TOC

22.5.50.62 - June 2022, Feature **2**

New features 2

Enhancements 3

Bug fixes 5

Security fixes 7

DAL OS firmware update guidelines **8**

Known issues **9**

Primary Responder mode considerations **10**

Devices that use DAL OS firmware **12**

Step updates **13**

DAL OS firmware update guidelines **14**

Glossary **15**

22.5.50.62 - June 2022, Feature

Release category: **Mandatory**

New features

1. Serial PPP dial-in mode for handling AT-based connection requests from a device connected to a serial port and providing IPv4 networking to the device [DALP-880]

2. New **Network** → **SCEP Client** settings and underlying functionality to support connecting to additional SCEP servers, including Fortinet FortiAuthenticator, DigiCert, EJBCA, and Windows server [DALP-1007, DALP-1022]

3. New **show scep** Admin CLI command for showing the sync status, expiration dates, and additional details of any configured SCEP clients [DAL-6069]

4. Support for enabling add-on features from Digi Remote Manager [DALP-673]

5. EX12/EX15/EX50: Containerized python environment is now available. To enable python support on your EX15/EX50 device running 21.11.60.63 or newer firmware, you must update to 22.5.50.62 firmware and install a Python container live image. See the linked knowledgebase article here

6. EX15/EX15W/EX50/IX20/IX20W/IX30/TX54/TX64: 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]

7. EX50: New 5G slice support under **Network** → **Modems** → **Default slice information** for configuring the slice type to set in the 5G modem [DAL-5973]

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

1. Remove time.accns.com from default list of NTP servers unless **Central management** → **Service** is set to **aView** at the time of updating firmware from version 22.2.9.85 or older [DAL-5543]

2. Added new **system.log.persistent_path** configuration setting to specify where system logs are stored locally, which could be on the device or to an external storage (e.g. USB flash drive, SD card, etc) [DALP-946]

3. New **Services** → **Location** → **Destination servers** → **Behavior when fix is invalid setting** to control the NMEA message content sent when there is no valid fix from any of the configured location sources [DAL-5984]

4. Improved the message shown on the **System** → **Configuration Maintenance** page of the web UI if an error is encountered when restoring from a backup config file [DAL-6141]

5. Include the hostname of the device in the client .ovpn file listed on the **Status** → **OpenVPN** → **Servers** page in the web UI [DAL-6157]

6. Add support for the CP210X serial driver for connecting to Cisco USB console ports [DAL-6119]

7. Filter out non-Internet type APNs from our APN fallback list [DAL-6227]

8. Automatically power cycle the cellular modem in the event that a modem reset Surelink action fails [DAL-6268]

9. Enable Surelink **reset_modem** action by default on cellular interfaces and set fail count to 3 [DAL-6275]
10. Add cellular APN and cellular connection duration as datapoints sent to DigiRM [DAL-5902]
11. Ensure modem is in enabled state before attempting to connect [DAL-6163]
12. Omit non-production modem firmware from the OTA query results in the **Status** → **Modems** page of the web UI [DAL-6301]
13. An issue with the default Wi-Fi AP SSIDs being too long on the TX64 Rail platform has been resolved. [DAL-6329]
14. EX50: Improved EX50 cellular throughput by integrating NSS acceleration drivers [DAL-5692]
15. IX30: Power off serial port when not enabled [DAL-5991]
16. IX30: Power off the Ethernet ports when not enabled [DAL-6063]
17. TX: The SCEP client support has been enhanced to work with a wider range of SCEP servers. The following SCEP servers have been tested:
    - Fortinet FortiAuthenticator
    - DigiCert
    - EJBCA
    - Windows Server

A new show scep CLI command has been added to display the status of the configured SCEP clients.

18. TX: The Wi-FI Scanner functionality has been updated to allow the Wi-Fi Scanner results to be pushed to one or more remote servers using a TCP or HTTP connections.

19. TX64: 5G slicing support for a single slice has been added to the TX64 5G platforms.

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]
6. EX50: Update to OpenSSL 3.0.3 to enable FIPS 140-2 support [DALP-738]
7. TX64: The OpenSSL package on the TX64 has been updated to 3.0.2.
8. TX54/LR54: The OpenSSL package on the TX54 and LR54 platforms has been updated to 1.1.1o. [DAL-6303]

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 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 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