Digi Accelerated Linux (DAL) Release Notes
Digi Accelerated/Enterprise Routers
Version 19.11.72.85

INTRODUCTION

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

SUPPORTED PRODUCTS

- Digi EX15
- Digi EX15W
- AcceleratedConcepts 5400-RM
- AcceleratedConcepts 5401-RM
- AcceleratedConcepts 6300-CX
- AcceleratedConcepts 6310-DX
- AcceleratedConcepts 6330-MX
- AcceleratedConcepts 6335-MX
- AcceleratedConcepts 6350-SR
- AcceleratedConcepts 6355-SR

KNOWN ISSUES

- none

UPDATE BEST PRACTICES

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

Digi recommends Digi Remote Manager or Digi aView for automated device updates. For more

information, follow the instructions for Digi Remote manager or Digi aView in the links below:

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

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

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

TECHNICAL SUPPORT

Get the help you need via our Technical Support team and online resources. Digi offers multiple support levels and professional services to meet your needs. All Digi customers have access to product documentation. firmware, drivers, knowledge base and peer-to-peer support forums.

Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

VERSION 19.11.72.85 (January 21, 2019)

This is a **recommended** release.

NEW FEATURES

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

ENHANCEMENTS

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

BUG FIXES

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

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

VERSION 19.11.72.58 (December 6, 2019)

This is a **mandatory** release.

NEW FEATURES

1. Re-themed web UI with improved navigation and functionality. New functionality includes:
   - The ability to view local filesystem contents [DAL-2110]
   - Help-text on login page
   - Quick-config access on status pages
   - new Dashboard overview page
   - Mobile-friendly UI
2. New network analyzer and packet capture tool, included in in both the Admin CLI and web UI [DAL-1575]
3. Added options under the *Network->Modem* section of the device configuration to setup SIM slot prioritization and SIM slot failback [DALP-287]
4. Added new *Preferred tunnel* option under *VPN->IPsec->Tunnels* to configure a tunnel to be a primary or failover tunnel [DAL-1478]
5. Add new **DHCP Hostname** option for IPv4 and IPv6 settings under the **Network->Interfaces** section of the configuration to allow the device to advertise its hostname to the DHCP server upon connection (disabled by default) [DALP-427]
6. Added ability to receive encrypted SMS commands from Digi Remote Manager [DALP-270]
7. Add support for the Telit LM960A18 LTE CAT18 module [DAL-1905]
8. Add support for Sierra Wireless EM7511 LTE CAT18 module [DAL-1414]
9. Add support for Quectel EG25-G LTE CAT4 module [DALP-339]
10. Add support for Quectel EG06 LTE CAT6 module [DALP-403]
11. Add Python support on all products (previously only available on the IX14 and Connect IT 16/48) [DAL-1907]
12. Add *system disable-cryptography* Admin CLI command to configure a device for *nocrypt* mode [DALP-491]
13. Once a device is set for *nocrypt* mode, a user must press the Erase button to reset the device to factory default settings to disable *nocrypt* mode and restore the device back to standard operation
14. Add *show usb* Admin CLI command [DAL-2029]

ENHANCEMENTS

1. 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
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

VERSION 18.10.225.15 (Nov 14, 2018)

This is a **recommended** release.

NEW FEATURES

6. IPSec IKEv2 support

7. GRE tunneling support with keepalives

8. DRM support on all ACL products

ENHANCEMENTS

15. Added configuration options for domain-based routing

    set as a Destination option in Policy-based routes

16. Change 6310-DX to passthrough mode by default (WAN port still enabled)

17. Updated DHCP tftpserver option to accept http URL

18. Updated the Status page of the local web UI to display WiFi channel and frequency information

19. Added configuration option to select the country for WiFi (controls Tx Power and Channel requirements)

20. Added configuration options to control IPSec SA lifetime and IKE lifetime settings

21. Added configuration options to use x509 or RSA authentication methods for IPSec tunnels

22. Added configuration option to the aView tunnel for it to use as an x.509 authentication the same signed SSL certificate used by the device to get its configuration settings from aView (disabled by default)

BUG FIXES

1. Fixed bug where OpenVPN connection information wasn't being cleared when OpenVPN restarts

2. Fixed bug where users had to lock the APN for a 1002-CM04 to connect with a Verizon SIM

VERSION 18.8.14.124 (Oct 10, 2018)

This is a **mandatory** release.

NEW FEATURES

2. Support for all Telit LE910 modem variants

3. Added CaptivePortal feature, which can be configured and applied to both wired and wireless interfaces

4. Added support in device configuration for setting up exernal USB-to-serial adapters and accessing them via the console login prompt

5. Added button on System page of web UI to reboot the device

6. Added new WiFi scanning and setup tool on System page of the local web UI

7. Added sftp tool

ENHANCEMENTS

1. Added option in device configuration to enable/disable roaming on a cellular modem interface

2. Added new options for Scheduled tasks → custom scripts to control memory limit, log output, single-threaded versus multi-threaded execution, and follow-up action(s) once the custom script finishes

3. Added new option for Network -> Modems -> Modem entries to limit the maximum number of interfaces that can be associated to a particular modem

4. Added crmstatic.bell.ca.ioe to APN fallback list for Bell Canada SIMs

5. Added 12655.mcs to APN fallback list for AT&T SIMs

6. Added orange.m2m.spec and orange.m2m to APN fallback list for Orange (France) SIMs

7. Added Telemach carrier (Slovenia), Telia carrier (Finland), data.dna.fi (Finland) and julkinen.dna.fi (Finland) APNs to APN fallback list

8. Updated local web UI to only show the Dashboard page if Intelliflow is enabled

9. Enhanced load speed of WebUI's status page by loading each page tab as a new page

10. Added ipsec option to Admin CLI to show debug info of device's IPSec tunnels

11. Added runtdump and runtget options to the modem utility in the shell console

12. Added requirement for user to provide login credentials when accessing the 3-pin serial console of the device

13. Enhanced serial login mode so sessions do not close/open on every reload

14. Track and display the RSRP, RSRQ, and band for Telit LE910 modems

15. Use RSRP and RSRQ of Telit modems for calculating signal strength, same as Sierra modems

16. Updated default QoS settings to use the correct TOS headers to prioritize SIP/VoIP traffic

17. Enhanced OpenVPN status in WebUI's tunnel page to include the state of 'connected'

18. Improved reliability of carrier SIM/firmware matching by referencing PLMN first, then ICCID if no matching PLMN is found

19. Added system log when someone presses the SIM select button

20. Enhanced system log to show HTTP error code when aView certificate cannot be obtained

21. Updated AT&T SSL certificate chain

22. Updated service for handling remote commands to only accept POST HTTP requests, and deny GET requests

SECURITY FIXES

3. Prevent HTTP Header Injection by allowing only alphanumeric characters in the username entered into the web UI

4. Prevent HTTPS Cross Site Request Forgery (CSRF) by not accepting auth token in the cookie of POST requests

5. Fixed vulnerability to WebUI clickjacking

BUG FIXES

1. Fixed bug with carrier SIM/firmware matching when ICCID or MNC weren't the typical number of characters

2. Fixed bug where signal strength LEDs were not displayed on 54xx-RM devices
    bug present in firmware versions 18.4.x.x

3. Fixed bug where Intelliflow would reset if network interfaces were enabled or disabled, or if the order of those interfaces changed

4. Fixed issue where WiFi AP would be setup first, choosing a channel, before the client connection, which would prevent it from scanning to find the desired SSID on the proper channel.

5. Fixed bug where IMEI would not be displayed if a SIM wasn't present

6. Fixed bug with obtaining internal temperature of Sierra-based modems

7. Fixed bug where serial port could not be used if a user pressed Ctrl+d at the login prompt (restarting the seriald process or rebooting the device would temporarily fix this)

8. Fixed bug where OpenVPN clients couldn't access other networks on the device running the OpenVPN server

9. Fixed bug preventing users from remotely changing configuration settings through a SSH command

10. Fixed bug with multicast support in OpenVPN

11. Fixed bug where user could be required to enter in credentials twice to login to the local web UI

12. Fixed bug where HTML/Javascript code could be executed from a SSH login without authenticating

13. Fixed bug where management priority value would not be reset correctly after switching from WAN primary to backup, or vice-versa

14. Fixed bug where tab completion in CLI would cause segmentation fault

15. Fixed bug where large-sized packets would be lost when sent through an IPSec tunnel built over a WAN connection with a MTU lower than 1500 (e.g. cellular)

16. Fixed bug where a policy-based router entry with a destination of "Zone Any" directed out an interface without a default route result in the firewall DROPping the packets

17. Fixed bug with reconnecting Telit modem after device was power cycled.

18. Fixed firmware downgrade functionality. Future firmware versions after 18.8.14.0 will be able to downgrade to 18.4.54.41 or newer

19. Fixed bug with performing WebUI OTA updates for Telit LE910-NA V2 modems (previously, only manual firmware upload and aView remote commands worked)

20. Fixed slowdown of initial connectivity with Optus SIMs

21. Removed reporting of MSL code on the Modem page of the WebUI (Sprint only)

22. Reduced TCP fragment limits for security vulnerability

23. Linux kernel update from 4.15 to 4.17

24. openssl update with 1.0.2o patch

25. stunnel update from 5.37 to 5.46

VERSION 18.4.54.41 (July 5, 2018)

This is a **recommended** release.

BUG FIXES

13. Fixed bug where resetting management priority option back to 0 would not set correctly unless the device was rebooted.

    Bug present in firmware versions 16.10.32-18.4.54.28

14. Fixed bug where ICCID values starting with 890 would have the zero not displayed in the web UI or Accelerated View

    Bug present in firmware versions 18.4.54-18.4.54.28

15. Fixed bug preventing devices from being configured to connect to Verizon-only SIMs

    Bug present in firmware versions 18.4.54-18.4.54.28

16. Fixed bug preventing SIM failover if no modem interfaces matched the SIM present in the active SIM slot, or if no SIM was detected in the active SIM slot.

    Bug present in firmware versions 18.4.54-18.4.54.28

17. Fix bug preventing Carrier Smart Select from functioning properly on cat3 and cat6 Sierra MC73xx/MC74xx modems.

    Bug present in firmware versions 18.4.54-18.4.54.28

18. Shorten the time between when a device establishes its tunnel to ispec.accns.com and when it logs its management IP address to aView. Previously, this could take up to 5 minutes. Now, it should happen within seconds.

19. Cleaned up the Configuration page of the local web UI to show the appropriate default settings when central management is enabled.

    bug present in firmware versions 18.4.54-18.4.54.28

20. Fixed bug where IPSec packets could be corrupted when sent through a Sierra modem.

    bug present in firmware versions 18.4.54-18.4.54.22

VERSION 18.4.54.28 (June 25, 2018)

This is a **recommended** release.

BUG FIXES

1. Fixed bug where firmware cannot be correctly downgraded from aView (bug present in firmware versions 17.10.74 to 18.4.54.22)
2. Fixed bug with mangling IPSec tunnel traffic on firmware 18.4.54 with Sierra modems
3. Fixed inbound modem passthrough filtering
4. Fixed bug preventing modem interfaces from establishing an IPv4-only or IPv6-only connection
5. Fixed bug where tab complete causes segmentation fault in empty arrays in CLI interface

VERSION 18.4.54.22 (May 25, 2018)

This is a **mandatory** release.

NEW FEATURES

1. Added Quality Of Service (QOS)
2. Added Telit modem firmware update support on devices
3. Added ability to toggle SIM slot based on remote command received from aView

ENHANCEMENTS

1. Major modem support update, including dual PDN/APN, support for multiple modems, and support for complex modem/SIM/APN mappings
2. Added configuration option to manually set SIM phone number
3. Added 11904.mcs and wbb.attbusines.net to the AT&T APN list
4. Added NAT keep alive configuration for IPSec tunnels
5. Added basic multi-interface support for PCAP based DAQ intrusion detection in SNORT
6. Added links to System page of web UI for downloading OpenVPN (.ovpn) configuration files
7. Improved system resources by stop reloading configurations in system pages of the web UI
8. Improved network interface/device status format on the Dashboard page of the web UI

9. Improved web UI Device Details page to auto-refresh values

10. Improved OpenVPN server configuration to allow specific designation of IP

11. Implemented "Server managed certificate" modes in OpenVPN

12. Redesigned network interface and modem configurations in WebUI

13. Updated IntelliFlow copyright information

14. Network > Advanced section is added from a WebUI restructuring

15. Improved SIM ICCID accuracy by revised search logic

SECURITY FIXES

1. Linux Kernel update: from 4.14 to 4.15

BUG FIXES

1. Fixed bug with LE910v2 LTE registration on AT&T

2. Fixed bug where IPSec's source address assignment was often incorrect

3. Fixed bug to allow IPv6 passthrough and DHCPv6 server to run on a device

4. Fixed rare bug where duplicate static IP addresses would cause DHCP server crash

5. Fixed rare bug where pressing the enter key for a text entry on the Configuration page of the web UI would inherently save the configuration instead of performing the "Add" action.

6. Fixed rare bug where cellular modem service would crash if no SIM was detected

7. Fixed bug with setting a custom gateway for static bearers

8. Fixed bug where OpenVPN tunnel names would clash for servers and clients due to the use of the same "o_" prefix

9. Fixed bug with incorrectly matching MAC addresses 6330-MX bootenv variables

10. Fixed bug where temperature milliCelsius was incorrectly converted to Celsius

11. Fixed bug where MNC and ICCID does not match correctly

12. Fixed bug where 540X signal strength was not displayed on LEDs