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 22.5.50.62

INTRODUCTION

This is a major 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

- 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]

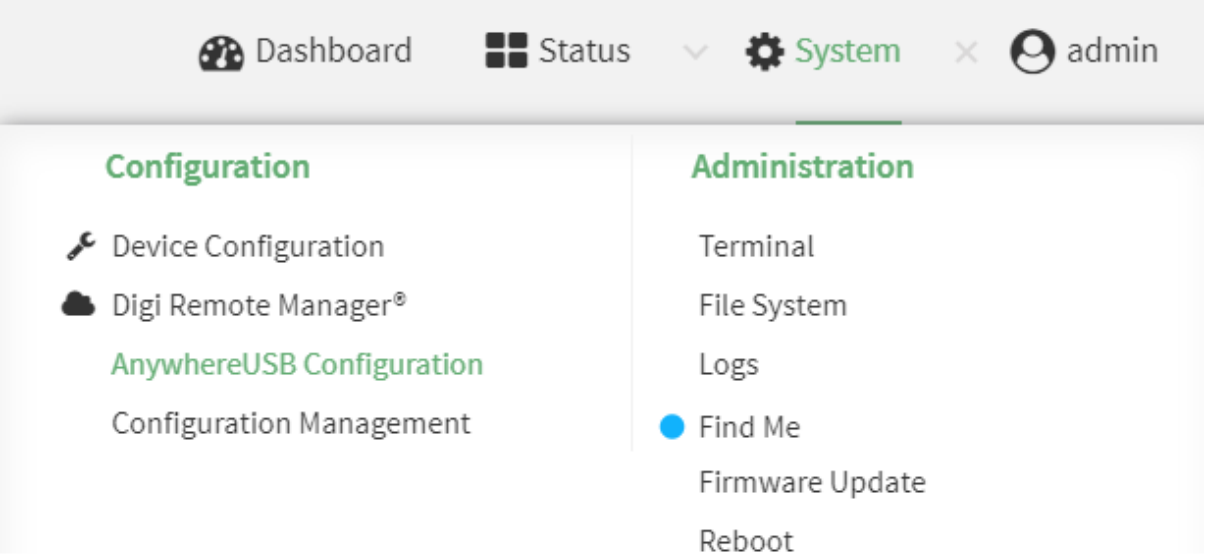
UPDATE CONSIDERATIONS

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

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

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

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

VERSION 22.5.50.62 (June 14, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
AnywhereUSB2i-22.5.50.62.bin	7f17cc9aec545bca7dd2f6298cb831b9226065d06e87b0ba9df4f32b27b19b812548322f8abc1315b36a268dba45ac37595f281399c6899fc66d8f9f607d2ab8	98894bba9ea24cabeed0712ffd2b2c05
AnywhereUSB8-22.5.50.62.bin	9564b3af45b20474bc5b8e8fced84d8c868e5cb37a90ed13a16392828abd5b67c9bd65af5903b69fd389202290f1b7e81f874f21d552494a04e1f2ff9f26c2c2	e37ae688cbde1a80cf5f1c3222e13b47
AnywhereUSB8W-22.5.50.62.bin	26f2f53c196e8017f5390706b550f17e1ef535d905733fd356ebcac37d2198e15d19eb9cd7fa8ff5af6db4714f46263f34f77c3fad2fa687bf2149232926308f	ce9d5a541635ad7648dd955c09863a90
AnywhereUSB24-22.5.50.62.bin	7421ba8886fad2b7d4932b16add6764fd0722c1e9c408c61cce52f952900a11710f378db8803959a9691be5a95a585da77003af00b8e14d8cbb346feb0b7cd10	31decd280d73f91782409a7bee68eb8d
AnywhereUSB24W-22.5.50.62.bin	109c74574978e343d241c496cd0c35189e4bb5e50c4041ba8d673d6ae512c8041d4f58e0af46038589fa2a2e868b1a2cb8ebffe5a56554389bdc1c38e89e8010	1cc0a42ff1e60a2b925a9214eca68720

FEATURES

1. New ***Network → SCEP Client*** settings and underlying functionality to support connecting to additional SCEP servers, including Fortinet FortiAuthenticator, DigiCert, EJBCA, and Windows server [DALP-1007, DALP-1022]
2. New *show scep* Admin CLI command for showing the sync status, expiration dates, and additional details of any configured SCEP clients [DAL-6069]
3. Support for enabling add-on features from Digi Remote Manager [DALP-673]

ENHANCEMENTS

1. Remove time.accns.com from default list of NTP servers unless ***Central management → Service*** is set to ***aView*** at the time of updating firmware from version 22.2.9.85 or older [DAL-5543]
2. Added new ***system.log.persistent_path*** configuration setting to specify where system logs are stored locally, which could be on the device or to an external storage (e.g. USB flash drive, SD card, etc) [DALP-946]
3. New ***Services → Location → Destination servers → Behavior when fix is invalid setting*** to

control the NMEA message content sent when there is no valid fix from any of the configured location sources [DAL-5984]

4. Improved the message shown on the ***System → Configuration maintenance*** page of the web UI if an error is encountered when restoring from a backup config file [DAL-6141]
5. Include the hostname of the device in the client .ovpn file listed on the ***Status → OpenVPN → Servers*** page in the web UI [DAL-6157]
6. Filter out non-Internet type APNs from our APN fallback list [DAL-6227]
7. Automatically power cycle the cellular modem in the event that a *modem reset* Surelink action fails [DAL-6268]
8. Enable Surelink *reset_modem* action by default on cellular interfaces and set fail count to 3 [DAL-6275]
9. Add cellular APN and cellular connection duration as datapoints sent to DigiRM [DAL-5902]
10. Ensure modem is in enabled state before attempting to connect [DAL-6163]
11. Omit non-production modem firmware from the OTA query results in the ***Status → Modems*** page of the web UI [DAL-6301]

BUG FIXES

The below bugs are all present on firmware versions 22.2.9.85 and older unless otherwise specified

1. Fixed issue preventing Telit LE910 family of modems from registering after changing APNs without a reboot [DAL-5971, DAL-6016, DAL-5203]
2. Fixed issue preventing connectivity with fast.t-mobile.com T-Mobile SIMs when used with a Quectel modem. Use PDP context 1 for connections on Quectel modems with T-Mobile SIMs [DAL-6401, DAL-5930]
3. Fixed issue where modem-based Location source would sometimes not report properly due to an initialization timing error with the modem [DAL-6163]
4. Fixed issue where an IPsec tunnel fails to re-establish the tunnel if SAs are deleted after phase 1 re-authentication [DAL-4959]
5. Fixed issue where the connection to Digi Remote Manager would delay up to 15 minutes before refreshing to use the active main Internet connection in the event of a network failover or failback [DAL-6164]
6. Fixed issue where ***OpenVPN → Advanced options → OpenVPN parameters*** text box was limited to 64 characters when synced with Digi Remote Manager. The new limit is now 64,000 characters [DAL-6002]
7. Fixed issue preventing OpenVPN server from authenticating clients with an external LDAP/TACACS+/RADIUS server [DAL-6159]
8. Fixed broken ***Go to Digi Remote Manager*** link in the local web UI [DAL-6088]
9. Fixed issue preventing LDAP external authentication for SSH and Telnet session [DAL-6098]
10. Fixed typo in description of *container delete* CLI command [DAL-5956]
11. Fixed output of *show containers* Admin CLI command to list all containers on the filesystem, not just those linked to configuration settings [DAL-5958]
12. Fixed issue where the *show location* output in the Admin CLI could include an incorrect timestamp if the configured location server(s) had a non-UTC timezone set
13. Fixed issue preventing ***Network → Interfaces → MAC address allowlist*** from implicitly denying access to devices not in the allowlist [DAL-6001]
14. Fixed ***Invalid lookup path for : network.interface*** error when running *cfg.get("network.interface")* in the digidevice.config python module [DAL-6005]
15. Fixed issue where TAIP messages would have the incorrect timestamp if the timezones between the device and server were different [DAL-6335]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a CVSS score of ***9.8 Critical***

1. Update to OpenSSL 1.1.1o (CVE-2022-0778, CVE-2022-1292) [DAL-6035]
2. Update to linux kernel 5.17 [DAL-6081]
3. Patch for "dirty pipe" vulnerability in Linux kernel (CVE-2022-0847) [DAL-5981]
4. Update gcc to version 11.2 and binutils to version 2.37 (CVE-2019-15847, CWE-331, CVE-2018-12886, CWE-209, CVE-2002-2439, CWE-190) [DAL-5444]
5. Update openvpn to version 2.5.6 (CVE 2022-054) [DAL-6229]

VERSION 22.2.9.85 (March 3, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
AnywhereUSB2i-22.2.9.85.bin	ca0b5b69ccda1dc0a21c01fa24f78724177ea5a98bfe3aefb3bc3681d5d3b48f554d97fd7c6169b4f3c7c39ca3589d03e9662fe136a58c3ed06046fe70688ef3	c20ae091cc48944d5dbf3fec8d220bc1
AnywhereUSB8-22.2.9.85.bin	c1fd9243246d9ce4aaef0855788f80cc1a2c276eaec4f3c7df851c9e205f7dc88f2e6a8d8d1a7084856eb82d8025691906bf2dd13d9a0745302cf89a7603c9a4	75c5f3cddac66e92446605fee467bc61
AnywhereUSB8W-22.2.9.85.bin	62edf3e91ea9ef0f102b53abbdc2d54a13656d732fff4d093d11aaf4108fffe3190e1e13e133c003beccb57a4fa6e385663693de853d88f3a8c28a530dc38330	b1a39000f8936f2b7eaf032b16c73dfd
AnywhereUSB24-22.2.9.85.bin	fe8fe98f9bb683f5a67b36b77c8b55d7ee29e54fa172396ef414ff36e83d7992688323c5d6d7f887e7e2a0822d829a2bf7e4a7fd85aeb47a21ee4fb008155875	a5126cbb230eb044aa9377612142dbd1
AnywhereUSB24W-22.2.9.85.bin	d28cde597f61e08d1290b02ac2a88e19d1c044bbcbe7ee1c4d1173cf45b73b37988912d1d8e871a3076cc4b6f90ee46fc7251df8438a1fdcc9800348fb64d736	6935c2095a6f807840f3be18bcb2bbb3

FEATURES

1. Added new option under ***System → Time → NTP → Use GNSS module*** to enable the device to use its internal GNSS module as a date/time sync source [DAL-5760]

ENHANCEMENTS

1. Update default Digi Remote Manager URL to edp12.devicecloud.com [DALP-972]
    1. In firmware versions 22.2.9.85 and newer, the default central management server changes from ***my.devicecloud.com*** to ***edp12.devicecloud.com***. This change enables more secure connection negotiation and enables support for device certificates. If your device connections are managed by a firewall, or your devices do not have direct access to public DNS servers, you may be required to make firewall changes to open connectivity to edp12.devicecloud.com, or to enable DNS.See https://www.digi.com/support/knowledge-base/firewall-concerns-for-outbound-edp-connections-to for more information about device connectivity to Digi Remote manager.
2. Increased web UI upload limit to 512MB [DAL-5694]
3. Added new ***Surelink Switch SIM*** and ***Switch SIM fail count*** options to specify how many times the Surelink test must run and fail on a cellular modem before the device switches to the alternate SIM slot [DAL-5717]
4. Support for standard SCEP servers [DALP-821]

1. Previously the SCEP client only supported syncing with Fortigate SCEP servers. Two new settings were added under the ***Network → SCEP Client*** options to control the CA identity and HTTP path to the CA

5. Renamed ***VPN → IPsec → Tunnels → Policies → Local network*** setting to ***Local traffic selector*** along with a new ***Dynamic*** option which allows users to configure a local network by protocol and/or port instead of a network address range [DAL-5645]
6. Added new ***VPN → IPsec → Advanced → Debug level*** option to specify the logging verbosity of IPsec messages in the device system logs (default is debug logging is disabled) [DAL-5720]
7. *1002-CM06/1003-CM07:* Utilize T-Mobile carrier firmware if available for the cellular modem when using Sprint Curiosity SIMs [DAL-5466]
8. New cat Admin CLI command for displaying file contents [DAL-5853]
9. Update /etc/config/scep_client/ directory to be read/write by admin users
10. Add ability for policy-based routes to override routing of packets through VPN tunnels, useful in the case where you only want packets from a certain source network to go through the tunnel [DAL-5317]

BUG FIXES

The below bugs are all present on firmware versions 21.11.60.63 and older unless otherwise specified

1. Fixed HFSC class hierarchy setup for QoS policies to limit bandwidth used for shared links [DAL-5814]
2. Fixed issue preventing scheduled maintenance window from updating the maintenance_window datapoint in Digi Remote Manager if the maintenance window start time was between 00:00-00:59 [DAL-5765]
3. Fixed bug preventing MMS SMS messages from being received and parsed properly, preventing large out-of-band config changes from being received from central management portals [DAL-5538]
4. Fixed issue preventing transport-mode IPsec tunnels from initializing properly [DAL-5718]
5. Fixed issue where only the first policy would be setup on IKEv2 IPsec tunnels [DAL-5347]
6. Fixed issue preventing port forwarding firewall setups if the ***Destination port(s)*** setting was left blank [DAL-5860]
7. Fixed intermittent issue where the ***show dhcp-leases*** CLI output would sometimes not include all leases [DAL-5688]
8. Fixed system log errors when performing TACACS command authorization without having a TACACS server configured [DAL-5512]
9. Fixed interruption of active serial port connections when a user changes the serial port mode in the Digi device's configuration settings [DAL-5698]
10. Fixed issue where Surelink tests aren't reloaded if a user updates the network bridge or Wi-Fi configuration settings on the device [DAL-5406]
11. Prevent modbus setup issue by not allowing users to configure the device to use reserved address ranges [DAL-5905]
12. Fixed intermittent race condition in Surelink that could lead to a delay in setting up a WAN connection [DAL-5934]
13. Fixed issue with digidevice.sms python module processing empty SMS messages [DAL-5883]
14. Fixed issue preventing remote file system access to the /opt/ directory through Digi Remote Manager [DAL-5659]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a Critical CVSS score of ***10 Critical***

1. Update python to version 3.10 [DAL-5499]
2. Update openssh to version 8.8p1 (CVE-2021-28041, CVE-2020-14145) [DAL-5451]
    1. This deprecates support for RSA signatures using the SHA-1 hash algorithm by default, which may prevent old machines from SSH-ing to the Digi device. Please ensure your SSH tool (TeraTerm, PuTTY, etc) is up to date. If you need to re-enable SHA-1 hash support, you can do so by adding the following lines to the ***Service → SSH → Custom configuration → Configuration file*** text box in the Digi device's configuration settings:
        1. HostkeyAlgorithms +ssh-rsa
        2. PubkeyAcceptedAlgorithms +ssh-rsa
3. Update dnsmasq to version 2.86 (CVE-2021-3448) [DAL-5331]
    1. Fix problem with DNS retries in 2.83/2.84
    2. Fix a problem, introduced in 2.83, which could see DNS replies being sent via the wrong socket. On machines running both IPv4 and IPv6 this could result in sporadic messages of the form "failed to send packet: Network is unreachable" and the lost of the query
4. Update to Linux kernel version 5.15 [DAL-5546]
5. Add new ***Service → Web administration → Minimum TLS version*** configuration setting to allow users to specify which TLS versions are allowed in the local web UI (default minimum is TLS 1.2) [DAL-5408]
6. Update busybox to version 1.34.0 [DAL-5631]
    1. CVE-2021-4237, CVE-2021-42374, CVE-2021-42375, CVE-2021-42376, CVE-2021-42377, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42383, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386
7. Update dbus to version 1.13.20 [DAL-5459]
    1. CVE-2020-12049, CVE-2019-12749
8. Update grub to version 2.06 [CVE-2021-3418] (DAL-5456]
9. Update bzip2 to version 1.0.8 (CVE-2019-12900, CVE-2011-4089, CVE-2010-0405) [DAL-5446]
10. Update procps to version 3.3.15 [DAL-5433]
    1. CVE-2018-1124, CVE-2018-1123, CVE-2018-1126, CVE-2018-1125
11. Hardened openssl build to include secure compilation flags
12. Update sqlite to version 3.37.2 [DAL-5669]

VERSION 21.11.60.63 (December 8, 2021)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
AnywhereUSB2i-21.11.60.63.bin	8942608687788cb21466f5680fdd4f62b24916a8f8a3bf2eeb9d826a6eb3dbae99be34f52350535597dd9caeb4df92997f3d2c4db5eee139a87521f5c9d819d6	f19bfdb94f71a9c5dfafbb62fe2fb379
AnywhereUSB8-21.11.60.63.bin	c2fdf5548ba24ddf0b2fa32ffeba5cd7d68ffe10675bc689937b84bbe5082a80a0f975b8e457836b77a5385fe8d66649539eb5bcc3b3d95f8fa81d4e2684a524	d78a8ea580cb1635a96c7e086483af77
AnywhereUSB8W-21.11.60.63.bin	edc4ea6c046d56a498516773f94dad719c482cfbec8110e1bdf233fc2972a4bcb2c8a8fe3bc2fa04b4c12f52314ce99f6df08be5506fc3c6a636298853f36f33	f8da19e940ac502b9e232ec65dc81675
AnywhereUSB24-21.11.60.63.bin	a6690828e353f527d817d21fcd9da33af4b3a53309d47632beff706a45688e5fc2783f0c66e20f22331eb7ce8da33cb3a1c52161d230ba1f0f7e80624f0aee7f	4adc750a2e30bdf7d802071e50198ee7

AnywhereUSB24W-21.11.60.63.bin	fa736f992747cad83efd5946f74061af74a6c8f20a0262697d10d498e7fc1cbd89d1286d8a540a1129c973ad23be37c3d9b52886976d55772dec6b10693e6eed	4995efbe6c44070c11422c3898af9835

FEATURES

1. New **System maintenance → Device firmware update** config option to allow the device to automatically update to new firmware when available (disabled by default) [DALP-630]
2. TACACS+ accounting and authorization for Admin CLI interactions [DALP-633]
    1. Includes two new configuration settings under the **Authentication → TACACS+** configuration settings for enabling TACACS command account and/or authorization
3. Add new *Authentication → Users → Username alias* option for providing an alternate username that can accommodate characters not typically allowed in a username [DALP-705]
4. PKI certificate-based authentication for WPA2/WPA3 Enterprise Wi-Fi client connections, including options for user-provided certificates or SCEP client integration for automatic certificate generation [DALP-828 & DALP-794]

ENHANCEMENTS

1. Improved Wi-Fi scanning tool on the **Status → Wi-Fi → Management** page in the web UI to automatically setup the underlying basic client-mode settings so the device can scan for nearby APs without requiring the user to first configure the client-mode settings [DALP-802]
2. New **show surelink** Admin CLI command for displaying details on the Surelink test(s) configured for a network interface or VPN tunnel [DALP-621]
3. Add new option under **Location → Destinations** for specifying the talker ID used in NMEA message strings [DAL-5038]
4. *1002-CMM1 CORE modems:* Use CID context 3 for any type of Verizon SIM when used with a ME910c1-WW modem [DAL-5428]
5. Include the mode indicator field in NMEA messages constructed when a GPS fix isn't obtained [DAL-5464]
6. Add support for auto-completing a parameter or AT command provided to the **xbee set|get|execute** Admin CLI commands [DAL-5196]
7. Change default IPsec IKE DH group to 14 for enhanced compatibility with industry standard settings [DAL-5344]
8. Disable serial history in remote access mode by default [DAL-5494]
9. Add new settings under cellular Surelink options to have the device reset the cellular modem if a specified number of Surelink tests fail [DAL-5441 & DAL-5485]
10. Add **datapro** APN to fallback list to be utilized with Airmob SIM cards [DAL-5548]
11. New **show containers** Admin CLI command for listing details about configured containers [DAL-5380]
12. Include SIM ICCID and phone number in the query_state response sent to Digi Remote Manager [DAL-5632]
13. Specify string encoding as UTF-8 in communication with DigiRM for compatibility with extended charactersets [DAL-5505]

BUG FIXES

The below bugs are all present on firmware versions 21.5.56.176 and older unless otherwise specified

1. Fixed issue preventing IPsec tunnels from being setup in Transport mode [DAL-5490]
2. *1002-CM04/1002-CME4 CORE modems:* Fixed issue where cellular modem firmware updates would not be applied to Telit LE910-family of modules unless the firmware file included a

carrier name in the filename [DAL-5616]

3. *1003-CM07 CORE modem:* Fixed issue preventing multi-carrier firmware updates on Sierra EM7411 modems [DAL-5473]
4. Fixed issue preventing **on boot** SIM preference schedule from taking effect (bug present on firmware versions 21.8.x and 21.5.x) [DAL-5547]
5. Fixed issue preventing internal firewall from functioning properly if a port forwarding rule was configured with the protocol type set to **other** (bug present on 21.8.x firmware) [DAL-5501]
6. Fixed issue preventing IPsec tunnels from being setup properly if the tunnel name was longer than 9 characters [DAL-5139]
7. Fixed formatting of cellular-related health metrics so they can be properly displayed under the *Settings → Status → Cellular* section in Digi Remote Manager [DALP-768]
8. Fixed error in system log when attempting to parse an empty config file [DAL-5402]
9. Fixed issue causing potential multi-minute delays in the *show modem name XX* Admin CLI command [DAL-5297]
10. Fixed issue where Surelink ping tests would utilize the same source IP address if coming from different network interfaces assigned to the same physical device/port [DAL-5478]
11. Fixed issue where Surelink **reboot** action would not be take if the Surelink **restart interface** action was also enabled [DAL-5485]
12. Fixed issue preventing the creation of config elements with dynamic array names via the local web API [DAL-5481]
13. Fixed issue preventing installation of sqlite3 python package via pip [DAL-5611]
14. Fixed issue preventing multiple config changes from being applied in a python script using the digidevice.config module [DAL-5192]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a Critical CVSS score of ***9.8 Critical***

1. Update to python version 3.6.15 [DAL-3190]
2. Update stunnel to version 5.60 [DAL-5291]
3. Update busybox to version 1.33.1 [DAL-5290]
4. Update to Linux kernel version 5.14 [DAL-5360]
5. Update OpenSSL to version 1.1.1l [DAL-5242]
6. Fixed issue where the TACACS shared secret was included in the system logs [DAL-5470]
7. Update libunbound to version 1.13.2 [DAL-5420]
8. Update libidn2 to version 2.3.2 [DAL-5439]
9. Update muslv to version 1.2.2 [DAL-5452]
10. Update rsync to version 3.2.3 [DAL-5431]
11. Update OpenVPN to version 2.5.4 [DAL-5435]

VERSION 21.8.24.129 (September 13, 2021)

This is a recommended releases

AnywhereUSB2i-21.8.24.129.bin

SHA512:
ba0c17ebcff3fe1e47ca9a344110d8de809fd436467e433057a2f5873165c899118c08c8d
e9f18736c3a00f77cf86322a889bde6c77396b88dce0a4958b63f5f

MD5: 6173cdce7ef322fd697b18c38953c8ac

AnywhereUSB8-21.8.24.129.bin

SHA512:
162cc7d7d4b4ce2f629481cef57156442fe0f79427624fb8a099e4baf037ba098d1a243adf2fca18b3e39eec3c1e08c98b1bebeceae37388963062b99c10d341

MD5: e32f0d23d45c5bc859f89ce5d8a1c0c7

AnywhereUSB24-21.8.24.129.bin

SHA512:
bdd3dec5e30a037a2c67100211ff7dbe2974b27656affb468235d2045ebe48ff055ecbc90f87f1bad49e9c2f57b3e1e3b74cebf6690dd39945293f0465a7b6cc

MD5: 88d602e4a8f0d4340095499336c51ab5

ANYWHEREUSB-specific CHANGES

1. Updated awusbd service to fix the following [DAL-5088]
    1. Enable automatic registration of unknown client IDs so they can be shown in the Hub status display
    2. Add device address to POWER cycle log msg
    3. Hub service hangs if SSL handshake does not complete
2. Python scripting support, including the digidevice python module [DALP-763]

FEATURES

1. LXC container support for running localized containers on the device [DALP-243]
    1. New ***System → Containers*** configuration settings for provisioning containers, providing virtual networking, and serial port access from the container
    2. ***lxc*** commands available in the shell console for managing/accessing/monitoring containers on the device
    3. Containers are based off the host DAL device's system. Packages installed to the container must be built for the CPU architecture designed
2. L2TPv3 static/unmanaged VPN tunneling [DAL-5137]
    1. VPN -> L2TPv3 ethernet configuration setting
    2. New Status -> VPN -> L2TPv3 Ethernet web UI page
3. 802.1x port-based network access control, configurable per network interface [DAL-5080]
4. New **Services → SSH → Custom configuration** settings for overriding or editing the SSH server options
5. New **Monitoring → Device event logs** options for sending local device event logs to Digi Remote Manager [DALP-808]
    1. Event logs are controlled under the **System → Log → Event categories** configuration settings
6. New ***VPN → IPsec → Tunnels → IKE → IKE fragmentation*** option to enable, disable, or force IPsec IKE fragmentation [DAL-4933]
7. New **MAC address allowlist/denylist** options to allow/deny packets based off of a range of source MAC addresses [DALP-799]
8. New **system time** CLI command for manually setting the local date and time [DALP-520]
9. New **monitoring metrics upload** CLI command for sending on-demand health metrics to Digi Remote Manager [DALP-727]
10. New **system script start** CLI command and **Status → Scripts** page in the web UI for manually starting custom scripts configured under the **System → Scheduled tasks → Custom scripts** settings with a **Run mode** of **manual** [DALP-741]
11. New **system find-me on|off** CLI command and **Status → Find Me** button in the web UI for flashing cellular-related LEDs to help locate the device onsite [DAL-5142]
12. New ***Network → Bridge → switchport*** bridge type configuration settings for enhanced VLAN

capabilities [DAL-5220]

1. trunked vs untrunked ports
2. virtual switch setups
3. VLAN layer 2 networking

ENHANCEMENTS

1. Added new **show l2tpeth** CLI command for viewing the status of any configured L2TPv3 tunnels [DAL-5220]
2. Update python pip to version 21.2.4 [DAL-5068]
3. Shortened fallback APN list by removing wildcard entries [DAL-5012]
4. 3G sunset support for EU carriers [DAL-5041]
5. Update messaging included in keepalive packets sent to Digi Remote Manager to prevent multi-second delays in keepalive responses [DALP-832]
6. Add **datapoint.upload_multiple** function to digidevice python module for uploading multiple datapoints to DigiRM at once [DALP-857]
7. Add **uptime** field to **show cloud** CLI output to indicate how long the device has been connected to Digi Remote Manager [DAL-1083]
8. Update **system support-report** CLI command to automatically store the support report in /var/log/ unless a path is specified [DAL-5027]
9. **system support-report** CLI command outputs helpful information for SCP-ing the file from the device to a remote destination [DAL-5027]
10. New **clear dhcp-lease** CLI command for removing all dynamic DHCP leases or certain DHCP leases based on MAC address or IP address [DAL-5127]
11. New **speedtest** CLI command for performing on-demand iPerf or nuttcp speedtests [DAL-5040]
12. Require local users to be assigned to a group [DAL-5060]
13. Add support for configuring multiple destination networks/interfaces for Multicast routes [DALP-853]
14. New **Network → Advanced → Sequential DHCP address allocation** configuration setting for controlling if DHCP addresses are assigned sequentially or randomly (disabled by default) [DAL-5136]
15. Persistent local date/time across reboots once a successful NTP sync occurs [DALP-806]
16. New ***System → Scheduled tasks → System maintenance → Maintnance window trigger*** configuration settings for controlling when/if a device tells Digi Remote Manager it is in a maintenance window and if updates should be pushed to the device [DAL-5010]
    Available maintenance window triggers are:
    1. Specified network interface is up
    2. Python API call
    3. Specific time window in the day
17. Read/write control to the /opt/ and /etc/config/analyzer/ directories through DigiRM and the local web UI [DAL-5117]
18. New options for setting up a custom default config file [DAL-4978]
    1. ***system backup*** CLI commands for generating a custom default config file based on the active config settings on the device
    2. ***System → File System*** page in the web UI for loading a configuration backup file as the custom default config
    3. ***Files → Persistent files*** folder accessible through Digi Remote Manager where users can upload a config backup, naming it custom-default-config.bin
19. Add option to clear a custom default config by performing a double erase sequence [DAL-

5017]

20. Updated CLI login helptext to include common tool-tips [DAL-5157]
21. Replace the cellular modem manufacturer name with the CORE modem model name in the CLI/webUI/metrics details [DAL-5171]
22. Ensure scheduled reboots with the **reboot_managed** command cause graceful shutdown of services on the device before rebooting [DAL-5150]

BUG FIXES

The below bugs are all present on firmware versions 21.5.56.106 and older unless otherwise specified

1. Fixed issue where Digi Remote Manager would remediate a DAL device every time it's scanned due to the local user passwords being hashed [DALP-834]
2. Fixed issue where the **system restore** CLI command could default the device if the config backup file was store in the /etc/config/ directory [DAL-5116]
3. Fixed the local web API to allow values with spaces [DAL-5039]
4. Fixed the local web API to allow array configuration settings [DAL-4895]
5. Fixed mdns service where it would occasionally crash [DAL-4663]
6. Fixed issue preventing **modem pin status** from returning valid results [DAL-5056]
7. Fixed bug with installing certain python modules using pip [DAL-5068]
8. Set default user-base directory to /etc/config/scripts/ so python pip can install module dependencies to a writeable location when pip install --user <module_name> is invoked [DAL-5068]
9. Prevent serial connection crashes when a incoming serial socket connection is sending so much data that the buffer fills up the system memory

SECURITY FIXES

1. Add STS header in HTTPS web UI [DAL-4991]
2. Update libcurl to version 7.77.0 (CVE-2021-22897, CVE-2021-22898, CVE-2021-22901)
3. Update to Linux kernel version 5.12

VERSION 21.5.56.106 (May 31, 2021)

This is a mandatory release

AnywhereUSB2i-21.5.56.106.bin

SHA512:
b1eb4ec2a2f20d78974bc93f3c412d8a045dcb652653eea59ee0c3a8112055e5a21b97569c65a4b3d8a9ddb289263178ece66abb2bf6b49bb998ba8d9962b365

MD5: f8ce2e9a8847d7f700aa4e4b4d00a8e1

AnywhereUSB8-21.5.56.106.bin

SHA512:
c196aa8fd575a95b4d59e9ebbc38dc14515c905decc5902184989aea4ee96941dba2fb10e02fbd0bbeb994c22ef16de32f384efb65d3b2606b9e32d1d8ded7ed

MD5: 3560581d5f4a0fbe436ab0a566f91069

AnywhereUSB24-21.5.56.106.bin

SHA512:
af24fbc4cfbc503fcb12af128655576869b82519489df2573b80908b98fbb2619caacccd6d043b2dac5b16e13c9e98b1a5d88acf49be99062a33e7301edcd2a9

MD5: 98b9a3a51a0bc55abf2ea9f07f019eb9

ANYWHEREUSB-specific CHANGES

1. Add CLI and web UI options for power cycling USB ports [DALP-792]
    1. **Power cycle not supported by 24-port with SKU less than 50001982-03**
    2. CLI command: **system anywhereusb powercycle port[n]**
    3. Web UI: **Cycle** button listed for each USB port on the **Status → AnywhereUSB** page
2. Fixed issue with Surelink behavior on AnywhereUSB Plus devices with multiple Internet connections (bug present on firmware versions 21.2.39.67 through 20.5.x) [DAL-4847]

FEATURES

1. Added options under **VPN → IPsec → tunnels → Remote** endpoint to add multiple endpoints and either round-robin between the endpoint or randomly select an endpoint to establish the tunnel to [DALP-160]
2. Added options under **VPN → IPsec → Advanced** to control IKE retransmit interval, IKE timeout, tunnel retry interval, and tunnel retry timeout [DALP-564]
3. New Surelink configuration options [DALP-787, DALP-274, & DALP-84]
    1. **Restart fail count** and **Reboot fail count** options to specify how many times the Surelink test must run and fail before a reboot/restart action is taken
    2. **Pass threshold** option to specify the number of times Surelink tests must pass before the interface is marked as working
    3. New **Test another interface's status** test type to pass/fail Surelink based on whether another network interface is up/down and has IP connectivity
4. SNMPv2c read-only support [DALP-809]
5. Enable SCEP client support for IPsec tunnel authentication [DALP-722]
6. Add **Scan** button on the Modem status page to initiate a network scan, list available carriers the SIM can connect on, and allow the user to select a particular PLMN/network to use [DAL-4338]
7. Add default **digi.device** local domain for simpler SSH/web access [DAL-4598]
    1. Requires using the Digi device as your DNS server for resolving digi.device to an IP address

ENHANCEMENTS

1. Add **System → Scheduled tasks → Reboot window** config option to add a random delay to the **Reboot time** if configured [DAL-4741]
2. Add read-only console access via Digi Remote Manager [DALP-336]
3. Add support for receiving additional remote commands from Digi Remote Manager:
    1. Perform a speed test and send the results to DigiRM [DALP-490]
    2. Perform automated cellular modem firmware update [DAL-4850]
4. Add option to retain the unique default password of the admin user when initially configuring the device [DALP-758]
5. Improved **Firewall → Port forwarding** options to support a range of ports, including 1:1 and many-to-one port mappings [DALP-560]
6. Added options to control packet filtering for the **Network → Analyzer** traffic analyzer [DALP-733]
7. Update voice settings on Telit and Quectel modems for continued connectivity after AT&T's 3G network sunset in February 2022 [DALP-760]
8. Add internet.gma.iot T-Mobile APN to fallback list [DAL-4906]
9. Support for Sierra cellular modem firmware with multiple CWE files in a single tarball [DAL-4860]
10. Include error messages along with error code if an issue is encountered when downloading device or cellular modem firmware [DAL-4854]
11. Added **Authentication → LDAP → Login attribute** configuration option to control the attribute ID used so it can match with the attribute set in an Active Directory server [DALP-120]
12. Update the titles of the columns in the **show dhcp-lease** CLI output to be more descriptive
13. Add **show dns** CLI command to display the active DNS servers and what interface they're associated to [DAL-3639]

14. Add **show ntp** CLI command to display the status of the NTP service and if it has synced with an external time server [DAL-4747]
15. Add **system firmware ota** commands to check, list, and update to new firmware from the Digi firmware server [DAL-4800]
16. Skip Auto-APN detection and use internet.telekom APN by default for Deutche-Telekom SIMs [DAL-4622]
17. Add LWM2M parameters to include AT&T Host IDs for devices with EM9191/LM940/LM960 modems [DAL-4823, DAL-4844, & DAL-4845]
18. Update from Quagga to FRRouting for BGP OSPF, RIPNG, and other routing services [DAL-4798]
19. Update python to version 3.6.13 [DAL-3190]
20. Return proper status code for custom scripts configured on the device [DAL-4670]
21. Rename MAC address filtering options to be called **Allowlist** and **Denylist** [DAL-4677]

BUG FIXES

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

1. Fixed issue when authenticating users if multiple TACACS servers were configured and the first server is unresponsive [DAL-4748]
2. Clear PDP cid 1 APN for Verizon SIMs using a vzwentp private APN with a ME910c1-WW modem [DAL-4525]
3. Fixed issue preventing devices with LM940 modems from automatically connecting with T-Mobile Hungary SIMs [DAL-4679]
4. Fixed issue where outbound SMS messages couldn't be sent using various carrier SIM cards (bug present on firmware versions 21.2.39.67 through 19.11.x) [DAL-4794]
5. Fixed issue where cellular connectivity wouldn't re-establish if a Quectel modem reset itself [DAL-4612]
6. Fixed issue where the device could stop participating in RIP routing if network interfaces are reset [DAL-4704]
7. Fixed issue where RIP, BGP, and other routing services would not setup properly if a user updated the configuration for the routing services on the device [DAL-4784]
8. Fixed issue preventing acceptance of default routes advertised via RIP [DAL-4799]
9. Fix issue preventing GRE interfaces from being specified within BGP and other routing services [DAL-4695]
10. Fixed issue preventing VPN tunnels from being specified within port forwarding rules [DAL-4524]
11. Fixed issue preventing configuration options from being applied en-masse from the CLI when using the output from the **show config cli_format** command [DAL-4713]
12. Fixed bug where a running network analyzer could be stopped in the CLI by issuing **Ctrl-C** [DAL-4652]
13. Fixed issue where GPS-based location health metrics weren't being sent to Digi Remote Manager (Bug present on firmware versions 21.2.x) [DAL-4310]
14. Fixed issue where the status of an OpenVPN client wasn't listed properly in the web UI [DAL-4357]
15. Fixed issue preventing access to multiple remote networks through an IPsec tunnel with the same policy [DAL-4816]
16. Fixed issue preventing multi-VRRP setups from setting up with the proper priority [DAL-4824]
17. Fixed issue where devices could try recovering Sierra modems in the middle of a modem firmware update [DAL-3929]

18. Fixed issue where wired Internet connectivity is interrupted during cellular modem firmware updates [DAL-4647]
19. Removed broken Babel routing service (bug present on firmware versions 21.2.39.67 through 19.11.x) [DAL-4769]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a Critical CVSS score of ***9.8 Critical***

1. Reduce password complexity to 8-character minimum [DAL-4506]
2. Update to OpenSSL 1.1.1k [DAL-4755]
    1. CVE-2021-3450 CVE-2021-3449
3. Update libcurl to version 7.76.0 [DAL-4774]
    1. CVE-2021-22876
       CVE-2021-22890
4. Update netsnmp to version 5.9 [DAL-4669]
    1. CVE-2018-18066
5. Update tcpdump to version 4.99.0 [DAL-4587]
    1. CVE-2018-10103 CVE-2018-10105 CVE-2018-14461 CVE-2018-14462 CVE-2018-14463 CVE-2018-14464 CVE-2018-14465 CVE-2018-14466 CVE-2018-14467 CVE-2018-14468 CVE-2018-14469 CVE-2018-14470 CVE-2018-14879 CVE-2018-14880 CVE-2018-14881 CVE-2018-14882 CVE-2018-16227 CVE-2018-16228 CVE-2018-16229 CVE-2018-16230 CVE-2018-16300 CVE-2018-16451 CVE-2018-16452 CVE-2019-15166 CVE-2020-8037
6. Reduced listening network services to least-privilege access [DAL-4703]
7. Removed weak SSH algorithms and protocols [DALP-817]
    1. ***Removed MAC Algorithms:*** umac-64-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, hmac-sha1
    2. ***Removed Key Exchange Algorithms:*** diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256

VERSION 21.2.39.67 (February 27, 2021)

This is a mandatory release

AnywhereUSB2-21.2.39.67.bin

SHA512:
ecb60aaf5e2eafb09dee1570a623927d25d95577e6f81c9c30ab3cc3e66ad185b5af942fd18180dd0fbe861619daa604e8b89944c3d7d533acbd67ab5b5ed854

MD5: 5c2626626d284b8e11a69568471e19c3

AnywhereUSB8-21.2.39.67.bin

SHA512:
81bc19d6e8c0770b34a2209948c705d5cd7570b6967aba163b03829f9dbc4fc5251aa2157f13d3f19e77b2092b743c3f8504e3f54cb846c9e1a3a8adcb527907

MD5: 48850d03ed59f6b5dc73cde722bb6fe8

AnywhereUSB24-21.2.39.67.bin

SHA512:
28123deaebbe39239085390598684bf960620610ab933c129f1961ad99d9441849677f306ef41a1f9d90433310fa0fae5e11e025ffe5d8aada3c19f3f48caaa4

MD5: 9718ed57ba1b24c136cc75a219b4a739

ANYWHEREUSB-specific CHANGES

1. Updated default keepalive timeout for the AnywhereUSB service from 11-seconds to 20-

seconds [DAL-4630]

2. *AnywhereUSB 8 Plus:* Fix broken link to User Guide [DAL-4436]

FEATURES

1. Add the Location service to all DAL products. DAL devices can utilize several location sources (cellular, GNSS, or user defined) to determine where it's located and report that to Digi Remote Manager or other servers [DAL-724]
2. Add geo-fencing configuration options. This new features is found under **Services → Location → Geofence**. It can be utilized to define one or more circular or polygonal geo-fence areas and then perform a set of actions when the device enters or leaves that area. Current options for actions to perform are either factory erasing the device or running a custom script. [DALP-711]
3. New **modem scan** CLI command for listing available carriers for the current modem and SIM setup.
4. New **Network → Interface → Modem → Network PLMN ID** config setting to lock the SIM card to a particular carrier based on its PLMN ID(note that the **Carrier selection mode** must be set to **Manual** or **Manual/Automatic** in order to lock the SIM to a specific carrier) [DALP-637]
5. Added local API to the web UI for automated configuration of the device [DALP-777]
6. Support remote CLI commands through Digi Remote Manager [DAL-4273]
7. New configuration options under **System → Scheduled tasks → System maintenance** to automatically check for device and modem firmware updates, then notify in the CLI and web UI when updates are available [DAL-4413]

ENHANCEMENTS

1. Allow hidden/debug config settings to be controlled and preserved by DigiRM [DAL-4445]
2. Asymmetric preshared keys for IPsec tunnels [DALP-707]
3. Don't display Aggressive/Main mode or Xauth selections for IKEv2 IPsec tunnels [DAL-4142]
4. Update name and description of certificate settings for OpenVPN clients and servers [DAL-4435]
5. Add digidevice.led python module to all products [DALP-710]
6. Add options to forward location information to a remote host over TCP [DALP-778]
7. Add new **Forward interval multiplier** configuration option under **Services → Location → Destination servers** to control the number of location update intervals to wait before sending location data to this server [DAL-4056]
8. Report location metrics as datapoints to DigiRM [DAL-4055]
9. Include the connection uptime of IPsec tunnels as datapoint metrics to Digi Remote Manager [DAL-4062]
10. Add iptables TRACE tool for enhanced firewall debugging [DAL-4182]
11. Improved accuracy of the status shown for a modem during a firmware update

BUG FIXES

1. Fixed issue where non-primary DNS were queried through the wrong interface when **use_dns** configuration option is set to primary [DAL-3156]
2. Report the phone number of the SIM as a health metric datapoint to Digi Remote Manager [DAL-4440]
3. Fixed incorrect format of ICCID and IMEI metrics reported to Digi Remote Manager [DAL-4440]
4. Fixed setup issue between custom firewall rules and IPsec tunnels [DAL-4433]

5. Fixed occasional issue preventing LM940 modems from re-establish their cellular connection after a modem firmware update [DAL-2933]
6. Fixed issue requiring a user to fix syslog configuration setting when updating from 20.5.x or older firmware to 20.8.x/20.11.x firmware [DAL-4426]
7. Fixed rare issue where **show system** CLI command would display incorrect uptime details [DAL-4350]
8. Fix issue with secondary CLI sessions showing stale configuration settings if the config is updated elsewhere [DAL-4446]
9. Updated message displayed in web UI to direct the user to refresh the page after erasing the device back to default settings [DAL-2326]
10. Fixed issue where dynamic DHCP leases were not displayed in the CLI or web UI (bug present on 20.11.x firmware versions) [DAL-4557]
11. Fixed inaccurate status of the Ethernet interface of a device in passthrough mode [DAL-4543]
12. Fixed issue preventing web UI access if two-factor authentication was enabled (bug present on 20.11.x firmware versions) [DAL-4509]
13. Fixed issue where CLI commands sent from DigiRM would crash the DAL device's connection to DigiRM [DAL-4412]
14. Fixed issue preventing WAN/cellular connections from working if the interface was configured with a single **Interface Up** Surelink test [DAL-4629]

SECURITY FIXES

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

1. Update libcurl to version 7.74.0 (CVE-2020-8169, CVE-2020-8177) [DAL-4336]
2. Update to python version 3.6.12 (CVE-2020-14422) [DAL-4364]
3. Update OpenSSL to version 1.1.1i (CVE-2020-1971) [DAL-4326]
4. Update dnsmasq to version 2.83 (CVE-2019-14834, CVE-2020-25681, CVE-2020-25682, CVE-2020-25683, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-25687) [DAL-3950]
5. Update web security settings with the following headers [DAL-4192]
    1. Pragma: no-cache
    2. Content-Security-Policy
    3. X-Content-Type-Options: nosniff
    4. X-XSS-Protection: 1; mode=block
6. Set SAMEORIGIN in X-Frame-Options to uppercase [DAL-4192]
7. Automatically de-activate active user logins/sessions if the password for that user changes
8. Removed support for https CBC ciphers [DAL-4408]
9. Fixed XSS vulnerability on serial page in the local web UI (Bug present on firmware versions 20.11.x and older) [DAL-4646]

VERSION 20.11.32.168 (December 23, 2020)

This is a recommended release

AnywhereUSB2-20.11.32.168.bin

SHA512:
1e58f363db72d07d008e4709e41ea536dd1d704de676ef88acd4c75c664ff3d075b951cc1bb2c7442f5d889d66f04466258394c5b0fe27ec5d9c989cf7104852

MD5: 77b1055fda97bddcb1dd2d7d20d5fb04

AnywhereUSB8-20.11.32.168.bin

SHA512:
0e66a03cb5954fc7ec4967c6abc906cf96f67ffbbbc182102a634e74083eacb077a54f97d3
ca73d8914f4ad509c523e2a9525375a8d0217b2c12582f7b2bb6e7

MD5: 9c46957e97fe5fe6d8e47cfda7da1231

AnywhereUSB24-20.11.32.168.bin

SHA512:
075bf62b1a437d42da97c3cd52985635da89c1d99e3315060a15daa03f7cf740db2520a9
b239c3f17286ac6fbc7948ffb2a089d5584671ef8b83e76c41e4930d

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. Removed QR code generator from the ***Authentication → Users → Two-factor authentication***, as Content-Security-Policy requirements prevent access to resources not served by the device's web UI [DAL-3629]
13. Added extra layer of firmware verification to ensure the firmware matches the target hardware variant and prevent firmware modifications (CVSS score 1.9 Medium CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:N) [DAL-3511]
14. Prevent command injection through modemadvanced, modem_install, and firmware webpages (CVSS score: 6.8 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N) [DAL-4093/DAL-4104/DAL-4046]
15. Prevent manual addition of files to an encrypted filesytem outside of the device itself (CVSS score: 6.1 Medium CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H) [DAL-4149]
16. Restrict memory allocation of tcpdump (CVSS score: 7.5 High CVE-2020-8037 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) [DAL-4226]

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