TOC

23.3.31.129 - May 2023, Feature

Release category: **Mandatory**

New features

1. **Redesigned Surelink configuration settings [DAL-6646]**

    1. Surelink configuration settings are now listed in a single section under each network interface, as opposed to a separate section for IPv4 vs IPv6. The layout of the connectivity tests and recovery actions to perform have been redesigned to provide a more streamlined setup. Any configured tests and recovery actions are performed in the order they are configured, along with a new capability for integrating custom scripts as a test or recovery action. See the Surelink section of the Digi device's user guide for additional details.

    2. **Important note:** When updating a device with non-default Surelink settings from 22.11.48.x or older firmware to 23.3.31.129 or newer, there are some instances where those Surelink settings will not migrate and the device will revert back to default Surelink settings. Digi strongly recommends that you test the new firmware release in a controlled environment with your application before you update production devices. Pay particular attention to your Surelink configuration settings before and after the firmware update, and review any changes before rolling out the 23.3.31.129 release to mission critical devices

        Note: Due to the SureLink configuration changes, the SureLink configuration may be not fully migrated from previous releases. Digi recommends that you review

the SureLink configuration before rolling out the 23.6.1.105 release to mission critical devices.

3. EX/IX: **Known migration issues with 22.11.48.x and older firmware:**

    1. If an IPv4 Surelink specifies one test but the IPv6 specifies all tests, then all tests will be selected and Surelink may not behave as expected. The same applies for the reverse - IPv4 specifies all tests and IPv6 specifies one test.

    2. The previous version didn't correctly go out the correct interface in every condition. It was possible to pass the ping test without the interface even being up. This is now fixed in 23.3.31.129 firmware and newer so tests are forced out the correct interfaces by marking the packet.

    3. If migrating from a very old version (firmware versions 20.2.x and older), the config cannot be migrated as it is incompatible. In this scenario, we use the default Surelink configuration for all interfaces

    4. If there are conflicting Surelink action or test settings for IPv4 and IPv6 (eg intervals etc), the device will use the IPv4 in preference when migrating the configuration as part of the firmware

2. DMVPN phase 1 spoke support with NHRP or mGRE, including compatibility with Cisco DMVPN hubs [DAL-6709]

3. Added ability to utilize the cellular modem as a time sync source under **System** → **Time** [DAL-6693]

Enhancements

1. ModemManager updated to version 1.20.6 [DAL-6406], which includes:
    1. Improved 5G SA-mode and NSA-mode performance
    2. RSRP/RSRQ/SINR statistics for 5G SA-mode connections
    3. Native multiplexing for dual-APN setups
2. US Cellular consumer SIM support has been updated so that configured APNs are not required.
3. Added **show surelink state** Admin CLI command to display the overall pass/fail status of the enabled Surelink tests [DAL-7070]
4. Added options under **Network** → **SD-WAN** → **WAN bonding** to configure the mode for each tunneled interface and the overall mode of the WAN bonding tunnel [DAL-7394]
5. Updated WAN bonding saneclient to version 20221103 for 5G and 1Gbps performance [DAL-7005]
6. Added new **show wan-bonding** Admin CLI command to display status of WAN Bonding tunnel [DAL-7395]
7. Added new **Status** → **WAN Bonding** page in the web UI to display status of the WAN Bonding tunnel [DAL-7395]
8. Added distance between the WAN bonding and Ethernet bonding setting sections in the configuration accordion

9. Added configuration settings under **System** → **Containers** to allow the container to be auto-started on boot with optional parameters and restart if the container stops {DAL-7021]

10. Added configuration settings under **System** → **Containers** to setup shared directories between the host filesystem and the container [DAL-7021]

11. Support for US cellular consumer SIMs without requiring the user to first configure the APN [DAL-7248]

12. Disable mDNS by default on EX/IX/TX products for improved cellular performance [DAL-7354] 12. Added GlobalGIG APNs to fallback APN list [DAL-6886]

13. The ITxPT support has been updated to support IPv6 for the MQTT broker, GNSS services.

14. Added new **AT&T LWM2M support** setting for enabling/disabling LWM2M on the modem (enabled by default) [DAL-7009]

15. Added IPv6 support for MQTT broker, location servers, and mDNS service [DAL-7111]

16. Include the system hostname (if configured) on the Dashboard page in the local web UI [DAL-7428]

17. Added support for SHA2 ciphers for IKEv2 IPsec tunnels [DAL-7038]

Bug fixes

1. Fixed issue preventing users from locking a device to use a blank APN [DAL-7248]
2. Pre-shared keys for configured Wi-Fi SSIDs are now obfuscated in Digi Remote Manager [DAL-7107]
3. Fixed issue where configuration options for selecting the Wi-Fi channel appeared as “None” in Digi Remote Manager [DAL-7482]
4. Fixed issue preventing device from falling back to its local system time when running as a NTP server [DAL-7233]
5. Fixed issue preventing SIM failover when the device was configured with separate network interfaces set to match by carrier instead of SIM slot [DAL-6910]
6. Removed 3-second stop/start delay when making configuration updates to the MQTT broker settings [DAL-7104]
7. Fixed issue where **tail** CLI command required a filter option in order to utilize the match option [DAL-7038]
8. Fixed issue preventing WAN bonding interface from appearing in the **show route** CLI output [DAL-6829]
9. Fixed issue where initial Surelink test would fail if the cellular modem was configured to be in passthrough mode [DAL-6224]
10. Fixed possible routing issue between GRE/IPsec with Cisco peer GRE/IPsec using VTI configuration [DAL-6722]
11. Fixed issue preventing SMTP notifications from using TLS encryption [DAL-7079]

12. Fixed issue where the latest WAN Bonding saneclient presets were not being included in the DAL firmware [DAL-7540]
13. Fixed issue where serial logging enabled on Realport serial ports never closes the logging session [DAL-6748]
14. IX: Fixed improper setup of Realport HW flow control on IX-series products [DAL-7081]
15. An issue with updating non-active firmware images on the EM9191 5G cellular modem has been resolved. [DAL-7451]

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 Linux kernel 6.1 [DAL-7179]
2. Update OpenSSL to version 3.0.8 and 1.1.1t [DAL-7261]

   CVE-2023-0401 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2023-0286 CVSS Score: 7.4 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

   CVE-2023-0217 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2023-0216 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2023-0215 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2022-4450 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2022-4304 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVE-2022-4203 CVSS Score: 4.9 Medium CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

CVE-2022-3996 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2023-0286 CVSS Score: 7.4 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

CVE-2023-0215 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2022-4450 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2022-4304 CVSS Score: 5.9 Medium CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

3. Update netifd to version 18.06 [DAL-6280] 4. Update libexpat to version 2.5.0 [DAL-7082]
4. Update libexpat to version 2.5.0 [DAL-7082]

   CVE-2022-23852 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2022-23990 CVSS Score: 7.5 High CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE-2022-22827 CVSS Score: 8.8 High CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

   CVE-2022-22826 CVSS Score: 8.8 High CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

   CVE-2022-22825 CVSS Score: 8.8 High CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

   CVE-2022-22824 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2022-22823 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE-2022-22822 CVSS Score: 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

5. Wi-Fi pre-shared keys are now obfuscated in Digi Remote Manager. [DAL-7107]

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