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
Digi Accelerated/Enterprise Routers
Version 22.5.50.63

INTRODUCTION

This is a patch firmware release for Digi EX50 devices. For all other Digi Enterprise products, use firmware version 22.5.50.62

SUPPORTED PRODUCTS

- Digi EX50
- Digi EX12/EX12-PR (use firmware version 22.5.50.62)
- Digi EX15/EX15W (use firmware version 22.5.50.62)
- Digi EX15-PR/EX15W-PR (use firmware version 22.5.50.62)
- **NOTE:** 22.2.9.85 is the final major firmware release for the 63xx-series products. Patch releases for critical software bugs or security vulnerabilities will be provided as needed until 3/31/2024. The end-of-life announcement for the 63xx-series products occurred on 2022-03-31 (see PCN #220331-01)

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]

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 for automated device updates. For more information, follow the instructions for Digi Remote manager in the link below:

1. **Instructions for Digi Remote Manager:**
   https://www.digi.com/resources/documentation/digidocs/90001436-13/default.htm#tasks/t_update_device_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 22.5.50.63 (July 12, 2022)

This is a ***recommended*** release

Firmware	sha512sum	md5sum
EX50-22.5.50.62.bin	d8a1d4bfe660b7eb705ac589940157df60903cc97052 1816f3aae82ceb14fa08a016a734ed6ae0d059df59d4 e81bd1954c4b461fec7ff205c8f56ad9574bba01	035d1ce819be09af1bee5d53b64aceb9

BUG FIXES

The below bugs are all present on firmware versions 22.5.50.62 and older unless otherwise specified

1. Fixed issue preventing connectivity with some Verizon SIMs [DAL-6384]

VERSION 22.5.50.62 (June 14, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
EX50-22.5.50.62.bin	c61fc171d3bd86adc91f8dc5af2c9723a9f3f3d463887e412147440d448b3e2fc741c586b291e4e0ccec41f8ca89a41dcd6d8ffc71080afcd22a31a5b24ac7d0	3dfecfcc114faf39a80dc06124aeb09a
EX15-22.5.50.62.bin	39dd81b222676736cd5991fcd2cd9e714d8b6401687e26a2b2ef1af26c8ccce6448aadb04d8dbe3b75fa77cb7168eb00c66dca38dd8fbc023bc949f66a8a88e6	d9b98e79530b26d8b502119eca78e792
EX15-PR-22.5.50.62.bin	31a9b861e52054cd302f685c283644f38dfa5c5c73b917f1c1ab120e125fa550f4ab09b4b2c51d26d7924c453f90720a0831befc8f736b48986c1d5cfc3aee8d	af718e7787d8afb9225f76ca1820c49b
EX15W-22.5.50.62.bin	fc4fc77983c5a163c2a00151f4fe8c8edc2d91184e675a22fe7b98b8ec9e8756b5297c38767452c428331b164a08d28e53d800cdd43b0f7b7b9c5c28f26c4b87	dc65dac79c98a9d16196a6b73fc7ccff
EX12-22.5.50.62.bin	a6af5be1a42d874363ae8e064bf0592103b39c38d0a24b8c06c758784a26618faea107b4b8bcfe219d63c0825010fe78f13a0238f0cecc3f9939f47885106831	1694474173bf8528ec244ebbcddbdc16
EX12-PR-22.5.50.62.bin	1507663e3c2a2c68e8050d5c931fac4f075a52274b2a17a9a1bcb8df8a3f218d202b1449286702c9895130b5aae35a6909bf02b8b96514830de53880689b27a0	b974bdc9405009c77aa6e4c854c6d2fc

FEATURES

1. *EX50/EX15/EX12: C*ontainerized python environment is now available. To enable python support on your EX15/EX50 device running 21.11.60.63 or newer firmware, you must update to 22.5.50.62 firmware and install a Python container live image. See the linked knowledgebase article here
2. 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]
3. 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]
4. New *show scep* Admin CLI command for showing the sync status, expiration dates, and additional details of any configured SCEP clients [DAL-6069]
5. Support for enabling add-on features from Digi Remote Manager [DALP-673]
6. *EX15/EX15W/EX50:* 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]
7. *EX50:* New 5G slice support under ***Network → Modems → Default slice information*** for configuring the slice type to set in the 5G modem [DAL-5973]

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. Add support for the CP210X serial driver for connecting to Cisco USB console ports [DAL-6119]
7. Filter out non-Internet type APNs from our APN fallback list [DAL-6227]
8. Automatically power cycle the cellular modem in the event that a *modem reset* Surelink action fails [DAL-6268]
9. Enable Surelink *reset_modem* action by default on cellular interfaces and set fail count to 3 [DAL-6275]
10. Add cellular APN and cellular connection duration as datapoints sent to DigiRM [DAL-5902]
11. Ensure modem is in enabled state before attempting to connect [DAL-6163]
12. Omit non-production modem firmware from the OTA query results in the ***Status → Modems*** page of the web UI [DAL-6301]
13. *EX50:* Improved EX50 cellular throughput by integrating NSS acceleration drivers [DAL-5692]

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]

SECURITY FIXES

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

1. *EX50:* Update to OpenSSL 3.0.3 to enable FIPS 140-2 support [DALP-738]
2. Update to OpenSSL 1.1.1o (CVE-2022-0778, CVE-2022-1292) [DAL-6035]
3. Update to linux kernel 5.17 [DAL-6081]
4. Patch for "dirty pipe" vulnerability in Linux kernel (CVE-2022-0847) [DAL-5981]
5. 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]
6. 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
EX50-22.2.9.85.bin	fd4fe82f644b4ff0fba0e0d205d98d656fe018813baf3a2b3498e6e0c62e554d635712d30ac45420e318ed5021de4068ccba861b350eb8866bd891707cf2242b	083974e026d14146ff99829b8aaae22a
EX15-22.2.9.85.bin	25c1986ff5c60ed91b4d2fc826a569a7de6e8b24745cd8403dcba9ee8a0a83c8b2eadb1e3e7a3d25808f367b3810ff004279e37a449281976d91a64f6ca8f504	4068a2c3a180a7949cbf7e2b6c375ac4
EX15-PR-22.2.9.85.bin	78c83b8fc5c809e4c28acce2e4d50561f3a01a5c21b5137eb4a3f8eaa812799e5eecb8d33d2eaf430611d5ee6a5179b879360986407cbd48f9bc79a6329b75ce	a5c1c0b5118471a0f993e3b2f2c44c3a
EX15W-22.2.9.85.bin	4f85327a4ae6d058f86c70186a3493e8211bfa9e7f23da8d35af566c93402511b8e868d6bb7429545f89c46cde8c364a26af03966b3f9989e16df825cbaa306d	e711481b0e6283aaaac6663a7ea23b7c
EX12-22.2.9.85.bin	c1c164e8b0fa33f5b9a01f6a7149426384b23155d6a02d5602b1229989bdda2f98162738c27e715bc2a9f292051cd0feb078f6d4f3dbb42bf5ad3e0f1cc34e9b	eb4f1e2fce0158556a01d203f5b5a844
EX12-PR-22.2.9.85.bin	0cf685860b107f333db758daba6c64f69728ad7d402dc9b820540be4c9e2e3547c82596d56ea3261aa1b99608e9b7052fc00340746861d9239cf304eb1c873cf	6d0b831432c6ee589f9cb3538f97143e
6300-CX-22.2.9.85.bin	e1954708760622d7021b044d3d755dcb47c6f59f78153ac944dc0762e6265430c8f96955039f42d91aa2d16cf21c009fbdf2ea41c78482a2fc24a12f4908c0f9	b09a56706fc45c40dc6042683da95f5c
6310-DX-22.2.9.85.bin	a170c7b50cff2d07cc2183b7f9ecd6a3b6958333b99e9280ed1b195215d9ebd47bc23b2a9e524489b21ab70791e19c2d6c8037bff3868f596dbaeef841e9cacd	a5de4d49d661cd46d7d5a26e26ad1c36
6330-MX-22.2.9.85.bin	5e220ab73b278c2baabf3849fea505ae61d9dbe9f804287d48816b0a6b0b2c483ea36d88226f00bff4a07c7a7ad049cfadbbe35556cfbda4af369179bbb7e458	fe596f8a682bc247292cf56721d8d788
6335-MX-22.2.9.85.bin	6262e531c6fb33d873a54b3e5837c7d35dd28899ad63da58cfcfe2b012dd4a3288540638c351c4b496bfa172ee15247f311d84e4f7a32f85376f77745fa23f98	40d4ceca8e0acc4f9ef022c6447fadaa
6350-SR-22.2.9.85.bin	39a49f783fe4ad70f7dd1ab17d1866889de8044f4faf2893ea92ffbd9197183101e56cb66925ef4c44f1266227	f8d71eb9e4a5778e8300b8f3e44a1573

	29e4b0b1535090e37c0195e1f0aa2cb333fc5d	
6355-SR-22.2.9.85.bin	adf0d5af361119877ccfe929a43eb11fbe4a16eedf13c6784c96b648705986bda34be4a89034b373b1ba8d55dc29cd585c983f933e862fe86b7bcdda39a19e1f	1226d0aaffbd442c11ffae5a40d2d75a

FEATURES

1. 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. *EX12-PR:* Add container support to PR products and remove from 63xx-series legacy Accelerated products [DAL-5498]
3. Increased web UI upload limit to 512MB [DAL-5694]
4. 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]
5. 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
6. 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]
7. 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]
8. 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]
9. *EX12/1002-CM06/1003-CM07:* Utilize T-Mobile carrier firmware if available for the cellular modem when using Sprint Curiosity SIMs [DAL-5466]
10. New cat Admin CLI command for displaying file contents [DAL-5853]
11. Update /etc/config/scep_client/ directory to be read/write by admin users
12. 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. *EX15:* Fixed link connectivity issues with 10Mbps Ethernet switches [DAL-5506]
15. *EX15:* Fixed intermittent link-dead messages when using an EX15 connected to a VeloCloud appliance [DAL-5657]
16. *EX50:* Fixed intermittent Wi-Fi LEDs when switching between Ethernet and cellular WAN connections [DAL-5660]

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

VERSION 21.11.60.63 (December 8, 2021)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
EX50-21.11.60.63.bin	53d0e73712a1f15c314011dee2fd7046516dd740eca147b9682b60926184a961c77df8df5e6d50c426b428f498c91cefc3719c7477c41e3eb969d6b8029a595a	292eaaf333af39920b8d9d6956f2386b
EX15-21.11.60.63.bin	2d84eaf652df1e6103bbe41225dcb7075d7c2f981615c18dd5b610751ff71c2a4ff7006a3f14721c253604113bf0d542b805a45e7ec90d669cca8b6237fe39b7	ef4059bc4615e7e8b2e3e944a2085bf0
EX15-PR-21.11.60.63.bin	4aa918d2b04396335233a3d52fb3e26e348c7f1f81f42ff50412a1389b09d0ebb36bb77b3ecf7af89c6532704aeb54ded5570a86f4ea3d432678de6701ef9506	f89df749b885b64ecc2ffeafd384819d
EX15W-21.11.60.63.bin	6103925bf9462917327e3c21645ceb71696e8337a552e574f47656e4028d0d0c756388fd4f36e9b3316ae92aca9f9d79344d445094ef020147fd1315dd9b09fc	dcb25bc09de8a7b40afebd94135f25c4
EX12-21.11.60.63.bin	8da05ae8d90d28f138371a5210c3a54f4635da0c7bb515a89b3993debac6a65e8c4095c5e5d3850d2af2d7404a5cf7870a43dfd2fb16a9a7824017d93426c589	d2a49b59b1eeeb9f5d921f8cdf8df7ed
EX12-PR-21.11.60.63.bin	f93f47cda19390794cf196ea9e0b94b68a1afce1fcf167521afa34af5cfc0d067e8cf254faba99074ed5ec755be824626b4e7ca3f3e621289793eb7c2e505dbe	342bfff345bc34e2ea0ddf282ea9abde
5400-RM-21.11.60.63.bin	fd6ce4439dc9be27e38bb5efff4cfa412378125af530b6a83f20bc59d69d0ab999ae523d342c606a8075784bfea3294771a95cd488cec9f3f08e56487e80b940	8e2b9edc3a6f723e6a589a2236c987d6
6300-CX-21.11.60.63.bin	524cca9f584b2916c4a86cdaa7b53d4cd8c9222e0b30e2ebe9f9421420c51af32508278a6d5615b30fa6f34f956471af7eb9dd45a2e3f1d741c5295c6d37da07	32a71a33283d90f8094a43826906fff1
6310-DX-21.11.60.63.bin	99cfea6e5564723f52f1cfecb1f59a49e9a3ac09b452136d2c4508db89e4f54cd2f4cf0892900f0e56218cdfa4474b382aa8748e8d9ec23fce11fa4b39f8c271	1cd76d7646cfbdd3c44786b5095bd13a
6330-MX-21.11.60.63.bin	891312e196b485e1ec933354a2434a39daeed6abdc9471bbc667a6357987daa40d198254c2e6e6b66fe8b79505ad3171e4d204105cd9a85698a3a3539d8a021e	200dcd7b024b1a0efdc80a585b0cd5d7
6335-MX-21.11.60.63.bin	8c807c2b334f8cfe38b44ab0506aa991797591426e60781ba29af208f3cad1f3bafa0dfc06a30feb34228db736ddac58022af4afd27269d131eb2ce68b6fde08	658cadda43a3a44bb5f84bf175546e87

6350-SR-21.11.60.63.bin	2ce178bcd59f631da7c6de3db3695e98ea1717a65f60990eff8f4f9fa8a8eb182eac75ce57f48d1ea3acf205885c4fb9a6f213044850fcd51806c502eb6c31b1	7edd85be585a44231df309f3888aa010
6355-SR-21.11.60.63.bin	d83938fa43c6cf5f2482b33d7fb13ed16c0082c9b678ca48d014119d8eff0f985d021f8dd97054cdeb3ff31ef4158b8c6b815d8a36f0e5a3f1248cde0bcf59b3	d24ad33e747367097c8c4a6ced8abbcd

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 21.8.24.139 and older unless otherwise specified

1. Fixed issue preventing IPsec tunnels from being setup in Transport mode [DAL-5490]
2. *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. *6350-SR/6355-SR:* Fixed issue preventing TACACS authentication [DAL-5411]
16. *EX15/EX15W/EX50:* Removal of python (including FirstNet PR variants) to accommodate firmware size restrictions within the device [DAL-5217]
    1. To enable python support on your EX15/EX50 device, a Python container must be installed. Contact your Digi sales representative for information.

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 21.8.24.139 (October 7, 2021)

This is a ***recommended*** release

Firmware	sha512sum	md5sum
EX15-21.8.24.139.bin	1779ca3f43492c80a0395734a4386ab1c3a69e0b116e2e7fbe03a3b5007c8937cda6a3df2a5541470715a8801cfbd3091fb4ee3319614ae046290caac3f83a5b	e480e350caad5a4a10244a11fe160039
EX15-PR-21.8.24.139.bin	52de2d7a603827e1380de827fa6d94cee25eeeae38bd9e3c6bb618a82230a25807c1f81a71f440bb53885e620cc9f58b6785ce8ca4bd144be625a9835629d042	ec305b13a91987831ff24cca17a50d1d
EX15W-21.8.24.139.bin	4d62bf7b6ffdd5efdc7f249e00ec397d6e8f88d56b04154f9adc3c4627986246de6098a27aefa7df3c70c4569bccd4ffa8dfb460c65c5da87c7746a112ca3cc4	4d08c703fc7c45853729da126f17d3c6
EX15W-PR-21.8.24.139.bin	a42fdd06472672515ba8bac0cd9428b47415efc5c768c3eb0583e1dac861150bd6f1b8619478e3cd007a8ea118dd21e4284de90737480c2850ba33e660673303	5f5bf8f7c7586d6f1796dfcf894da1e2
6310-DX-21.8.24.139.bin	92347ee09c37f1bab4813a3756024587c050d4f2f22fbde50615daaf09ad11e905fef172c9dc569a776875b83cf263b0ffa0aed79f2601c87e354ca00d9b413b	3aadbff455984b62077d35d9528572d0
6330-MX-21.8.24.139.bin	1d38c081045ad808f1991e639ef5d8d063bd595fdd2f728310e5387d0e739bd0910f18d7d38176e59c739cdd28582286e7357c49c23f6ecf7d38983bfab50aba	213ef4e601e8effe3a988257e974a8a8
6335-MX-21.8.24.139.bin	0a0f25cdd2e35d25f7ff84418f29f22a6542b539559f8b9f8a4e8b93e6ca2d728758f114406d27a633d64d8239570a87e8d245340f60d20a4c9d80a1f4a03d64	428f3fdd82631f8d2f8667d57240e5f1
6350-SR-21.8.24.139.bin	41cf2dd528b7f4e5fe011e162a2bd36f2c7e3505d555c10214510f326ac71a63c6bf208e48285804fb83876e108e1fdff238f22eb73d7ce731ecf0f761c9234c	b4f637204ffa98b2c645c17aa7c21e17
6355-SR-21.8.24.139.bin	82c36e465c617924982e54b5a6eb922d2342a5b891e46e92b0d533a57c2b94538b5e1621fb50484f53299ee6ad25a831037b581dfbe9ecd9231b77b1eb3aefd0	e43eee9e25c69f0aa3349bffe0cbfbac

BUG FIXES

1. Fixed issue where device would not re-establish its cellular connection after updating to 21.8.24.129 firmware [DAL-5346]
2. Prevent automated health metrics uploads and manually initiated/generated health metrics from interfering with each other

VERSION 21.8.24.129 (September 13, 2021)

This is a ***recommended*** release

Firmware	sha512sum	md5sum
EX15-21.8.24.129.bin	a08c8e7f6f6831483d430c7cc52778e0571e0f497b382f4315c2978b701cb8b57b205c756437058a7c9e2e9385b71ef229155a8862e780527394cd4301be340b	805942af7cf38f37dd7bff27df5aeaa3
EX15-PR-21.8.24.129.bin	2d0e1e34a79e2434fd1a5e9d8b917067e64a92f39cb0e869c9b09e90e3611dffc7b0933812516d44ed090c676a77c376f8de9eca6522b79f82a41549fa5e89b5	15ec4ed16eceb610536a3af93bdbb33a
EX15W-21.8.24.129.bin	aebc4969ebee5a7fd94bf8fbca27a7052771163e019e9a5b0b76b448ec7bb0da7d6c0d5d4393f45ed502c4a1b115e8fc7123d966ab266ee0d604e22d9e0f6c21	667963b40d2f62335fcfb7cbc43b7edb

EX15W-PR-21.8.24.129.bin	192622b105db250dfc5c4bd99a58ace277861f0df6039937ab1ba16678d2d4fc993d385208792befde1450573d19f9f9b0bb2c7cb1ab27630b069bc6a11aabf0	881164a73c4e6708d4ba1d17bd3077dc
5400-RM-21.8.24.129.bin	babf7b89190d5ad8c3b4903d3edfe3ab872ea71b0ad02900fa6172fce1a4af72487ddf0e5d818fb82f6e5bb744be1d8d0920868eb09b6c229187355128d4b147	023299ab540a32ed54c988f0c43abad4
EX12-21.8.24.129.bin	f8fada739adb49c5a6e289f1af4d92ec42e30fa32c930e3f9240529d7f4271f2897ee9d2091fb19aed30f128e17219ba7b0e4b5aa81e5848e4968110ec9b0f2d	6dddae0fecd389ab9542a4c0ac998ebd
EX12-PR-21.8.24.129.bin	02af6daee1390d5fc690836df41510e499634a6f5e6478db9fe0696ebc34157ba802b6136242e8ff806efd5b1bb10b64ef56b26832003f47afb8b2cc6724903d	6650ff1e17acd9d9045b0c751caea420
6300-CX-21.8.24.129.bin	cb7f632ea3ed42b45d87971a63c86a0d1204410fcdc09904ab448733f400f602781ac989b8933cfd41cfd824b13540ddfab17522a4845f2a95c93744816881b3	fda77d3f345ab01f44e57c796a5cfe33
6310-DX-21.8.24.129.bin	3a76bf7aee1b3bd006738b2fa74b9773b335739397c0665f8a176d81a7cfa3c23c9faac4bdad9fd18ceab608e66547243c6c43e4bffb325c35b1d4d4a3d2e043	298a7305ce3336fccaa39f176f72e884
6330-MX-21.8.24.129.bin	227a3aee7a36ff61c4cc24e74ee3d620ed9e0d7093da0e0d6171e1ce325e36c6f8f5eba20ef9b0518bda0ad1c468a2726ae0697ba077ae5fd0332b960fc716ca	5977492ad98fbb97b9b8c0e33875360d
6335-MX-21.8.24.129.bin	fc4dca4232b663b487647355107a1ad0f0a9e90d32861c67edbb5b9fe4b9f8b3c2b6f5750406f63ee1f23fc1301e7be7ba93c051ef65788a7f48860ed7fa57f3	754b6dccb122bbd9965a7801b8d80f1d
6350-SR-21.8.24.129.bin	4453d6ae44fad43dea8a616129660c9af9c3650a152ce876d8e3bd0483381e2894c8a48c89e97c1f754b6aa2774b261e0c1ca75799482c79ddddd9b23496c565	de2a887d429dd984608258f64191b0d3
6355-SR-21.8.24.129.bin	cb12b1b94a0b2e7673487eb5135fdcdc03802958e3ad82362388208acd63bb2fa266df3fbf478425c4b93e9e82d6447ebb098a1545b3f0dab16b67e4561b6508	3abd13d15a9132c95030032c7a18c3ce

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. *EX15/EX15W/6310-DX:* Enable passthrough mode on both cellular and wired WAN connections by default [DAL-5107]
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. *EX15W/6330-MX/6350-SR:* 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]

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 **mandatory** release

Firmware	sha512sum	md5sum
5400-RM-21.5.56.176.bin	45151bf2ae2c377f6946c6c441feaee087d6c8e55c3d485bae803a22ecaadeba328d1edbebf290d3b4f6640eb330818f1382303bcd80ef54612661666c58e2cd	39032d354685bae9219968cda0fd2f5e
EX12-21.5.56.176.bin	02a8e146b95bc4d6f858ee6cde7eeb34f93237680ffade5783d8da8c9aae731ba854b7f2adb8e1aaea3767b83ab1faab06e8c254e1ef003eb7a1357f1217f8a9	da79434ba9c68edd079cecdf468d6bbe
EX12-PR-21.5.56.176.bin	330fc8520159418384326ab9792b1159e19909d087b7e8d8cfef09630c5df1053172bf980d56c3d188a6900c11de5590ffd173a9e7e4fe397b60519f9f38ad0a	826d44b01f79cd3baadf5f88768da34b

ENHANCEMENTS

1. 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)
2. 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
EX15-21.5.56.106.bin	1e8cdd2c5660d0925cae88da6412c61a1469d00109929efa72c68a42555f9f9bad5749c2a5570236ff5fc14501e637e7f98f3af81030fcaa522cacedb38a4986	5e8f4745983b3e29a92076a1795c1ccc
EX15-PR-21.5.56.106.bin	d81dccd56b425f9696b98985a0e849129271bc20c91fb2c5f4410a3f0e5acc8c543996a33ad15eb9d7bed2b42814429374f82acf0359fdcbffcbfac6d202eaa4	86337bceff211ea31aeec4aab113bbf2
EX15W-21.5.56.106.bin	7ed1ee587c110170b1ea394780c9600914164f67c5db77509480c848c743cd91f933ad89978d174b3f7893c91ad832bf7ddf14b90792c0fd03d5e2ea4055c4e3	b8c6feb1c2e86b43db12c1b30bc60386
EX15W-PR-21.5.56.106.bin	7bfc627f8a78c75138ead26fc5cce287a9f18239207c5abf679d9b91de4d3b1b05a6ced2f27481400b7372c741a2f35862446d146be73b418061dfe40335a977	c27cf3d57876cd176f8686df9d68ddce
6300-CX-21.5.56.106.bin	efc15e3e64555ab7ea931fcb1e30609ca45cfa51ccaf288d084477719cbac09376d97ec4981dff8c3031f3ff2136aa0ae274c0e0bd49b2d40c07827c6407aba0	e7275b80875845dc58694a57b13c77ca
6310-DX-21.5.56.106.bin	97d002e7f99b7578c286f54a2cae3297a62db1004a58b7482d69415c6583c94cfe3d4a3cfbf70cbefe9ea6720602f3ab22de7dac3971211973308e4049d51951	33aa6f94c0fbf7391362453503366732
6330-MX-21.5.56.106.bin	c9842e32294608a8f402e80d2e407b6cfe3eb66188e7eac806de52ecf046bf847d01e43b15c16a0c62fdd920f274bf2b01556b63319419baf447b45f31b1c7c5	ddf0229f64af1a9a558053b05b88bfee
6335-MX-21.5.56.106.bin	8326227e13ccf09daff4d2f987c8ba360621430d4003db5bd0d0df6531810ec3ac9d82b25a627ac4ac5f09f0b1ddd57480d3d3a309993aac456507c5fceb7202	797a304fcb74c2488c018229373da034

6350-SR-21.5.56.106.bin	e5dd59ca54ee0fd43819c18b519ca768576a63ccc015e7622b22fff0647b7db7b20755a966297cdd427e27a86ce4da4ca0db1a8f3cedf1737f1e6dd5dc1299db	a51db34fbe906049dc8ce6d39dfa09df
6355-SR-21.5.56.106.bin	494bf783c21e556c84d4181014d3ff0a648fc23c030b8fc68e62728c392fe4c9a75b91e8b2fe00fbc42a21eb2655b043cecedec98f5672985d8ed5908bb57336	1cb41f4ffe78e04078892e50664fab81

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. Add option to lock a 5G SIM to 5G-SA only or 5G-NSA only [DAL-4785]
19. Add step to power off Sierra EM919x modems before rebooting the device [DAL-4739]
20. Update from Quagga to FRRouting for BGP OSPF, RIPNG, and other routing services [DAL-4798]
21. Update python to version 3.6.13 [DAL-3190]
22. Return proper status code for custom scripts configured on the device [DAL-4670]
23. 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]

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 21.2.39.67 (February 27, 2021)

EX12-21.2.39.67.bin

SHA512:
d1cd96a3a0004874209ad87acef74cd80ae695eda4d614c7ee07e54fa4635980cdd8d13cd28c045e8e9b8a5aac18e509032580c8b7f9a2f64f01f2c54bc65fd3

MD5: 6f422c1c3f1324b5c58c72b23c4d0e8d

EX12-PR-21.2.39.67.bin

SHA512:
e8b6eb1e2ebd4f810e103138fdd8fa9e0a3cb3ee9a613a635984e28fded6a873fa27812114628adfc63f5310e8114ee48de0d3959ededf6c1c3d2962d05653d5

MD5: 212e450aa6eec6e6ef76d4b39553e3e9

EX15-21.2.39.67.bin

SHA512:
ca00f52fd57c901115fb360ec22b2591de9b7eca542b1a14c8385d00423a2f9dadbcc68a0a6d5067a7568d77199a361d68609431ccd5fa2ebdb075587bb16d77

MD5: b4db0fb96d39ca1742c1a24d653b479c

EX15-PR-21.2.39.67.bin

SHA512:
a16fef890859003ef2f5e39b453a3425b84358be6c6427a17af69cd77179097aa5a4a09326c696ec9b238dc511f8e3a66f2b6fae416eb051504b9a8ddf677e86

MD5: 8323ef118600a4e1a9da481095ee6d57

EX15W-21.2.39.67.bin

SHA512:
a252302c2c6208dd243e1088b87e5e69d656586dc67060043303fcd7dbc07d0a9bf4784042d974dd6c4975d115e559b7bf6be593c1587e398e0f8d2a3976d150

MD5: ad4807daf027489f586a5db03391963d

EX15W-PR-21.2.39.67.bin

SHA512:
7a5f2d2009d4667d6275f7d70733d59359a608dae7983cb17073877f9bf0c324c6736faf5e3384248f3f5eec6e6be79bb0ecb19c9f660f69114735f42ccbbaf0

MD5: 956d2134b32efc2522a7796bc732b072

5400-RM-21.2.39.67.bin

SHA512:
5fd6aaa4461cfadf8e99357453cd98eeb37f87e4db5c7b86876f15963e646ef8cf8a3ceaf2083810e074f17a46d47dff83a1bb697914ee7519cd182b432a5dd7

MD5: e7f807e658ad07554295ad5e3ab483e1

5401-RM-21.2.39.67.bin

SHA512:
bdb09db0a6dcd78caa070a2d34201a44e3566d29825b0b504d8a5e5bdf5e7bdbb66c6c1bf56ac8e89c2b983ff537878f7492a88ca9366cafa07eebe39aaf3ed9

MD5: 160aed03d7468a60f7c7b5d6f5934df3

6300-CX-21.2.39.67.bin

SHA512:

2ccbc4023724efc8010389f14d155b723b1d2ccc2eccf8b415bc43a84aac934a8b9cba4941dfd09284a9ada8b8dca4980720005c3a3223c0192adb91d13f3db4

MD5: 4fede0c4124b4db8d90a1c23ef8b82af

6310-DX-21.2.39.67.bin

SHA512:

03065095a051aaa72dfcf18d8ece4f41541c32e281879e6e471e85ec1dcb2eac38efb2986ddd6bb167e2f7e1f4e17cb2d3c57ad511869e7b7f4ef2925a1a4da2

MD5: 0fbf35610bdb32a2507149758759a708

6330-MX-21.2.39.67.bin

SHA512:

e1d74d7ab50edfb2f045fde9e43d0acaaff6acb3486af02bd5f341128f1636e78b403e44d4505a4a96d4811e01ca7614250e8cd4561305184cea1e7eeeb77c29

MD5: 687ff1b262946cbbe7f5ffc3ff2c5bf7

6335-MX-21.2.39.67.bin

SHA512:

cf31b12d714ce03fbe4fa250849d04b17e8fa58d1d4d1484fbb23ff7780beeeea8a14a4feab95a0e6e937f3a03a22035d52bafe4d39f9d045e90d679c3ff9746

MD5: 15ba4d5c01726f8bce39d88808c4aba1

6350-SR-21.2.39.67.bin

SHA512:

b7adadc8e1b63001f746fd6ce355e44960ecb6d03e1c01922b34d648d6466157642e8048cd0142e062a28d148a3c94eae63df80b8e5c1fc36d04294c791c0b15

MD5: ff2fa98f75a606bf21304e8e4f8221cf

6355-SR-21.2.39.67.bin

SHA512:

e38794189d5fff5e910bbd43066c714fef9f2a7773248e484bcbaf3c7f2de503da082363b8d0d57a74c2034012943464c926975c7c81be4d389093e3c70919db

MD5: b0807f0d9e5eb10f8703e4eecc4bd282

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. *EX15W:* Added new **DFS Client Support** configuration setting to support 5GHz DFS Wi-Fi channels in client mode [DALP-720]
2. *EX15W:* 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. *1002-CMG4:* Disable GEA1 on EG25-G modem [DAL-4250]
21. *1002-CMG4:* Disable voice services on EG25-G modules [DAL-4560]

BUG FIXES

24. Fixed issue with utilizing software flow control on serial ports set in remote-access mode [DAL-3630]
25. Fix issue where a serial port could lock up and prevent access if flow control was enabled [DAL-4585]
26. Fixed issue where non-primary DNS were queried through the wrong interface when **use_dns** configuration option is set to primary [DAL-3156]
27. Report the phone number of the SIM as a health metric datapoint to Digi Remote Manager [DAL-4440]
28. Fixed incorrect format of ICCID and IMEI metrics reported to Digi Remote Manager [DAL-4440]

29. Fixed setup issue between custom firewall rules and IPsec tunnels [DAL-4433]
30. Fixed occasional issue preventing LM940 modems from re-establish their cellular connection after a modem firmware update [DAL-2933]
31. 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]
32. Fixed rare issue where **show system** CLI command would display incorrect uptime details [DAL-4350]
33. Fix issue with secondary CLI sessions showing stale configuration settings if the config is updated elsewhere [DAL-4446]
34. Updated message displayed in web UI to direct the user to refresh the page after erasing the device back to default settings [DAL-2326]
35. 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]
36. Fixed inaccurate status of the Ethernet interface of a device in passthrough mode [DAL-4543]
37. Fixed issue preventing web UI access if two-factor authentication was enabled (bug present on 20.11.x firmware versions) [DAL-4509]
38. Fixed issue where CLI commands sent from DigiRM would crash the DAL device's connection to DigiRM [DAL-4412]
39. Fixed issue preventing WAN/cellular connections from working if the interface was configured with a single **Interface Up** Surelink test [DAL-4629]
40. Fix rare issue where Wi-Fi hotspots would stop responding to DHCP requests if restarted many times [DAL-4298]
41. Fixed output of the **show wifi ap name <ap_name>** and **show wifi client name <client_name>** CLI commands [DAL-1615]
42. Fixed inaccurate status of the Ethernet interface of a device in passthrough mode [DAL-4543]
43. *PR products:* Fixed issue preventing usage of the digidevice.config python module on PR firmware products [DAL-4378]
44. *EX12:* Fixed connectivity of EX12 devices with T-Mobile private APN SIMs [DAL-4544]
45. *1003-CM11*: Fixed occasional issue preventing LM940 modems from re-establish their cellular connection after a modem firmware update [DAL-2933]
46. *1003-CM11:* Fixed timing issue after updating firmware on LM940 modems that preventing the modem from reconnecting unless rebooted [DAL-4614]
47. 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

8. Update hostapd to address CVE-2019-16275 and CVE-2019-13377 [DAL-4232]
9. Update wpa_supplicant to address CVE-2019-16275 [DAL-4233]
10. Update libcurl to version 7.74.0 (CVE-2020-8169, CVE-2020-8177) [DAL-4336]
11. Update to python version 3.6.12 (CVE-2020-14422) [DAL-4364]
12. Update OpenSSL to version 1.1.1i (CVE-2020-1971) [DAL-4326]
13. 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]
14. 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
15. Set SAMEORIGIN in X-Frame-Options to uppercase [DAL-4192]
16. Automatically de-activate active user logins/sessions if the password for that user changes
17. Removed support for https CBC ciphers [DAL-4408]
18. Fixed XSS vulnerability on serial page in the local web UI (Bug present on firmware versions 20.11.x and older) [DAL-4646]
19. *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]

VERSION 20.11.32.138 (December 2, 2020)

EX12-20.11.32.138.bin

SHA512:
8ca00542ccca7a8a03cd720405e2d85a1d78660c804bf312f9599bc404830a7b40074abb5d3dad60ba7f2402609a2f22dc5f7e793d7dfaf845f8db18c8c68d17

MD5: 73958d8bb5acc31d4f75b3066f04daad

EX12-PR-20.11.32.138.bin

SHA512:
a2d9f823f8753ffa2cb00c04232f9f314afcddad221b4b76c4d392401d5725a06cd8787231837c0e7c4329da473afbe6ee861f2ebd4da1e5e8d17f8aac7f1eab

MD5: 211d1005b5c812c3c36d3b55ac355dc2

EX15-20.11.32.138.bin

SHA512:
83fd656aed56d972543f4d19e003825593d79dc439846b03a3d7116599cba9e1c06a55c1f5c984a01a5f6820c1fc8f5b7491f1a9ef793a2aed223575dac15ef8

MD5: 8fd4e699bd27cc9da81cb726225021c9

EX15-PR-20.11.32.138.bin

SHA512:
efffe94ed40519d132067cb2c0239d85428b039cea25f88955313913ade9170f9e990714dac13d3fc0d0d22630a01145c878482f435f34fea8acb6528c87bc95

MD5: fb31340e93ad3bde71d0e5a5c90fd1dc

EX15W-20.11.32.138.bin

SHA512:
63ad84ec0ca6798137890486076e46b6f4f39447f5f5fed3eeef4e5485a169ace26c919c51d9f9b2de67cb6ae59768e913270bb526ef0e866fe6889d735deaf7

MD5: 3518774a2339b0babd56c57bd129838d

EX15W-PR-20.11.32.138.bin

SHA512:
9b67783334b0acab900682db7d817d8f9f7cd797601ea5778cc335f36845189a968094b4
29e45a564e33d42614d0030ffe71a57fc66cbe2321b9fb7994a2b849

MD5: 54c8f6fad14ff7bda2b3d119afe31ff1

5400-RM-20.11.32.138.bin

SHA512:
75a6c795d0bca41f73516f5f1287ca8529f446fdd5ca6d2bbf6062be7e60bd4b2fc9a79dd
98b44c39f33f4cdd834644e9e1004a2c656886a9b51e254e24fc3d8

MD5: 8fe0c22df1a24065b9b1ec32e90e2ded

5401-RM-20.11.32.138.bin

SHA512:
826fbdb9d9c7cd8c768debabf4219d5828ef3e07b3c50d78d94a3d32553ec0696c3cfe05
2d61f773e37d66fc09bf710ff2a500fb9bf7f37240fb630259e54434

MD5: 8364adb9346a60462941abae20eebff7

6300-CX-20.11.32.138.bin

SHA512:
2b1e79bb7242c2730b5e29aa54ba9f1b8a2b5bd9a2f5b6176f07f1c338aae8a8270d76e2
3bbea6e0311233cc9eb0d4b406d73192b57a3736bb9e43f66b6b4f32

MD5: eccedc3709db885fac85a9323c6924e1

6310-DX-20.11.32.138.bin

SHA512:
e63f8d4a08967a20a1876d24b828392667dd904fd23053a032408329118dfc248b658a8a
521084258342fea0d8579916a8a97ba4831b5a2d59d0f6a827a8b77f

MD5: 2f9e15eb0ac42fd1ce74b67eedd28f1d

6330-MX-20.11.32.138.bin

SHA512:
9d87a8256f2326d48c5492b31eb0bc11e7e7e02c916db704f532aeb2e6a48359aadaf5ff8
fa49912c4f873e8fdd657d6578b5a0e061b53df5b51a55597b7f9e8

MD5: 953f27a0d01baa3e84a1b356e1e769b0

6335-MX-20.11.32.138.bin

SHA512:
9b5ecf97e76055ddbfcf836839e41276c9e14707a4ea074c965d3f7194b1710efda59e216
835db75715095d6cf7de76deb01bf5e68849b535b4a57673159ad49

MD5: 461913ddf3b1649155a6de015a54dc76

6350-SR-20.11.32.138.bin

SHA512:
5571ae02a4d2bea4f412906ae91a61d453794007fbddd339d58feca739f93e12233342b0
b3e7718d33fc3a82473e9eb516790eba7a85d1255de0a4320ff06f56

MD5: 6583d1f6001bb872de247c1b193b0480

6355-SR-20.11.32.138.bin

SHA512:
1701987867b894df7a4f22163c7bdc51e8210178fe105146e9976dfe4efff6bee21f9b7ebd
38615ad4da05b5dd2f0795d729b4b8ccbbe66ab80e9eea2c171a35

MD5: 1dc366811ebb098422a17ff4d3c8cdb4

FEATURES

1. *EX12/EX15/EX15W:* 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 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]

BUG FIXES

1. *EX12*: Enable Surelink on cellular modem by default (bug affects EX12 devices on firmware versions 20.8.x and older) [DAL-3795]
2. Fixed missing default settings in configuration profiles created in Digi Remote Manager (bug affects firmware versions 20.8.x and older) [DALP-658]
3. 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]
4. 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]
5. 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]

6. 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]
7. 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]
8. Fixed some formatting output of the **show system verbose** CLI command (bug affects firmware versions 20.8.x and older) [DAL-3805]
9. Fixed issue preventing VRRP interoperability between DAL devices and SarOS devices (bug affects firmware versions 20.8.x and older) [DAL-4130]
10. Update VRRP+ to properly handle changes in network interface statuses bug affects firmware versions 20.8.x and older) [DAL-4274]
11. Removed poorly formatted script contents from the **show scripts** CLI command output [DAL-3315]
12. Fixed non-working **system disable-cryptography** CLI command [DAL-4169]
13. Fixed second-stage erase functionality on devices not enabled for aView management [DAL-3944]
14. Fixed issue preventing multicast traffic from being sent through a GRE tunnel [DAL-3879]
15. Fixed issue preventing a firewall rule from being setup for OSFPv2 entries [DAL-3869]
16. Fixed rare crash caused when a Quectel modem disconnected [DAL-3867]
17. 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]
18. Fixed issue preventing 1002-CMG4 modems from connecting with Verizon private APNs (bug affects firmware versions 20.8.x and older) [DAL-3605/DAL-3276]
19. Removed SIM slot 2 references and options from the configuration settings in the 6300_CX [DAL-3930]
20. Disable the internal Qualcomm GPSoneXTRA application on Telit LE910c4-NF modules from downloading data from the Qualcomm commercial XTRA server (bug affects firmware versions 20.8.x and older) [DAL-4009]

SECURITY FIXES

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

1. Secureboot with signed firmware images for the EX15/EX15W (CVSS score 5.7 Medium CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H) [DALP-646]
2. Disallow TCP forwarding from incoming SSH connections [DAL-3938]
3. 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]
4. 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]
5. 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]
6. OpenSSL updated to vesion 1.1.1h (CVSS score: n/a) [DAL-4037]
7. 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]
8. Linux shell/bash updated to version 5.0 (CVSS score: n/a) [DAL-3763]
9. jQuery updated to version 3.5.1 (CVSS Score: 6.1 Medium CVE-2020-11022 CVE-2020-11023) [DAL-3547]
10. Updated WebU session token to use AES-256-GCM cipher (CVSS score: n/a) [DAL-4000]
11. 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]

12. Add script CSP headers to the web UI (CVSS score: n/a) [DAL-3629]
13. 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]
14. 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]
15. 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]
16. 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]
17. 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]
18. Removed expired aView and AVWOB certificates [DAL-3467]
19. Encode MAC address in URL used to sync with aView to prevent privileged escalation [DAL-4304]

VERSION 20.8.22.32 (August 28, 2020)

EX12-20.8.22.32.bin

SHA512:
b5f1371048906d6dc452d3db2e041e645f60d590d800955334bb31bada8843b89728d1fe926dfd3fd10f30b0a9b8ccb24f5e47738b6851afa069d54643a6eb98

MD5: b6bef9cbec0b4fe972db73443342e8ee

EX15-20.8.22.32.bin

SHA512:
9ae10cd5000bb8a01ab42bfd4019b56d3657506305724b4d8889cb665b25783c47587cd09ad4562bc32ecdd9d813449e2216f37e83e9463740988f75e547ecdd

MD5: 1d20c64a6c7cd9f0f5da2bf881a92292

EX15W-20.8.22.32.bin

SHA512:
85162831b4c98c4a9a434b4a9eb57c9e203e33b4982be70f142d921d5db92f0c293b8dcf38af8eeb0d43b5ad3ad7b855aa4016fe1557417d5c85468f4f9ed481

MD5: 604328982da3a12f45e3f025727d1817

5400-RM-20.8.22.32.bin

SHA512:
c72d28ac55f1d9dd22c12c638d56b8d322c856bad9004b4e588184d6885b1f59a45a1bb0ffe1c9e450a25fc2f641a67345118fbd88f679ff7d6083d4ceadbc75

MD5: 16ef2d441b0f350235bb1671e613779e

5401-RM-20.8.22.32.bin

SHA512:
3bcdb3e979504bd3a9ef11e938d90f3815996eb7de296fb04f46d835682b02fb81100372de205a4a7cd0cbc6d6f6ee88d48927e989cea023e013682023c173ed

MD5: d7a62d4d5c254a77e088fa81c1e333dd

6310-DX-20.8.22.32.bin

SHA512:
23fef21ee2f1f36f199a19084eea11d56122b5aedb66ee44e557e893e7f6f9a2a477176ae0e24d80c202609d7614ad022164acf98db35a31c06f72929ecfd2b5

MD5: cd9d262772f73b4a2533f6a217e80457

6330-MX-20.8.22.32.bin

SHA512:
f1d539c3d0dac46fd3af34a0c46f71341b2ab81d968a48d78bc22f09697cb645676d02d9d0eaeaf96bf26400188e86d46201b00a0d1e6652cf909c6b06f52d85

MD5: 680d983cb67dfdaf95d472112d0d74f6

6335-MX-20.8.22.32.bin

SHA512:
eeca51acdf9104b5dd80a49ed57bea6c096e755e4c50f05f909cb714eaa4ce2dd04aa78858d16d79838f0a6dee62950113f1b944b079a1bb8f6d2c102d3101cd

MD5: cdef93effb68deceae0c700e926c9e2a

6350-SR-20.8.22.32.bin

SHA512:
cd451d5fd6704c78d7572466b006ef743698cf6525b923160e31aa7df95c3722fbc83c67f04406be5bb61baa778143a31a3d8b322387f212e9024530879cc110

MD5: 06cd7ad939156dc778629c5c208ff3f3

6355-SR-20.8.22.32.bin

SHA512:
89b6bca6237bcc1b31edcedce25e10cf88d51a0c75c09908fe81811ad68fc175a1d3c29f8c413e7bbcc618cec9684be7297789f39733ac91755e5f912ea17e0d

MD5: 70ea993770c9ab679d432637845c69a3

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]
    1. Note: not available on the 6300-CX, 5400-RM, or 5401-RM
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 6300-CX, 5400-RM, or 5401-RM
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

9. 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. Fixed T-Mobile IPv4 connectivity on EX12 [DAL-3489]
2. Fix LED behavior to account for Surelink pass/fail results [DAL-3688]
3. Fixed issue preventing RADIUS/TACACS+ authentication from working unless local-user authentication was also configured [DAL-3701]
4. Fixed issue preventing 1002-CMG4 modem from connecting with Verizon private APN SIMs [DAL-3276]
5. 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]
6. Fixed bug where IPsec tunnels with multiple policies would only properly route traffic for the last policy configured [DAL-3448]
7. Fixed missing CPU usage stats in **show system** CLI output [DAL-2540]
8. 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]
9. Fixed issue preventing network interfaces from initializing if the interface name was longer than 7 characters [DAL-2327]
10. Fixed issue preventing WAN passthrough mode if WAN was configured with a static IP [DAL-3097]
11. Fixed errors displayed in CLI when configuring a USB serial port in remote access mode [DAL-3207]
12. Fixed issue preventing users from configuring an IP address as a remote syslog server [DAL-3433]
13. Handle incorrect value occasionally returned by by Telit LM940/LM960 module when querying to see which SIM slot is in use [DAL-3481]
14. Fixed issue preventing cellular modem connectivity if a custom gateway/subnet was configured but the modem wasn't in passthrough mode [DAL-3585]
15. Fixed issue causing aView IPsec tunnel (if enabled) to randomly fail when device was in passthrough mode [DAL-3657]
16. Fixed permission issue on /opt/custom/ directory preventing users from setting up custom CSS and logos [DAL-3710]
17. 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]
3. New configuration options are under the **Login failure lockout** section for each user in the **Authentication → User** settings
4. 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]

5. 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]
6. 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]
7. 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]
8. 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]
9. 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. *EX15W/6350-SR:* 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. Enable drivers for SD card on EX12 [DALP-512]
3. Add a **statusall** option to the **show ipsec** CLI command to display verbose IPsec status [DAL-2711]
4. Use modem PDP context 1 when an AT&T SIM in inserted to match new requirements from AT&T [DAL-3093]
5. Add AT&T FirstNet IMSIs so they can be differentiated from other types of AT&T SIMs [DAL-3163]
6. Added Python HID module to allow the DAL device to control PSUs via Python programs [DAL-2092]
7. Allow network analyzer to be configured to monitor any network interface instead of just wired Ethernet ports [DAL-2146]
8. Added option to **ping** CLI command to ping a broadcast address [DAL-2571]
9. Added new health metric to report the interface used by the DAL device for its configured IPsec tunnels [DAL-2710]
10. Added new health metric to report the LTE SNR value of the modem(s) on the DAL device [DAL-2904]
11. Limit metrics upload to no more than 2 per minute if backlogged [DAL-2870]
12. 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]
13. Report device SKU in RCI response to Digi Remote Manager [DAL-2940]
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. 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]
17. Fixed issue preventing automated and console-based OTA modem firmware updates on Telit LE910c4-NF module (bug affects firmware versions 20.2.x and older) [DAL-3052]
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. *EX15W/6350-SR/6330-MX:* 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 20.2.162.162 (April 17, 2020)

This is a **recommended** release

ENHANCEMENTS

1. Use ***ims*** instead of ***vzwims*** APN on Verizon SIMs for proper IMS registration [DAL-2883]

BUG FIXES

1. *EX12:* Fixed potential SIM switch failure on Telit LE910c4-NF modem caused by issuing an improper AT command when generating a support report [DAL-2883]
2. *EX12/1002-CM04/1003-CM11:* Fixed cellular high-speed throughput performance issues caused by CPU slowdown and timing of gathering cellular signal details [DAL-2802]
3. *EX12/1003-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]

VERSION 20.2.162.157 (April 13, 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]

BUG FIXES

1. Fix health metrics warnings in Digi Remote Manager stating the local filesystem's /opt/ directory was full when it wasn't [DAL-2769]
2. Fixed missing Rx/Tx bytes in ***show modem*** CLI command output [DAL-2804]
3. Fixed issue preventing multicast packets from being sent through a network bridge [DAL-2774]
4. Fixed auto-reboot after restoring configuration file through local web UI [DAL-2862]
5. Fixed inability to update modem firmware on Sierra EM7511 modules [DAL-2794]
6. Fixed improper modem firmware selection on Telit LM960 module when using a T-Mobile SIM [DAL-2376]
7. 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]
8. 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 LM960 LTE CAT18 modem support [DALP-487]
2. Quectel EC25-AF LTE CAT4 modem support [DAL-1817]
3. Digi Remote Manager is set as the default portal for all DAL products [DALP-393]
    1. 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.
4. Added SureLink™ default connectivity tests on all WAN interfaces [DALP-402]
    1. 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.
5. Background Wi-Fi AP roaming/scanning [DALP-435]
    1. New **Background scanning** configuration settings under Client WiFi entries
6. New web UI pages added under the ***System*** drop-down with enhanced serial details and configuration [DALP-465]
7. Support for firmware/OTA updates on Quectel modems [DALP-419]
8. 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. *5400-RM only:* Update FIPs products to openssl version 1.0.2u [DAL-2342]
16. Update libcurl to version 7.69.0 (CVE-2019-15601) [DAL-2732]
17. Update pppd to version 2.4.8 (CVE-2020-8597) [DAL-2732]
18. Fix elevated root access through custom scripts when no-shell is enabled [DAL-2628]
19. 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. *EX15/EX15W only:* Fix unstable Gigabit Ethernet connections when device is in passthrough mode [DAL-2642]
19. Fix broken SCP/SFTP file transfers when **idle_timeout** was set to a value other than *nil* [DAL-985]
20. Fix occassional issue where expired DHCP leases were not cleared [DAL-2310]

21. Fixed output of **show modem** CLI command when cellular modem re-initializes
22. Fix potential initialization issues after updating firmware [DAL-2762]

VERSION 19.11.72.85 (January 21, 2019)

This is a **recommended** release.

NEW FEATURES

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

ENHANCEMENTS

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

BUG FIXES

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

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

VERSION 19.11.72.58 (December 6, 2019)

This is a **mandatory** release.

NEW FEATURES

1. Re-themed web UI with improved navigation and functionality. New functionality includes:
    1. The ability to view local filesystem contents [DAL-2110]
    2. Help-text on login page
    3. Quick-config access on status pages
    4. new Dashboard overview page
    5. 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. 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
2. Added the ability to push OpenVPN routes in subnet mode [DAL-2224]
3. Add cellular IMEI and firmware version, along with bluetooth and accelerometer info to show manufacture command in the Admin CLI [DAL-2030]
4. Add the % measurement value to the CPU usage in the show system output of the Admin CLI
5. Device is passthrough mode with an IPv6 connection now honors and utilizes the MTU in IPv6 Ras
6. When using Verizon SIMs, utilize the OMADM process to auto-discover the APN [DAL-1371]
7. Enhance modem firmware update tool to support multiple modem installations [DAL-2148]
8. 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]
9. Removed 192.168.210.254 Default IP gateway [DAL-2095]
10. Added support for sending RFC2136 compatible DNS updates to external DNS servers [DALP-446]
11. 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]
12. Updated the filename of the support report generated through the web UI or CLI to include the Digi name [DAL-1434]

SECURITY FIXES

1. Updated OpenSSL to version 1.1.1d [DALP-304]

BUG FIXES

1. *EX15W only:* Fixed slow performance of Wi-Fi driver (issue present on 19.8.1.61 and older firmware) [DAL-2181]
2. *EX15W only:* Fixed bug where WiFi clients would be disconnected in areas with congested Wi-Fi

channels [DAL-2178]

3. 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]
4. 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]
5. Fixed bug with timing of RCI callbacks from Digi Remote Manager (bug present in firmware versions 19.8.1.61 and older) [DAL-2091]
6. Fixed bug where RX/TX data usage metrics reported to DRM could be mistakenly calculated as a negative sum [DAL-1972]
7. Fixed crash in IPsec configuration with more than 6 for IKE Phase 1 proposals or more than 10 IKE Phase 2 proposals [DAL-2066]
8. Fixed bug in reporting the reboot counter metric to DRM [DAL-1932]
9. Fixed bug where persistent system logs could not be remotely accessed through DRM [DAL-2060]
10. Fixed bug where DRM would always shows the device's connected method as ethernet [DAL-1993]
11. Prevent users from selecting non-production firmware versions when perform modem OTA updates [DAL-1662]
12. 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]
7. *EX15/EX15W only:* Fixed bug where a DAL device in passthrough mode would ignore any custom gateway/netmask settings in its configuration settings (bug present on firmware version 19.8.1.43) [DAL-1454]
8. *EX15/EX15W only:* Fixed bug preventing a modem OTA firmware update from recovering if the update was interrupted, such as from a power loss or reboot (bug present on firmware versions 19.8.1.43 and older) [DAL-2051]

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 strongswan bypass-lan plugin 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. Fixed bug where an apostrophe in a WiFi's WPA pre-shared key would result in the SSID not being broadcasted [DAL-1633]
3. Fix issues where Telit QMI modems would disconnect from USB hub and not recover [DAL-1321/DAL-1556]
4. 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]
5. 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]
6. 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]
7. Fix issue where a DHCP relay endpoint couldn't be setup through modem or IPSec interfaces [DAL-956]
8. Close any open sessions on a serial port when configuration update changes the mode of the serial port
9. Fix bug in `show network` CLI output when both IPv4 and IPv6 networks were available
10. Fix bug where `show network` CLI command would show incorrect output when no SIM was present
11. Fix bug in returning dynamic-only ref_enums in device config to Digi Remote Manager [DAL-1323]
12. Fix service serversocket binding when cc_acl restarts [DAL-1411]
13. Fix reloading of displayed configuration options when enabling/disabling aView central management in the local web UI [DAL-834]
14. Fix reloading of the Dashboard page when enabling/disabling Intelliflow in the local web UI

[DAL-780]

15. Reset LEDs displayed during reboot instead of freezing the LEDs to show the last known device state before the reboot [DAL-886]
16. Fix bug where Digi Remote Manager RCI thread blocks indefinitely waiting for config write lock [DAL-573]
17. Fix bug where `ls` command in the admin CLI required a terminating / on the path [DAL-1251]
18. 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]
19. Fix labeling and format errors in show wifi CLI output
20. Fix multiple SSID traversal with WiFi-as-WAN client setups [DAL-1246]
21. Fix bug with show openvpn name CLI command output [DAL-1191 & DAL-1192]
22. Fix bug with carrier, plmn, and modem status output in show modem CLI command
23. Fix column spacing and lower-casing consistency in show arp CLI output [DAL-1173]
24. Fix parsing of carrier names when posting cellular modem details to Digi Remote Manager [DAL-1553 & DAL-1326]
25. Fix error showing signal strength of WiFi network(s) when the signal was 0% [DAL-1404]
26. Limit decimal numbers reported to Digi Remote Manager to six decimal places [DAL-807]
27. *6310-DX only:* Fixed CPU slowdown due to kernel update (bug present on firmware versions 19.5.88.59 - 19.8.1.30) [DAL-1687]
28. Fixed bug with Sierra MC73xx-series cellular modules in 6300-CX and 1002-CM03 products where the modem would require a power cycle after upgrading the firmware of the modem in order to reconnect [DAL-1716]
29. Fixed issue with Telit LE910-NAv2 cellular modules in 1002-CM04 CORE modems not receiving SMS messages while cellular data session was active/online (bug present on firmware versions 19.8.1.30 and older) [DAL-1634]
30. Add Telus m2m APNs to fallback list [DALP-452]

VERSION 19.5.88.81 (June 26, 2019)

This is a **mandatory** release.

NEW FEATURES

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

SECURITY FIXES

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

BUG FIXES

1. Fixed bug where IPSec tunnel would cause a system crash when the tunnel was established over QMI-based modems [DAL-1170]
2. Fixed aView tunnel issue where the tunnel drops over time and remote commands fail [DAL-776]
3. Fixed bug preventing QMI-based Telit modems (CAT1 and CAT-M1 modules in particular) from

connecting with vzwstatic APNs (bug present on 19.5.88.59 firmware)

4. Fixed bug where the 1003-CM modem (LTE CAT11 Telit LM940) would shut-down and not recover its cellular connection if temperatures were too high
5. Fixed bug where the cellular modem occasionally would not initialize properly on devices with a large number of serial ports

VERSION 19.5.88.59 (May 24, 2019)

This is a **mandatory** release.

NEW FEATURES

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

ENHANCEMENTS

1. Improvements to CLI show serial [DAL-1175]
2. Improved reliability of security chip from userspace access due to wakeup
3. Send interface name with cellular status events [DAL-916]
4. Updated ipset version to 7.1 [DAL-917]
5. Update to newest shadow-4.6 package
6. TACACS+ authorization for more server implementations [DAL-933]
7. stunnel updated to version 5.52 [DAL-915]
8. Additional health metrics required for DRM 3.0 [DAL-810]
9. Add support for Telit ME910C1_WW
10. Direct remote serial port access via WebUI (shellinabox) [DAL-775]
11. Dual-APN Support on Telit LE910-NAv2 (1002-CM04) [DAL-818]
12. Improved OpenVPN operation and customization [DAL-798]
13. Update to linux-5.0 [DAL-842]
14. Add ***description*** field to system group [DAL-581]
15. Upgrade MC7455 to 02.30.01.01 (SWI9X30C 2.0 Release 23) added latest Sierra firmware for MC7455 and MC7430 [DAL-759]
16. Add an additional APN for Bouygues in France [DAL-840]
17. Improved Telit location reporting [DALP-226]
18. Improved collection of network LINK and Speed reporting
19. Implement Digi Remote Manager health metrics [DAL-707]
20. Added latest Telit LE910_XX_V2 firmware md5 sums

SECURITY FIXES

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

BUG FIXES

1. Fix issue on 6300-CX preventing WebUI based firmware update up to 1 in 3 tries [DAL-1194]
2. Remote cloud connections were locked until while long running commands completed [DAL-1177]
3. Fix major issue with multiple IPsec policies When two remote subnets are configured in 2 Policies for an IKEv2 tunnel only Policy 2 traffic will pass [DAL-934]
4. Corrections to CLI show route [DAL-1176]
5. CLI ***show system*** output included outdated current time and uptime [DAL-1172]
6. Errors on console during WebUI firmware update [DAL-1140]
7. Faster fetching of signal attributes for LE910_NA_V2 modem
8. Fixed bug with parsing out MCC/MNC from AT#RFSTS response (LE910NAv2)
9. Fixed cloud connector crash on shutdown
10. Fixed process management issue with cloud connector and configuration
11. Check for configured serial ports in ***show serial*** command
12. Fixed bug where ***show serial*** option is visible for devices with no serial ports [DAL-1114]
13. Web GUI input validation rewording to be consistent
14. DAL-CLI: fix typos in descriptions, titles, and minimums
15. WebUI: Ensure correct versions of static files are loaded (using md5hash)
16. Serial ports were mistakenly listed under ***Network*** for metrics and state
17. Metrics had incorrect title, "System" in descriptors/state.
18. ModemManager: Telit error reporting patch
19. Intelliflow crash fix (divide by 0 on some datasets)
20. Intelliflow improve error reporting
21. System maintenance tasks do not run during duration window if reboot time is set [DAL-960]
22. SPIKE: Asynchronous CLI under DRM [URMA-1996]
23. Firmware update through WebUI doesn’t recover when some other page is clicked during the update process [DAL-869]
24. Signal/dbm/percentage inaccurate on Verizon 2G and 3G connections with MC7354 [DAL-786]
25. Verify and fix dual APN support on the LM940 [DAL-742]

26. Unable to establish dual-APN connection with AT&T using Sierra modem [DAL-813]
27. Telit: Added logic to protect new C1_AP modems from being bricked [DAL-744]
28. Telit: Added firmware check sum for version 414 of LE910-EU1 [DAL-822]
29. Update Telit LE910C1-NS modem firmware from 25.00.244 to 25.00.246 [NPIX-939]
30. Fix MTU support for PPP based connections
31. Added md5 sums for the latest Telit firmware for LE910_NA1

VERSION 19.1.134.81 (Feb 14, 2019)

This is a **mandatory** release.

NEW FEATURES

1. Support for sending device health metrics to DRM
2. PPPoE via WAN Ethernet support
3. Added option to upgrade Telit cellular modules to custom firmware images

   The custom firmware image must be a .tar.gz compressed file include the .bin firmware image itself and a .md5 file containing the md5sum output for the .bin image
4. Support for the Telit LM940 LTE cat11 module, including OTA firmware updates and carrier switching
5. Initial support for the Sierra EM7430 LTE cat6 module
6. Added 2-factor authentication support to all devices (previously only available on 5400-RM and 635x-SR products)

ENHANCEMENTS

2. Added support for upgrading Telit LE910_XX modules to the latest xx5 firmware
3. Update aView defaults to tunnel to ipsec.accns.com endpoint for remote commands
4. Added 18327.mcs and 13631.mcs AT&T APNs
5. Added intra.vzwentp Verizon APN
6. Add Network->Modem options to basic options when central management is enabled
7. Added ability to set custom DHCP options under the IPv4 -> DHCP server -> Advanced settings configuration options for a network interface
8. Updated entries created under the System -> Scheduled tasks -> Custom scripts to be enabled by default. Previously, newly created custom scripts would be disabled by default
9. Updated custom SNMP MIB to include OIDs for all available cellular modem metrics (RSRP, RSRQ, RSSI, MCC, MNC, etc.)
10. Added GRE and IP-tunnel details to the Tunnels tab on the Status page of the local web UI
11. Updated the progress bar shown during modem firmware updates on the System page of the local web UI to change to red if the firmware update fails
12. Added Telit-specific AT commands to mmcli-dump file included in a support report generated from the System page of the local web UI
13. Allow atcmd tool in the Admin CLI to run whether ModemManager is enabled or disabled

SECURITY FIXES

1. Updated ModemManager to version 1.10.0
2. Updated wget to version 1.19.5
3. Updated strongswan from version 5.5.3 to version 5.7.1
4. Updated openssl to version 1.0.2q
5. Updated pcre to version 8.42
6. Updated glib to version 2.57.1
7. Update to Linux kernel 4.19.13

BUG FIXES

1. Fixed bug where firewall setup would crash if multiple modem interfaces were configured in the settings of the device
2. Fixed bug where OTA updates to Telit modules could be interrupted by loss of power, but would not resume after power was restored
3. Fixed bug where 2G location details were not stored or reported properly
4. Fixed bug where location details for Telit modems were not stored or reported properly