TOC

24.6.17.54/24.6.17.56 - June 2024, Feature

Release category: **Mandatory**

New feature

Release 24.6.17.56 for IX10

1. For the IX10, Hybrid IPv4 addressing mode support was added to the Ethernet interface.

   In this mode, the device will first attempt to get an IPv4 address using DHCP. If it fails to get an IPv4 address after 1 minute, it will revert to using the static configured IPv4 address. This allows the IX10 (when running default configuration) to automatically connect to and be managed by Digi Remote Manager when connected into a network that supports DHCP. The addressing type must be changed to either dhcp or static when the first configuration change is made on the device.

Enhancements

Release 24.6.17.54 for all products

1. The **WAN-Bonding** support has been enhanced with the following updates
   a. SureLink support.
   b. Encryption support.
   c. SANE client has been updated to 1.24.1.2.
   d. Support for configuring multiple WAN Bonding servers.

e. Enhanced status and statistics.

f. The WAN Bonding status is now included in the metrics sent to Digi Remote Manager.

2. The **cellular** support has been enhanced with the following updates

   a. The special PDP context handling for the EX50 (EM9191) modem which was causing issues with some carriers. A common method is now used to set the PDP context.

   b. The cellular connection back-off algorithm has been removed as the cellular modems have built-in back off algorithms that should be used.

   c. The cellular APN lock parameter has been changed to APN selection to allow the user to select between using the built-in Auto-APN list, the configured APN list or both.

   d. The cellular Auto-APN list has been updated.

   e. The MNS-OOB-APN01.com.attz APN has been removed from the Auto-APN fallback list.

3. The **Wireguard** support has been updated to allow the user to generate a client configuration that can be copied onto another device.

   This is done using the command wireguard generate <tunnel> <peer>

   Extra information may be needed from the client depending on config:

   a. How the client machine connects to the DAL device. This is needed if the client is initiating any connections and there is no keepalive value.

    b. If the client generates their own private/public key, they will need to set add that to their configuration file. If this is used with 'Device managed public key', every time a generate is called on a peer, a new private/public key is generated and set for that peer, this is because we do not store any private key information of any clients on the device.

4. The SureLink support has been updated to

    a. Shutdown the cellular modem before power cycling it.

    b. Export the INTERFACE and INDEX environment variables so that they can be used in custom action scripts.

5. The uploading of device events to Digi Remote Manager has been enabled by default.

6. The logging of SureLink events has been disabled by default as it was causing the event log to be saturated with test pass events.

   SureLink messages will still appear in the system message log.

7. The **show surelink** command has been updated.

8. The status of the System Watchdog tests can now be obtained via Digi Remote Manager, the Web UI and using CLI command show watchdog.

9. The Speedtest support has been enhanced with the following updates

    a. To allow it to run on any zone with src_nat enabled.

    b. Better logging when a Speedtest fails to run.

10. The Digi Remote Manager support has been updated to only re-establish connection to Digi Remote Manager if there is a new route/interface it should utilize to get to Digi Remote Manager.

11. A new configuration parameter, **system** > **time** > **resync_interval**, has been added to allow the user to configure the system time resynchronization interval.

12. Support for USB printers has been enabled. It is possible to configure to device to listen for printer requests via the socat command

    ```
    socat - u tcp-listen:9100,fork,reuseaddr OPEN:/dev/usblp0
    ```

13. The SCP client command has been updated with a new legacy option to use the SCP protocol for file transfers instead of the SFTP protocol.

14. Serial connection status information has been added to the Query State response message that is sent to Digi Remote Manager.

15. Duplicate IPsec messages have been removed from the system log.

16. The debug log messages for the health metrics support have been removed.

17. The help text for the FIPS mode parameter has been updated to warn the user the device will automatically reboot when changed and that all configuration will be erased if disabled.

18. The help text for the SureLink delayed_start parameter has been updated.

19. Support for the Digi Remote Manager RCI API compare_to command has been added.

20. IX30: The IX30 analog IO calibration data has been removed from configuration backups.
21. TX40: The TX40 Wi-Fi driver has been updated
    a. Supports up to 64 client connections.
    b. Can now support 2 Wi-Fi Client interfaces, one on the 2.4 GHz band and one on the 5 GHz band.
    c. In total, the TX40 can support up to 3 interfaces, with any combinations of Access Points and clients.
22. TX54: The TX54 Bluetooth scanner support has been updated with new filtering and data forwarding options.

Security fixes

1. The setting for **Client isolation on Wi-Fi Access Points** has been changed to be enabled by default. [DAL-9243]
2. The Modbus support has been updated to support the Internal, Edge and Setup zones by default. [DAL-9003]
3. The Linux kernel has been updated to 6.8. [DAL-9281]
4. The StrongSwan package has been updated to 5.9.13 [DAL-9153]

   CVE-2023-41913 CVSS Score: 9.8 Critical
5. The OpenSSL package has been updated to 3.3.0. [DAL-9396]
6. The OpenSSH package has been updated to 9.7p1. [DAL-8924]

CVE-2023-51767 CVSS Score: 7.0 High

CVE-2023-48795 CVSS Score: 5.9 Medium

7. The DNSMasq package has been updated to 2.90. [DAL-9205]

   CVE-2023-28450 CVSS Score: 7.5 High

8. The rsync package has been updated 3.2.7 for the TX64 platforms. [DAL-9154]

   CVE-2022-29154 CVSS Score: 7.4 High

9. The udhcpc package has been updated to resolve a CVE issue. [DAL-9202]

   CVE-2011-2716 CVSS Score: 6.8 Medium

10. The c-ares package has been updated to 1.28.1. [DAL9293-]

    CVE-2023-28450 CVSS Score: 7.5 High

11. The jerryscript package has been updated to resolve a number CVEs.

    CVE-2021-41751 CVSS Score: 9.8 Critical

    CVE-2021-41752 CVSS Score: 9.8 Critical

    CVE-2021-42863 CVSS Score: 9.8 Critical

    CVE-2021-43453 CVSS Score: 9.8 Critical

    CVE-2021-26195 CVSS Score: 8.8 High

    CVE-2021-41682 CVSS Score: 7.8 High

CVE-2021-41683 CVSS Score: 7.8 High

CVE-2022-32117 CVSS Score: 7.8 High

12. The AppArmor package has been updated to 3.1.7. [DAL-8441]
13. The following iptables/netfilter packages have been updated [DAL-9412]
    a. nftables 1.0.9
    b. libnftnl 1.2.6
    c. ipset 7.21
    d. conntrack-tools 1.4.8
    e. iptables 1.8.10
    f. libnetfilter_log 1.0.2
    g. libnetfilter_cttimeout 1.0.1
    h. libnetfilter_cthelper 1.0.1
    i. libnetfilter_conntrack 1.0.9
    j. libnfnetlink 1.0.2
14. The following packages have been updated [DAL-9387]

a. libnl 3.9.0

b. iw 6.7

c. strace 6.8

d. d. net-tools 2.10

e. ethtool 6.7

f. MUSL 1.2.5

15. The http-only flag is now being set on Web UI headers. [DAL-9220]

Bug fixes

1. The **WAN Bonding** support has been updated with the following fixes

    a. The client is now automatically restarted when client configuration changes are made. [DAL-8343]

    b. The client is now automatically restarted if it has stopped or crashed. [DAL-9015]

    c. The client is now not restarted if an interface goes up or down. [DAL-9097]

    d. The sent and receive statistics has been corrected. [DAL-9339]

    e. The link on the Web UI dashboard now takes the user to the Web-Bonding status page instead of the configuration page. [DAL-9272]

f. The CLI show route command has been updated to show the WAN Bonding interface. [DAL-9102]

g. Only the required ports rather than all ports are now opened in the firewall for incoming traffic in the Internal zone. [DAL-9130]

h. The show wan-bonding verbose command has been updated to comply with style requirements. [DAL-7190]

i. Data was not being sent through the tunnel due to an incorrect route metric. [DAL-9675]

j. The show wan-bonding verbose command. [DAL-9490, DAL-9758]

k. Reduced memory usage that causes issues on some platforms. [DAL-9609]

2. The **SureLink** support has been updated with the following fixes

a. An issue where re-configuring or remove static routes could cause routes being incorrectly added to the routing table has been resolved. [DAL-9553]

b. An issue where static routes were not being updated if the metric was configured as 0 has been resolved. [DAL-8384]

c. An issue where the TCP test to a hostname or FQDN can fail if the DNS request goes out of the wrong interface has been resolved. [DAL-9328]

d. An issue where disabling SureLink after an update routing table action leaves orphaned static routes has been resolved. [DAL-9282]

e. An issue where the show surelink command displaying incorrect status has been resolved. [DAL-8602, DAL-8345, DAL-8045]

f. An issue with SureLink being enabled on LAN interfaces causing issues with tests being run on other interfaces has been resolved. [DAL-9653]

3. An issue with the HW encryption on the EX15 platforms that was introduced in the 24.3 release has been resolved. [DAL-9682]

4. An issue where IP packets could be sent out of the wrong interface, including those with private IP addresses which could lead to being disconnected from the cellular network has been resolved. [DAL-9443]

5. The SCEP support has been updated to resolve an issue when a certificate has been revoked. It will now perform a new enrollment request as the old key/certificates are no longer considered secure to perform a renewal. Old revoked certificates and keys are now removed from the device. [DAL-9655]

6. An issue with how OpenVPN generated in server certificates has been resolved. [DAL-9750]

7. An issue where Digi Remote Manager would continue to display a device as connected if it had been booted locally has been resolved. [DAL-9411]

8. An issue with SureLink on IPsec tunnels using strict routing has been resolved. [DAL-9784]

9. A race condition when an IPsec tunnel is brought down and reestablished quickly could prevent the IPsec tunnel coming up has been resolved. [DAL-9753]

10. An issue when running multiple IPsec tunnels behind the same NAT where only interface could come up has been resolved. [DAL-9341]

11. An issue with IP Passthrough mode where the cellular interface would be brought down if the LAN interface goes down which meant the device was no longer accessible via Digi Remote Manager has been resolved. [DAL-9562]

12. An issue with multicast packets not being forwarded between bridge ports has been resolved. This issue was introduced in DAL 24.3. [DAL-9315]

13. An issue where an incorrect Cellular PLMID was being displayed has been resolved. [DAL-9315]

14. An issue with an incorrect 5G bandwidth being reported by the EX50 5G devices has been resolved. [DAL-9249]

15. An issue with selecting 5G_SA mode with the on the EX50 5G with the EM9191 modem running the 03.14.10 firmware has been resolved. [DAL-9346]

16. An issue with the RSTP support where it may initialize correct in some configurations has been resolved. [DAL-9204]

17. An issue where a device would attempt to upload the maintenance status to Digi Remote Manager when it is disabled has been resolved. [DAL-6583]

18. An issue with the Web UI drag and drop support which could cause some parameters being incorrectly updated has been resolved. [DAL-8881]

19. An issue with the Serial RTS toggle pre-delayed not being honored has been resolved. [DAL-9330]

20. An issue with the Watchdog triggering a reboot when not necessary has been resolved. [DAL-9257]

21. An issue where DMVPN could take a long time to come up on the EX50 has been resolved. [DAL-9254]

22. An issue where modem firmware updates would fail due to the index of the modem changing during the update and the status result not being reported to Digi Remote Manager has been resolved. [DAL-9524]

23. An issue with the cellular modem firmware update on Sierra Wireless modems has been resolved. [DAL-9471]

24. An issue with how the cellular statistics were being reported to Digi Remote Manager has been resolved. [DAL-9651]

25. IX40: An issue with IX40 5G units outside of North America selecting an incorrect generic cellular firmware image has been resolved. [DAL-9266]

26. IX40: An issue with the IX40 5G modem VoLTE and SIM hotswap settings being re-enabled after a carrier switch which resulted in longer connection times. [DAL-9264, DAL-9265]

27. IX20: An issue with the IX20W Wi-Fi connecting to Access Points using DFS channels with the DAL 24.3 release has been resolved. [DAL-8933]

28. IX10: An issue with IX10 SIM LEDs behavior has been resolved. [DAL-9593]

29. TX54: An issue with the HW encryption on the TX54 platforms that was introduced in the 24.3 release has been resolved. [DAL-9682]

30. TX54/TX64: The Wi-Fi driver support for the TX54 and TX64 platforms has been updated to improve performance. [DAL-9060]

31. TX64: An issue with the TX64 where the device can crash when connecting to a Wi-Fi Access Point has been resolved. [DAL-9317]

32. TX40: An issue with TX40 5G units outside of North America selecting an incorrect generic cellular firmware image has been resolved. [DAL-9266]

33. TX40: An issue with the TX40 5G units modem VoLTE and SIM hotswap settings being re-enabled after a carrier switch which resulted in longer connection times. [DAL-9264, DAL-9265]

34. TX40: An issue with the TX40 where changing the location service configuration could cause the cellular modem to disconnect has been resolved. [DAL-9201]

35. TX64: An issue where TX64 could not always connect to Wi-Fi Access Points using DFS channels has been resolved. [DAL-9298]

36. TX64: An issue with an incorrect 5G bandwidth being reported by the TX64 5G devices has been resolved. [DAL-9249]

37. TX64: An issue with selecting 5G_SA mode with the on the TX64 5G with the EM9191 modem running the 03.14.10 firmware has been resolved. [DAL-9346]

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