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

Digi Accelerated Linux (DAL) Release Notes
Digi Connect EZ Serial Servers
Version 23.6.1.105

INTRODUCTION

This is a major release for ConnectEZ products. This is a mandatory production firmware release.

The Digi Connect EZ products are a family of next-generation, multi-port serial servers that connect serial peripheral devices over an IP network. They provide a modern, secure platform with expanded network connectivity and functionality relevant to today's applications.

- Serial servers provide secure, easy EIA 232/422/485 serial-to-Ethernet integration of virtually any device into wired Ethernet networks. They are ideal for use in a wide variety of demanding industrial applications such as automation, robotics control, centralized device monitoring and management, data acquisition, and point -of-sale applications requiring COM/TTY ports, serial tunneling or TCP/UDP functionality.
- Enhanced access control, management and configuration capabilities support key security requirements for critical infrastructure and distributed systems. The built-in Python environment enables application development and customization at the device level, including full device connection control, data manipulation and event-based actions.
- Management and configuration of the device is possible through Digi Remote Manager, web services, CLI connectivity with mass configuration and customization tools available to pre-configure devices prior to deployment

SUPPORTED PRODUCTS

- Digi Connect EZ Mini
- Digi Connect EZ 2
- Digi Connect EZ 4
- Digi Connect EZ 4i
- Digi Connect EZ 8
- Digi Connect EZ 8 Wi-Fi
- Digi Connect EZ 8 MEI
- Digi Connect EZ 8 I/O
- Digi Connect EZ 8 I/O SW
- Digi Connect EZ 16
- Digi Connect EZ 16 MEI
- Digi Connect EZ 32
- Digi Connect EZ 32 MEI

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]
- 1002-CM06 CORE modems are not usable with Connect EZ 8 devices. The 1002-CM06 CORE modem is end-of-life and no longer sold by Digi. It is suggested to utilize the 1002-CMG4-GLB CORE modem with the Connect EZ 8 products. [DAL-8068]

UPDATE BEST PRACTICES

Digi recommends the following best practices:

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

Digi recommends Digi Remote Manager or Digi aView for automated device updates. For more information, follow the instructions for Digi Remote manager or Digi aView in the links below:

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

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

1. Download the firmware file from the Digi firmware support page.
2. Connect to the device's web UI by connecting your PC to the LAN 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 23.6.1.105 (July 16, 2023)

This is a ***mandatory*** release

Part Number	Firmware	sha512sum	md5sum
EZ01-Mxxx	ConnectEZ1-23.6.1.103.bin	e89ba7698284311688b43b4df501ff706161f12fb10768b0a49ab093c44466751359aad7f2d1d164f884be78cfd738ac17fe0cf2128e281818fa2f49950d588f	88702d4065d88d5f6d43d0405140f1c4
EZ02-Cxxx	ConnectEZ2-23.6.1.103.bin	e36ef23d403e6a693b401ada92e79bc3b25a95d2ab6142850fe3fc4e62db4cf9e6e6202becb8ebe248e81009c6738920d79c056b9172b89875e22188d1c0373a	ff129378c0bf8827f106fd4a2eb694c0
EZ04-xxxx	ConnectEZ4-23.6.1.103.bin	713e37a2f57841aadc69dc57d636db7123a36a2bb9aaacaecdf6f6a3757c47fbc731b88b5fa67169b9271ffb468e08a5474e41183f14f09d51e5e8bfeeaca025	ab595ff2eca5867146885f8e6dfa74bc
EZ08-Axxx	ConnectEZ8-23.6.1.103.bin	fe6790edb691a9c71a6ada5b8732654bcae530713adafd0886d0446eb0e91aee293a8285f7936f5280fd4bf4133a13212b002e900ecc338676af11f64746e913	73add9c4e06b71355d26a69cab34feff
EZ08-Bxxx	ConnectEZ8W-23.6.1.103.bin	74e4d8175d21d7c451c8baea898a0f9a5af952d6b230c19e0958db8ae1cf5dc01f17ca1a61bd5274645c1eff781654bde3210a63a2faaaf66131d56c0526f377	42caa1d31caeec35a08302cd41fc97fa
EZ08-Cxxx	ConnectEZ8M-23.6.1.103.bin	2147b2d214a3840d8717f4c08ebfac9c68dd492fbcd619a47ee8f38735a751c882492a673cc04d93b00f566d69819b2f613663798a85d1ab6e8f66d661d7ad66	ca0937879e727a6a1749904d626d6e49
EZ08-Dxxx	ConnectEZ8IO-23.6.1.103.bin	bd894bb9f9fba8176d2b15f1d57dfb87a829c79ffc00253809eb734b27bc224f7f257190ce68dfd06c104f3246587e8d53ce78361ee6665f950d24be5190bb69	c44bf9f50dd63bbe9049a8e06ffad3af
EZ08-Exxx	ConnectEZ8IOS-23.6.1.103.bin	ca1d79019e9fe28d971178bff615fb37585aedd16ff8e50a327d9a9f76f4314f1a0f21969876aed6f9ef75ee21237532b5736f139f5840c0b81722c6abb9b387	d8f5e95c14e693e3d3c8bb00b8171be1
EZ16-Axxx	ConnectEZ16-23.6.1.103.bin	18ff6306450818e253ec8b44afcc00299e3b92ef8f988c8c6a2689c37320a33189c1b03820e6e489653c5758d8602eb5ff9d81675567484775cbf3a06e2df8d3	42fba48f5673b42c904363ea3e98a993

EZ16-Cxxx	ConnectEZ16M-23.6.1.103.bin	c3094a8f3d6d458e9a89cbf703e2913919e76b6823a2cf8f1bd6b61f4bdb1a895c6caec7e5571b6372dda9887f0ff908051dfad2332ea5422a73cbf2adcceb2c	20238a7be362b0a3b86329a2289f85c8
EZ32-Axxx	ConnectEZ32-23.6.1.103.bin	bc18ee3f49ba2245c6fea9194f01d9ec0f1b12a7bbb41e2f9edd7e2410d94aef66cd0e7ec9683a6830b5214e732bf17f2ac795eef67039ab2a8248004095666b	eb5f5580e14250865f3e4a732f498371
EZ32-Cxxx	ConnectEZ32M-23.6.1.103.bin	423ae911a9d88f6866320650774c99044c8d461e8c39d278709200b5056230098edd9d8bac94439326853ff9ea6e7a320613b58d5b56e3d0984d7d309db3d07f	b45e8f38d0c9f09af3aafd55e151911c

FEATURES

1. Added new ***Modem emulator*** mode to serial ports to allow them to act as a dial-up modem emulator for handling incoming AT dial-ins [DAL-6669]
2. Added ability to receive a remote command from Digi Remote Manager to perform a SIM survey, which will attempt connections to each SIM inserted into the Digi device, then switch back to its previously-used setup before the SIM survey and report each of the SIMs' connection details to Digi Remote Manager (signal strength, APN used, connection status, cellular tower info, etc)
3. New unsolicited query_state RCI responses in DigiRM for reporting system temperature and modem firmware versions [DAL-6550]

ENHANCEMENTS

1. Add ***System → Advanced Watchdog*** configuration options to monitor memory usage, critical services and automatically reboot if those services fail
2. Automatically generate a support report in /opt/digi-support-watchdog-mem-full.bin before a device reboots due to a watchdog memory-full condition [DAL-7948]
3. Added option for receiving modem_firmware_update remote command from Digi Remote Manager with a specific modem firmware version to update to [DAL-7656]
4. Added the following details to the metrics sent to Digi Remote Manager about the cellular modems inside the Digi device [DAL-7800]
    1. Add a unique ID tag to the response messages sent to DigiRM after a modem firmware update was initiated
    2. Include modem name and updated version in the modem firmware metric
    3. Ensures that modem firmware versions listed for the device are updated in DigiRM after a modem firmware update completes
5. Report the modem IMEI to Digi Remote Manager even when no SIM is installed [DAL-6778]
6. Added the following new values to the datastream metrics and RCI query_state responses reported to Digi Remote Manager [DAL-6868, DAL-6549, DAL-6655, DAL-6576]
    1. cellular/x/sim/y/registration - roaming/registration status of the modem
    2. metrics/eth/1/surelink/rtt - ICMP ping round-trip time for the Surelink ping test
    3. metrics/eth/1/surelink/fail_count - Count of failed Surelink tests, which gets reset if the tests start passing
    4. vpn/ipsec/x/disconnects - number of disconnects the device has had on an IPsec tunnel
    5. eth/x/link - up/down psychical link status of the Ethernet port
    6. metrics/wifi/x/ - rx/tx/packet-count statistics for any configured Wi-Fi client-mode connections
    7. metrics/wifi-ap/ - rx/tx/packet-count statistics for any configured Wi-Fi access points
    8. sys/chassis/voltage - input power supply voltage

9. sys/chassis/temp - temperature of the device

7. Immediately upload all health metrics on the first time it establishes a connection to Digi Remote Manager [DAL-7559, DAL-7504]
8. Display the active interface used to connect to Digi Remote Manager in the Dashboard page of the web UI and the show cloud Admin CLI output [DAL-6446]
9. Updated the minimum-allowed location update and cellular modem update interval to 1-second [DAL-7440]
10. Added new Location source option to directly poll the cellular modem's GPS port [DAL-7682]
11. Added new ***VPN → IP tunnels → Enable open routing*** configuration setting to allows packets destined for an address which is not explicitly in our routing table to exit the iptunnel [DAL-7076]
12. Added new ***Network → Advanced → TCP retries2*** configuration setting to control the number of times an unacknowledged TCP data packet will be retransmitted before the connection is considered lost (default 15 retries) [CEZ-570]
13. Update the help text descriptions for all serial port modes for additional clarity
14. Updated the SSH server enabled for serial ports to reference any configured custom SSH options in ***Services → SSH → Custom configuration*** [DAL-7863]
15. Added a new configuration setting under the options for a serial port set in PPP dial-in mode to control whether a default route gets added for the PPP interface (default: disabled) [DAL-7798]
16. Improved wording in the error message when a TACACS server cannot authorize the full CLI command due to RFC length constraints [DAL-7852]
17. Create a system log if WAN Bonding is enabled but unsubscribed [DAL-7882]
18. Removed the ***Network → SD-WAN configuration*** configuration section [DAL-7881]

BUG FIXES

1. Fixed errant IPv6 packets from being transmitted over a PPP dial-in serial connection [DAL-7799]
2. Fixed issue where WI-Fi hotspots would not startup correctly if they weren't linked to a network bridge [DAL-7623]
3. Fixed issue with improper LWM2M setting on LTE Cat-M modems preventing registration issues with AT&T and Verizon [DAL-7383]
4. Log message about intelliFlow being unsubscribed only if intelliFlow is enabled
5. Fixed configuration migration of IPsec Surelink settings from 23.3.x firmware to not add an ***update_routing_table*** action, as that action is not applicable to IPsec tunnels [DAL-7892]
6. Fixed incorrect status reported for Surelink status of IPsec and OpenVPN tunnels in the CLI and web UI [DAL-7893]
7. Fixed issue in Surelink migration from 22.11 and older firmware where IPsec and OpenVPN tunnels would not have their Surelink settings migrated over [DAL-7747]
8. Fixed issue in Surelink migration from 22.11 and older firmware where success_condition=all wasn't always properly migrated [DAL-7803]
9. Fixed issue in Surelink migration from 22.11 and older firmware where ping tests switched their default ping size from 20 to 1 byte, which can cause issues on some cellular networks [DAL-7769]
10. Fixed incorrect Surelink status reporting when Surelink was disabled on a network interface [DAL-7552]
11. Fixed logic of default DNS test so skipped tests are considered passing tests [DAL-7814]
12. Fixed rare issue where the device would report its MAC address as all zeroes when it initially

connected to Digi Remote Manager [DAL-1609]

13. Fixed issue with utilizing BGP capability 70 to DMVPN hubs [DAL-7740]
14. Fixed bug where SNMP wouldn't provide updated settings if someone configured a new hostname for the device [DAL-7442]
15. Fixed bug where Intelliflow data would reset each time a network interface update happened on the Digi device [DAL-7579]
16. Fixed but preventing users from configuring network subnets in OSPF routes [DAL-7603]
17. Fixed issue where multiple SSIDs were not being scanned when DFS client support was enabled [DAL-7608]
18. Fixed issue preventing EG25-G & EC25-AF modems from connecting with certain SIMs with APNs that required username/password authentication [DAL-7644]
19. Fixed missing ICCID and modem firmware revision was not reported by the device [DAL-7757]
20. Fixed rare issue where LM940 would power off after a modem firmware update [DAL-7719]
21. Fixed intermittent issue where LM940 modem would disappear after switching SIM slots [DAL-7638]
22. Fixed issue preventing devices from performing OTA firmware updates through the ***System → Firmware update*** page in the web UI or the system firmware ota CLI command [DAL-7539]
23. Fixed minor bugs in Realport authentication timing [DAL-7651]

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 Linux kernel version 6.3 [DAL-7606]
2. Updated busybox to version 1.36.1 [DAL-7819]
3. Update to OpenSSL version 1.1.1u [DAL-7818]
4. Update libcurl to version 8.1.2 [DAL-7817]
5. Update OpenSSH to version 9.3p1 [DAL-7816]
6. Update libgmp to version 6.2.1 [DAL-7820]
7. Update OpenVPN to version 2.6.4 [DAL-7822]
8. Update strongswan to version 5.9.10 [DAL-7823]
9. Update dnsmasq to version 2.89 [DAL-7533]
10. Update netifd/ubus/UCI/libublox to OpenWRT 19.07 build [DAL-6766]

VERSION 23.3.31.129 (May 4, 2023)

This is a ***mandatory*** release

Part Number	Firmware	sha512sum	md5sum
EZ01-Mxxx	ConnectEZ1-23.3.31.129.bin	210de552b71a4e54133461854b4284363a10981f6be3b5022a2d043ae4a2de01d4932492f09b41cc894a5d4297e8200f773af847eb1035396017683b4db92762	071f2145c9bfbd6e1fcb19268f86cd78
EZ02-Cxxx	ConnectEZ2-23.3.31.129.bin	3c50b37870bdf99fe1f798d0319f0db7c9db4569b4273138b945b056e44855412eb249a902d78e28ba1321145aa518e00b6f04351021bb0262de43a99e647534	c9a25cff9dd6e0ae6315bf4c9d5890c7
EZ04-xxxx	ConnectEZ4-	21ad4195119a3fd4b6982283dcbd1b44fa5f7	ed79f6cc9877b5a2e08ecc03b7d

	23.3.31.129.bin	cac066338fdcd281b6cd440661b08612205a73b4eacecf5fe24bfa2ce17c123ba9ee74c382f85e6eb77f17d9a08	77dd5
EZ08-Axxx	ConnectEZ8-23.3.31.129.bin	5101f4a05d2172214aef8391dde0071b872dafb23c150ac09cd95cdec1ef7b267b5ce97ca10a389ea26c445e5ce2e85266529d58473d2afda0440b116fcc4ab	2025bd6a5bb7bedb47ea3413315b23df
EZ08-Bxxx	ConnectEZ8W-23.3.31.129.bin	2a8ab62a3404c0c091827cbeeef596f1204c7fd58e4c887230e951e4eefc3d0815627305d5bf1421a96bed62b2cd0a45182ccdb5ed0dcb82d1dd7efe601549e0	499e4087305d73ad4e233893df8815fb
EZ08-Cxxx	ConnectEZ8M-23.3.31.129.bin	11ccedca457360e72b716abe6fb65bff406e456357fcc986ae6274f9e8f4f41fcd83fe3266c8d9891ce83ce2dee035f3e6d3d0ae19088fe9aba700f9d7f204bd	20646806f684e899581091c0a8cf9f6d
EZ08-Dxxx	ConnectEZ8IO-23.3.31.129.bin	03509125f81ffd0fc9b54bad96fa04f46816226f4cb7d46b0d8202020c294b0106530786679cf4921be530ef20913a7584e2d03c64f54616c6273b2cea38af19	b94e596125a0d997715a834594557334
EZ08-Exxx	ConnectEZ8IOS-23.3.31.129.bin	471a6339cf1b8bae012bb5b3ac04b97006cb096b82372571655d44006d0a6857f61826a4f20119fc4fbd773ac7dc205287df43b0f206e068fe6b6e7d64a95a49	a1296965d7bb1723e38d2235c2def4f1
EZ16-Axxx	ConnectEZ16-23.3.31.129.bin	3b548195a40e1593375d2273621e58d3ce7a8fb7b9a509febe543cb0a89c044e665237970e90a459e363bc587eb2aa111bdbd69c7f0445cf0fe117d1bf0658e9	277c6dcb1040edddcfda247ad6c04b74
EZ16-Cxxx	ConnectEZ16M-23.3.31.129.bin	4ac19cae05a93c2c2a85f4fcfd2f7ab76c59e084673643e2106a82ea0e979fbaa2aca3e5422de0c32d309b334247a647bcf0a3a100e0c67f18a23d6e85fc9f56	0c86c8cb2d58950e9c828f46f317ca91
EZ32-Axxx	ConnectEZ32-23.3.31.129.bin	a2a1780945234fd182a37649d48610817c063dfdb70ae92e1200765de8e2e2f3bff43085b3dc4ba810181245699a505c5af6c5810ec377308ba0ba98f0426fca	1dd6b074d969b56bb81dad03b06e8342
EZ32-Cxxx	ConnectEZ32M-23.3.31.129.bin	613cf09858634f9727d27b043910ae104532166c4e5009b496ac5aea04d88a52acf30d009bb90693fc6cb37d58d92f72029c04b6c2992111566702cb46e844b9	9d68578a37d788ff8b264c7ccbe8972f

FEATURES

1. Redesigned Surelink configuration settings [DAL-6646]
    1. Surelink configuration settings are now listed in a single section under each network interface, as opposed to a separate section for IPv4 vs IPv6. The layout of the connectivity tests and recovery actions to perform have been redesigned to provide a more streamlined setup. Any configured tests and recovery actions are performed in the order they are configured, along with a new capability for integrating custom scripts as a test or recovery action. See the Surelink section of the Digi device's user guide for additional details.
    2. ***Important note:*** when upgrading a device with non-default Surelink settings from 22.11.48.x or older firmware to 23.3.31.129 or newer, there are some instances where those Surelink settings will not migrate and the device will revert back to default Surelink settings. Digi strongly recommends that you test the new firmware release in a controlled environment with your application before you update production devices. Pay particular attention to your Surelink configuration settings before and after the firmware update, and review any changes before rolling out the 23.3.31.129 release to

mission critical devices

3. ***Known migration issues with 22.11.48.x and older firmware:***
    1. If an IPv4 Surelink specifies one test but the IPv6 specifies all tests, then all tests will be selected and Surelink may not behave as expected. The same applies for the reverse - IPv4 specifies all tests and IPv6 specifies one test.
    2. The previous version didn't correctly go out the correct interface in every condition. It was possible to pass the ping test without the interface even being up. This is now fixed in 23.3.31.129 firmware and newer so tests are forced out the correct interfaces by marking the packet.
    3. If migrating from a very old version (firmware versions 20.2.x and older), the config cannot be migrated as it is incompatible. In this scenario, we use the default Surelink configuration for all interfaces
    4. If there are conflicting Surelink action or test settings for IPv4 and IPv6 (eg intervals etc), the device will use the IPv4 in preference when migrating the configuration as part of the firmware
2. DMVPN phase 1 spoke support with NHRP or mGRE, including compatibility with Cisco DMVPN hubs [DAL-6709]
3. Added ability to utilize the cellular modem as a time sync source under ***System → Time*** [DAL-6693]

ENHANCEMENTS

1. ModemManager updated to version 1.20.6 [DAL-6406], which includes:
    1. improved 5G SA-mode and NSA-mode performance
    2. RSRP/RSRQ/SINR statistics for 5G SA-mode connections
    3. Native multiplexing for dual-APN setups
2. Added ***show surelink state*** Admin CLI command to display the overall pass/fail status of the enabled Surelink tests [DAL-7070]
3. Added options under ***Network → SD-WAN → WAN bonding*** to configure the mode for each tunneled interface and the overall mode of the WAN bonding tunnel [DAL-7394]
4. Updated WAN bonding saneclient to version 20221103 for 5G and 1Gbps performance [DAL-7005]
5. Added new ***show wan-bonding*** Admin CLI command to display status of WAN Bonding tunnel [DAL-7395]
6. Added new ***Status → WAN Bonding*** page in the web UI to display status of the WAN Bonding tunnel [DAL-7395]
7. Added distance between the WAN bonding and Ethernet bonding setting sections in the configuration accordion
8. Added configuration settings under ***System → Containers*** to allow the container to be auto-started on boot with optional parameters and restart if the container stops {DAL-7021]
9. Added configuration settings under ***System → Containers*** to setup shared directories between the host filesystem and the container [DAL-7021]
10. Support for US cellular consumer SIMs without requiring the user to first configure the APN [DAL-7248]
11. Disable mDNS by default on EX/IX/TX products for improved cellular performance [DAL-7354]
12. Added GlobalGIG APNs to fallback APN list [DAL-6886]
13. Added new ***AT&T LWM2M support*** setting for enabling/disabling LWM2M on the modem (enabled by default) [DAL-7009]
14. Added IPv6 support for MQTT broker, location servers, and mDNS service [DAL-7111]

15. Include the system hostname (if configured) on the Dashboard page in the local web UI [DAL-7428]
16. Added support for SHA2 ciphers for IKEv2 IPsec tunnels [DAL-7038]

BUG FIXES

1. Fixed issue preventing users from locking a device to use a blank APN [DAL-7248]
2. Pre-shared keys for configured Wi-Fi SSIDs are now obfuscated in Digi Remote Manager [DAL-7107]
3. Fixed issue where configuration options for selecting the Wi-Fi channel appeared as “None” in Digi Remote Manager [DAL-7482]
4. Fixed issue preventing device from falling back to its local system time when running as a NTP server [DAL-7233]
5. Fixed issue preventing SIM failover when the device was configured with separate network interfaces set to match by carrier instead of SIM slot [DAL-6910]
6. Removed 3-second stop/start delay when making configuration updates to the MQTT broker settings [DAL-7104]
7. Fixed issue where ***tail*** CLI command required a filter option in order to utilize the match option [DAL-7038]
8. Fixed issue preventing WAN bonding interface from appearing in the ***show route*** CLI output [DAL-6829]
9. Fixed issue where initial Surelink test would fail if the cellular modem was configured to be in passthrough mode [DAL-6224]
10. Fixed possible routing issue between GRE/IPsec with Cisco peer GRE/IPsec using VTI configuration [DAL-6722]
11. Fixed issue where serial logging enabled on Realport serial ports never closes the logging session [DAL-6748]
12. Fixed issue preventing SMTP notifications from using TLS encryption [DAL-7079]
13. Fixed invalid link in the local web UI to the product user guide [DAL-7304]

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 Linux kernel 6.1 [DAL-7179]
2. Update OpenSSL to version 3.0.8 and 1.1.1t [DAL-7261]
3. Update netifd to version 18.06 [DAL-6280]
4. Update libexpat to version 2.5.0 [DAL-7082]

VERSION 22.11.48.11 (March 24, 2023)

This is a ***recommended*** release

Firmware	sha512sum	md5sum
ConnectEZ8-22.11.48.11.bin	71A8F8524FD2197F01C8F858A065B01A75155FCD69BC6299A881D1A960CF66774C6A3437C5237F3648458241722861DF634CD35927C83DC7810360B061C2FB00	DDB203856B1967E928D5352FB326C600
ConnectEZ8W-22.11.48.11.bin	77B0E7AED770F3147A1AC3D4E519908A9D6733C4C70ADCB13D4B0349EB8B9D043D76146304C7F7C5AE3C8EE285EE1C74BB12FFB376236C54B2ED5D166E201497	7ACF0D42D6767EA92A8F5D9FFEFF1352

ConnectEZ8M-22.11.48.11.bin	BD211E9AE01CD525161DF6E93E416D0B61C C2E4A799764E349957F18ABB59645C3C202 4105E6F2FB55E82751E0313F5C27F8A93DE3 2D0A0BE1A7F9C647E38CA7	C13A7F8B35F6639B7198460EB1996056
ConnectEZ8IO-22.11.48.11.bin	26C1E39BCCEBA4A5770214D8544AF86B88F 7E0F8A7A4390FF947C2301FCC3D3771EBF2 1B65A57B496F5BC9B4DE7D663A64B083281 FDF7A342BCA6EBCA06F58FE	85B860F168882381496F62A332DE0FA2
ConnectEZ8IOS-22.11.48.11.bin	08C34D43E30EC31459DF0D4D560DDBC9F6 80C3099D2BB547E2CD87A23E181E97DEBC2 A0167075F1BB6BD3A2B510D071D2B4BAD7 F900819DED44A459A37C2FF07	9A3004A5A7A5F1F54D1A316649C90F37
ConnectEZ16-22.11.48.11.bin	9AEAF9E4C6519D8A6F4EA858D1712FE3DE3 0739C4A4515DEAAA363A2DC8C52B5F02AA8 CAE30C7A76C970202AA0782E5A2BAF47E0D 9CE5B9D26404239CB63126A	5672444F942F84FD46C19036C641854B
ConnectEZ16M-22.11.48.11.bin	C5B82356C459B2BE7BE19AB74450350AE8D 663D12D6B135A66085CEE32FFC7FF019C82 912F17EE34068F7112047E9BE714C93F4739 ABE15A2478EDB0901E2039	F8480FC3E86C11D825B95EF1AE058D38
ConnectEZ32-22.11.48.11.bin	9945C2BC4F275AED021F95E9FCDEEE2C9AB 13F8DF5A15A994E5D2B44C34FA75118F47D 419AD308DE5530996DEB02A5EB3A44661EC B2F4F7F9EE6EF034175896C	FD416FD3AB0794AAB6D80BF58F1BD666
ConnectEZ32M-22.11.48.11.bin	5E929B571DDE764EB54DECD5834E96CCBB 17143403D655834E021420F321BF7D2DA106 3D58D8B6436392F4006C112208B884F01083 3733EDCA6AB036DD2A0362	EB479EA7280B3DF50CB8EF3BDB959B38

FEATURES

1. Added support for 8, 16, and 32-port variants of the Connect EZ product family.

VERSION 22.11.48.10 (November 24, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
ConnectEZ1-22.11.48.10.bin	7d55a9d4d5e0075d16ae75e76a606b974e3118 9a7afd9d68e8b029e160fced1f707ca5c6f68421 a75605165dd477d2cc211485e99d0c5d896985 37bbef32c6cb	ebef16391cd74d38d0a56f5409ca5566
ConnectEZ2-22.11.48.10.bin	63a36e7838dec7c9a3215397c37484710d98da 9071bd5288285792665daeb6ab113e2ad22e39 1648f7db77c9f74def73dd280ed44ff87bb3135 bd39aa8683871	79bf296b33c435e2f12f7e0dde107742
ConnectEZ4-22.11.48.10.bin	b3153e847637eab8353ff29cd1d7ce4714d256 ffe8b8eedc23d5b7608d3c2fded5edb53785f62 c326299bb3e0c5f19bdaae5c8bec91e7896025 6f597c92154ef	c36bdbec6856f8e3941103934feb965d

FEATURES

1. Updated the intelliFlow feature to integrate with Digi Remote Manager for aggregated insights and analytics [DAL-6656]
2. Add options under ***Network → Routes → Routing services*** for configuring Next-hop routing

protocol (NHRP) advertisements [DAL-6711]

3. Added advanced watchdog to monitor critical services and automatically reboot if those services fail. The advanced watchdog also monitors system memory usage and will automatically log an error and reboot the device when memory usage exceeds 95%. The advanced watchdog settings can be configured and the ***System → Advanced watchdog*** section of the device's configuration [DAL-6094]

ENHANCEMENTS

1. Added new ***System → External Storage*** page in the web UI for mounting and interacting with external storag devices. These settings can also be configured under the ***System → Storage*** configuration settings [DAL-6683 & 6686]
    1. Removed ***system storage*** Admin CLI commands. These actions for mounting and interacting with external storage devices are now controlled through the ***System → External Storag***e page in the web UI, or under the ***System → Storage configuration*** settings
2. New **System → Log → Event categories → External Storage** system event log for notifying when a device's external storage exceeds a specified percentage used (configurable with the Percent used setting for the external storage device) [DAL-6687
3. Add option under ***VPN → IP Tunnels → Mode*** for supporting mGRE tunnels [DAL-6709]
4. Added option under Network → Advanced settings to allow ICMP redirect messages (disabled by default) [DAL-6013]
5. Disable automatic modem/device firmware update options if using DigiRM [DAL-5738]
6. Added new ***Signal strength query interval*** setting under the ***Network → Modems*** configuration options to control how often the cellular modem is polled for signal strength and other network status updates (default is once every 5 seconds) [DAL-6272]
7. Display the LTE Cat-M or NB-IoT network type in the Admin CLI, local web UI, and Digi Remote Manager metrics for devices with ME910c1-WW modems [DAL-6155]
8. New ***tail*** and ***grep*** Admin CLI commands
9. Send container datapoints to DigiRM with the configured container name instead of container index number [DAL-6551]
10. Update wording of help text for the ***Authentication → Methods*** options in the device configuration settings to provide clarification on the mode of operation between authoritative versus non-authoritative options [DAL-6928]
11. Add modem scan timeout option to ***Scan*** window on the ***Status → Modems*** page in the web UI [DAL-6938]
12. Update error message in the web UI when restoring a configuration backup if the web connection is lost before a response is received [DAL-6553]
13. Added new ***Data logging*** options under ***Serial*** configuration settings to have any data sent/received on the serial port logged to the system logs in addition to whatever mode the serial port is in [DAL-6719]
    1. Remove options in the local web UI and Admin CLI for manually starting/stopping/clearing serial logs. These actions are now controlled under the ***Data logging*** configuration settings

BUG FIXES

1. Fixed occasional issue where containers could not start due to a permissions issue [DAL-7041]
2. Fixed intermittent issue preventing configuration restores from the Admin CLI due to the output of the ***show config cli_forma***t command presenting configuration settings in the wrong order [DAL-6435]

3. Fixed issue in digidevice.sms python library where it couldn't process MMS messages [DAL-6952]
4. fix output of iperf speedtests in the Admin CLI [DAL-7001]
5. Disable GPS reading on ME910c1-WW modems to prevent CPU utilization spike from ModemManager [DAL-6575]
6. Fixed intermittent issue with SIM failover on devices with Telit LM940 modems [DAL-6569]
7. Fixed intermittent issue preventing modem firmware updates if no SIM card was inserted into the active SIM slot [DAL-6309]
8. Fixed issue resulting is slow upload speeds for clients connected to a Wi-Fi hotspot [DAL-6674]
9. Fixed intermittent issue in IPsec strict routing mode where a default route change could result in packets not going through the IPsec tunnel [DAL-6518]
10. Fixed intermittent issue where a device configured as a L2TP LAC would sometimes drop its tunnel and not automatically reconnect [DAL-5415]
11. Fixed intermittent issue where a device configured as a L2TP server would sometimes drop packets from L2TP client tunnels [DAL-6696]
12. Fixed issue preventing L2TP tunnels from running if they were configured with a name longer than 12 characters [DAL-6718]

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 Linux kernel to version 5.19 [DAL-6558]
2. update shellinabox to version 2.21 [DAL-5430]
3. update systemd to version 245 [DAL-5421]
4. Prevent escalated filesystem access through DigiRM [DAL-6784]
5. update OpenSSL to version 1.1.1s [DAL-6991]
6. update jquery to version 3.6.1 and jquery-ui to version 1.13.2 [DAL-5686]
7. update default OpenVPN server cipher from AES-256-CBC to AES-256-GCM [DAL-5737]

VERSION 22.8.33.50 (August 26, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
ConnectEZ1-22.8.33.50.bin	a619fa418fbe70626c246f55ff579ee4fcf5fe7b9011dd3a5bf776ac01cadf849c86d4c48b1fde0c800dc2ded39ff9c0bfd0dd0dcb36a0588f57c22f6e8230ba	75d269dd5d039673908134fc4871885b
ConnectEZ2-22.8.33.50.bin	fd61703ef7d05917f04871526135159ccfa2bd7de0e997ec73b68ef8a09b1663b0e2c7c1083c46acb5e592dcc557e016e045b2247d02722e375e517670f5e401	bd5826aa433441366c4c8231d2860231
ConnectEZ4-22.8.33.50.bin	7900594e2b1f2ce1212bd3ae5cd823ba6af25dd644917713423a7444ba41780ac6d9aed9fe712ea48fc17d33f23393edba8a713f97b585d0345c8fa53077e6f5	649ae99a1a5c5ffb0284ee233c964bc4

FEATURES

1. Added configuration options for running a PPPoE server in IP passthrough mode [DALP-

1045]

ENHANCEMENTS

1. Update firmware OTA downloads to utilize the Digi Remote Manager firmware repository (firmware.devicecloud.com) [DALP-606]
2. Always display ***Central management → Firmware server*** configuration setting regardless of which central management service is selected [DAL-5719]
3. Always display ***Central management → Speedtest server*** configuration setting regardless of which central management service is selected [DAL-6527]
4. New ***modem firmware ota download*** Admin CLI command for downloading cellular modem firmware from the Digi firmware repository [DAL-6541]
5. Add ability to specify DFS channels under ***Network → Wi-Fi → Client mode connections*** for background scanning when ***DFS client support*** is enabled [DALP-1004]
6. Add cellular carrier name and ***PLMN ID to Status → Modems*** page in the web UI [DAL-6554]
7. Mark Containers as a premium feature enabled via Digi Remote Manager [DALP-1038]
8. Support the ability to start/stop containers via RCI commands from Digi Remote Manager [DAL-6468]
9. Added new metrics for sending container status, name, CPU load, and disk usage as datapoints to DigiRM [DAL-6404]
10. New ***show eth*** Admin CLI command to show the link status of each Ethernet port [DAL-6126]
11. New ***poweroff*** CLI command to perform a graceful shutdown of the device without automatically rebooting [DALP-982]
12. Added new ***Strict routing*** setting to IPsec tunnels that, if enabled, will only route packets through the tunnel if both the source IP and destination IP match the IPsec tunnel's policies instead of NAT-ing traffic that only matches the remote network policy [DAL-5317]
13. Added new MS-CHAPv2 option under ***L2TP → L2TP network servers → Authentication method*** to support clients that require MS-CHAPv2 for authentication to a L2TP/IPsec server [DAL-6327]
14. Store kernel crashes and debug logs across reboots and automatically add them to the system logs in /var/log/ [DAL-6496]
15. Include AT#FWSWITCH output in support reports [DAL-6580]
16. Added ***network.modem.modem.gea1_cipher*** debug config setting that can be can enable GEA1 cipher and speed up initial connectivity and SIM failover on Quectel modems [DAL-5258]
17. Automatically refresh the ***System → Firmware Update*** page in the web UI after a user clicks the Duplicate Firmware button [DAL-4750]

BUG FIXES

All bug fixes listed below affect firmware versions 22.5.50.62 or older unless specified otherwise

1. Added new ***Network → Routes → Routing services → BGP → Networks*** section for defining specific IP networks to advertise to BGP peers [DAL-6368]
2. Fixed issue where manual carrier selection through the web UI, configuration settings, or Admin CLI would fail to connect if the SIM required a APN username/password with CHAP authentication [DAL-6552]
3. Fixed L2TP setups so it only adds a default route for the tunnel if the defaultroute custom PPP setting is specified [DAL-6328]
4. Add ***timeout*** option to ***modem scan*** Admin CLI command to allow users to specify a longer scan period for SIMs that can roam to a larger number of nearby carriers

5. Fixed buffer limitation of 1024 characters when copy/pasting text into the Admin CLI [DAL-6445]
6. Fixed issue where kernel-level system logs were logged with UTC timestamps regardless of the locally-configured timezone [DAL-6408]
7. Fixed issue with sending UCS-2 formatted SMS messages with UTF-16 characters [DAL-6318]
8. Fixed issue preventing the Digi device from connecting to Digi Remote Manager over a HTTP proxy through an IPsec tunnel [DAL-6430]
9. Fixed permission issue with starting containers added via Digi Remote Manager [DAL-5844]
10. Fixed invalid format of SIM ICCID metric sent to Digi Remote Manager [DAL-6394]
11. Fixed issue where Wi-Fi client would not reconnect if the config settings were disabled and then re-enabled [DAL-6592]
12. Fixed issue where the ***Reset modem*** Surelink option would prevent the ***SIM failover*** Surelink option from taken affect if both Surelink settings were enabled (affects firmware versions 22.2.x through 22.5.x) [DAL-6343]

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 OpenSSL to version 3.0.5 and 1.1.1q (CVE 2022-2274, CVE-2022-2068)
2. Update Linux kernel to version 5.18

VERSION 22.5.50.62 (June 14, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
ConnectEZ1-22.5.50.62.bin	d3b02d2e79a9954c077e1784e2c4a2afc44f633cfeeb59f0395f2dc95391805fca28ab315ef52d1b607c415e2a68942de7adde769ec8e5ac7ed5d33b39d24c82	b2cbc7a102093f5c6afbd46f2c99e4ca
ConnectEZ2-22.5.50.62.bin	e38f89c31a24ba6fc5a30a23086d263f65d3f8834e1e1615fa0461940c6866e22970a845f2260b4bbdf4f5644bbf3bffb436fc276e3455e8c80a97d3094deca7	03f89aa30242c95b6e45b175fff7f166
ConnectEZ4-22.5.50.62.bin	1bf52e4b1c6633b12dba19de2c545326ba588219bbaf99aa6ed4ddfcab4b438ccd954bf9e936098306234f917f930056dcfb13e9e97794c93fab7d0e6ec4c537	270b746722aa2a552f8f1aa4801b277b

FEATURES

1. Serial PPP dial-in mode for handling AT-based connection requests from a device connected to a serial port and providing IPv4 networking to the device [DALP-880]
2. 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]
3. New *show scep* Admin CLI command for showing the sync status, expiration dates, and additional details of any configured SCEP clients [DAL-6069]
4. 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. Add support for the CP210X serial driver for connecting to Cisco USB console ports [DAL-6119]
7. Filter out non-Internet type APNs from our APN fallback list [DAL-6227]
8. Automatically power cycle the cellular modem in the event that a *modem reset* Surelink action fails [DAL-6268]
9. Enable Surelink *reset_modem* action by default on cellular interfaces and set fail count to 3 [DAL-6275]
10. Add cellular APN and cellular connection duration as datapoints sent to DigiRM [DAL-5902]
11. Ensure modem is in enabled state before attempting to connect [DAL-6163]

12. 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 Connect EZ 8 devices from being setup using the Digi Navigator tool [DAL-6117]
2. Fixed issue preventing Telit LE910 family of modems from registering after changing APNs without a reboot [DAL-5971, DAL-6016, DAL-5203]
3. 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]
4. Fixed issue where modem-based Location source would sometimes not report properly due to an initialization timing error with the modem [DAL-6163]
5. Fixed issue where an IPsec tunnel fails to re-establish the tunnel if SAs are deleted after phase 1 re-authentication [DAL-4959]
6. 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]
7. 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]
8. Fixed issue preventing OpenVPN server from authenticating clients with an external LDAP/TACACS+/RADIUS server [DAL-6159]
9. Fixed broken ***Go to Digi Remote Manager*** link in the local web UI [DAL-6088]
10. Fixed issue preventing LDAP external authentication for SSH and Telnet session [DAL-6098]
11. Fixed typo in description of *container delete* CLI command [DAL-5956]
12. Fixed output of *show containers* Admin CLI command to list all containers on the filesystem, not just those linked to configuration settings [DAL-5958]
13. 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
14. Fixed issue preventing ***Network → Interfaces → MAC address allowlist*** from implicitly denying access to devices not in the allowlist [DAL-6001]
15. Fixed ***Invalid lookup path for : network.interface*** error when running *cfg.get("network.interface")* in the digidevice.config python module [DAL-6005]
16. 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
ConnectEZ1-22.2.9.85.bin	9dd7241813f855270a53b0798609a20fbefc24f9092efc81b0fc36427add488bc2498a069ecb28a1b688882c716bbe2b81c7d438cc479933c56347442f769cd5	a613480a1c66d12ecb103bb6941b5f4a
ConnectEZ2-22.2.9.85.bin	756f0a53e77e18a2cce24685a822bd56e9fbf956c3d7bd88d4052c4f501fb92201059b505681c13b1f73062cd343e991a9a196bae5421c9ca9a645b51f9a1a94	9c629a6f06b85a50385de06d34cc240e
ConnectEZ4-22.2.9.85.bin	b2c3e6dee453ef17072d65982d3a18c9b72b0b9d4ff112046ff6a0499e7b6ef4f0c3bcf90962ab8e6f0a61e335b510422eaf2edb420fa019155a22bb11975585	67e282adccfef72fb68c666bda690769

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. Added new ***Serial → Autoconnect → Socket ID string*** option to send the configured text to the remote server(s) when a TCP socket connection is opened to the serial port [DAL-5700]
8. *1002-CM06/1003-CM07:* Utilize T-Mobile carrier firmware if available for the cellular modem when using Sprint Curiosity SIMs [DAL-5466]
9. New cat Admin CLI command for displaying file contents [DAL-5853]

10. Update /etc/config/scep_client/ directory to be read/write by admin users
11. 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 21.11.60.65 (January 14, 2022)

This is a ***recommended*** release

Firmware	sha512sum	md5sum
ConnectEZ1-21.11.60.63.bin	77e3498b9eae2b45c5d2e81d4aa7a60e41d4dd5f1392bbe823475ca09c51f0d854dbaac205b2a23796d9d3ad63a7ab2aa6747158131efb9bb07b84318517ab37	3a2bb459e216f723e389d00c657ff7c5
ConnectEZ2-21.11.60.63.bin	29f2983b2e4225b121c95331758231bb70749c2536be41376cf8b4110771ce9a28d8cf3a005d3f746c05dc6a53ec28aaada037ba63e05349ab8fb274c41b421a	d1a3cde5302237a47d95550d1d503b0c
ConnectEZ4-21.11.60.63.bin	a213a8a1fde092e2ce842c662adfdf922fcf4f683a5e8ce152654a76c923226a20e9cd96fb30401f04f22b7c3dec29927b41b96b749e67c91380fb1a26a89c9f	4829ce82228e0813e64840454fc1f8e1

BUG FIXES

1. Fixed bug where only the first policy would be applied if an IPsec IKEv2 tunnel was configured with multiple remote networks (bug present on firmware version 21.11.60.63 through 21.1.39.67) [DAL-5347]
2. Fixed bug preventing access to the local web UI and connectivity to Digi Remote Manager if the ConnectEZ was reset back to default settings (bug present on firmware version 21.11.60.63) [DAL-5739]

VERSION 21.11.60.63 (December 8, 2021)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
ConnectEZ1-21.11.60.63.bin	fedd384edbf3700017b6b5b628c43d11c4193c4f3fbcc3b39a234bda0b9613c5a58f2ee5efcde073ca0de19c9a4d3249c77375f2f34529029000658789 9dd66	0dc75be78f62820c70999d6f19bca169
ConnectEZ2-21.11.60.63.bin	09ffbc1826572a5dac45c85f3fba67e69c6daec9056d6c4d8b88b1af680cdfeeb5636fdb084bfa3d5b065c496cdb7963983d0df77fc8f42b4f153e36957c6240	371425816d304d226822ab986360acc8
ConnectEZ4-21.11.60.63.bin	40e9c3f3a40108e2df8c9d30972c0be263286855258d2ddd1a71d6d0a00dcf610d15f4c142c7443e9e21a14743ffa49903cf08ca92a1e71b6f9590987ef2ec67	65917cda49e97eb2f9b32e5e0de6cd03

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 21.8.24.139 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 taken 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 21.8.24.139 (November 12, 2021)

This is a **mandatory** release

Connect EZ Mini

SHA-1: 069160b3c5d47ebfbbbb964da96b87c820ea491c

SHA-512:

f9d044c2393f6b8c99deea2e7cb141f45fc4f94c59ff144370cdea60a14ab8e72e8de972d6a109001ae1a8ffcde703895a4456115513ef7981f4eb5c7fdfa9f4

Connect EZ 2

SHA-1: 408f3b1e3209bcf0cf2992470c7d69737b6b99d1

SHA-512:

432bf292165f635fbbe38e08a90e7c1a56b6a48a0738c86285e4318ee5bee4ad1e0e7ba13c9da022e618bf08fd5001f7a195610a1bfb182ab878a8b89197443d

Connect EZ 4 / Connect EZ 4i

SHA-1: 9434c8e2efe91d71c214c8eb5347ce730260213f

SHA-512:

264ddb85165f712be099fc0b4f3561ba00f1088a925d8298f143389095461a342c03e2d7ea80f14556ab8eb27804760d7d9c0a772d8920f1703f3e36255f557a

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 21.5.56.108 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 21.2.39.67 (March 1, 2021)

Connect EZ Mini

SHA-1:

748c4f92df2c1ba0c3918ceb792d35229720fd2b

SHA-512:

eedc041aac7d5cf531e14fe3ca71bbd28545484c7b5f7ecddb901dce5c392781a88b97808f87b2044fb968435247ddb74ddc02bb8501ae1c4597bbbf6dacd499

Connect EZ 2

SHA-1:

7822e097f4cb3fc44f561c2360995cebbdf93db5

SHA-512:

f805990877e252806f7a4c91eb9c737fc54601d7f71496e56a7602e045b3f21a547d127d7c111a3d772a4021894176c324be1f0b3509054aa11a3b4a05a97570

Connect EZ 4 / Connect EZ 4i

SHA-1:

60571448d09cfac38337df7093390b135a89f649

SHA-512:

08aa6139a139485ef406acf8bcfd82d2f6ca8423b7c97688c437345dc9a499c62b907435d8cd2e0172b3f37be1b2f6ea15f09a772aec6485c463703e05087f9f

This is the initial release of the Connect EZ family of products.

FEATURES

None

ENHANCEMENTS

None

BUG FIXES

None

SECURITY FIXES

None