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 Release Notes
AnywhereUSB Plus
Version 20.11.32.168

INTRODUCTION

This is a patch firmware release for AnywhereUSB Plus products.

AnywhereUSB Plus is a Remote USB 3.1 Hub that implements USB over IP technology over Gigabit Ethernet networks. The Hub enables communication with USB-enabled devices from virtualized systems and from remote host computers. You can securely deploy AnywhereUSB Plus Remote USB 3.1 Hubs in non-secure environments, making it ideal for point-of-sale, kiosks, surveillance, industrial automation, or any mission-critical enterprise application.

The AnywhereUSB 2 Plus is a Gigabit Ethernet-attached solution that provides 2 USB 3.1 Gen 1 ports to connect a wide range of peripheral devices such as USB license dongles, scanners, printers, cameras, storage media, or other USB devices.

The 8- and 24-port models provide support for 10 Gigabit Ethernet and include SFP+ interfaces.

SUPPORTED PRODUCTS

- AnywhereUSB 2 Plus
- AnywhereUSB 8 Plus
- AnywhereUSB 24 Plus

KNOWN ISSUES

- non-primary DNS servers are still queried through the wrong interface when ***use_dns*** configuration option is set to ***primary*** (resolved by changing ***use_dns*** to either ***always*** or ***never***) [DAL-3156]
- 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]

UPDATE CONSIDERATIONS

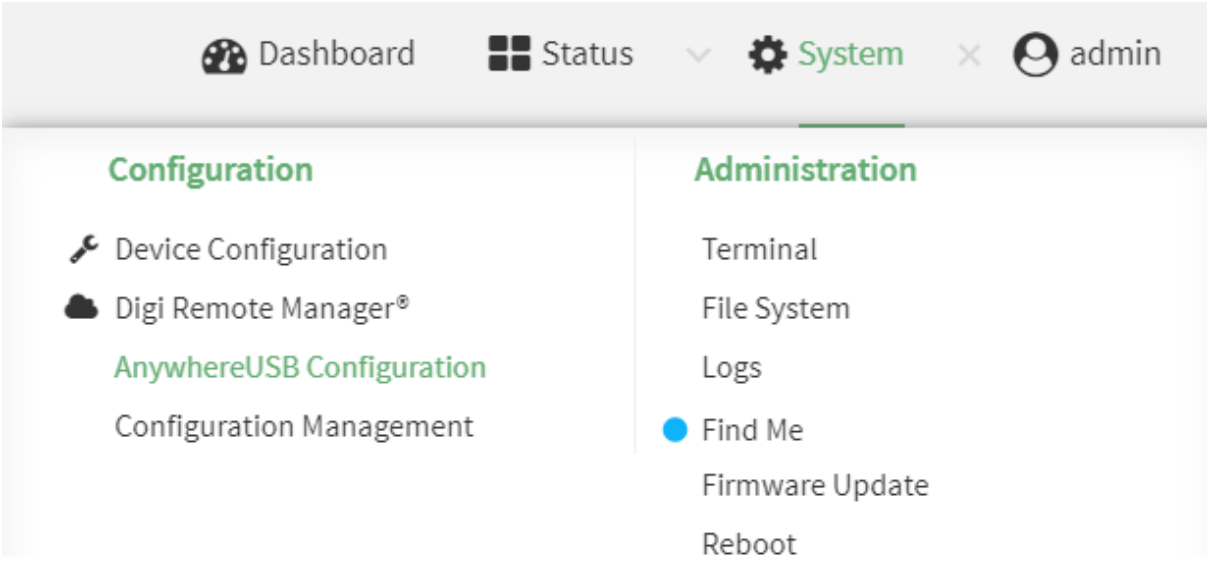
Starting with version 19.11.x of firmware of AnywhereUSB Plus, Digi has standardized on a single user interface for all new products. There are differences in the location of configuration features,

however units updated from the previous firmware to this version will have their configuration automatically migrated.

Because of the differences in the interface, users should first review the documentation to familiarize themselves with the new look and feel. The documentation for this version is located on the Digi support site at:

https://www.digi.com/resources/documentation/digidocs/90002383/default.htm

To configure an AnywhereUSB feature, click on the **System** menu located at the top right of the Web Page to open the **AnywhereUSB Configuration** page. For additional configuration, please refer to the link above for the updated documentation.



UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application.

To update the AnywhereUSB Plus firmware from 3.0.x to the new firmware follow these steps:

1. Software is available through Digi Support Site
2. Connect to the device's web UI by connecting your PC to the Ethernet port of the device.
3. Use the AnywhereUSB manager to find your hub and open the Web UI
4. Select the ***Administration->Firmware update*** on the left side of the page.
5. Select the ***Choose File*** button next to the ***Select Firmware*** section.
6. Browse for and select the downloaded firmware file.
7. Click the ***Update*** button.

To update the AnywhereUSB Plus firmware from 19.11.x or 20.x to the new firmware, 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 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

VERSION 20.11.32.168 (December 23, 2020)

This is a recommended release

AnywhereUSB2-20.11.32.168.bin

SHA512:
1e58f363db72d07d008e4709e41ea536dd1d704de676ef88acd4c75c664ff3d075b951cc1bb2c7442f5d889d66f04466258394c5b0fe27ec5d9c989cf7104852

MD5: 77b1055fda97bddcb1dd2d7d20d5fb04

AnywhereUSB8-20.11.32.168.bin

SHA512:
0e66a03cb5954fc7ec4967c6abc906cf96f67ffbbbc182102a634e74083eacb077a54f97d3ca73d8914f4ad509c523e2a9525375a8d0217b2c12582f7b2bb6e7

MD5: 9c46957e97fe5fe6d8e47cfda7da1231

AnywhereUSB24-20.11.32.168.bin

SHA512:
075bf62b1a437d42da97c3cd52985635da89c1d99e3315060a15daa03f7cf740db2520a9b239c3f17286ac6fbc7948ffb2a089d5584671ef8b83e76c41e4930d

MD5: 39a28482fe0e629b831424bf7e1d874e

ANYWHEREUSB-specific CHANGES

1. Fixed bug preventing large-sized USB traces from being saved properly (affects firmware version 20.11.32.139) [DAL-4422]
2. Fixed bug preventing USB trace initiated from the CLI from saving (affects firmware version 20.11.32.139) [DAL-4421]

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 20.11.32.139) [DAL-4414]

VERSION 20.11.32.138 (December 2, 2020)

This is a ***mandatory*** release

AnywhereUSB2-20.11.32.138.bin

SHA256: de5bb74d7dabf56ae2637e3b12ad5b90a3ad0c799102202fc72c92db0fa4a390

MD5: 7b1bb4ea725366ba65da5714c6d67df9

AnywhereUSB8-20.11.32.138.bin

SHA256: d9b1d985da0420998fe2f4feb1b464bda2f73bcc442874555658d1141e466e8b

MD5: d634c879bd13264ff8854e917a2e8bb4

AnywhereUSB24-20.11.32.138.bin

SHA256: d53e3c9863e2827db0b08eaaa5666f16df584b53236c303b8e62b28237f7013a

MD5: bc32f136c562de23946acd25057e46c7

ANYWHEREUSB-specific CHANGES

1. Update AnywhereUSB service to recognize additional USB devices, including Hamilton Microlab Starlet USB device s [AWG3-2527]
2. Fixed race condition in starting the AnywhereUSB Manager service if the device had WAN bonding enabled (bug affects firmware versions 20.8.x and older) [DAL-4114/DAL-4231]
3. Address memory leaks causing awusb manager service to crash over time (bug affects firmware versions 20.8.x and older) [DAL-4043/DAL-3793]
4. 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]
5. Fixed exploit through firmware update process (CVSS score 6.0 Medium CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N) [DAL-4255]
6. Add AppArmor to AnywhereUSB Plus products (CVSS score: n/a) [DAL-4248]

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. Support for the Sierra EM9190/9191 5G modems [DALP-686]
5. Support for the Sierra EM7411 LTE CAT7 modem [DALP-608]
6. IPv6 IPsec tunnel support for full IPv6 tunnels, IPv6-over-IPv4, or IPv4-over-IPv6 tunnels [DALP-581]
7. 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]

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. Updated **show modem** CLI command to display historical information about the modem if it is in the process of updating firmware [DAL-1504]
7. Added new **Services → Ping responder** configuration settings for controlling what interfaces and firewall zones the DAL device responds to ICMP requests on [DAL-1565]
8. Enhance IPSec tunnels to wait for passing Surelink tests (if configured) before initiating outbound tunnels [DAL-3878/DAL-3774]

9. Add m2m.telus.iot Telus APN to fallback list [DAL-3911]
10. Add psmtneorm and edneopate010.dpa AT&T APNs to fallback list [DAL-4041/DAL-4045]
11. Add reseller and tracfone.vzwentp Tracfone APNs to the AT&T and Verizon fallback lists DAL-4098]
12. Add new 890103 and 890141 ICCID prefixes and 31030 PMND ID matchers to AT&T APN fallback list [DAL-3934/DAL-4041]
13. Add service.qcdm.secure option to enable/disable encrypted QXDM access to the cellular modem in the DAL device [DAL-3964]
14. Add missing modem firmware and SIM details to datapoints uploaded to Digi Remote Manager [DAL-4040]
15. Show uptime for connection to Digi Remote Manager on the Dashboard web UIpage in days/hours/minutes/seconds instead of just minutes [DAL-3691]
16. 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]
17. 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]
18. Updated the help text on the login page to provide a more generic image [DAL-3916]
19. Removed duplicate modem signal information from the **Modem → Status** page [DAL-3680]
20. 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]
21. Added a **defaultroute** option for matching policy-based routes to the device's active default route [DAL-4130]
22. Hide the **Monitoring → Device Health** configuration options if the device is not enabled for Digi Remote Manager central mangement [DAL-3825]
23. Update header types for the cellular modem name and network type on the Dashboard page
24. Create system log when Surelink DNS tests are skipped because the interface doesn't have any DNS servers [DAL-4224]
25. 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]

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. 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]
13. 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]
14. 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]
15. 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]

VERSION 20.8.22.32 (August 28, 2020)

This is a ***mandatory*** release

AnywhereUSB2-20.8.22.32.bin

SHA256: cfafbefc02e6e81f1b112a278a411fbd275a95af1a38852026bf9840b31b61ee

MD5: 31aaa3f715136cada4fda5a149b9f45b

AnywhereUSB8-20.8.22.32.bin

SHA256: 0fbab85974ffa70fe178c081122a14d7e0649cf34ae9191fd241e226a9cf711a

MD5: 68befc0e9d4de7a1ab6e7dbf120a16fe

AnywhereUSB24-20.8.22.32.bin

SHA256: a2a29213c7b32731214ca86e417ae64b9ea369a11f98d8439071017e3e7005f0

MD5: 36d204c06955bfe53e63912a50ca79a0

ANYWHEREUSB-specific CHANGES

1. ***AnywhereUSB 24 Plus only:*** 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. Added keep-alive interval and keep-alive timeout configuration options along with an option to set custom configuration options to the **Services → AnywhereUSB Manager** settings [DAL-3400 & DALP-442]
3. Fixed issue preventing switching SIM slots on AnywhereUSB Plus devices with a CORE modem [DAL-3571]

FEATURES

1. 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
2. DMNR Verizon Private Network support with new settings under **VPN → NEMO** [DALP-457]
3. 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
4. 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 **Central management** configuration options for any DAL product to sync with aView, ARMT, or AVWOB [DALP-626]
4. 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]
5. 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]
6. Added new **Monitoring→Device Health→Data point tuning** configuration options to fine tune what datapoints are uploaded as health metrics to Digi Remote Manager
7. 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]
8. Reduced data usage by 80% (based on default settings) for reporting health metrics to Digi Remote Manager [DAL-3394]
9. Fade **Configuration saved** pop-up window 5 seconds after clicking the **Apply** button [DAL-3451]

10. 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]
11. Add options in CLI to show and manually stop any custom scripts or applications [DALP-533]
12. 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]
13. Add **system duplicate-firmware** CLI command to copy active firmware to the secondary firmware partition [DALP-565]
14. Move **update firmware** CLI command to be under **system** [DAL-3092]
15. Add **show vrrp** CLI command to display the status of any configured VRRP instances [DAL-2953]
16. Use a random unprivileged port for performing ntp time syncs if standard port 123 fails [DAL-3650]
17. 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]
18. Update to ModemManager 2020-05-19 [DAL-3254]
    1. libqmi: updated to 1.25.4+
    2. ibmbim: updated to 1.20.4+
    3. libgudev: updated to version 233
    4. Improved support for Quectel EC25/EG25 modules

BUG FIXES

1. Fixed issue preventing 1002-CMG4 modem from connecting with Verizon private APN SIMs [DAL-3276]
2. 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]
3. Fixed bug where IPsec tunnels with multiple policies would only properly route traffic for the last policy configured [DAL-3448]
4. Fixed missing CPU usage stats in **show system** CLI output [DAL-2540]
5. 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]
6. fix issue preventing network interfaces from initializing if the interface name was longer than 7 characters [DAL-2327]
7. Fixed issue preventing WAN passthrough mode if WAN was configured with a static IP [DAL-3097]
8. Fixed errors displayed in CLI when configuring a USB serial port in remote access mode [DAL-3207]
    1. **Note:** USB ports configured in application mode are not available to or manageable via the AnywhereUSB protocol or features of this product
9. Fixed issue preventing users from configuring an IP address as a remote syslog server [DAL-3433]
10. Handle incorrect value occasionally returned by by Telit LM940/LM960 module when querying to see which SIM slot is in use [DAL-3481]
11. Fixed issue preventing cellular modem connectivity if a custom gateway/subnet was configured but the modem wasn't in passthrough mode [DAL-3585]
12. 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) [DAL-3393]

VERSION 20.5.38.58 (July 20, 2020)

This is a **mandatory** release

AnywhereUSB2-20.5.38.58.bin

SHA256: 1a20d612acc4c0edc3d412ed5daefa960692018fe95a064344264e122e00fcde

MD5: 2a899809b55ddcd2aaacdb4c44014aa1

AnywhereUSB8-20.5.38.58.bin

SHA256: 1a52c271a3a4a966e390ec22325801ff19a9142a22fa3fbeb79204a5e72da959

MD5: c7fd0f53b2ab5dddba05d1de5ee3cc73

AnywhereUSB24-20.5.38.58.bin

SHA256: 25206acfb35e210f19c974d13b4992a6963bbad9de3c420f90155ea1b27be085

MD5: f9f5a6bab651ce18f9e034b2005ade32

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]
    1. ***Note:*** USB ports configured in application mode are not available to or manageable via the AnywhereUSB protocol or features of this product

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. Added Python HID module to allow the DAL device to control PSUs via Python programs [DAL-2092]
5. Allow network analyzer to be configured to monitor any network interface instead of just wired Ethernet ports [DAL-2146]
6. Added option to **ping** CLI command to ping a broadcast address [DAL-2571]
7. Added new health metric to report the interface used by the DAL device for its configured IPsec tunnels [DAL-2710]
8. Added new health metric to report the LTE SNR value of the modem(s) on the DAL device [DAL-2904]
9. Limit metrics upload to no more than 2 per minute if backlogged [DAL-2870]
10. 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]

11. Report device SKU in RCI response to Digi Remote Manager [DAL-2940]
12. Add wbdata APN to fallback list [DAL-3182]
13. Improved recovery of Telit modem firmware updates should the update get interrupted [DAL-2984]
14. Fixed spelling of **System utilization** chart on Intelliflow page in the local web UI [DAL-2260]
15. 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]
16. Commonize the format and naming of rx/tx health metrics reported to Digi Remote Manager [DAL-2896]
17. Add IPv6 options to **traceroute** CLI command [DAL-2618]
18. Add count of bytes transmitted and received to the output of the **show network interface X** CLI command [DAL-2980]
19. 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]
20. 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]
21. Display the secondary/alternate firmware image version as the **Alt. Firmware Version** in the output of the **show system** CLI command [DAL-3057]
22. Retain modem firmware files in the event that the firmware upgrade was interrupted [DAL-2856]
23. Renamed OpenVPN server **device type** configuration options to clarify which options are OpenVPN managed versus device-only [DAL-2857]
24. 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]
25. 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]
26. Add support for AES_GCM family of IPsec ciphers [DAL-2715]
27. 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. Fix VRRP crashes by upgrading keepalived to version 20.0.20 (bug affects firmware versions 20.2.x) [DAL-3181]
2. Prevent IPsec tunnel from being setup if its local network/interface is down (bug affects firmware versions 20.2.x and older) [DAL-2336]
3. 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]
4. Update analyzer to continue running even if the users SSH session ends (bug affects firmware versions 20.2.x and older) [DAL-2154]
5. 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]

6. 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]
7. Fixed issue preventing backup IPsec tunnel from being established when primary/preferred tunnel was down (bug affects firmware versions 20.2.x) [DAL-3024]
8. 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]
9. Fixed failing SureLink IPv6 ping tests (bug affects firmware versions 19.11.x through 20.2.x) [DAL-2488]
10. Fixed issue with applying policy-based routes to incoming packets from the Internet (bug affects firmware versions 20.2.x and older) [DAL-2589]
11. Fixed bug preventing passthrough mode from functioning if multicast was also enabled (bug affects firmware versions 20.2.x and older) [DAL-2709]
12. 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]
13. Fixed error displayed in **show modem** CLI output when modem was not connected (bug affects firmware versions 20.2.x and older) [DAL-2959]
14. 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]
15. Fix non-working custom DHCP options (bug affects firmware versions 20.2.x) [DAL-3071]
16. 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]
17. 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]
18. Removed unsupported LED options listed for LR54 units in their digidevice.led Python module options (bug affects firmware versions 20.2.x) [DAL-3250]
19. 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)
20. 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]
21. Prevent interruptions to QCDM/QXDM port on Sierra modems caused by ModemManager interaction [DAL-3469]
22. Fixed bug preventing dual-APN connectivity with AT&T SIMs and Sierra modems [DAL-3586]
23. Fixed bug in USB drivers/setup caused by multiple ***set configuration*** operations run by the Linux kernel [AWG3-2302]

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]
15. 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]
16. Add failed login attempts to event log sent to remote syslog servers, if enabled [DAL-3492]

VERSION 20.2.162.162 (March 17, 2020)

This is a **mandatory** release

AnywhereUSB2-20.2.162.162.bin

SHA256: bf4a063872d6bf6cbf1f7ad6aa22df1308553ea297e0b30a3756669af3108cfe

MD5: 773a6f0248bdd887b4d8fde5f2d704a5

AnywhereUSB8-20.2.162.162.bin

SHA256: 50e1a77ffa74cc0663b1d68330aad8d6963d6c83da516263387103208b1b03f5

MD5: be69d10de50907bc32e05f94023f8eb8

AnywhereUSB24-20.2.162.162.bin

SHA256: fe8b91efbfa5d40d44c3d66b7ec8a3ab8953e7d38e26449effcaa636dcf6e347

MD5: 7e6f85b48f8182233e0c39b1e5f8af08

ENHANCEMENTS

1. Add MAC address is support report filename [DAL-2863]
2. Use ***ims*** instead of ***vzwims*** APN on Verizon SIMs for proper IMS registration [DAL-2883]
3. Add USB packet capture tools in CLI under the ***system usbtrace*** command [DAL-2638]

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)

AnywhereUSB2-20.2.162.90.bin

SHA256: e6f6a76858bfca0af08821c4f68557888d63fe778a8900151bc2340dcbf3fd4b

MD5: 039158e0e2a57a90b7349104b3aa625c

NEW FEATURES

1. Telit LM960 LTE CAT18 modem support [DALP-487]
2. Quectel EC25-AF LTE CAT4 modem support [DAL-1817]
3. Digi Remote Manager is set as the default portal for all DAL products [DALP-393]
    1. Central management via Digi Remote Manager will not be automatically enabled if you upgrade a device running 19.11.x or older 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 device will sync with Digi Remote Manager by default.
4. Added SureLink™ default connectivity tests on all WAN interfaces [DALP-402]
    1. SureLink tests (previously referred to as ***Active Recovery***) will not be enabled by default if you upgrade a device from 19.11.x or older DAL firmware to 20.2.x or newer firmware, but can be enabled if desired. However, if the device running 20.2.x or newer firmware gets reset (e.g. if someone presses the Erase button on the device, or erases its config through the web UI or Admin CLI), the default SureLink tests **will** *be enabled* as part of the default settings of the device.
5. 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]
    1. Includes new configuration options:
    2. **Allow shell** - NOTE if this options is disabled and subsequently re-enabled, the DAL device will **reset to default settings**
        1. **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*** commands 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.
        2. Under each user group under **Authentication → Groups** in the configuration settings:
            1. **Admin access**
            2. **Access level**
            3. **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. Prevent AnywhereUSB 8/24 Plus devices from downgrading to 19.11.x or older firmware
19. Add USB snooping/logging/debug control
20. Increase default max system log size from 1,000 lines to 3,000
21. Renamed **Signal Strength** references to **Signal Quality** [DAL-2707]
22. On the Network Status page of the web UI, add **Interface is up** message in SureLink status details
23. Add **service.qcdm.modem.device** and **service.qcdm.modem.interface_number** config options for specifying QCDM/QXDM port for a modem [DAL-2497]

SECURITY FIXES

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

BUG FIXES

1. Fixed bug where SureLink™ DNS tests took longer than the configured timeout to complete [DAL-2702]
2. Fixed SSL validation bug preventing modem OTA updates [DAL-2547]
3. Fixed bug where newly-created network Bridges would not be listed as options under the Device drop-down for network interfaces [DAL-2575]

4. 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]
5. Fixed bug where a device configured with multiple SSH keys would only honor the last SSH key in the list [DAL-2506]
6. Display the active cellular band for Quectel modems [DAL-2298]
7. Fixed bug where the web UI would display bytes transmitted/received for network interfaces as ***N/A*** [DAL-2295]
8. Fixed bug where the web UI wouldn't show IP information for client devices connected to an OpenVPN server running on the DAL device [DAL-2251]
9. Fix formatting output of ***show config*** CLI command when the configuration settings contained an array [DAL-2594]
10. Fix bug when adding a new element to an array in the ***config*** mode of the CLI [DAL-2594]
11. Fix bug where CLI ping and traceroute commands would ignore any interface specified in the command [DAL-2605]
12. Fix bug where SureLink™ default tests would continue to pass if cellular modem lost its active data connection [DAL-2609]
13. Fix a bug handling certificate files with spaces
14. Fixed padding issue with downloading SCEP CA certificates [DAL-2212]
15. Fixed rare issue with passthrough ancillary DNS not resolving if ***ancillary DNS redirect*** issue was disabled
16. Fixed issue with active serial logins when a serial-related configuration change was applied to the DAL device [DAL-2696]
17. Remove accns certs
18. Improve sorting order in AnywhereUSB Manager
19. Remove custom serial web page from AnywhereUSB Products
20. Fix bug preventing AnywhereUSB Plus devices from connecting through Gigabit Ethernet switches
21. Fix non-working ***Find Me*** feature in web UI
22. *AWUSB 8/24 Plus:* Fixed timezone offset when saving time to onboard RTC
23. *AWUSB 8/24 Plus:* Fix bug where devices with an internal realtime clock would not adjust their local time to the configured timezone
24. *AWUSB 8/24 Plus:* Fix ECDHC bus routing
25. Fixed output of **show modem** CLI command when cellular modem re-initializes
26. Fix potential initialization issues after updating firmware [DAL-2762]

VERSION 19.11.72.85 (January 20, 2019)

Initial Release with new User Interface

82004379_19.11.72.85_AW02_EOS_B.bin

SHA256: d6bef8ec97d55d13b9481b50fe1d2c92516b907eb127241bf1a9b8ce7d229109

MD5: f8c8178c5903da4b1eb9553708972f39

882004378_19.11.72.85_AW08_EOS_b.bin

SHA256: 4cfc5c331352bf0901dcc573e0a944457356c7b10e0f3c1137bfa6eb757e43ae

MD5: 6f8c7e2b3987fc4c4f62dae2a77572b9

82004377_19.11.72.85_AW24_EOS_B.bin

SHA256: 624828734761f1f537ee56092aa012fe02d5f09053627203c0a6e0cc6e533b54

MD5: 0c6949aff8b1c5107cf01a3dc8a91af6

New Features

- Cellular support is now available via the Digi Core Module
- VPN
  - IPsec with certificate and pre-shared key authentication
  - HW encryption for IPsec
  - OpenVPN
  - GRE
- Digi Remote Manager
  - Remote Management
  - Device Health Metrics
- IPv4/IPv6
- Routing
  - Static Routes
  - Policy based Routing
  - Routing services (BGP, OSPF, RIP, IS-IS)
  - Multicast
- Port Forwarding
- Packet Filtering
- Packet Analyzer