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

Digi IX Firmware Release Notes
Version 24.9.79.161 (December 2024)

INTRODUCTION

This is a firmware release for the Digi IX products.

SUPPORTED PRODUCTS

- Digi IX10
- Digi IX20/IX20W
- Digi IX30
- Digi IX40

IMPORTANT INFORMATION

Upgrading to the 24.9.79.151 or later firmware
When upgrading to **24.9.79.151** or later firmware, the device must be running either the **24.6.17.54** or **24.6.17.69** or later firmware first.

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]
- Due to changes in the firewall, it is currently not possible to bridge traffic from devices connected on an Ethernet port or Wi-Fi AP in a bridged interface to a remote IP device via a gateway connected to an Ethernet port in the same bridged interface. [DAL-9799]

UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you deploy 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 for automated device updates. For more information, see the Digi Remote Manager User Guide.

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

1. Log into the Web UI.
2. Navigate to the **System > Firmware Update** page.
3. Click on the **Download from Server** tab.
4. Select the appropriate firmware version.
5. Click **UPDATE FIRMWARE**.
6. The device will automatically reboot once the firmware update is complete.

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 devices 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 on when to apply the firmware update must be made by the customer after appropriate review and validation.

Primary Responder (PR) Support

From the 23.12.1.56 release, the IX20 and IX20W Primary Responder devices can now use the standard IX20 and IX20W firmware releases which support a Primary Responder (PR) mode.

To update your PR device, you must first update it to the **23.9.20.67** PR firmware release and then update to the 23.12.1.56 firmware or later.

The PR mode should be auto-enabled when the device is updated.

VERSION 24.9.79.161 (December 2024)

This is a **recommended** release.

Firmware	sha512sum	md5sum
IX10-24.9.79.161.bin	59c9ebfcb46805c4af0c4e25ba4b6610675b9e61f282e6cd14a2163eea596b4715060396b9bd71aabc837cf72fde0b5affca0e7e3f782f6c06058c73026142fb	6c670149361747050a0291a5e7959e36
IX20-24.9.79.161.bin	6af68bbd2762d4e1d4a8d14dc41e4257c29bcbfb6b9ff9228f95e06640dd7d208bfecf91f94d38e96fc73625fa46aecf43d571f32b729b7adc6a29c541a3f91f	be968b6c10a3a4b57e083f984f8c0289
IX20W-24.9.79.161.bin	bc46270dbc623f7508e644a7208df5282fd0becd178b972189b31fa04ad3705173c269e1cb87c8d8f8e71366097c684f1538a73189c2d4845180379458f5b803	6f8d1b1a76b682423ef7712cc5185407
IX30-24.9.79.161.bin	69aeb9dbbc16c4b1b9d1763b177b31644da022294f4911ddb9d636297db5509d3a54cf8af09973ae0a7664715897d2f027f65b33f5b093aaa318f4eeedf3b022	a15599a5c88c457415f1340bdaaf596c
IX40-24.9.79.161.bin	89bba0f70010f3da96d52d7acaf22851e98ef92d0e75a471e13e63942b5217babc3c991394119c904cabf802fe01ebb30c9753504e68f5727f658a5bf829cace	782c689e2b44f6f06ef4f921eef3913a

BUG FIXES

1. An issue where the device would not connect to Digi Remote Manager if it is not able to sync it's system time with a NTP server, or through the cellular modem or GNSS has been resolved. [DAL-10564]
2. An issue with the IX10 IPv4 Hybrid Addressing mode where the device would not provide an IPv4 address when in DHCP/LAN mode has been resolved. [DAL-10509]
3. The size limit for configuration lists being uploaded to Digi Remote Manager has been increased from 100 to 300. [DAL-10481]

VERSION 24.9.79.151 (November 2024)

This is a **mandatory** release.

Firmware	sha512sum	md5sum
IX10-24.9.79.151.bin	e0a67ceb6e0c469b10dd48ba7503fa028e039af3aaa5bb2d205db5f21409e6e4cc54207188d71deccc53e212ba9ca5e3f82cc241b31916b789c7e7c0e41f1dec	51b9907a5ab720ed57ce0a302031d941
IX20-24.9.79.151.bin	8fb3df2e2938f94b007c3b7a81a57eea82e5dbb7cea8ff2791e68472d01fde564aa859bd681a72ac6baa9a293e872712adcb25aaf6465ad33fa1c7114a9bd89b	60dabf1ef0017c847922554ff30aae72
IX20W-24.9.79.151.bin	18f73ae852a7d76f7c72b2b63a99c889203ce008ce93c6a10a17fd598863f1779e6f45eb737caea4f0f565c3f4e9e2fa27fe24d7b54b87d56d958925c79c8312	5684128f7816d382077f1d2a70586c67
IX30-24.9.79.151.bin	b6797a6205e0b4df18f5f6a5d1c627b65218d21a44fbeef76b01d374f6477e43f594ca4becfe051e6c1d150b6037747506cef4622f2390ce98423768459a7ef9	d5b799914e2500d2d2e285b3f82cb9cd
IX40-24.9.79.151.bin	1392e6dc7de9d878c5e3da2585fdf6049c4b26903c57d337a66d6cb8d2fc6cf8a09a9126fcc940381c8d35bb12e759d4f70fdad9ce7df56476f24013ead5f0dd	0a98f51c628d66294a8930befeb72e2a

NEW FEATURES

1. Support for **encrypted firmware images** has been added

   In order to update to the 24.9.79.151 or later firmware, the device must be running either the 24.6.17.54, 24.6.17.56 or 24.6.17.69 firmware.

2. Support for a new asynchronous Query State mechanism has been added to allow the device to push detailed status information to Digi Remote Manager for the following functional groups:
   - System
   - Cloud
   - Ethernet
   - Cellular
   - Interface
3. A new Configuration Rollback feature when configuring the device using Digi Remote Manager has been added. With this rollback feature, if the device loses its connection with Digi Remote Manager due to a configuration change, it will roll back to its previous configuration and reconnect to Digi Remote Manager.

ENHANCEMENTS

1. The **defaultip** and **defaultlinklocal** interfaces have been renamed to **setupip** and **setuplinklocal** respectively.

   The **setupip** and **setuplinklocal** interfaces can be used to initial connect to and do initial configuration using a common IPv4 192.168.210.1 address.
2. The cellular support has been updated to default to use CID 1 instead of 2. The device will check for a saved CID for the SIM/Modem combination before using the default CID so that existing connected device are unaffected.
3. The configuration support has been updated so that the user must re-enter their original password when changing their password.
4. Support for configuring a custom SST 5G slicing option has been added.
5. The Wireguard support has been updated on the Web UI to have a button to create peer configurations.
6. The **system factory-erase** CLI command has been updated to prompt the user to confirm the command.

   This can overridden using the **force** parameter.
7. The **Python config module** has been updated to allow configuration items to created and deleted.
8. Support for configuring TCP timeout values has been added. The new configuration is under the Network > Advanced menu.
9. Support for displaying a message for users not using 2FA when logging in when **PrimaryResponder** mode is enabled has been added.
10. The email notification support has been updated to allow the notifications to be sent to a SMTP server using no authentication.

11. The **Ookla Speedtest** support has been updated to include the cellular statistics when the test is run over a cellular interface.
12. Support for displaying the 5G NCI (NR Cell Identity) status in DRM, Web UI and CLI has been added.
13. The CLI and Web UI Serial page has been updated to allow the user to set sequential IP port numbers for SSH, TCP, telnet, UDP services on multiple serial ports.
14. The modem logging has been updated to log the APN instead of the index and remove other unnecessary log entries.
15. The way the watchdog calculates the amount of memory that is being used has been updated.
16. The title and description for the password_pr parameter has been updated to help distinguish it from the password parameter.

SECURITY FIXES

1. The Linux kernel has been updated to v6.10 [DAL-9877]
2. The OpenSSL package has been updated to v3.3.2 [DAL-10161]
   CVE-2023-2975 CVSS Score: 5.3 Medium
3. The OpenSSH package has been updated to v9.8p1 [DAL-9812]
   CVE-2024-6387 CVSS Score: 8.1 High
4. The ModemManager package has been updated to v1.22.0 [DAL-9749]
5. The libqmi package has been updated to v1.34.0 [DAL-9747]
6. The libmbim package has been updated to v1.30.0 [DAL-9748]
7. The pam_tacplus package has been updated to v1.7.0 [DAL-9698]
   CVE-2016-20014 CVSS Score: 9.8 Critical
   CVE-2020-27743 CVSS Score: 9.8 Critical
   CVE-2020-13881 CVSS Score: 7.5 High
8. The linux-pam package has been updated to v1.6.1 [DAL-9699]
   CVE-2022-28321 CVSS Score: 9.8 Critical
   CVE-2010-4708 CVSS Score: 7.2 High
9. The pam_radius package has been updated to v2.0.0 [DAL-9805]
   CVE-2015-9542 CVSS Score: 7.5 High
10. The unbound package has been updated to v1.20.0 [DAL-9464]
    CVE-2023-50387 CVSS Score: 7.5 High
11. The libcurl package has been updated to v8.9.1 [DAL-10022]
    CVE-2024-7264 CVSS Score: 6.5 Medium
12. The GMP package has been updated to v6.3.0 [DAL-10068]
    CVE-2021-43618 CVSS Score: 7.5 High
13. The expat package has been updated to v2.6.2 [DAL-9700]
    CVE-2023-52425 CVSS Score: 7.5 High
14. The libcap package has been updated to v2.70 [DAL-9701]
    CVE-2023-2603 CVSS Score: 7.8 High

15. The libconfuse package has been updated with latest patches. [DAL-9702]
    CVE-2022-40320 CVSS Score: 8.8 High
16. The libtirpc package has been updated to v1.3.4 [DAL-9703]
    CVE-2021-46828 CVSS Score: 7.5 High
17. The glib package has been updated to v2.81.0 [DAL-9704]
    CVE-2023-29499 CVSS Score: 7.5 High
    CVE-2023-32636 CVSS Score: 7.5 High
    CVE-2023-32643 CVSS Score: 7.8 High
18. The protobuf package has been updated to v3.21.12 [DAL-9478]
    CVE-2021-22570 CVSS Score: 5.5 Medium
19. The dbus package has been updated to v1.14.10 [DAL-9936]
    CVE-2022-42010 CVSS Score: 6.5 Medium
    CVE-2022-42011 CVSS Score: 6.5 Medium
    CVE-2022-42012 CVSS Score: 6.5 Medium
20. The lxc package has been updated to v6.0.1 [DAL-9937]
    CVE-2022-47952 CVSS Score: 3.3 Low
21. The Busybox v1.36.1 package has been patched to resolve a number of CVEs. [DAL-10231]
    CVE-2023-42363 CVSS Score: 5.5 Medium
    CVE-2023-42364 CVSS Score: 5.5 Medium
    CVE-2023-42365 CVSS Score: 5.5 Medium
    CVE-2023-42366 CVSS Score: 5.5 Medium
22. The Net-SNMP v5.9.3 package has been updated to resolve a number of CVEs.
    CVE-2022-44792 CVSS Score: 6.5 Medium
    CVE-2022-44793 CVSS Score: 6.5 Medium
23. **SSH support** is now disabled by default for devices that have Primary Responder support enabled. [DAL-9538]
24. Support for **TLS compression** has been removed. [DAL-9425]
25. The Web UI session token is now expired when the user logs out. [DAL-9539]
26. The device's MAC address has been replaced with the serial number in the Web UI login page title bar. [DAL-9768]

BUG FIXES

4. An issue where the same ICCID was being reported for both SIM1 and SIM2 has been resolved. [DAL-9826]
5. An issue where the 5G band information was not being displayed on the IX40 has been resolved. [DAL-8926]
6. The system > schedule > reboot_time parameter has been updated to be a full parameter and can now be configured via Digi Remote Manager. Previously it was an alias parameter which can be configured by Digi Remote Manager. [DAL-9755]
7. An issue where a device could get stuck using a particular SIM slot even though no SIM was detected has been resolved. [DAL-9828]
8. An issue where US Cellular would be displayed as the carrier when connected to Telus has

been resolved. [DAL-9911]

9. An issue where an invalid status could be returned to Digi Remote Manager when doing a cellular modem firmware update has been resolved. [DAL-10382]
10. An issue where 2 Ethernet ports were being displayed by Digi Remote Manager for the IX10 platform has been resolved. [DAL-9913]
11. An issue with Wireguard where the public key generated using the Web UI not being saved correctly when has been resolved. [DAL-9914]
12. An issue where IPsec tunnels disconnected when old SAs were being deleted has been resolved. [DAL-9923]
13. An issue where starting BGP would cause an error to be output on the Console port has been resolved. [DAL-10062]
14. An issue where a serial bridge would fail to connect when FIPS mode was enabled has been resolved. [DAL-10032]
15. An issue where the serial port could stall when changing the setting of a serial port has been resolved. [DAL-5230]
16. An issue where a firmware update file downloaded from Digi Remote Manager could cause the device to disconnect to more than 30 minutes has been resolved. [DAL-10134]
17. An issue with the RealPort support on the IX40 has been resolved. [DAL-10224]
18. An issue with the SystemInfo group in the Accelerated MIB not being indexed correctly has been resolved. [DAL-10173]
19. The Deutsche Telekom 26202 PLMN ID and 894902 ICCID prefix have been added to ensure the correct Provider FW is displayed. [DAL-10212]
20. The help text for the Hybrid Addressing mode has been updated to indicate that the IPv4 address mode needs to be configured to either Static or DHCP. [DAL-9866]
21. An issue where the default values for boolean parameters where not being displayed in the Web UI has been resolved. [DAL-10290]
22. An issue with validating configuration changes made by a custom script have been resolved. [DAL-10450]
23. An issue preventing read-only users from running the **show surelink** or **event list** CLI commands has been resolved. [DAL-10418]
24. An issue where a blank APN was being written in mm.json file has been resolved. [DAL-10285]
25. An issue where the watchdog would incorrectly reboot the device when the memory warning threshold is exceeded has been resolved. [DAL-10286]
26. An issue where the IX20W had significantly slowed down has been resolved. [DAL-10182]
27. The Python live image has been updated to include the libsqlite3.so library which is required by the Python sqlite3 module. [DAL-9661]

VERSION 24.6.17.69 (September 2024)

This is a **mandatory** patch release.

Firmware	sha512sum	md5sum
IX10-24.6.17.69.bin	0054ca5b04f3e6900f77313f5c1f81c7d058e4535e88c5	3694ed0dced19312547fac8342a794ea

	43e3beb48e7efed94f9b16b2f98d47eee00f1cd133ff2a296eb3bbe1561925e70514e2393f642c9424	
IX20-24.6.17.69.bin	c4d2b27e5fb4cc6b376389224b18ed5269ddf407beb5fe5fca495101874909f28fad2bbcfa36ad78d4893a8324f57607164a2cb1463a0b98b7cdeb4690f91a0f	d65c1fabe853207cccb31955e5981b8a
IX20W-24.6.17.69.bin	d3a5fbc695017bf596251fbef4aa24af3bbe1ad6f1df6147c9c6ebba5a71d1631e09961101a97e4bc966bb7f6feae1eb80c635b470529647d123c216e7412f6d	d777eae761c1e7a594bc953174615602
IX30-24.6.17.69.bin	eb33933c54c59720a6c9d38f0e451342cce4579ad8c5625eef45e9396778e19a2fdc4aca08422ea452e80ab982ce0a1d14138d757a5c72d874451fc954f32c65	c364cff388d9ccf77ed9ea6542e8fc1d
IX40-24.6.17.69.bin	b62923d02b198665c70eb8b1e0b49115df11881339d18610907559c8be0b16a317a6983e69c5c3933ed326ffc5d548d18d205a5e88a610a6b7135ffb02d9ed7d	40f30418c3c6faf8f0f6772fe12520f4

BUG FIXES

1. An issue that prevented IPsec tunnels that use IKEv2 from re-keying has been resolved. This was introduced in the 24.6.17.56 release. [DAL-9959]
2. An issue where the device would revert to a saved custom default configuration (using the custom-default-config.bin file) when a device was updated to DAL 23.9 or later has been resolved. [DAL-9970]
3. Some SureLink changes that were causing SIM failover issues in the 24.6.17.54 release have been removed. [DAL-9570, DAL-9592, DAL-9666, DAL-9828]

VERSION 24.6.17.54 / 24.6.17.56 (June 2024)

This is a **mandatory** release.

Firmware	sha512sum	md5sum
IX10-24.6.17.56.bin	2549ef2777139db0a164d88f2a4a7b0c5203ad8419b5b8aa84529874f25cfd556464321371c65fbec48e7bcb2c17efc80a64b59ab701ae0ad49cc2c863b820ad	05d64c3e3b1974d17fc50e57ba8d7c95
IX20-24.6.17.54.bin	22b5b72b9062cb08705ce0ddd81d29ec36b6e28f007d5708b4eb91a6c0aeaadedddcf7406ac9a47f38827e14249f03167d3d0cf3ee16f02a9ad2d8c71751524a	2f31c65c200456e13b63bed5e04535f3
IX20W-24.6.17.54.bin	cb11040195e5bfcdaa7134579277466e5d113cf4cbc113f4722406f0795af5aaefddc8538d4022b5001ba1d5d09c22f7af3310fbbae6a7bdc99218ebf25cbc3c	23ae535fd5d0d2846b7ceec20ca12430
IX30-24.6.17.54.bin	79d31c9ae3a83d0a1ec2e316d00cc5486bf2c2c60c0d408c8a565bc52d9e4aaa20037075afde971442cd13d958fffd15e6a44c5c886a2c56d702ba2a281edd55	0a51ef3dd95a0a6848f22f6fb09aa4e7
IX40-24.6.17.54.bin	426d11c2a447d742b42de59faebf65a2f5b0095d30efc646b4436f51bacd1bce0aa5a12c837c374f3f78125fa4d37fd6d42801e70a2f46f34e17c570293b16c4	f3bc0be4bbf5a90e3dc5b84860d0aae0

NEW FEATURES

1. Hybrid IPv4 addressing mode support added for the IX10 Ethernet interface.

   In this mode, the device will first attempt to get an IPv4 address using DHCP. If it fails to get an IPv4 address after 1 minute, it will revert to using the static configured IPv4 address.
   This allows the IX10 (when running default configuration) to automatically connect to and be managed by Digi Remote Manager when connected into a network that supports DHCP.

The addressing type must be changed to either dhcp or static when the first configuration change is made on the device.

ENHANCEMENTS

1. The **WAN-Bonding** support has been enhanced with the following updates
    a. SureLink support.
    b. Encryption support.
    c. SANE client has been updated to 1.24.1.2.
    d. Support for configuring multiple WAN Bonding servers.
    e. Enhanced status and statistics.
    f. The WAN Bonding status is now included in the metrics sent to Digi Remote Manager.
2. The **cellular** support has been enhanced with the following updates
    a. The cellular connection back-off algorithm has been removed as the cellular modems have built-in back off algorithms that should be used.
    b. The cellular APN lock parameter has been changed to APN selection to allow the user to select between using the built-in Auto-APN list, the configured APN list or both.
    c. The cellular Auto-APN list has been updated.
    d. The MNS-OOB-APN01.com.attz APN has been removed from the Auto-APN fallback list.
3. The **Wireguard** support has been updated to allow the user to generate a client configuration that can be copied onto another device.

    This is done using the command wireguard generate <tunnel> <peer>

    Extra information may be needed from the client depending on config:
    a. How the client machine connects to the DAL device. This is needed if the client is initiating any connections and there is no keepalive value.
    b. If the client generates their own private/public key, they will need to set add that to their configuration file.

    If this is used with 'Device managed public key', every time a generate is called on a peer, a new private/public key is generated and set for that peer, this is because we do not store any private key information of any clients on the device.
4. The SureLink support has been updated to
    a. Shutdown the cellular modem before power cycling it.
    b. Export the INTERFACE and INDEX environment variables so that they can be used in custom action scripts.
5. The uploading of device events to Digi Remote Manager has been enabled by default.
6. The logging of SureLink events has been disabled by default as it was causing the event log to be saturated with test pass events.

    SureLink messages will still appear in the system message log.
7. The **show surelink** command has been updated.
8. The status of the System Watchdog tests can now be obtained via Digi Remote Manager, the Web UI and using CLI command show watchdog.
9. The Speedtest support has been enhanced with the following updates
    a. To allow it to run on any zone with src_nat enabled.
    b. Better logging when a Speedtest fails to run.

10. The Digi Remote Manager support has been updated to only re-establish connection to Digi Remote Manager if there is a new route/interface it should utilize to get to Digi Remote Manager.
11. A new configuration parameter, **system > time > resync_interval**, has been added to allow the user to configure the system time resynchronization interval.
12. Support for USB printers has been enabled. It is possible to configure to device to listen for printer requests via the socat command
    ```
    socat - u tcp-listen:9100,fork,reuseaddr OPEN:/dev/usblp0
    ```
13. The SCP client command has been updated with a new legacy option to use the SCP protocol for file transfers instead of the SFTP protocol.
14. The IX30 analog IO calibration data has been removed from configuration backups.
15. Serial connection status information has been added to the Query State response message that is sent to Digi Remote Manager.
16. Duplicate IPsec messages have been removed from the system log.
17. The debug log messages for the health metrics support have been removed.
18. The help text for the FIPS mode parameter has been updated to warn the user the device will automatically reboot when changed and that all configuration will be erased if disabled.
19. The help text for the SureLink delayed_start parameter has been updated.
20. Support for the Digi Remote Manager RCI API compare_to command has been added.

SECURITY FIXES

1. The setting for **Client isolation on Wi-Fi Access Points** has been changed to be enabled by default. [DAL-9243]
2. The **Modbus** support has been updated to support the Internal, Edge and Setup zones by default. [DAL-9003]
3. The Linux kernel has been updated to 6.8. [DAL-9281]
4. The StrongSwan package has been updated to 5.9.13 [DAL-9153]

   CVE-2023-41913 CVSS Score: 9.8 Critical
5. The OpenSSL package has been updated to 3.3.0. [DAL-9396]
6. The OpenSSH package has been updated to 9.7p1. [DAL-8924]

   CVE-2023-51767 CVSS Score: 7.0 High

   CVE-2023-48795 CVSS Score: 5.9 Medium
7. The DNSMasq package has been updated to 2.90. [DAL-9205]

   CVE-2023-28450 CVSS Score: 7.5 High
8. The udhcpc package has been updated to resolve a CVE issue. [DAL-9202]

   CVE-2011-2716 CVSS Score: 6.8 Medium
9. The c-ares package has been updated to 1.28.1. [DAL9293-]

   CVE-2023-28450 CVSS Score: 7.5 High
10. The jerryscript package has been updated to resolve a number CVEs.

    CVE-2021-41751 CVSS Score: 9.8 Critical

    CVE-2021-41752 CVSS Score: 9.8 Critical

    CVE-2021-42863 CVSS Score: 9.8 Critical

CVE-2021-43453 CVSS Score: 9.8 Critical

CVE-2021-26195 CVSS Score: 8.8 High

CVE-2021-41682 CVSS Score: 7.8 High

CVE-2021-41683 CVSS Score: 7.8 High

CVE-2022-32117 CVSS Score: 7.8 High

11. The AppArmor package has been updated to 3.1.7. [DAL-8441]
12. The following iptables/netfilter packages have been updated [DAL-9412]
    a. nftables 1.0.9
    b. libnftnl 1.2.6
    c. ipset 7.21
    d. conntrack-tools 1.4.8
    e. iptables 1.8.10
    f. libnetfilter_log 1.0.2
    g. libnetfilter_cttimeout 1.0.1
    h. libnetfilter_cthelper 1.0.1
    i. libnetfilter_conntrack 1.0.9
    j. libnfnetlink 1.0.2
13. The following packages have been updated [DAL-9387]
    a. libnl 3.9.0
    b. iw 6.7
    c. strace 6.8
    d. net-tools 2.10
    e. ethtool 6.7
    f. MUSL 1.2.5
14. The http-only flag is now being set on Web UI headers. [DAL-9220]

BUG FIXES

1. The **WAN Bonding** support has been updated with the following fixes
    a. The client is now automatically restarted when client configuration changes are made. [DAL-8343]
    b. The client is now automatically restarted if it has stopped or crashed. [DAL-9015]
    c. The client is now not restarted if an interface goes up or down. [DAL-9097]
    d. The sent and receive statistics has been corrected. [DAL-9339]
    e. The link on the Web UI dashboard now takes the user to the Web-Bonding status page instead of the configuration page. [DAL-9272]
    f. The CLI show route command has been updated to show the WAN Bonding interface. [DAL-9102]
    g. Only the required ports rather than all ports are now opened in the firewall for incoming traffic in the Internal zone. [DAL-9130]
    h. The show wan-bonding verbose command has been updated to comply with style requirements. [DAL-7190]

i. Data was not being sent through the tunnel due to an incorrect route metric. [DAL-9675]
j. The show wan-bonding verbose command. [DAL-9490, DAL-9758]
k. Reduced memory usage that causes issues on some platforms. [DAL-9609]

2. The **SureLink** support has been updated with the following fixes
    a. An issue where re-configuring or remove static routes could cause routes being incorrectly added to the routing table has been resolved. [DAL-9553]
    b. An issue where static routes were not being updated if the metric was configured as 0 has been resolved. [DAL-8384]
    c. An issue where the TCP test to a hostname or FQDN can fail if the DNS request goes out of the wrong interface has been resolved. [DAL-9328]
    d. An issue where disabling SureLink after an update routing table action leaves orphaned static routes has been resolved. [DAL-9282]
    e. An issue where the show surelink command displaying incorrect status has been resolved. [DAL-8602, DAL-8345, DAL-8045]
    f. An issue with SureLink being on enabled on LAN interfaces causing issues with tests being run on other interfaces has been resolved. [DAL-9653]
3. An issue where IP packets could be sent out of the wrong interface, including those with private IP addresses which could lead to being disconnected from the cellular network has been resolved. [DAL-9443]
4. The SCEP support has been updated to resolve an issue when a certificate has been revoked. It will now perform a new enrollment request as the old key/certificates are no longer considered secure to perform a renewal. Old revoked certificates and keys are now removed from the device. [DAL-9655]
5. An issue with IX40 5G units outside of North America selecting an incorrect generic cellular firmware image has been resolved. [DAL-9266]
6. An issue with the IX40 5G modem VoLTE and SIM hotswap settings being re-enabled after a carrier switch which resulted in longer connection times. [DAL-9264, DAL-9265]
7. An issue with the IX20W Wi-Fi connecting to Access Points using DFS channels with the DAL 24.3 release has been resolved. [DAL-8933]
8. An issue with how OpenVPN generated in server certificates has been resolved. [DAL-9750]
9. An issue with IX10 SIM LEDs behavior has been resolved. [DAL-9593]
10. An issue where Digi Remote Manager would continue to display a device as connected if it had been booted locally has been resolved. [DAL-9411]
11. An issue with SureLink on IPsec tunnels using strict routing has been resolved. [DAL-9784]
12. A race condition when an IPsec tunnel is brought down and reestablished quickly could prevent the IPsec tunnel coming up has been resolved. [DAL-9753]
13. An issue when running multiple IPsec tunnels behind the same NAT where only interface could come up has been resolved. [DAL-9341]
14. An issue with IP Passthrough mode where the cellular interface would be brought down if the LAN interface goes down which meant the device was no longer accessible via Digi Remote Manager has been resolved. [DAL-9562]
15. An issue with multicast packets not being forwarded between bridge ports has been resolved.

This issue was introduced in DAL 24.3. [DAL-9315]

16. An issue where an incorrect Cellular PLMID was being displayed has been resolved. [DAL-9315]
17. An issue with the RSTP support where it may initialize correct in some configurations has been resolved. [DAL-9204]
18. An issue where a device would attempt to upload the maintenance status to Digi Remote Manager when it is disabled has been resolved. [DAL-6583]
19. An issue with the Web UI drag and drop support which could cause some parameters being incorrectly updated has been resolved. [DAL-8881]
20. An issue with the Serial RTS toggle pre-delayed not being honored has been resolved. [DAL-9330]
21. An issue with the Watchdog triggering a reboot when not necessary has been resolved. [DAL-9257]
22. An issue where modem firmware updates would fail due to the index of the modem changing during the update and the status result not being reported to Digi Remote Manager has been resolved. [DAL-9524]
23. An issue with the cellular modem firmware update on Sierra Wireless modems has been resolved. [DAL-9471]
24. An issue with how the cellular statistics were being reported to Digi Remote Manager has been resolved. [DAL-9651]

VERSION 24.3.28.88 (March 2024)

This is a **mandatory** release.

Firmware	sha512sum	md5sum
IX10-24.3.28.88.bin	6ac41d4e94421bb03861987e8031a4367ddd497d7a7db0599bce28b53d21f130ac1314080c34b8c31da3dcc1a168bd57d9490ae2db35d1f7386f2c6f9a156712	c2edb9578c5f652f84528812a1769263
IX20-24.3.28.88.bin	c008edba922020029839ae9d3cc6bbb7475972b0718f70dcb4b492f45ace665aea6619a5cc23ebeda5398ae357006c1c328339de9c1c99bb9d6a480df73f4570	92a2984b76354ddc44dfcbb6fc24c070
IX20W-24.3.28.88.bin	0ebbd1cdc8cb8303f1699c4137c6d08e3a47fe3469c60794ab89b3d16c0dea01e694b376ae1a49be69fe5ce1ea2a0121aec1051dbe06a6642abc2ba46de59d4d	b45823bb4280055d413c4647dc5c275d
IX30-24.3.28.88.bin	06a0634944fa722009be679c72605f71f0edbda7e267d7a0a86d273c855a38c3b130cc7667bcd088d1d1bb077f240469bfa6f6fde0dd4024fa06a1e152710290	1373a8da46e6bce0aa009ec407c8bdd1
IX40-24.3.28.88.bin	b9ef6efb6756907c9bca288813ccb0f48c4f0842061df6b2960c5728d2fcccbb652c7d32374d78bf176b4859b232a9cf61bf96013e085535e94c9ac699a62ad1	0ce35c9fb7ee332e2c5d42614d68d0b0

NEW FEATURES

1. Support for **WireGuard** VPNs has been added.
2. Support for a new **Ookla based speed test** has been added.

   Note: This is a Digi Remote Manager exclusive feature.
3. Support for **GRETap** Ethernet tunneling has been added.

ENHANCEMENTS

1. The **WAN Bonding** support has been updated
    a. Support for a WAN Bonding backup server has been added.
    b. The WAN Bonding UDP port is now configurable.
    c. The WAN Bonding client has been updated to 1.24.1
2. Support for configuring which **4G** and **5G cellular bands** can and cannot be used for a cellular connection has been added.

    Note: This configuration should be used with care as it could lead to poor cellular performance or even preventing the device from connecting to the cellular network.
3. The **System Watchdog** has been updated to allow for monitoring of interfaces and cellular modems.
4. The **DHCP server support** has been updated
    a. To offer a specific IP address for a DHCP request received on a particular port.
    b. Any requests for the **NTP server** and **WINS server options** will be ignored if the options is configured to **none**.
5. Support for **SNMP traps** to be sent when an event occurs has been added. It can be enabled on a per-event type basis.
6. Support for **Email notifications** to be sent when an event occurs has been added. It can be enabled on a per-event type basis.
7. A button has been added to the Web UI **Modem Status** page to update the modem to the latest available modem firmware image.
8. The OSPF support has been updated to add the capability to link OSPG routes through a DMVPN tunnel. There are two new configuration options
    a. A new option has been added to **Network > Routes > Routing services > OSPFv2 > Interfaces > Network type** to specify the network type as a DMVPN tunnel.
    b. A new Redirect setting has been added to **Network > Routes > Routing services > NHRP > Network** to allow redirection of packets between spokes.
9. The location service has been updated
    a. To support an interval_multiplier of 0 when forwarding NMEA and TAIP messages. In this case, the NMEA/TAIP messages will be forwarded immediately rather than caching and waiting for the next interval multiple.
    b. To only display the NMEA and TAIP filters depending on the select type.
    c. To display the HDOP value in Web UI, **show location** command and in the metrics pushed up to Digi Remote Manager.
10. A configuration option has been added to the Serial interface support to disconnect any active sessions if the serial port DCD or DSR pins are disconnected.

    A new CLI command **system serial disconnect** has been added to support this.

    The Serial status page in the Web UI has also been updated with the option.
11. The Digi Remote Manager keepalive support has been updated to more quickly detect stale connections and so can recover the Digi Remote Manager connection more quickly.
12. The redistribution of connected and static routes by BGP, OSPFv2, OSPFv3, RIP and RIPng has been disabled by default.

13. The **show surelink** command has been updated to have a summary view and an interface/tunnel specific view.
14. The **Web UI serial status page** and the **show serial** command have been updated to display the same information. Previously some information was only available on one or the other.
15. The **LDAP support** has been updated to support a group name alias.
16. Support for connecting a **USB printer** to a device via a USB port has been added. This feature can used via Python or socat to open a TCP port to process printer requests.
17. The default timeout of the Python digidevice cli.execute function has been updated to 30 seconds to prevent command timeouts on some platforms.
18. The Verizon 5G V5GA01INTERNET APN has been added to the fallback list.
19. The help text for modem antenna parameter has been updated to include a warning that it may cause connectivity and performance issues.
20. The help text for the DHCP hostname option parameter has been updated to clarify its use.

SECURITY FIXES

1. The Linux kernel has been updated to version 6.7 [DAL-9078]
2. The Python support has been updated to version 3.10.13 [DAL-8214]
3. The Mosquitto package has been updated to version 2.0.18 [DAL-8811]
   CVE-2023-28366 CVSS Score: 7.5 High
4. The OpenVPN package has been updated to version 2.6.9 [DAL-8810]
   CVE-2023-46849 CVSS Score: 7.5 High
   CVE-2023-46850 CVSS Score: 9.8 Critical
5. The rsync package has been updated to version 3.2.7 [DAL-9154]
   CVE-2022-29154 CVSS Score: 7.4 High
   CVE-2022-37434 CVSS Score: 9.8 Critical
   CVE-2018-25032 CVSS Score: 7.5 High
6. The DNSMasq package has been patched to resolve CVE-2023-28450. [DAL-8338]
   CVE-2023-28450 CVSS Score: 7.5 High
7. The udhcpc package has been patched to resolved CVE-2011-2716. [DAL-9202]
   CVE-2011-2716
8. The default SNMP ACL settings have been updated to prevent access via External zone by default if the SNMP service is enabled. [DAL-9048]
9. The netif, ubus, uci, libubox packages have been updated to OpenWRT version 22.03 [DAL-8195]

BUG FIXES

1. The following **WAN Bonding** issues have been resolved
   a. The WAN Bonding client is not restarted if the client stops unexpectedly. [DAL-9015]
   b. The WAN Bonding client was being restarted if an interface went up or down. [DAL-9097]
   c. The WAN Bonding interface staying disconnected if a cellular interface cannot connect. [DAL-9190]
   d. The **show route** command not displaying the WAN Bonding interface. [DAL-9102]

    e. The **show wan-bonding** command displaying incorrect interface status. [DAL-8992, DAL-9066]
    f. Unnecessary ports being opened in the firewall. [DAL-9130]
    g. An IPsec tunnel configured to tunnel all traffic whilst using a WAN Bonding interface causing the IPsec tunnel to not pass any traffic. [DAL-8964]
2. An issue where **data metrics** being uploaded to Digi Remote Manager being lost has been resolved. [DAL-8787]
3. An issue that caused **Modbus RTUs** to unexpectedly timeout has been resolved. [DAL-9064]
4. An **RSTP** issue with the bridge name lookup has been resolved. [DAL-9204]
5. An issue with the GNSS active antenna support on the IX40 4G has been resolved. [DAL-7699]
6. The following issues with cellular status information have been resolved
    a. Cellular signal strength percentage not being reported correctly. [DAL-8504]
    b. Cellular signal strength percentage being reported by the /metrics/cellular/1/sim/signal_percent metric. [DAL-8686]
    c. The 5G signal strength being reported for the IX40 5G devices. [DAL-8653]
7. The following issues with the SNMP Accelerated MIB have been resolved
    a. The cellular tables not working correct on devices with cellular interfaces not called “modem” has been resolved. [DAL-9037]
    b. Syntax errors that prevented if from being correctly parsed by SNMP clients. [DAL-8800]
    c. The runtValue table not being correctly indexed. [DAL-8800]
8. The following PPPoE issues have been resolved
    a. The client session was not being reset if the server goes away has been resolved. [DAL-6502]
    b. Traffic stopping being routed after a period of time. [DAL-8807]
9. An issue with the DMVPN phase 3 support where firmware rules needed to the disabled in order to honor default routes inserted by BGP has been resolved. [DAL-8762]
10. An issue with the DMVPN support taking a long time to come up has been resolved. [DAL-9254]
11. The Location status page in the Web UI has been updated to display the correct information when the source is set to user-defined.
12. An issue with the Web UI and **show cloud** command displaying an internal Linux interface rather than the DAL interface has been resolved. [DAL-9118]
13. An issue with the IX40 5G antenna diversity which would cause the modem to go into a “dump” state has been resolved. [DAL-9013]
14. An issue where devices using a Viaero SIM could not connect to 5G networks has been resolved. [DAL-9039]
15. An issue with the SureLink configuration migration resulting some blank settings has been resolved. [DAL-8399]
16. An issue where configuration was been committed at boot-up after an update has been resolved. [DAL-9143]
17. The **show network** command has been corrected to always display the TX and RX bytes values.

18. The NHRP support has been updated to not log messages when disabled. [DAL-9254]

VERSION 23.12.1.61 (January 2024)

This is a **recommended** release.

Firmware	sha512sum	md5sum
IX10-23.12.1.61.bin	98c83baadd505f93a07f25e5c9e26fea53dbab142a643938635ce2c3b62d69414ea4c6a493ab1a8885e165829bcd6df20066d8f8bd944e82f956b9e3dc688875	d3f9f103122f2633d9074ee6de625ccd
IX20-23.12.1.61.bin	193cf424e44caf61f8ce654bde1a43b12f97a1d4b7e60805e296910467d021986bc937bd6565366c8a7e08a9d37d9813a8700b0f659bde85681ca42c2de09128	65d4909efc3740cba6217610e1d5ebdf
IX20W-23.12.1.61.bin	a7014afba718ab0758b7d203fcc6b5ace2401ce3ae86ca6a853476a4821d7c321f066248b9b8670bc09f643797c5811613669a05302a10ac07a01f15a4d30676	b6058b3ef4d092c4f143e9a69eff8fde
IX30-23.12.1.61.bin	7353d631602e9ddcca54a2c6520d924d5f32491e566d63dc1575103946988d418dc59cd82797eef8f4a0113edfa549687648a410ab1062983b7fa40e32e75c03	eb7c656baf99572e028aafe60810fccb
IX40-23.12.1.61.bin	14903c3f8c743c74f1aea9aac5857b9fcb11e7fd909a685486ad45397de2bfeb8c154649d6ab7fc47f1dc3b950d318bc36aed85a73f1899261c0c31e8c1f5955	097fdbc8d0f05097d3f1c3b020ba197f

NEW FEATURES

There are no new features in this release.

ENHANCEMENTS

There are no enhancements in this release.

SECURITY FIXES

There are no security fixes in this release.

BUG FIXES

1. An issue where an incorrect WAN Bonding status was being reported via the Web UI has been resolved. [DAL-8892]
2. The ITxPT GNSS version has been corrected to be v2.2.1. [DAL-8972, DAL-8990]

VERSION 23.12.1.56 (December 2023)

This is a ***mandatory*** release.

Firmware	sha512sum	md5sum
IX10-23.12.1.56.bin	6c96079d7a5b5480f75ea44dcdb713a7d700b8451045e13cba9e849957694ce66b6a11eb7172de4e6af41560c0fb9f4e725a94db5631fbdc297d442619919654	57a30fba4aa3947fbe1ee16b85417efc
IX20-23.12.1.56.bin	06ba26b7ffe9f4d4a0c31ff963d6e478610135806ffc42f550a9c08ea28e3359ac3a1ff57c7ccce1aa11cb3cc7747c42f86acd4b1caa400510726f5ffa25a025	f8ae68f543828a22dd9fd4c4b65cbab7
IX20W-23.12.1.56.bin	e100230bb2708d63d27ff2d7e8b1e898a3b99c69ffb0	a15fe253c01a506e22225c206acac436

	d0657dbf82dd9a00cdeb28e38e7062b895627c09513 d69d08e70ae04ac784a86c0317b781af3ed55c85f	
IX30-23.12.1.56.bin	fc8d1c971f92efcb8995e1d955921ef4a9472d80efa81 77bd475bc387673bee60e160d99a99e50a81f91d054f 1f417d61f1840d0bd2199aae8941a12a51712b6	ce7db9237812b19aab0e4ed57d1fc5e6
IX40-23.12.1.56.bin	cc6dfd2ffb9c36234825d4e8ad0ef0b022d473f26b9cc e1f0795414f29ffd63aaca2ebe2a1b25c7c48126a4975 c10c373cfc201b0ab9f6cbceaefcfdee2dfd96	70a2e70bd543dd6632bdba01797528ac

NEW FEATURES

1. Support for linking OSPF routes through a DMVPN tunnel has been added.
    a. A new configuration option **Point-to-Point DMVPN** has been added to **Network > Routes > Routing services > OSPFv2 > Interface > Network** parameter.
    b. A new configuration parameter **redirect** has been added to the **Network> Routes > Routing services > NHRP > Network** configuration.
2. Support for the **Rapid Spanning Tree Protocol (RSTP)** has been added.
3. Support for **device initiated RealPort** connections has been added.

ENHANCEMENTS

1. A new option **After** has been added to the **Network > Modems Preferred SIM** configuration to prevent a device from switching back to the preferred SIM for the configured amount of time.
2. The **WAN Bonding** support has been updated
    a. New options have been added to the **Bonding Proxy** and **Client devices** configuration to direct traffic from specified network through the internal WAN Bonding Proxy to provide improved TCP performance through the WAN Bonding server.
    b. New options have been added to set the **Metric** and **Weight** of the WAN Bonding route which can be used to control the priority of the WAN Bonding connection over other WAN interfaces.
3. A new DHCP server option to support BOOTP clients has been added. It is disabled by default.
4. The status of Premium Subscriptions has been added the System Support Report.
5. A new object_value argument have been added to the local Web API that can be used to configure a single value object.
6. The SureLink actions **Attempts** parameter has been renamed to the **SureLink Test failures** to better describe its use.
7. A new **vtysh** option has been added to the CLI to allow access to the **FRRouting** integrated shell.
8. A new **RealPort** option has been added to control the minimum TLS version that can be used.
9. A new **modem sms** command has been added to CLI for sending outbound SMS messages.
10. A new **Authentication > serial > Telnet Login** parameter to been added to control whether a user must supply authentication credentials when opening a Telnet connection to direct access a serial port on the device.
11. The OSPF support has been updated to support the setting the Area ID to an IPv4 address or a number.
12. The mDNS support has been updated to allow a maximum TXT record size of 1300 bytes.
13. The migration of the SureLink configuration from 22.11.x.x or earlier releases has been

improved.

14. 5G slicing is now supported on the IX40.
15. A new ***System → Advanced watchdog → Fault detection tests → Modem check and recovery*** configuration setting has been added to control whether the watchdog will monitor the initialization of the cellular modem inside the device and automatically take recovery actions to reboot the system if the modem doesn't initialize properly (enabled by default).

SECURITY FIXES

1. The Linux kernel has been updated to version 6.5 [DAL-8325]
2. An issue with sensitive SCEP details appearing the SCEP log has been resolved. [DAL-8663]
3. An issue where a SCEP private key could be read via the CLI or Web UI has been resolved. [DAL-8667]
4. The musl library has been updated to version 1.2.4 [DAL-8391]
5. The OpenSSL library has been updated to version 3.1.3 [DAL-8447]

   CVE-2023-4807 CVSS Score: 7.8 High

   CVE-2023-3817 CVSS Score: 5.3 Medium
6. The OpenSSH package has been updated to version 9.5p1 [DAL-8448]
7. The curl package has been updated to version 8.4.0 [DAL-8469]

   CVE-2023-38545 CVSS Score: 9.8 Critical

   CVE-2023-38546 CVSS Score: 3.7 Low
8. The frrouting package has been updated to version 9.0.1 [DAL-8251]

   CVE-2023-41361 CVSS Score: 9.8 Critical

   CVE-2023-47235 CVSS Score: 7.5 High

   CVE-2023-38802 CVSS Score: 7.5 High
9. The sqlite package has been updated to version 3.43.2 [DAL-8339]

   CVE-2022-35737 CVSS Score: 7.5 High
10. The netif, ubus, uci, libubox packages have been updated to OpenWRT version 21.02 [DAL-7749]

BUG FIXES

1. An issue with DMVPN that cause NHRP routing through tunnels to Cisco hubs to be unstable has been resolved. [DAL-8668]
2. An issue that prevented the handling of incoming SMS message from Digi Remote Manager has been resolved. [DAL-8671]
3. An issue that could cause a delay in connecting to Digi Remove Manager when booting up has been resolved. [DAL-8801]
4. An issue with MACsec where the interface could fail to re-establish if the tunnel connection was interrupted has been resolved. [DAL-8796]
5. An intermittent issue with the SureLink restart-interface recovery action on an Ethernet interface when re-initializing the link has been resolved. [DAL-8473]
6. An issue that prevented the Autoconnect mode on a Serial port from reconnecting until the timeout had expired has been resolved. [DAL-8564]
7. An issue that prevented IPsec tunnels from being established through a WAN Bonding

interface have been resolved. [DAL-8243]

8. An intermittent issue where SureLink could trigger a recovery action for an IPv6 interface even if no IPv6 tests were configured has been resolved. [DAL-8248]
9. An issue with SureLink custom tests has been resolved. [DAL-8414]
10. An issue with the IX40 5G unit not connecting to the Orange network in France has been resolved. [DAL-8512]
11. An issue with LDAP authentication not working when LDAP is the only configured authentication method has been resolved. [DAL-8559]
12. An issue where local non-admin user passwords were not migrated after enabling Primary Responder mode has been resolved. [DAL-8740]
13. An issue where a disabled interface would show received/sent values of N/A in the Web UI Dashboard has been resolved. [DAL-8427]
14. An issue that prevented users from manually registering some Digi router types with Digi Remote Manager via the Web UI has been resolved. [DAL-8493]
15. An issue where the system uptime metric was reporting an incorrect value to Digi Remote Manager has been resolved. [DAL-8494]
16. An issue that prevented the pulse counter digital input from working if the debounce period was set to a non-zero value has been resolved. [DAL-8891]
17. An issue where Digi Remote Manager would display an incomplete firmware version for the EG25-G modem has been resolved. [DAL-7108]
18. An issue where the IX40 WWAN LED should show an incorrect status for dual-APN configurations has been resolved. [DAL-8439]
19. An intermittent issue with migrating IPsec SureLink setting from devices running 22.11.x.x or earlier has been resolved. [DAL-8415]
20. An issue where SureLink was not reverting the routing metrics when failing back on an interface has been resolved. [DAL-8887]
21. An issue where the CLI and Web UI would not show the correct networking details when WAN Bonding was enabled has been resolved. [DAL-8866]
22. An issue with the show wan-bonding CLI command has been resolved. [DAL-8899]
23. An issue that prevent devices from connecting to Digi Remote Manager over a WAN Bonding interface has been resolved. [DAL-8882]

VERSION 23.9.20.67 (December 2023)

This is a ***recommended*** release.

Firmware	sha512sum	md5sum
IX10-23.9.20.67.bin	561fa1e0e66c5ce71ddd222f2804c12500ab4b0f5d3f02b3debe141dd884c636c2987f6eef124e6793092cca0f13e61165414d2ed36567f572aa2664d97f5df0	8ed907a8821086983aa83d13813f5ee9
IX20-23.9.20.67.bin	0e4e91929c8f866af65539a1c114b6fcf39a234a0ff154d2651ea22349a8c8eabf6a51967bb4bd9e37e66f237eb17108a301e84125118c69e686e68377dd388a	05fdd8dae282d3058185306a4c5cd184
IX20-PR-23.9.20.67.bin	f05afab23a9f196cf3d6edc561530666c481274ed873f	090b5239bdffe1d72f3a31214db1313e

	598131cc0177523e1c2d9ca576919f29a69a767877cde47f63d053fcbc257126e0221847489c1e94a5d	
IX20W-23.9.20.67.bin	54932d73ef3466c6d8407b0a583ce88175076cd6890b3d694c3a1b934875c36baab097fbf1c147b2634bc7aaf5c97d7e9fff6bd0b5e6693a8c4c83091eecb5e0	c62334880985fec0b83a9359774a75e0
IX20W-PR-23.9.20.67.bin	f2576e24a07050ca03582d254f6b9656cda8218f939f96a703c2a676eec252c0546d180bde75bb67cb3ec60c5482ac2408333c6398fd800e9ee38556cad059a4	f59d0a2f3d427ca29d8ed155fa402cd8
IX30-23.9.20.67.bin	98017961d9a40319247643b1c104e0312f188d0241817eaa6c13a93f7044fc9a8f9b87c642278998f5f39304f7cb0fc1f6f4afa392e973281c5b72d7fbd4fdac	aff28c5557ef4872e0fc268205dce40e
IX40-23.9.20.67.bin	20af623ac259f95c8cec964757e21d3e05fb235a50c383c7d06603e28cd26ca6d3a11d81bfadd91a23d15aaa1738eae16243a33a881cbb8c07e73f5c9f093ee4	9c79d5ce95d3b12a7183f82b55a281c5

NEW FEATURES

There are no new features with this release.

ENHANCEMENTS

There are no enhancements with this release.

SECURITY FIXES

There are no security fixes with this release.

BUG FIXES

1. An issue with SureLink which would take the interface out of service with the first test failure if the first action is “Update Routing table” has been resolved. This could cause devices with one WAN interface to unnecessarily it’s lose interface connection. [DAL-8500]

VERSION 23.9.20.63 (October 11, 2023)

This is a ***recommended*** release.

Firmware	sha512sum	md5sum
IX10-23.9.20.63.bin	b3a18197332c4b52ebd5c237ec6811967f5c7859a313fd788ff6f7f381e4128171a79658d92c77e8fc524f968e6fd7fac915189f74dbab62ccea1c86c82d840e	1391ed613f7b9d1fa142bb0c04960461
IX20-23.9.20.63.bin	ee4729525e70c46bb125f233b9cdde77c80346bde0de2d887c38d6ce1be86cbc59279d7eb38fdd076d0a8297c51dd0b74405974626f9d6affb7eacd93973fea5	0fe8b6de83a72ef5321d504f988025a8
IX20-PR-23.9.20.6.bin	e94f11f3019456f6ea544ec5a3e8532bec6d4ac6a4e79b13e892c5f98b86db13cf92fa7801d70ebf2f4dc5eba2e252124b3439848e345cc42249a41f59d2ed7e	27f11d7d686a1b73b8703d6b18c9645c
IX20W-23.9.20.63.bin	6197787b21b5aec6d010d187fbc0b313e77e46c07edf4bd8fb48c138384676851d5e7bfbb7c787e86c3989b00cee060fab0317c3455b8dc50e2cd033eccd0bc3	fffc026cf37e7640a4abcba62ebd0a08
IX20W-PR-23.9.20.63.bin	47cd5c0e11ca63349d94ff0d14f7d669e3f1fe230e1e8f1121cf61b56c306a9751908e353b21f692725116e78404823196c1c98247cae80dbb1c9571b7163751	d41d740c70918a5290ff601daee40bf2

IX30-23.9.20.63.bin	89147b3ddd3300024a8788b949f9dfc9a7c66524f1d3 46147a809bb20a5229782484690897c5df5d215a3a02 da840548459c1103eaf6e0027d70b87edf188d33	c43e6c2260c2396d92da061cfc688fc3

FEATURES

1. *IX20W:* Added support for setting up a Wi-Fi hotspot captive portal, including integration with hotspotsystems.com, under the ***Network → Hotspots*** configuration settings [DAL-6825]
2. Added ***Status → Premium Features*** page to the web UI for locally viewing and managing subscription licenses available from Digi Remote Manager [DAL-6636]
3. Added a link to the ***Dashboard*** of the local web UI to register and add the device to Digi Remote Manager [DAL-6787]'
4. Updated the layout of the ***Dashboard*** page of the web UI to combine the network interface and cellular modem details into a single ***Network Activity*** panel [DAL-7361]
5. Added MACsec (802.1ae) support and configuration options under ***VPN → MACsec*** [DAL-6825]
6. Improved support for integration with HotspotSystems [DAL-7722]
    1. PSD2 SessGarden
    2. Login/Logout URL
    3. Configurable remote webserver FQDN
7. Added new ***System → Primary Responder mode*** setting to lock down the device to comply with AT&T FirstNet and Verizon Response Verify security options (disabled by default) [DAL-7849]
8. Added new ***Services → DNS → Domain allowlist*** configuration settings to control what domains are accessible through the Digi device (default is to allow all domains) [DAL-6741]

ENHANCEMENTS

1. Added new ***Services → DNS → Fallback server setting*** to control what DNS server is used as the fallback in the event that no configured or DHCP-obtained DNS servers are available [DAL-7439]
2. Removed mention of DHCP set in ***System → Containers → Address*** help text [DAL-6453]
3. Add nrbroadband APN to the fallback list for AT&T SIMs [DAL-8038]
4. Add NFOD-INET-APN01.com.attz APN to fallback list for AT&T SIMs [DAL-8337]
5. Add fbb.home APN to fallback list for T-Mobile SIMs [DAL-8105]
6. Add iot.tmowholesale APN to fallback list for T-Mobile SIMs [DAL-8026]
7. Updated PLMN and ICCID prefix list for T-Mobile SIMs [DAL-8105]
8. Added a new DHCP option to ***Network → Interface → WWAN → Type*** configuration setting to support advertising the device's hostname over a cellular network [DAL-7641]
9. Added new ***Network → Interface → IPv4 → Force link*** option to keep the IP network interface up even when the physical Ethernet link for that interface is down (disabled by default) [DAL-8066]
10. Added symlinks in / root directory for file system directories accessible remotely through Digi Remote Manager [DAL-7646]
11. Add serial number to SNMP MIB [DAL-7720]
12. Added new configuration settings under ***Services → SNMP*** to provide a dynamic set of properties and values to add as OIDs to the SNMP query response
13. Added new ***PDP context index*** setting when configuring an APN to control what PDP context the APN gets written to within the SIM [DAL-6573]
14. Added ***network.modem.modem.dhcp_relay*** debug setting to enable DHCP relay support

within the cellular modem (disabled by default) [DAL-7312]

15. Updated the input voltage and system/CPU temperature metrics to limit the measurement to one decimal point of accuracy [DAL-7958]
16. Updated the Containers status page in the web UI to validate the name of the container file being uploaded [DAL-7617]
17. Added help text to the pop-up modem when performing modem firmware updates on the ***Status → Modems*** page in the web UI [DAL-8174]
18. Update ***Status → Serial*** web UI page to show Log button in ***modem emulator*** mode
19. Updated the ***System → Firmware*** page in the web UI and the pop-up notification in the CLI/webUI to include the build date of the firmware [DAL-8022]
20. Updated the setup of serial ports configured with remote TCP listeners to utilize the SSL version specified in the ***Services → Web administration → Minimum TLS version*** configuration setting (Default TLS v1.2) [DAL-7915]
21. Added new ***System → Containers → Working directory*** configuration setting to specify the path within the container to use an the initial working directory when starting the container [DAL-8007]
22. Renamed the title and updated the help text of the ***System → Containers → Clone DAL*** configuration setting, which is now titled ***Clone host system libraries*** [DAL-7989]
23. Improved the log messages while the cellular modem is connecting to better reflect the Surelink state and why Surelink tests were skipped [DAL-8085]
24. Add WAN Bonding status and details to support report information [DAL-8371]
25. Updated the help text for TACACS+ under ***Authentication*** config settings to note that the ***#*** character cannot be used in the TACACS secret key [DAL-8273]
26. Add ***#swpkgv*** AT command to support report for additional firmware details from Telit modems

BUG FIXES

All bugs listed affect firmware versions 23.6.1.118 and older unless specified.

1. Fixed issue preventing modem firmware OTA updates from completing when initiated via Digi Remote Manager and the update was done over the device's cellular connection [DAL-8333]
2. Fixed race condition where the NTP server failed to start if an active NTP sync was in progress [DAL-8122]
3. Fixed issue where Surelink fail_count metric was not reported to Digi Remote Manager when Surelink tests were passing [DAL-7975]
4. Fixed rare issue where the cellular carrier reported to DigiRM would be "0" instead of the carrier name [DAL-7924]
5. Fixed occasional issue where the device would not update Digi Remote Manager with the new firmware revision after a modem firmware update was initiated from Digi Remote Manager [DAL-7983]
6. Fixed issue where Surelink metrics weren't reported properly to Digi Remote Manager for bridge interfaces on the device [DAL-7990]
7. Fixed issue where the cellular APN metric was not being reported to Digi Remote Manager (affects firmware versions 23.3.x through 23.6.1.105) [DAL-8055]
8. Removed meaningless warning in system logs stating that there was an invalid key for the anywhereusb service (affects firmware versions 23.6.1.x) [DAL-8000]
9. Fixed issue where the Digi device could connect with the configured APN list out of order if it had previously connected with one of the configured APNs [DAL-8335]
10. *1003-CM07 CORE modem:* Fixed issue preventing failover to secondary SIM slot with EM7411 modems (affects firmware versions 23.6.1.x) [DAL-8191]

11. *1003-CM07 CORE modem:* Fixed rare issue where the EM7411 and EM7511 cellular modems could initialize in the wrong mode and prevent cellular connectivity [DAL-7923]
12. Fixed issue preventing cellular connections with the secondary SIM slot if multiple network interfaces were configured per-SIM slot (affects firmware versions 23.3.x through 23.6.1.x) [DAL-8115]
13. Fixed issue where the wrong destination IP and MAC address was used for Surelink ping tests on GRE tunnels [DAL-8385]
14. Fixed issue where cellular utilization reports in Digi Remote Manager would be skewed due to the device reporting incorrect Rx/Tx data usage metrics to Digi Remote Manager (affects firmware versions 23.6.1.x) [DAL-8380]
15. Fixed issue where WPA2 mixedmode Wi-Fi client-mode connections would revert to WPA-only and prevent connection to WPA2 APs [DAL-8443]

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 all product firmwares to use OpenSSL version 3.0.8, including configuration setting to enable FIPS 140-2 compliance
2. Updated OpenSSH to version 9.3p2 [DAL-8097]
    1. CVE-2023-38408 (9.8 Critical)

VERSION 23.6.1.117 (August 2, 2023)

This is a ***mandatory*** release.

Firmware	sha512sum	md5sum
IX20W-23.6.1.117.bin	a74f2eb9d94ee182b8ac53efd0516a34f487c92ced760aee09b93208e8871acced3cc86fee6aa9a0be274dc83001835868dd7c32bf3a1cf567ea68cff9f35809	8b1a597af161baf41e100f68cb761150
IX20W-PR-23.6.1.117.bin	91bfc403d76de6a069813f0b4eb4c58925ab8f630db5d509b3fdf0941a873881c507e9814001d25990e471653dea8ed5ad23c87789e1975417359c86065ac34f	44add284250b0be1e72ad0ee8f020e28
IX30-23.6.1.117.bin	bfbb63b896e33ca36f794d5984306341cd8595d44b264cd2b95ec48a610f10c2fd63bf6e873d9f590c1c16283785430b903c19733946b9c9c8c06b7e162ecb9f	8f90987cc56b3241f08625c54cc53e82

ENHANCEMENTS

1. Added nrbroadband APN to AT&T fallback list [DAL-8038]
2. Added new metrics reported to Digi Remote Manager to track the number of disconnects on each WAN interface [DAL-7880]

BUG FIXES

1. Add support for automatically recognizing AT&T SIMs with ICCID prefix 890128 and PLMN ID 310280 [DAL-8038]
2. Fixed issue where the cellular APN metric was not being reported to Digi Remote Manager (issue present on 23.6.1.105 firmware) [DAL-8055]
3. Fixed issue where devices with multiple cellular modems would not report metrics for the secondary modem to Digi Remote Manager properly [DAL-7681]

4. Fixed issue preventing WPA2 Enterprise AP & client-mode connections from working [DAL-8073]
5. *IX30:* Fixed issue where the LEDs on the IX30 would not update beyond their initial boot-up state (issue present on 23.6.1.105 firmware) [DAL-8127]

VERSION 23.6.1.105 (July 16, 2023)

This is a ***mandatory*** release.

Firmware	sha512sum	md5sum
IX10-23.6.1.105.bin	431f7fd489c3af2d2e1203ce7d94342bcaa37f54e1deb8ef2bdb258b11ff55f3e3380f6964cb0dfda8eaf4a5488cef949f9b575fb285aff21c9216a65674e48c	cee633d6779d5f28639734edac5d98ed
IX20-23.6.1.105.bin	a5119a1fea0410b88cb46541a5f06e25f92f880cc6511ea59cc1f417e8dc14d0f4fbc4a62b4c0725b4ba36da8945716531bc7a9271f4fb8caf306aa7a1cacc52	85986ffc9c0c37bb0e6011461841932d
IX20-PR-23.6.1.105.bin	568cd5908729dd958703a1606c7578f420588758311aa595fc842366d5a3661a60615e8633f4ffd07be3123d240ccbd796c1f996c4791f5c6a689bf0c6f63b1b	3892d50c0daa44630e4bc6e6e132095b
IX20W-23.6.1.105.bin	009fcaaea86e5be4fdce948051d7f35a12a237ffd78a7ece3d0cc86bb44b2a7a80110af8c9865c4053c059ba0c4397adccefe93b77a2de3d42dd9144cdc82bc7	d5f21d92fa7cbebf4c4a0a66278d126d
IX20W-PR-23.6.1.105.bin	ae57456902258bc68874f05b02d0832ad76da0494e78b23e88174952fab4de989fdc45d8dc7a88418886f8733e0bcf862bfbc768df46eab79028df531a283caa	0e13575a13ce8066a8b00665327decd9
IX30-23.6.1.105.bin	50b0782ad7ccf451fede02d2a9a33b4afa7334315ae960b831f7e7e45203d45ae0ba019aee7bd987e2676a35450bd66fce6ccc7be5d4dd9eb8ba73c56a752adc	ec4cdc7b46c1aa7ba2224413afe8df95

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. *IX10:* 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 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 IX20W to utilize OpenSSL 3.1.1 [DAL-7818]
5. Update libcurl to version 8.1.2 [DAL-7817]
6. Update OpenSSH to version 9.3p1 [DAL-7816]
7. Update libgmp to version 6.2.1 [DAL-7820]
8. Update OpenVPN to version 2.6.4 [DAL-7822]
9. Update strongswan to version 5.9.10 [DAL-7823]
10. Update dnsmasq to version 2.89 [DAL-7533]
11. 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.

Firmware	sha512sum	md5sum
IX10-23.3.31.129.bin	c4bb60d94ec4b8da73dc56c33b4ffa526900e92ebf41ca179721cbadef5d4431296c75242c2ad34611597214d933759580f075f2b998255022500e73f643f2d7	cf0ad30558f182b3068c4ac522aaf04c
IX20-23.3.31.129.bin	cba2f27cd262bbecdc093233da58004d2cc7ecc94f662a9783c6ae8f7bff8eacf4657cccfe384b46c4369c73380d4fa88a737ef050fb91f318df5f66c4d97b9d	dd479a0c6a00175c968d30975fdbc47f
IX20-PR-23.3.31.129.bin	ff23ed64389128ae47b710aaa95c41f37f56739e03d9faf75e8334d3020968e9a6a08a358366b3f519537dac23795148306c6977a63f52fa6972a2490b411702	6305060ca4c91dbad5004a8f6c40449f
IX20W-23.3.31.129.bin	4eaaed083dc65823815bad791d53eb159ce4d71c10b8566afdb7a3b4a68c91677508efed03c08fd8650b5fcaea61cac4c01e428abe8068dbea0c64de1e3d4c39	b70004c29a1115f692b84f5fd7e9a595
IX20W-PR-23.3.31.129.bin	fef413796f75a99e240543565b14713430a789551702e53b56de5f69987950a2c6a7adae635ded2232bd655a81c7b03b446f377f129e19ffc740dc3edbe97a14	54964edc3a78f4a6e2d7737f0a72b687
IX30-23.3.31.129.bin	b9ddc5120278310e07fb987fa49a44a7699feb1be8ba0894a1e2ae6d85e2c5ddbd856e73422652d37aa1c9cd72f09883064562415fa1ff71fc675625a20fba7b	3a2324c156a0ceda92f07d80c961f38e

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 improper setup of Realport HW flow control on IX-series products [DAL-7081]
14. Reduce cellular GSM 2G Tx power consumption by 2dB for IECEx/ATEX compliance [DAL-7043]
15. Fixed issue where the latest WAN Bonding saneclient presets were not being included in the DAL firmware [DAL-7540]

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 22.11.48.16 (January 15, 2023)

This is a ***recommended*** release.

Firmware	sha512sum	md5sum
IX10-22.11.48.16.bin	83230fa9ffeee6c5cca2f511565a2757d1a031ff3b9a0335cf74fecf1fe56cc1d040e1013baebc203d9847dda9a7451167737927641d83859b9f58531bfcc208	d018c44b30144122249094ff90aeda7b

ENHANCEMENTS

1. Add support for SHA2-512 and SHA2-256 hash algorithms for IKEv2 IPsec tunnels for interoperability with Cisco ASA devices [DAL-7071]

VERSION 22.11.48.10 (November 24, 2022)

This is a ***mandatory*** release

Firmware	sha512sum	md5sum
IX10-22.11.48.10.bin	f5f0abe5c16dd04f699da1ccb178bd6961fc8fac5eb75	eddcfb583b8255e1f1e0dce24e0d35b2

	23c08060fe0700415cce05068f5fead9e3ec5103f6e64 22fe1043380d9d5badbe08d167393e9337d202	
IX20-22.11.48.10.bin	16c1f6dea048e30ceb51d371366451d53d2f5510e6f3 e3b7ea681afe3574f7e0e6ca2672886d6202660b310a 82b42f51ddbe11bb455a5c6019926a9738acb967	46499364d8972d2c16d808387565c899
IX20-PR-22.11.48.10.bin	0b0509e84fbf41ba2502d7bc522cddc5435790f80fea7 c9295889c0878fdecd51b6a565437849b8005b0f5937 aed7464777cffdbeab4257147011ef7ec2e0571	934af77638846899051d9bcb086cf96f
IX20W-22.11.48.10.bin	3f5025b8425d6b776ddf0516f22f39a8b012b9e9fa6e9 23bb239dcf5e145ba380e3f3d6412288a21a38c90256 91c5826ce44b3da1beb04a9651043f88383ec19	5f14352f6be099cf032834434f1a385a
IX20W-PR-22.11.48.10.bin	e70744b63593f48034c29d29d951b6ce5859752810d6 a3ba19ca73428186c9f3e5975d485c32d34340bc65f8 e46e159fde5d46c1b8cdb08142ffcd4ec2a85969	4747a40fb0b91647e22f18f18a36f551
IX30-22.11.48.10.bin	c773f39b1fbbafb4e2941f73caea84c6001c89a05d684 79e1dee15b5ecf6e4b8e4f2bb7b7bc27b052305f75e5 481e26aebe726159c27931fa01b01348ec35af8	0ef714336355ad543a27d25d4a2f9b34

FEATURES

1. New MQTT Broker service with configuration options for:
    1. multiple MQTT clients with unique topics and authentication credentials
    2. pre-shared key encryption with multiple configurable keys
    3. pattern filtering for topic access control
2. Updated the intelliFlow feature to integrate with Digi Remote Manager for aggregated insights and analytics [DAL-6656]
3. Add options under ***Network → Routes → Routing services*** for configuring Next-hop routing protocol (NHRP) advertisements [DAL-6711]
4. 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. Add option under ***VPN → IP Tunnels → Mode*** for supporting mGRE tunnels [DAL-6709]
2. Added option under Network → Advanced settings to allow ICMP redirect messages (disabled by default) [DAL-6013]
3. Disable automatic modem/device firmware update options if using DigiRM [DAL-5738]
4. 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]
5. 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]
6. New ***tail*** and ***grep*** Admin CLI commands
7. Send container datapoints to DigiRM with the configured container name instead of container index number [DAL-6551]
8. 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]

9. Add modem scan timeout option to ***Scan*** window on the ***Status → Modems*** page in the web UI [DAL-6938]
10. 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]
11. 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
IX10-22.8.33.50.bin	56fb5cb26fa92d6e9717475703bdf547b06f8b01f369261fb73282769a88ff734cda1c1fedba027826d16a0037df665bf959e5a865c9fb903dab46c47267e20c	979aacc00bca4dabdf446e8a896968ab
IX20-22.8.33.50.bin	4488be68efcd61ec8cd92962766356af237f1d8c48c6250787580a9e7bdaa18684963ab2814fa9c2a96bc6a4b0597f6284102510e5fd48974670c8402a47df36	ecc66c016554f7cecb3fc080963763af
IX20-PR-22.8.33.50.bin	13a7bd1e478f63ff16933a02dd2cf37facce38956877921d9430e26b8150975f3a5415c039b93a81c8409f8f2652f17a4a6134f8bf069fab02a4f367856e289d	65d0d90683f610b522a20e69af36eba9
IX20W-22.8.33.50.bin	eb355b3df54fa54c2688f96a9b051f00a520100259de7556ff171a97f10cc0477590d2829c533e9feb1b0456c597589aa769655088d9e1b088a2155963f6c645	d20e2593379c3d7f9a25e54be6031000
IX20W-PR-22.8.33.50.bin	c635bd76729c3cc0375a62b16fa37091ed97d85d4187efa6dc7fdef5a686ff4541f060052b48badc27cb03c22cfe2b2815e4fad99238a2037f405e56a668b706	032efb7952bd77c6fd9ee13b6690d02d
IX30-22.8.33.50.bin	4fb0a50325f1690a03533333ebb3111e392cf8cafe6c1fdb553cd6e4c16bff46d880c064fc6f19f0e5daba29f13967981bc948621038ce9a63988e6a49cd8cb8	fd9780c601f0a13ddc060db4e4845f8f

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]
18. Support for the Telit LN920 cellular modem [DAL-5863]
19. New ***System → Power → LEDs enabled*** config setting that can be disabled to turn off all LEDs on the device to reduce power consumption
20. Add disclaimer to ***Network → SD-WAN → WAN bonding*** settings to note that a DigiRM license is required
21. Update WAN Bonding client to version 2022-04071718

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]
13. Fixed issue with downloading client ovpn file from the local web UI [DAL-6561]
14. Fixed issue where the connection to DigiRM would fail if WAN Bonding was enabled [DAL-6386]

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
IX10-22.5.50.62.bin	ad9504775bee8d434cb9731f09de058502da86a42b25d609c661757e41451f5ee24bc90cfc0ae006853cbabf66d889d4a3142311915598895d2d38cfabbcb901	a8b0d2cae8f30a9fe13ae906379c1e80
IX14-22.5.50.62.bin	9583de5c93cbac4ff1ad46cdfd87a68fdd09a52a06569095ff1292e230cdbd0b3695de62330e480b7329224b6525f83bf0bf269725d025689a9d14937b075575	0b5c613bdd54c9de45c6a14508be32e7
IX20-22.5.50.62.bin	db2cd7812dc9f7bb9115264287320b4a4177ebbaabb7747c96e8bd89d56bf8c32218e9f815ebac168eabf973a85e0c69043241b0cb87363491f6abd9be4aab81	De7bee9e3fc4ae2a8d608025c18ccf8a
IX20-PR-22.5.50.62.bin	f1b04b9db3b637ee1c7cd8b140b37447c01e8de26d5dcfa80ca32411e77bc03df15b42bf7d3279d8f729ca08b68dd80a3efa03a70ec84893110c907cd90520da	5afb2f08b775ab24c2f5356aabb2d723
IX20W-22.5.50.62.bin	7f55e5d96edd4498d8c728c2ffbd67b9feece3d4a23302532b4114222d3926bb848386f4ce061ebc4d7ad6ec7ef49000bdf7c293b54d6ec84cf373ea4e2d85fd	1d61fc036ff8f5045a4ae992fc4e0f64
IX20W-PR-22.5.50.62.bin	464bbef647e200db4ffb23f8a04867ce42266cfb544ad09dc4af19ea465ec20a053e17b9354743b62377c90f889c66759d65f10bd5165da58254cef71ad75cc4	ff885f72a10f90c3028ea1966306e007
IX30-22.5.50.62.bin	2d83f722c8f764f9f04fe82fb1b8dea14efce31db12e9c5f9a1b3b940830b1ea134a2fc2a1f87be71517f7a5cfc131a2089c29cc2541a6a9489429d07f6de7ff	046a5ac8268aae76bb8df1032d213458

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 settings under ***System → Power*** for setting CPU performance level and adjusting power consumption [DALP-983]
3. Realport serial mode added to IX10 and IX30 devices (already available on IX20/IX20W devices on 22.2.x firmware) [DALP-998]
4. 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]
5. New *show scep* Admin CLI command for showing the sync status, expiration dates, and additional details of any configured SCEP clients [DAL-6069]
6. Support for enabling add-on features from Digi Remote Manager [DALP-673]
7. *IX20/IX20W/IX30:* New ***Network → SD-WAN → WAN Bonding*** add-on feature via Digi Remote Manager for bonding multiple outbound Internet connections together for increased maximum throughput or data redundancy [DALP-108]

8. *IX10:* Support for the Fibocom FM101-CG-20 cellular module [DALP-974]
9. *IX10*: Support for the Telit ME310G1-W1 cellular module [DALP-986]

ENHANCEMENTS

12. 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]
13. 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]
14. 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]
15. 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]
16. Include the hostname of the device in the client .ovpn file listed on the ***Status → OpenVPN → Servers*** page in the web UI [DAL-6157]
17. *IX30:* Power off serial port when not enabled [DAL-5991]
18. *IX30:* Power off the Ethernet ports when not enabled [DAL-6063]
19. Add support for the CP210X serial driver for connecting to Cisco USB console ports [DAL-6119]
20. Filter out non-Internet type APNs from our APN fallback list [DAL-6227]
21. Automatically power cycle the cellular modem in the event that a *modem reset* Surelink action fails [DAL-6268]
22. Enable Surelink *reset_modem* action by default on cellular interfaces and set fail count to 3 [DAL-6275]
23. Add cellular APN and cellular connection duration as datapoints sent to DigiRM [DAL-5902]
24. Ensure modem is in enabled state before attempting to connect [DAL-6163]
25. 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]
16. *IX10/IX30:* Fixed bug where RTS toggle config setting would be applied in RS-485 serial mode, which should only be used in RS-232 mode [DAL-5990]

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
IX10-22.2.9.85.bin	9360d83f83e004d75e8863918634eb177ff2387dc255ff4e5eca84fbe8a0f8bd8ca5f5fe861f056ee7697f982dd8783d3f09cace10052c97e931d3018489a889	93ce9e08efffcc1e9420c958291dfbf6
IX14-22.2.9.85.bin	5a36679940aae964adc3fb137b5ced97b5bf562ca4d056691536fd2a7930e415d35a5e03692af62012a6c216664433bf8f8ad3e026b0b6fa565cd56d1a4316fb	9bc23e39734752a33b15fc4ae75877ec
IX20-22.2.9.85.bin	08702600be63bddede307768253c2c15990f61ec928ea9847498140e67144578187a610f4755afdf17be287a2b7df572230039c72626e48a0e1d5c8f9d0b9c33	de03896ac8097f90ed05e8cdc8dddf57
IX20-PR-22.2.9.85.bin	ae3b43f9e9e5b4b34796efce156f9a0da735dc2e18f0d475a87aa00801dd3a120b553ce549c86cfe62335010dc8ec8dcb85bc27e9eae6fabab7d3ce06134d83b	1ad392435b190289464159dd08f51c05
IX20W-22.2.9.85.bin	21ab62ae2f481d145cc626f9db19df52c4b7cf950918e1e8148acd67c656f1915af2755c7b840a472e8bb878bd488546ba9e79ff2fb30a133dd41e73f500c943	2ce90377d5cc9a3211abdee0a3c3e87a

IX20W-PR-22.2.9.85.bin	8f8c100e1645ed86822fbd1828100cb8c0e4db2ce7bd46c74078e09a3b42059755bc0fd34c5a17cbf55d009a75ce3030a27047e841947439c6d2c25969cce501	71631fe390b34cbb1eddc1b1a4a1fb35
IX30-22.2.9.85.bin	d89b26404a4512d3ae040e7e00bc6401ba11fafc7a84b807e6a02dec3501a4612c056f27d88128690dca8cc114d5b379de3080a385934671fe7541b81c44e2e0	e6910d5da40bfdeb74fecccc833e41a6

FEATURES

5. Initial release for the IX30 product
6. *IX10/IX20:* Realport serial mode support [DAL-5742]
    1. Realport DTR-pin flow control is not available on the IX10. Will be coming in our 22.5 release (see DALP-998)
7. 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. *IX20-PR/IX20W-PR:* Add container support to PR products [DAL-5498]
3. *IX10:* Support for the Quectel EC25-AFXD modem [DAL-5787]
4. *IX10:* Add ODIS/LWM2M parameters for EC25-AFXD modem [DAL-5840]
5. Increased web UI upload limit to 512MB [DAL-5694]
6. 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]
7. 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
8. 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]
9. 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]
10. 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]
11. *1002-CM06/1003-CM07:* Utilize T-Mobile carrier firmware if available for the cellular modem when using Sprint Curiosity SIMs [DAL-5466]
12. New cat Admin CLI command for displaying file contents [DAL-5853]
13. Update /etc/config/scep_client/ directory to be read/write by admin users

14. 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. *IX20W:* Fixed issue preventing Wi-Fi metrics from being uploaded to DigiRM

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]
13. *IX20W-PR:* On PR FirstNet products, enable the ***Network → Wi-Fi → Access points → Digi AP → Isolate clients*** setting by default so Wi-Fi clients connecting to the Digi device's SSIDs are isolated from each other by default

VERSION 21.11.60.63 (December 8, 2021)

This is a ***mandatory*** release.

Firmware	sha512sum	md5sum
IX10-21.11.60.63.bin	892bf3099cda0a8c5991030af092b8a56241b1e47bcb77235a3c7f79034032bb8c5903f423af37dbfc0443340d385c47047126f061bf9b935aca92c76951613e	b3302801d9c7b0be073291e3204463eb
IX14-21.11.60.63.bin	dc9b8c18607e746749d6007a8545bf16b0da4e5448aa06719a576c7d8270628cc893a034bebcf7c675124f445c32e92fa6416b53fce7d0f1c123b84f94bacc0b	644774a75aedd007306ea4f9431f3147
IX20-21.11.60.63.bin	0117847cd52661c6403fbe51f60f9cf725e3e3b5f823fe6b3ed1216ed463856836e5648fa039a4e543f7b0ee019a19c29ab10d1d4c107a86bdef9ebf652f872e	e61a492f997e743b909e0b30a86915fa
IX20-PR-21.11.60.63.bin	867e7c32b49c2e029f194901795520f04090823fed9a59938df8de3606486bb0d8dfd2b655e5dcac8e6a82239bcb2d1a664c11357297f3704b4a2f85bb6b7aaf	1ecf60261eedcb3ac92ad7cf9ab00078
IX20W-21.11.60.63.bin	4d3214368640fb94c808b58adaf345caef5988e0d750e9e36dca3539c7a8313538ff21eb65ee76442e46a15d5de52ad6933d5baba5571d8c1cfe28f9b36342d9	b664624f58cd808ee5ade9bf678c538e
IX20W-PR-21.11.60.63.bin	40172c2aa46e1ee12a4a4c3f03b5c7aaaa6eee8ab85ebdc11383954aa2e1bbaea4a357ae2c34685ca2bede0017366a2d48df6c86d3f36b94c441dcf216aca30b	fe23cc6563b955a9b56551ce2484b843

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

4. 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]
5. New **show surelink** Admin CLI command for displaying details on the Surelink test(s) configured for a network interface or VPN tunnel [DALP-621]
6. Add new option under **Location → Destinations** for specifying the talker ID used in NMEA message strings [DAL-5038]
7. *1002-CMM1 CORE modems:* Use CID context 3 for any type of Verizon SIM when used with a ME910c1-WW modem [DAL-5428]
8. Include the mode indicator field in NMEA messages constructed when a GPS fix isn't obtained [DAL-5464]
9. Add support for auto-completing a parameter or AT command provided to the **xbee set|get|execute** Admin CLI commands [DAL-5196]
10. Change default IPsec IKE DH group to 14 for enhanced compatibility with industry standard settings [DAL-5344]
11. Disable serial history in remote access mode by default [DAL-5494]
12. 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]
13. Add **datapro** APN to fallback list to be utilized with Airmob SIM cards [DAL-5548]
14. New **show containers** Admin CLI command for listing details about configured containers [DAL-5380]
15. Include SIM ICCID and phone number in the query_state response sent to Digi Remote Manager [DAL-5632]
16. 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

17. Fixed issue preventing IPsec tunnels from being setup in Transport mode [DAL-5490]
18. *IX14 or 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]
19. *1003-CM07 CORE modem:* Fixed issue preventing multi-carrier firmware updates on Sierra EM7411 modems [DAL-5473]
20. 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]
21. 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]

22. Fixed issue preventing IPsec tunnels from being setup properly if the tunnel name was longer than 9 characters [DAL-5139]
23. 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]
24. Fixed error in system log when attempting to parse an empty config file [DAL-5402]
25. Fixed issue causing potential multi-minute delays in the *show modem name XX* Admin CLI command [DAL-5297]
26. 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]
27. Fixed issue where Surelink **reboot** action would not be take if the Surelink **restart interface** action was also enabled [DAL-5485]
28. Fixed issue preventing the creation of config elements with dynamic array names via the local web API [DAL-5481]
29. Fixed issue preventing installation of sqlite3 python package via pip [DAL-5611]
30. Fixed issue preventing multiple config changes from being applied in a python script using the digidevice.config module [DAL-5192]
31. *IX20W:* Fixed issue where the Wi-Fi LED was always illuminated even if no client or AP connections were enabled [DAL-5296]

SECURITY FIXES

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

16. Update to python version 3.6.15 [DAL-3190]
17. Update stunnel to version 5.60 [DAL-5291]
18. Update busybox to version 1.33.1 [DAL-5290]
19. Update to Linux kernel version 5.14 [DAL-5360]
20. Update OpenSSL to version 1.1.1l [DAL-5242]
21. Fixed issue where the TACACS shared secret was included in the system logs [DAL-5470]
22. Update libunbound to version 1.13.2 [DAL-5420]
23. Update libidn2 to version 2.3.2 [DAL-5439]
24. Update muslv to version 1.2.2 [DAL-5452]
25. Update rsync to version 3.2.3 [DAL-5431]
26. Update OpenVPN to version 2.5.4 [DAL-5435]

VERSION 21.8.24.143 (October 22, 2021)

This is a **recommended** release.

Firmware	sha512sum	md5sum
IX20W-21.8.24.143.bin	162af9869025b8d1e981056a2df798e57d9ed7c25d3fd62352ed3a2f05756f09bdc9cea3779f4146a89211d4842c50782a957a9f10d6c198e7a5fe92abe05a86	14b176f00318d8d3809c2e2cc10aa81c
IX20W-PR-21.8.24.143.bin	9572bc92b930dcb6d1847abc6bd0472a6266ce15a303d58e7b5882edd881830195accf8bea2b8b3822f66ba1db1bbe0b72e3748148b013da1c9ef1b66c788042	de72b8df160dfae4f47f2d9700cf869a

ENHANCEMENTS

1. Update Wi-Fi driver for EU compliance [CELL-106]

VERSION 21.8.24.139 (October 7, 2021)

This is a **recommended** release.

Firmware	sha512sum	md5sum
IX10-21.8.24.139.bin	6c2c4ed22272aabf55343dabbe9417cfae7f16a1b081f1dc26abea5590bba01abfb05bb4567b29b3438e70f87a5d7d0c846ed53ec0b6ad98f547cd37230866d7	1e49403ab57e49afd8c7fb8ca7b81a12
IX14-21.8.24.139.bin	ecfb2d23f7a2c25d2d1f3ca458d9b71f7fccbc89efc7a08f8f716bf388eee05509ae32dd4e66424fd067ff7e86a4e000f7fa9eb48e2b36f59d25c1cff66d347e	a64c9360277fc10f5d7461fd35395981
IX20-21.8.24.139.bin	f886867d7cc79f48a27879be622e81aa1ff89c0c9e46026dff432edcb42a7955f97653e1aa833ca2590b77be6b94a358fa9d4b3c001a925985f1b88d9a90e4da	596efbf49c309959df18b9a77742b666
IX20-PR-21.8.24.139.bin	8d0c5e4216f5601186379d5cd88c196f225edce8400afe16c6ad6d6fa21fa261452edd3282c19645de306d01861200cd9d1066dbd9aa322d6a91eb53cc582936	c2a1676970d34512265823fac293c2ef
IX20W-21.8.24.139.bin	6ffb74f74283d85436eea1d4efc0ce117fe1b2cd6567116eee65a3c4fbdddfbb567a5bd1a9ed1e9cdfc3ac4234c6fef3b5a2711b5a6dc95e31fe8e3c50780462	054e6e7070de9008f4704c900da6cb26
IX20W-PR-21.8.24.139.bin	96706b477b790872821868be1b4825afde7fbe14507486ac186edd4c4e8b8a2e4752b2144ba976464800b84b572c8a5556c26de07e1c1a9c8d23c10095affbc5	8b5d94ab590a09e6965af19c9a5a4035

BUG FIXES

1. Fixed issue where device would not re-establish its cellular connection after updating to 21.8.24.129 firmware [DAL-5346]
2. Prevent automated health metrics uploads and manually initiated/generated health metrics from interfering with each other
3. IX10: Fix RTS pin control on RS485 serial port when used as a Modbus gateway (bug present on firmware versions 21.8.24.129 and older) [DAL-5322]

VERSION 21.8.24.129 (September 13, 2021)

This is a **recommended** release.

Firmware	sha512sum	md5sum
IX10-21.8.24.129.bin	3c5a6ad86c4e9145a735e16dc13168f97956223b5806e721f3d02e8828ff7cc15bcf233d9c5f3a9694d62aaffbd9fa45f612036152ab7fcd88706bab0fddf6cc	fa2e2f8850bacc0b28a5c905dc3ecadb
IX14-21.8.24.129.bin	ca591c8a989255f781d68e7f1cb09843eed20120d54285a6c300ff6eb5fa74805cf8c7a9bcbcdc97d6d5feec21dc50680988dbb10963d75e04385986156c84e5	73cf5050c90222207308f0a0445fd90d
IX20-21.8.24.129.bin	047eb31e4483a1d97ef6d836e1275a492865db42b4792fc0d9d8c07254f8f274e4b45641b8da6faabf88e6c7e1966f5b633ba6588412cb2d57a86f60c3fde689	733c3866a5cc0251125e67261270cf26
IX20-PR-21.8.24.129.bin	938cdad630fa6b5de137f275e47b6a44dee06f36599fb3f0a5207007a6319bb0d4c35355145e74b3ba4a19d8a3b4b7c3bd61fa4502e9e688bc22678b2174ba11	9fc034e8f092b78288dace719548194f

IX20W-21.8.24.129.bin	476f90b0e3d8c838d60bdfe387bbed51b3333636dfc28f250e6da7af751cb34af8fad3bd4dcaef85d600a622e66188c008ce975be661322248116a2fcf1e682e	d07c79b084cf7c3d968d6f3a5268edf7
IX20W-PR-21.8.24.129.bin	d92ba876ba220c6713747c7b7fc7e95915d47881fa2554f3b9e79266ac00edabab4fff17279ddd9595f8b8dbdfc9dc0da2022bff343b3551c8a282b234bdc286	c22e5f0be35e1a939b0c092961b1ba09

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. *IX10:* Add option to utilize GPS from cellular modem inside the IX10 as a source for the Location service [DALP-849]
2. Added new **show l2tpeth** CLI command for viewing the status of any configured L2TPv3 tunnels [DAL-5220]

3. Update python pip to version 21.2.4 [DAL-5068]
4. Shortened fallback APN list by removing wildcard entries [DAL-5012]
5. 3G sunset support for EU carriers [DAL-5041]
6. Update messaging included in keepalive packets sent to Digi Remote Manager to prevent multi-second delays in keepalive responses [DALP-832]
7. Add **datapoint.upload_multiple** function to digidevice python module for uploading multiple datapoints to DigiRM at once [DALP-857]
8. Add **uptime** field to **show cloud** CLI output to indicate how long the device has been connected to Digi Remote Manager [DAL-1083]
9. Update **system support-report** CLI command to automatically store the support report in /var/log/ unless a path is specified [DAL-5027]
10. **system support-report** CLI command outputs helpful information for SCP-ing the file from the device to a remote destination [DAL-5027]
11. 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]
12. New **speedtest** CLI command for performing on-demand iPerf or nuttcp speedtests [DAL-5040]
13. Require local users to be assigned to a group [DAL-5060]
14. Add support for configuring multiple destination networks/interfaces for Multicast routes [DALP-853]
15. New **Network → Advanced → Sequential DHCP address allocation** configuration setting for controlling if DHCP addresses are assigned sequentially or randomly (disabled by default) [DAL-5136]
16. Persistent local date/time across reboots once a successful NTP sync occurs [DALP-806]
17. 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
18. *IX20W:* Remove the requirement to set a Wi-Fi SSID and passphrase to initially configure the device [DAL-5101]
19. Read/write control to the /opt/ and /etc/config/analyzer/ directories through DigiRM and the local web UI [DAL-5117]
20. 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
21. Add option to clear a custom default config by performing a double erase sequence [DAL-5017]
22. Updated CLI login helptext to include common tool-tips [DAL-5157]
23. Replace the cellular modem manufacturer name with the CORE modem model name in the CLI/webUI/metrics details [DAL-5171]
24. Ensure scheduled reboots with the **reboot_managed** command cause graceful shutdown of services on the device before rebooting [DAL-5150]

25. *IX14:* Add hashes for recognizing Telit LE910 xx8 firmware for firmware updates [DAL-5086]

BUG FIXES

The below bugs are all present on firmware versions 21.5.56.176 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 21.5.56.176

This is a **recommended** release.

Firmware	sha512sum	md5sum
IX10-21.5.56.176.bin	478bc6507e074c98f88194e53f015da154f5d4029f24c ccba5cefae856daf16e30a0d43aae5711c75f288f44c7 3e2298dc4885c5ad5958ecbafb4e2a9f4ae602	c5af97051dd6191ea87d11791ffa5271

ENHANCEMENTS

1. Add support for the Quectel EC25-AU cellular modem (DAL-5085)
2. Prevent race condition where DAL could try initiating a cellular connection before the modem is configured and fully setup (max wait time of 5 minutes for the modem to be configured before attempting to connect)
3. Added new **IKE fragmentation** and **Maximum IKE fragment size** config options under **VPN → IPsec** to control whether large packets are fragmented through IPsec tunnels and the size of packets that should be fragmented [DAL-4933]
    1. default **IKE fragmentation**: always
    2. default **Maximum IKE fragment size**: 1280 bytes

VERSION 21.5.56.106 (May 31, 2021)

This is a **mandatory** release.

Firmware	sha512sum	md5sum

IX10-21.5.56.106.bin	ec6989222c10826f1b8248dd7d17e573fabcdb435bc03bca0e3111c8debd38f62431835e2c1dd348b9eb8f62d78e3b27879954c73ce28375f2b45dee7e7fd216	461c270cba2f0393dd2283e610d7d8f2
IX14-21.5.56.106.bin	098c09f80df65dffa9050fab0d38bfb7f08d84b3964e137cc93a358551f7217d31bff65908ad9d6c724354f4634acd2a0aaf662af6e643bd63aae3ffeefac9b4	976fe84d343cb7c4120a0d44f11297ed
IX20-21.5.56.106.bin	dc240873c338e5fb7df1df47e00664be7d896965808765958b67da9f16239f86fc13e2d9e8d79f61e1c4650121822006591986ef48afd9cfb6113987e27c1e76	4487a01d3a5430f448daf61a68129471
IX20-PR-21.5.56.106.bin	f2b98641e5d62a461f3e4c2dd7e3db63f1aa04a972fd4414ee9af893d693f3b5dd803e1095b9d2fcbb210d9ca2664ac317a165e33a89f1c12d7288713b00c76f	5c13536b93607cbb6b0d2ad4799ab8cb
IX20W-21.5.56.106.bin	6f25269f1e35dbf61e536b33c9a6982196e83ca28ef4cd2652946e261899c6d7a6ba4351fb07eac1d0a240b86a4888d0fbc61e67fe45f5905451e1cc76ab7e91	34fc88207b8187623044ad8b8650a9dc
IX20W-PR-21.5.56.106.bin	4c70cbf4ccc7c2e9e98868a4bb85402c725a4fd88f35f001ab74ef450c2983f42545d66d53672fdaa00e1d6ad86bee661e61030059a2693784ceed69d4af8406	a487820df1e6f09714ad49e54dcfaef1

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
8. New **UDP serial** mode that can be applied to one or more serial ports for setting up outbound serial-over-UDP connections [DALP-696]
9. New **Autoconnect** options for streaming outbound serial traffic when in remote access mode
10. Support for WPA3 Wi-Fi encryption [DALP-701]
    1. WPA2/WPA3 Personal
    2. WPA3 Enhanced Open
    3. WPA3 Personal
11. Support for WPA and WPA/WPA2 mixed modes with TKIP support [DALP-827]

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 on the **Serial Configuration** page in the web UI where users could inadvertently bring up the Copy dialog window by dragging and dropping any element from the page [DAL-4923]
19. Fixed issue where wired Internet connectivity is interrupted during cellular modem firmware updates [DAL-4647]
20. Removed broken Babel routing service (bug present on firmware versions 21.2.39.67 through 19.11.x) [DAL-4769]
21. Fixed overlapping 5GHz Wi-Fi channel ranges causing AP/client conflicts in connecting in Switzerland and Liechtenstein [DAL-4733]
22. Removed error message caused by inability to access file descriptors on PR products [DAL-4930]
23. Use PDP cid 1 for Telstra SIMs with a Quectel EG25-G modem [DAL-4810]
24. *IX14:* Fixed issue preventing IX14 units from updating their cellular modem to firmware version 20.00.xx7 [DAL-4867]
25. *IX10*: Fixed issue where RS485 serial connections would spit out junk messages during bootup [DAL-4724]

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 (PR products still have 10-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 21.2.39.79 (April 1, 2021)

This is a ***recommended*** release.

IX20-21.2.39.67.bin

SHA512:
3dbcfd33a66474d7fdb308d292868f8a044207f687039afb9404ae44d1feb30925075a9935cbb395a868398514343a2e97e0c4fd62ce1eda373152f6c13a86c3

MD5: 5aca7b9224e9d3104eb0f29d29883cf6

IX20-PR-21.2.39.67.bin

SHA512:
176308c72b7a706ca0c036314944a5b88a4e8451b3a5f9fe8230ee61588db265e27bf98721f5d23af83657a6baa68d7adc5d825498dab291ee2ccafeb5e98c95

MD5: 3993f737da1d405ce36fa7e0370ccd14

IX20W-21.2.39.67.bin

SHA512:
4bfb707b256352b2a44cde67ae2700c1f9f02acc785ab52a521934a5dec2b88f01b6564b05a7d3ee2be5ff3958273b9dc8eca17407e1efd24c985989f2b275a0

MD5: 1904551bb372c568cba6fc644912b18e

IX20W-PR-21.2.39.67.bin

SHA512:
f721b6ba36cc555b88e9e515dc6a96eae53b32abbe03b86e5d7158b5752078e2953d0cf67b55316dec12b073e413aa5113245d388ff8b470eebd4da002a32db7

MD5: aa85293fdc99c41c7a8b50926e029c46

BUG FIXES

26. *IX20W:* Fixed issue where Wi-Fi network crashes when under heavy load [DAL-4667]

VERSION 21.2.39.67 (February 27, 2021)

This is a ***mandatory*** release.

IX14-21.2.39.67.bin

SHA512:
39234c8644fff88e0ac8503e80e023f92ebe768a5ce9cd7648be38e202fd592e0fd9f35ab44fddd3d9321d50c42ad1146ae089875ffe8cccb0e60e23dd863502

MD5: d6ed79ec3b2db14738451c15038fd5aa

IX10-21.2.39.67.bin

SHA512:
72a8ef1e4e892ea431b101063eb040b6cffe37351f7d27556836a33915f0cf8e241b2296ed2d6cc3d69e2dee05bdba08273d58f81f2333fa36d88bc17a087547

MD5: 8e7d2ca15d40de7d7955fa5d5d7773cc

IX20-21.2.39.67.bin

SHA512:
525dbe3d67ae2db90c3c28bb98acbab9b893be87e7432d3930baad8fe827bed5a92231e8c7eaa4a9b945b231ddcb9f5972d552dc52aedabdcd1711431e281a1d

MD5: 1b6bc3ac24b0bd009177c77d076efbf8

IX20-PR-21.2.39.67.bin

SHA512:
33b393e3bfd347070b4086267dd29dfe327e2c81ae8a695635433f2fdbb156cd29af3ceb86feaf5731b7fc8fb07b58ba010ee1a749c2d165467d5e3b6428fd30

MD5: b8a737e16faee85f34678e2d9de8e330

IX20W-21.2.39.67.bin

SHA512:
ac896a32a704728834385eae13555d07c7901c8f74794c1848e592b1570268df0f9b4149f13f24bb807742cdfe493323d82ad9386efe33e82d118e403c1a8f1b

MD5: efa574c9e98186bddcbafdb2c7df56f9

IX20W-PR-21.2.39.67.bin

SHA512:
a3feb157fb421d8787d5f8c51a898f3bd88954874d7dd967ed56fd5fae60e25cead4cc4024eb0384b556635436bbc068e876721f4e44c0845b1deb9021f6307e

MD5: 3c1900f45ed730d15ae13ea5d074481c

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. Added new **DFS Client Support** configuration setting to support 5GHz DFS Wi-Fi channels in client mode [DALP-720]
2. Add 5GHz frequencies to the list of channels that can be scanned for client-mode Wi-Fi background scanning [DAL-2570]
3. Set 2.4GHz default Wi-Fi bandwidth to 20MHz [DALP-772]
4. Update default background scanning settings for Wi-Fi clients to the following:
    1. Scan threshold: -75dB
    2. Short interval: 5s
    3. Long interval: 300s
5. Updated Surelink recovery of Wi-Fi connections to restart the Wi-Fi module if restarting the network connection fails to recover the setup [DAL-4387]
6. Added settings under **Authentication → Serial** to control Certificate Management for TCP and autoconnect serial port setups [DALP-682]
7. Allow hidden/debug config settings to be controlled and preserved by DigiRM [DAL-4445]
8. Asymmetric preshared keys for IPsec tunnels [DALP-707]
9. Don't display Aggressive/Main mode or Xauth selections for IKEv2 IPsec tunnels [DAL-4142]
10. Update name and description of certificate settings for OpenVPN clients and servers [DAL-4435]
11. Add digidevice.led python module to all products [DALP-710]
12. Add options to forward location information to a remote host over TCP [DALP-778]
13. 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]
14. Report location metrics as datapoints to DigiRM [DAL-4055]
15. Include the connection uptime of IPsec tunnels as datapoint metrics to Digi Remote Manager [DAL-4062]
16. Report the phone number of the SIM as a health metric datapoint to Digi Remote Manager [DAL-4440]
17. Fixed incorrect format of ICCID and IMEI metrics reported to Digi Remote Manager [DAL-4440]
18. Add iptables TRACE tool for enhanced firewall debugging [DAL-4182]
19. Improved accuracy of the status shown for a modem during a firmware update
20. *IX10/1002-CMG4:* Disable GEA1 on EG25-G modem [DAL-4250]
21. *IX10/1002-CMG4:* Disable voice services on EG25-G modules [DAL-4560]
22. *IX10:* Enable QXDM support on IX10 [DAL-4512]

BUG FIXES

1. *IX14:* Fixed reboot loop issue on IX14 device running default settings on 20.11.x firmware [DAL-4507]
2. Fixed issue with utilizing software flow control on serial ports set in remote-access mode [DAL-3630]
3. Fix issue where a serial port could lock up and prevent access if flow control was enabled [DAL-4585]
4. Fixed issue where non-primary DNS were queried through the wrong interface when **use_dns** configuration option is set to primary [DAL-3156]

5. Report the phone number of the SIM as a health metric datapoint to Digi Remote Manager [DAL-4440]
6. Fixed incorrect format of ICCID and IMEI metrics reported to Digi Remote Manager [DAL-4440]
7. Fixed setup issue between custom firewall rules and IPsec tunnels [DAL-4433]
8. Fixed occasional issue preventing LM940 modems from re-establish their cellular connection after a modem firmware update [DAL-2933]
9. 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]
10. Fixed rare issue where **show system** CLI command would display incorrect uptime details [DAL-4350]
11. Fix issue with secondary CLI sessions showing stale configuration settings if the config is updated elsewhere [DAL-4446]
12. Updated message displayed in web UI to direct the user to refresh the page after erasing the device back to default settings [DAL-2326]
13. 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]
14. Fixed inaccurate status of the Ethernet interface of a device in passthrough mode [DAL-4543]
15. Fixed issue preventing web UI access if two-factor authentication was enabled (bug present on 20.11.x firmware versions) [DAL-4509]
16. Fixed issue where CLI commands sent from DigiRM would crash the DAL device's connection to DigiRM [DAL-4412]
17. Fixed issue preventing WAN/cellular connections from working if the interface was configured with a single **Interface Up** Surelink test [DAL-4629]
18. Fix rare issue where Wi-Fi hotspots would stop responding to DHCP requests if restarted many times [DAL-4298]
19. Fixed output of the **show wifi ap name <ap_name>** and **show wifi client name <client_name>** CLI commands [DAL-1615]
20. Fixed inaccurate status of the Ethernet interface of a device in passthrough mode [DAL-4543]
21. *PR products:* Fixed issue preventing usage of the digidevice.config python module on PR firmware products [DAL-4378]
22. *1003-CM11*: Fixed occasional issue preventing LM940 modems from re-establish their cellular connection after a modem firmware update [DAL-2933]
23. *1003-CM11:* Fixed timing issue after updating firmware on LM940 modems that preventing the modem from reconnecting unless rebooted [DAL-4614]
24. Fixed issue causing aView-initiated speed tests to report the same upload/download speeds [DAL-4420]

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 hostapd to address CVE-2019-16275 and CVE-2019-13377 [DAL-4232]
2. Update wpa_supplicant to address CVE-2019-16275 [DAL-4233]
3. Update libcurl to version 7.74.0 (CVE-2020-8169, CVE-2020-8177) [DAL-4336]
4. Update to python version 3.6.12 (CVE-2020-14422) [DAL-4364]
5. Update OpenSSL to version 1.1.1i (CVE-2020-1971) [DAL-4326]
6. 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]

7. 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
8. Set SAMEORIGIN in X-Frame-Options to uppercase [DAL-4192]
9. Automatically de-activate active user logins/sessions if the password for that user changes
10. Removed support for https CBC ciphers [DAL-4408]
11. Fixed XSS vulnerability on serial page in the local web UI (Bug present on firmware versions 20.11.x and older) [DAL-4646]
12. *PR products*: Removed debug config options from PR firmware for changing https ciphers [DAL-4417]

VERSION 20.11.32.168 (December 23, 2020)

This is a recommended release.

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 20.11.32.138) [DAL-4414]
2. *IX10-only:* Fixed bug preventing serial port signal mode from being set to RS-485 when in application or modbus modes (affects firmware versions 20.11.32.138 through 20.8.22.32) [DAL-4424]

VERSION 20.11.32.138 (December 2, 2020)

This is a ***mandatory*** release.

IX14-20.11.32.138.bin

SHA512:
723d71598e538fa1ad1dc4a54c9d80d6e7a0d2fcf67c9b040e8c181085e55a4f9958ace580b4fb68ebdaa4106ef1f9cba98520f43e54342fd5b13488cbde3e00

MD5: c0ffb2f67e9126ab15bb62cd92de94ab

IX10-20.11.32.138.bin

SHA512:
e4850185fa3714a4e15b78f620f3985bbe3c47564c7907a68a61b1a2814d7756d7c14fa811360ed6279bb7fd55fc47a6ba5a012a0a4c36d7852a312b366d454a

MD5: d1780394cbfdeb398e0dd7cfa8f07707

IX20-20.11.32.138.bin

SHA512:
00ed82ef515d85f624cbc8c5ccf04736f907e61e955655f7aa051c567599b69f7575892dbc214086b017176ce0260931601e3100d7c883bf1f3ff4f0cc9ec140

MD5: dce476fb431f95954776d783c26c2dda

IX20-PR-20.11.32.138.bin

SHA512:
12478faf7c902916ddd0e171efb19ba0b8773eec7ad6b97ba7bf797fefeb91cc3cfa57f078b

fd475ac7692b2af22acfd2e63f3cb23e155c53d546d35162fc984

MD5: 2d0aa54d637a6579a9206dbf4b6b9797

IX20W-20.11.32.138.bin

SHA512:

a5f1fd71a11ac6f335124a709873b9315a9b46f01ed26ded488cc0b003e5d6cd0af93906f5
81494702dd06faf109a224e026246bb107945d9d8ba12bf970f27e

MD5: cdac8fb0a7cbb99649514d06f01680ec

IX20W-PR-20.11.32.138.bin

SHA512:

bc978f56f4cd58d22cfa928db3fa5c3fb3fa37eb9de9e08788b5b9baedfc1b742b1fc2197c4
e4d69ee600f70d25460adc96bfc16975f49c4160ab5740d3a944c

MD5: 45e59c1b8e42ab6e233c4f03d0b459dd

FEATURES

1. *IX20/IX20W:* New PR product variants and firmware for FirstNet/ResponseVerify products [DALP-674]
    1. PR stands for Primary Responder and indicates a security hardened, feature-restricted firmware targeted to comply with AT&T FirstNet and Verizon ResponseVerify certifcation security requirements. It is the same DAL firmware under the hood, but with several features removed to comply with FirstNet and ResponseVerify security restrictions. Below is a list of changes for PR products:
        1. ***Services → Telnet*** removed
        2. Removed ***Telnet*** option from Remote access options if a serial port was set in Remote access mode
        3. WPA1 Wi-Fi encryption option (WPA Personal) removed
        4. Default Wi-Fi SSID disabled by default
        5. interactive shell removed
            1. ***Firewall → custom rules*** always has sandbox enabled with limited shell command and filesystem access to only allow iptables interaction
            2. ***System → Scheduled tasks → Custom scripts*** always has sandbox option enabled with limited shell command and filesystem access to allow CLI access and python script execution
            3. No inbound SCP/SFTP support
2. Add **ssh** and **telnet** commands to Admin CLI [DALP-664]
3. 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]
4. Add new configuration options under **Network → Devices** for setting the link speed/duplex of the device's Ethernet port(s) [DALP-135]
5. Add options for starting, stopping, and viewing serial port activity logs through the CLI, web UI, or Digi Remote Manager [DALP-458]
6. Support for the Sierra EM9190/9191 5G modems [DALP-686]
7. Support for the Sierra EM7411 LTE CAT7 modem [DALP-608]
8. IPv6 IPsec tunnel support for full IPv6 tunnels, IPv6-over-IPv4, or IPv4-over-IPv6 tunnels [DALP-581]
9. 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]
10. Inclusion of the Python pip for installing external modules/libraries [DAL-4078]

ENHANCEMENTS

1. Add **Services → Location** options for configuring GPS or GNSS location communication [DALP-724]
2. GPS/GNSS support for the IX10 and 1002-CMG4 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. Added new **Status → Modbus Gateway** service page to the web UI to display information about modbus clients and servers connected to the gateway [DALP-671]
7. Added **show modbus-gateway** CLI command to view the status of Modbus gateway service [DALP-671]
8. Updated **show modem** CLI command to display historical information about the modem if it is in the process of updating firmware [DAL-1504]
9. Added new **Services → Ping responder** configuration settings for controlling what interfaces and firewall zones the DAL device responds to ICMP requests on [DAL-1565]
10. Enhance IPSec tunnels to wait for passing Surelink tests (if configured) before initiating outbound tunnels [DAL-3878/DAL-3774]
11. Add m2m.telus.iot Telus APN to fallback list [DAL-3911]
12. Add psmtneorm and edneopate010.dpa AT&T APNs to fallback list [DAL-4041/DAL-4045]
13. Add reseller and tracfone.vzwentp Tracfone APNs to the AT&T and Verizon fallback lists DAL-4098]
14. Add new 890103 and 890141 ICCID prefixes and 31030 PMND ID matchers to AT&T APN fallback list [DAL-3934/DAL-4041]
15. Add service.qcdm.secure option to enable/disable encrypted QXDM access to the cellular modem in the DAL device [DAL-3964]
16. Add missing modem firmware and SIM details to datapoints uploaded to Digi Remote Manager [DAL-4040]
17. Show uptime for connection to Digi Remote Manager on the Dashboard web UIpage in days/hours/minutes/seconds instead of just minutes [DAL-3691]
18. 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]
19. 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]
20. Updated the help text on the login page to provide a more generic image [DAL-3916]
21. Added option when copying serial port settings on the **System → Serial Configuration** page to optionally copy the label of the serial port [DAL-3842]
22. Removed duplicate modem signal information from the **Modem → Status** page [DAL-3680]
23. 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]
24. Added a **defaultroute** option for matching policy-based routes to the device's active default route [DAL-4130]
25. Hide the **Monitoring → Device Health** configuration options if the device is not enabled for Digi Remote Manager central mangement [DAL-3825]
26. Update header types for the cellular modem name and network type on the Dashboard page
27. Create system log when Surelink DNS tests are skipped because the interface doesn't have

any DNS servers [DAL-4224]

28. Hide main/aggressive mode option when using IKEv2 [DAL-4142]
29. Add reboot watchdog to IX20/IX20W devices to prevent soft-reboot hangs [DAL-3392]

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]
16. 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]
17. Fixed issue preventing IX10 devices and 1002-CMG4 modems from connecting with Verizon private APNs (bug affects firmware versions 20.8.x and older) [DAL-3605/DAL-3276]

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]
17. Removed expired aView and AVWOB certificates [DAL-3467]
18. Encode MAC address in URL used to sync with aView to prevent privileged escalation [DAL-4304]

VERSION 20.8.22.32 (August 28,2020)

This is the initial production firmware release for the IX10 product. This is a ***mandatory*** release.

IX14-20.8.22.32.bin

SHA512:
deea32a3fd22257be2e08596162a83778966cfec751725ae533ec90bf0cf43466e6cd21ba649ab4812fa6ffbcfb29400a71f3cca14dc27c478d9da69221fd1c5

MD5: 1c64b417f36e6425576f999506da9d79

IX10-20.8.22.32.bin

SHA512:
1b681cc342211b3ae2ee849ea3230670ab48a52b667b626520f40b6e33f316c320f2d9916ee5c63c371492a0ea632f979fc397f638ea111bafd243c4063f86b7

MD5: 3749095e4ef0e0d862a64cf1f01ba121

IX20-20.8.22.32.bin

SHA512:
8f7772b60cf18abdd8325dc6fa8e4e4cc7a0f1d4eb201070fc14e6855fc1f05170ba40cb45a83167170467d9e348e64f059184c25c82487005ea5691b8658cee

MD5: 55d7da428951313542aaf9a76e3eb410

IX20W-20.8.22.32.bin

SHA512:
c505383dd71a250f3692ea54ccc10e2e4b718670fb58afbf4f8448f30cbd25620eb451d6e8123d7d0cad1e56a1f67f97c7bd997fa215053901c105884fa00ca9

MD5: afc9527ff7a3f03a617fbf8c6a1079ee

FEATURES

1. Add new **System → Scheduled taks → Allow scheduled scripts to handle SMS** configuration option to allow custom python scripts to handle sending/receiving SMS messages [DALP-488]
2. Add digidevice.sms python module for sending/receiving SMS messages in a custom python script [DALP-488]
3. 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
4. DMNR Verizon Private Network support with new settings under **VPN → NEMO** [DALP-457]
5. Added Serial Modbus Gateway service for utilizing the Modbus protocol to communicate with serial ports [DALP-573]
    1. Configuration settings for the Modbus Gateway are found under ***Services → Modbus Gateway***
6. MQTT client support via Paho Python module [DALP-590]
7. 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. Note: not available on the IX14
8. 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
    2. 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 **service.modbus.debug** config option to enable debug logging on Serial Modbus [DAL-3561]
4. Add **Central management** configuration options for any DAL product to sync with aView, ARMT, or AVWOB [DALP-626]
5. 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]
6. 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]
7. Added configuration option under **Serial → TCP connection** to specify encrypted vs non-encrypted connection types
8. Added configuration option under **Serial → TCP/Telnet/SSH connections** to enable/disable TCP keep-alive messages and nodelay
9. Added new **Base settings** checkbox on custom serial configuration page in the web UI to allow users to specify whether they want to copy the base serial settings or not [DAL-3775]
10. Added new **Monitoring→Device Health→Data point tuning** configuration options to fine tune what datapoints are uploaded as health metrics to Digi Remote Manager
11. 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]

12. Reduced data usage by 80% (based on default settings) for reporting health metrics to Digi Remote Manager [DAL-3394]
13. Fade **Configuration saved** pop-up window 5 seconds after clicking the **Apply** button [DAL-3451]
14. 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]
15. Add options in CLI to show and manually stop any custom scripts or applications [DALP-533]
16. 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]
17. Add **system duplicate-firmware** CLI command to copy active firmware to the secondary firmware partition [DALP-565]
18. Move **update firmware** CLI command to be under **system** [DAL-3092]
19. Add **show vrrp** CLI command to display the status of any configured VRRP instances [DAL-2953]
20. Use a random unprivileged port for performing ntp time syncs if standard port 123 fails [DAL-3650]
21. 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]
22. Added new options under **Network → Wi-Fi** to control Tx Power of the Wi-Fi module (default 100%) and allow multiple RADIUS servers for WPA2 Enterprise [DALP-85]
23. Include up/down status of hotspots in the **show hotspot** CLI output [DAL-2184]
24. 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. Fix LED behavior to account for Surelink pass/fail results [DAL-3688]
2. Fixed issue preventing RADIUS/TACACS+ authentication from working unless local-user authentication was also configured [DAL-3701]
3. Fixed issue preventing 1002-CMG4 modem from connecting with Verizon private APN SIMs [DAL-3276]
4. 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]
5. Fixed bug where IPsec tunnels with multiple policies would only properly route traffic for the last policy configured [DAL-3448]
6. Fixed missing CPU usage stats in **show system** CLI output [DAL-2540]
7. 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]
8. Fixed issue preventing network interfaces from initializing if the interface name was longer than 7 characters [DAL-2327]
9. Fixed issue preventing WAN passthrough mode if WAN was configured with a static IP [DAL-3097]

10. Fixed errors displayed in CLI when configuring a USB serial port in remote access mode [DAL-3207]
11. Fixed issue preventing users from configuring an IP address as a remote syslog server [DAL-3433]
12. Handle incorrect value occasionally returned by by Telit LM940/LM960 module when querying to see which SIM slot is in use [DAL-3481]
13. Fixed issue preventing cellular modem connectivity if a custom gateway/subnet was configured but the modem wasn't in passthrough mode [DAL-3585]
14. Fixed issue causing aView IPsec tunnel (if enabled) to randomly fail when device was in passthrough mode [DAL-3657]
15. Fixed permission issue on /opt/custom/ directory preventing users from setting up custom CSS and logos [DAL-3710]
16. Fixed issue preventing VLANs from being assigned to Wi-Fi SSIDs [DAL-3113]

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. Prevent cross-site scripting on the Wi-Fi and Bluetooth scanner pages in the local web UI (Score: 3.8 Low CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L) [DAL-3628]
6. 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]
7. 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]
8. Fixed leaked file descriptors on serial connections [DAL-3202]

VERSION 20.5.38.58 (July 20, 2020)

This is a **recommended** release.

ENHANCEMENTS

1. 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. Fixed delay in connecting with FirstNet SIMs caused by interference from Lightweight M2M

(LWM2M) service on Telit modules [DAL-3236]
2. Prevent interruptions to QCDM/QXDM port on Sierra modems caused by ModemManager interaction [DAL-3469]
3. Fixed bug preventing dual-APN connectivity with AT&T SIMs and Sierra modems [DAL-3586]

SECURITY FIXES

The highest level vulnerability that has been fixed in this release is listed as a High CVSS score of 6.5, which is rated as a Medium

1. 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]
2. Add failed login attempts to event log sent to remote syslog servers, if enabled [DAL-3492]

VERSION 20.5.38.39 (May 29, 2020)

This is a **mandatory** release

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. Added new **WiFi → Access points → [ssid_name] → Isolate clients** option to enable/disable WiFi client isolation [DAL-2019]
4. Add configuration options under **Central management** for a proxy connection to Digi Remote Manager [DAL-3150]
5. 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]
6. 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]
7. *IX20W:* Add new WiFi SSID and passphrase, enabled by default. The default SSID is now <device model>-<serial num> and the default passphrase is the unique default password of the device [DAL-3050]

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. Add AT&T FirstNet IMSIs so they can be differentiated from other types of AT&T SIMs [DAL-3163]
5. Added Python HID module to allow the DAL device to control PSUs via Python programs [DAL-2092]
6. Allow network analyzer to be configured to monitor any network interface instead of just wired Ethernet ports [DAL-2146]
7. Added option to **ping** CLI command to ping a broadcast address [DAL-2571]

8. Added new health metric to report the interface used by the DAL device for its configured IPsec tunnels [DAL-2710]
9. Added new health metric to report the LTE SNR value of the modem(s) on the DAL device [DAL-2904]
10. Limit metrics upload to no more than 2 per minute if backlogged [DAL-2870]
11. 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]
12. Report device SKU in RCI response to Digi Remote Manager [DAL-2940]
13. *IX14:* Report the SKU on IX14 variants (was already reported for other IX-series products) [DAL-2539]
14. Add wbdata APN to fallback list [DAL-3182]
15. Improved recovery of Telit modem firmware updates should the update get interrupted [DAL-2984]
16. Fixed spelling of **System utilization** chart on Intelliflow page in the local web UI [DAL-2260]
17. 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]
18. Commonize the format and naming of rx/tx health metrics reported to Digi Remote Manager [DAL-2896]
19. Add IPv6 options to **traceroute** CLI command [DAL-2618]
20. Add count of bytes transmitted and received to the output of the **show network interface X** CLI command [DAL-2980]
21. 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]
22. 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]
23. Display the secondary/alternate firmware image version as the **Alt. Firmware Version** in the output of the **show system** CLI command [DAL-3057]
24. Retain modem firmware files in the event that the firmware upgrade was interrupted [DAL-2856]
25. Renamed OpenVPN server **device type** configuration options to clarify which options are OpenVPN managed versus device-only [DAL-2857]
26. 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]
27. 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]
28. Add support for AES_GCM family of IPsec ciphers [DAL-2715]

BUG FIXES

1. Load FirstNet-specific firmware on Telit LM960 modems when a FirstNet SIM is present (bug affects firmware versions 20.2.x and older) [DAL-3163]
2. Fix VRRP crashes by upgrading keepalived to version 20.0.20 (bug affects firmware versions 20.2.x) [DAL-3181]
3. Prevent IPsec tunnel from being setup if its local network/interface is down (bug affects firmware versions 20.2.x and older) [DAL-2336]

4. 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]
5. Update analyzer to continue running even if the users SSH session ends (bug affects firmware versions 20.2.x and older) [DAL-2154]
6. 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]
7. Fixed bug preventing stale conntrack entries from being flushed when a WiFi-as-WAN (client mode) network changes, connects, or re-connects (bug affects firmware versions 20.2.x and older) [DAL-2775]
8. 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]
9. Fixed issue preventing backup IPsec tunnel from being established when primary/preferred tunnel was down (bug affects firmware versions 20.2.x) [DAL-3024]
10. 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]
11. Fixed failing SureLink IPv6 ping tests (bug affects firmware versions 19.11.x through 20.2.x) [DAL-2488]
12. Fixed issue with applying policy-based routes to incoming packets from the Internet (bug affects firmware versions 20.2.x and older) [DAL-2589]
13. Fixed bug preventing passthrough mode from functioning if multicast was also enabled (bug affects firmware versions 20.2.x and older) [DAL-2709]
14. 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]
15. Fixed error displayed in **show modem** CLI output when modem was not connected (bug affects firmware versions 20.2.x and older) [DAL-2959]
16. *IX20W:* Fixed bug preventing default WiFi settings from working on certain platforms (bug affects firmware versions 20.2.162.164) [DAL-3049]
17. 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]
18. Fix non-working custom DHCP options (bug affects firmware versions 20.2.x) [DAL-3071]
19. 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]
20. 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]
21. Removed unsupported LED options listed for LR54 units in their digidevice.led Python module options (bug affects firmware versions 20.2.x) [DAL-3250]
22. *IX20W:* Fixed client connectivity through Captive Portals (bug affects firmware versions 20.2.x) [DAL-3251]
23. 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)
24. 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]

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]

VERSION 20.2.162.164 (May 6, 2020)

Initial product release for IX20 and IX20W

VERSION 20.2.162.162 (March 17, 2020)

This is a **mandatory** release

ENHANCEMENTS

1. Add MAC address is support report filename [DAL-2863]
2. Add firstnet-broadband APN for AT&T FirstNet SIMs [DAL-2876]
3. Use ***ims*** instead of ***vzwims*** APN on Verizon SIMs for proper IMS registration [DAL-2883]

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)

This is a **mandatory** release.

NEW FEATURES

1. Telit LE910c1-LA modem support [DAL-2391]
2. Telit LM960 LTE CAT18 modem support [DALP-487]
3. Quectel EC25-AF LTE CAT4 modem support [DAL-1817]
4. Digi Remote Manager is set as the default portal for all DAL products [DALP-393]
   - Central management via Digi Remote Manager will not be enabled if you upgrade a device running 19.11.x or older firmware that was previously syncing with an aView instance 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.
5. Added SureLink™ default connectivity tests on all WAN interfaces [DALP-402]
   - 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.
6. Background Wi-Fi AP roaming/scanning [DALP-435]
   - New **Background scanning** configuration settings under Client WiFi entries
7. New web UI pages added under the ***System*** drop-down with enhanced serial details and configuration [DALP-465]
8. Support for firmware/OTA updates on Quectel modems [DALP-419]
9. AT&T LWM2M support for Telit LM940/LM960 modems [DAL-2476]

ENHANCEMENTS

1. Prevent access to web UI until HTTPS is ready [DAL-603]
   1. Until the SSL cert is generated, users trying to access the web UI via standard http will

receive a redirect page stating that the cert is generating. Once the SSL cert is generated, users accessing the web UI via standard http will be automatically redirected to the https link

2. Show multiple bands for Telit modems if carrier-aggregation is supported and active [DAL-2624]
3. Update wording of help text for WiFi Background Scanning config settings to better reflect their usage [DAL-6673]
4. Added additional Telit-specific AT commands to mmcli-dump of support report
5. Improved Role-based access on local web UI, SSH, and remote access [DALP-415]

   Includes new configuration options

   - **Allow shell** - NOTE if this options is disabled and subsequently re-enabled, the DAL device will **reset to default settings**
     - **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 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.
   - Under each user group under **Authentication → Groups** in the configuration settings:
     - **Admin access**
     - **Access level**
     - **Interactive shell access**
6. New default break sequence ***~b*** for serial connections [DALP-253]
7. Report MCC/MNC/CID/LAC values in health metrics to Digi Remote Manager [DAL-2502]
8. Add digicpn.gw12.vzwentp Verizon APN to fallback list [DAL-2283]
9. Change default OpenVPN Certificate Issuer details from Accelerated to Digi [DAL-2449]
10. Change default SSL certification from Accelerated to Digi [DAL-1336]
11. Dual-APN support on Sierra EM7511 modem [DAL-2311]
12. Include AT#RESETINFO and Quectel-specific AT commands in support report [DAL-2394]
13. Rename ***Configuration Management*** page under the System section of the web UI to ***Configuration Maintenance*** [DAL-2549]
14. Added link under ***System*** drop-down in web UI to download the support report
15. Update the ***Digi Remote Manager*** link under the ***System*** drop-down in the web UI to open in a new tab [DAL-2294]
16. Update the ***Authentication → Idle*** timeout setting to have a default value of 10-minutes (previously the default was blank) [DAL-2292]
17. Send up to 4 IPsec tunnels' details as health metrics reported to Digi RM [DAL-1476]
18. Change the default behavior of the ***SIM failover alternative*** settings from ***None*** to ***Reset modem*** [DAL-2687]
19. Renamed ***Signal Strength*** references to ***Signal Quality*** [DAL-2707]
20. On the Network Status page of the web UI, add ***Interface is up*** message in SureLink status details
21. Add ***service.qcdm.modem.device*** and ***service.qcdm.modem.interface_number*** config options

for specifying QCDM/QXDM port for a modem [DAL-2497]

SECURITY FIXES

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

BUG FIXES

1. Fixed bug where SureLink™ DNS tests took longer than the configured timeout to complete [DAL-2702]
2. Fixed SSL validation bug preventing modem OTA updates [DAL-2547]
3. Fixed bug where WiFi hotspot intermittently worked [DAL-2547]
4. Fixed bug where newly-created network Bridges would not be listed as options under the Device drop-down for network interfaces [DAL-2575]
5. Fixed bug where the primary/active interface was not reported correctly to Digi aView when the DAL device was configured for load-balancing between two WAN interfaces [DAL-2568]
6. Fixed bug where a device configured with multiple SSH keys would only honor the last SSH key in the list [DAL-2506]
7. Display the active cellular band for Quectel modems [DAL-2298]
8. Fixed bug where the web UI would display bytes transmitted/received for network interfaces as ***N/A*** [DAL-2295]
9. Fixed bug where the web UI wouldn't show IP information for client devices connected to an OpenVPN server running on the DAL device [DAL-2251]

10. Fix formatting output of ***show config*** CLI command when the configuration settings contained an array [DAL-2594]
11. Fix bug when adding a new element to an array in the ***config*** mode of the CLI [DAL-2594]
12. Fix bug where CLI ping and traceroute commands would ignore any interface specified in the command [DAL-2605]
13. Fix bug where SureLink™ default tests would continue to pass if cellular modem lost its active data connection [DAL-2609]
14. Fix a bug handling certificate files with spaces
15. Fixed padding issue with downloading SCEP CA certificates [DAL-2212]
16. Fixed rare issue with passthrough ancillary DNS not resolving if ***ancillary DNS redirect*** issue was disabled
17. Fixed issue with active serial logins when a serial-related configuration change was applied to the DAL device [DAL-2696]
18. Fixed output of **show modem** CLI command when cellular modem re-initializes
19. Fix potential initialization issues after updating firmware [DAL-2762]

VERSION 19.11.72.85 (January 21, 2019)

This is a **recommended** release.

NEW FEATURES

1. Added new digidevice.led python module for controlling LEDs on the device [DAL-2303]

ENHANCEMENTS

1. Include each interface's MTU to the output of the ***show route verbose*** command in the Admin CLI [DAL-2378]

BUG FIXES

Unless otherwise stated, any bugs mentioned here only affect earlier versions of 19.11.x

1. Fixed bug preventing users from configuring an IPsec tunnel with a remote network of 0.0.0.0/0 [DAL-2253]
2. Fixed timing issue between Active Recovery tests and reloading the devices firewall rules, which if done in the wrong order could result in the device not sending traffic through the validated connection [DAL-2000]
3. Fixed bug where the local web UI would show a *N/A* value for an interface's bytes transmitted/received [DAL-2295]
4. Fixed slowdown in Wi-Fi bridge/repeater mode due to GRO (Generic Receive Offload) being enabled [DAL-2353]

VERSION 19.11.72.58 (December 6, 2019)

This is a **mandatory** release.

NEW FEATURES

1. Re-themed web UI with improved navigation and functionality. New functionality includes:
    - The ability to view local filesystem contents [DAL-2110]
    - Help-text on login page
    - Quick-config access on status pages

- new Dashboard overview page
- Mobile-friendly UI

2. New network analyzer and packet capture tool, included in in both the Admin CLI and web UI [DAL-1575]
3. Added options under the *Network->Modem* section of the device configuration to setup SIM slot prioritization and SIM slot failback [DALP-287]
4. Added new *Preferred tunnel* option under *VPN->IPsec->Tunnels* to configure a tunnel to be a primary or failover tunnel [DAL-1478]
5. Add new ***DHCP Hostname*** option for IPv4 and IPv6 settings under the ***Network->Interfaces*** section of the configuration to allow the device to advertise its hostname to the DHCP server upon connection (disabled by default) [DALP-427]
6. Added ability to receive encrypted SMS commands from Digi Remote Manager [DALP-270]
7. Add support for the Telit LM960A18 LTE CAT18 module [DAL-1905]
8. Add support for Sierra Wireless EM7511 LTE CAT18 module [DAL-1414]
9. Add support for Quectel EG25-G LTE CAT4 module [DALP-339]
10. Add support for Quectel EG06 LTE CAT6 module [DALP-403]
11. Add Python support on all products (previously only available on the IX14 and Connect IT 16/48) [DAL-1907]
12. Add *system disable-cryptography* Admin CLI command to configure a device for *nocrypt* mode [DALP-491]
13. Once a device is set for *nocrypt* mode, a user must press the Erase button to reset the device to factory default settings to disable *nocrypt* mode and restore the device back to standard operation
14. Add *show usb* Admin CLI command [DAL-2029]

ENHANCEMENTS

1. Improved WebUI performance with crypto speedup
2. Default user changed from root to admin [DAL-936]. Once a device is upgraded to 19.11.72.58 or newer firmware
    1. If you do have an admin user configured, it will not be touched by the update
    2. If you do not have an admin user configured, a new one will appear. It will have the same credentials/settings as the root user
    3. If you had a root user configured (e.g. not factory defaults) it will be preserved to maintain existing user access
    4. Restoring the device to factory defaults after update will result in only the admin user. If you have a root user and do a factory default, you have to login with the admin user instead of root, using the same default password printed on the bottom of the device
3. Added the ability to push OpenVPN routes in subnet mode [DAL-2224]
4. Add cellular IMEI and firmware version, along with bluetooth and accelerometer info to show manufacture command in the Admin CLI [DAL-2030]
5. Add the % measurement value to the CPU usage in the show system output of the Admin CLI
6. Device is passthrough mode with an IPv6 connection now honors and utilizes the MTU in IPv6 RAs
7. When using Verizon SIMs, utilize the OMADM process to auto-discover the APN [DAL-1371]
8. Enhance modem firmware update tool to support multiple modem installations [DAL-2148]
9. Created new Edge firewall zone to prevent the device's DNS services from being advertised on the network, which still allowing SSH and web UI access [DAL-2085]
10. Removed 192.168.210.254 Default IP gateway [DAL-2095]

11. Added support for sending RFC2136 compatible DNS updates to external DNS servers [DALP-446]
12. Add new options under ***VPN->IPsec->Tunnels->Local endpoint->ID->ID Type*** for using the device's MAC address or serial number as its local endpoint ID [DALP-437]
13. Updated the filename of the support report generated through the web UI or CLI to include the Digi name [DAL-1434]
14. Updated the filename of the support report generated through the web UI or CLI to include the Digi name [DAL-1434]

SECURITY FIXES

1. Provisioning the device via Bluetooth using the Digi Manager mobile app is disabled after first-time configuration of the IX14 is complete [DAL-673]
2. Updated OpenSSL to version 1.1.1d [DALP-304]

BUG FIXES

1. Fixed bug where provisioning an IX14 via Bluetooth using the Digi Manager mobile app would disable first-time configuration password requirements (bug present in firmware versions 19.8.1.61 and older) [DAL-552]
2. Fixed bug where Telit LM940 module inside the 1003-CM11 CORE modem could disconnect and not recover due to it starting up in the wrong mode or its serial ports not responding [DAL-1843]
3. Fixed bug where a device in passthrough mode drops received packets from cellular WAN larger than its MTU (bug present in firmware versions 19.5.x through 19.8.1.61) [DAL-2137]
4. Fixed bug with timing of RCI callbacks from Digi Remote Manager (bug present in firmware versions 19.8.1.61 and older) [DAL-2091]
5. Fixed bug where RX/TX data usage metrics reported to Digi Remote Manager could be mistakenly calculated as a negative sum [DAL-1972]
6. Fixed crash in IPsec configuration with more than 6 for IKE Phase 1 proposals or more than 10 IKE Phase 2 proposals [DAL-2066]
7. Fixed bug in reporting the reboot counter metric to Digi Remote Manager [DAL-1932]
8. Fixed bug where persistent system logs could not be remotely accessed through Digi Remote Manager [DAL-2060]
9. Fixed bug where Digi Remote Manager would always shows the device's connected method as ethernet [DAL-1993]
10. Prevent users from selecting non-production firmware versions when perform modem OTA updates [DAL-1662]
11. Fixed bug preventing Linux clients from querying a DAL device running a NTP server [DAL-1815]

VERSION 19.8.1.61 (October 22, 2019)

This is a **recommended** release.

ENHANCEMENTS

1. Skip auto-APN detection when using Telus SIM cards [DAL-1928]
2. Add QCDM service for accessing QXDM ports of Qualcomm-based modems [DAL-1904]
3. Add microcom tool [DAL-1872]

BUG FIXES

1. Fixed bug in runt where the boot version was reported incorrectly (bug present in firmware version 19.8.1.43) [DAL-1828]
2. Fixed registration delays on devices with Telit modems using Sprint SIM cards (bug present in firmware versions 19.8.1.43 and older) [DAL-1872]
3. Fixed stability issues with 1003-CM11 modem (bug present in firmware versions 19.8.1.43 and older) [DAL-1843]
4. Fixed bug preventing devices using a 1002-CM06 modem (Sierra MC7455) with a Telus SIM from loading the Telus carrier-firmware onto the modem (bug present in firmware versions 19.8.1.43 and older) [DAL-1823]
5. Fixed memory leak causing a DAL device in passthrough mode to stop responding to ARP requests on its LAN port (bug present in firmware versions 19.8.1.43 and older) [DAL-1686]
6. Fixed bug preventing SSH keys from being used to authenticate when establishing a SSH session to the DAL device (bug present in firmware version 19.8.1.43) [DAL-1742]

VERSION 19.8.1.43 (August 30, 2019)

This is a **mandatory** release.

NEW FEATURES

1. Telit LE910c4-NF modem support
2. WAN passthrough, allowing for multi-WAN passthrough setups [DALP-163 & DAL-959]
    - As a result, passthrough settings are not under the Modem section anymore, and instead are by default listed under the Network-Interface->LAN section for devices with passthrough enabled by default. To change a device defaulting in passthrough mode to router mode, simply change the "Network->Interfaces->LAN->Interface type" from "IP Passthrough" to "Ethernet", and then you'll see the normal router-mode configurations options available.
3. Auto-generated CLI documentation [DAL-1091]

ENHANCEMENTS

1. ModemManager update to version 1.10.2 [DAL-885]
2. Add verbose system log error messages when issues are encountered posting device health metrics to Digi Remote Manager [DAL-203]
3. Add system log when 1003-CM11 modem (LM940) carrier aggregation is disabled due to temperature limits
4. Include Telit carrier aggregation details in device support report [DAL-1435]
5. Add support for python RCI/SCI data_service callbacks and requests from Digi Remote Manager [DAL-1003]
6. Implement protocol to be used for all local communication between cc_acld and connector clients [DAL-203]
7. Include SIM locked/ready status in show modem CLI output [DAL-1320]
8. Update show modem CLI output formatting to have a summary mode that can be used to display the status of the modem(s) in the device, and the verbose output to display additional information for each modem, including the SIM, registration and attachment status [DAL-1184]

9. Improved formatting in the show route CLI output, including finer distinction of static routes [DAL-1176]
10. Include policy and connection details in show ipsec CLI output, along with improved status details [DAL-1190 & DAL-1174]
11. Improve labeling in output of the show network interface X CLI command
12. Show OpenVPN client list and rx/tx bytes in show openvpn CLI output [DAL-1192]
13. Add filtering options in show log CLI command [DAL-1181]
14. Add CPU usage, device temperature (if available), device description, and location details in show system CLI output [DAL-1172]
15. Updated local web UI logout link to list the name of the logged in user [DAL-1142]
16. Renamed the section of central management options from config to cloud [DAL-1255 & DAL-1256]
17. Added configuration option to have DHCP leases file persistent or clear across reboot [DAL-1196]
18. Update CLI table formatting to double space & blank fields [DAL-1186]
19. Add bypass-lan plugin to strongswan to allow 0.0.0.0/0 remote IPSec networks [DAL-1007]

SECURITY FIXES

1. Update Linux kernel to version 5.1.14 [DAL-1076]
2. Busybox update to version 1.31.0 [DAL-1161]
    - The new busybox shell environment no longer allows local variable statements such as the following:
        - local ip_addr='1.2.3.4'
    - and instead the variable must be set without the local option, such as:
        - ip_addr='1.2.3.4'
    - includes update to httpd webUI
3. Remove option to change Wi-Fi country code on US-products [DAL-1402]
4. Update dnsmasq2 to version 2.80 to address DNS cache snooping (CVE-2017-15107) [DAL-1386]
5. Update conntrack-tools to version 1.4.5
6. Update libnetfilter_conntrack to version 1.0.7
7. Update libmnl to version 1.0.4
8. Update bind to version 9.14.2 [DAL-1338]
9. Update iptables to version 1.8.3
10. Update libqmi to version 1.23.1 [DAL-885]
11. Update libmbim to version 1.18.0 [DAL-885]
12. Update stunnel to version 5.54 [DAL-1162]
13. Update quagga to version 1.2.4 (CVE-2016-1245 and CVE-2017-5495) [DAL-1160]
14. Update tar to version 1.32 [DAL-1159]
15. Add Digi Remote Manager serial port configuration to all DAL products with managed serial ports (previously only available on Connect IT products) [DAL-1213]
16. Remove unused user passwords from /etc/password [DAL-1316]

BUG FIXES

1. Fixed bug causing loss of cellular connectivity on devices in passthrough mode with IPSec tunnels built through the cellular passthrough connection (issue present on firmware versions 19.5.x) [DAL-1612]
2. Fix issues where Telit QMI modems would disconnect from USB hub and not recover [DAL-1321/DAL-1556]
3. Fix issues where QMI-based modems would disconnect from cellular network and not automatically re-attach (bug present in 19.5.x firmware) [DAL-1375]
4. Fix issue where logging out of the local web UI from the Terminal page would result in the left-side navbar still showing the menu instead of the ***Log in*** link [DAL-863]
5. Fix issue where client devices sending a DHCP request over WiFi to an external server would fail due to the ARP broadcast reply packets having the wrong source MAC address [DAL-1526]
6. Fix issue where a DHCP relay endpoint couldn't be setup through modem or IPSec interfaces [DAL-956]
7. Close any open sessions on a serial port when configuration update changes the mode of the serial port
8. Fix bug in `show network` CLI output when both IPv4 and IPv6 networks were available
9. Fix bug where `show network` CLI command would show incorrect output when no SIM was present
10. Fix bug in returning dynamic-only ref_enums in device config to Digi Remote Manager [DAL-1323]
11. Fix service serversocket binding when cc_acl restarts [DAL-1411]
12. Fix reloading of displayed configuration options when enabling/disabling aView central management in the local web UI [DAL-834]
13. Fix reloading of the Dashboard page when enabling/disabling Intelliflow in the local web UI [DAL-780]
14. Reset LEDs displayed during reboot instead of freezing the LEDs to show the last known device state before the reboot [DAL-886]
15. Fix bug where Digi Remote Manager RCI thread blocks indefinitely waiting for config write lock [DAL-573]
16. Fix bug where `ls` command in the admin CLI required a terminating / on the path [DAL-1251]
17. Fix output of `show wifi` CLI output to show which physical radio a WiFi-as-WAN client is on, instead of a device name [DAL-1171]
18. Fix labeling and format errors in show wifi CLI output
19. Fix multiple SSID traversal with WiFi-as-WAN client setups [DAL-1246]
20. Fix bug with show openvpn name CLI command output [DAL-1191 & DAL-1192]
21. Fix bug with carrier, plmn, and modem status output in show modem CLI command
22. Fix column spacing and lower-casing consistency in show arp CLI output [DAL-1173]
23. Fix parsing of carrier names when posting cellular modem details to Digi Remote Manager [DAL-1553 & DAL-1326]
24. Fix error showing signal strength of WiFi network(s) when the signal was 0% [DAL-1404]
25. Limit decimal numbers reported to Digi Remote Manager to six decimal places [DAL-807]

26. Fixed issue with Telit LE910-NAv2 cellular modules not receiving SMS messages while cellular data session was active/online (bug present on firmware versions 19.8.1.30 and older) [DAL-1634]
27. Add Telus m2m APNs to fallback list [DALP-452]

VERSION 19.5.88.81 (June 26, 2019)

This is a **mandatory** release.

NEW FEATURES

1. Added support for getting NMEA location information from a UDP port (default port 2948) [DAL-1084]

SECURITY FIXES

1. Kernel patch for SACK attack (CVE-2019-11477). For more information, see https://www.digi.com/resources/security

BUG FIXES

1. Fixed bug where IPSec tunnel would cause a system crash when the tunnel was established over QMI-based modems [DAL-1170]
2. Fixed aView tunnel issue where the tunnel drops over time and remote commands fail [DAL-776]
3. Fixed bug preventing QMI-based Telit modems (CAT1 and CAT-M1 modules in particular) from connecting with vzwstatic APNs (bug present on 19.5.88.59 firmware)
4. Fixed bug where the 1003-CM modem (LTE CAT11 Telit LM940) would shut-down and not recover its cellular connection if temperatures were too high
5. Fixed bug where the cellular modem occasionally would not initialize properly on devices with a large number of serial ports

VERSION 19.5.88.59 (May 24, 2019)

This is a **mandatory** release.

NEW FEATURES

1. New CLI with more commands/consistency [DAL-773]
2. Enable Multicast DNS service on all platforms [DAL-972]
3. Implement RADIUS authentication support for users [DAL-903]
4. Add NTP Server option (disabled by default) [DAL-340]
5. Add sftp server to all DAL platforms [DAL-859]
6. ECC Custom Cert Support [DAL-764]

ENHANCEMENTS

1. Improvements to CLI show serial [DAL-1175]
2. Improved reliability of security chip from userspace access due to wakeup
3. Send interface name with cellular status events [DAL-916]
4. Updated ipset version to 7.1 [DAL-917]
5. Update to newest shadow-4.6 package
6. TACACS+ authorization for more server implementations [DAL-933]
7. stunnel updated to version 5.52 [DAL-915]

8. Additional health metrics required for Digi Remote Manager 3.0 [DAL-810]
9. Add support for Telit ME910C1_WW
10. Direct remote serial port access via WebUI (shellinabox) [DAL-775]
11. Dual-APN Support on Telit LE910-NAv2 (1002-CM04) [DAL-818]
12. Improved OpenVPN operation and customization [DAL-798]
13. Update to linux-5.0 [DAL-842]
14. Add ***description*** field to system group [DAL-581]
15. Upgrade MC7455 to 02.30.01.01 (SWI9X30C 2.0 Release 23) added latest Sierra firmware for MC7455 and MC7430 [DAL-759]
16. Add an additional APN for Bouygues in France [DAL-840]
17. Improved Telit location reporting [DALP-226]
18. Improved collection of network LINK and Speed reporting
19. Implement Digi Remote Manager health metrics [DAL-707]
20. Added latest Telit LE910_XX_V2 firmware md5 sums

SECURITY FIXES

1. Update to openssl-1.0.2r (security) CVE-2019-1559
2. busybox: fix for CVE-2014-9645 [DAL-1159]
3. busybox: fix for CVE-2017-16544 [DAL-1159]
4. libcurl: update to 7.64.1 (CVE-2017-8816, CVE-2017-8817, CVE-2017-8818, CVE-2018-0500 CVE-2018-1000300, CVE-2018- 1000301, CVE-2018-14618, CVE-2018-16839, CVE-2018-16840, CVE-2018-16842 CVE-2018-16890, CVE-2019-3822, CVE-2019- 3823)
5. libcurl: fixes for CVE-2018-1000007, CVE-2017-8818, CVE-2017-8816, CVE-2018- 1000005 Zebra 0.99.24: fix for CVE-2016-1245
6. busybox fixes for CVE-2016-6301, CVE-2016-2148, CVE-2017-16544, CVE-2016-2147, CVE- 2017-15874, CVE-2014-9645, CVE-2011-5325 [DAL-1159]
7. pppd update to 2.4.7 (CVE-2014-3158, CVE-2015-3310)
8. Kernel patch to resolve CVE-2019-11815

BUG FIXES

1. Remote cloud connections were locked until while long running commands completed [DAL-1177]
2. Fix major issue with multiple IPsec policies When two remote subnets are configured in 2 Policies for an IKEv2 tunnel only Policy 2 traffic will pass [DAL-934]
3. Corrections to CLI show route [DAL-1176]
4. CLI ***show system*** output included outdated current time and uptime [DAL-1172]
5. Errors on console during WebUI firmware update [DAL-1140]
6. Faster fetching of signal attributes for LE910_NA_V2 modem
7. Fixed bug with parsing out MCC/MNC from AT#RFSTS response (LE910NAv2)
8. Fixed cloud connector crash on shutdown
9. Fixed process management issue with cloud connector and configuration
10. Check for configured serial ports in ***show serial*** command

11. Fixed bug where ***show serial*** option is visible for devices with no serial ports [DAL-1114]
12. Web GUI input validation rewording to be consistent
13. DAL-CLI: fix typos in descriptions, titles, and minimums
14. WebUI: Ensure correct versions of static files are loaded (using md5hash)
15. Serial ports were mistakenly listed under ***Network*** for metrics and state
16. Metrics had incorrect title, "System" in descriptors/state.
17. ModemManager: Telit error reporting patch
18. Intelliflow crash fix (divide by 0 on some datasets)
19. Intelliflow improve error reporting
20. System maintenance tasks do not run during duration window if reboot time is set [DAL-960]
21. SPIKE: Asynchronous CLI under Digi Remote Manager [URMA-1996]
22. Firmware update through WebUI doesn't recover when some other page is clicked during the update process [DAL-869]
23. Signal/dbm/percentage inaccurate on Verizon 2G and 3G connections with MC7354 [DAL-786]
24. Verify and fix dual APN support on the LM940 [DAL-742]
25. Unable to establish dual-APN connection with AT&T using Sierra modem [DAL-813]
26. Telit: Added logic to protect new C1_AP modems from being bricked [DAL-744]
27. Telit: Added firmware check sum for version 414 of LE910-EU1 [DAL-822]
28. Update Telit LE910C1-NS modem firmware from 25.00.244 to 25.00.246 [NPIX-939]
29. Fix MTU support for PPP based connections
30. Added md5 sums for the latest Telit firmware for LE910_NA1

VERSION 19.1.134.81 (Feb 14, 2019)

- Initial mass production release for Digi IX14