (877) 912-3444
www.digi.com

Digi TX/LR Firmware Release Notes
Version 23.6.1.105 (July 2023)

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

KNOWN ISSUES

- The Serial status and statistics for the TX54 are incorrect on the Web UI and CLI. [DAL-5763]
- 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]

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. Log into the Web UI.
2. Navigate to the **System > Firmware Update** page.
3. Click on the **Download from Server** tab.
4. Select the appropriate firmware version.
5. Click **UPDATE FIRMWARE**.
6. The device will automatically reboot once the firmware update is complete.

Upgrading TX64 from releases 21.11.60.63 or earlier

If you are upgrading your TX64 device by using the local Web UI, you must first upgrade to release **22.2.9.85** prior to upgrading to the current release.

Upgrading TX54 from releases 21.8.24.139 or earlier

If you are upgrading your TX54 device by using the local Web UI, you must first upgrade to release **22.5.50.62** before upgrading to the current release.

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 on when to apply the firmware update must be made by the customer after appropriate review and validation.

VERSION 23.6.1.105 (July 2023)

This is a **mandatory** release.

NEW FEATURES

1. The ability to do a **SIM survey** on a device using Digi Remote Manager has been added. A connection will be attempted on each installed SIM and a report detailing the SIM connection details such as connection status, signal strength, APN used and cellular tower information is generated. The device will revert to the original setup once the SIM survey is complete.
2. A new serial port **modem emulator** mode to allow them to act as a dial-up modem emulator has been added.

ENHANCEMENTS

1. Better support for updating cellular modem firmware using Digi Remote Manager has been added.
2. A new **VPN iptunnel open routing** configuration has been added to allow packets destined for an IP address which is not explicitly in the device's routing table to exit the VPN tunnel.
3. The following new datastream metrics being reported to Digi Remote Manager have been added:
    - cellular/x/sim/y/registration
    - eth/x/link
    - eth/x/surelink/rtt
    - eth/x/surelink/fail_count
    - wifi/x
    - wifi-ap/x
    - vpn/ipsec/x/disconnects
    - sys/chassis/voltage
    - sys/chassis/temp
4. The device will immediately upload all health metrics to Digi Remote Manager when it establishes a connection for the first time. Previously it would take for the configured **Monitoring > Device Health** metric.
5. The device will now report the cellular modem IMEI to Digi Remote Manager even when there is no SIM installed in the device.
6. A SSH server configured on serial ports will now use any configured custom SSH options in **Services > SSH > Custom** configuration.
7. The Web UI dashboard has been updated to display the interface being used for the Digi Remote Manager connection.
8. A new TCP retry configuration has been added to control the number of times an unacknowledged TCP data packet will be transmitted before the configuration is considered as lost. The default is 15 retries.
9. The help text is in the Serial port modes have been updated for additional clarity.
10. The error message reported when a TACACS+ server cannot authorize the full CLI command due to the RFC length constraints has been updated.
11. A new serial port configuration setting has been added for serial ports in PPP dial-in mode to control whether a default route gets added for the PPP interface. The default is disabled.
12. The **Network > SD-WAN** configuration will not be displayed if the firmware does not support **WAN Bonding**.
13. A system log message will now be generated if WAN Bonding is enabled but unsubscribed.
14. A Support Report will be automatically generated in /opt/digi-support-watchdog-mem-full.bin before a device reboots due to a watchdog timeout.

SECURITY FIXES

1. The Linux kernel has been updated to version 6.3 [DAL-7606]
2. The Busybox package has been updated to version 1.34.0 [DAL-7819]

CVE-2022-28391 CVSS Score: 8.8 High CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

3. The OpenSSL package has been updated to 3.1.1 on the TX64 platforms and 1.1.1u on the TX54 and LR54 platforms. [DAL-7818]

   CVE-2018-16395 CVSS Score: 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
4. The libcurl package has been updated to 8.1.2 [DAL-7817]
5. The OpenSSH package has been updated to version 9.3p1 [DAL-7816]

   CVE-2021-36368 CVSS Score: 3.7 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
6. The libgmp package has been updated to version 6.2.1 [DAL-7820]

   CVE-2021-43618 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
7. The OpenVPN package has been updated to version 2.6.4 [DAL-7822]

   CVE-2020-27569 CVSS Score: 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

   CVE-2020-7224 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2016-7798 CVSS Score:7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
8. The StrongSwan package has been updated to version 5.9.10 [DAL-7823]
9. The DNSmasq package has been updated to version 2.89 [DAL-7533]

   CVE-2021-45951 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2021-45952 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2021-45953 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2021-45954 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2021-45955 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2021-45956 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2021-45957 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
10. Netifd, ubus, UCI and libublox have been updated to OpenWRT 19.07 [DAL-6766]

BUG FIXES

1. An issue with Wi-Fi Hotspot not starting correctly if they were not linked to a network bridge has been resolved. [DAL-7623]
2. An incorrect SureLink status was being reported on IPsec and OpenVPN tunnels has been resolved. [DAL-7893]
3. An incorrect SureLink status was being reported when SureLink was disabled on a network interface has been resolved. [DAL-7552]
4. A SureLink issue where a skipped DNS tests could result in a SureLink failure has been resolved. [DAL-7814]
5. The following issues with SureLink configuration migration from 22.11 and older firmware has been resolved:
   - IPsec and OpenVPN configurations were not being migrated. [DAL-7747]
   - The success_condition setting was not always being correctly migrated. [DAL-7803]
   - The update_routing_table action was being added but was not applicable to IPsec tunnels. [DAL-7892]
   - The SureLink ping test default packet size has been changed from 1 byte to 20 bytes as it was causing issues on some cellular networks. [DAL-7769]
6. The incorrect reporting of the cellular TAC when using a TX54 5G device has been resolved.

[DAL-7941]

7. An issue with errant IPv6 packets being transmitted over a PPP dial-in serial port has been resolved. [DAL-7799]
8. A log message indicating that intelliFlow is unsubscribed will now only be logged if intelliFlow is enabled.
9. An issue where a device would report its MAC address as all zeros when it initially connects to Digi Remote Manager has been fixed. [DAL-1609]
10. An issue using BGP capability 70 on DMVPN hubs has been resolved. [DAL-7740]
11. An issue where a TX54 device getting stuck in a reboot loop if there are updated from 21.11 to 22.11 or 23.3 has been resolved. [DAL-7667]
12. An issue with LTE 4G connectivity with Bell Mobility SIMs has been resolved. [DAL-7350]
13. An issue that caused an error message in the system logs where the Web UI would try to obtain the WAN Bonding status before a user is authenticated.
14. An issue where SNMP wouldn't provide updated settings if a new hostname has been configured has resolved. [DAL-7442]
15. An issue with TX64 devices where /opt directory was not being created during manufacturing, resulting in the device not being able to store configuration changes has been resolved. [DAL-7586]
16. An OSPF issue that prevent IP networks being configured has been resolved. [DAL-7603]
17. A Wi-Fi issue that would prevent multiple SSIDs being scanned when DFS client mode was enabled has been resolved. [DAL-7608]
18. An issue in RealPort authentication has been resolved. [DAL-7651]
19. The following issues with the LM940 cellular modem have been resolved:
    - The LM940 cellular modem could be powered off after a cellular modem firmware update has been resolved. [DAL-7719]
    - The LM940 cellular modem could disappear from the USB bus after switching SIMs. [DAL-7638]

VERSION 23.3.31.129 (April 2023)

This is a **mandatory** release.

NEW FEATURES

1. The **SureLink** support has been updated.
    - The SureLink configuration has been moved from the IPv4 and IPv6 level configuration to interface level.
    - The recovery actions configuration has been changed to be list based so that you can configure a list of recovery actions to be taken on the configured number of SureLink test failures.
    - Support for custom tests and recovery actions have been added.
    - The **show surelink state** CLI command has been added to display the overall pass/fail status of the tests and recovery actions to be taken.

Note: Due to the SureLink configuration changes, the SureLink configuration may be not fully migrated from previous releases. Digi recommends that you review the SureLink configuration before rolling out the 23.6.1.105 release to mission critical devices.

2. **DMVPN phase 1 spoke** support with **NHRP** and **mGRE** including compatibility with Cisco DMVPN hubs has been added.
3. Support for using the **cellular** modem as a **time sync source** has been added.

ENHANCEMENTS

1. **WAN Bonding** support has been updated
    - Options have been added to configure the mode for each tunneled interface and the overall mode.
    - Distance between the WAN bonding and Ethernet bonding settings have been added.
    - The saneclient has been updated to 20221103 for 5G and 1 Gbps performance.
    - A **show wan-bonding** CLI command has been added.
    - A new **Status > WAN Bonding** status page has been added to the Web UI.
2. The **Container** support has been updated
    - Containers can be configured to auto-start on boot with optional parameters and to restart if the container stops.
    - Configuration has been added to setup shared directories between the host file system and the container.
3. The Modem Manager package has been updated to 1.20.6. This includes
    - Improved 5G SA and NSA mode performance.
    - RSRP, RSRQ and SINR statistics for 5G SA mode connections.
    - Native multiplexing for dual-APN setups.
4. **mDNS** support has been disabled by default in order to improve cellular performance.
5. The **ITxPT** support has been updated to support IPv6 for the MQTT broker, GNSS services.
6. **US Cellular** consumer SIM support has been updated so that configured APNs are not required.
7. A new setting to enable/disable **AT&T LWM2M** on the modem has been added. It is disabled by default.
8. The Web UI has been updated to display the system hostname (if configured) on the dashboard page.
9. The IPsec support has been updated to include SHA2 ciphers for IKEv2 IPsec tunnels.
10. **GlobalGIG** APNs have been added to the fallback APN list.

SECURITY FIXES

1. The Linux kernel has been updated to 6.1. [DAL-7179]
2. The OpenSSL package has been updated to 3.0.8 on the TX64 platforms and 1.1.1t on the TX54 and LR54 platforms. [DAL-7261]

    CVE-2023-0401 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

    CVE-2023-0286 CVSS Score: 7.4 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

    CVE-2023-0217 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2023-0216 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2023-0215 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2022-4450 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2022-4304 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVE-2022-4203 CVSS Score: 4.9 Medium CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

CVE-2022-3996 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2023-0286 CVSS Score: 7.4 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

CVE-2023-0215 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2022-4450 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2022-4304 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

3. The netifd package has been updated to 18.06. [DAL-6280]
4. The libexpat package has been updated to 2.5.0. [DAL-7082]

   CVE-2022-23852 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2022-23990 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2022-22827 CVSS Score: 8.8 High CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

   CVE-2022-22826 CVSS Score: 8.8 High CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

   CVE-2022-22825 CVSS Score: 8.8 High CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

   CVE-2022-22824 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2022-22823 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2022-22822 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
5. Wi-Fi pre-shared keys are now obfuscated in Digi Remote Manager. [DAL-7107]

BUG FIXES

1. An issue with updating non-active firmware images on the EM9191 5G cellular modem has been resolved. [DAL-7451]
2. An issue preventing users from locking a device to use a blank APN has been resolved. [DAL-7248]
3. An issue where Wi-Fi channel configuration options appearing as “None” has been resolved. [DAL-7482]
4. An issue that prevented the device from falling back to its local system time when running as a NTP server has been resolved. [DAL-7233]
5. An issue that prevented SIM failover when the device was configured with separate network interfaces set to by carrier instead of SIM slot has been resolved. [DAL-6910]
6. The 3 second stop/start delay when making configuration updates to the MQTT broker settings has been removed. [DAL-7104]
7. An issue with the **tail** CLI command where the match option would only work if the filter option is also set has been resolved. [DAL-7038]
8. An issue that prevented the WAN bonding interface appearing in the **show route** CLI command output. [DAL-6829]
9. An issue where the initial SureLink test would fail if the cellular modem is configured in passthrough mode has been resolved. [DAL-6224]

10. A GRE/IPsec routing problem with a Cisco peer using VTI configuration has been resolved. [DAL-6722]
11. An issue with serial logging enabled on RealPort serial ports that never closed the logging session has been resolved. [DAL-6748]
12. An issue that prevented SMTP notifications from using TLS encryption has been resolved. [DAL-7097]

VERSION 22.11.48.12 (Mar 2023)

This is a **mandatory** release.

NEW FEATURES

1. Support for the TX54 5G variants has been added.

   This release can be used on all TX54 variants.

VERSION 22.11.48.10 (Dec 2022)

This is a **mandatory** release.

NEW FEATURES

1. **ITxPT support** has been added for the TX54 and TX64 platforms. The following services are supported
   - Time Service
   - GNSS Location Service
   - MQTT Broker Service
2. Support for a **MQTT broker** has been added to the TX54 and TX64 platforms.
3. Support for a **FIPS mode** has been added to the TX64 platforms.
4. Support for using **intelliFlow** in **Digi Remote Manager** has been added.

   Note: A Digi Remote Manager Premier license is required.
5. Support for **NHRP** has been added.
6. A system watchdog that monitors critical services and resources and will reboot the system if those services or resources fail has been added.

ENHANCEMENTS

1. DMVPN phase 1 spoke support has been added.
2. The cellular signal strength and quality statistics have been updated to make then more reactive. There is a new **Network > modem > *Interface* > query_interval** has been added to allow the user to configure the rate at which it is update. The default is 30 seconds.
3. Serial port data logging options have been added to the Serial configuration to allow any sent and received on a serial port to be logged, along with the port and mode information. The previous Web UI and CLI command that allowed the serial logs to be manually started, stopped and cleared have been removed.
4. The automatic device and cellular module firmware update options are disabled if Digi Remote Manager in order to prevent conflicts with Digi Remote Manager configurations.
5. Support for enabling / disabling ICMP redirects has been added. ICMP redirects are disabled by default.

6. The CLI commands **tail** and **grep** have been added to allow for better monitoring and searching of the system log and files.
7. The container datapoints that are sent to Digi Remote Manager are now sent with the configured container name instead of the container index.
8. A modem scan timeout option has been added to the **Status > Modems > Carrier Scan** Web UI page.
9. The help text for the **Authentication > methods** has been updated to provide clarification on the mode of operation between authoritative versus non-authoritative options.
10. The error messages in the Web UI when restoring a configuration backup if the web connection is lost before receiving a response has been updated.

SECURITY FIXES

1. The Linux kernel has been updated to 5.19 [DAL-6558]
2. The OpenSSL package has been updated to 3.0.7 on the TX64 platforms and to 1.1.1s on the TX54 and LR54 platforms. [DAL-6991]

   CVE-2022-3786 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3. The shellinabox package has been updated to v2.21. [DAL-5430]

   CVE-2018-16789 CVSS Score: 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H, CWE-835
4. The systemd package has been updated to v245. [DAL-5421]

   CVE-2020-1712 CVSS Score: 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, CWE-416

   CVE-2019-3844 CVSS Score: 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

   CVE-2019-3843 CVSS Score: 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

   CVE-2018-6954 CVSS Score: 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

   CVE-2018-16864 CVSS Score: 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, CWE-770

   CVE-2018-15688 CVSS Score: 8.8 High CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, CWE-119

   CVE-2018-15686 CVSS Score: 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, CWE-502

   CVE-2017-9445 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H, CWE-787

   CVE-2017-9217 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H, CWE-20

   CVE-2017-18078 CVSS Score: 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, CWE-59

   CVE-2017-1000082 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, CWE-20

   CVE-2013-4391 CVSS Score: 7.5 High CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P, CWE-190
5. The jquery package has been updated to v3.6.1 and the jquery_ui package 1.13.2. [DAL-5686]

   CVE-2021-41184 CVSS Score: 6.1 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

   CVE-2021-41183 CVSS Score: 6.1 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

   CVE-2021-41182 CVSS Score: 6.1 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
6. An issue that allowed escalated file system access through Digi Remote Manager has been resolved. [DAL-6784]
7. The default OpenVPN server cipher has been to AES-256-GCM as AES-256-CBC has been deprecated. [DAL-5737]

BUG FIXES

1. An issue with that caused low upload performance with Wi-Fi hotspots has been resolved. [DAL-6674]
2. An intermittent issue with the SIM failover with platforms using the Telit LM940 cellular module has been resolved. [DAL-6569]
3. An intermittent issue that meant that containers could not start due to a permission issue has been resolved. [DAL-7041]
4. An intermittent issue that prevented configuration restores from the CLI due to the output of **show config cli_format** command giving configuration settings in the wrong order has been resolved. [DAL-6435]
5. An intermittent issue with the **digidevice.sms** Python library where it couldn't process MMS messages has been resolved. [DAL-6952]
6. An issue that prevented cellular module firmware updates when no SIM was inserted in the active SIM slot. {DAL-6309]
7. An intermittent issue that caused system performance issues when heavily utilizing VPN tunnels on the TX54 and LR54 platforms has been resolved. [DAL-5926, DAL-6534, DAL-6731]
8. An issue with the output of the **iperf** speedtests has been resolved. [DAL-7001]
9. An issue that prevented the creation of password-protected configuration backup files has been resolved. [DAL-6931]
10. An intermittent issue with the IPsec strict routing mode when a default route change could result in packet not going through the IPsec tunnel has been resolved. [DAL-6518]
11. An intermittent issue where a device configured as a L2TP LAC would drop its tunnel and not automatically reconnect has been resolved. [DAL-5415]
12. An intermittent issue when a device configured as a L2TP server would sometimes drop packets from L2TP client tunnels has been resolved. [DAL-6696, DAL-6724]
13. An issue that prevented L2TP tunnel from running if configured with a name longer than 12 characters has been resolved. [DAL-6718]

DEPRECATION

1. The Bluetooth scanner support has been removed on the TX64 platforms. [DAL-6803]

VERSION 22.8.33.50 (Sept 2022)

This is a **mandatory** release.

NEW FEATURES

1. Support for **DMVPM** has been added.
2. Support for a **PPPoE server** in IP passthrough mode has been added.

ENHANCEMENTS

2. Support for passive Wi-Fi background scanning on 5GHz DFS channels when DFS client support is enabled has been added.
3. Support for starting and stopping a container and getting container status using Digi Remote Manager has been added.
4. The device and cellular module firmware repository has been moved from

firmware.accns.com to **firmware.devicecloud.com** repository.

5. New **system firmware ota download** and **modem ota download** CLI commands have been adding for downloading device or cellular module firmware from the Digi firmware repository.
6. Support for sending container statistics to Digi Remote Manager has been added.
7. A new **strict routing** option has been added to the IPsec support that will only forward packets over the IPsec tunnel if both the source and destination IP addresses match the IPsec tunnel's policies instead of NATing the traffic that only matches the remote network policy.
8. A new **system power profile** configuration setting has been added for the TX64 and TX64 Rail platforms which can be used to manage the CPU frequency and power usage of the device. There are four levels
    - Auto
    - Manual
    - Power Save
    - Performance

    The default setting is Performance.
9. A new **system power leds_enabled** configuration setting has been added for the TX64 and TX64 Rail platforms. The LEDs can disabled in order to reduce power consumption. When disabled, the WWAN1 Signal LED will flash every 15 seconds to indicate the device is powered up.
10. A new **show eth** CLI command has been added to display the status of each Ethernet interface.
11. A **poweroff** CLI command has been added to gracefully power down the device.

    On a TX54 or TX64 that has the ignition sense line connected and is ON, the device will reboot.
12. The **5G-NSA** option has been added to the cellular access technology configuration.
13. The configuration for the speed test and firmware servers has been added to the Digi Remote Manager configuration.
14. The Cellular carrier name and PLMN ID have been added to the **Status > Modems** Web UI page.
15. A **network** configuration parameter has been added to **BGP** to allow the user to configure which networks should be advertised.
16. A configuration option has been added to enable and disable aView style SMS control messages if Digi Remote Manager is being used.
17. Support for MS-CHAPv2 authentication of remote peers on PPP answering interfaces (e.g. PPP over L2TP, PPP over Serial interfaces, PPPoE server in IP passthrough mode) has been added.
18. The ability to store kernel crash information and debug logs across reboots and automatically add them to the system logs has been added.
19. A message indicating that the **WAN Bonding** support requires a Digi Remote Manager license is now shown when in configuration Web UI page.
20. The **System > Update Firmware** Web UI page is now automatically updated when the user clicks on the **Duplicate Firmware** button.

SECURITY FIXES

1. The OpenSSL package has been updated to 3.0.5 on the TX64 platforms and to 1.1.1q on the

TX54 and LR54 platforms. [DAL-6442, DAL-6470]

CVE 2022-2274 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2022-2068 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

2. The Linux kernel has been updated to 5.18 [DAL-6345]

BUG FIXES

1. An issue with the TX54 and TX64 that prevented it from switching back from SIM2 to SIM1 has been resolved. [DAL-5945]
2. An issue that prevent TX54 and TX64 devices using the LM940 cellular module from connecting to the Verizon network has been resolved. [DAL-6186]
3. An issue with the second cellular module on the TX54 and TX64 taking a long time to connect during boot up has been resolved. [DAL-6321]
4. An issue where the SureLink **Reset modem** option would prevent the SureLink SIM failover option from taking affect if both options are enabled has been resolved. [DAL-6343]
5. An issue where the Wi-Fi Client using the second Wi-Fi module would not reconnect to a Wi-Fi Access Point if the signal is lost has been resolved. [DAL-6048]
6. Connectivity issues on a TX64 5G and TX64 Rail platforms with a Vodafone SIM where the device would switch to using Verizon firmware instead of Generic firmware has been resolved. [DAL-6603]
7. An issue with L2TP where a default route was being incorrectly added to the routing table has been resolved. [DAL-6328]
8. An issue when starting a container as a non-privileged user that would fail due permission errors has been resolved. [DAL-5844]
9. An issue where the system log could display entries in the local time and UTC time has been resolved. [DAL-6408, DAL-6520]
10. An issue that prevent the device connecting to Digi Remote Manager via a HTTP proxy over an IPsec tunnel has been resolved. [DAL-6430]
11. An issue with the TX64 Rail platform with Ethernet interfaces continually going up and down when configured in 1Gbps, full duplex mode has been resolved. [DAL-6472]
12. A CLI command line character limitation that prevented long commands or a series of commands being cut and pasted into the CLI has been resolved. [DAL-6445]
13. An issue that prevented the device from connecting to Digi Remote Manager when WAN Bonding is active has been resolved. [DAL-6386]
14. An issue when attempting to download the OpenVPN client configuration template file when the device has a default system name has been resolved. [DAL-6561]
15. An issue where manual carrier selection through the web UI, configuration settings, or Admin CLI would fail to connect if the SIM required an APN username/password with CHAP authentication has been resolved. [DAL-6535, DAL-6552]
16. An issue with sending UCS-2 formatted SMS messages with UTF-16 characters has been resolved. [DAL-6318]
17. A formatting issue with the SIM ICCID metric being sent to Digi Remote Manager has been resolved. [DAL-6394]

VERSION 22.5.50.62 (June 2022)

This is a **mandatory** release.

NEW FEATURES

1. WAN bonding support for bonding multiple WAN connections together for increased maximum throughout or redundancy has been added to the TX54 and TX64 platforms.

   Note: This support can only be enabled using Digi Remote Manager.
2. A Serial PPP dial-in mode for handling AT based connection requests from a device connected on a serial port and providing IPv4 networking to the device.

ENHANCEMENTS

1. The SCEP client support has been enhanced to work with a wider range of SCEP servers.

   The following SCEP servers have been tested:

   - Fortinet FortiAuthenticator
   - DigiCert
   - EJBCA
   - Windows Server

   A new **show scep** CLI command has been added to display the status of the configured SCEP clients.
2. The Wi-FI Scanner functionality has been updated to allow the Wi-Fi Scanner results to be pushed to one or more remote servers using a TCP or HTTP connections.
3. The SureLink “Reset Modem” action has been enabled by default on cellular interfaces with the fail count set to 3. The modem will be automatically power cycled in the event the modem fails to reset correctly.
4. 5G slicing support for a single slice has been added to the TX64 5G platforms.
5. The location support has been updated to support different NMEA sentence content options when forwarding the NMEA sentences to a remote server and there is no valid fix.
6. The cellular APN and connection time have been added to the data points that are uploaded to Digi Remote Manager.
7. The Web UI has been updated to no longer display deprecated cellular modem firmware images on the Modem status page.
8. The NTP server time.accns.com has been removed from the list of default NTP servers unless the aView management system is being used.
9. A new **system.log.persistent_path** configuration option has been added to allow the logs to be stored to a specific location including an external device like a USB flash drive.
10. The Web UI **System > Configuration Maintenance** page has been updated to improve the message displayed when an error is encountered when restoring a back configuration file.
11. The hostname of the device is now included in the OpenVPN client *.ovpn configuration file on the WebUI **Status > OpenVPN > Servers** page.
12. Support for connecting to the Cisco USB Console ports has been added.
13. The APN fallback list has been updated to remove the non-Internet type APNs.

SECURITY FIXES

1. The OpenSSL package on the TX64 has been updated to 3.0.2.
2. The OpenSSL package on the TX54 and LR54 platforms has been updated to 1.1.1o. [DAL-6303]
3. The Linux kernel has been updated to 5.17 [DAL-6081]
4. A Linux kernel patch for the “dirty pipe” vulnerability has been added. [DAL-5981]

   CVE-2002-0847 CVSS Score: 7.5 High CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P
5. The OpenVPN package has been updated to 2.5.6. [DAL-6229]

   CVE 2022-0547 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
6. The gcc tools have been updated to 11.2 and the binutils tools has been updated to 2.37. [DAL-5444]

   CVE-2019-15847 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N, CWE-331

   CVE-2018-12886 CVSS Score: 8.1 High CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H, CWE-209

   CVE-2002-2439 CVSS Score 7/8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, CWE-190

BUG FIXES

1. An issue with the location support for devices configured with a non-UTC timezone which would report an incorrect UTC time when receiving TAIP messages. [DAL-6267. DAL-6335]
2. An issue with missing RSSI values for SSIDs for SSIDs found by the Wi-Fi Scanner when used on a Wi-Fi 6 module has been resolved. [DAL-6030]
3. An issue where an IPsec tunnel failing to reestablish the tunnel if the SAs are deleted after phase 1 re-authentication has been resolved. [DAL-4959]
4. An issue where the connection to Digi Remote Manager could be delayed up to 15 minutes before refreshing to use the active main WAN connection in the event of a network failover or failback has been resolved. [DAL-6164]
5. An issue with the default Wi-Fi AP SSIDs being too long on the TX64 Rail platform has been resolved. [DAL-6329]
6. An issue where OpenVPN > Advanced options > OpenVPN parameters text box was limited to 64 characters when synced with Digi Remote Manager has been resolved. The limited is now 64,000 characters. [DAL-6002]
7. An issue resulting from a race condition when disconnecting from Digi Remote Manager which could cause the Cloud Connector firmware to crash has been resolved. [DAL-5971]
8. An issue that could prevent Wi-Fi Hotspots from initializing correctly has been resolved. [DAL-6306, DAL-6313]
9. An issue that prevented an OpenVPN server from authenticating clients with an external LDAP, TACACS+ or RADIUS server has been resolved. [DAL-6159]
10. An issue that prevented LDAP external authentication for SSH and Telnet sessions has been resolved. [DAP-6098]
11. The **show containers** CLI command has updated to list all containers on the file system and not just those link to configuration settings.
12. Broken links on the Web UI for Digi Remote Manager on the Dashboard and **System > Digi Remote Manager** have been resolved. [DAL-6088]
13. An issue preventing an interface’s MAC address **allowlist** from implicitly denying access to

devices not in the allowlist has been resolved. [DAL-6001]

14. An issue with Python digidevice.config module which could result in a segmentation fault has been resolved. [DAL-6005]

VERSION 22.2.9.85 (March 2022)

This is a **mandatory** release.

NEW FEATURES

15. The internal GNSS module on the TX54 and TX64 platforms can now be used as a time source for the NTP server support.

ENHANCEMENTS

1. Added a SureLink option to switch SIMs if the SureLink tests fail for a configured number of times.
2. A set of new container CLI commands have been added to create, delete and interact with containers.
3. The default URL for Digi Remote Manager has changed to edp12.devicecloud.com.
4. The SCEP client support has been updated with two new settings to allow the user to configure a CA identity and the HTTP URL path for the CA.
5. A debug configuration option has been added to the IPsec support to allow the user to debug an IPsec tunnel.
6. A new serial port option has been added to send a configured string to a remote server when a TCP socket connection is opened on the serial port.
7. The location support has been enhanced with the following new settings
    - UDR support enable/disable (default: disabled)
    - Automatic attenuation enable/disable (default: enabled)
    - Minimum satellite signal level required for navigation (default: 6 dBHz)
    - Minimum number of satellites required for navigation (default: 3)
    - Maximum number of satellites required for navigation (default: 18)
8. The ability for policy-based routes to override the routing of packets through VPN tunnels has been added. This is useful in the case where you only want packets from a certain source network to go through the VPN tunnel.
9. A new TX54 and TX64 **system power ignition off_delay** CLI command has been added to allow the devices power off delay to updated without the configuration being updated. This means the next device reboot it will revert to its configured power off delay.
10. A new configuration setting has been added to allow the user to specify the minimum TLS version that can be used with the Web UI. By default, the minimum is TLS 1.2.
11. If a Sprint Curiosity SIM is being used, T-Mobile carrier firmware will now be used if available.
12. A new **cat** CLI command has been added for displaying the contents of a file.

SECURITY FIXES

1. The DNSMasq package has been updated to version 2.86 [DAL-5331]

    CVE-2021-3448 CVSS Score: 4.0 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N

2. The OpenSSH package has been updated to version 8.8p1 [DAL-5451]
   CVE-2021-28041 CVSS Score: 7.1 High CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
   CVE-2020-14145 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
3. The Linux kernel has been updated to 5.15 [DAL-5546]
4. The Busybox package has been updated to version 1.34.0 [DAL-5631]
   CVE-2021-42373 CVSS Score: 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2021-42374 CVSS Score: 5.3 Medium CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H
   CVE-2021-42375 CVSS Score: 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2021-42376 CVSS Score: 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2021-42377 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42378 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42379 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42380 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42381 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42382 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42383 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42384 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42385 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
   CVE-2021-42386 CVSS Score: 7.2 High CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
5. The dbus package has been updated to version 1.13.20 [DAL-5459]
   CVE-2020-12049 CVSS Score: 5.5 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
   CVE-2019-12749 CVSS Score: 7.1 High CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
6. The GRUB package has been updated to version 2.06 [DAL-5456]
   CVE-2021-3418 CVSS Score: 6.4 Medium CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
7. The bzip2 package has been updated to version 1.08 [DAL-5446]
   CVE-2019-12900 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
   CVE-2011-4089 CVSS Score: 4.6 Medium CVSS:2.0/AV:L/AC:L/Au:N/C:P/I:P/A:P
   CVE-2010-0405 CVSS Score: 5.1 Medium CVSS:2.0/AV:N/AC:H/Au:N/C:P/I:P/A:P
8. The procps package has been updated to version 3.3.15 [DAL-5433]
   CVE-2018-1123 CVSS Score: 7.5 High CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-1124 CVSS Score: 7.8 High CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
   CVE-2018-1125 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
   CVE-2018-1126 CVSS Score: 9.8 Critical CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
9. The OpenSSL build has been updated to include secure compilation flags. [DAL-5472]

BUG FIXES

1. An issue where the TCP socket to location servers were not being properly closed between location messages has been resolved. [DAL-5716]
2. An issue that prevented the device from updating the maintenance window status with Digi Remote Manager if the maintenance window start time was between 00:00-00:59 has been resolved. [DAL-5765]

3. An issue with IPsec where only the first policy would be setup on tunnels using IKEv2 has been resolved. [DAL-5347]
4. An issue preventing IPsec transport mode tunnels from initializing properly has been resolved. [DAL-5718]
5. An issue with SureLink DNS tests that could prevent an interface from coming up has been resolved. [DAL-5934]
6. An issue with QoS HFSC setup to limit bandwidth user for shared links has been resolved. [DAL-5814]
7. An issue preventing port forwarding firewall setups if the destination port(s) setting was left blank has been resolved. [DAL-5680]
8. An issue that where the TX54 and LR54 platforms failing to negotiate with some 10Mbps Ethernet switches has been resolved. [DAL-5506]
9. An issue with the Web UI allowing invalid Modbus client filter values to be configured has been resolved. [DAL-5905]
10. An issue with the Python digidevice SMS module where the callback stops working after a number of SMS messages have sent or received has been resolved. [DAL-5883]
11. An intermittent issue with the **show dhcp-leases** command where not all of the leases were being displayed has been resolved. [DAL-5688]
12. An issue preventing persistent containers from initializing has been resolved. [DAL-5847]
13. An issue with **sh: out of range** was being outputted when starting the test_lxc container has been resolved. [DAL-5845]
14. An issue with the CLI when a TACACS+ server is not configured correctly has been resolved. [DAL-5512]
15. An issue with interruptions of active serial port connections when changes are made to the serial port mode has been resolved. [DAL-5698]
16. An issue preventing MMS SMS message from being received and parsed properly, preventing large out-of-band configuration changes from being from aView/ARMT has been resolved. [DAL-5538]

For information on earlier firmware versions, please visit https://www.digi.com/support