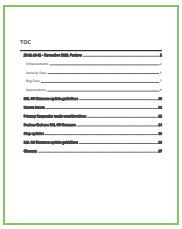
TOC

25.8.1.6 - August 2025, Feature



Release category: **Mandatory**

Features

1. eSIM support has been added to the following platforms:
    - EX15 (using the EG25-G modem module)
    - EX50 (using RM520N-GL modem module)
    - IX10 (using EG25-G modem module)
    - IX20 (using EG25-G modem module)
    - IX40 5G
    - TX40 5G

Enhancement

1. The Factory Erase support has been updated with the following:
    - A new configuration to perform a complete factory erase with a single button push.
    - Non system files in the /opt directory will be erased.
    - Remove the APNs configured in the cellular module.

2. A network performance monitoring feature has been added that will periodically test the network. It will send out a number of ping packets and collect minimum, maximum and average latency, jitter, and packet loss. It can also do an hourly SpeedTest over the interface to collect upload and download rates.

   The results are uploaded to Digi Remote Manager as part of the Query State data.

3. The **SSH support** has been updated so that **only SSH key authentication can be used in Primary Responder mode**.

   - **Users that use SSH passwords with Primary Responder SHOULD update their configuration to use SSH keys before updating to this firmware version.**

4. Python has been included in the IX30 build for the IX30-0EG4 variant. This means the live image is no longer required.

5. Added support for Docomo and KDDI carriers for modem firmware selection and default APNs.

Security fixes

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

1. The Busybox package has been patched to resolve CVE-2022-48174 [DAL-11784]

   CVE-2022-48174 CVSS Score: 9.8 Critical

2. The Curl package has been updated to version 8.13.0

   CVE-2025-0725 CVSS Score: 7.3 High

3. The OpenSSL package has been updated to v3.5.1 [DAL-11808]

CVE-2024-13176 CVSS Score: 4.1 Medium

CVE-2025-4575 CVSS Score: 6.5 Medium

4. The StrongSwan package has been updated to v6.0.1 [DAL-10822]
5. The NTP package has been updated to v4.2.8p18 [DAL-11270]

   CVE-2023-26551 CVSS Score: 5.6 Medium

   CVE-2023-26552 CVSS Score: 5.6 Medium

   CVE-2023-26553 CVSS Score: 5.6 Medium

   CVE-2023-26554 CVSS Score: 5.6 Medium

   CVE-2023-26555 CVSS Score: 6.4 Medium
6. The libcurl package has been updated to v8.13.0 [DAL-11547]

   CVE-2025-0725 CVSS Score: 7.3 High
7. The OpenSSH package has been updated to 10.0p2 [DAL-11584]

   CVE-2025-32728 CVSS Score: 3.8 Low
8. The net-tools package has been patched to resolve a CVE. [DAL-11548]

   CVE-2025-46836 CVSS Score: 6.6 Medium
9. The CA certificates on the device have been updated. [DAL-11668]

- Added the CA certificate from edp12.devicecloud.com
- Refreshed CA certificates using the 2025-05-20 Mozilla bundle
- Certificates with sha1WithRsaEncryption signatures have been removed.
- Remove references to unique.crt (used with AView)

10. An issue with the DAL self-signed certificate not being renewed when it expires has been resolved. [DAL-11641]

Bug fixes

1. An issue with the EX50 device not being able to connect to the carrier Softbank has been resolved. [DAL-10697]
2. An issue with the TX40 Wi-Fi not working in the 25.5 release has been resolved. [DAL-11733]
3. An issue with the TX64 5G device not being able to connect to the carrier Softbank has been resolved. [DAL-10697]
4. An issue with the OpenVPN server not starting properly from boot up has been resolved. [DAL-11240]
5. An issue where SureLink was attempting to test an IPsec tunnel before it had fully come up which prevented the IPsec from being fully established has been resolved. [DAL-11449]
6. An issue with the IPsec uptime and disconnect query state statistics being incorrect has been resolved. [DAL-11752]
7. An issue setting the baud rate to 5787 for RealPort has been resolved. [DAL-11661]

8. An issue when using a proxy to connect to Digi Remote Manager has been resolved. [DAL-11675]

9. An issue when changing a user password and not being verified in Primary Responder mode has been resolved. [DAL-11664]

10. An issue with commas and single and double quotes being used in the APN usernames and passwords which were causing authentication failures has been resolved. [DAL-11594]

    - Commas should not be used in APN usernames or passwords.
    - Single quotes can be used in APN usernames and passwords.
    - Double quotes should not be used except with the Telit FN990 cellular module.

11. An issue where scheduled scripts were not being started at boot up due to system clock changes has been resolved. [DAL-11743]

12. An issue with cellular band selection has been resolved. [DAL-11741]

13. An issue with mounting the shared read/write directories inside a container has been resolved. [DAL-10854]

14. An issue with TX54 5G units (using the Telit MV31-W modem) not displaying the RSRP and RSRQ for LTE connections has been resolved. [DAL-11815]

15. An issue with the Modbus gateway support reading a serial port not configured for Modbus has been resolved. [DAL-11366]

Deprecated

1. The health metrics feature has been disabled by default as they have been obsoleted. Digi Remote Manager now uses the Query State data to generate metrics, which are more efficient and use less bandwidth.

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

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.

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.

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