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

Digi ConnectPort X4/X4H Release Notes

Digi ConnectPort X4/X4H (82001536)

Version 2.27.3 (July 2022)

INTRODUCTION

These are the release notes for the Digi ConnectPort X4/X4H.

The Digi ConnectPort X4 (and X4 4G) is a hardened, upgradeable wireless gateway for Drop-in Networking. The ConnectPort X4 aggregates and transports ZigBee/802.15.4 network traffic to central data applications over cellular, Wi-Fi, or Ethernet connections. The ConnectPort X4 4G supports IEEE 802.16e, known as WiMAX (Worldwide Interoperability for Microwave Access), rather than cellular as the mobile wireless technology.

ConnectPort X4 gateways are a key element of Digi's Drop-in Networking family of products - a collection of hardware components that also includes Digi's XBee® adapters, modules, extenders, and bridges - which together enable distributed electronic devices to be wirelessly networked where no wired infrastructure exists, or where access to an existing network is prohibited.

The ConnectPort X4 (and X4 4G) includes support for Industrial Automation protocols and capabilities. See http://www.digi.com/support/ for complete documentation related to these protocols and special capabilities.

The standard ConnectPort X4 IA (and X4 4G IA) hardware includes screw terminals for 9-30Vdc power supply and EIA-232/422/485 field selectable serial port.

SUPPORTED PRODUCTS

- Digi ConnectPort X4
- Digi ConnectPort X4 NEMA
- Digi ConnectPort X4 IA

KNOWN ISSUES

1. You may encounter "out of memory" problems when upgrading to the latest version of the 82001536 firmware, if you are trying to upgrade an older ConnectPort X4 device that has only 16MB of RAM (rather than 32MB as is in the newer devices). In this case, please upgrade using Digi firmware part

82003073, which is slightly smaller and uses less memory than is the case for 82001536. Refer to the “HIGHLIGHTED PRODUCT CHANGES” section for additional information.

2. Problems have been encountered with some Linksys VPN appliance models when using different Diffie-Hellman group settings for phase 1 and phase 2. To work around this issue and successfully establish the VPN tunnel, use the same Diffie-Hellman group for both phase 1 and phase 2 settings.

3. Digi RealPort can only be used if the Modbus Bridge function is disabled. You cannot use RealPort with Modbus/RTU or ASCII to access the Modbus Bridge function.

4. Do not attempt to “Port Forward” TCP 502 or UDP 502 to local Modbus/TCP servers while the Modbus Bridge is active - this causes NEITHER function to work. Disable the Modbus Bridge if you desire traditional Router/NAT function for Modbus/TCP port 502.

5. IA routes targeting Zigbee/PWAN remotes assume each route can run independently. Thus three routes targeting the same extended MAC might potentially try to send three requests at once, which will confuse a serial protocol like Modbus/RTU. Use the new “scattered-route” design to convert such multiple routes to a single route, which promises only one outstanding request is sent at once.

UPDATE CONSIDERATIONS

1. As of 2.22.1 product defaults have changed to conform with California SB-327. See the product documentation and version history below for details.

2. Support for WiFi modules has been completely removed from the product. This version of firmware will be rejected by those variants should an upgrade be attempted.

3. 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.

4. It is recommended that you perform a backup of your device’s settings prior to upgrading your firmware. If you should need to revert back to a previous version of firmware, this will ensure that you will be able to restore your device to its previous settings in the event that some settings are not restored properly after downgrading the firmware.

   To backup your device settings, follow this simple procedure:

   1. Open the web user interface and navigate to the “Administration” section and select “Backup/Restore”.
   2. Click the “Backup” button and select the location to where you want to save your backup file.

   To restore:

    1. Navigate to the same section within the web UI.
    2. Click the “Browse” button to select the backup file you saved in the previous steps.
    3. Click the “Restore” button to upload the configuration settings contained in your backup file.

5. 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.

6. X4 gateways containing an LE910 module that need to operate on the AT&T network must be updated to at least gateway version 2.27.1 and Telit modem version 20.00.525. Failure to do so will likely encounter an issue to attach to the cellular network.

   Update the gateway firmware first and then please see the document at (https://www.digi.com/resources/documentation/digidocs/PDFs/90002337.pdf) for details on performing the necessary update procedure.

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:
    1. Device firmware
    2. Modem/Module firmware
    3. Configuration
    4. 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.

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, knowledge base and peer-to-peer support forums.

Visit us at https://www.digi.com/support to find out more.

CHANGE LOG

2.27.3 – 82001536_AA (July 2022)

This is a recommended release

MD5: 604a94e1d41851ea5e7849b204866e9d
SHA256: 788f1c6f7466dbc83058dd268b79b2f7a324b6e3efd90d70c6fa093bc1210051

ENHANCEMENTS

This release adds recognition and the ability to perform firmware updates to the XBee S2C NG Zigbee module when found on the Zigbee network.

2.27.2 – 82001536_Z (May 2022)

This is a recommended release

ENHANCEMENTS

This release adds recognition and the ability to perform firmware updates to the XBee RR Zigbee module when found on the Zigbee network.

BUG FIXES

1. This release fixes a problem with CPX4 variants containing the Telit LE910 cellular module when operating on AT&T caused by the 3G shutdown. Modules may not attach to the network with certain SIM cards. After update to this 2.27.1 firmware or later the Telit firmware must also be updated using a script available on the Digi support site.

   Please see the document at (https://www.digi.com/resources/documentation/digidocs/PDFs/90002337.pdf) for details on performing the necessary update procedure.

2.26.2 – 82001536_Y (September 2021)

This is a recommended release

ENHANCEMENTS

1. Modified Telit LE910 initialization to prepare module for 3G sunset behavior by selecting +CEMODE=2 for PS/CS mode 2 operation.

SECURITY FIXES

Additional security fixes have been made to the Treck stack to add fixes for:

- CVE-2020-27336
- CVE-2020-27337
- CVE-2020-27338

2.26.1 – 82001536_X (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.

2.26.0 – 82001536_W (July 2020)

ENHANCEMENTS

Added support for updating the Telit HE910-D modem firmware. A python script is available on the support site to perform the update of the Telit HE910-D modem. This script is run on the device and performs a two stage update process that updates the Telit HE910-D firmware from version 12.00.028 to 12.01.020. This fixes issue CPX4-119 where the Telit HE910-D modem permanently stops connecting to the network.

2.24.0 – 82001536_V (April 2020)

This is a recommended release.

SECURITY FIXES

Researchers from JSOF (https://jsof-tech.com/), have found vulnerabilities within 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.

2.22.1 – 82001536_U (December 2019)

This is a recommended release.

SECURITY FIXES

1. Changes for California SB-327

   In order to comply with regulations in the state of California (SB-327), this firmware now supports being manufactured with a unique per-device password. Existing products manufactured prior to this change will continue to default to the prior fixed value 'dbps' but will be impacted by changes to defaults that have been made.

   When applicable, this password is the initial factory default value for the 'root' and 'custom' users and the Digi Device Discovery (ADDP) tools and can be found printed on a label attached to the product. As always, Digi recommends that users take the opportunity to change the passsword to a value known only to themselves when performing the initial configuration of the product.

   - The default factory settings for login suppression have changed. All products will require login out of the box.

     The prior behavior can be recovered in the CLI with the command 'set login suppress=on' or in the WebUI on the Configuration->Users page by unchecking and applying the "Enable user logins" checkbox.

   - SNMP has been disabled in the factory defaults. Prior behavior can be recovered with the 'set service' command in the CLI or in the Configuration->Network->"Network Services Settings" page in the WebUI.

2. Numerous upgrades and improvements to internal TLS stack.

   This product uses WolfSSL which was upgraded from version 3.15.3 to version 4.1.0. Full details can be found at https://www.wolfssl.com/docs/wolfssl-changelog/.

---

*Release Notes Part Number: 93000698