# Digi Accelerated Linux (DAL) Release Notes
# Connect IT Console Servers
# Version 21.8.24.129

## INTRODUCTION

This is a major firmware release for all DAL supported products.  This is a recommended production firmware release

## SUPPORTED PRODUCTS

- Connect IT 4
- Connect IT 16
- Connect IT 48
- Connect IT Mini

## KNOWN ISSUES

- Cellular metrics are not shown under the **Settings → Status → Communications** section of Digi Remote Manager, but are shown under the **Data Streams** for the device.  [DALP-768]
- Health metrics are uploaded to Digi Remote Manager unless the **Monitoring > Device Health > Enable** option is de-selected and either the **Central Management > Enable option** is de-selected or the **Central Management > Service** option is set to something other than Digi Remote Manager [DAL-3291]
- The ability to send/receive data through a T-Mobile SIM in a 1003-CM11 (Telit LM940) modem running firmware version 24.01.547 can be delayed up to 15 minutes after initially connecting (downgrade the 1003-CM11 modem to 24.01.544 or older firmware to mitigate)  [DAL-4981]
- IPsec tunnels with names longer than 8 characters will not have their remote networks routed properly  [DAL-5139]

## UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you update production devices.
2. Unless otherwise noted, apply updates in the following order:
   a. Device firmware
   b. Modem firmware
   c. Configuration
   d. Application

Digi recommends Digi Remote Manager or Digi aView for automated device updates. For more information, follow the instructions for Digi Remote manager or Digi aView in the links below:

1. **Instructions for Digi Remote Manager:**
   https://www.digi.com/resources/documentation/digidocs/90001436-13/default.htm#tasks/t_update_device_firmware.htm
2. **Instructions for Digi aView:**
   https://www.digi.com/resources/documentation/digidocs/acl-kb/default.htm#Subsystems/kb-6300-cx/update-firmware.htm

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

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

## TECHNICAL SUPPORT

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

## CHANGE LOG

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

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

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

### VERSION 21.8.24.129 (September 13, 2021)

This is a **recommended** release
ConnectITmini-21.8.24.129.bin
   SHA512:
      4f582ccdc3ce7e025aee4c32e350e8402cc7cfa796703410cf5029bf722e800bf6b88ca9b5
      b9f005524e4cba003561cde9f5ad431a169af20d3343f02f22dfd8
   MD5:      98865a8e8c3939e461881af0ef2be82d
ConnectIT4-21.8.24.129.bin
   SHA512:
      51fc38ed148a77508b0eed170a8a2c8ef8a5b9cf112ef0cf319a28f33e6a580c15ded4720e
      60413d8eca7fbfa97f0fdcfcb475463c113d13a53399c8a52b4daa
   MD5:      7d05cb036823dcebb407683c8bd3ce30

ConnectIT16-21.8.24.129.bin

SHA512:
2d005a9359f80f80a2fa0e8d0d03986759902b46734f4f4bc2db629a71e8c849936cb56ef
19a27cb3245b9e6f01711807794e3c5e35e8c3164a355ab776b1df5

MD5:     3c9ddc1c4fcd125c2b14725d3fe98f22

ConnectIT48-21.8.24.129.bin

SHA512:
44fc24a64825191b02cba1cac9710433a071af93aa1610a19697c69babfe256753c026737
34c83a0a3e21b5c3e6aa5ce0cf70c902843fe66ee8c7f8fc645fdb7

MD5:     1478631931bcee4286732a929438e148


## 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. Added new **show l2tpeth** CLI command for viewing the status of any configured L2TPv3 tunnels  [DAL-5220]
2. Update python pip to version 21.2.4  [DAL-5068]
3. Shortened fallback APN list by removing wildcard entries  [DAL-5012]
4. 3G sunset support for EU carriers  [DAL-5041]
5. Update messaging included in keepalive packets sent to Digi Remote Manager to prevent multi-second delays in keepalive responses  [DALP-832]
6. Add **datapoint.upload_multiple** function to digidevice python module for uploading multiple datapoints to DigiRM at once  [DALP-857]
7. Add **uptime** field to **show cloud** CLI output to indicate how long the device has been connected to Digi Remote Manager  [DAL-1083]
8. Update **system support-report** CLI command to automatically store the support report in /var/log/ unless a path is specified  [DAL-5027]
9. **system support-report** CLI command outputs helpful information for SCP-ing the file from the device to a remote destination  [DAL-5027]
10. 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]
11. New **speedtest** CLI command for performing on-demand iPerf or nuttcp speedtests  [DAL-5040]
12. Require local users to be assigned to a group  [DAL-5060]
13. Add support for configuring multiple destination networks/interfaces for Multicast routes  [DALP-853]
14. New **Network → Advanced → Sequential DHCP address allocation** configuration setting for controlling if DHCP addresses are assigned sequentially or randomly (disabled by default)  [DAL-5136]
15. Persistent local date/time across reboots once a successful NTP sync occurs  [DALP-806]
16. 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
17. Read/write control to the /opt/ and /etc/config/analyzer/ directories through DigiRM and the local web UI  [DAL-5117]
18. 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
19. Add option to clear a custom default config by performing a double erase sequence  [DAL-5017]
20. Updated CLI login helptext to include common tool-tips  [DAL-5157]
21. Replace the cellular modem manufacturer name with the CORE modem model name in the CLI/webUI/metrics details  [DAL-5171]

22. 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 21.5.56.108 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 21.5.56.108 (June 3, 2021)

This is a **mandatory** release

ConnectITmini-21.5.56.108.bin

> SHA512:
> > d36007e1ed293fd0d518836d6ddb490dd0859a5918ff00008696fc168e63cb244ccf3870b 52a66737c19836e7069f90036044e9c4a593bb65c3ab1a35f35de32

> MD5:     119b0311362a503b9a16168ed4743bef

ConnectIT4-21.5.56.108.bin

> SHA512:
> > 5f4561ad0e6e5ed51e82df881e16b1656a4527c8e031030c6ed8d5b27175a1c45af00c0bf 204db51e25796f433f42b5f53f73690b2952065effd3dded52bf3f3

> MD5:     7749f09ece4c6fb46d9353ce286eadf3

ConnectIT16-21.5.56.108.bin

> SHA512:
> > 15c0646ec73a786dd3253ee0ee44e649b8008361059ea42872de697a75f020404e1a4d2 53cb4ffabdde2bcee7e8466ec4aada5f4a98d266384e45ef8760338ee

> MD5:     ecddba3f266c3f6752a3a55a69b418ab

ConnectIT48-21.5.56.108.bin

> SHA512:
> > 567356efd1414bd5ec4913cf6fce29d7d7cbc561013866eef0676f4d8a25944e49850ee68 d5040469c5e90999fc27445cba9045fff4168038e60b89230db457a

> MD5:     fcda1309ebda0da247b23b64b570285a

## 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

## ENHANCEMENTS

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

120]

12. Update the titles of the columns in the **show dhcp-lease** CLI output to be more descriptive

13. Add **show dns** CLI command to display the active DNS servers and what interface they're associated to  [DAL-3639]

14. Add **show ntp** CLI command to display the status of the NTP service and if it has synced with an external time server  [DAL-4747]

15. Add **system firmware ota** commands to check, list, and update to new firmware from the Digi firmware server  [DAL-4800]

16. Skip Auto-APN detection and use internet.telekom APN by default for Deutche-Telekom SIMs  [DAL-4622]

17. Add LWM2M parameters to include AT&T Host IDs for devices with EM9191/LM940/LM960 modems  [DAL-4823, DAL-4844, & DAL-4845]

18. Update from Quagga to FRRouting for BGP OSPF, RIPNG, and other routing services  [DAL-4798]

19. Update python to version 3.6.13  [DAL-3190]

20. Return proper status code for custom scripts configured on the device  [DAL-4670]

21. Rename MAC address filtering options to be called **Allowlist** and **Denylist**  [DAL-4677]

## BUG FIXES

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

1. Fixed issue when authenticating users if multiple TACACS servers were configured and the first server is unresponsive  [DAL-4748]

2. Clear PDP cid 1 APN for Verizon SIMs using a vzwentp private APN with a ME910c1-WW modem  [DAL-4525]

3. Fixed issue preventing devices with LM940 modems from automatically connecting with T-Mobile Hungary SIMs   [DAL-4679]

4. Fixed issue where outbound SMS messages couldn't be sent using various carrier SIM cards (bug present on firmware versions 21.2.39.67 through 19.11.x)   [DAL-4794]

5. Fixed issue where cellular connectivity wouldn't re-establish if a Quectel modem reset itself  [DAL-4612]

6. Fixed issue where the device could stop participating in RIP routing if network interfaces are reset  [DAL-4704]

7. Fixed issue where RIP, BGP, and other routing services would not setup properly if a user updated the configuration for the routing services on the device  [DAL-4784]

8. Fixed issue preventing acceptance of default routes advertised via RIP  [DAL-4799]

9. Fix issue preventing GRE interfaces from being specified within BGP and other routing services  [DAL-4695]

10. Fixed issue preventing VPN tunnels from being specified within port forwarding rules  [DAL-4524]

11. Fixed issue preventing configuration options from being applied en-masse from the CLI when using the output from the **show config cli_format** command  [DAL-4713]

12. Fixed bug where a running network analyzer could be stopped in the CLI by issuing **Ctrl-C** [DAL-4652]

13. Fixed issue where GPS-based location health metrics weren't being sent to Digi Remote Manager  (Bug present on firmware versions 21.2.x)  [DAL-4310]

14. Fixed issue where the status of an OpenVPN client wasn't listed properly in the web UI  [DAL-4357]

15. Fixed issue preventing access to multiple remote networks through an IPsec tunnel with the same policy  [DAL-4816]

16. Fixed issue preventing multi-VRRP setups from setting up with the proper priority  [DAL-4824]
17. Fixed issue where devices could try recovering Sierra modems in the middle of a modem firmware update  [DAL-3929]
18. Fixed issue on the **Serial Configuration** page in the web UI where users could inadvertently bring up the Copy dialog window by dragging and dropping any element from the page [DAL-4923]
19. Fixed issue where wired Internet connectivity is interrupted during cellular modem firmware updates  [DAL-4647]
20. Removed broken Babel routing service (bug present on firmware versions 21.2.39.67 through 19.11.x)  [DAL-4769]

## 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  [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)

This is a **mandatory** release

ConnectITmini-21.2.39.67.bin

    SHA256:

        6a0fda83f27055a1346d74eded4ba012c67de647d3237b77908b1a72ac80cfc9b0144c2c4
2b41868bc654af6e5900126ce0c68bb0781f5d085d1582ebff774f8

    MD5:     37d5b03c24823114e235ac6724cb082c

ConnectIT4-21.2.39.67.bin

    SHA256:

        bb80bb050eb96f164234b5e77b3e1c8a17c002a1e90de92e0c9089ef2cd7ac37cdd08c72
2d455349425ff0c7c53b062ac174be46a90c281e45f64c3b3dca7ac8

    MD5:     ccc31728eb1f685b8af4091b531deebc

ConnectIT16-21.2.39.67.bin

    SHA256:

        6b9a1661d0e718d54a0e7086e0c67abe6a42b6e9efb213680592c19b16f94470092bdf96
8f006d5fda22dd3955f3b0488681498f24135500efcf1d9f7c6b6c61

    MD5:     8cabc90a773ff8489cb7c786cc1716d9

ConnectIT48-21.2.39.67.bin

    SHA256:

        7c891bf64414341c006eaee42de28d312e116739a4ccc5e457627727931034f530c502c5f
28c477c390d339661564d49ff155df9e59fce3783b60f19f6302286

    MD5:     abbe72dda27f97a2d36579b81945a99a

## FEATURES

1. Add the Location service to all DAL products. DAL devices can utilize several location sources (cellular, GNSS, or user defined) to determine where it's located and report that to Digi Remote Manager or other servers [DAL-724]

2. Add geo-fencing configuration options. This new features is found under **Services → Location → Geofence**. It can be utilized to define one or more circular or polygonal geo-fence areas and then perform a set of actions when the device enters or leaves that area. Current options for actions to perform are either factory erasing the device or running a custom script. [DALP-711]

3. New **modem scan** CLI command for listing available carriers for the current modem and SIM setup.

4. New **Network → Interface → Modem → Network PLMN ID** config setting to lock the SIM card to a particular carrier based on its PLMN ID(note that the **Carrier selection mode** must be set to **Manual** or **Manual/Automatic** in order to lock the SIM to a specific carrier) [DALP-637]

5. Added local API to the web UI for automated configuration of the device [DALP-777]

6. Support remote CLI commands through Digi Remote Manager [DAL-4273]

7. New configuration options under **System → Scheduled tasks → System maintenance** to automatically check for device and modem firmware updates, then notify in the CLI and web UI when updates are available [DAL-4413]

## ENHANCEMENTS

1. Added settings under **Authentication → Serial** to control Certificate Management for TCP and autoconnect serial port setups [DALP-682]

2. Allow hidden/debug config settings to be controlled and preserved by DigiRM [DAL-4445]

3. Asymmetric preshared keys for IPsec tunnels [DALP-707]

4. Don't display Aggressive/Main mode or Xauth selections for IKEv2 IPsec tunnels [DAL-4142]

5. Update name and description of certificate settings for OpenVPN clients and servers [DAL-4435]
6. Add digidevice.led python module to all products [DALP-710]
7. Add options to forward location information to a remote host over TCP [DALP-778]
8. 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]
9. Report location metrics as datapoints to DigiRM [DAL-4055]
10. Include the connection uptime of IPsec tunnels as datapoint metrics to Digi Remote Manager [DAL-4062]
11. Add iptables TRACE tool for enhanced firewall debugging [DAL-4182]
12. Improved accuracy of the status shown for a modem during a firmware update

## BUG FIXES

1. Fixed issue with utilizing software flow control on serial ports set in remote-access mode [DAL-3630]
2. Fix issue where a serial port could lock up and prevent access if flow control was enabled [DAL-4585]
3. Fixed issue where non-primary DNS were queried through the wrong interface when **use_dns** configuration option is set to primary [DAL-3156]
4. Report the phone number of the SIM as a health metric datapoint to Digi Remote Manager [DAL-4440]
5. Fixed incorrect format of ICCID and IMEI metrics reported to Digi Remote Manager [DAL-4440]
6. Fixed setup issue between custom firewall rules and IPsec tunnels [DAL-4433]
7. Fixed occasional issue preventing LM940 modems from re-establish their cellular connection after a modem firmware update [DAL-2933]
8. 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]
9. Fixed rare issue where **show system** CLI command would display incorrect uptime details [DAL-4350]
10. Fix issue with secondary CLI sessions showing stale configuration settings if the config is updated elsewhere [DAL-4446]
11. Updated message displayed in web UI to direct the user to refresh the page after erasing the device back to default settings [DAL-2326]
12. 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]
13. Fixed inaccurate status of the Ethernet interface of a device in passthrough mode [DAL-4543]
14. Fixed issue preventing web UI access if two-factor authentication was enabled (bug present on 20.11.x firmware versions) [DAL-4509]
15. Fixed issue where CLI commands sent from DigiRM would crash the DAL device's connection to DigiRM [DAL-4412]
16. Fixed issue preventing WAN/cellular connections from working if the interface was configured with a single **Interface Up** Surelink test [DAL-4629]

## SECURITY FIXES

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

1. Update libcurl to version 7.74.0  (CVE-2020-8169, CVE-2020-8177)  [DAL-4336]
2. Update to python version 3.6.12  (CVE-2020-14422)  [DAL-4364]
3. Update OpenSSL to version 1.1.1i  (CVE-2020-1971)  [DAL-4326]
4. 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]
5. 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
6. Set SAMEORIGIN in X-Frame-Options to uppercase  [DAL-4192]
7. Automatically de-activate active user logins/sessions if the password for that user changes
8. Removed support for https CBC ciphers  [DAL-4408]
9. Fixed XSS vulnerability on serial page in the local web UI (Bug present on firmware versions 20.11.x and older)  [DAL-4646]

## 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)

This is a **mandatory** release

ConnectITmini-20.11.32.138.bin

SHA256:
8aa6206f0957f2c2c739ca7fa2c0791c9d01d42503f0d7e7b5e7b6dddd6bd1e1de23a767
40a194557fcb7bf88078ef0ac2908d5f3df9d8545de1ac2cf2216b75

MD5:     5b85b919a0824e083f6cbc683385c373

ConnectIT4-20.11.32.138.bin

SHA256:
4dd5d927bea5cdb091393bf2aa91cc06670960bf54b4ca2885741c758f9c25aa3d399146
01903a0c0c39f23d193e6b6b7a5b213f80aba58892d2f9487de33e27

MD5:     93b8e5b3b9edf8a8e54e22518c0fe4be

ConnectIT16-20.11.32.138.bin

SHA256:
6fdb0d0d75364253f1ea7eae328f7eeff0d999c021b2bcb5a353e13aa299fe052bbcd6519
4352ea43a6ecf0585166dd55b641590d0412a62cccea141a96a07d9

MD5:     40c04f4e978117146ef1ffa1ff34b032

ConnectIT48-20.11.32.138.bin

SHA256:

3befaf4ea4d9a5263f5595f910fcc44a35745431689a90535112e326efe8b51bbc205f5706
4204fa57a02507da65cc6df5c6b5c9c78eaee44133cca410efe6ac

MD5:      f15d325b2eaf90d03178c861da448d82

## FEATURES

1. Add **ssh** and **telnet** commands to Admin CLI  [DALP-664]

2. 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]

3. Add new configuration options under **Network → Devices** for setting the link speed/duplex of the device's Ethernet port(s)  [DALP-135]

4. Add options for starting, stopping, and viewing serial port activity logs through the CLI, web UI, or Digi Remote Manager  [DALP-458]

5. Support for the Sierra EM9190/9191 5G modems  [DALP-686]

6. Support for the Sierra EM7411 LTE CAT7 modem  [DALP-608]

7. IPv6 IPsec tunnel support for full IPv6 tunnels, IPv6-over-IPv4, or IPv4-over-IPv6 tunnels  [DALP-581]

8. 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]

9. 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 Quectel EG25-G 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. Added python to the ConnectIT4 product  [DAL-4061]

29. Hide main/aggressive mode option when using IKEv2  [DAL-4142]

## BUG FIXES

1. Fixed missing default settings in configuration profiles created in Digi Remote Manager (bug affects firmware versions 20.8.x and older) [DALP-658]

2. Fixed missing option for setting the **SIM Slot Preference** in configuration profiles in Digi Remote Manager (bug affects firmware versions 20.8.x and older)  [DAL-3912]

3. Fixed format of user passwords when displayed in Digi Remote Manager (bug affects firmware versions 20.8.x and 20.5.338.58)  [DAL-3889]

4. Fixed issue with policy-based routing not working in conjunction with multiple IPsec tunnels (bug affects firmware versions 20.8.x and older)  [DAL-3515]

5. Fixed issue preventing OpenVPN server-managed certificates from being re-generated if the process was interrupted (bug affects firmware versions 20.8.x and older) [DAL-3803]

6. Fixed issue preventing OpenVPN client from using an autogenerated config file from a tap-bridge openvpn server (bug affects firmware versions 20.8.x and older)  [DAL-3881]

7. Fixed some formatting output of the **show system verbose** CLI command (bug affects firmware versions 20.8.x and older)  [DAL-3805]

8. Fixed issue preventing VRRP interoperability between DAL devices and SarOS devices (bug affects firmware versions 20.8.x and older)  [DAL-4130]

9. Update VRRP+ to properly handle changes in network interface statuses bug affects firmware versions 20.8.x and older)  [DAL-4274]

10. Removed poorly formatted script contents from the **show scripts** CLI command output [DAL-3315]

11. Fixed non-working **system disable-cryptography** CLI command  [DAL-4169]
12. Fixed second-stage erase functionality on devices not enabled for aView management [DAL-3944]
13. Fixed issue preventing multicast traffic from being sent through a GRE tunnel  [DAL-3879]
14. Fixed issue preventing a firewall rule from being setup for OSFPv2 entries  [DAL-3869]
15. Fixed rare crash caused when a Quectel modem disconnected  [DAL-3867]
16. Fixed behavior of the WWAN Service LED to blink when a modem firmware update is in progress (bug affects firmware versions 20.8.x and older)  [DAL-3963]
17. Fixed issue preventing ConnectIT-Mini devices and Quectel EG25-G modules from connecting with Verizon private APNs (bug affects firmware versions 20.8.x and older)  [DAL-3605/DAL-3276]
18. Removed SIM slot 2 references and options from the configuration settings in the ConnectIT-Mini  [DAL-3930]


## SECURITY FIXES

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

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

18. Encode MAC address in URL used to sync with aView to prevent privileged escalation [DAL-4304]

## VERSION 20.8.22.32 (August 28, 2020)

This is a **mandatory** release

ConnectITmini-20.8.22.32.bin

    SHA256: 9c21f9662754e77def26af3ea0804f84267f17c28e2ce40bfad5bce655a1add3

    MD5: 926608bbdeff50c962f034ecd71c65f4

ConnectIT4-20.8.22.32.bin

    SHA256: ab46ac98bc661fa5e56559c6328229d18b10e2c76960ad077c464fb1e75a03f3

    MD5: 4d519c4318a4eac129739ae82cdef244

ConnectIT16-20.8.22.32.bin

    SHA256: 4ae37b9d855c87afd767d02a89121a49cbe95e857df6fd4cd220cb838a7ac790

    MD5: f89c26333c0a346e7635e082db92c639

ConnectIT48-20.8.22.32.bin

    SHA256: 3235a52e53cd7a27cf04badf66f4cc7bd5aa1fdd2415ae1fe705e1c4a7f9093d

    MD5: 926ae9e13ee56d080bec471f064761f6

## 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 ConnectIT4
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 ConnectIT4 or ConnectIT-Mini
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. Update to ModemManager 2020-05-19 [DAL-3254]
    1. libqmi: updated to 1.25.4+
    2. ibmbim: updated to 1.20.4+
    3. libgudev: updated to version 233
    4. Improved support for Quectel EC25/EG25 modules

## BUG FIXES

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

## SECURITY FIXES

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

1. Update to Linux kernel 5.7 (CVE-2020-10732 CVSS Score: 4.4 Medium CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L)  [DAL-3322]
2. Added local user login rate limiting to default lockout additional login attempts for 15 minutes after 5 login failures per user (Score: 6.7 Medium CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N) [DAL-3390 and DAL-3505]
   1. New configuration options are under the **Login failure lockout** section for each user in the **Authentication → User** settings
3. Prevent /etc/config/start from running when shell is disabled (Score: 5.2 Medium CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:L) [DAL-2846]
4. Prevent file path expansion on **Firmware Update** and **File System** pages in the local web UI (Score: 3.2 Low CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N) [DAL-3513, DAL- 3471, & DAL-3518]
5. 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]
6. 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](CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N)) [DAL-3393]

7. 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. Add configuration options under **Central management** for a proxy connection to Digi Remote Manager [DAL-3150]
4. 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]
5. 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]

### ENHANCEMENTS

1. Added the ability to configure DHCP pools larger than /24 subnets [DAL-2864]
2. Add a **statusall** option to the **show ipsec** CLI command to display verbose IPsec status

[DAL-2711]

3. Use modem PDP context 1 when an AT&T SIM in inserted to match new requirements from AT&T  [DAL-3093]

4. Add AT&T FirstNet IMSIs so they can be differentiated from other types of AT&T SIMs  [DAL-3163]

5. Added Python HID module to allow the DAL device to control PSUs via Python programs [DAL-2092]

6. Allow network analyzer to be configured to monitor any network interface instead of just wired Ethernet ports  [DAL-2146]

7. Added option to **ping** CLI command to ping a broadcast address  [DAL-2571]

8. Added new health metric to report the interface used by the DAL device for its configured IPsec tunnels [DAL-2710]

9. Added new health metric to report the LTE SNR value of the modem(s) on the DAL device [DAL-2904]

10. Limit metrics upload to no more than 2 per minute if backlogged [DAL-2870]

11. Added new **Locally authenticate CLI** configuration option to control whether a user is required to provide device-level authentication when accessing the console of the device through Digi Remote Manager.  Default is to allow console access without providing device-level authentication, since the user is already logged in and authenticated through Digi Remote Manager [DAL-1510]

12. Report device SKU in RCI response to Digi Remote Manager  [DAL-2940]

13. Add wbdata APN to fallback list  [DAL-3182]

14. Improved recovery of Telit modem firmware updates should the update get interrupted [DAL-2984]

15. Fixed spelling of **System utilization** chart on Intelliflow page in the local web UI  [DAL-2260]

16. 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]

17. Commonize the format and naming of rx/tx health metrics reported to Digi Remote Manager [DAL-2896]

18. Add IPv6 options to **traceroute** CLI command  [DAL-2618]

19. Add count of bytes transmitted and received to the output of the **show network interface X** CLI command  [DAL-2980]

20. 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]

21. 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]

22. Display the secondary/alternate firmware image version as the **Alt. Firmware Version** in the output of the **show system** CLI command  [DAL-3057]

23. Retain modem firmware files in the event that the firmware upgrade was interrupted  [DAL-2856]

24. Renamed OpenVPN server **device type** configuration options to clarify which options are OpenVPN managed versus device-only  [DAL-2857]

25. 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]

26. 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]

27. 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 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]

8. Fixed issue preventing backup IPsec tunnel from being established when primary/preferred tunnel was down (bug affects firmware versions 20.2.x)  [DAL-3024]

9. 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]

10. Fixed failing SureLink IPv6 ping tests (bug affects firmware versions 19.11.x through 20.2.x)  [DAL-2488]

11. Fixed issue with applying policy-based routes to incoming packets from the Internet (bug affects firmware versions 20.2.x and older)   [DAL-2589]

12. Fixed bug preventing passthrough mode from functioning if multicast was also enabled (bug affects firmware versions 20.2.x and older)  [DAL-2709]

13. 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]

14. Fixed error displayed in **show modem** CLI output when modem was not connected (bug affects firmware versions 20.2.x and older)   [DAL-2959]

15. 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]

16. Fix non-working custom DHCP options (bug affects firmware versions 20.2.x)  [DAL-3071]

17. 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]

18. 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]

19. Removed unsupported LED options listed for LR54 units in their digidevice.led Python module options (bug affects firmware versions 20.2.x)  [DAL-3250]

20. 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)

21. 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 (March 17, 2020)

This is a **mandatory** release

## ENHANCEMENTS

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

## BUG FIXES

1. *1002-CM04/1003-CM11:* Fixed cellular high-speed throughput performance issues caused by CPU slowdown and timing of gathering cellular signal details [DAL-2802]
2. *1003-CM11:* Fixed inability to utilize SIM slot 2 of an device with a Telit LE910c4-NF or LM940 modem when the two SIM slots contained SIMs from differing carriers [DAL-2897 & DAL-2986]
3. Fix health metrics warnings in Digi Remote Manager stating the local filesystem's /opt/ directory was full when it wasn't [DAL-2769]
4. Fixed missing Rx/Tx bytes in **show modem** CLI command output [DAL-2804]
5. Fixed issue preventing multicast packets from being sent through a network bridge [DAL-2774]
6. Fixed auto-reboot after restoring configuration file through local web UI [DAL-2862]

7. Fixed inability to update modem firmware on Sierra EM7511 modules [DAL-2794]
8. Fixed improper modem firmware selection on Telit LM960 module when using a  T-Mobile SIM [DAL-2376]
9. Fixed bug causing the configured **Reboot Time** to always occur in UTC instead of local timezone (issue present in older 20.2.162.x firmware versions)[DAL-2859]
10. Fixed bug preventing analyzer from being stopped in the CLI [DAL-2892]

## SECURITY FIXES

1. Fix cross-site scripting (XSS) vulnerability on various Status pages in the local web UI [DAL-2818]
2. Fix cross-site scripting (XSS) vulnerability on Configuration page in the local web UI [DAL-2819]
3. Fix cross-site scripting (XSS) vulnerability on Terminal page in the local web UI [DAL-2823]
4. Fix cross-site scripting (XSS) vulnerability on File System page in the local web UI [DAL-2823]
5. Prevent script injection exploit on the Configuration Maintenance page in the local web UI [DAL-2797]
6. Prevent unauthorized read/write access to /opt/config/ and /opt/boot when `Interactive Shell` is disabled [DAL-2865]
7. Prevent analyzer output from being saved outside of the /etc/config/analyzer directory [DAL-2672]

## VERSION 20.2.162.90 (March 11, 2020)

This is a **mandatory** release.

## NEW FEATURES

1. Telit 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]
   - 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]
   - 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. New web UI pages added under the **System** drop-down with enhanced serial details and configuration  [DALP-465]
6. Support for firmware/OTA updates on Quectel modems  [DALP-419]
7. 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. Added additional Telit-specific AT commands to mmcli-dump of support report

4. 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**

5. New default break sequence *~b* for serial connections  [DALP-253]

6. Report MCC/MNC/CID/LAC values in health metrics to Digi Remote Manager  [DAL-2502]

7. Add digicpn.gw12.vzwentp Verizon APN to fallback list  [DAL-2283]

8. Change default OpenVPN Certificate Issuer details from Accelerated to Digi  [DAL-2449]

9. Change default SSL certification from Accelerated to Digi  [DAL-1336]

10. Dual-APN support on Sierra EM7511 modem  [DAL-2311]

11. Include AT#RESETINFO and Quectel-specific AT commands in support report  [DAL-2394]

12. Rename **Configuration Management** page under the System section of the web UI to **Configuration Maintenance**  [DAL-2549]

13. Added link under **System** drop-down in web UI to download the support report

14. Update the **Digi Remote Manager** link under the **System** drop-down in the web UI to open in a new tab  [DAL-2294]

15. Update the **Authentication → Idle** timeout setting to have a default value of 10-minutes (previously the default was blank)  [DAL-2292]

16. Send up to 4 IPsec tunnels' details as health metrics reported to Digi RM  [DAL-1476]

17. Change the default behavior of the **SIM failover alternative** settings from **None** to **Reset modem**  [DAL-2687]

18. Renamed **Signal Strength** references to **Signal Quality** [DAL-2707]

19. On the Network Status page of the web UI, add **Interface is up** message in SureLink status details

20. Add **service.qcdm.modem.device** and **service.qcdm.modem.interface_number** config

options for specifying QCDM/QXDM port for a modem [DAL-2497]

## SECURITY FIXES

1. Update to Linux kernel version 5.4.8
2. Removed plain-text passwords displayed in the output of the **show config** CLI command [DAL-2513]
3. Added backoff timer when maximum number of SSH/UI login retries is exceeded [DAL-2590]
4. Update to Python version 3.6.10 [DAL-2534]
5. Update tcpdump to version 4.9.3 (CVE-2017-16808 CVE-2018-14468 CVE-2018-14469 CVE-2018-14470 CVE-2018-14466 CVE-2018-14461 CVE-2018-14462 CVE-2018-14465 CVE-2018-14881 CVE-2018-14464 CVE-2018-14463 CVE-2018-14467 CVE-2018-14463 CVE-2018-10103 CVE-2018-10105 CVE-2018-14879 CVE-2018-14880 CVE-2018-16451 CVE-2018-14882 CVE-2018-16227 CVE-2018-16229 CVE-2018-16301 CVE-2018-16230 CVE-2018-16452 CVE-2018-16300 CVE-2018-16228 CVE-2019-15166 CVE-2019-15167) [DAL-2611]
6. Update libpcap to version 1.9.1 [DAL-2611]
7. Update e2fsprogs to version 1.45.5 (CVE-2019-15161 CVE-2019-15162 CVE-2019-15163 CVE-2019-15164 CVE-2019-15165 CVE-2017-16808) [DAL-2611]
8. Update openvpn to version 2.4.4 (CVE-2017-12166) [DAL-2614]
9. Update libldns to version 1.7.1 (CVE-2017-1000231 CVE-2017-1000232) [DAL-2613]
10. Update libxml2 to version 2.9.10 (CVE-2018-9251 CVE-2018-14567) [DAL-2612]
11. Restrict /etc/config/ to admin-only users [DAL-1396]
12. Remove plaintext password from RADIUS debug logs [DAL-2640]
13. Prevent Framebusting JavaScript click-jacking [SEC-494]
14. Prevent users from gaining elevated shell access through custom scripts [DAL-2628]
15. Update libcurl to version 7.69.0 (CVE-2019-15601) [DAL-2732]
16. Update pppd to version 2.4.8 (CVE-2020-8597) [DAL-2732]
17. Fix elevated root access through custom scripts when no-shell is enabled [DAL-2628]
18. Obfuscate sensitive device configuration settings [DAL-1388]

## BUG FIXES

1. *Connect IT 16/48 only:* Fixed timezone offset when saving time to onboard RTC [DAL-2678]
2. *Connect IT 16/48 only:* Fix bug where devices with an internal realtime clock would not adjust their local time to the configured timezone [DAL-2272]
3. Fixed bug where SureLink™ DNS tests took longer than the configured timeout to complete [DAL-2702]
4. Fixed SSL validation bug preventing modem OTA updates [DAL-2547]
5. Fixed bug where newly-created network Bridges would not be listed as options under the Device drop-down for network interfaces [DAL-2575]
6. 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]
7. Fixed bug where a device configured with multiple SSH keys would only honor the last SSH key in the list [DAL-2506]
8. Display the active cellular band for Quectel modems [DAL-2298]
9. Fixed bug where the web UI would display bytes transmitted/received for network interfaces as **N/A** [DAL-2295]

10. Fixed bug where the web UI wouldn't show IP information for client devices connected to an
11. OpenVPN server running on the DAL device  [DAL-2251]
12. Fix formatting output of **show config** CLI command when the configuration settings contained an array  [DAL-2594]
13. Fix bug when adding a new element to an array in the **config** mode of the CLI  [DAL-2594]
14. Fix bug where CLI ping and traceroute commands would ignore any interface specified in the command  [DAL-2605]
15. Fix bug where SureLink™ default tests would continue to pass if cellular modem lost its active data connection  [DAL-2609]
16. Fix a bug handling certificate files with spaces
17. Fixed padding issue with downloading SCEP CA certificates  [DAL-2212]
18. Fixed rare issue with passthrough ancillary DNS not resolving if **ancillary DNS redirect** issue was disabled
19. Fixed issue with active serial logins when a serial-related configuration change was applied to the DAL device  [DAL-2696]
20. Fixed output of **show modem** CLI command when cellular modem re-initializes
21. 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

2. 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]

## VERSION 19.11.72.58 (December 6, 2019)

This is a **mandatory** release.

### NEW FEATURES

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

- new Dashboard overview page
- Mobile-friendly UI

2. Added new custom page in the web UI for configuring Power Controllers [DAL-2121]

3. New network analyzer and packet capture tool, included in in both the Admin CLI and web UI [DAL-1575]

4. Added options under the *Network->Modem* section of the device configuration to setup SIM slot prioritization and SIM slot failback [DALP-287]

5. Added new *Preferred tunnel* option under *VPN->IPsec->Tunnels* to configure a tunnel to be a primary or failover tunnel [DAL-1478]

6. 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]

7. Added ability to receive encrypted SMS commands from Digi Remote Manager [DALP-270]

8. Add support for the Telit LM960A18 LTE CAT18 module [DAL-1905]

9. Add support for Sierra Wireless EM7511 LTE CAT18 module [DAL-1414]

10. Add support for Quectel EG25-G LTE CAT4 module [DALP-339]

11. Add support for Quectel EG06 LTE CAT6 module [DALP-403]

12. Add Python support on all products (previously only available on the IX14 and Connect IT 16/48) [DAL-1907]

13. Add *system disable-cryptography* Admin CLI command to configure a device for *nocrypt* mode [DALP-491]

14. 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

15. Add *show usb* Admin CLI command [DAL-2029]

## ENHANCEMENTS

1. *Connect IT Mini only:* Assign new **Edge** firewall zone to LAN Ethernet port by default to prevent the device's DNS services from being advertised on the network [DAL-2085]

2. Default user changed from root to admin [DAL-936]. Once a device is upgraded to 19.11.72.58 or newer firmware
    - If you do have an admin user configured, it will not be touched by the update
    - 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
    - If you had a root user configured (e.g. not factory defaults) it will be preserved to maintain existing user access
    - Restoring the device to factory defaults after update will result in only the admin user. If you have a root user and do a factory default, you have to login with the admin user instead of root, using the same default password printed on the bottom of the device

3. Added the ability to push OpenVPN routes in subnet mode [DAL-2224]

4. Add cellular IMEI and firmware version, along with bluetooth and accelerometer info to show manufacture command in the Admin CLI [DAL-2030]

5. Add the % measurement value to the CPU usage in the show system output of the Admin CLI

6. Device is passthrough mode with an IPv6 connection now honors and utilizes the MTU in IPv6 RAs

7. When using Verizon SIMs, utilize the OMADM process to auto-discover the APN [DAL-1371]

8. Enhance modem firmware update tool to support multiple modem installations [DAL-2148]

9.  Created new Edge firewall zone to prevent the device's DNS services from being advertised on the network, which still allowing SSH and web UI access [DAL-2085]

10. Removed 192.168.210.254 Default IP gateway [DAL-2095]

11. Added support for sending RFC2136 compatible DNS updates to external DNS servers [DALP-446]

12. Add new options under VPN->IPsec->Tunnels->Local endpoint->ID->ID Type for using the device's MAC address or serial number as its local endpoint ID [DALP-437]

13. Updated the filename of the support report generated through the web UI or CLI to include the Digi name [DAL-1434]

## SECURITY FIXES

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

## BUG FIXES

4.  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]

5.  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]

6.  Fixed bug with timing of RCI callbacks from Digi Remote Manager (bug present in firmware versions 19.8.1.61 and older) [DAL-2091]

7.  Fixed bug where RX/TX data usage metrics reported to DRM could be mistakenly calculated as a negative sum [DAL-1972]

8.  Fixed crash in IPsec configuration with more than 6 for IKE Phase 1 proposals or more than 10 IKE Phase 2 proposals [DAL-2066]

9.  Fixed bug in reporting the reboot counter metric to DRM [DAL-1932]

10. Fixed bug where persistent system logs could not be remotely accessed through DRM [DAL-2060]

11. Fixed bug where DRM would always shows the device's connected method as ethernet [DAL-1993]

12. Prevent users from selecting non-production firmware versions when perform modem OTA updates [DAL-1662]

13. Fixed bug preventing Linux clients from querying a DAL device running a NTP server [DAL-1815]

14. *Connect IT 4 and Mini:* Fixed bug where early DCD interrupts on a serial port could cause the device to not boot up  [DAL-1873]

## VERSION 19.8.1.61 (October 22, 2019)

This is a **recommended** release.

## ENHANCEMENTS

1.  Skip auto-APN detection when using Telus SIM cards [DAL-1928]

2.  Add QCDM service for accessing QXDM ports of Qualcomm-based modems  [DAL-1904]

3.  Add microcom tool [DAL-1872]

## BUG FIXES

1.  Fixed bug in runt where the boot version was reported incorrectly (bug present in firmware

version 19.8.1.43) [DAL-1828]

2. Fixed registration delays on devices with Telit modems using Sprint SIM cards (bug present in firmware versions 19.8.1.43 and older) [DAL-1872]

3. Fixed stability issues with 1003-CM11 modem (bug present in firmware versions 19.8.1.43 and older) [DAL-1843]

4. Fixed bug preventing devices using a 1002-CM06 modem (Sierra MC7455) with a Telus SIM from loading the Telus carrier-firmware onto the modem (bug present in firmware versions 19.8.1.43 and older) [DAL-1823]

5. Fixed memory leak causing a DAL device in passthrough mode to stop responding to ARP requests on its LAN port (bug present in firmware versions 19.8.1.43 and older) [DAL-1686]

6. Fixed bug preventing SSH keys from being used to authenticate when establishing a SSH session to the DAL device (bug present in firmware version 19.8.1.43) [DAL-1742]

## VERSION 19.8.1.43 (August 30, 2019)

This is a **mandatory** release.

### NEW FEATURES

1. Telit LE910c4-NF modem support
2. WAN passthrough, allowing for [multi-WAN passthrough setups](#) [DALP-163 & DAL-959]
   - As a result, passthrough settings are not under the Modem section anymore, and instead are by default listed under the Network-Interface->LAN section for devices with passthrough enabled by default.  To change a device defaulting in passthrough mode to router mode, simply change  the "Network->Interfaces->LAN->Interface type" from "IP Passthrough" to "Ethernet", and then you'll see the normal router-mode configurations options available.
3. Support for managing network-enabled power strips and power outlets with the powerman tool [DALP-193]
4. 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]
8. Improved formatting in the `show route` CLI output, including finer distinction of static routes [DAL-1176]
9. Include policy and connection details in `show ipsec` CLI output, along with improved status details [DAL-1190 & DAL-1174]
10. Improve labeling in output of the `show network interface` X CLI command
11. Show OpenVPN client list and rx/tx bytes in `show openvpn` CLI output [DAL-1192]
12. Add filtering options in `show log` CLI command [DAL-1181]
13. Add CPU usage, device temperature (if available), device description, and location details in `show system` CLI output [DAL-1172]
14. Updated local web UI logout link to list the name of the logged in user [DAL-1142]
15. Renamed the section of central management options from `config` to `cloud` [DAL-1255 & DAL-1256]

16. Added configuration option to have DHCP leases file persistent or clear across reboot [DAL-1196]

17. Update CLI table formatting to double space & blank fields [DAL-1186]

18. Add bypass-lan plugin to strongswan to allow 0.0.0.0/0 remote IPSec networks [DAL-1007]

## SECURITY FIXES

1. Update Linux kernel to version 5.1.14 [DAL-1076]

2. Busybox update to version 1.31.0 [DAL-1161]

   - The new busybox shell environment no longer allows local variable statements such as the following:
     - `local ip_addr='1.2.3.4'`
   - and instead the variable must be set without the `local` option, such as:
     - `ip_addr='1.2.3.4'`
   - includes update to httpd webUI

3. Update dnsmasq2 to version 2.80 to address DNS cache snooping (CVE-2017-15107) [DAL-1386]

4. Update conntrack-tools to version 1.4.5

5. Update libnetfilter_conntrack to version 1.0.7

6. Update libmnl to version 1.0.4

7. Update bind to version 9.14.2 [DAL-1338]

8. Update iptables to version 1.8.3

9. Update libqmi to version 1.23.1 [DAL-885]

10. Update libmbim to version 1.18.0 [DAL-885]

11. Update stunnel to version 5.54 [DAL-1162]

12. Update quagga to version 1.2.4 (CVE-2016-1245 and CVE-2017-5495) [DAL-1160]

13. Update tar to version 1.32 [DAL-1159]

14. 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 issue where Connect IT16/48 devices would fail to start up if a 1003-CM modem was inserted [DAL-1605]

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 rare issue where Connect IT 4 booted without access to flash

6. 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]

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 missing WAN config options in Connect IT 4 devices' default config options

14. Fix reloading of displayed configuration options when enabling/disabling aView central management in the local web UI   [DAL-834]

15. Fix reloading of the Dashboard page when enabling/disabling Intelliflow in the local web UI [DAL-780]

16. Reset LEDs displayed during reboot instead of freezing the LEDs to show the last known device state before the reboot [DAL-886]

17. Fix bug where Digi Remote Manager RCI thread blocks indefinitely waiting for config write lock [DAL-573]

18. Fix bug where `ls` command in the admin CLI required a terminating / on the path [DAL-1251]

19. Fix bug with show openvpn name CLI command output [DAL-1191 & DAL-1192]

20. Fix bug with carrier, plmn, and modem status output in show modem CLI command

21. Fix column spacing and lower-casing consistency in show arp CLI output [DAL-1173]

22. Fix parsing of carrier names when posting cellular modem details to Digi Remote Manager [DAL-1553 & DAL-1326]

23. Limit decimal numbers reported to Digi Remote Manager to six decimal places [DAL-807]

24. Fixed bug with Sierra MC73xx-series cellular modules in 1002-CM03 CORE modems where the modem would require a power cycle after upgrading the firmware of the modem in order to reconnect [DAL-1716]

25. 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]

26. Add Telus m2m APNs to fallback list [DALP-452]

27. *Connect IT 16/48 only:* Fix bug causing the device to reset to default settings if the device experienced a power loss (bug present on firmware versions 19.3 - 19.8.1.30) [DAL-1666]

## 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 19.3.58.59 (March 14, 2019)

- Initial product release