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

Digi Accelerated Linux (DAL) Release Notes
Digi Accelerated Routers and Console Servers
Version 19.5.88.81

INTRODUCTION

This is a production firmware release for all DAL supported products. This is a mandatory production firmware release that addresses the "SACK" Vulnerability - (CVE-2019-11477). For more information, see https://www.digi.com/resources/security

SUPPORTED PRODUCTS

- Digi EX15
- 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

- EX15 with a 1003-CM11 modem (LTE CAT11 Telit LM940) left online disconnects randomly over time (DAL-1214)

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 here or the instructions for Digi aView here. 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 19.5.88.81 (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

1. Added support for upgrading Telit LE910_XX modules to the latest xx5 firmware
2. Update aView defaults to tunnel to ipsec.accns.com endpoint for remote commands
3. Added 18327.mcs and 13631.mcs AT&T APNs
4. Added intra.vzwentp Verizon APN
5. Add Network->Modem options to basic options when central management is enabled
6. Added ability to set custom DHCP options under the IPv4 -> DHCP server -> Advanced settings configuration options for a network interface
7. 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
8. Updated custom SNMP MIB to include OIDs for all available cellular modem metrics (RSRP, RSRQ, RSSI, MCC, MNC, etc.)
9. Added GRE and IP-tunnel details to the Tunnels tab on the Status page of the local web UI
10. 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
11. Added Telit-specific AT commands to mmcli-dump file included in a support report generated from the System page of the local web UI
12. 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

1. IPSec IKEv2 support
2. GRE tunneling support with keepalives
3. DRM support on all ACL products

ENHANCEMENTS

1. Added configuration options for domain-based routing
   set as a Destination option in Policy-based routes
2. Change 6310-DX to passthrough mode by default (WAN port still enabled)
3. Updated DHCP tftpserver option to accept http URL
4. Updated the Status page of the local web UI to display WiFi channel and frequency information
5. Added configuration option to select the country for WiFi (controls Tx Power and Channel requirements)
6. Added configuration options to control IPSec SA lifetime and IKE lifetime settings
7. Added configuration options to use x509 or RSA authentication methods for IPSec tunnels
8. 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

1. Support for all Telit LE910 modem variants
2. Added CaptivePortal feature, which can be configured and applied to both wired and wireless interfaces
3. Added support in device configuration for setting up exernal USB-to-serial adapters and accessing them via the console login prompt
4. Added button on System page of web UI to reboot the device
5. Added new WiFi scanning and setup tool on System page of the local web UI
6. 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

1. Prevent HTTP Header Injection by allowing only alphanumeric characters in the username entered into the web UI
2. Prevent HTTPS Cross Site Request Forgery (CSRF) by not accepting auth token in the cookie of POST requests
3. 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

1. 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
2. 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
3. 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
4. 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
5. 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
6. 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.
7. 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
8. 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