DIGI INTERNATIONAL
9350 Excelsior Blvd, Suite 700
Hopkins, MN 55343, USA
+1 (952) 912-3444 | +1 (877) 912-3444
www.digi.com

Firmware Release Notes
Digi Connect
Version 2.26.1 (October 2020)

INTRODUCTION

This is a production release of firmware for a limited group of the Digi Connect family of wired products.

The Digi Connect embedded and stand-alone device servers allow you to add web-enabled networking using a variety of connectivity options. The Digi Connect device servers provide powerful "plug-and-play", customizable and future-safe features, and performance in one of the smallest solutions available.

SUPPORTED PRODUCTS

- 82004424 Digi Connect ME -S 4MB
- 82001607 Digi Connect ME 9210 4/8 -SSW

KNOWN ISSUES

The Digi part number associated with the operating system in the Digi Connect ME -S 4MB has changed from 82001120 -> 82004424. The part number change is not associated with any functional differences beyond the enhancements and/or bug fixes noted below.

To eliminate potential issues with downgrade attempts this firmware will not allow negotiation of a connection with a TLS protocol version prior to 1.2. Users requiring interoperability with legacy protocol versions should not upgrade to this firmware unless they have this capability in the devices and servers they use it with.

As a result of limiting the TLS protocol, if the customer wishes to use Encrypted Realport they will need to update to a version that supports TLS 1.2. Unencrypted RealPort is not impacted. Digi is in the process of updating the currently supported Encrypted RealPort drivers so this will become possible as those releases occur. Please refer to the RealPort driver page http://www.digi.com/support/realport/ for updates and information.

Our password hashing algorithm includes a key-stretching portion to make brute-force attacks more costly. This algorithm in our new security code has more overhead and login will now take more time (3-8 seconds).

KNOWN ISSUES
The unit must be power cycled for new port sharing settings to take effect.

It is not currently possible to configure the escape characters used by client applications (connect,

telnet, and rlogin).

If the standard web service (HTTP) is disabled, the encrypted web service (HTTPS) stops operating. They will be made independently selectable in a future release.

When attempting to upgrade the firmware on a unit which has password authentication enabled, the initial release of the firmware would fail. This current release includes a workaround to this behavior by allowing the user to disable passwords during the time period of the firmware upgrade.

In order to clear the persistent configuration storage from the CLI one can execute the "boot action=factory" command. The only web accessible method for clearing the storage is available via the reset functionality in the administrative pages at "admin/factory_defaults.htm".

When attempting to replace files in the file system, simply overwrite the existing version of the file rather than deleting the file first. Attempting to delete the file first defeats the internal file versioning maintained by the firmware, and can confuse your browser's cache.

For the most consistent experience with the user interface, it is suggested that you clear your Internet cache.

Microsoft Internet Explorer 6 Service Pack 1 (SP1) has a known problem where it displays the error message "Internet Explorer Cannot Open" when you use an HTTPS URL to access this Digi product. The following Microsoft article explains the problem:

http://support.microsoft.com/default.aspx?kbid=812935

Digi devices do not support SSL renegotiation. This can cause problems with some Open SSL applications that do not correctly handle this situation. To work around this problem, use the "openssl -quiet" option.

There is no IPV6 support for IA (Industrial Automation) or Modem Emulation.

TFTP using IPv6 addresses is not supported.

Backup using IPv6 addresses is supported using the Web UI but not CLI.

Downgrading a unit from an IPv6-enabled EOS to an IPv4-only EOS will result in the loss of some IP address settings. To insure that settings are not lost in this situation, a user is advised to do a back-up of their device prior to upgrading it to an IPv6-enabled EOS. If, after upgrading, a user wishes to go back to an IPv4-only EOS, they should:

- Upload the IPv4-only EOS to the device
- Revert the device to factory defaults
- Restore the device using the saved backup configuration

The IA route option "set ia route connect={active|passive}" is not supported in this release. Contrary to what is stated in the Command Reference manual, connect cannot be set to active.

Setting the Serial Profile to Industrial Automation only works smoothly if you have NOT set IA parameters manually by Telnet or command line. Use one method only - either Web UI or Telnet.

RESETTING THE UNIT

Digi Connect device server firmware has an enhanced ability to be both soft reset as well as reset to its factory defaults.

Both functions may be invoked on the ME and the Wi-ME via manipulation of pin 20 on the module's header:

- If the module is running (i.e. more than a few seconds after power on), holding pin 20 low for a second and then raising it will soft reset the unit
- If pin 20 is held low for more than 10 seconds from the power on or release from hard reset of the unit, and then raised, it will reset the unit to its factory default state

For all devices, the action takes effect when reset is released.

ADDITIONAL INFORMATION

On initial boot of this device, it will generate encryption key material: an RSA key for SSL/TLS operations, and a DSA key for SSH operations. This process can take as long as 40 minutes to complete. Until the corresponding key is generated, the device will be unable to initiate or accept that type of encrypted connection. It will also report itself as 100% busy but, since key generation takes place at a low priority, the device will still function normally. On subsequent reboots, the device will use its existing keys and will not need to generate another unless a reset to factory defaults is done, which will cause a new key to be generated on the next reboot.

USING MODBUS BRIDGE

This image includes a Modbus protocol bridge. Modbus is one of the most common "third party" interfaces for industrial equipment. The full protocol specification can be found at www.modbus.org

The Modbus Bridge functionality enables Masters and Slave to communicate using any combination of the 3 official dialects:

- Modbus/TCP transported by TCP/IP or UDP/IP
- Modbus/RTU transported by serial, TCP/IP, or UDP/IP
- Modbus/ASCII transported by serial, TCP/IP, or UDP/IP

One-serial port bridges are defined by the role of the attached serial device. Selecting the "Industrial Automation" serial port profile enable you to define either:

1) Serial Modbus master accessing remote IP-based Modbus slaves
2) Remote Modbus masters sharing a serial Modbus slave(s).

See Digi Support Document 90000638 for more details on various ways to setup and use a Modbus Protocol Bridge:
http://ftp1.digi.com/support/documentation/90000638_a.pdf

See Digi Support Document 90000649 for more details on how the message queuing and processing works within a Modbus Bridge:
http://ftp1.digi.com/support/documentation/90000649_a.pdf

UPDATE CONSIDERATIONS

In order to add compliance with California's Senate Bill No. 327, for information privacy of connected devices, the handling of the root password for newly manufactured products is changing.

Products manufactured after January 1, 2020 will no longer use a fixed, default password. Rather, a

per-device, unique password will be assigned during manufacturing, and will be visible on a product label. It will still be possible to change the password for the user on a per-device basis.

Products manufactured prior to the adoption of the new product labeling are grandfathered in and will continue to operate as before.

UPDATE BEST PRACTICES

Digi recommends the following best practices:

1. Test the new release in a controlled environment with your application before you update production devices.
2. Unless otherwise noted, apply updates in the following order:
    a. Device firmware
    b. Modem firmware
    c. Configuration
    d. Application

Digi recommends Digi Remote Manager for automated device updates. For more information, go to https://www.digi.com/products/iot-platform/digi-remote-manager. If you prefer manually updating one device at a time, follow these steps from the manual:

1. Firmware update process

TECHNICAL SUPPORT

Get the help you need via our Technical Support team and online resources. Digi offers multiple support levels and professional services to meet your needs. All Digi customers have access to product documentation, firmware, drivers, and knowledge base and peer-to-peer support forums. Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

VERSION 2.26.1 October, 2020

This is a recommended release

SECURITY FIXES

Removed ICMP command 165 processing from network stack. This was the cause of a false positive in security scan software reporting our system as possibly vulnerable to Ripple20 after this had already been addressed.

VERSION 2.24.0 April 2020

This is a recommended release

SECURITY FIXES

Researchers from JSOF (https://jsof-tech.com/), have found vulnerabilities within in the Treck TCP/IP, IPv4, IPv6, DHCP, DHCPv6 and DNS products.

For Digi products we have rated the vulnerabilities as a high level risk. We recommend that customers immediately review and deploy the latest firmware associated with this release note to protect their devices. At time of release of this firmware, there is no known in the wild exploit of these

vulnerabilities.

Digi's internal scoring of the vulnerabilities is a CVSSv3.0 Score of 7.4.
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Digi will be coordinating a public disclosure of the vulnerabilities with JSOF that is tentatively set for May 14th, 2020. We are also working with the Cert Coordination Center and have been assigned VU#257161 pertaining to these issues.

Many thanks to the researchers Moshe Kol and Shlomi Oberman of JSOF for reporting these vulnerabilities.

VERSION 2.22.1 November 25, 2019

This is a mandatory release.

NEW FEATURES

In order to add compliance with California's Senate Bill No. 327, for information privacy of connected devices, the handling of the root password for newly manufactured products is changing.

Products manufactured after January 1, 2020 will no longer use a fixed, default root password. Rather, a per-device, unique password will be assigned during manufacturing, and will be visible on a product label. It will still be possible to change the password for the root user on a per-device basis.

Products manufactured prior to the adoption of the new product labeling are grandfathered in and will continue to operate as before.

NOTE: the Digi Device Discovery tool will, for these newly manufactured products, require the unique password in order to make a configuration change or reset the product via the discovery tool.

Changing the administrative password does not change the password associated with the discovery protocol (ADDP). The ADDP password can be changed via the CLI with the command:

newpass name=addp

ENHANCEMENTS

None

SECURITY FIXES

Researchers have discovered new denial-of-service (DoS) vulnerabilities in Linux and FreeBSD kernels, including a severe vulnerability called SACK Panic that could allow malicious actors to remotely crash servers and disrupt communications, according to an advisory.

"The vulnerabilities specifically relate to the Maximum Segment Size (MSS) and TCP Selective Acknowledgement (SACK) capabilities. The most serious, dubbed "SACK Panic," allows a remotely-triggered kernel panic on recent Linux kernels," the advisory stated. This vulnerability also goes back a long time (since Linux v2.6.29 that was released 10 years ago).

"The issues have been assigned multiple CVEs: CVE-2019-11477 is considered an important severity, whereas CVE-2019-11478 and CVE-2019-11479 are considered a Moderate severity".

BUG FIXES

None

VERSION 2.17.6.5

ENHANCEMENTS

None

BUG FIXES

NDS-907, KRACK vulnerability addressed in Wi-ME product.

VERSION 2.17.6.4

ENHANCEMENTS

None

BUG FIXES

NDS-907, KRACK vulnerability addressed in Wi-ME product.

Version 2.17.6.4

BUG FIXES

NDS-220, altpin changes were not preserved across port closes via the RealPort protocol.

NDS-203, adjust branding, forcing Device Cloud to reference valid "devicecloud.com" URLs.

NDS-200, prevent Device Cloud from displaying or caching "cleartext" password files.

NDS-223, remove references to installation CD

NDS-391, fix Device Cloud SSL connections when in IP passthrough mode

NDS-222/NDS-214, improve security of SSH server by removing weak connection protocols

NDS-575, Fix critical vulnerability - CVE-2014-9222

NDS-574, Fix related critical vulnerability - CVE-2014-9223

VERSION 2.17.6

BUG FIXES

NDS-164, fixed an issue where connecting to a Digi device via HTTPS with a newer browser results in a failure to connect because the Digi device is presenting an obsolete SSL protocol version