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 22.8.33.52

INTRODUCTION

This is a patch firmware release for the IX15 product. For all other IX-series products, use firmware version 22.8.33.50

SUPPORTED PRODUCTS

- Digi IX10
- Digi IX15
- Digi IX20/IX20W
- Digi IX20-PR/IX20W-PR
- Digi IX30
- **NOTE:** 22.5.50.62 is the final major firmware release for the IX14 product. The end-of-life announcement for the IX14 occurred on 2021-07-21 (see PCN #210721-01)

KNOWN ISSUES

- 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]
- *IX14:* remote HTTPS access to the web UI fails unless the ***Network → Interface → Modem → IPv4 → MTU*** configuration option is set to 1420 or lower [DAL-5788]
- *IX14:* the initial cellular connection after booting up or switching SIM slots can be delayed by 5 minutes [DAL-5489, DAL-5258]

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 LAN Ethernet port of the device and then going to http://192.168.210.1.
3. Select the ***System*** tab on the top navigation bar of the page, then select ***Firmware Update***.
4. Select the ***Browse*** button in the ***Upload file*** 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

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 device 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 22.8.33.52 (September 29, 2022)

This is a ***recommended*** release

Firmware	sha512sum	md5sum
IX15-22.8.33.52.bin	5ab5cd4c7aef522dc4ea89cc3cd344c8b8dfc24908ea8cddc99c19e70adcf94edb31ace57ceafeab320f3dce658ebd5d816bfb555edf8537e20e7bbd684363f2	2be6a40241d9e326210655c97d9e7f88

BUG FIXES

1. Fixed issue preventing users from invoking the ***digidevice.appmonitor*** python module [DAL-6756]

VERSION 22.8.33.50 (August 26, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
IX10-22.8.33.50.bin	56fb5cb26fa92d6e9717475703bdf547b06f8b01f369261fb73282769a88ff734cda1c1fedba027826d16a0037df665bf959e5a865c9fb903dab46c47267e20c	979aacc00bca4dabdf446e8a896968ab
IX15-22.8.33.50.bin	c4e959f0b69a41091ee2109d595bb79b63ecd8e88baf182730feea4233cd11fa70109bd11b6f20242088ea6fe56519ca9aeaa08fd05865641376e7199d74937a	0282f42d5d552ff2bf1521610b797314
IX20-22.8.33.50.bin	4488be68efcd61ec8cd92962766356af237f1d8c48c6250787580a9e7bdaa18684963ab2814fa9c2a96bc6a4b0597f6284102510e5fd48974670c8402a47df36	ecc66c016554f7cecb3fc080963763af
IX20-PR-22.8.33.50.bin	13a7bd1e478f63ff16933a02dd2cf37facce38956877921d9430e26b8150975f3a5415c039b93a81c8409f8f2652f17a4a6134f8bf069fab02a4f367856e289d	65d0d90683f610b522a20e69af36eba9
IX20W-22.8.33.50.bin	eb355b3df54fa54c2688f96a9b051f00a520100259de7556ff171a97f10cc0477590d2829c533e9feb1b0456c597589aa769655088d9e1b088a2155963f6c645	d20e2593379c3d7f9a25e54be6031000
IX20W-PR-22.8.33.50.bin	c635bd76729c3cc0375a62b16fa37091ed97d85d4187efa6dc7fdef5a686ff4541f060052b48badc27cb03c22cfe2b2815e4fad99238a2037f405e56a668b706	032efb7952bd77c6fd9ee13b6690d02d
IX30-22.8.33.50.bin	4fb0a50325f1690a03533333ebb3111e392cf8cafe6c1fdb553cd6e4c16bff46d880c064fc6f19f0e5daba29f13967981bc948621038ce9a63988e6a49cd8cb8	fd9780c601f0a13ddc060db4e4845f8f

FEATURES

1. Added configuration options for running a PPPoE server in IP passthrough mode [DALP-1045]
2. Added Realport serial mode to the IX15 [DAL-6330]

ENHANCEMENTS

1. Update firmware OTA downloads to utilize the Digi Remote Manager firmware repository (firmware.devicecloud.com) [DALP-606]
2. Always display ***Central management → Firmware server*** configuration setting regardless of which central management service is selected [DAL-5719]
3. Always display ***Central management → Speedtest server*** configuration setting regardless of which central management service is selected [DAL-6527]
4. New ***modem firmware ota download*** Admin CLI command for downloading cellular modem firmware from the Digi firmware repository [DAL-6541]
5. Add ability to specify DFS channels under ***Network → Wi-Fi → Client mode connections*** for background scanning when ***DFS client support*** is enabled [DALP-1004]
6. Add cellular carrier name and ***PLMN ID to Status → Modems*** page in the web UI [DAL-6554]
7. Mark Containers as a premium feature enabled via Digi Remote Manager [DALP-1038]
8. Support the ability to start/stop containers via RCI commands from Digi Remote Manager [DAL-6468]
9. Added new metrics for sending container status, name, CPU load, and disk usage as datapoints to DigiRM [DAL-6404]
10. New ***show eth*** Admin CLI command to show the link status of each Ethernet port [DAL-6126]

11. New ***poweroff*** CLI command to perform a graceful shutdown of the device without automatically rebooting [DALP-982]
12. Added new ***Strict routing*** setting to IPsec tunnels that, if enabled, will only route packets through the tunnel if both the source IP and destination IP match the IPsec tunnel's policies instead of NAT-ing traffic that only matches the remote network policy [DAL-5317]
13. Added new MS-CHAPv2 option under ***L2TP → L2TP network servers → Authentication method*** to support clients that require MS-CHAPv2 for authentication to a L2TP/IPsec server [DAL-6327]
14. Store kernel crashes and debug logs across reboots and automatically add them to the system logs in /var/log/ [DAL-6496]
15. Include AT#FWSWITCH output in support reports [DAL-6580]
16. Added ***network.modem.modem.gea1_cipher*** debug config setting that can be can enable GEA1 cipher and speed up initial connectivity and SIM failover on Quectel modems [DAL-5258]
17. Automatically refresh the ***System → Firmware Update*** page in the web UI after a user clicks the Duplicate Firmware button [DAL-4750]
18. Support for the Telit LN920 cellular modem [DAL-5863]
19. New ***System → Power → LEDs enabled*** config setting that can be disabled to turn off all LEDs on the device to reduce power consumption
20. Add disclaimer to ***Network → SD-WAN → WAN bonding*** settings to note that a DigiRM license is required
21. Update WAN Bonding client to version 2022-04071718
22. *IX15:* Added options under ***Services → Modbus gateway*** for communicating with XBee devices in addition to serial ports [DAL-6334/DAL-5933]

BUG FIXES

All bug fixes listed below affect firmware versions 22.5.50.62 or older unless specified otherwise

1. Added new ***Network → Routes → Routing services → BGP → Networks*** section for defining specific IP networks to advertise to BGP peers [DAL-6368]
2. Fixed issue where manual carrier selection through the web UI, configuration settings, or Admin CLI would fail to connect if the SIM required a APN username/password with CHAP authentication [DAL-6552]
3. Fixed L2TP setups so it only adds a default route for the tunnel if the defaultroute custom PPP setting is specified [DAL-6328]
4. Add ***timeout*** option to ***modem scan*** Admin CLI command to allow users to specify a longer scan period for SIMs that can roam to a larger number of nearby carriers
5. Fixed buffer limitation of 1024 characters when copy/pasting text into the Admin CLI [DAL-6445]
6. Fixed issue where kernel-level system logs were logged with UTC timestamps regardless of the locally-configured timezone [DAL-6408]
7. Fixed issue with sending UCS-2 formatted SMS messages with UTF-16 characters [DAL-6318]
8. Fixed issue preventing the Digi device from connecting to Digi Remote Manager over a HTTP proxy through an IPsec tunnel [DAL-6430]
9. Fixed permission issue with starting containers added via Digi Remote Manager [DAL-5844]
10. Fixed invalid format of SIM ICCID metric sent to Digi Remote Manager [DAL-6394]
11. Fixed issue where Wi-Fi client would not reconnect if the config settings were disabled and then re-enabled [DAL-6592]
12. Fixed issue where the ***Reset modem*** Surelink option would prevent the ***SIM failover***

Surelink option from taken affect if both Surelink settings were enabled (affects firmware versions 22.2.x through 22.5.x) [DAL-6343]

13. Fixed issue with downloading client ovpn file from the local web UI [DAL-6561]
14. Fixed issue where the connection to DigiRM would fail if WAN Bonding was enabled [DAL-6386]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a CVSS score of ***9.8 Critical***

1. Update OpenSSL to version 3.0.5 and 1.1.1q (CVE 2022-2274, CVE-2022-2068)
2. Update Linux kernel to version 5.18

VERSION 22.5.50.62 (June 14, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
IX10-22.5.50.62.bin	ad9504775bee8d434cb9731f09de058502da86a42b25d609c661757e41451f5ee24bc90cfc0ae006853cbabf66d889d4a3142311915598895d2d38cfabbcb901	a8b0d2cae8f30a9fe13ae906379c1e80
IX14-22.5.50.62.bin	9583de5c93cbac4ff1ad46cdfd87a68fdd09a52a06569095ff1292e230cdbd0b3695de62330e480b7329224b6525f83bf0bf269725d025689a9d14937b075575	0b5c613bdd54c9de45c6a14508be32e7
IX15-22.5.50.62.bin	54b42f367aee67c3f848a177ec8aeb9e803ef490cdd3584da1cf5dbbf5abb63a4f60db79716fe945d7c8b5115e91e88e4a5c294e5157af5fe93986ad039392e2	d6ded45a1058528c3bcd7b11ef0a4f21
IX20-22.5.50.62.bin	db2cd7812dc9f7bb9115264287320b4a4177ebbaabb7747c96e8bd89d56bf8c32218e9f815ebac168eabf973a85e0c69043241b0cb87363491f6abd9be4aab81	De7bee9e3fc4ae2a8d608025c18ccf8a
IX20-PR-22.5.50.62.bin	f1b04b9db3b637ee1c7cd8b140b37447c01e8de26d5dcfa80ca32411e77bc03df15b42bf7d3279d8f729ca08b68dd80a3efa03a70ec84893110c907cd90520da	5afb2f08b775ab24c2f5356aabb2d723
IX20W-22.5.50.62.bin	7f55e5d96edd4498d8c728c2ffbd67b9feece3d4a23302532b4114222d3926bb848386f4ce061ebc4d7ad6ec7ef49000bdf7c293b54d6ec84cf373ea4e2d85fd	1d61fc036ff8f5045a4ae992fc4e0f64
IX20W-PR-22.5.50.62.bin	464bbef647e200db4ffb23f8a04867ce42266cfb544ad09dc4af19ea465ec20a053e17b9354743b62377c90f889c66759d65f10bd5165da58254cef71ad75cc4	ff885f72a10f90c3028ea1966306e007
IX30-22.5.50.62.bin	2d83f722c8f764f9f04fe82fb1b8dea14efce31db12e9c5f9a1b3b940830b1ea134a2fc2a1f87be71517f7a5cfc131a2089c29cc2541a6a9489429d07f6de7ff	046a5ac8268aae76bb8df1032d213458

FEATURES

1. Serial PPP dial-in mode for handling AT-based connection requests from a device connected to a serial port and providing IPv4 networking to the device [DALP-880]
2. New settings under ***System → Power*** for setting CPU performance level and adjusting power consumption [DALP-983]
3. Realport serial mode added to IX10 and IX30 devices (already available on IX20/IX20W devices on 22.2.x firmware) [DALP-998]
4. New ***Network → SCEP Client*** settings and underlying functionality to support connecting to additional SCEP servers, including Fortinet FortiAuthenticator, DigiCert, EJBCA, and

Windows server [DALP-1007, DALP-1022]

5. New *show scep* Admin CLI command for showing the sync status, expiration dates, and additional details of any configured SCEP clients [DAL-6069]
6. Support for enabling add-on features from Digi Remote Manager [DALP-673]
7. *IX20/IX20W/IX30:* New ***Network → SD-WAN → WAN Bonding*** add-on feature via Digi Remote Manager for bonding multiple outbound Internet connections together for increased maximum throughput or data redundancy [DALP-108]
8. *IX10:* Support for the Fibocom FM101-CG-20 cellular module [DALP-974]
9. *IX10*: Support for the Telit ME310G1-W1 cellular module [DALP-986]

ENHANCEMENTS

1. Remove time.accns.com from default list of NTP servers unless ***Central management → Service*** is set to ***aView*** at the time of updating firmware from version 22.2.9.85 or older [DAL-5543]
2. Added new ***system.log.persistent_path*** configuration setting to specify where system logs are stored locally, which could be on the device or to an external storage (e.g. USB flash drive, SD card, etc) [DALP-946]
3. New ***Services → Location → Destination servers → Behavior when fix is invalid setting*** to control the NMEA message content sent when there is no valid fix from any of the configured location sources [DAL-5984]
4. Improved the message shown on the ***System → Configuration maintenance*** page of the web UI if an error is encountered when restoring from a backup config file [DAL-6141]
5. Include the hostname of the device in the client .ovpn file listed on the ***Status → OpenVPN → Servers*** page in the web UI [DAL-6157]
6. *IX30:* Power off serial port when not enabled [DAL-5991]
7. *IX30:* Power off the Ethernet ports when not enabled [DAL-6063]
8. Add support for the CP210X serial driver for connecting to Cisco USB console ports [DAL-6119]
9. Filter out non-Internet type APNs from our APN fallback list [DAL-6227]
10. Automatically power cycle the cellular modem in the event that a *modem reset* Surelink action fails [DAL-6268]
11. Enable Surelink *reset_modem* action by default on cellular interfaces and set fail count to 3 [DAL-6275]
12. Add cellular APN and cellular connection duration as datapoints sent to DigiRM [DAL-5902]
13. Ensure modem is in enabled state before attempting to connect [DAL-6163]
14. Omit non-production modem firmware from the OTA query results in the ***Status → Modems*** page of the web UI [DAL-6301]

BUG FIXES

The below bugs are all present on firmware versions 22.2.9.85 and older unless otherwise specified

1. Fixed issue preventing Telit LE910 family of modems from registering after changing APNs without a reboot [DAL-5971, DAL-6016, DAL-5203]
2. Fixed issue preventing connectivity with fast.t-mobile.com T-Mobile SIMs when used with a Quectel modem. Use PDP context 1 for connections on Quectel modems with T-Mobile SIMs [DAL-6401, DAL-5930]
3. Fixed issue where modem-based Location source would sometimes not report properly due to an initialization timing error with the modem [DAL-6163]
4. Fixed issue where an IPsec tunnel fails to re-establish the tunnel if SAs are deleted after phase 1 re-authentication [DAL-4959]

5. Fixed issue where the connection to Digi Remote Manager would delay up to 15 minutes before refreshing to use the active main Internet connection in the event of a network failover or failback [DAL-6164]
6. Fixed issue where ***OpenVPN → Advanced options → OpenVPN parameters*** text box was limited to 64 characters when synced with Digi Remote Manager. The new limit is now 64,000 characters [DAL-6002]
7. Fixed issue preventing OpenVPN server from authenticating clients with an external LDAP/TACACS+/RADIUS server [DAL-6159]
8. Fixed broken ***Go to Digi Remote Manager*** link in the local web UI [DAL-6088]
9. Fixed issue preventing LDAP external authentication for SSH and Telnet session [DAL-6098]
10. Fixed typo in description of *container delete* CLI command [DAL-5956]
11. Fixed output of *show containers* Admin CLI command to list all containers on the filesystem, not just those linked to configuration settings [DAL-5958]
12. Fixed issue where the *show location* output in the Admin CLI could include an incorrect timestamp if the configured location server(s) had a non-UTC timezone set
13. Fixed issue preventing ***Network → Interfaces → MAC address allowlist*** from implicitly denying access to devices not in the allowlist [DAL-6001]
14. Fixed ***Invalid lookup path for : network.interface*** error when running *cfg.get("network.interface")* in the digidevice.config python module [DAL-6005]
15. Fixed issue where TAIP messages would have the incorrect timestamp if the timezones between the device and server were different [DAL-6335]
16. *IX10/IX30:* Fixed bug where RTS toggle config setting would be applied in RS-485 serial mode, which should only be used in RS-232 mode [DAL-5990]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a CVSS score of ***9.8 Critical***

1. Update to OpenSSL 1.1.1o (CVE-2022-0778, CVE-2022-1292) [DAL-6035]
2. Update to linux kernel 5.17 [DAL-6081]
3. Patch for “dirty pipe” vulnerability in Linux kernel (CVE-2022-0847) [DAL-5981]
4. Update gcc to version 11.2 and binutils to version 2.37 (CVE-2019-15847, CWE-331, CVE-2018-12886, CWE-209, CVE-2002-2439, CWE-190) [DAL-5444]
5. Update openvpn to version 2.5.6 (CVE 2022-054) [DAL-6229]

VERSION 22.2.9.85 (March 3, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
IX10-22.2.9.85.bin	9360d83f83e004d75e8863918634eb177ff2387dc255ff4e5eca84fbe8a0f8bd8ca5f5fe861f056ee7697f982dd8783d3f09cace10052c97e931d3018489a889	93ce9e08efffcc1e9420c958291dfbf6
IX14-22.2.9.85.bin	5a36679940aae964adc3fb137b5ced97b5bf562ca4d056691536fd2a7930e415d35a5e03692af62012a6c216664433bf8f8ad3e026b0b6fa565cd56d1a4316fb	9bc23e39734752a33b15fc4ae75877ec
IX15-22.2.9.85.bin	2719692985804cc59f0e483963b367ca6443b27110704cc64dfbbca99b30a42e83ee9e8792d52c573231edb8a6222c7be108849852fc1d698231ad80e2fd6333	70b95f91849e1a2f3ff8e309f736a2dc
IX20-22.2.9.85.bin	08702600be63bddede307768253c2c15990f61ec928ea9847498140e67144578187a610f4755afdf17be287a2b7df572230039c72626	de03896ac8097f90ed05e8cdc8dddf57

	e48a0e1d5c8f9d0b9c33	
IX20-PR-22.2.9.85.bin	ae3b43f9e9e5b4b34796efce156f9a0da735dc2e18f0d475a87aa00801dd3a120b553ce549c86cfe62335010dc8ec8dcb85bc27e9eae6fabab7d3ce06134d83b	1ad392435b190289464159dd08f51c05
IX20W-22.2.9.85.bin	21ab62ae2f481d145cc626f9db19df52c4b7cf950918e1e8148acd67c656f1915af2755c7b840a472e8bb878bd488546ba9e79ff2fb30a133dd41e73f500c943	2ce90377d5cc9a3211abdee0a3c3e87a
IX20W-PR-22.2.9.85.bin	8f8c100e1645ed86822fbd1828100cb8c0e4db2ce7bd46c74078e09a3b42059755bc0fd34c5a17cbf55d009a75ce3030a27047e841947439c6d2c25969cce501	71631fe390b34cbb1eddc1b1a4a1fb35
IX30-22.2.9.85.bin	d89b26404a4512d3ae040e7e00bc6401ba11fafc7a84b807e6a02dec3501a4612c056f27d88128690dca8cc114d5b379de3080a385934671fe7541b81c44e2e0	e6910d5da40bfdeb74fecccc833e41a6

FEATURES

1. Initial release for the IX30 product
2. *IX10/IX20:* Realport serial mode support [DAL-5742]
    1. Realport DTR-pin flow control is not available on the IX10. Will be coming in our 22.5 release (see DALP-998)
3. Added new option under ***System → Time → NTP → Use GNSS module*** to enable the device to use its internal GNSS module as a date/time sync source [DAL-5760]

ENHANCEMENTS

1. Update default Digi Remote Manager URL to edp12.devicecloud.com [DALP-972]
    1. In firmware versions 22.2.9.85 and newer, the default central management server changes from ***my.devicecloud.com*** to ***edp12.devicecloud.com***. This change enables more secure connection negotiation and enables support for device certificates. If your device connections are managed by a firewall, or your devices do not have direct access to public DNS servers, you may be required to make firewall changes to open connectivity to edp12.devicecloud.com, or to enable DNS.See https://www.digi.com/support/knowledge-base/firewall-concerns-for-outbound-edp-connections-to for more information about device connectivity to Digi Remote manager.
2. *IX20-PR/IX20W-PR:* Add container support to PR products [DAL-5498]
3. *IX15:* Updated the ***System → File System*** page in the web UI to allow access to the /etc/config/xbee-profiles/ directory for managing XBee config profiles [DAL-5710]
4. *IX10:* Support for the Quectel EC25-AFXD modem [DAL-5787]
5. *IX10:* Add ODIS/LWM2M parameters for EC25-AFXD modem [DAL-5840]
6. Increased web UI upload limit to 512MB [DAL-5694]
7. Added new ***Surelink Switch SIM*** and ***Switch SIM fail count*** options to specify how many times the Surelink test must run and fail on a cellular modem before the device switches to the alternate SIM slot [DAL-5717]
8. Support for standard SCEP servers [DALP-821]
    1. Previously the SCEP client only supported syncing with Fortigate SCEP servers. Two new settings were added under the ***Network → SCEP Client*** options to control the CA identity and HTTP path to the CA
9. Renamed ***VPN → IPsec → Tunnels → Policies → Local network*** setting to ***Local traffic selector*** along with a new ***Dynamic*** option which allows users to configure a local network by protocol and/or port instead of a network address range [DAL-5645]

10. Added new ***VPN → IPsec → Advanced → Debug level*** option to specify the logging verbosity of IPsec messages in the device system logs (default is debug logging is disabled) [DAL-5720]
11. Added new ***Serial → Autoconnect → Socket ID string*** option to send the configured text to the remote server(s) when a TCP socket connection is opened to the serial port [DAL-5700]
12. *1002-CM06/1003-CM07:* Utilize T-Mobile carrier firmware if available for the cellular modem when using Sprint Curiosity SIMs [DAL-5466]
13. New cat Admin CLI command for displaying file contents [DAL-5853]
14. Update /etc/config/scep_client/ directory to be read/write by admin users
15. Add ability for policy-based routes to override routing of packets through VPN tunnels, useful in the case where you only want packets from a certain source network to go through the tunnel [DAL-5317]

BUG FIXES

The below bugs are all present on firmware versions 21.11.60.63 and older unless otherwise specified

1. Fixed HFSC class hierarchy setup for QoS policies to limit bandwidth used for shared links [DAL-5814]
2. Fixed issue preventing scheduled maintenance window from updating the maintenance_window datapoint in Digi Remote Manager if the maintenance window start time was between 00:00-00:59 [DAL-5765]
3. Fixed bug preventing MMS SMS messages from being received and parsed properly, preventing large out-of-band config changes from being received from central management portals [DAL-5538]
4. Fixed issue preventing transport-mode IPsec tunnels from initializing properly [DAL-5718]
5. Fixed issue where only the first policy would be setup on IKEv2 IPsec tunnels [DAL-5347]
6. Fixed issue preventing port forwarding firewall setups if the ***Destination port(s)*** setting was left blank [DAL-5860]
7. Fixed intermittent issue where the ***show dhcp-leases*** CLI output would sometimes not include all leases [DAL-5688]
8. Fixed system log errors when performing TACACS command authorization without having a TACACS server configured [DAL-5512]
9. Fixed interruption of active serial port connections when a user changes the serial port mode in the Digi device's configuration settings [DAL-5698]
10. Fixed issue where Surelink tests aren't reloaded if a user updates the network bridge or Wi-Fi configuration settings on the device [DAL-5406]
11. Prevent modbus setup issue by not allowing users to configure the device to use reserved address ranges [DAL-5905]
12. Fixed intermittent race condition in Surelink that could lead to a delay in setting up a WAN connection [DAL-5934]
13. Fixed issue with digidevice.sms python module processing empty SMS messages [DAL-5883]
14. *IX20W:* Fixed issue preventing Wi-Fi metrics from being uploaded to DigiRM

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a Critical CVSS score of ***10 Critical***

1. Update python to version 3.10 [DAL-5499]
2. Update openssh to version 8.8p1 (CVE-2021-28041, CVE-2020-14145) [DAL-5451]
    1. This deprecates support for RSA signatures using the SHA-1 hash algorithm by default,

which may prevent old machines from SSH-ing to the Digi device. Please ensure your SSH tool (TeraTerm, PuTTY, etc) is up to date. If you need to re-enable SHA-1 hash support, you can do so by adding the following lines to the ***Service → SSH → Custom configuration → Configuration file*** text box in the Digi device's configuration settings:

1. HostkeyAlgorithms +ssh-rsa
2. PubkeyAcceptedAlgorithms +ssh-rsa

3. Update dnsmasq to version 2.86 (CVE-2021-3448) [DAL-5331]
   1. Fix problem with DNS retries in 2.83/2.84
   2. Fix a problem, introduced in 2.83, which could see DNS replies being sent via the wrong socket. On machines running both IPv4 and IPv6 this could result in sporadic messages of the form "failed to send packet: Network is unreachable" and the lost of the query
4. Update to Linux kernel version 5.15 [DAL-5546]
5. Add new ***Service → Web administration → Minimum TLS version*** configuration setting to allow users to specify which TLS versions are allowed in the local web UI (default minimum is TLS 1.2) [DAL-5408]
6. Update busybox to version 1.34.0 [DAL-5631]
   1. CVE-2021-4237, CVE-2021-42374, CVE-2021-42375, CVE-2021-42376, CVE-2021-42377, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42383, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386
7. Update dbus to version 1.13.20 [DAL-5459]
   1. CVE-2020-12049, CVE-2019-12749
8. Update grub to version 2.06 [CVE-2021-3418] (DAL-5456]
9. Update bzip2 to version 1.0.8 (CVE-2019-12900, CVE-2011-4089, CVE-2010-0405) [DAL-5446]
10. Update procps to version 3.3.15 [DAL-5433]
    1. CVE-2018-1124, CVE-2018-1123, CVE-2018-1126, CVE-2018-1125
11. Hardened openssl build to include secure compilation flags
12. Update sqlite to version 3.37.2 [DAL-5669]
13. *IX20W-PR:* On PR FirstNet products, enable the ***Network → Wi-Fi → Access points → Digi AP → Isolate clients*** setting by default so Wi-Fi clients connecting to the Digi device's SSIDs are isolated from each other by default

VERSION 21.11.60.63 (December 8, 2021)

This is a ***mandatory*** releases

Firmware	sha512sum	md5sum
IX10-21.11.60.63.bin	892bf3099cda0a8c5991030af092b8a56241b1e47bcb77235a3c7f79034032bb8c5903f423af37dbfc0443340d385c47047126f061bf9b935aca92c76951613e	b3302801d9c7b0be073291e3204463eb
IX14-21.11.60.63.bin	dc9b8c18607e746749d6007a8545bf16b0da4e5448aa06719a576c7d8270628cc893a034bebcf7c675124f445c32e92fa6416b53fce7d0f1c123b84f94bacc0b	644774a75aedd007306ea4f9431f3147
IX15-21.11.60.63.bin	08251a5129d41c812e8d04fd338415590467d5c1cbf369f6bb74a8d900421c77e5ca1508fad75c23b8231c96f08f93b123c070de7bbb0a9dc9206af5ae0017e5	05118bfdeb4098ab014fca7cf44d29b6
IX20-21.11.60.63.bin	0117847cd52661c6403fbe51f60f9cf725e3e3b5f823fe6b3ed1216ed463856836e5648fa039a4e543f7b0ee019a19c29ab10d1d4c107a86bdef9ebf652f872e	e61a492f997e743b909e0b30a86915fa
IX20-PR-21.11.60.63.bin	867e7c32b49c2e029f194901795520f04090823fed9a59938df8de3606486bb0d8dfd2b655e5dcac8e6a82239bcb2d1a664c11357297f3704b4a2f85bb6b7aaf	1ecf60261eedcb3ac92ad7cf9ab00078

IX20W-21.11.60.63.bin	4d3214368640fb94c808b58adaf345caef5988e0d750e9e36dca3539c7a8313538ff21eb65ee76442e46a15d5de52ad6933d5baba5571d8c1cfe28f9b36342d9	b664624f58cd808ee5ade9bf678c538e
IX20W-PR-21.11.60.63.bin	40172c2aa46e1ee12a4a4c3f03b5c7aaaa6eee8ab85ebdc11383954aa2e1bbaea4a357ae2c34685ca2bede0017366a2d48df6c86d3f36b94c441dcf216aca30b	fe23cc6563b955a9b56551ce2484b843

FEATURES

1. New **System maintenance → Device firmware update** config option to allow the device to automatically update to new firmware when available (disabled by default) [DALP-630]
2. TACACS+ accounting and authorization for Admin CLI interactions [DALP-633]
    1. Includes two new configuration settings under the **Authentication → TACACS+** configuration settings for enabling TACACS command account and/or authorization
3. Add new *Authentication → Users → Username alias* option for providing an alternate username that can accommodate characters not typically allowed in a username [DALP-705]
4. PKI certificate-based authentication for WPA2/WPA3 Enterprise Wi-Fi client connections, including options for user-provided certificates or SCEP client integration for automatic certificate generation [DALP-828 & DALP-794]

ENHANCEMENTS

1. Improved Wi-Fi scanning tool on the **Status → Wi-Fi → Management** page in the web UI to automatically setup the underlying basic client-mode settings so the device can scan for nearby APs without requiring the user to first configure the client-mode settings [DALP-802]
2. New **show surelink** Admin CLI command for displaying details on the Surelink test(s) configured for a network interface or VPN tunnel [DALP-621]
3. Add new option under **Location → Destinations** for specifying the talker ID used in NMEA message strings [DAL-5038]
4. *1002-CMM1 CORE modems:* Use CID context 3 for any type of Verizon SIM when used with a ME910c1-WW modem [DAL-5428]
5. Include the mode indicator field in NMEA messages constructed when a GPS fix isn't obtained [DAL-5464]
6. Add support for auto-completing a parameter or AT command provided to the **xbee set|get|execute** Admin CLI commands [DAL-5196]
7. Change default IPsec IKE DH group to 14 for enhanced compatibility with industry standard settings [DAL-5344]
8. Disable serial history in remote access mode by default [DAL-5494]
9. Add new settings under cellular Surelink options to have the device reset the cellular modem if a specified number of Surelink tests fail [DAL-5441 & DAL-5485]
10. Add **datapro** APN to fallback list to be utilized with Airmob SIM cards [DAL-5548]
11. New **show containers** Admin CLI command for listing details about configured containers [DAL-5380]
12. Include SIM ICCID and phone number in the query_state response sent to Digi Remote Manager [DAL-5632]
13. Specify string encoding as UTF-8 in communication with DigiRM for compatibility with extended charactersets [DAL-5505]

BUG FIXES

The below bugs are all present on firmware versions 21.5.56.176 and older unless otherwise

specified

1. Fixed issue preventing IPsec tunnels from being setup in Transport mode [DAL-5490]
2. *IX14 or 1002-CM04/1002-CME4 CORE modems:* Fixed issue where cellular modem firmware updates would not be applied to Telit LE910-family of modules unless the firmware file included a carrier name in the filename [DAL-5616]
3. *1003-CM07 CORE modem:* Fixed issue preventing multi-carrier firmware updates on Sierra EM7411 modems [DAL-5473]
4. Fixed issue preventing **on boot** SIM preference schedule from taking effect (bug present on firmware versions 21.8.x and 21.5.x) [DAL-5547]
5. Fixed issue preventing internal firewall from functioning properly if a port forwarding rule was configured with the protocol type set to **other** (bug present on 21.8.x firmware) [DAL-5501]
6. Fixed issue preventing IPsec tunnels from being setup properly if the tunnel name was longer than 9 characters [DAL-5139]
7. Fixed formatting of cellular-related health metrics so they can be properly displayed under the *Settings → Status → Cellular* section in Digi Remote Manager [DALP-768]
8. Fixed error in system log when attempting to parse an empty config file [DAL-5402]
9. Fixed issue causing potential multi-minute delays in the *show modem name XX* Admin CLI command [DAL-5297]
10. Fixed issue where Surelink ping tests would utilize the same source IP address if coming from different network interfaces assigned to the same physical device/port [DAL-5478]
11. Fixed issue where Surelink **reboot** action would not be take if the Surelink **restart interface** action was also enabled [DAL-5485]
12. Fixed issue preventing the creation of config elements with dynamic array names via the local web API [DAL-5481]
13. Fixed issue preventing installation of sqlite3 python package via pip [DAL-5611]
14. Fixed issue preventing multiple config changes from being applied in a python script using the digidevice.config module [DAL-5192]
15. *IX20W:* Fixed issue where the Wi-Fi LED was always illuminated even if no client or AP connections were enabled [DAL-5296]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a Critical CVSS score of ***9.8 Critical***

1. Update to python version 3.6.15 [DAL-3190]
2. Update stunnel to version 5.60 [DAL-5291]
3. Update busybox to version 1.33.1 [DAL-5290]
4. Update to Linux kernel version 5.14 [DAL-5360]
5. Update OpenSSL to version 1.1.1l [DAL-5242]
6. Fixed issue where the TACACS shared secret was included in the system logs [DAL-5470]
7. Update libunbound to version 1.13.2 [DAL-5420]
8. Update libidn2 to version 2.3.2 [DAL-5439]
9. Update muslv to version 1.2.2 [DAL-5452]
10. Update rsync to version 3.2.3 [DAL-5431]
11. Update OpenVPN to version 2.5.4 [DAL-5435]

VERSION 21.8.24.143 (October 22, 2021)

This is a **recommended** release

Firmware	sha512sum	md5sum
IX20W-21.8.24.143.bin	162af9869025b8d1e981056a2df798e57d9ed7c25d3fd62352ed3a2f05756f09bdc9cea3779f4146a89211d4842c50782a957a9f10d6c198e7a5fe92abe05a86	14b176f00318d8d3809c2e2cc10aa81c
IX20W-PR-21.8.24.143.bin	9572bc92b930dcb6d1847abc6bd0472a6266ce15a303d58e7b5882edd881830195accf8bea2b8b3822f66ba1db1bbe0b72e3748148b013da1c9ef1b66c788042	de72b8df160dfae4f47f2d9700cf869a

ENHANCEMENTS

1. Update Wi-Fi driver for EU compliance [CELL-106]

VERSION 21.8.24.139 (October 7, 2021)

This is a **recommended** release

Firmware	sha512sum	md5sum
IX10-21.8.24.139.bin	6c2c4ed22272aabf55343dabbe9417cfae7f16a1b081f1dc26abea5590bba01abfb05bb4567b29b3438e70f87a5d7d0c846ed53ec0b6ad98f547cd37230866d7	1e49403ab57e49afd8c7fb8ca7b81a12
IX14-21.8.24.139.bin	ecfb2d23f7a2c25d2d1f3ca458d9b71f7fccbc89efc7a08f8f716bf388eee05509ae32dd4e66424fd067ff7e86a4e000f7fa9eb48e2b36f59d25c1cff66d347e	a64c9360277fc10f5d7461fd35395981
IX20-21.8.24.139.bin	f886867d7cc79f48a27879be622e81aa1ff89c0c9e46026dff432edcb42a7955f97653e1aa833ca2590b77be6b94a358fa9d4b3c001a925985f1b88d9a90e4da	596efbf49c309959df18b9a77742b666
IX20-PR-21.8.24.139.bin	8d0c5e4216f5601186379d5cd88c196f225edce8400afe16c6ad6d6fa21fa261452edd3282c19645de306d01861200cd9d1066dbd9aa322d6a91eb53cc582936	c2a1676970d34512265823fac293c2ef
IX20W-21.8.24.139.bin	6ffb74f74283d85436eea1d4efc0ce117fe1b2cd6567116eee65a3c4fbdddfbb567a5bd1a9ed1e9cdfc3ac4234c6fef3b5a2711b5a6dc95e31fe8e3c50780462	054e6e7070de9008f4704c900da6cb26
IX20W-PR-21.8.24.139.bin	96706b477b790872821868be1b4825afde7fbe14507486ac186edd4c4e8b8a2e4752b2144ba976464800b84b572c8a5556c26de07e1c1a9c8d23c10095affbc5	8b5d94ab590a09e6965af19c9a5a4035

BUG FIXES

2. Fixed issue where device would not re-establish its cellular connection after updating to 21.8.24.129 firmware (affects all IX-series products except the IX15) [DAL-5346]
3. Prevent automated health metrics uploads and manually initiated/generated health metrics from interfering with each other
4. IX10/IX15: Fix RTS pin control on RS485 serial port when used as a Modbus gateway (bug present on firmware versions 21.8.24.129 and older) [DAL-5322]

VERSION 21.8.24.129 (September 13, 2021)

This is a **recommended** release

Firmware	sha512sum	md5sum
IX10-21.8.24.129.bin	3c5a6ad86c4e9145a735e16dc13168f97956223b5806	fa2e2f8850bacc0b28a5c905dc3ecadb

	e721f3d02e8828ff7cc15bcf233d9c5f3a9694d62aaffbd9fa45f612036152ab7fcd88706bab0fddf6cc	
IX14-21.8.24.129.bin	ca591c8a989255f781d68e7f1cb09843eed20120d54285a6c300ff6eb5fa74805cf8c7a9bcbcdc97d6d5feec21dc50680988dbb10963d75e04385986156c84e5	73cf5050c90222207308f0a0445fd90d
IX15-21.8.24.129.bin	278b465d127b1c1fbfa53b1a6d04212464de34a47fad41444ae33e5c37128d8ebfa1c25e2260bca629b40d1a3d8b86db27d0481721323a8342eb80338cdb8d38	12bca5e2e75bfd9a93e6742a4e7333f4
IX20-21.8.24.129.bin	047eb31e4483a1d97ef6d836e1275a492865db42b4792fc0d9d8c07254f8f274e4b45641b8da6faabf88e6c7e1966f5b633ba6588412cb2d57a86f60c3fde689	733c3866a5cc0251125e67261270cf26
IX20-PR-21.8.24.129.bin	938cdad630fa6b5de137f275e47b6a44dee06f36599fb3f0a5207007a6319bb0d4c35355145e74b3ba4a19d8a3b4b7c3bd61fa4502e9e688bc22678b2174ba11	9fc034e8f092b78288dace719548194f
IX20W-21.8.24.129.bin	476f90b0e3d8c838d60bdfe387bbed51b3333636dfc28f250e6da7af751cb34af8fad3bd4dcaef85d600a622e66188c008ce975be661322248116a2fcf1e682e	d07c79b084cf7c3d968d6f3a5268edf7
IX20W-PR-21.8.24.129.bin	d92ba876ba220c6713747c7b7fc7e95915d47881fa2554f3b9e79266ac00edabab4fff17279ddd9595f8b8dbdfc9dc0da2022bff343b3551c8a282b234bdc286	c22e5f0be35e1a939b0c092961b1ba09

FEATURES

1. LXC container support for running localized containers on the device [DALP-243]
    1. New ***System → Containers*** configuration settings for provisioning containers, providing virtual networking, and serial port access from the container
    2. ***lxc*** commands available in the shell console for managing/accessing/monitoring containers on the device
    3. Containers are based off the host DAL device's system. Packages installed to the container must be built for the CPU architecture designed
2. L2TPv3 static/unmanaged VPN tunneling [DAL-5137]
    1. VPN -> L2TPv3 ethernet configuration setting
    2. New Status -> VPN -> L2TPv3 Ethernet web UI page
3. 802.1x port-based network access control, configurable per network interface [DAL-5080]
4. New **Services → SSH → Custom configuration** settings for overriding or editing the SSH server options
5. New **Monitoring → Device event logs** options for sending local device event logs to Digi Remote Manager [DALP-808]
    1. Event logs are controlled under the **System → Log → Event categories** configuration settings
6. New ***VPN → IPsec → Tunnels → IKE → IKE fragmentation*** option to enable, disable, or force IPsec IKE fragmentation [DAL-4933]
7. New **MAC address allowlist/denylist** options to allow/deny packets based off of a range of source MAC addresses [DALP-799]
8. New **system time** CLI command for manually setting the local date and time [DALP-520]
9. New **monitoring metrics upload** CLI command for sending on-demand health metrics to Digi Remote Manager [DALP-727]
10. New **system script start** CLI command and **Status → Scripts** page in the web UI for manually starting custom scripts configured under the **System → Scheduled tasks → Custom scripts** settings with a **Run mode** of **manual** [DALP-741]

11. New **system find-me on|off** CLI command and **Status → Find Me** button in the web UI for flashing cellular-related LEDs to help locate the device onsite [DAL-5142]
12. New ***Network → Bridge → switchport*** bridge type configuration settings for enhanced VLAN capabilities [DAL-5220]
    1. trunked vs untrunked ports
    2. virtual switch setups
    3. VLAN layer 2 networking

ENHANCEMENTS

1. *IX10:* Add option to utilize GPS from cellular modem inside the IX10 as a source for the Location service [DALP-849]
2. Added new **show l2tpeth** CLI command for viewing the status of any configured L2TPv3 tunnels [DAL-5220]
3. Update python pip to version 21.2.4 [DAL-5068]
4. Shortened fallback APN list by removing wildcard entries [DAL-5012]
5. 3G sunset support for EU carriers [DAL-5041]
6. Update messaging included in keepalive packets sent to Digi Remote Manager to prevent multi-second delays in keepalive responses [DALP-832]
7. Add **datapoint.upload_multiple** function to digidevice python module for uploading multiple datapoints to DigiRM at once [DALP-857]
8. Add **uptime** field to **show cloud** CLI output to indicate how long the device has been connected to Digi Remote Manager [DAL-1083]
9. Update **system support-report** CLI command to automatically store the support report in /var/log/ unless a path is specified [DAL-5027]
10. **system support-report** CLI command outputs helpful information for SCP-ing the file from the device to a remote destination [DAL-5027]
11. New **clear dhcp-lease** CLI command for removing all dynamic DHCP leases or certain DHCP leases based on MAC address or IP address [DAL-5127]
12. New **speedtest** CLI command for performing on-demand iPerf or nuttcp speedtests [DAL-5040]
13. Require local users to be assigned to a group [DAL-5060]
14. Add support for configuring multiple destination networks/interfaces for Multicast routes [DALP-853]
15. New **Network → Advanced → Sequential DHCP address allocation** configuration setting for controlling if DHCP addresses are assigned sequentially or randomly (disabled by default) [DAL-5136]
16. Persistent local date/time across reboots once a successful NTP sync occurs [DALP-806]
17. New ***System → Scheduled tasks → System maintenance → Maintnance window trigger*** configuration settings for controlling when/if a device tells Digi Remote Manager it is in a maintenance window and if updates should be pushed to the device [DAL-5010]
    Available maintenance window triggers are:
    1. Specified network interface is up
    2. Python API call
    3. Specific time window in the day
18. *IX20W:* Remove the requirement to set a Wi-Fi SSID and passphrase to initially configure the device [DAL-5101]
19. Read/write control to the /opt/ and /etc/config/analyzer/ directories through DigiRM and

the local web UI [DAL-5117]

20. New options for setting up a custom default config file [DAL-4978]
    1. ***system backup*** CLI commands for generating a custom default config file based on the active config settings on the device
    2. ***System → File System*** page in the web UI for loading a configuration backup file as the custom default config
    3. ***Files → Persistent files*** folder accessible through Digi Remote Manager where users can upload a config backup, naming it custom-default-config.bin
21. Add option to clear a custom default config by performing a double erase sequence [DAL-5017]
22. Updated CLI login helptext to include common tool-tips [DAL-5157]
23. Replace the cellular modem manufacturer name with the CORE modem model name in the CLI/webUI/metrics details [DAL-5171]
24. Ensure scheduled reboots with the **reboot_managed** command cause graceful shutdown of services on the device before rebooting [DAL-5150]
25. *IX14:* Add hashes for recognizing Telit LE910 xx8 firmware for firmware updates [DAL-5086]
26. *IX15*: Update XBee profiles to firmware version X00D [DAL-5155]

BUG FIXES

The below bugs are all present on firmware versions 21.5.56.176 and older unless otherwise specified

1. Fixed issue where Digi Remote Manager would remediate a DAL device every time it's scanned due to the local user passwords being hashed [DALP-834]
2. Fixed issue where the **system restore** CLI command could default the device if the config backup file was store in the /etc/config/ directory [DAL-5116]
3. Fixed the local web API to allow values with spaces [DAL-5039]
4. Fixed the local web API to allow array configuration settings [DAL-4895]
5. Fixed mdns service where it would occasionally crash [DAL-4663]
6. Fixed issue preventing **modem pin status** from returning valid results [DAL-5056]
7. Fixed bug with installing certain python modules using pip [DAL-5068]
8. Set default user-base directory to /etc/config/scripts/ so python pip can install module dependencies to a writeable location when pip install --user <module_name> is invoked [DAL-5068]
9. Prevent serial connection crashes when a incoming serial socket connection is sending so much data that the buffer fills up the system memory

SECURITY FIXES

1. Add STS header in HTTPS web UI [DAL-4991]
2. Update libcurl to version 7.77.0 (CVE-2021-22897, CVE-2021-22898, CVE-2021-22901)
3. Update to Linux kernel version 5.12

VERSION 21.5.56.176

This is a **recommended** release

Firmware	sha512sum	md5sum
IX10-21.5.56.176.bin	478bc6507e074c98f88194e53f015da154f5d4029f24c ccba5cefae856daf16e30a0d43aae5711c75f288f44c7	c5af97051dd6191ea87d11791ffa5271

	3e2298dc4885c5ad5958ecbafb4e2a9f4ae602	

ENHANCEMENTS

1. Add support for the Quectel EC25-AU cellular modem (DAL-5085)
2. Prevent race condition where DAL could try initiating a cellular connection before the modem is configured and fully setup (max wait time of 5 minutes for the modem to be configured before attempting to connect)
3. Added new **IKE fragmentation** and **Maximum IKE fragment size** config options under **VPN → IPsec** to control whether large packets are fragmented through IPsec tunnels and the size of packets that should be fragmented [DAL-4933]
    1. default **IKE fragmentation**: always
    2. default **Maximum IKE fragment size***:* 1280 bytes

VERSION 21.5.56.106 (May 31, 2021)

This is a **mandatory** release

Firmware	sha512sum	md5sum
IX10-21.5.56.106.bin	ec6989222c10826f1b8248dd7d17e573fabcdb435bc03bca0e3111c8debd38f62431835e2c1dd348b9eb8f62d78e3b27879954c73ce28375f2b45dee7e7fd216	461c270cba2f0393dd2283e610d7d8f2
IX14-21.5.56.106.bin	098c09f80df65dffa9050fab0d38bfb7f08d84b3964e137cc93a358551f7217d31bff65908ad9d6c724354f4634acd2a0aaf662af6e643bd63aae3ffeefac9b4	976fe84d343cb7c4120a0d44f11297ed
IX15-21.5.56.106.bin	972d7a1bc7bbfb80040aed46c12f97626566872e4d379218509ac7aac8fc2de62fc50843ec87dc214792cbc3b5f375c90c5d8a8c244b6a49b0b35366a6c949ce	f038938d9a556142fca3c923055ebe31
IX20-21.5.56.106.bin	dc240873c338e5fb7df1df47e00664be7d896965808765958b67da9f16239f86fc13e2d9e8d79f61e1c4650121822006591986ef48afd9cfb6113987e27c1e76	4487a01d3a5430f448daf61a68129471
IX20-PR-21.5.56.106.bin	f2b98641e5d62a461f3e4c2dd7e3db63f1aa04a972fd4414ee9af893d693f3b5dd803e1095b9d2fcbb210d9ca2664ac317a165e33a89f1c12d7288713b00c76f	5c13536b93607cbb6b0d2ad4799ab8cb
IX20W-21.5.56.106.bin	6f25269f1e35dbf61e536b33c9a6982196e83ca28ef4cd2652946e261899c6d7a6ba4351fb07eac1d0a240b86a4888d0fbc61e67fe45f5905451e1cc76ab7e91	34fc88207b8187623044ad8b8650a9dc
IX20W-PR-21.5.56.106.bin	4c70cbf4ccc7c2e9e98868a4bb85402c725a4fd88f35f001ab74ef450c2983f42545d66d53672fdaa00e1d6ad86bee661e61030059a2693784ceed69d4af8406	a487820df1e6f09714ad49e54dcfaef1

FEATURES

1. Added options under **VPN → IPsec → tunnels → Remote** endpoint to add multiple endpoints and either round-robin between the endpoint or randomly select an endpoint to establish the tunnel to [DALP-160]
2. Added options under **VPN → IPsec → Advanced** to control IKE retransmit interval, IKE timeout, tunnel retry interval, and tunnel retry timeout [DALP-564]
3. New Surelink configuration options [DALP-787, DALP-274, & DALP-84]
    1. **Restart fail count** and **Reboot fail count** options to specify how many times the Surelink test must run and fail before a reboot/restart action is taken
    2. **Pass threshold** option to specify the number of times Surelink tests must pass before the interface is marked as working
    3. New **Test another interface's status** test type to pass/fail Surelink based on whether

another network interface is up/down and has IP connectivity

4. SNMPv2c read-only support [DALP-809]
5. Enable SCEP client support for IPsec tunnel authentication [DALP-722]
6. Add **Scan** button on the Modem status page to initiate a network scan, list available carriers the SIM can connect on, and allow the user to select a particular PLMN/network to use [DAL-4338]
7. Add default **digi.device** local domain for simpler SSH/web access [DAL-4598]
    1. Requires using the Digi device as your DNS server for resolving digi.device to an IP address
8. New **UDP serial** mode that can be applied to one or more serial ports for setting up outbound serial-over-UDP connections [DALP-696]
9. New **Autoconnect** options for streaming outbound serial traffic when in remote access mode
10. Support for WPA3 Wi-Fi encryption [DALP-701]
    1. WPA2/WPA3 Personal
    2. WPA3 Enhanced Open
    3. WPA3 Personal
11. Support for WPA and WPA/WPA2 mixed modes with TKIP support [DALP-827]

ENHANCEMENTS

1. Add **System → Scheduled tasks → Reboot window** config option to add a random delay to the **Reboot time** if configured [DAL-4741]
2. Add read-only console access via Digi Remote Manager [DALP-336]
3. Add support for receiving additional remote commands from Digi Remote Manager:
    1. Perform a speed test and send the results to DigiRM [DALP-490]
    2. Perform automated cellular modem firmware update [DAL-4850]
4. Add option to retain the unique default password of the admin user when initially configuring the device [DALP-758]
5. Improved **Firewall → Port forwarding** options to support a range of ports, including 1:1 and many-to-one port mappings [DALP-560]
6. Added options to control packet filtering for the **Network → Analyzer** traffic analyzer [DALP-733]
7. Update voice settings on Telit and Quectel modems for continued connectivity after AT&T's 3G network sunset in February 2022 [DALP-760]
8. Add internet.gma.iot T-Mobile APN to fallback list [DAL-4906]
9. Support for Sierra cellular modem firmware with multiple CWE files in a single tarball [DAL-4860]
10. Include error messages along with error code if an issue is encountered when downloading device or cellular modem firmware [DAL-4854]
11. Added **Authentication → LDAP → Login attribute** configuration option to control the attribute ID used so it can match with the attribute set in an Active Directory server [DALP-120]
12. Update the titles of the columns in the **show dhcp-lease** CLI output to be more descriptive
13. Add **show dns** CLI command to display the active DNS servers and what interface they're associated to [DAL-3639]
14. Add **show ntp** CLI command to display the status of the NTP service and if it has synced with an external time server [DAL-4747]
15. Add **system firmware ota** commands to check, list, and update to new firmware from the

Digi firmware server [DAL-4800]

16. Skip Auto-APN detection and use internet.telekom APN by default for Deutche-Telekom SIMs [DAL-4622]
17. Add LWM2M parameters to include AT&T Host IDs for devices with EM9191/LM940/LM960 modems [DAL-4823, DAL-4844, & DAL-4845]
18. Update from Quagga to FRRouting for BGP OSPF, RIPNG, and other routing services [DAL-4798]
19. Update python to version 3.6.13 [DAL-3190]
20. Return proper status code for custom scripts configured on the device [DAL-4670]
21. Rename MAC address filtering options to be called **Allowlist** and **Denylist** [DAL-4677]

BUG FIXES

The below bugs are all present on firmware versions 21.2.39.67 and older unless otherwise specified

1. Fixed issue when authenticating users if multiple TACACS servers were configured and the first server is unresponsive [DAL-4748]
2. Clear PDP cid 1 APN for Verizon SIMs using a vzwentp private APN with a ME910c1-WW modem [DAL-4525]
3. Fixed issue preventing devices with LM940 modems from automatically connecting with T-Mobile Hungary SIMs [DAL-4679]
4. Fixed issue where outbound SMS messages couldn't be sent using various carrier SIM cards (bug present on firmware versions 21.2.39.67 through 19.11.x) [DAL-4794]
5. Fixed issue where cellular connectivity wouldn't re-establish if a Quectel modem reset itself [DAL-4612]
6. Fixed issue where the device could stop participating in RIP routing if network interfaces are reset [DAL-4704]
7. Fixed issue where RIP, BGP, and other routing services would not setup properly if a user updated the configuration for the routing services on the device [DAL-4784]
8. Fixed issue preventing acceptance of default routes advertised via RIP [DAL-4799]
9. Fix issue preventing GRE interfaces from being specified within BGP and other routing services [DAL-4695]
10. Fixed issue preventing VPN tunnels from being specified within port forwarding rules [DAL-4524]
11. Fixed issue preventing configuration options from being applied en-masse from the CLI when using the output from the **show config cli_format** command [DAL-4713]
12. Fixed bug where a running network analyzer could be stopped in the CLI by issuing **Ctrl-C** [DAL-4652]
13. Fixed issue where GPS-based location health metrics weren't being sent to Digi Remote Manager (Bug present on firmware versions 21.2.x) [DAL-4310]
14. Fixed issue where the status of an OpenVPN client wasn't listed properly in the web UI [DAL-4357]
15. Fixed issue preventing access to multiple remote networks through an IPsec tunnel with the same policy [DAL-4816]
16. Fixed issue preventing multi-VRRP setups from setting up with the proper priority [DAL-4824]
17. Fixed issue where devices could try recovering Sierra modems in the middle of a modem firmware update [DAL-3929]
18. Fixed issue on the **Serial Configuration** page in the web UI where users could inadvertently bring up the Copy dialog window by dragging and dropping any element from the page [DAL-4923]

19. Fixed issue where wired Internet connectivity is interrupted during cellular modem firmware updates [DAL-4647]
20. Removed broken Babel routing service (bug present on firmware versions 21.2.39.67 through 19.11.x) [DAL-4769]
21. Fixed overlapping 5GHz Wi-Fi channel ranges causing AP/client conflicts in connecting in Switzerland and Liechtenstein [DAL-4733]
22. Removed error message caused by inability to access file descriptors on PR products [DAL-4930]
23. Use PDP cid 1 for Telstra SIMs with a Quectel EG25-G modem [DAL-4810]
24. *IX14:* Fixed issue preventing IX14 units from updating their cellular modem to firmware version 20.00.xx7 [DAL-4867]
25. *IX10/IX15*: Fixed issue where RS485 serial connections would spit out junk messages during bootup [DAL-4724]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a Critical CVSS score of ***9.8 Critical***

1. Reduce password complexity to 8-character minimum (PR products still have 10-character minimum) [DAL-4506]
2. Update to OpenSSL 1.1.1k [DAL-4755]
    1. CVE-2021-3450 CVE-2021-3449
3. Update libcurl to version 7.76.0 [DAL-4774]
    1. CVE-2021-22876
       CVE-2021-22890
4. Update netsnmp to version 5.9 [DAL-4669]
    1. CVE-2018-18066
5. Update tcpdump to version 4.99.0 [DAL-4587]
    1. CVE-2018-10103 CVE-2018-10105 CVE-2018-14461 CVE-2018-14462 CVE-2018-14463 CVE-2018-14464 CVE-2018-14465 CVE-2018-14466 CVE-2018-14467 CVE-2018-14468 CVE-2018-14469 CVE-2018-14470 CVE-2018-14879 CVE-2018-14880 CVE-2018-14881 CVE-2018-14882 CVE-2018-16227 CVE-2018-16228 CVE-2018-16229 CVE-2018-16230 CVE-2018-16300 CVE-2018-16451 CVE-2018-16452 CVE-2019-15166 CVE-2020-8037
6. Reduced listening network services to least-privilege access [DAL-4703]
7. Removed weak SSH algorithms and protocols [DALP-817]
    1. ***Removed MAC Algorithms:*** umac-64-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, hmac-sha1
    2. ***Removed Key Exchange Algorithms: diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256***

VERSION 21.2.39.79 (April 1, 2021)

This is a ***Recommended*** release

IX20-21.2.39.67.bin

SHA512:
3dbcfd33a66474d7fdb308d292868f8a044207f687039afb9404ae44d1feb30925075a9935cbb395a868398514343a2e97e0c4fd62ce1eda373152f6c13a86c3

MD5: 5aca7b9224e9d3104eb0f29d29883cf6

IX20-PR-21.2.39.67.bin

SHA512:

176308c72b7a706ca0c036314944a5b88a4e8451b3a5f9fe8230ee61588db265e27bf987
21f5d23af83657a6baa68d7adc5d825498dab291ee2ccafeb5e98c95

MD5: 3993f737da1d405ce36fa7e0370ccd14

IX20W-21.2.39.67.bin

SHA512:

4bfb707b256352b2a44cde67ae2700c1f9f02acc785ab52a521934a5dec2b88f01b6564b
05a7d3ee2be5ff3958273b9dc8eca17407e1efd24c985989f2b275a0

MD5: 1904551bb372c568cba6fc644912b18e

IX20W-PR-21.2.39.67.bin

SHA512:

f721b6ba36cc555b88e9e515dc6a96eae53b32abbe03b86e5d7158b5752078e2953d0cf
67b55316dec12b073e413aa5113245d388ff8b470eebd4da002a32db7

MD5: aa85293fdc99c41c7a8b50926e029c46

BUG FIXES

26. *IX20W:* Fixed issue where Wi-Fi network crashes when under heavy load [DAL-4667]

VERSION 21.2.39.67 (February 27, 2021)

This is a ***mandatory*** release

IX14-21.2.39.67.bin

SHA512:

39234c8644fff88e0ac8503e80e023f92ebe768a5ce9cd7648be38e202fd592e0fd9f35ab4
4fddd3d9321d50c42ad1146ae089875ffe8cccb0e60e23dd863502

MD5: d6ed79ec3b2db14738451c15038fd5aa

IX10-21.2.39.67.bin

SHA512:

72a8ef1e4e892ea431b101063eb040b6cffe37351f7d27556836a33915f0cf8e241b2296ed
2d6cc3d69e2dee05bdba08273d58f81f2333fa36d88bc17a087547

MD5: 8e7d2ca15d40de7d7955fa5d5d7773cc

IX20-21.2.39.67.bin

SHA512:

525dbe3d67ae2db90c3c28bb98acbab9b893be87e7432d3930baad8fe827bed5a92231e
8c7eaa4a9b945b231ddcb9f5972d552dc52aedabdcd1711431e281a1d

MD5: 1b6bc3ac24b0bd009177c77d076efbf8

IX20-PR-21.2.39.67.bin

SHA512:

33b393e3bfd347070b4086267dd29dfe327e2c81ae8a695635433f2fdbb156cd29af3ceb8
6feaf5731b7fc8fb07b58ba010ee1a749c2d165467d5e3b6428fd30

MD5: b8a737e16faee85f34678e2d9de8e330

IX20W-21.2.39.67.bin

SHA512:

ac896a32a704728834385eae13555d07c7901c8f74794c1848e592b1570268df0f9b4149f
13f24bb807742cdfe493323d82ad9386efe33e82d118e403c1a8f1b

MD5: efa574c9e98186bddcbafdb2c7df56f9

IX20W-PR-21.2.39.67.bin

SHA512:

a3feb157fb421d8787d5f8c51a898f3bd88954874d7dd967ed56fd5fae60e25cead4cc4024
eb0384b556635436bbc068e876721f4e44c0845b1deb9021f6307e

MD5: 3c1900f45ed730d15ae13ea5d074481c

FEATURES

1. Add the Location service to all DAL products. DAL devices can utilize several location sources (cellular, GNSS, or user defined) to determine where it's located and report that to Digi Remote Manager or other servers [DAL-724]
2. Add geo-fencing configuration options. This new features is found under **Services → Location → Geofence**. It can be utilized to define one or more circular or polygonal geo-fence areas and then perform a set of actions when the device enters or leaves that area. Current options for actions to perform are either factory erasing the device or running a custom script. [DALP-711]
3. New **modem scan** CLI command for listing available carriers for the current modem and SIM setup.
4. New **Network → Interface → Modem → Network PLMN ID** config setting to lock the SIM card to a particular carrier based on its PLMN ID(note that the **Carrier selection mode** must be set to **Manual** or **Manual/Automatic** in order to lock the SIM to a specific carrier) [DALP-637]
5. Added local API to the web UI for automated configuration of the device [DALP-777]
6. Support remote CLI commands through Digi Remote Manager [DAL-4273]
7. New configuration options under **System → Scheduled tasks → System maintenance** to automatically check for device and modem firmware updates, then notify in the CLI and web UI when updates are available [DAL-4413]

ENHANCEMENTS

1. Added new **DFS Client Support** configuration setting to support 5GHz DFS Wi-Fi channels in client mode [DALP-720]
2. Add 5GHz frequencies to the list of channels that can be scanned for client-mode Wi-Fi background scanning [DAL-2570]
3. Set 2.4GHz default Wi-Fi bandwidth to 20MHz [DALP-772]
4. Update default background scanning settings for Wi-Fi clients to the following:
    1. Scan threshold: -75dB
    2. Short interval: 5s
    3. Long interval: 300s
5. Updated Surelink recovery of Wi-Fi connections to restart the Wi-Fi module if restarting the network connection fails to recover the setup [DAL-4387]
6. Added settings under **Authentication → Serial** to control Certificate Management for TCP and autoconnect serial port setups [DALP-682]
7. Allow hidden/debug config settings to be controlled and preserved by DigiRM [DAL-4445]
8. Asymmetric preshared keys for IPsec tunnels [DALP-707]
9. Don't display Aggressive/Main mode or Xauth selections for IKEv2 IPsec tunnels [DAL-4142]
10. Update name and description of certificate settings for OpenVPN clients and servers [DAL-4435]
11. Add digidevice.led python module to all products [DALP-710]
12. Add options to forward location information to a remote host over TCP [DALP-778]
13. Add new **Forward interval multiplier** configuration option under **Services → Location → Destination servers** to control the number of location update intervals to wait before sending location data to this server [DAL-4056]
14. Report location metrics as datapoints to DigiRM [DAL-4055]
15. Include the connection uptime of IPsec tunnels as datapoint metrics to Digi Remote

Manager [DAL-4062]

16. Report the phone number of the SIM as a health metric datapoint to Digi Remote Manager [DAL-4440]
17. Fixed incorrect format of ICCID and IMEI metrics reported to Digi Remote Manager [DAL-4440]
18. Add iptables TRACE tool for enhanced firewall debugging [DAL-4182]
19. Improved accuracy of the status shown for a modem during a firmware update
20. *IX10/1002-CMG4:* Disable GEA1 on EG25-G modem [DAL-4250]
21. *IX10/1002-CMG4:* Disable voice services on EG25-G modules [DAL-4560]
22. *IX10:* Enable QXDM support on IX10 [DAL-4512]

BUG FIXES

1. *IX14:* Fixed reboot loop issue on IX14 device running default settings on 20.11.x firmware [DAL-4507]
2. Fixed issue with utilizing software flow control on serial ports set in remote-access mode [DAL-3630]
3. Fix issue where a serial port could lock up and prevent access if flow control was enabled [DAL-4585]
4. Fixed issue where non-primary DNS were queried through the wrong interface when **use_dns** configuration option is set to primary [DAL-3156]
5. Report the phone number of the SIM as a health metric datapoint to Digi Remote Manager [DAL-4440]
6. Fixed incorrect format of ICCID and IMEI metrics reported to Digi Remote Manager [DAL-4440]
7. Fixed setup issue between custom firewall rules and IPsec tunnels [DAL-4433]
8. Fixed occasional issue preventing LM940 modems from re-establish their cellular connection after a modem firmware update [DAL-2933]
9. Fixed issue requiring a user to fix syslog configuration setting when updating from 20.5.x or older firmware to 20.8.x/20.11.x firmware [DAL-4426]
10. Fixed rare issue where **show system** CLI command would display incorrect uptime details [DAL-4350]
11. Fix issue with secondary CLI sessions showing stale configuration settings if the config is updated elsewhere [DAL-4446]
12. Updated message displayed in web UI to direct the user to refresh the page after erasing the device back to default settings [DAL-2326]
13. Fixed issue where dynamic DHCP leases were not displayed in the CLI or web UI (bug present on 20.11.x firmware versions) [DAL-4557]
14. Fixed inaccurate status of the Ethernet interface of a device in passthrough mode [DAL-4543]
15. Fixed issue preventing web UI access if two-factor authentication was enabled (bug present on 20.11.x firmware versions) [DAL-4509]
16. Fixed issue where CLI commands sent from DigiRM would crash the DAL device's connection to DigiRM [DAL-4412]
17. Fixed issue preventing WAN/cellular connections from working if the interface was configured with a single **Interface Up** Surelink test [DAL-4629]
18. Fix rare issue where Wi-Fi hotspots would stop responding to DHCP requests if restarted many times [DAL-4298]
19. Fixed output of the **show wifi ap name <ap_name>** and **show wifi client name <client_name>** CLI commands [DAL-1615]

20. Fixed inaccurate status of the Ethernet interface of a device in passthrough mode [DAL-4543]
21. *PR products:* Fixed issue preventing usage of the digidevice.config python module on PR firmware products [DAL-4378]
22. *1003-CM11*: Fixed occasional issue preventing LM940 modems from re-establish their cellular connection after a modem firmware update [DAL-2933]
23. *1003-CM11:* Fixed timing issue after updating firmware on LM940 modems that preventing the modem from reconnecting unless rebooted [DAL-4614]
24. Fixed issue causing aView-initiated speed tests to report the same upload/download speeds [DAL-4420]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a Critical CVSS score of 8.1 High

1. Update hostapd to address CVE-2019-16275 and CVE-2019-13377 [DAL-4232]
2. Update wpa_supplicant to address CVE-2019-16275 [DAL-4233]
3. Update libcurl to version 7.74.0 (CVE-2020-8169, CVE-2020-8177) [DAL-4336]
4. Update to python version 3.6.12 (CVE-2020-14422) [DAL-4364]
5. Update OpenSSL to version 1.1.1i (CVE-2020-1971) [DAL-4326]
6. Update dnsmasq to version 2.83 (CVE-2019-14834, CVE-2020-25681, CVE-2020-25682, CVE-2020-25683, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-25687) [DAL-3950]
7. Update web security settings with the following headers [DAL-4192]
    1. Pragma: no-cache
    2. Content-Security-Policy
    3. X-Content-Type-Options: nosniff
    4. X-XSS-Protection: 1; mode=block
8. Set SAMEORIGIN in X-Frame-Options to uppercase [DAL-4192]
9. Automatically de-activate active user logins/sessions if the password for that user changes
10. Removed support for https CBC ciphers [DAL-4408]
11. Fixed XSS vulnerability on serial page in the local web UI (Bug present on firmware versions 20.11.x and older) [DAL-4646]
12. *PR products*: Removed debug config options from PR firmware for changing https ciphers [DAL-4417]

VERSION 20.11.32.168 (December 23, 2020)

This is a recommended release.

ENHANCEMENTS

1. Use PDP context 1 with Telus carrier SIMs [DAL-4332]

BUG FIXES

1. Fixed bug preventing Ethernet speed/duplex adjustment (affects firmware version 20.11.32.138) [DAL-4414]
2. *IX10-only:* Fixed bug preventing serial port signal mode from being set to RS-485 when in application or modbus modes (affects firmware versions 20.11.32.138 through 20.8.22.32) [DAL-4424]

VERSION 20.11.32.138 (December 2, 2020)

This is a ***mandatory*** release

IX14-20.11.32.138.bin

SHA512:
723d71598e538fa1ad1dc4a54c9d80d6e7a0d2fcf67c9b040e8c181085e55a4f9958ace580b4fb68ebdaa4106ef1f9cba98520f43e54342fd5b13488cbde3e00

MD5: c0ffb2f67e9126ab15bb62cd92de94ab

IX10-20.11.32.138.bin

SHA512:
e4850185fa3714a4e15b78f620f3985bbe3c47564c7907a68a61b1a2814d7756d7c14fa811360ed6279bb7fd55fc47a6ba5a012a0a4c36d7852a312b366d454a

MD5: d1780394cbfdeb398e0dd7cfa8f07707

IX20-20.11.32.138.bin

SHA512:
00ed82ef515d85f624cbc8c5ccf04736f907e61e955655f7aa051c567599b69f7575892dbc214086b017176ce0260931601e3100d7c883bf1f3ff4f0cc9ec140

MD5: dce476fb431f95954776d783c26c2dda

IX20-PR-20.11.32.138.bin

SHA512:
12478faf7c902916ddd0e171efb19ba0b8773eec7ad6b97ba7bf797fefeb91cc3cfa57f078bfd475ac7692b2af22acfd2e63f3cb23e155c53d546d35162fc984

MD5: 2d0aa54d637a6579a9206dbf4b6b9797

IX20W-20.11.32.138.bin

SHA512:
a5f1fd71a11ac6f335124a709873b9315a9b46f01ed26ded488cc0b003e5d6cd0af93906f581494702dd06faf109a224e026246bb107945d9d8ba12bf970f27e

MD5: cdac8fb0a7cbb99649514d06f01680ec

IX20W-PR-20.11.32.138.bin

SHA512:
bc978f56f4cd58d22cfa928db3fa5c3fb3fa37eb9de9e08788b5b9baedfc1b742b1fc2197c4e4d69ee600f70d25460adc96bfc16975f49c4160ab5740d3a944c

MD5: 45e59c1b8e42ab6e233c4f03d0b459dd

FEATURES

1. *IX20/IX20W:* New PR product variants and firmware for FirstNet/ResponseVerify products [DALP-674]
    1. PR stands for Primary Responder and indicates a security hardened, feature-restricted firmware targeted to comply with AT&T FirstNet and Verizon ResponseVerify certifcation security requirements. It is the same DAL firmware under the hood, but with several features removed to comply with FirstNet and ResponseVerify security restrictions. Below is a list of changes for PR products:
        1. ***Services → Telnet*** removed
        2. Removed ***Telnet*** option from Remote access options if a serial port was set in Remote access mode
        3. WPA1 Wi-Fi encryption option (WPA Personal) removed
        4. Default Wi-Fi SSID disabled by default
        5. interactive shell removed
            1. ***Firewall → custom rules*** always has sandbox enabled with limited shell command and filesystem access to only allow iptables interaction

    2. ***System → Scheduled tasks → Custom scripts*** always has sandbox option enabled with limited shell command and filesystem access to allow CLI access and python script execution
    3. No inbound SCP/SFTP support
2. Add **ssh** and **telnet** commands to Admin CLI [DALP-664]
3. Add new **modem firmware** CLI commands for performing local or over-the-air remote firmware updates to the cellular modem(s) in the device [DAL-2811]
4. Add new configuration options under **Network → Devices** for setting the link speed/duplex of the device's Ethernet port(s) [DALP-135]
5. Add options for starting, stopping, and viewing serial port activity logs through the CLI, web UI, or Digi Remote Manager [DALP-458]
6. Support for the Sierra EM9190/9191 5G modems [DALP-686]
7. Support for the Sierra EM7411 LTE CAT7 modem [DALP-608]
8. IPv6 IPsec tunnel support for full IPv6 tunnels, IPv6-over-IPv4, or IPv4-over-IPv6 tunnels [DALP-581]
9. IPsec XFRM interfaces for enhanced control over IPsec tunnels and the network interfaces associated to them. This allows users to select tunnels for multiple networking features, including static routes, policy-based routes, access control lists, and routing priority based on metric. [DAL-490]
10. Inclusion of the Python pip for installing external modules/libraries [DAL-4078]

ENHANCEMENTS

1. Add **Services → Location** options for configuring GPS or GNSS location communication [DALP-724]
2. GPS/GNSS support for the IX10 and 1002-CMG4 modem [DALP-713]
3. Add cellular technology icon to the Dashboard in the web UI [DAL-3673]
4. Add link to product User Guide under the User drop-down menu at the top-right of the web UI [DALP-569]
5. Added help button to **System → File System** page of the web UI [DALP-569]
6. Added new **Status → Modbus Gateway** service page to the web UI to display information about modbus clients and servers connected to the gateway [DALP-671]
7. Added **show modbus-gateway** CLI command to view the status of Modbus gateway service [DALP-671]
8. Updated **show modem** CLI command to display historical information about the modem if it is in the process of updating firmware [DAL-1504]
9. Added new **Services → Ping responder** configuration settings for controlling what interfaces and firewall zones the DAL device responds to ICMP requests on [DAL-1565]
10. Enhance IPSec tunnels to wait for passing Surelink tests (if configured) before initiating outbound tunnels [DAL-3878/DAL-3774]
11. Add m2m.telus.iot Telus APN to fallback list [DAL-3911]
12. Add psmtneorm and edneopate010.dpa AT&T APNs to fallback list [DAL-4041/DAL-4045]
13. Add reseller and tracfone.vzwentp Tracfone APNs to the AT&T and Verizon fallback lists DAL-4098]
14. Add new 890103 and 890141 ICCID prefixes and 31030 PMND ID matchers to AT&T APN fallback list [DAL-3934/DAL-4041]
15. Add service.qcdm.secure option to enable/disable encrypted QXDM access to the cellular modem in the DAL device [DAL-3964]

16. Add missing modem firmware and SIM details to datapoints uploaded to Digi Remote Manager [DAL-4040]
17. Show uptime for connection to Digi Remote Manager on the Dashboard web UIpage in days/hours/minutes/seconds instead of just minutes [DAL-3691]
18. Updated network bridges to use the MAC address of the first device listed in ***Network → Bridges → [bridge_name] → Devices*** as the MAC address for the bridged interface [DAL-3949]
19. Add link in the firmware update window on the **Status → Modem** page to direct users to the configuration options to schedule a modem firmware update [DALP-725]
20. Updated the help text on the login page to provide a more generic image [DAL-3916]
21. Added option when copying serial port settings on the **System → Serial Configuration** page to optionally copy the label of the serial port [DAL-3842]
22. Removed duplicate modem signal information from the **Modem → Status** page [DAL-3680]
23. Added a **DSCP** option to policy-based routes to allows users to match the routing rule by the type of DSCP field in the packet [DAL-3867]
24. Added a **defaultroute** option for matching policy-based routes to the device's active default route [DAL-4130]
25. Hide the **Monitoring → Device Health** configuration options if the device is not enabled for Digi Remote Manager central mangement [DAL-3825]
26. Update header types for the cellular modem name and network type on the Dashboard page
27. Create system log when Surelink DNS tests are skipped because the interface doesn't have any DNS servers [DAL-4224]
28. Hide main/aggressive mode option when using IKEv2 [DAL-4142]
29. Add reboot watchdog to IX20/IX20W devices to prevent soft-reboot hangs [DAL-3392]

BUG FIXES

1. Fixed missing default settings in configuration profiles created in Digi Remote Manager (bug affects firmware versions 20.8.x and older) [DALP-658]
2. Fixed missing option for setting the **SIM Slot Preference** in configuration profiles in Digi Remote Manager (bug affects firmware versions 20.8.x and older) [DAL-3912]
3. Fixed format of user passwords when displayed in Digi Remote Manager (bug affects firmware versions 20.8.x and 20.5.338.58) [DAL-3889]
4. Fixed issue with policy-based routing not working in conjunction with multiple IPsec tunnels (bug affects firmware versions 20.8.x and older) [DAL-3515]
5. Fixed issue preventing OpenVPN server-managed certificates from being re-generated if the process was interrupted (bug affects firmware versions 20.8.x and older) [DAL-3803]
6. Fixed issue preventing OpenVPN client from using an autogenerated config file from a tap-bridge openvpn server (bug affects firmware versions 20.8.x and older) [DAL-3881]
7. Fixed some formatting output of the **show system verbose** CLI command (bug affects firmware versions 20.8.x and older) [DAL-3805]
8. Fixed issue preventing VRRP interoperability between DAL devices and SarOS devices (bug affects firmware versions 20.8.x and older) [DAL-4130]
9. Update VRRP+ to properly handle changes in network interface statuses bug affects firmware versions 20.8.x and older) [DAL-4274]
10. Removed poorly formatted script contents from the **show scripts** CLI command output [DAL-3315]
11. Fixed non-working **system disable-cryptography** CLI command [DAL-4169]
12. Fixed second-stage erase functionality on devices not enabled for aView management [DAL-

3944]

13. Fixed issue preventing multicast traffic from being sent through a GRE tunnel [DAL-3879]
14. Fixed issue preventing a firewall rule from being setup for OSFPv2 entries [DAL-3869]
15. Fixed rare crash caused when a Quectel modem disconnected [DAL-3867]
16. Fixed behavior of the WWAN Service LED to blink when a modem firmware update is in progress (bug affects firmware versions 20.8.x and older) [DAL-3963]
17. Fixed issue preventing IX10 devices and 1002-CMG4 modems from connecting with Verizon private APNs (bug affects firmware versions 20.8.x and older) [DAL-3605/DAL-3276]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a Critical CVSS score of **9.1**

1. Disallow TCP forwarding from incoming SSH connections [DAL-3938]
2. Remove sensitive information from HTTP GET requests (CVSS score: 5.7 Medium CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:N) [DAL-3938]
3. Update to linux kernel 5.8 (CVSS score: 3.7 Low CVE-2020-16166 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N) [DALP-678]
4. OpenSSH updated to version 8.3p1 (CVSS score: 2.2 Low CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N) [DAL-3299]
5. OpenSSL updated to vesion 1.1.1h (CVSS score: n/a) [DAL-4037]
6. OpenVPN updated to version 2.4.9 (CVSS score 9.1 Critical CVE-2018-7544 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H) [DAL-3862]
7. Linux shell/bash updated to version 5.0 (CVSS score: n/a) [DAL-3763]
8. jQuery updated to version 3.5.1 (CVSS Score: 6.1 Medium CVE-2020-11022 CVE-2020-11023) [DAL-3547]
9. Updated WebU session token to use AES-256-GCM cipher (CVSS score: n/a) [DAL-4000]
10. Prevent web asset access from unauthorized logins (CVSS score: 5.3 Medium CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) [DAL-3835]
11. Add script CSP headers to the web UI (CVSS score: n/a) [DAL-3629]
12. Removed QR code generator from the ***Authentication → Users → Two-factor authentication***, as Content-Security-Policy requirements prevent access to resources not served by the device's web UI [DAL-3629]
13. Added extra layer of firmware verification to ensure the firmware matches the target hardware variant and prevent firmware modifications (CVSS score 1.9 Medium CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:N) [DAL-3511]
14. Prevent command injection through modemadvanced, modem_install, and firmware webpages (CVSS score: 6.8 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N) [DAL-4093/DAL-4104/DAL-4046]
15. Prevent manual addition of files to an encrypted filesytem outside of the device itself (CVSS score: 6.1 Medium CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H) [DAL-4149]
16. Restrict memory allocation of tcpdump (CVSS score: 7.5 High CVE-2020-8037 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) [DAL-4226]
17. Removed expired aView and AVWOB certificates [DAL-3467]
18. Encode MAC address in URL used to sync with aView to prevent privileged escalation [DAL-4304]

VERSION 20.8.22.32 (August 28,2020)

This is the initial production firmware release for the IX10 product. This is a ***mandatory*** release

IX14-20.8.22.32.bin

SHA512:
deea32a3fd22257be2e08596162a83778966cfec751725ae533ec90bf0cf43466e6cd21ba649ab4812fa6ffbcfb29400a71f3cca14dc27c478d9da69221fd1c5

MD5: 1c64b417f36e6425576f999506da9d79

IX10-20.8.22.32.bin

SHA512:
1b681cc342211b3ae2ee849ea3230670ab48a52b667b626520f40b6e33f316c320f2d9916ee5c63c371492a0ea632f979fc397f638ea111bafd243c4063f86b7

MD5: 3749095e4ef0e0d862a64cf1f01ba121

IX20-20.8.22.32.bin

SHA512:
8f7772b60cf18abdd8325dc6fa8e4e4cc7a0f1d4eb201070fc14e6855fc1f05170ba40cb45a83167170467d9e348e64f059184c25c82487005ea5691b8658cee

MD5: 55d7da428951313542aaf9a76e3eb410

IX20W-20.8.22.32.bin

SHA512:
c505383dd71a250f3692ea54ccc10e2e4b718670fb58afbf4f8448f30cbd25620eb451d6e8123d7d0cad1e56a1f67f97c7bd997fa215053901c105884fa00ca9

MD5: afc9527ff7a3f03a617fbf8c6a1079ee

FEATURES

1. Add new **System → Scheduled taks → Allow scheduled scripts to handle SMS** configuration option to allow custom python scripts to handle sending/receiving SMS messages [DALP-488]
2. Add digidevice.sms python module for sending/receiving SMS messages in a custom python script [DALP-488]
3. Add ability to load custom factory config file from the local filesystem, which if present is loaded when the device is reset to default settings [DALP-394]
    1. The config file is the same as what can be downloaded when a user saves/exports the configuration from the **Configuration Maintenance** page in the local web UI. That .bin config file can be placed in /opt/custom-default-config.bin
4. DMNR Verizon Private Network support with new settings under **VPN → NEMO** [DALP-457]
5. Added Serial Modbus Gateway service for utilizing the Modbus protocol to communicate with serial ports [DALP-573]
    1. Configuration settings for the Modbus Gateway are found under ***Services → Modbus Gateway***
6. MQTT client support via Paho Python module [DALP-590]
7. Added 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 [DALP-589]
    1. Configuration options found under ***Network → Interfaces → Ethernet bonding***. Bond devices created here can then be assigned to network interfaces
    2. Note: not available on the IX14
8. VRRP+ options added under ***Network → VRRP → VRRP+*** for validating primary or backup connectivity and automatically changing VRRP priority [DALP-289]
    1. Note a SureLink test must also be enabled for the network interface the VRRP entry is assigned to
    2. Cisco Umbrella content filtering options added under ***Firewall → Web filtering*** service

configuration section [DALP-524]

ENHANCEMENTS

1. Disable voice services on Quectel EC25-AF when using T-Mobile SIMs [DAL-3707]
2. Add **-I** source address option to the ping CLI command [DAL-3682]
3. Add **service.modbus.debug** config option to enable debug logging on Serial Modbus [DAL-3561]
4. Add **Central management** configuration options for any DAL product to sync with aView, ARMT, or AVWOB [DALP-626]
5. Add **4GM** and **4GT** options to the **Network->Modems→Access technology** settings to specify a CAT-M modem to only connect on LTE CAT-M1 or NB-IoT, respectively [DALP-472]
6. Add options under **System → Log → Server list** to allow users to specify the TCP/UDP protocol and port of the remote syslog server [DALP-593]
7. Added configuration option under **Serial → TCP connection** to specify encrypted vs non-encrypted connection types
8. Added configuration option under **Serial → TCP/Telnet/SSH connections** to enable/disable TCP keep-alive messages and nodelay
9. Added new **Base settings** checkbox on custom serial configuration page in the web UI to allow users to specify whether they want to copy the base serial settings or not [DAL-3775]
10. Added new **Monitoring→Device Health→Data point tuning** configuration options to fine tune what datapoints are uploaded as health metrics to Digi Remote Manager
11. Added new **Monitoring→Device Health → Only report changed values to Digi Remote Manager** option to control sending metrics to Digi Remote Manager on the basis of whether the values have changed since they were last reported [DAL-3386]
12. Reduced data usage by 80% (based on default settings) for reporting health metrics to Digi Remote Manager [DAL-3394]
13. Fade **Configuration saved** pop-up window 5 seconds after clicking the **Apply** button [DAL-3451]
14. Added new **Status → Scripts** page in the web UI to view custom scripts and applications configured in the device, along with their status (running vs idle) [DALP-533]
15. Add options in CLI to show and manually stop any custom scripts or applications [DALP-533]
16. Added **Duplicate firmware** option on the Firmware Update page in the local web UI to copy the active firmware to the secondary firmware partition [DALP-565]
17. Add **system duplicate-firmware** CLI command to copy active firmware to the secondary firmware partition [DALP-565]
18. Move **update firmware** CLI command to be under **system** [DAL-3092]
19. Add **show vrrp** CLI command to display the status of any configured VRRP instances [DAL-2953]
20. Use a random unprivileged port for performing ntp time syncs if standard port 123 fails [DAL-3650]
21. Added new **Authoritative** option under TACACS+, RADIUS, and LDAP user authentication methods to prevent falling back to additional authentication methods if enabled [DAL-3314 & DALP-540]
22. Added new options under **Network → Wi-Fi** to control Tx Power of the Wi-Fi module (default 100%) and allow multiple RADIUS servers for WPA2 Enterprise [DALP-85]
23. Include up/down status of hotspots in the **show hotspot** CLI output [DAL-2184]
24. Update to ModemManager 2020-05-19 [DAL-3254]
    1. libqmi: updated to 1.25.4+

2. ibmbim: updated to 1.20.4+
3. libgudev: updated to version 233
4. Improved support for Quectel EC25/EG25 modules

BUG FIXES

1. Fix LED behavior to account for Surelink pass/fail results [DAL-3688]
2. Fixed issue preventing RADIUS/TACACS+ authentication from working unless local-user authentication was also configured [DAL-3701]
3. Fixed issue preventing 1002-CMG4 modem from connecting with Verizon private APN SIMs [DAL-3276]
4. Fixed issue where device would remain connected to Digi Remote Manager even after cloud.service was changed to aView or disabled. Rebooting the device previously resolved the issue [DAL-3504]
5. Fixed bug where IPsec tunnels with multiple policies would only properly route traffic for the last policy configured [DAL-3448]
6. Fixed missing CPU usage stats in **show system** CLI output [DAL-2540]
7. Fixed improper value of the active SIM slot in the **modem sim-slot show** CLI command output when SIM slot 2 was in use [DAL-3569]
8. Fixed issue preventing network interfaces from initializing if the interface name was longer than 7 characters [DAL-2327]
9. Fixed issue preventing WAN passthrough mode if WAN was configured with a static IP [DAL-3097]
10. Fixed errors displayed in CLI when configuring a USB serial port in remote access mode [DAL-3207]
11. Fixed issue preventing users from configuring an IP address as a remote syslog server [DAL-3433]
12. Handle incorrect value occasionally returned by by Telit LM940/LM960 module when querying to see which SIM slot is in use [DAL-3481]
13. Fixed issue preventing cellular modem connectivity if a custom gateway/subnet was configured but the modem wasn't in passthrough mode [DAL-3585]
14. Fixed issue causing aView IPsec tunnel (if enabled) to randomly fail when device was in passthrough mode [DAL-3657]
15. Fixed permission issue on /opt/custom/ directory preventing users from setting up custom CSS and logos [DAL-3710]
16. Fixed issue preventing VLANs from being assigned to Wi-Fi SSIDs [DAL-3113]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a High CVSS score of **6.7**

1. Update to Linux kernel 5.7 (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) [DAL-3322]
2. Added local user login rate limiting to default lockout additional login attempts for 15 minutes after 5 login failures per user (Score: 6.7 Medium CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N) [DAL-3390 and DAL-3505]
    1. New configuration options are under the **Login failure lockout** section for each user in the **Authentication → User** settings
3. Prevent /etc/config/start from running when shell is disabled (Score: 5.2 Medium CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:L) [DAL-2846]
4. Prevent file path expansion on **Firmware Update** and **File System** pages in the local web UI (Score: 3.2 Low CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N) [DAL-3513, DAL- 3471, &

DAL-3518]

5. Prevent cross-site scripting on the Wi-Fi and Bluetooth scanner pages in the local web UI (Score: 3.8 Low CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L) [DAL-3628]
6. Obfuscate text when showing the SIM PIN (Score: 3.2 Low CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N) [DAL-3462]
7. Set HTTP Auth Cookie as secure in the local web UI (Score: 3.1 Low CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N) [DAL-3393]
8. Fixed leaked file descriptors on serial connections [DAL-3202]

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 Digi Remote Manager 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 Digi Remote Manager [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 Digi Remote Manager 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]

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 Digi Remote Manager 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 Digi Remote Manager [DAL-1932]
8. Fixed bug where persistent system logs could not be remotely accessed through Digi Remote Manager [DAL-2060]
9. Fixed bug where Digi Remote Manager 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 Digi Remote Manager 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. Remote cloud connections were locked until while long running commands completed [DAL-1177]
2. 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]
3. Corrections to CLI show route [DAL-1176]
4. CLI ***show system*** output included outdated current time and uptime [DAL-1172]
5. Errors on console during WebUI firmware update [DAL-1140]
6. Faster fetching of signal attributes for LE910_NA_V2 modem
7. Fixed bug with parsing out MCC/MNC from AT#RFSTS response (LE910NAv2)
8. Fixed cloud connector crash on shutdown
9. Fixed process management issue with cloud connector and configuration
10. Check for configured serial ports in ***show serial*** command

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