

TOC

24.9.79.151 - November 2024, Feature	2
New features	2
Enhancements	3
Security fixes	4
Bug fixes	8
DAL OS firmware update guidelines	12
Known issues	13
Primary Responder mode considerations	14
Devices that use DAL OS firmware	16
Step updates	17
DAL OS firmware update guidelines	18
Glossary	19

24.9.79.151 - November 2024, Feature

Release category: **Mandatory**

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 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.
17. TX40: The amount of messages logged by the TX40 Wi-Fi driver to prevent the system log from being saturated with Wi-Fi debug messages.

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

1. An issue where the same ICCID was being reported for both SIM1 and SIM2 has been resolved. [DAL-9826]
2. 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]
3. An issue where a device could get stuck using a particular SIM slot even though no SIM was detected has been resolved. [DAL-9828]
4. An issue where US Cellular would be displayed as the carrier when connected to Telus has been resolved. [DAL-9911]
5. An issue with Wireguard where the public key generated using the Web UI not being saved correctly when has been resolved. [DAL-9914]
6. 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]


7. An issue where IPsec tunnels disconnected when old SAs were being deleted has been resolved. [DAL-9923]
8. An issue where starting BGP would cause an error to be output on the Console port has been resolved. [DAL-10062]
9. An issue where a serial bridge would fail to connect when FIPS mode was enabled has been resolved. [DAL-10032]
10. An issue where the serial port could stall when changing the setting of a serial port has been resolved. [DAL-5230]
11. 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]
12. An issue with the SystemInfo group in the Accelerated MIB not being indexed correctly has been resolved. [DAL-10173]
13. An issue with the RSRP and RSRQ not being reported on EX50 devices has been resolved. [DAL-10211]
14. The Deutsche Telekom 26202 PLMN ID and 894902 ICCID prefix have been added to ensure the correct Provider FW is displayed. [DAL-10212]
15. 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]
16. An issue where the default values for boolean parameters were not being displayed in the Web UI has been resolved. [DAL-10290]

17. An issue with validating configuration changes made by a custom script have been resolved. [DAL-10450]
18. An issue preventing read-only users from running the show surelink or event list CLI commands has been resolved. [DAL-10418]
19. An issue where a blank APN was being written in mm.json file has been resolved. [DAL-10285]
20. An issue where the watchdog would incorrectly reboot the device when the memory warning threshold is exceeded has been resolved. [DAL-10286]
21. The Python live image has been updated to include the libsqlite3.so library which is required by the Python sqlite3 module. [DAL-9661]
22. The following issues with the Bluetooth scanner have been resolved
 - a. Some detected Bluetooth devices were missing from data sent to remote servers. [DAL-9902]
 - b. The Bluetooth scanner data being sent to remote devices did not include host-name and location fields. [DAL-9904]
 - c. The device would reboot intermittently when the Bluetooth scanner feature was enabled with an output filter. A new purge_timeout option has been added to allow the user to specify that old sightings are to be removed from the list of confirmed static devices after the specified time in seconds. The default is 0s which means purge_timeout is disabled by default.

23. IX20: An issue where the IX20W had significantly slowed down has been resolved. [DAL-10182]
24. TX40: An issue where the Wi-Fi clients connected to a TX40 not being displayed on CLI **show wifi ap <name>** command and on the Web UI has been resolved. [DAL-10127]
25. TX40: An issue where the 5G band information was not being displayed on the TX40 has been resolved. [DAL-8926]
26. TX40: An issue where the TX40 GNSS support could lose its fix after remaining connected for many days has been resolved. [DAL-9905]
27. TX54: The 5G support on the TX54 platforms has been updated to default to NSA mode. [DAL-9953]
28. TX64: An issue with the RSRP and RSRQ not being reported on TX64 5G devices has been resolved. [DAL-10211]

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 **PR¹** 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.

¹Primary 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	EX12	IX10	IX15	TX40
	EX15	IX20		TX54
Connect IT 4	EX50	IX25		TX64
		IX30		TX64 RAIL
		IX40		

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