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

Digi Accelerated Linux (DAL) Release Notes
IX-series
Version 20.5.38.58

INTRODUCTION

This is patch firmware release for the all IX-series products.

SUPPORTED PRODUCTS

- Digi IX14
- Digi IX20
- Digi IX20W

KNOWN ISSUES

- GRE and passthrough interfaces do not work when interface name is longer than 7 characters [DAL-2327]
- 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]
- ping interface xxxx CLI command fails when sent through a GRE tunnel [DAL-3300]

UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you update 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 or Digi aView for automated device updates. For more information, follow the instructions for Digi Remote manager or Digi aView in the links below:

1. **Instructions for Digi Remote Manager:**
   https://www.digi.com/resources/documentation/digidocs/90001436-13/default.htm#tasks/t_update_device_firmware.htm
2. **Instructions for Digi aView:**

https://www.digi.com/resources/documentation/digidocs/acl-kb/default.htm#Subsystems/kb-6300-cx/update-firmware.htm

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

1. Download the firmware file from the Digi firmware support page.
2. Connect to the device's web UI by connecting your PC to the WAN Ethernet port of the device and then going to http://192.168.210.1.
3. Select the ***System*** tab on the left side of the page.
4. Select the ***Browse*** button next to the ***Firmware image*** section.
5. Browse for and select the downloaded firmware file.
6. Click the ***Update Firmware*** button.

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, knowledge base and peer-to-peer support forums. Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

VERSION 20.5.38.58 (July 20, 2020)

This is a **recommended** release

ENHANCEMENTS

1. Increased minimum password complexity to at least 10 characters containing at least one uppercase letter, one lowercase letter, one number, and one special character [DAL-3491]
    1. Note: Devices that were running older firmware that had user passwords that do not meet these minimum requirements after upgrading to 20.5.38.58 will still be able to use that password to authenticate with the device. However, if the user attempts to update user's password in the DAL device's configuration settings after upgrading to 20.5.38.58, the updated password must comply with the new minimum requirements

BUG FIXES

1. Fixed delay in connecting with FirstNet SIMs caused by interference from Lightweight M2M (LWM2M) service on Telit modules [DAL-3236]
2. Prevent interruptions to QCDM/QXDM port on Sierra modems caused by ModemManager interaction [DAL-3469]
3. Fixed bug preventing dual-APN connectivity with AT&T SIMs and Sierra modems [DAL-3586]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a High CVSS score of 6.5, which is rated as a Medium

1. Removed ***remote_control*** service used when receiving remote commands from aView/ARMT/AVWOB in favor of HTTPS secure commands. Vulnerability discovered by Stig Palmquist (CVE pending) [DAL-3460]
2. Add failed login attempts to event log sent to remote syslog servers, if enabled [DAL-3492]

VERSION 20.5.38.39 (May 29, 2020)

This is a **mandatory** release

FEATURES

1. LDAP user authentication [DALP-192]
2. Add option on the **System → Firmware Update** page in the web UI to have the DAL device query a firmware server for available firmware updates [DALP-481]
3. Added new **WiFi → Access points → [ssid_name] → Isolate clients** option to enable/disable WiFi client isolation [DAL-2019]
4. Add configuration options under **Central management** for a proxy connection to Digi Remote Manager [DAL-3150]
5. Added new **Enable watchdog** configuration option to monitor the connection to Digi Remote Manager, along with options to reboot the device or restart its connection to Digi Remote Manager if the watchdog times out. The default settings are to restart the connection to DigiRM if the watchdog times out after 30 minutes [DAL-2954]
6. New **application** mode for serial ports to allow full control of serial ports through custom python/shell programs. Also allows additional USB-to-serial adapters to be configured and connected to using the */dev/serial/<config_key_name>* path [DAL-2807]
7. *IX20W:* Add new WiFi SSID and passphrase, enabled by default. The default SSID is now <device model>-<serial num> and the default passphrase is the unique default password of the device [DAL-3050]

ENHANCEMENTS

1. Added the ability to configure DHCP pools larger than /24 subnets [DAL-2864]
2. Add a **statusall** option to the **show ipsec** CLI command to display verbose IPsec status [DAL-2711]
3. Use modem PDP context 1 when an AT&T SIM in inserted to match new requirements from AT&T [DAL-3093]
4. Add AT&T FirstNet IMSIs so they can be differentiated from other types of AT&T SIMs [DAL-3163]
5. Added Python HID module to allow the DAL device to control PSUs via Python programs [DAL-2092]
6. Allow network analyzer to be configured to monitor any network interface instead of just wired Ethernet ports [DAL-2146]
7. Added option to **ping** CLI command to ping a broadcast address [DAL-2571]
8. Added new health metric to report the interface used by the DAL device for its configured IPsec tunnels [DAL-2710]
9. Added new health metric to report the LTE SNR value of the modem(s) on the DAL device [DAL-2904]
10. Limit metrics upload to no more than 2 per minute if backlogged [DAL-2870]
11. Added new **Locally authenticate CLI** configuration option to control whether a user is required to provide device-level authentication when accessing the console of the device through Digi Remote Manager. Default is to allow console access without providing device-level authentication, since the user is already logged in and authenticated through DigiRM [DAL-1510]
12. Report device SKU in RCI response to Digi Remote Manager [DAL-2940]
13. *IX14:* Report the SKU on IX14 variants (was already reported for other IX-series products) [DAL-2539]

14. Add wbdata APN to fallback list [DAL-3182]
15. Improved recovery of Telit modem firmware updates should the update get interrupted [DAL-2984]
16. Fixed spelling of **System utilization** chart on Intelliflow page in the local web UI [DAL-2260]
17. Added new **Health sample upload window** debug configuration option to provide a delay window/jitter when uploading health metrics to Digi Remote Manager (default 2-minutes) [DAL-2607]
18. Commonize the format and naming of rx/tx health metrics reported to Digi Remote Manager [DAL-2896]
19. Add IPv6 options to **traceroute** CLI command [DAL-2618]
20. Add count of bytes transmitted and received to the output of the **show network interface X** CLI command [DAL-2980]
21. Updated **mmcli-dump** command used when generating a support report to only run its list of AT commands on the cellular modem once [DAL-3013]
22. Updated placement of the **Apply** button on the **Device Configuration** page of the web UI to account for usability on smaller screens and keep it always visible when scrolling [DAL-3029]
23. Display the secondary/alternate firmware image version as the **Alt. Firmware Version** in the output of the **show system** CLI command [DAL-3057]
24. Retain modem firmware files in the event that the firmware upgrade was interrupted [DAL-2856]
25. Renamed OpenVPN server **device type** configuration options to clarify which options are OpenVPN managed versus device-only [DAL-2857]
26. Changed the **Idle timeout** configuration settings for remote-access serial ports to use to *blank* instead of *0s*, to better match the format of the **Idle timeout** option for user login sessions [DAL-2623]
27. Added a 5-second wait time between setting LTE band configuration updates on a Telit modem and rebooting the modem to apply the configuration change [DAL-2972]
28. Add support for AES_GCM family of IPsec ciphers [DAL-2715]

BUG FIXES

1. Load FirstNet-specific firmware on Telit LM960 modems when a FirstNet SIM is present (bug affects firmware versions 20.2.x and older) [DAL-3163]
2. Fix VRRP crashes by upgrading keepalived to version 20.0.20 (bug affects firmware versions 20.2.x) [DAL-3181]
3. Prevent IPsec tunnel from being setup if its local network/interface is down (bug affects firmware versions 20.2.x and older) [DAL-2336]
4. Fixed rare issue where the cellular modem could not initialize after resetting the modem (bug affects firmware versions 20.2.x and older) [DAL-1409]
5. Update analyzer to continue running even if the users SSH session ends (bug affects firmware versions 20.2.x and older) [DAL-2154]
6. Prevent re-uploading of invalid health metrics data if DigiRM sends a response that the contents of the health metrics are invalid (bug affects firmware versions 20.2.x and older) [DAL-2868]
7. Fixed bug preventing stale conntrack entries from being flushed when a WiFi-as-WAN (client mode) network changes, connects, or re-connects (bug affects firmware versions 20.2.x and older) [DAL-2775]
8. Fixed timing issue where an IPsec tunnel configured to be built through a specific interface would not be brought down properly if that network interface went down (bug affects firmware versions 20.2.x and older) [DAL-3023]

9. Fixed issue preventing backup IPsec tunnel from being established when primary/preferred tunnel was down (bug affects firmware versions 20.2.x) [DAL-3024]
10. Fixed intermittent reporting issue where web UI and CLI would list the modem as registered when it was actually connected (bug affects firmware versions 20.2.x and older) [DAL-2329]
11. Fixed failing SureLink IPv6 ping tests (bug affects firmware versions 19.11.x through 20.2.x) [DAL-2488]
12. Fixed issue with applying policy-based routes to incoming packets from the Internet (bug affects firmware versions 20.2.x and older) [DAL-2589]
13. Fixed bug preventing passthrough mode from functioning if multicast was also enabled (bug affects firmware versions 20.2.x and older) [DAL-2709]
14. Fixed rare issue with not receiving a SCEP certificate from the server due to timing issues between requesting the certificate with a private key and when that certificate can be downloaded (bug affects firmware versions 20.2.x and older) [DAL-2850]
15. Fixed error displayed in **show modem** CLI output when modem was not connected (bug affects firmware versions 20.2.x and older) [DAL-2959]
16. *IX20W:* Fixed bug preventing default WiFi settings from working on certain platforms (bug affects firmware versions 20.2.162.164) [DAL-3049]
17. Fixed bug preventing local configuration backups if the configuration directory contained files or directory paths longer than 100 characters (bug affects firmware versions 20.2.x and older) [DAL-3137]
18. Fix non-working custom DHCP options (bug affects firmware versions 20.2.x) [DAL-3071]
19. Fix corrupted configuration schema settings after issuing a **config revert** CLI command (bug affects firmware versions 19.8.x through 20.2.x) (bug affects firmware versions 20.2.x and older) [DAL-3194]
20. Fixed issue where IPsec tunnel is built through default route instead of the configured local interface (bug affects firmware versions 20.2.x) [DAL-2889]
21. Removed unsupported LED options listed for LR54 units in their digidevice.led Python module options (bug affects firmware versions 20.2.x) [DAL-3250]
22. *IX20W:* Fixed client connectivity through Captive Portals (bug affects firmware versions 20.2.x) [DAL-3251]
23. Removed empty, blank row from **Filesystem** page in the web UI when listing the contents of an empty directory (bug affects firmware versions 20.2.x and older)
24. Fixed issue preventing users from downloading the ovpn client configuration file from the web UI on the Chrome browser (bug affects firmware versions 20.2.x and older) [DAL-3262]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a High CVSS score of ***7.5***

1. Update to openssh-8.2p1 (CVE-2019-6111 – CVSS Score: 5.8) [DAL-2860]
2. Fixed user escalation exploit through **cloud.drm.sms** configuration option (CVSS Score:6.0 Severity:Medium Matrix: AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N) [DAL-2887]
3. Fixed user escalation exploit through **Label** configuration setting for serial ports (CVSS Score: 6.0 Severity: Medium Matrix: AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N) [DAL-3011]
4. Fixed password exploit through web token (CVSS Score: 5.6 Severity: Medium Matrix: AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:N) [DAL-3069]
5. Update StrongSwan to 5.8.3 [DAL-2866]
6. Updated iputils to s20190709 and traceroute to version 2.1.0 [DAL-2338]
7. Upgrade Linux kernel to version 5.6 [DAL-2873]
8. Update ipset to version 7.6 [DAL-2853]

9. Update OpenSSL to 1.1.1g (CVE-2020-1967 - CVSS Score – 7.5 HIGH) [DAL-2977]
10. Prevent DOM XSS (cross-site scripting) exploit on **Terminal** page in the web UI (CVSS Score: 4.2 Severity: Medium Matrix: AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N) [DAL-3068]
11. Prevent user escalation exploit through netflash options in web UI (CVSS Score: 4.1 Severity: Medium Matrix: AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N) [DAL-3129]
12. Prevent use-after-free exploit in CLI configuration of OpenVPN (CVSS Score: 5.7 Severity: Medium Matrix: AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N) [DAL-2963]
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 (CVSS Score: 4.6 Severity: Medium Matrix: AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:N) [DAL-3200]
14. Prevent unauthenticated users from downloading the ovpn client configuration file from the web UI (CVSS Score: 5.6 Severity: Medium Matrix: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) [DAL-3133]

VERSION 20.2.162.164 (May 6, 2020)

Initial product release for IX20 and IX20W

VERSION 20.2.162.162 (March 17, 2020)

This is a **mandatory** release

ENHANCEMENTS

1. Add MAC address is support report filename [DAL-2863]
2. Add firstnet-broadband APN for AT&T FirstNet SIMs [DAL-2876]
3. Use ***ims*** instead of ***vzwims*** APN on Verizon SIMs for proper IMS registration [DAL-2883]

BUG FIXES

1. *1002-CM04/1003-CM11:* Fixed cellular high-speed throughput performance issues caused by CPU slowdown and timing of gathering cellular signal details [DAL-2802]
2. *1003-CM11:* Fixed inability to utilize SIM slot 2 of an device with a Telit LE910c4-NF or LM940 modem when the two SIM slots contained SIMs from differing carriers [DAL-2897 & DAL-2986]
3. Fix health metrics warnings in Digi Remote Manager stating the local filesystem's /opt/ directory was full when it wasn't [DAL-2769]
4. Fixed missing Rx/Tx bytes in ***show modem*** CLI command output [DAL-2804]
5. Fixed issue preventing multicast packets from being sent through a network bridge [DAL-2774]
6. Fixed auto-reboot after restoring configuration file through local web UI [DAL-2862]
7. Fixed inability to update modem firmware on Sierra EM7511 modules [DAL-2794]
8. Fixed improper modem firmware selection on Telit LM960 module when using a T-Mobile SIM [DAL-2376]
9. Fixed bug causing the configured ***Reboot Time*** to always occur in UTC instead of local timezone (issue present in older 20.2.162.x firmware versions)[DAL-2859]
10. Fixed bug preventing analyzer from being stopped in the CLI [DAL-2892]

SECURITY FIXES

1. Fix cross-site scripting (XSS) vulnerability on various Status pages in the local web UI [DAL-2818]
2. Fix cross-site scripting (XSS) vulnerability on Configuration page in the local web UI [DAL-2819]
3. Fix cross-site scripting (XSS) vulnerability on Terminal page in the local web UI [DAL-2823]
4. Fix cross-site scripting (XSS) vulnerability on File System page in the local web UI [DAL-2823]

5. Prevent script injection exploit on the Configuration Maintenance page in the local web UI [DAL-2797]
6. Prevent unauthorized read/write access to /opt/config/ and /opt/boot when `Interactive Shell` is disabled [DAL-2865]
7. Prevent analyzer output from being saved outside of the /etc/config/analyzer directory [DAL-2672]

VERSION 20.2.162.90 (March 11, 2020)

This is a **mandatory** release.

NEW FEATURES

1. Telit LE910c1-LA modem support [DAL-2391]
2. Telit LM960 LTE CAT18 modem support [DALP-487]
3. Quectel EC25-AF LTE CAT4 modem support [DAL-1817]
4. Digi Remote Manager is set as the default portal for all DAL products [DALP-393]
   - Central management via Digi Remote Manager will not be enabled if you upgrade a device running 19.11.x or older firmware that was previously syncing with an aView instance to 20.2.x or newer firmware, but can be enabled if desired. However, if the device running 20.2.x or newer firmware gets reset (e.g. if someone presses the Erase button on the device, or erases its config through the web UI or Admin CLI), the device will sync with Digi Remote Manager by default.
5. Added SureLink™ default connectivity tests on all WAN interfaces [DALP-402]
   - SureLink tests (previously referred to as ***Active Recovery***) will not be enabled by default if you upgrade a device from 19.11.x or older DAL firmware to 20.2.x or newer firmware, but can be enabled if desired. However, if the device running 20.2.x or newer firmware gets reset (e.g. if someone presses the Erase button on the device, or erases its config through the web UI or Admin CLI), the default SureLink tests **will** *be enabled* as part of the default settings of the device.
6. Background Wi-Fi AP roaming/scanning [DALP-435]
   - New **Background scanning** configuration settings under Client WiFi entries
7. New web UI pages added under the ***System*** drop-down with enhanced serial details and configuration [DALP-465]
8. Support for firmware/OTA updates on Quectel modems [DALP-419]
9. AT&T LWM2M support for Telit LM940/LM960 modems [DAL-2476]

ENHANCEMENTS

1. Prevent access to web UI until HTTPS is ready [DAL-603]
   1. Until the SSL cert is generated, users trying to access the web UI via standard http will receive a redirect page stating that the cert is generating. Once the SSL cert is generated, users accessing the web UI via standard http will be automatically redirected to the https link
2. Show multiple bands for Telit modems if carrier-aggregation is supported and active [DAL-2624]
3. Update wording of help text for WiFi Background Scanning config settings to better reflect their usage [DAL-6673]
4. Added additional Telit-specific AT commands to mmcli-dump of support report
5. Improved Role-based access on local web UI, SSH, and remote access [DALP-415]

Includes new configuration options

- **Allow shell** - NOTE if this options is disabled and subsequently re-enabled, the DAL device will **reset to default settings**
    - **If disabled, the following changes are implemented**

      a) Forced all custom scripts to be sandboxed.

      b) Script sandboxing uses a tighter profile that prevents /bin/sh access.

      c) Sandbox custom firewall scripts to a profile that only allows iptables/ipset/arptables/ip and access to /proc and /sys files. Basically all things firewall related but very locked down. The commands are still run in the shell, but no external commands are available, so the script is limited to basic loops and variable access and no escaping.
- Under each user group under **Authentication → Groups** in the configuration settings:
    - **Admin access**
    - **Access level**
    - **Interactive shell access**

6. New default break sequence ***~b*** for serial connections [DALP-253]
7. Report MCC/MNC/CID/LAC values in health metrics to Digi Remote Manager [DAL-2502]
8. Add digicpn.gw12.vzwentp Verizon APN to fallback list [DAL-2283]
9. Change default OpenVPN Certificate Issuer details from Accelerated to Digi [DAL-2449]
10. Change default SSL certification from Accelerated to Digi [DAL-1336]
11. Dual-APN support on Sierra EM7511 modem [DAL-2311]
12. Include AT#RESETINFO and Quectel-specific AT commands in support report [DAL-2394]
13. Rename ***Configuration Management*** page under the System section of the web UI to ***Configuration Maintenance*** [DAL-2549]
14. Added link under ***System*** drop-down in web UI to download the support report
15. Update the ***Digi Remote Manager*** link under the ***System*** drop-down in the web UI to open in a new tab [DAL-2294]
16. Update the ***Authentication → Idle*** timeout setting to have a default value of 10-minutes (previously the default was blank) [DAL-2292]
17. Send up to 4 IPsec tunnels' details as health metrics reported to Digi RM [DAL-1476]
18. Change the default behavior of the ***SIM failover alternative*** settings from ***None*** to ***Reset modem*** [DAL-2687]
19. Renamed ***Signal Strength*** references to ***Signal Quality*** [DAL-2707]
20. On the Network Status page of the web UI, add ***Interface is up*** message in SureLink status details
21. Add ***service.qcdm.modem.device*** and ***service.qcdm.modem.interface_number*** config options for specifying QCDM/QXDM port for a modem [DAL-2497]

SECURITY FIXES

1. Update to Linux kernel version 5.4.8
2. Removed plain-text passwords displayed in the output of the ***show config*** CLI command [DAL-2513]

3. Added backoff timer when maximum number of SSH/UI login retries is exceeded [DAL-2590]
4. Update to Python version 3.6.10 [DAL-2534]
5. Update tcpdump to version 4.9.3 (CVE-2017-16808 CVE-2018-14468 CVE-2018-14469 CVE-2018-14470 CVE-2018-14466 CVE-2018-14461 CVE-2018-14462 CVE-2018-14465 CVE-2018-14881 CVE-2018-14464 CVE-2018-14463 CVE-2018-14467 CVE-2018-14463 CVE-2018-10103 CVE-2018-10105 CVE-2018-14879 CVE-2018-14880 CVE-2018-16451 CVE-2018-14882 CVE-2018-16227 CVE-2018-16229 CVE-2018-16301 CVE-2018-16230 CVE-2018-16452 CVE-2018-16300 CVE-2018-16228 CVE-2019-15166 CVE-2019-15167) [DAL-2611]
6. Update libpcap to version 1.9.1 [DAL-2611]
7. Update e2fsprogs to version 1.45.5 (CVE-2019-15161 CVE-2019-15162 CVE-2019-15163 CVE-2019-15164 CVE-2019-15165 CVE-2017-16808) [DAL-2611]
8. Update openvpn to version 2.4.4 (CVE-2017-12166) [DAL-2614]
9. Update libldns to version 1.7.1 (CVE-2017-1000231 CVE-2017-1000232) [DAL-2613]
10. Update libxml2 to version 2.9.10 (CVE-2018-9251 CVE-2018-14567) [DAL-2612]
11. Restrict /etc/config/ to admin-only users [DAL-1396]
12. Remove plaintext password from RADIUS debug logs [DAL-2640]
13. Prevent Framebusting JavaScript click-jacking [SEC-494]
14. Prevent users from gaining elevated shell access through custom scripts [DAL-2628]
15. Update libcurl to version 7.69.0 (CVE-2019-15601) [DAL-2732]
16. Update pppd to version 2.4.8 (CVE-2020-8597) [DAL-2732]
17. Fix elevated root access through custom scripts when no-shell is enabled [DAL-2628]
18. Obfuscate sensitive device configuration settings [DAL-1388]

BUG FIXES

1. Fixed bug where SureLink™ DNS tests took longer than the configured timeout to complete [DAL-2702]
2. Fixed SSL validation bug preventing modem OTA updates [DAL-2547]
3. Fixed bug where WiFi hotspot intermittently worked [DAL-2547]
4. Fixed bug where newly-created network Bridges would not be listed as options under the Device drop-down for network interfaces [DAL-2575]
5. Fixed bug where the primary/active interface was not reported correctly to Digi aView when the DAL device was configured for load-balancing between two WAN interfaces [DAL-2568]
6. Fixed bug where a device configured with multiple SSH keys would only honor the last SSH key in the list [DAL-2506]
7. Display the active cellular band for Quectel modems [DAL-2298]
8. Fixed bug where the web UI would display bytes transmitted/received for network interfaces as ***N/A*** [DAL-2295]
9. Fixed bug where the web UI wouldn't show IP information for client devices connected to an OpenVPN server running on the DAL device [DAL-2251]
10. Fix formatting output of ***show config*** CLI command when the configuration settings contained an array [DAL-2594]
11. Fix bug when adding a new element to an array in the ***config*** mode of the CLI [DAL-2594]

12. Fix bug where CLI ping and traceroute commands would ignore any interface specified in the command [DAL-2605]
13. Fix bug where SureLink™ default tests would continue to pass if cellular modem lost its active data connection [DAL-2609]
14. Fix a bug handling certificate files with spaces
15. Fixed padding issue with downloading SCEP CA certificates [DAL-2212]
16. Fixed rare issue with passthrough ancillary DNS not resolving if ***ancillary DNS redirect*** issue was disabled
17. Fixed issue with active serial logins when a serial-related configuration change was applied to the DAL device [DAL-2696]
18. Fixed output of **show modem** CLI command when cellular modem re-initializes
19. Fix potential initialization issues after updating firmware [DAL-2762]

VERSION 19.11.72.85 (January 21, 2019)

This is a **recommended** release.

NEW FEATURES

1. Added new digidevice.led python module for controlling LEDs on the device [DAL-2303]

ENHANCEMENTS

1. Include each interface's MTU to the output of the ***show route verbose*** command in the Admin CLI [DAL-2378]

BUG FIXES

Unless otherwise stated, any bugs mentioned here only affect earlier versions of 19.11.x

1. Fixed bug preventing users from configuring an IPsec tunnel with a remote network of 0.0.0.0/0 [DAL-2253]
2. Fixed timing issue between Active Recovery tests and reloading the devices firewall rules, which if done in the wrong order could result in the device not sending traffic through the validated connection [DAL-2000]
3. Fixed bug where the local web UI would show a *N/A* value for an interface's bytes transmitted/received [DAL-2295]
4. Fixed slowdown in Wi-Fi bridge/repeater mode due to GRO (Generic Receive Offload) being enabled [DAL-2353]
5. EX15/EX15W only: Fixed bug preventing VLAN setups from working (bug present on all firmware versions older than 19.11.72.85) [DAL-2264]

VERSION 19.11.72.58 (December 6, 2019)

This is a **mandatory** release.

NEW FEATURES

1. Re-themed web UI with improved navigation and functionality. New functionality includes:
    - The ability to view local filesystem contents [DAL-2110]
    - Help-text on login page
    - Quick-config access on status pages
    - new Dashboard overview page

- Mobile-friendly UI

2. New network analyzer and packet capture tool, included in in both the Admin CLI and web UI [DAL-1575]
3. Added options under the *Network->Modem* section of the device configuration to setup SIM slot prioritization and SIM slot failback [DALP-287]
4. Added new *Preferred tunnel* option under *VPN->IPsec->Tunnels* to configure a tunnel to be a primary or failover tunnel [DAL-1478]
5. Add new ***DHCP Hostname*** option for IPv4 and IPv6 settings under the ***Network->Interfaces*** section of the configuration to allow the device to advertise its hostname to the DHCP server upon connection (disabled by default) [DALP-427]
6. Added ability to receive encrypted SMS commands from Digi Remote Manager [DALP-270]
7. Add support for the Telit LM960A18 LTE CAT18 module [DAL-1905]
8. Add support for Sierra Wireless EM7511 LTE CAT18 module [DAL-1414]
9. Add support for Quectel EG25-G LTE CAT4 module [DALP-339]
10. Add support for Quectel EG06 LTE CAT6 module [DALP-403]
11. Add Python support on all products (previously only available on the IX14 and Connect IT 16/48) [DAL-1907]
12. Add *system disable-cryptography* Admin CLI command to configure a device for *nocrypt* mode [DALP-491]
13. Once a device is set for *nocrypt* mode, a user must press the Erase button to reset the device to factory default settings to disable *nocrypt* mode and restore the device back to standard operation
14. Add *show usb* Admin CLI command [DAL-2029]

ENHANCEMENTS

1. Improved WebUI performance with crypto speedup
2. Default user changed from root to admin [DAL-936]. Once a device is upgraded to 19.11.72.58 or newer firmware
    1. If you do have an admin user configured, it will not be touched by the update
    2. If you do not have an admin user configured, a new one will appear. It will have the same credentials/settings as the root user
    3. If you had a root user configured (e.g. not factory defaults) it will be preserved to maintain existing user access
    4. Restoring the device to factory defaults after update will result in only the admin user. If you have a root user and do a factory default, you have to login with the admin user instead of root, using the same default password printed on the bottom of the device
3. Added the ability to push OpenVPN routes in subnet mode [DAL-2224]
4. Add cellular IMEI and firmware version, along with bluetooth and accelerometer info to show manufacture command in the Admin CLI [DAL-2030]
5. Add the % measurement value to the CPU usage in the show system output of the Admin CLI
6. Device is passthrough mode with an IPv6 connection now honors and utilizes the MTU in IPv6 RAs
7. When using Verizon SIMs, utilize the OMADM process to auto-discover the APN [DAL-1371]
8. Enhance modem firmware update tool to support multiple modem installations [DAL-2148]
9. Created new Edge firewall zone to prevent the device's DNS services from being advertised on the network, which still allowing SSH and web UI access [DAL-2085]

10. Removed 192.168.210.254 Default IP gateway [DAL-2095]
11. Added support for sending RFC2136 compatible DNS updates to external DNS servers [DALP-446]
12. Add new options under ***VPN->IPsec->Tunnels->Local endpoint->ID->ID Type*** for using the device's MAC address or serial number as its local endpoint ID [DALP-437]
13. Updated the filename of the support report generated through the web UI or CLI to include the Digi name [DAL-1434]
14. Updated the filename of the support report generated through the web UI or CLI to include the Digi name [DAL-1434]

SECURITY FIXES

1. Provisioning the device via Bluetooth using the Digi Manager mobile app is disabled after first-time configuration of the IX14 is complete [DAL-673]
2. Updated OpenSSL to version 1.1.1d [DALP-304]

BUG FIXES

1. Fixed bug where provisioning an IX14 via Bluetooth using the Digi Manager mobile app would disable first-time configuration password requirements (bug present in firmware versions 19.8.1.61 and older) [DAL-552]
2. Fixed bug where Telit LM940 module inside the 1003-CM11 CORE modem could disconnect and not recover due to it starting up in the wrong mode or its serial ports not responding [DAL-1843]
3. Fixed bug where a device in passthrough mode drops received packets from cellular WAN larger than its MTU (bug present in firmware versions 19.5.x through 19.8.1.61) [DAL-2137]
4. Fixed bug with timing of RCI callbacks from Digi Remote Manager (bug present in firmware versions 19.8.1.61 and older) [DAL-2091]
5. Fixed bug where RX/TX data usage metrics reported to DRM could be mistakenly calculated as a negative sum [DAL-1972]
6. Fixed crash in IPsec configuration with more than 6 for IKE Phase 1 proposals or more than 10 IKE Phase 2 proposals [DAL-2066]
7. Fixed bug in reporting the reboot counter metric to DRM [DAL-1932]
8. Fixed bug where persistent system logs could not be remotely accessed through DRM [DAL-2060]
9. Fixed bug where DRM would always shows the device's connected method as ethernet [DAL-1993]
10. Prevent users from selecting non-production firmware versions when perform modem OTA updates [DAL-1662]
11. Fixed bug preventing Linux clients from querying a DAL device running a NTP server [DAL-1815]

VERSION 19.8.1.61 (October 22, 2019)

This is a **recommended** release.

ENHANCEMENTS

1. Skip auto-APN detection when using Telus SIM cards [DAL-1928]
2. Add QCDM service for accessing QXDM ports of Qualcomm-based modems [DAL-1904]

3. Add microcom tool [DAL-1872]

BUG FIXES

1. Fixed bug in runt where the boot version was reported incorrectly (bug present in firmware version 19.8.1.43) [DAL-1828]
2. Fixed registration delays on devices with Telit modems using Sprint SIM cards (bug present in firmware versions 19.8.1.43 and older) [DAL-1872]
3. Fixed stability issues with 1003-CM11 modem (bug present in firmware versions 19.8.1.43 and older) [DAL-1843]
4. Fixed bug preventing devices using a 1002-CM06 modem (Sierra MC7455) with a Telus SIM from loading the Telus carrier-firmware onto the modem (bug present in firmware versions 19.8.1.43 and older) [DAL-1823]
5. Fixed memory leak causing a DAL device in passthrough mode to stop responding to ARP requests on its LAN port (bug present in firmware versions 19.8.1.43 and older) [DAL-1686]
6. Fixed bug preventing SSH keys from being used to authenticate when establishing a SSH session to the DAL device (bug present in firmware version 19.8.1.43) [DAL-1742]

VERSION 19.8.1.43 (August 30, 2019)

This is a **mandatory** release.

NEW FEATURES

1. Telit LE910c4-NF modem support
2. WAN passthrough, allowing for multi-WAN passthrough setups [DALP-163 & DAL-959]
    - As a result, passthrough settings are not under the Modem section anymore, and instead are by default listed under the Network-Interface->LAN section for devices with passthrough enabled by default. To change a device defaulting in passthrough mode to router mode, simply change the "Network->Interfaces->LAN->Interface type" from "IP Passthrough" to "Ethernet", and then you'll see the normal router-mode configurations options available.
3. Auto-generated CLI documentation [DAL-1091]

ENHANCEMENTS

1. ModemManager update to version 1.10.2 [DAL-885]
2. Add verbose system log error messages when issues are encountered posting device health metrics to Digi Remote Manager [DAL-203]
3. Add system log when 1003-CM11 modem (LM940) carrier aggregation is disabled due to temperature limits
4. Include Telit carrier aggregation details in device support report [DAL-1435]
5. Add support for python RCI/SCI data_service callbacks and requests from Digi Remote Manager [DAL-1003]
6. Implement protocol to be used for all local communication between cc_acld and connector clients [DAL-203]
7. Include SIM locked/ready status in `show modem` CLI output [DAL-1320]
8. Update `show modem` CLI output formatting to have a summary mode that can be used to

display the status of the modem(s) in the device, and the verbose output to display additional information for each modem, including the SIM, registration and attachment status [DAL-1184]

9. Improved formatting in the `show route` CLI output, including finer distinction of static routes [DAL-1176]
10. Include policy and connection details in `show ipsec` CLI output, along with improved status details [DAL-1190 & DAL-1174]
11. Improve labeling in output of the `show network interface X` CLI command
12. Show OpenVPN client list and rx/tx bytes in `show openvpn` CLI output [DAL-1192]
13. Add filtering options in `show log` CLI command [DAL-1181]
14. Add CPU usage, device temperature (if available), device description, and location details in `show system` CLI output [DAL-1172]
15. Updated local web UI logout link to list the name of the logged in user [DAL-1142]
16. Renamed the section of central management options from `config` to `cloud` [DAL-1255 & DAL-1256]
17. Added configuration option to have DHCP leases file persistent or clear across reboot [DAL-1196]
18. Update CLI table formatting to double space & blank fields [DAL-1186]
19. Add bypass-lan plugin to strongswan to allow 0.0.0.0/0 remote IPSec networks [DAL-1007]

SECURITY FIXES

1. Update Linux kernel to version 5.1.14 [DAL-1076]
2. Busybox update to version 1.31.0 [DAL-1161]
    - The new busybox shell environment no longer allows local variable statements such as the following:
        - `local ip_addr='1.2.3.4'`
    - and instead the variable must be set without the `local` option, such as:
        - `ip_addr='1.2.3.4'`
    - includes update to httpd webUI
3. Remove option to change Wi-Fi country code on US-products [DAL-1402]
4. Update dnsmasq2 to version 2.80 to address DNS cache snooping (CVE-2017-15107) [DAL-1386]
5. Update conntrack-tools to version 1.4.5
6. Update libnetfilter_conntrack to version 1.0.7
7. Update libmnl to version 1.0.4
8. Update bind to version 9.14.2 [DAL-1338]
9. Update iptables to version 1.8.3
10. Update libqmi to version 1.23.1 [DAL-885]
11. Update libmbim to version 1.18.0 [DAL-885]
12. Update stunnel to version 5.54 [DAL-1162]
13. Update quagga to version 1.2.4 (CVE-2016-1245 and CVE-2017-5495) [DAL-1160]
14. Update tar to version 1.32 [DAL-1159]
15. Add Digi Remote Manager serial port configuration to all DAL products with managed serial ports (previously only available on Connect IT products) [DAL-1213]

16. Remove unused user passwords from /etc/password [DAL-1316]

BUG FIXES

1. Fixed bug causing loss of cellular connectivity on devices in passthrough mode with IPSec tunnels built through the cellular passthrough connection (issue present on firmware versions 19.5.x) [DAL-1612]
2. Fix issues where Telit QMI modems would disconnect from USB hub and not recover [DAL-1321/ DAL-1556]
3. Fix issues where QMI-based modems would disconnect from cellular network and not automatically re-attach (bug present in 19.5.x firmware) [DAL-1375]
4. Fix issue where logging out of the local web UI from the Terminal page would result in the left-side navbar still showing the menu instead of the ***Log in*** link [DAL-863]
5. Fix issue where client devices sending a DHCP request over WiFi to an external server would fail due to the ARP broadcast reply packets having the wrong source MAC address [DAL-1526]
6. Fix issue where a DHCP relay endpoint couldn't be setup through modem or IPSec interfaces [DAL-956]
7. Close any open sessions on a serial port when configuration update changes the mode of the serial port
8. Fix bug in `show network` CLI output when both IPv4 and IPv6 networks were available
9. Fix bug where `show network` CLI command would show incorrect output when no SIM was present
10. Fix bug in returning dynamic-only ref_enums in device config to Digi Remote Manager [DAL-1323]
11. Fix service serversocket binding when cc_acl restarts [DAL-1411]
12. Fix reloading of displayed configuration options when enabling/disabling aView central management in the local web UI [DAL-834]
13. Fix reloading of the Dashboard page when enabling/disabling Intelliflow in the local web UI [DAL-780]
14. Reset LEDs displayed during reboot instead of freezing the LEDs to show the last known device state before the reboot [DAL-886]
15. Fix bug where Digi Remote Manager RCI thread blocks indefinitely waiting for config write lock [DAL-573]
16. Fix bug where `ls` command in the admin CLI required a terminating / on the path [DAL-1251]
17. Fix output of `show wifi` CLI output to show which physical radio a WiFi-as-WAN client is on, instead of a device name [DAL-1171]
18. Fix labeling and format errors in show wifi CLI output
19. Fix multiple SSID traversal with WiFi-as-WAN client setups [DAL-1246]
20. Fix bug with show openvpn name CLI command output [DAL-1191 & DAL-1192]
21. Fix bug with carrier, plmn, and modem status output in show modem CLI command
22. Fix column spacing and lower-casing consistency in show arp CLI output [DAL-1173]
23. Fix parsing of carrier names when posting cellular modem details to Digi Remote Manager [DAL-1553 & DAL-1326]

24. Fix error showing signal strength of WiFi network(s) when the signal was 0% [DAL-1404]
25. Limit decimal numbers reported to Digi Remote Manager to six decimal places [DAL-807]
26. Fixed issue with Telit LE910-NAv2 cellular modules not receiving SMS messages while cellular data session was active/online (bug present on firmware versions 19.8.1.30 and older) [DAL-1634]
27. Add Telus m2m APNs to fallback list [DALP-452]

VERSION 19.5.88.81 (June 26, 2019)

This is a **mandatory** release.

NEW FEATURES

1. Added support for getting NMEA location information from a UDP port (default port 2948) [DAL-1084]

SECURITY FIXES

1. Kernel patch for SACK attack (CVE-2019-11477). For more information, see https://www.digi.com/resources/security

BUG FIXES

1. Fixed bug where IPSec tunnel would cause a system crash when the tunnel was established over QMI-based modems [DAL-1170]
2. Fixed aView tunnel issue where the tunnel drops over time and remote commands fail [DAL-776]
3. Fixed bug preventing QMI-based Telit modems (CAT1 and CAT-M1 modules in particular) from connecting with vzwstatic APNs (bug present on 19.5.88.59 firmware)
4. Fixed bug where the 1003-CM modem (LTE CAT11 Telit LM940) would shut-down and not recover its cellular connection if temperatures were too high
5. Fixed bug where the cellular modem occasionally would not initialize properly on devices with a large number of serial ports

VERSION 19.5.88.59 (May 24, 2019)

This is a **mandatory** release.

NEW FEATURES

1. New CLI with more commands/consistency [DAL-773]
2. Enable Multicast DNS service on all platforms [DAL-972]
3. Implement RADIUS authentication support for users [DAL-903]
4. Add NTP Server option (disabled by default) [DAL-340]
5. Add sftp server to all DAL platforms [DAL-859]
6. ECC Custom Cert Support [DAL-764]

ENHANCEMENTS

1. Improvements to CLI show serial [DAL-1175]
2. Improved reliability of security chip from userspace access due to wakeup
3. Send interface name with cellular status events [DAL-916]
4. Updated ipset version to 7.1 [DAL-917]
5. Update to newest shadow-4.6 package
6. TACACS+ authorization for more server implementations [DAL-933]
7. stunnel updated to version 5.52 [DAL-915]

8. Additional health metrics required for DRM 3.0 [DAL-810]
9. Add support for Telit ME910C1_WW
10. Direct remote serial port access via WebUI (shellinabox) [DAL-775]
11. Dual-APN Support on Telit LE910-NAv2 (1002-CM04) [DAL-818]
12. Improved OpenVPN operation and customization [DAL-798]
13. Update to linux-5.0 [DAL-842]
14. Add ***description*** field to system group [DAL-581]
15. Upgrade MC7455 to 02.30.01.01 (SWI9X30C 2.0 Release 23) added latest Sierra firmware for MC7455 and MC7430 [DAL-759]
16. Add an additional APN for Bouygues in France [DAL-840]
17. Improved Telit location reporting [DALP-226]
18. Improved collection of network LINK and Speed reporting
19. Implement Digi Remote Manager health metrics [DAL-707]
20. Added latest Telit LE910_XX_V2 firmware md5 sums

SECURITY FIXES

1. Update to openssl-1.0.2r (security) CVE-2019-1559
2. busybox: fix for CVE-2014-9645 [DAL-1159]
3. busybox: fix for CVE-2017-16544 [DAL-1159]
4. libcurl: update to 7.64.1 (CVE-2017-8816, CVE-2017-8817, CVE-2017-8818, CVE-2018-0500 CVE-2018-1000300, CVE-2018- 1000301, CVE-2018-14618, CVE-2018-16839, CVE-2018-16840, CVE-2018-16842 CVE-2018-16890, CVE-2019-3822, CVE-2019- 3823)
5. libcurl: fixes for CVE-2018-1000007, CVE-2017-8818, CVE-2017-8816, CVE-2018- 1000005 Zebra 0.99.24: fix for CVE-2016-1245
6. busybox fixes for CVE-2016-6301, CVE-2016-2148, CVE-2017-16544, CVE-2016-2147, CVE- 2017-15874, CVE-2014-9645, CVE-2011-5325 [DAL-1159]
7. pppd update to 2.4.7 (CVE-2014-3158, CVE-2015-3310)
8. Kernel patch to resolve CVE-2019-11815

BUG FIXES

1. Fix issue on 6300-CX preventing WebUI based firmware update up to 1 in 3 tries [DAL-1194]
2. Remote cloud connections were locked until while long running commands completed [DAL-1177]
3. Fix major issue with multiple IPsec policies When two remote subnets are configured in 2 Policies for an IKEv2 tunnel only Policy 2 traffic will pass [DAL-934]
4. Corrections to CLI show route [DAL-1176]
5. CLI ***show system*** output included outdated current time and uptime [DAL-1172]
6. Errors on console during WebUI firmware update [DAL-1140]
7. Faster fetching of signal attributes for LE910_NA_V2 modem
8. Fixed bug with parsing out MCC/MNC from AT#RFSTS response (LE910NAv2)
9. Fixed cloud connector crash on shutdown
10. Fixed process management issue with cloud connector and configuration

11. Check for configured serial ports in ***show serial*** command
12. Fixed bug where ***show serial*** option is visible for devices with no serial ports [DAL-1114]
13. Web GUI input validation rewording to be consistent
14. DAL-CLI: fix typos in descriptions, titles, and minimums
15. WebUI: Ensure correct versions of static files are loaded (using md5hash)
16. Serial ports were mistakenly listed under ***Network*** for metrics and state
17. Metrics had incorrect title, "System" in descriptors/state.
18. ModemManager: Telit error reporting patch
19. Intelliflow crash fix (divide by 0 on some datasets)
20. Intelliflow improve error reporting
21. System maintenance tasks do not run during duration window if reboot time is set [DAL-960]
22. SPIKE: Asynchronous CLI under DRM [URMA-1996]
23. Firmware update through WebUI doesn't recover when some other page is clicked during the update process [DAL-869]
24. Signal/dbm/percentage inaccurate on Verizon 2G and 3G connections with MC7354 [DAL-786]
25. Verify and fix dual APN support on the LM940 [DAL-742]
26. Unable to establish dual-APN connection with AT&T using Sierra modem [DAL-813]
27. Telit: Added logic to protect new C1_AP modems from being bricked [DAL-744]
28. Telit: Added firmware check sum for version 414 of LE910-EU1 [DAL-822]
29. Update Telit LE910C1-NS modem firmware from 25.00.244 to 25.00.246 [NPIX-939]
30. Fix MTU support for PPP based connections
31. Added md5 sums for the latest Telit firmware for LE910_NA1

VERSION 19.1.134.81 (Feb 14, 2019)

- Initial mass production release for Digi IX14