TOC

22.2.9.85 - March 2022, Feature

Release category: **Mandatory**

New features

1. Added new option under **System** → **Time** → **NTP** → **Use GNSS module** to enable the device to use its internal GNSS module as a date/time sync source [DAL-5760]
2. Initial release for the IX30 product
3. IX10/IX20: Realport serial mode support [DAL-5742]
    1. Realport DTR-pin flow control is not available on the IX10. Will be coming in our 22.5 release (see DALP-998)
4. TX54/TX64: The internal GNSS module on the TX54 and TX64 platforms can now be used as a time source for the NTP server support.

Enhancements

1. Update default Digi Remote Manager URL to edp12.devicecloud.com [DALP-972]
    1. In firmware versions 22.2.9.85 and newer, the default central management server changes from **my.devicecloud.com** to **edp12.devicecloud.com**. This change enables more secure connection negotiation and enables support for device certificates. If your device connections are managed by a firewall, or your devices do not have direct access to public DNS servers, you may be required to make firewall changes to open connectivity to edp12.devicecloud.com, or to enable DNS. See https://www.digi.com/support/knowledge-base/firewall-concerns-for-

outbound-edp-connections-to for more information about device connectivity to Digi Remote manager.

2. Increased web UI upload limit to 512MB [DAL-5694]

3. Added new **Surelink Switch SIM** and **Switch SIM fail count** options to specify how many times the Surelink test must run and fail on a cellular modem before the device switches to the alternate SIM slot [DAL-5717]

4. Support for standard SCEP servers [DALP-821] 1.

   Previously the SCEP client only supported syncing with Fortigate SCEP servers. Two new settings were added under the **Network** → **SCEP Client** options to control the CA identity and HTTP path to the CA

5. Renamed **VPN** → **IPsec** → **Tunnels** → **Policies** → **Local network** setting to **Local traffic selector** along with a new **Dynamic** option which allows users to configure a local network by protocol and/or port instead of a network address range [DAL-5645]

6. Added new **VPN** → **IPsec** → **Advanced** → **Debug level** option to specify the logging verbosity of IPsec messages in the device system logs (default is debug logging is disabled) [DAL-5720]

7. Added new **Serial** → **Autoconnect** → **Socket ID** string option to send the configured text to the remote server(s) when a TCP socket connection is opened to the serial port [DAL-5700]

8. New cat Admin CLI command for displaying file contents [DAL-5853]

9. Update /etc/config/scep_client/ directory to be read/write by admin users

10. Add ability for policy-based routes to override routing of packets through VPN tunnels, useful in the case where you only want packets from a certain source network to go through the tunnel [DAL-5317]

11. EX12-PR: Add container support to PR products and remove from 63xx-series legacy Accelerated products [DAL-5498]

12. EX12/1002-CM06/1003-CM07: Utilize T-Mobile carrier firmware if available for the cellular modem when using Sprint Curiosity SIMs [DAL-5466]

13. IX20-PR/IX20W-PR: Add container support to PR products [DAL-5498]

14. IX10: Support for the Quectel EC25-AFXD modem [DAL-5787]

15. IX10: Add ODIS/LWM2M parameters for EC25-AFXD modem [DAL-5840]

16. IX: 1002-CM06/1003-CM07: Utilize T-Mobile carrier firmware if available for the cellular modem when using Sprint Curiosity SIMs [DAL-5466]

17. TX54/TX64: A new TX54 and TX64 system power ignition off_delay CLI command has been added to allow the devices power off delay to updated without the configuration being updated. This means the next device reboot it will revert to its configured power off delay.

Bug fixes

The below bugs are all present on firmware versions 21.11.60.63 and older unless otherwise specified

1. Fixed HFSC class hierarchy setup for QoS policies to limit bandwidth used for shared links [DAL-5814]

2. Fixed issue preventing scheduled maintenance window from updating the maintenance_window datapoint in Digi Remote Manager if the maintenance window start time was between 00:00-00:59 [DAL-5765]

3. Fixed bug preventing MMS SMS messages from being received and parsed properly, preventing large out-of-band config changes from being received from central management portals [DAL-5538]

4. Fixed issue preventing transport-mode IPsec tunnels from initializing properly [DAL-5718]

5. Fixed issue where only the first policy would be setup on IKEv2 IPsec tunnels [DAL-5347]

6. Fixed issue preventing port forwarding firewall setups if the Destination port(s) setting was left blank [DAL-5860]

7. Fixed intermittent issue where the show dhcp-leases CLI output would sometimes not include all leases [DAL-5688]

8. Fixed system log errors when performing TACACS command authorization without having a TACACS server configured [DAL-5512]

9. Fixed interruption of active serial port connections when a user changes the serial port mode in the Digi device’s configuration settings [DAL-5698]

10. Fixed issue where Surelink tests aren’t reloaded if a user updates the network bridge or Wi-Fi configuration settings on the device [DAL-5406]

11. Prevent modbus setup issue by not allowing users to configure the device to use reserved address ranges [DAL-5905]
12. Fixed intermittent race condition in Surelink that could lead to a delay in setting up a WAN connection [DAL-5934]
13. Fixed issue with digidevice.sms python module processing empty SMS messages [DAL-5883]
14. EX15: Fixed link connectivity issues with 10Mbps Ethernet switches [DAL-5506]
15. EX15: Fixed intermittent link-dead messages when using an EX15 connected to a VeloCloud appliance [DAL-5657]
16. EX50: Fixed intermittent Wi-Fi LEDs when switching between Ethernet and cellular WAN connections [DAL-5660]
17. IX20W: Fixed issue preventing Wi-Fi metrics from being uploaded to DigiRM
18. TX54/LR54: An issue that where the TX54 and LR54 platforms failing to negotiate with some 10Mbps Ethernet switches has been resolved. [DAL-5506]

Security fixes

The highest level vulnerability that has been fixed in this release is listed as a Critical CVSS score of 10 Critical

1. Update python to version 3.10 [DAL-5499]
2. Update openssh to version 8.8p1 (CVE-2021-28041, CVE-2020-14145) [DAL-5451]

1. This deprecates support for RSA signatures using the SHA-1 hash algorithm by default, which may prevent old machines from SSH-ing to the Digi device. Please ensure your SSH tool (TeraTerm, PuTTY, etc) is up to date. If you need to re-enable SHA-1 hash support, you can do so by adding the following lines to the **Service → SSH → Custom configuration → Configuration file** text box in the Digi device's configuration settings:

    1. HostkeyAlgorithms +ssh-rsa

    2. PubkeyAcceptedAlgorithms +ssh-rsa

3. Update dnsmasq to version 2.86 (CVE-2021-3448) [DAL-5331]

    1. Fix problem with DNS retries in 2.83/2.84

    2. Fix a problem, introduced in 2.83, which could see DNS replies being sent via the wrong socket. On machines running both IPv4 and IPv6 this could result in sporadic messages of the form "failed to send packet: Network is unreachable" and the lost of the query

4. Update to Linux kernel version 5.15 [DAL-5546]

5. Add new **Service → Web administration → Minimum TLS version** configuration setting to allow users to specify which TLS versions are allowed in the local web UI (default minimum is TLS 1.2) [DAL-5408]

6. Update busybox to version 1.34.0 [DAL-5631]

CVE-2021-4237, CVE-2021-42374, CVE-2021-42375, CVE-2021-42376, CVE-2021-42377, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42383, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386

7. Update dbus to version 1.13.20 [DAL-5459]

   CVE-2020-12049, CVE-2019-12749

8. Update grub to version 2.06 [CVE-2021-3418] (DAL-5456]

9. Update bzip2 to version 1.0.8 (CVE-2019-12900, CVE-2011-4089, CVE-2010-0405) [DAL-5446]

10. Update procps to version 3.3.15 [DAL-5433] 1. CVE-2018-1124, CVE-2018-1123, CVE-2018-1126, CVE-2018-1125

11. Hardened openssl build to include secure compilation flags

12. Update sqlite to version 3.37.2

13. The OpenSSL build has been updated to include secure compilation flags. [DAL-5472]

14. IX20W-PR: On PR FirstNet products, enable the **Network** → **Wi-Fi** → **Access points** → **Digi AP** → **Isolate clients** setting by default so Wi-Fi clients connecting to the Digi device's SSIDs are isolated from each other by default

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