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

Digi XBee Gateway Cellular Release Notes

Digi XBee Gateway Cellular

Version 3.2.32.11 (November 2022)

INTRODUCTION

These are the release notes for Digi XBee Gateway Cellular.

The XBee Gateway is a small ZigBee to IP gateway that provides low-cost IP networking of RF devices and sensor networks. Featuring an easy development environment, XBee Gateway enables custom applications to run locally while interfacing across existing Ethernet/Wi-Fi networks for WAN connectivity to cloud-based software applications.

The XBee Gateway products feature an end-to-end development environment based on Digi's DIA framework, allowing for rapid M2M-specific application development on the industry standard Python scripting engine. Digi ESP provides an IDE featuring device detection, debugging, compiling and downloading of Digi DIA/Python code to Digi gateways.

Digi Remote Manager, a Digi-hosted remote management service, offers a platform for secure, scalable access to an unlimited number of remote assets. In addition, the Remote Manager web services provide seamless integration from Digi gateways into customer back office applications.

SUPPORTED PRODUCTS

- XBee Gateway 3G International

KNOWN ISSUES

- OTA update of sleepy XBee 3 nodes with long sleep periods (greater than several seconds) may not succeed. Workaround: configure the node with a shorter sleep period or disable sleep while updating.

UPDATE CONSIDERATIONS

- As of firmware version 3.2.30.4, the factory default settings for ADDP and HTTP/HTTPS web UI access have changed. Updating to 3.2.30.4 does not change the existing configuration of the gateway.

    - ADDP is now Read-Only by default.
    - Accessing the web interface by HTTP is disabled by default; access to the web interface by HTTP (port 80) redirects to HTTPS (port 443).
    - Accessing the configuration of the product via the web interface now requires user authentication. Use the `python` username and password to authenticate.

- XBee Gateway devices shipped with firmware version 3.2.30 or higher are manufactured with a unique per-device password. Devices shipped with older firmware have no unique per-device password.

- Be aware that firmware downgrade is not supported on XBee Gateway devices.

- In order to update to firmware version 3.2.31.x or newer, the XBee Gateway must already have 3.2.7.x or newer installed. This is because as of 3.2.31, the XBee Gateway firmware is cryptographically signed with a newer certificate which was introduced in the 3.2.7 firmware release (released June 2014).

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 firmware
    3. XBee firmware
    4. Configuration
    5. 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 the instructions in the XBee Gateway user guide: Update firmware from the XBee Gateway web interface

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

VERSION 3.2.32.11 (November 2022)

This is a recommended release

ENHANCEMENTS

- Added a `<mobile><enabled>` element to RCI configuration for all cellular XBee Gateway variants. When set to “off” the connection status will be disabled and the system will not repeatedly try to enable

it.

- Updated Python from baseline of 2.7.1 to 2.7.18. Refer to the What's New in Python 2.7 documentation for information on language and standard library changes. [DBL-1078]
    - Changes to the `ssl` module may require modifications to your existing Python application code. Refer to the "Python SSL changes" section below, and the Python ssl documentation, for more information.
    - As with every new release it is strongly recommended that thorough validation testing be performed in a test environment with the new version prior to deployment into a production environment.
- Doing an XBee discovery with the clear option will wipe out the cached version information for the nodes. This allows the version information to update when changed due to an out of band update, i.e over a local serial update. [XBGW-3266]

SECURITY FIXES

- Updated to OpenSSL 1.1.1q
- Update chrony to receive security issue fixes
    - CVE-2012-4502
    - CVE-2012-4503
    - CVE-2014-0021
    - CVE-2015-1853
    - CVE-2015-1821
    - CVE-2015-1822
    - CVE-2016-1567
    - CVE-2020-14367
- Update Dropbear SSH to receive security issue fixes
    - CVE-2020-36254
    - CVE-2019-12953
    - CVE-2018-15599
- Update Busybox to version 1.34.1 to receive security issue fixes
- Update wpa_supplicant to version 2.10 to receive security issue fixes

BUG FIXES

- The stored source route record for a given remote node is now cleared after a TX error. [XBGW-3345]

Python SSL changes

This release updates the Python installation inside of XBee Gateway from a baseline of Python 2.7.1 to Python 2.7.18, the final 2.7 release. The most important change resulting from this update to be aware of is that server certificate verification is now enabled by default in HTTP client code in the Python standard library.

In earlier firmware releases, Python did not perform this verification by default. As a result, updating to firmware 3.2.32.x or newer will require you to review and test your existing Python application, and if your code uses `httplib` (directly or indirectly) and creates HTTPS connections, you will need to modify it to work correctly.

There are two options:

1. Upload the correct CA certificate into the gateway, and update the code to pass an SSL context configured for that CA certificate into the HTTPS connection. (Due to space limitations, XBee Gateway does not ship with a set of CA certificates, so managing this certificate is left to the user.)

2. *Not recommended for security reasons*: Add the line `ssl._https_verify_certificates(False)` early in your Python code, to disable this HTTPS server verification by default. This will revert Python to using the more permissive behavior.

VERSION 3.2.31.20 (July 2022)

This is a recommended release.

ENHANCEMENTS

- XBee Over-the-Air (OTA) can now update S2C NG Zigbee firmware.
- Improved timeout behavior of XBee 3 Over-the-Air (OTA) updates.
- Updated ppp and busybox packages to receive security issue fixes
    - ppp
        - CVE-2018-11574
        - CVE-2020-8597
        - CVE-2014-3158
    - busybox
        - CVE-2018-1000517
        - CVE-2018-1000500
        - CVE-2016-6301
        - CVE-2016-2148
        - CVE-2018-20679
        - CVE-2019-5747
        - CVE-2013-1813 NOTE: The busybox change includes fixes that modify shell script and command behavior. As with every new release it is strongly recommended that thorough validation testing be performed in a test environment with the new version prior to deployment into a production environment.
- Modify cellular configuration in preparation for the global 3G sunset.

BUG FIXES

- Fix repeated “size error” message in xbee.log. [XBGW-3092]
- XBee OTA updates could get stuck in the “Scheduled” state. [XBGW-3093]
- XBee OTA updates could cause the xbee daemon to restart, losing memory of network state and update progress. [XBGW-3170]
- Reliability improvements to XBee S2/S2C Over-the-Air (OTA) updates. [XBGW-3225]
- On a failed XBee OTA update, attempt to update with other XBee nodes on the network first, before trying Recovery Mode. [XBGW-3236]
- Adjust implicit timeout for Remote AT Commands to improve reliability on large XBee networks. [XBGW-3184]

FIRMWARE UPDATE CONSIDERATIONS

This firmware release has switched to an updated signing certificate, which was first included in the 3.2.7.x firmware release. It is not possible to update directly from a firmware older than 3.2.7.x to this release or a newer release. To update from pre-3.2.7 firmware, first install 3.2.30.9.

VERSION 3.2.30.9 (September 2020)

This is a recommended release

ENHANCEMENTS

- XBee Over-the-Air (OTA) can now update XBee 3 device firmware and file system images.

VERSION 3.2.30.6 (May 2020)

This is a recommended release.

SECURITY FIXES

- High level security updates (CVSSv3 scoring 7.3 - CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N) to address common weakness enumerations (CWE-250) - Execution with unnecessary privilege within the product. These were discovered and reported to Digi by Jake Valletta and Sam Sabetan from FireEye Mandiant. [XBGW-3005]
- Updated to OpenSSL 1.0.2u

VERSION 3.2.30.4 (December 2019)

This is a recommended release.

NEW FEATURES

- Changes for California SB-327. See ENHANCEMENTS below.
- Created new Authentication web page.
    - New web page added allowing the python user password to be changed. [XBGW-2965]
    - Web UI authentication enable/disable option added to web UI. [XBGW-2966]
- RCI `do_command set_password` can be used to set the python user password. See product documentation for more information. [XBGW-2967]

ENHANCEMENTS

- 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 password ‘dbps’ for the python user, but will be impacted by changes to defaults that have been made.

  When applicable, this password is the initial factory default value for the ‘python’ user and can be found printed on a label attached to the product. As always, Digi recommends that users take the opportunity to change the password to a value known only to themselves when performing the initial configuration of the product.

    - The default factory setting for ADDP is now Read-Only. This means the XBee Gateway can be discovered using the Digi Device Discovery tool, but configuration may only be performed via the web interface, SSH, or through Digi Remote Manager. Note that ADDP on XBee Gateway does not support a password - keep this in mind if you choose to configure ADDP to be Read-Write, or if upgrading an existing product where ADDP is Read-Write by default.
    - Accessing the configuration of the product via the web interface now requires user authentication. You may use the `python` username and password to authenticate.
    - Accessing the web interface by HTTP is now disabled in factory defaults; access to the web interface by HTTP (port 80) redirects to HTTPS (port 443).

SECURITY FIXES

- Fixes to address Selective ACK security issues
    - CVE-2019-11477 SACK Panic
    - CVE-2019-11478 SACK Slowness
    - CVE-2019-11479 Excess Resource Consumption Due to Low MSS Values

BUG FIXES

None.

VERSION 3.2.29.7 (February 11, 2019)

This is a recommended release.

NEW FEATURES

None.

ENHANCEMENTS

None.

SECURITY FIXES

None.

BUG FIXES

- When resetting the XBee Gateway to factory defaults, the factory default password will now be used (user/pass: `python`/`dbps`). [XBGW-2781]
- Fixed issue where DNS lookups were being cached even if the zone/file CNAME mapping had been updated. [XBGW-2904]

Release Notes Part Number: 93000760