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 WS Terminal Server
Version 3.2.17.34 (August 27, 2019)

INTRODUCTION

This is a production release of firmware for the Digi Connect WS.

Digi Connect WS is intended to be used with a data acquisition system to connect to RS-232 serial devices and send data from these serial devices to the data acquisition system without adjusting or manipulating the format. The extended safety terminal server complies with IEC 60601-1 3rd edition and can be used in environments requiring this level of testing, including being placed within the patient environment when used as part of a medical electrical (ME) system.

SUPPORTED PRODUCTS

- DC-WS-1-INT Digi Connect WS Terminal Server1 Port
- DC-WS-4-INT Digi Connect WS Terminal Server 4 port
- DC-WS-8-INT Digi Connect WS Terminal Server 8 port

KNOWN ISSUES

There is a configuration section in the web interface which indicates that validation via a peer certificate is possible, but this is not yet supported. At this time, only validation by testing for a valid certificate authority is supported.

Note: Once the firmware have been updated to Revision E it will not be possible to downgrade it to an older Revision. The product does not support downgrading to a previous version.

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 3.2.17.34

Build Date:	8/27/2019
Checksum:	8347b5c1c59cd4deaa3f9895dca4759e 82003588_3.2.17.34_F.bin

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 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 user on a per-device basis.

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 3.2.17.33

Build Date:	3/6/2019
Checksum:	13d3975b51465221dfe7036a234bfec3 82003588_3.2.17.33_E.bin82001972_E

ENHANCEMENTS

DCWS-326 Serial Communication Service enhanced to allow encrypted as well as authenticated socket connections.

DCWS-212 Certificate management enhancement to allow the replacement of the device identity certificate and key, as well as in support of validation of peer certificates for secure socket connections to serial ports.

DCWS-292 Security enhancement to restrict encrypted sockets to TLS 1.2.

DCWS-295 Enhanced Wi-Fi diagnostic support.

BUG FIXES

DCWS-342 Update Digi logo in web interface.

VERSION 3.2.17.25

Build Date:	5/3/2018
Checksum:	8917b7085adca9ee89fb9e9621022b7c 82003588_D.bin

HIGHLIGHTED PRODUCT CHANGES

Add support for new hardware.

Additional flash chips were added to qualified vendor list.