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 20.2.162.162

INTRODUCTION

This is a production 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

- GRE and passthrough interfaces do not work when interface name is longer than 7 characters [DAL-2327]
- Enabling passthrough and multicast causes the firewall to fail [DAL-2709]

UPDATE CONSIDERATIONS

Initial DAL release of the AnywhereUSB Plus family of products.

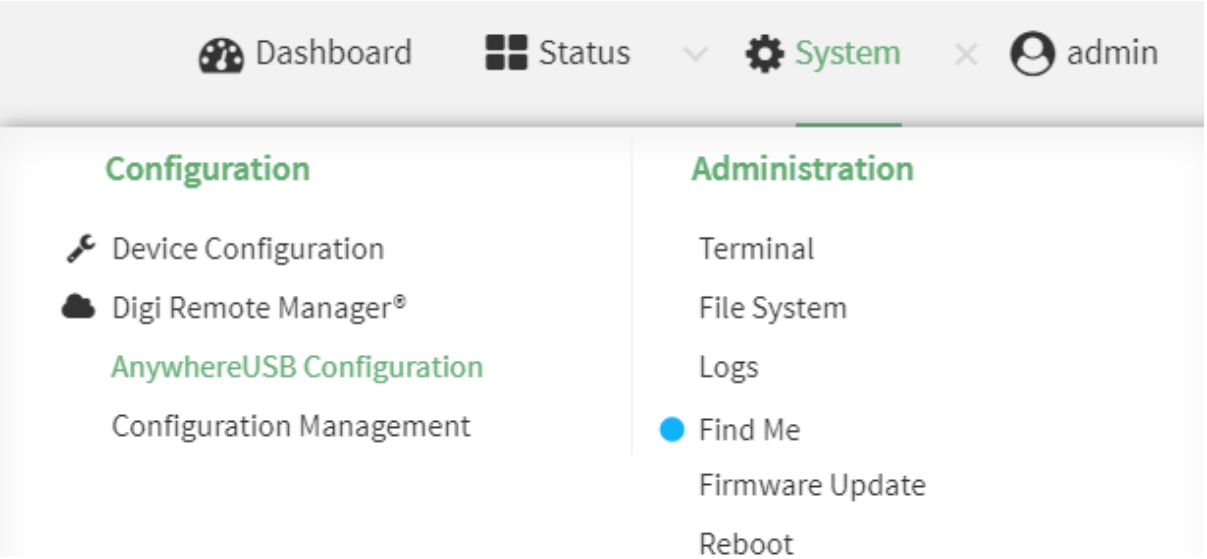
Starting with this version of firmware of AnywhereUSB Plus (release 19.11), Digi has standardized on a single user interface for all new products. There are differences in the location of configuration features, however units updated from the previous firmware to this version will have their configuration 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 3.0.0.5x to the new 20.2 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.

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 20.2.162.162 (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. Add firstnet-broadband APN for AT&T FirstNet SIMs [DAL-2876]
3. Use ***ims*** instead of ***vzwims*** APN on Verizon SIMs for proper IMS registration [DAL-2883]
4. 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. Update wording of help text for WiFi Background Scanning config settings to better reflect their usage [DAL-6673]
4. Added additional Telit-specific AT commands to mmcli-dump of support report
5. Improved Role-based access on local web UI, SSH, and remote access [DALP-415]
    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**

6. New default break sequence ***~b*** for serial connections [DALP-253]
7. Report MCC/MNC/CID/LAC values in health metrics to Digi Remote Manager [DAL-2502]
8. Add digicpn.gw12.vzwentp Verizon APN to fallback list [DAL-2283]
9. Change default OpenVPN Certificate Issuer details from Accelerated to Digi [DAL-2449]
10. Change default SSL certification from Accelerated to Digi [DAL-1336]
11. Dual-APN support on Sierra EM7511 modem [DAL-2311]
12. Include AT#RESETINFO and Quectel-specific AT commands in support report [DAL-2394]
13. Rename ***Configuration Management*** page under the System section of the web UI to ***Configuration Maintenance*** [DAL-2549]
14. Added link under ***System*** drop-down in web UI to download the support report
15. Update the ***Digi Remote Manager*** link under the ***System*** drop-down in the web UI to open in a new tab [DAL-2294]
16. Update the ***Authentication → Idle*** timeout setting to have a default value of 10-minutes (previously the default was blank) [DAL-2292]
17. Send up to 4 IPsec tunnels' details as health metrics reported to Digi RM [DAL-1476]
18. Change the default behavior of the ***SIM failover alternative*** settings from ***None*** to ***Reset modem*** [DAL-2687]
19. Prevent AnywhereUSB 8/24 Plus devices from downgrading to 19.11.x or older firmware
20. Add USB snooping/logging/debug control
21. Increase default max system log size from 1,000 lines to 3,000
22. Renamed **Signal Strength** references to **Signal Quality** [DAL-2707]
23. On the Network Status page of the web UI, add **Interface is up** message in SureLink status details
24. 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 WiFi hotspot intermittently worked [DAL-2547]
4. Fixed bug where newly-created network Bridges would not be listed as options under the Device drop-down for network interfaces [DAL-2575]
5. Fixed bug where the primary/active interface was not reported correctly to Digi aView when the DAL device was configured for load-balancing between two WAN interfaces [DAL-2568]
6. Fixed bug where a device configured with multiple SSH keys would only honor the last SSH key in the list [DAL-2506]
7. Display the active cellular band for Quectel modems [DAL-2298]
8. Fixed bug where the web UI would display bytes transmitted/received for network interfaces as ***N/A*** [DAL-2295]
9. Fixed bug where the web UI wouldn't show IP information for client devices connected to an OpenVPN server running on the DAL device [DAL-2251]
10. Fix formatting output of ***show config*** CLI command when the configuration settings contained an array [DAL-2594]
11. Fix bug when adding a new element to an array in the ***config*** mode of the CLI [DAL-2594]
12. Fix bug where CLI ping and traceroute commands would ignore any interface specified in the command [DAL-2605]
13. Fix bug where SureLink™ default tests would continue to pass if cellular modem lost its active data connection [DAL-2609]

14. Fix a bug handling certificate files with spaces
15. Fixed padding issue with downloading SCEP CA certificates [DAL-2212]
16. Fixed rare issue with passthrough ancillary DNS not resolving if ***ancillary DNS redirect*** issue was disabled
17. Fixed issue with active serial logins when a serial-related configuration change was applied to the DAL device [DAL-2696]
18. Remove accns certs
19. Improve sorting order in AnywhereUSB Manager
20. Remove custom serial web page from AnywhereUSB Products
21. Fix bug preventing AnywhereUSB Plus devices from connecting through Gigabit Ethernet switches
22. Fix non-working ***Find Me*** feature in web UI
23. *AWUSB 8/24 Plus:* Fixed timezone offset when saving time to onboard RTC
24. *AWUSB 8/24 Plus:* Fix bug where devices with an internal realtime clock would not adjust their local time to the configured timezone
25. *AWUSB 8/24 Plus:* Fix ECDHC bus routing
26. Fixed output of **show modem** CLI command when cellular modem re-initializes
27. 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