TOC

26.7.90.14 - August 2026, Feature

Release category: **Mandatory**

These release notes document the changes since the DAL LTS 26.2.148.163 release. There has been a number of enhancements, security fixes, and bug fixes.

Enhancements

1. A new configuration option under **Network** > **Interface** > **WWAN/Modem** > **Modem** > **Connection** attempts per APN has been added to try an APN multiple times before moving to the next APN in the list (default: 1). The per-APN setting in the Custom APN list the number of attempts to be configured per APN.

2. A new configuration setting under **Network** > **Modems** > **WWAN** > **eSIM** bootstrap profile allows users to disable the bootstrap profile on the eSIM (default: enabled).

3. A new configuration setting under **VPN** > **IPsec** > **IKE** > **Phase 1** reauthentication allows rekeying instead of re-authenticating IKEv2 tunnels (default: rekey).

4. EX50-2: The Verizon OTA wait is now skipped when there is an APN that has been cached from a prior successful connection. This reduces reconnection delays.

5. Multicast IGMP proxy is now supported on all DAL platforms except EX12/EX15.

6. Multicast routing diagnostics have been added to the support report (ip_mr_vif, ip_mr_cache, igmp, igmp6, mroute, igmpproxy.conf, smcroute routes/groups, bridge mdb, mc_forwarding).

7. Multicast routing information is now included in the query_state details reported to Digi Remote Manager.

8. A new configuration option under **Central management** > **DRM** > **Maximum retry interval** has been added to configure exponential backoff for EDP connection retries (default max retry interval: 10 minutes).

9. The default **Central management** > **DRM** > **Restart timeout** has been updated from 30 minutes to 1 hour.

10. New configuration options **Central management** > **DRM** > **Management interface order** and **Management interface order failover timeout** allow configuring a preferred ordered list of interfaces for establishing the DRM EDP connection.

11. A new configuration option under **Services** > **DNS** > **No upstream server** allows the DNS server on the device to resolve only locally configured hostnames without using upstream DNS servers.

12. The skip-peer IPsec state has been added to query_state reporting sent to Digi Remote Manager.

13. The **Modem registration_timeout** configuration parameter is now a non-debug setting.

14. internet4gd.gdsp and blank APNs have been added to the built-in fallback APN list for Vodafone (PLMN 26202).

15. **IX25/IX30-2**: Support for Telstra firmware has been added for the IX25 and IX30-2 platforms.

Security fixes

Package updates will include all security updates for the stated release, unless stated otherwise.

1. The OpenSSL package has been updated to version 3.6.3.
    - CVE-2026-28386 CVSS Score: 7.5 High
    - CVE-2026-28387 CVSS Score: 8.1 High
    - CVE-2026-28388 CVSS Score: 7.5 High
    - CVE-2026-28389 CVSS Score: 7.5 High
    - CVE-2026-28390 CVSS Score: 7.5 High
    - CVE-2026-31789 CVSS Score: 9.8 Critical
    - CVE-2026-31790 CVSS Score: 7.5 High
2. The socat package has been updated to version 1.8.1.3.
    - CVE-2024-54661 CVSS Score: 9.8 Critical
3. The Ookla binaries have been updated to version 3.9.
    - CVE-2022-35409 CVSS Score: 9.1 Critical
    - CVE-2022-46393 CVSS Score: 9.8 Critical
    - CVE-2023-43615 CVSS Score: 7.5 High

- CVE-2023-52353 CVSS Score: 7.5 High
- CVE-2024-23775 CVSS Score: 7.5 High
- CVE-2025-47917 CVSS Score: 9.8 Critical
- CVE-2025-48965 CVSS Score: 7.5 High

4. The expat package has been updated to version 2.8.2.
    - CVE-2026-50219 CVSS Score: 5.9 Medium
    - CVE-2026-56131 CVSS Score: 4.9 Medium
    - CVE-2026-56132 CVSS Score: 6.9 Medium
    - CVE-2026-56403 CVSS Score: 6.9 Medium
    - CVE-2026-56404 CVSS Score: 6.9 Medium
    - CVE-2026-56405 CVSS Score: 6.9 Medium
    - CVE-2026-56406 CVSS Score: 6.9 Medium
    - CVE-2026-56407 CVSS Score: 6.9 Medium
    - CVE-2026-56408 CVSS Score: 6.9 Medium
    - CVE-2026-56409 CVSS Score: 6.5 Medium
    - CVE-2026-56410 CVSS Score: 6.9 Medium

- CVE-2026-56411 CVSS Score: 6.9 Medium
- CVE-2026-56412 CVSS Score: 5.9 Medium

5. The libldns package has been updated to version 1.9.2
    - CVE-2026-10846 CVSS Score: High 7.5
6. The libpcap package has been updated to version 1.10.6.
    - CVE-2025-11961 CVSS Score: 1.9 Low
    - CVE-2025-11964 CVSS Score: 1.9 Low
7. The libusb package has bene updated to version 1.0.30.
    - CVE-2026-23679 CVSS Score: 6.9 Medium
    - CVE-2026-47104 CVSS Score: 5.0 Medium
8. The sqlite package has been updated to version 3530300.
    - CVE-2025-70873 CVSS Score: 7.5 High
    - CVE-2026-11822 CVSS Score: 7.8 High
9. The musl package updated to version 1.2.6.
    - CVE-2026-6042 CVSS Score: 3.3 Low
    - CVE-2026-40200 CVSS Score: 8.1 High

Bug fixes

1. An issue where an IPsec weighted round robin failover would tear down a newly established tunnel on the backup peer has been resolved.

2. EX50-2: An issue when failing over with Verizon static SIMs taking more than 20 minutes has been resolved.

3. EX50-2: An issue where the cached APN could be overwritten with a blank APN resulting in longer reconnection times has been resolved.

4. IX25: An issue with the IX25 Ignition Sense not detecting the ignition line correctly has been resolved.

5. The following issues with Query State have been resolved:

    a. A failure due to the ARP cache exceeding 100 entries has been resolved. ARP table, DHCP leases, IPv4/IPv6 routes, BGP prefix/access lists, and DNS server counts have all had their limits increased.

    b. A timing issue when collecting IPsec tunnel details while the tunnel was reconnecting.

    c. Odd spikes in the Cellular RX/TX bytes being reported.

    d. Details may not be sent to Digi Remote Manager due to missing IPsec, Cellular, or GNSS location source details.

6. Details may not be reported to Digi Remote Manager due to failed NTP re-synchronizations.

7. An issue where SINR was not being reported for 5G connections with Telit modems has been resolved.

8. An issue when enabling an eSIM profile could report a failure when the profile was actually successfully enabled has been resolved.

9. An issue where remote serial SSH/TCP connections would fail with LDAP authentication has been resolved.

10. An issue where EDP connections would be attempted three times in succession each time the device tried to connect to Digi Remote Manager has been resolved. Only one attempt is now made per connection interval.

11. An issue where firmware downloads could get interrupted due to the presence of an old or corrupted firmware file on the local device filesystem has been resolved.

12. An issue with the eSIM profile change report not being generated and sent to Digi Remote Manager has been resolved.

13. An issue with accessing the serial port via the Digi Remote Manager terminal has been resolved.

14. IX25 Redcap: An issue with the IX25 RedCap modem needing to be reset when switching SIMs, resulting in the device being disconnected from the network for over 5 minutes, has been resolved.

15. IX25 Redcap: An issue with the IX25 RedCap modem where VoLTE enabled caused a delay when switching from Verizon to T-Mobile has been resolved.

16. IX40: The watchdog has been updated to detect a problem when an all zeros are read when checking the Ethernet PHY on the IX40.

17. The watchdog has been updated to detect when the EM9191 modem does not appear on the USB bus after boot and to reboot the device after 3 minutes if the modem is not detected.

Deprecations

1. IX25: The Python support has been removed from IX25 firmware image and is now provided as a separate live image that can be downloaded from Digi Remote Manager.

DAL OS firmware update guidelines

Digi recommends that users of DAL OS devices update firmware in Digi Remote Manager.

> **TIP** If you are updating many routers, see Best practice | Update the firmware on multiple routers using a template.

It is also recommended that you review the following:

- Release information
- What's new and release notes for the current firmware version running on your devices, as well as any newer ones as this information may affect your update plan.

Known issues

- **TX54 product models**

  The Serial status and statistics for the TX54 are incorrect on the Web UI and CLI (DAL-5763].

- **Bridging traffic from devices connected on an Ethernet port or Wi-Fi AP**

  Due to the 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].

- **IPsec using Default Router as the Local Endpoint**

  There is an issue with IPsec where the tunnel will not come up when the default route is used as the Local Endpoint and the tunnel is not acting as the initiator. Specifying the interface type for the local endpoint should resolve the issue. [DAL-11361].

- **SSH / SCP login slow when FIPS mode is enabled**

  Logging into SSH or SCP when FIPS mode is enabled can take more than 20 seconds. [DAL-12606].

Primary Responder mode considerations

DAL OS 23.9 and later supports a PR[1] mode that can be enabled on any device. When enabled, the device acts as a Primary Responder PR device with a security-hardened, feature-restricted firmware targeted to comply with AT&T FirstNet® and Verizon ResponseVerify™ security requirements.

Features not available	Features available but disabled by default	Features enabled when PR mode is enabled
Telnet	SSH*	FIPS mode
Raw TCP listeners for serial ports	Wi-Fi pre-configured access points	
Wi-Fi WPA1 encryption	Internal serial console port	
Backup configuration file restore	USB ports	

*For DAL OS 25.8 feature release and newer, Primary Responder mode now requires key-based SSH authorization.

Additional considerations

- Users are prompted to enable two-factor authentication.
- A notification will appear in both the Web UI and CLI if the DAL device has Primary Responder mode enabled, but there are local users who do not have two-factor authentication enabled.

[1]Primary responder

- The `system custom-default-config` CLI command available in release 24.12 cannot be run in Primary Responder mode.

Devices that use DAL OS firmware

Changes to DAL OS firmware for supported Cellular business unit devices are documented in this documentation portal and in the corresponding device user guides:

Console server	Enterprise	Industrial	IoT gateway and cellular router	Transportation
Connect IT Mini Connect IT 4	EX12 EX15 EX50	IX10 IX20 IX25 IX30 IX40	IX15	TX40 TX54 TX64 TX64 RAIL TX65

Step updates

If your devices are running a firmware version **earlier than 24.6.17.54** and you want to update them to version **24.9.79.151** or newer:

1. Do a step update to version **24.6.17.69**.
2. Proceed with updating to newer versions.

Glossary

#

2FA
Two Factor Authentication

A

AI
Artificial Intelligience

API
Application Programming Interface

AT
Attention

C

CA
Carrier Aggregation

CLI
Command Line Interface

CMP
Connectivity Management Portal

CSV
Comma Separated Values

CTS
Clear to Send

D

DAL OS
: Digi Accelerated Linux Operating System

DANI
: Digi Artifical Network Intelligience

DCD
: Data Carrier Detect

DL
: Download

DRM
: Digi Remote Manager

DSR
: Data Set Ready

DSSS
: Dual SIM Single Standby

E

eID
: Embedded Identity Document

eIM
: eSIM IoT Remote Manager

eMBB
: Enhanced Mobile Broadband

ERC/CIP

Ethereum Request for Comments/Cardano Improvement Proposal

eSIM

Embedded Subscriber Identity Module

eUICC

Embedded Universal Integrated Circuit Card

EX

Enterprise

F

FOTA

Firmware Over-the-Air

G

GPS

Global Positioning System

GSMA

Global System for Mobile Communications Association

H

HTTPS

Hypertext Transfer Protocol Secure

I

IMSI

International Mobile Subscriber Identity

IP
: Internet Protocol

IPA
: IoT Profile Assistant

IX
: Industrial

J

JSON
: JavaScript Object Notation

L

LAN
: Local Area Network

LPA
: Local Profile Assistant

LTS
: Long Term Support

M

MBIM
: Mobile Broadband Interface Model

MCP
: Model Context Protocol

mDNS
: Multicast Domain Name System

MIoT

Massive Internet of Things

MNO

Mobile Network Operator

MSP

Managed Service Provider

MVNO

Mobile Virtual Network Operator

N

NMEA

National Marine Electronics Association

NSA

Non-Standalone

O

OTA

Over the Air

P

PLC

Programmable Logic Controller

PLMN ID

Public Land Mobile Network Identifier

PR

Primary responder

Q

QoS
: Quality of Service

R

RSP
: Remote SIM Provisioning

RTU
: Remote Terminal Unit

S

SA
: Standalone

SGP
: Standardized Global Platform (for Secure Remote SIM Provisioning)

SIM
: Subscriber Identity Module

SPN
: Service Provider Name

SSH
: Secure Shell or Secure Socket Shell

SSO
: Single Sign On

T

TAIP
Trimble ASCII Interface Protocol

TCP
Transmission Control Protocol

TX
Transportation

U

UI
User Interface

UL
Upload

URL
Uniform Resource Locator

URLLC
Ultra-Reliable Low Latency Communication

V

VLAN
Virtual Local Area Network

VR
Virtual Reality

W

WAN

Wide Area Network

WLAN

Wide Local Area Network

WWAN

Wireless Wide Area Network