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 ES SB 4/8
Version 2.26.1 (October, 2020)

INTRODUCTION

This is a production release of firmware for the Digi Connect ES SB 4 and Digi Connect ES SB 8.

Connect ES SB is an improved version of the Connect ES product that adds performance and reliably improvements plus an Ethernet Uplink option that provides routing and NAT capabilities for Ethernet devices. Connect ES SB has a real time clock and a new logging facility, plus new network features such as DNS proxy, DHCP server, and packet forwarding. The optional uplink provides a separate Ethernet interface for connecting this device to the network infrastructure, while providing 4 Ethernet ports for local Ethernet devices. NAT and packet forwarding allow the local devices to have a presence on the network while simplifying administration of the local devices.

SUPPORTED PRODUCTS

- Digi Connect ES 4 SB
- Digi Connect ES 8 SB
- Digi Connect ES 4 SB SW
- Digi Connect ES 8 SB SW

KNOWN ISSUES

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.

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

IP ADDRESS ASSIGNMENT NOTES

The Digi Connect ES supports three IPv4 assignment methods:

* Static IP address
* DHCP
* Auto-IP

If a static address is enabled, it will be used.

If a static address is not enabled, and DHCP is enabled, the unit will use an address supplied by a DHCP server regardless of the state of Auto-IP configuration.

If a static address is not enabled, and Auto-IP is enabled, it will be used to generate an address ONLY if DHCP is disabled, or if DHCP is enabled and a DHCP server has not responded to the DHCP query. If both are enabled, Auto-IP has assigned an address, and then a DHCP server responds, the Auto-IP address will be discarded and the DHCP address will be used.

RESETTING THE UNIT

One feature of the Digi Connect ES firmware is an ability for a user to both soft reset the unit as well as reset the unit to its factory defaults.

Both functions may be invoked via the "reset" hole between the power switch and the ethernet ports

* If the unit is running, holding the button for a second and then releasing it will soft reset the unit.

* If the button is pressed for more than 10 seconds from the power on of the unit, it will prepare to reset the unit to its factory default state. Once the unit is prepared to reset, it will blink "1-5-1" on the red LED. Releasing the button will then reset the configuration.

ENABLING THE WEB USER INTERFACE

The embedded web user interface is ALWAYS available at the following URL:

http://ip-address-of-device/home.htm

It is also available as the default configuration interface at the following URL:

http://ip-address-of-device

ADDITIONAL INFORMATION

The configuration save and restore tools will save every configurable parameter (including IP configuration) except for some related to password authentication.

On initial boot of this device, it will generate some 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.

PYTHON

The Connect ES SB makes available the Python programming language (http://www.python.org). To use Python on this product, you may need to download our Python standard library files from:

http://ftp1.digi.com/support/sampleapplications/40002643_B.zip

This file should be renamed 'python.zip' and placed on the product using the 'Applications -> Python' page in the products WebUI.

Our implementation of Python, its limitations and capabilities are documented on the Digi Developer wiki at http://www.digi.com/wiki/developer/index.php/Python_Wiki.

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 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.

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.

ENHANCEMENTS

Added SSH support for secure device access.

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 2.22.1.1 March 26, 2020

ENHANCEMENTS

X.509 Certificate Management has been added to provide mechanisms for replacing the identity key and certificate pair for the device, as well as to enable server authentication for specific features like “autoconnect” and “pmodem”. The feature is ported from the ConnectPort TS product line, and applicable documentation is available in the “Digi Connect Family and ConnectPort TS Family: User Guide”.

http://www.digi.com/resources/documentation/digidocs/pdfs/90000565.pdf

VERSION 2.22.1 November 25, 2019

This is a mandatory release.

ENHANCEMENTS

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

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".

VERSION 2.21.1

82001972_E (2.21.1)

ENHANCEMENTS

This release contains a new TLS implementation

- We now support many more modern and secure cipher suite options as well. This release provides added support for elliptic curve encryption, more hash algorithms, and block modes.
- Support for DSA keys and DSA signed certificates has been removed
- Some places where MD5 was being used as a hash have been modified to no longer use MD5 as it has been compromised. For legacy compatibility most places will still allow MD5 but users are encouraged to change this to something more secure.

VERSION 2.15.0.13

82001972_D1 (2.15.0.13)

BUG FIXES

- NDS-575, Fix critical vulnerability - CVE-2014-9222
- NDS-574, Fix related critical vulnerability - CVE-2014-9223