

# TOC

---

<b>25.11.10.42 - November 2025, Feature</b> .....	<b>2</b>
Enhancements .....	2
Security fixes .....	5
Bug fixes .....	7
Deprecations .....	9
<b>DAL OS firmware update guidelines</b> .....	<b>10</b>
<b>Known issues</b> .....	<b>11</b>
<b>Primary Responder mode considerations</b> .....	<b>12</b>
<b>Devices that use DAL OS firmware</b> .....	<b>14</b>
<b>Step updates</b> .....	<b>15</b>
<b>DAL OS firmware update guidelines</b> .....	<b>16</b>
<b>Glossary</b> .....	<b>17</b>

# 25.11.10.42 - November 2025, Feature

Release category: **Recommended**



There have been a number of enhancements, security fixes, bug fixes, and a deprecation for this release.

## Enhancements

1. A number of updates have been made to the eSIM support:
  - a. Support for bootstrap profiles. Traffic on the bootstrap profile is restricted to the following connections to allow for carrier profiles to be uploaded:

Host	Allowed connections
Digi Remote Manager	<ul style="list-style-type: none"><li>• edp12.devicecloud.com</li><li>• proxy.devicecloud.com</li><li>• test.idigi.com</li><li>• tm1.idigi.com</li><li>• dm1.devicecloud.com</li><li>• dm2.devicecloud.com</li></ul>
NTP	<ul style="list-style-type: none"><li>• time.devicecloud.com</li></ul>
Kigen	<ul style="list-style-type: none"><li>• eim-production-0.kigen.com</li></ul>

- b. Support for eSIM profile failover when making a cellular connection has been added. The device will attempt make a connection using each profile on the eSIM until a successful cellular connection is established, with the bootstrap profile being the last profile to be used.
  - c. eSIM information including profiles is now included in the Query State information. The information is pushed up to Digi Remote Manager on change rather than waiting for the next upload interval.
2. The Wi-Fi WPA3 Enterprise support has been updated with a new WPA3-192 security option to support better compatibility.

The original WPA3 Enterprise security setting has been updated to use 128-bit WPA3.

The new WPA3-192 Enterprise security setting use 192-bit WPA3.



**NOTE** Users currently using WPA3 Enterprise setting will be migrated to the new WPA3-192 setting.

3. The configuration support has been updated to minimize the CPU and memory utilization on the device.
4. The Web UI has been updated to reduce the time taken to load pages.
5. A REST API has been added to allow the query state information to be retrieved directly from the device.
6. A new option has been added to configure which interface to use for Digi Remote Manager connections.

The new configuration is **cloud > drm > drm\_interface <interface>**.

7. The IPsec support has been updated as follows:

- The IPsec peer configuration has moved from **vpn > ipsec > tunnels > name > remote > hostnames** to **vpn > ipsec > tunnels > name > remote > peers**
- The peer selection configuration parameter has changed from **vpn > ipsec > tunnels > name > remote > hostname\_selection** to **vpn > ipsec > tunnels > name > remote > peer\_selection**
- A new weighted round-robin algorithm has been added to allow certain peers to be more likely used.
- An individual peer ID can now be configured for each peer if required.
- The IPsec certificate and key settings have been made private so that it is not possible to read the values once they have been entered.

8. The SNMP trap support has been updated to allow the hostname to be used when sending a trap. The default is to use the MAC address.

9. The local Web UI link to documentation has been updated to use the new [Digi Cellular and Networking documentation portal](#).

10. The following new T-Mobile IOT APNs have been added to the APN list

- iot.cc
- static.iot
- static.iot.t-mobile.com

11. The priority of the AT&T broadband and Verizon vzwinternet APNs have been increased so that they are attempted first when using the built-in APN list.
12. The firmware update process, when used via the CLI or Web UI, has been updated to check for a minimum firmware version to help users to update to required intermediate firmware version first.

## Security fixes

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

1. The Linux kernel has been updated to 6.12.46 [DAL-11496]
2. The OpenSSL package has been updated to v3.5.4 [DAL-12433]
  - [CVE-2025-9230](#) CVSS Score: 7.5 High
  - [CVE-2025-9231](#) CVSS Score: 6.5 Medium
  - [CVE-2025-9232](#) CVSS Score: 5.9 Medium
3. The expat library has been updated to v2.7.3 [DAL-12434]
  - [CVE-2025-59375](#) CVSS Score: 7.5 High
4. The jerryscript package has been updated to version 3.0.0 [DAL-12398]
5. The glib library has been updated to v2.86.0 [DAL-11997]

- [CVE-2025-6052](#) CVSS Score: 7.5 High
  - [CVE-2025-7039](#) CVSS Score: 3.7 Low
6. The procps package has been updated to v4.0.5 [DAL-11961]
- [CVE-2018-1121](#) CVSS Score: 5.9 Medium
  - [CVE-2023-4016](#) CVSS Score: 3.3 Low
7. The Linux PAM library has been updated to v1.7.1 [DAL-11972]
- [CVE-2020-27780](#) CVSS Score: 9.8 Critical
  - [CVE-2022-28321](#) CVSS Score: 9.8 Critical
  - [CVE-2024-22365](#) CVSS Score: 5.5 Medium
  - [CVE-2025-6020](#) CVSS Score: 7.8 High
8. The sqlite package has been updated to v3.50.4 [DAL-11945]
- [CVE-2025-6965](#) CVSS Score: 7.2 High
9. An issue with TACACS+ accepting unauthenticated replies has been resolved. [DAL-12391]

## Bug fixes

1. The following issues with the Query State support has been resolved.
  - Gaps in the SureLink RTT value being reported. [DAL-12451]
  - Query state data not been uploaded to Digi Remote Manager for a period of time. [DAL-12539]
2. An issue with configured scripts not starting at boot-up has been resolved. [DAL-11743]
3. The following issues with IPsec have been resolved:
  - A missing firewall rule was causing packets to be dropped. [DAL-11998, DAL-12113]
  - The internal Linux interface name was being reported instead of the DAL interface name in the Query State information. [DAL-12046]
  - Using Default route as the local endpoint and not acting as the initiator would prevent the IPsec tunnel from coming up. [DAL-11361]
4. An issue with IX40 and TX40 occasionally not getting an IPv4 address when using a 5G multi-slice SIM has been resolved. [DAL-12258]
5. The following issues with WAN Bonding have been resolved:
  - The WAN Bonding status not being reported in the Query State information. [DAL-12298]

- The WAN Bonding server IP address being incorrectly displayed in show wan-bonding command. [DAL-12173]
  - The interface used to connect to Digi Remote Manager when using WAN Bonding was being incorrectly displayed. [DAL-10738]
6. An issue where Digi Remote Manager cannot access files via symbolic links to files in directories that Digi Remote Manager cannot access has been resolved. [DAL-12292]
  7. An issue where ModemManager can be unintentionally disabled when a modem is being updated has been resolved. [DAL-12285]
  8. An issue where a serial port Rx displays 0 if no signals are active has been resolved. [DAL-12281]
  9. An issue with cellular related events not being sent to remote syslog servers has been resolved. [DAL-12209]
  10. A memory leak experienced when accessing the runt table in the Accelerated MIB has been resolved. [DAL-12176]
  11. An issue with the Wireguard client on Windows 10 has been resolved. [DAL-12083]
  12. An issue where the cellular module would not initialize if the modem match setting was set to “any” has been resolved. [DAL-11942]
  13. An issue with Python scripts using the threading module where a NoneType exception was being unexpectedly thrown has been resolved. [DAL-10521]


14. An issue with the auto APN support for AT&T where a blank APN could be used has been resolved. [DAL-12558]
15. An issue with Wi-Fi where the WPA supplicant process was not terminated correctly has been resolved. [DAL-12554]
16. An error message that was being displayed regarding disabled interfaces when running a SpeedText on Digi Remote Manager over a specific interface has been resolved. [DAL-12447]
17. Excessive debug messages related to the scheduling of scripts have been removed. [DAL-12578]

## **Deprecations**

1. The health metrics support has been removed from DAL. [DAL-9683]

# 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<sup>1</sup>** 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.

---

<sup>1</sup>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
<a href="#">Connect IT Mini</a>	<a href="#">EX12</a>	<a href="#">IX10</a>	<a href="#">IX15</a>	<a href="#">TX40</a>
<a href="#">Connect IT 4</a>	<a href="#">EX15</a>	<a href="#">IX20</a>		<a href="#">TX54</a>
	<a href="#">EX50</a>	<a href="#">IX25</a>		<a href="#">TX64</a>
		<a href="#">IX30</a>		<a href="#">TX64 RAIL</a>
		<a href="#">IX40</a>		


# 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 Intelligence

**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 Artificial Network Intelligence

### **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