GNX Configuration Server

Configuration Guide

SIERRA WIRELESS®

41114355 Rev. 2

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless product are used in a normal manner with a well-constructed network, the Sierra Wireless product should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless product, or for failure of the Sierra Wireless product to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless product in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless product **MUST BE POWERED OFF**. The Sierra Wireless product can transmit signals that could interfere with this equipment.

The driver or operator of any vehicle should not operate the Sierra Wireless product while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

In accordance with ANSI/ISA 12.12.1-2011, Section 16 and CSA C22.2 No 213, Section 5.5, the following instructions and warnings apply:

This apparatus is suitable for use in Class I, Division 2, Groups A, B, C and D.

Warning: *EXPLOSION HAZARD–SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2.*

Avertissement: *RISQUE D'EXPLOSION–LA SUBSTITUTION DE COMPOSANTS PEUT RENDRE CE MATERIEL INACCEPTABLE POUR LES EMPLACEMENTS DE CLASSE I, DIVISION 2.*

Warning: *EXPLOSION HAZARD–DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS THE AREA IS KNOWN TO BE NON-HAZARDOUS.*

Avertissement: *RISQUE D'EXPLOSION–NE PAS DEBRANCHER TANT QUE LE CIRCUIT EST SOUS TENSION, A MOINS QU'IL NE S'AGISSE D'UN EMPLACEMENT NON DANGEREUX.*

Warning: *DO NOT USE THE USB CONNECTOR IN A HAZARDOUS AREA.*

Avertissement: *NE PAS UTILISER DE CONNECTEUR USB DANS LES ENVIRONNEMENTS DANGEREUX.*

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product may contain technology developed by or for Sierra Wireless Inc. This product includes technology licensed from QUALCOMM®. This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from MMP Portfolio Licensing.

Copyright

Trademarks

Sierra Wireless®, AirLink®, AirVantage® and the Sierra Wireless logo are registered trademarks of Sierra Wireless.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

Other trademarks are the property of their respective owners.

Contact Information

Sales information and technical support, including warranty and returns	Web: sierrawireless.com/company/contact-us/ Global toll-free number: 1-877-687-7795 6:00 am to 5:00 pm PST
Corporate and product information	Web: sierrawireless.com

Revision History

Revision number	Release date	Changes
1	April 13, 2022	First release
2	August 11, 2022	Chapter 3, replaced WinAgents TFTP Server with Open TFTP

Contents

1: Introduction

This chapter describes hardware recommendations and the software required to install and operate the GNX Configuration Server. It also includes installation instructions for the recommended FTP/TFTP servers.

Overview

This document describes how a GNX customer can set up and configure private GNX Servers so that after Sierra Wireless retires the GNX Servers, a customer can continue to operate and manage a fleet of GNX devices.

Sierra Wireless will retire the GNX Servers at the end of 2022 per the bulletin “GNX Server End of Life Announcement” available on The Source.

If you are planning to install and configure your own private GNX Servers, you must contact Sierra Wireless support by July 1 2022 to request support. You cannot transfer your GNX devices to your GNX server without the assistance of Sierra Wireless.

Hardware Recommendations

The GNX Configuration Server can potentially hold thousands of configuration files. To achieve satisfactory performance, it is recommended that the GNX Configuration Server meets or exceeds the following hardware specifications:

- Intel Xeon or higher compatible processor
- 8 GB RAM
- 200GB hard drive
- Network connection
- UPS Backup

Software Requirements

Deployed GNX devices expect the GNX Configuration Server to simultaneously provide configuration and firmware upgrade files via FTP/TFTP connections. The following software components have been verified to provide these services to GNX deployed devices.

- Windows 10 Server or later
- FTP Server: FileZilla Server
- TFTP Server: Open TFTP Server SP
- VIN Server: Provided and licensed by Sierra Wireless

Directory Structure

The GNX Configuration Server has several folders where the applications can access and save data for the core services provided.

C:\TFTPRoot

This directory and subdirectories contain the unit serial_number.cfg configuration files and the fleet.cfg configuration files for all GNX devices.

GNX firmware update files (*.gxe) should be placed directly in the TFTPRoot directory.

Ublox radio firmware update files (*.upd) version 30.44 and under should be placed directly in the TFTPRoot directory.

The system administrator (admin) logs into this folder to add, remove or edit configuration files and deposit GNX Firmware update files.

C:\TFTPRoot\radiofw

Ublox radio firmware update files (*.upd) version 30.55 and over should be placed in the C:\TFTPRoot\radiofw directory.

C:\debug

This folder will contain the JLog results generated by GNX using a MEMREADRAW command specifying the JLog memory region to read and the IP address where to send the JLog data; in this case the IP of the GNX Configuration Server (XX.XX.XX.XX):

```
AT!GXDIAG MEMREADRAW 30080000 4000 VIATFTP XX.XX.XX.XX FILENAME
filename.gxd;
```

The produced filename.gxd contains hex data. The application JLogDecoder.exe or JLogDecoderv1_7.exe are necessary to decode the JLog files.

The JLogDecoder.exe or JLogDecoderv1_7.exe applications must reside in the debug folder.

C:\VINserver

The VINserver folder should contain all the VIN based database files and VIN Server application:

- OBDOdoVINLookup.txt
- OBDSeatbeltVINLookup.txt
- SerialRanges.txt
- OBDOdoServer.exe

Any VIN server activity generated by the application will be saved in this folder by creating a daily log with the GNX serial numbers and the VIN numbers of the devices who has queried the VIN server.

C:\TFTPRoot\OBDODO

The OBDODO directory will contain the proprietary configuration files the GNX Configuration Server will provide to a requesting GNX device needing to read proprietary odometers. These configuration files are provided by Sierra Wireless. See also VIN Server on page 21.

C:\activity

The activity logger captures daily log files MMDDYY.txt that contain an ASCII text list of factory resets and FOTA events generated by GNX devices. The ActivityLogger.exe application should start with the server and the activity folder should contain the following files:

- ActivityLogger.exe
- config.txt

Scheduled Tasks

The following are scheduled tasks that exist only to restart key functions on server reboot:

- OBDOdoServer.exe: Starts with the server. C:\VINserver\OBDOdoServer.exe listen for OBD vehicle odometer configuration requests.
- ActivityLogger.exe: Starts with the server. C:\activity\ActivityLogger.exe listens for FOTA messages from GNX.

TFTP Firewall & security considerations

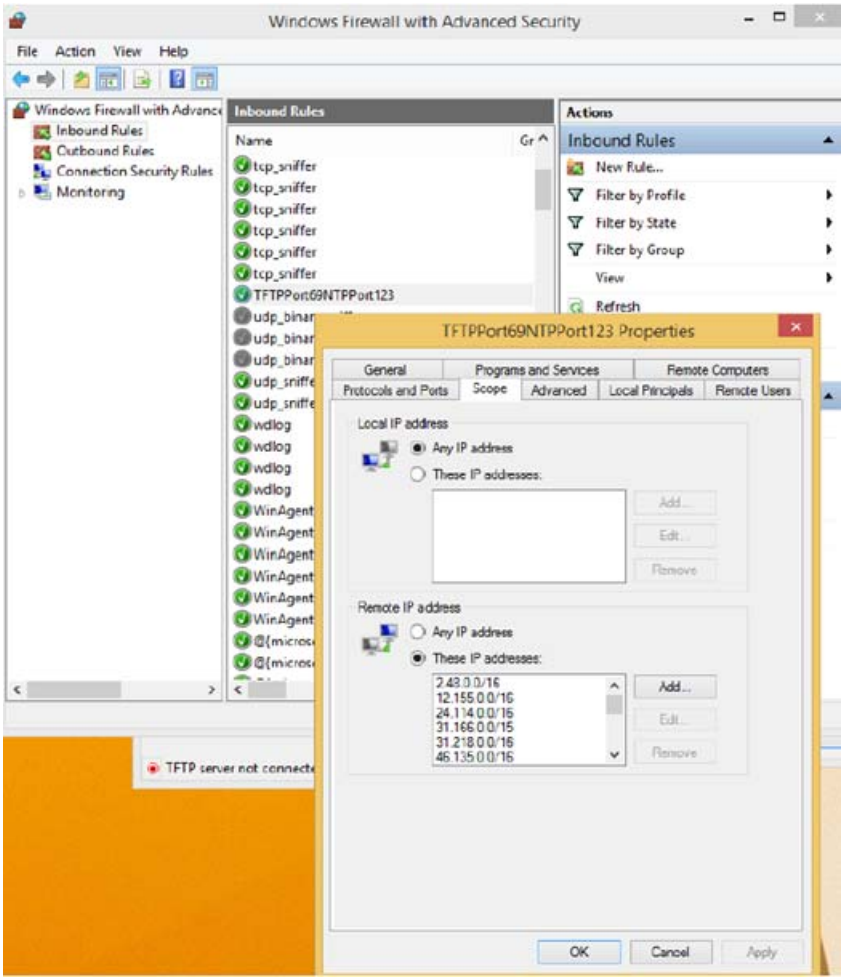
In recent years, open TFTP servers have been used for DDoS amplification attacks where the attacker reads a short filename (\x, \x.pdf) using a spoofed source IP so that the server will send a File Not Found message to the spoofed source IP, which is the attack target. In theory an even more effective attack would be for an attacker to know the name of a file of length >= 512 bytes and send a read request for that file.

To reduce the chances of our TFTP server being used for such a DDoS amplification, port 69 is only opened to subnets from which GNX devices are legitimately reading configuration files. These subnets fall into two categories:

1. NAT firewalls of wireless carriers
2. NAT firewalls of our customers, where they receive data via VPN from the wireless carrier

Since neither of these categories of subnets is likely to be the target of a DDoS attack, opening the Windows firewall port 69 to only these subnets greatly reduces the chance that the GNX TFTP server will be successfully used for DDoS amplification.

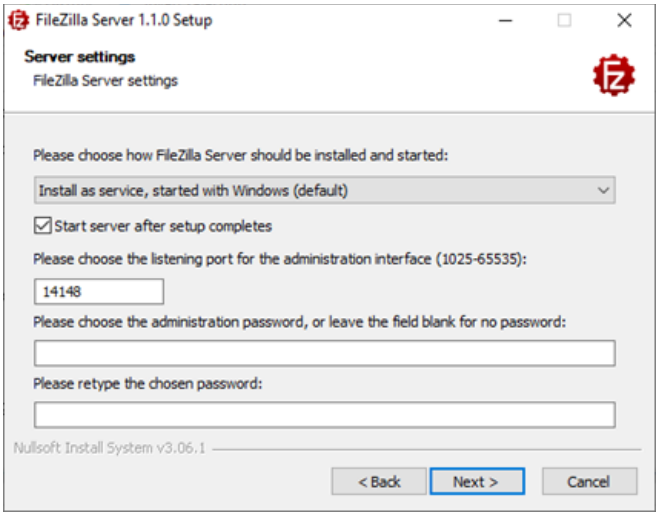
In Windows firewall InboundRules, the rule TFTPPort69NTPPort123 is used to selectively open subnets to TFTP traffic, using the scope tab. Whitelisted subnets are also copied to the file C:\TFTPRoot\whitelist.txt for future reference (and to allow sharing with IT, who use the same whitelist to filter access to SMTP relay and NTP). See the screenshot below:


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
tcp_sniffer
TFTPPort69NTPPort123
wdlog
WinAgent
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
TFTPPort69NTPPort123 Properties
General
Programs and Services
Remote Computers
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
Local IP address
Any IP address
These IP addresses:
Add...
Edit...
Remove
Remote IP address
Any IP address
These IP addresses:
2.48.0.0/16
12.155.0.0/16
24.114.0.0/16
31.186.0.0/15
31.218.0.0/16
46.135.0.0/16
Add...
Edit...
Remove
OK
Cancel
Apply
TFTP server not connecte

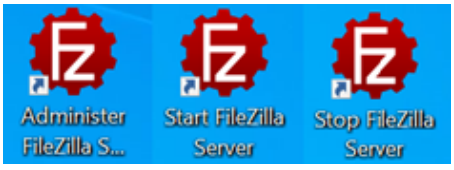
2: Installation

FileZilla FTP Server

Download and install the FileZilla Server file **FileZilla_Server_1.1.0_win64-setup.exe** or higher. Make sure to also install the FileZilla Administration interface and keep the default configuration provided by the installer, including the port for the Administration Interface.



After the installation is complete, there should be 3 FileZilla icons on the desktop, Click **Start FileZilla Server** to start the FTP server and click **Administer FileZilla Server** for FTP server setup.



Open TFTP Server

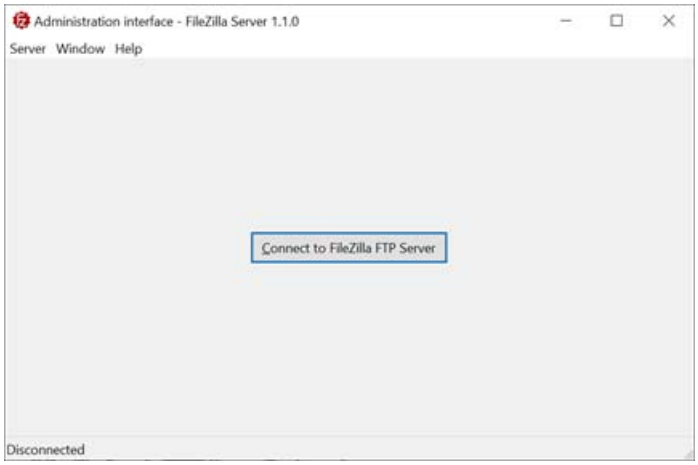
Download and execute the **Open TFTP Server** installation file **OpenTFTPServerSP64bitInstallerV1.70.exe**. Make sure to accept the default options provided by the installer. This process installs the Open TFTP Server Service on Windows.

3: Server Startup and Configuration

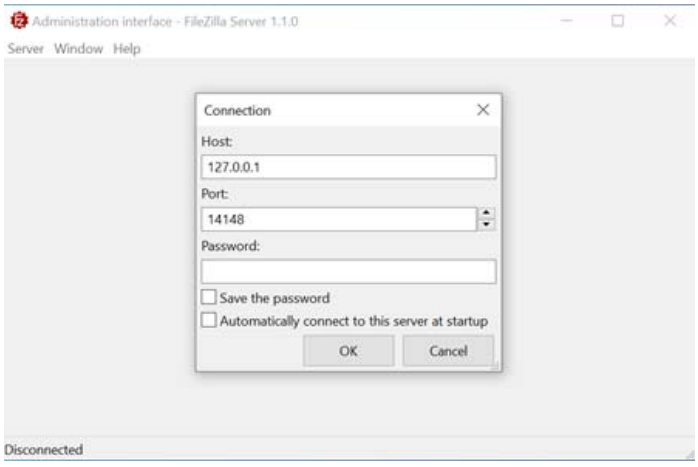
FileZilla FTP Server Configuration

To configure FileZilla FTP Server for GNX Configuration Server:

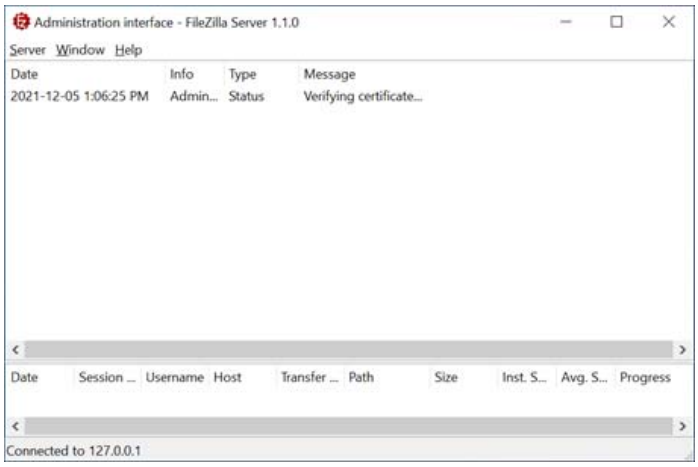
1. On the desktop, click **Start FileZilla Server** to start the FileZilla FTP service.
2. Start the FTP server configuration application: on the desktop, click **Administer FileZilla Server** and click the **Connect to FileZilla FTP Server** button.



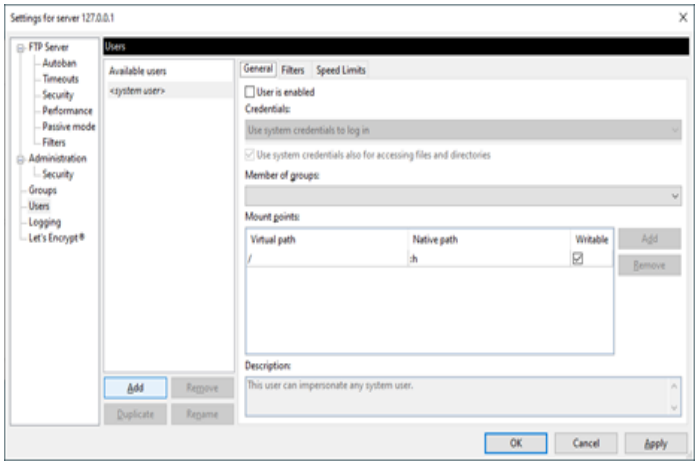
3. Select the localhost and the default FileZilla Administration port in order to run the FileZilla Administration Interface and connect to the local FTP server.
4. Click OK to connect.



5. Verify the FileZilla FTP Administrator is connected to the running FileZilla FTP server with no errors.



6. Once connected to the FTP server, go to **Server > Configure** on the FileZilla FTP Administrator interface:



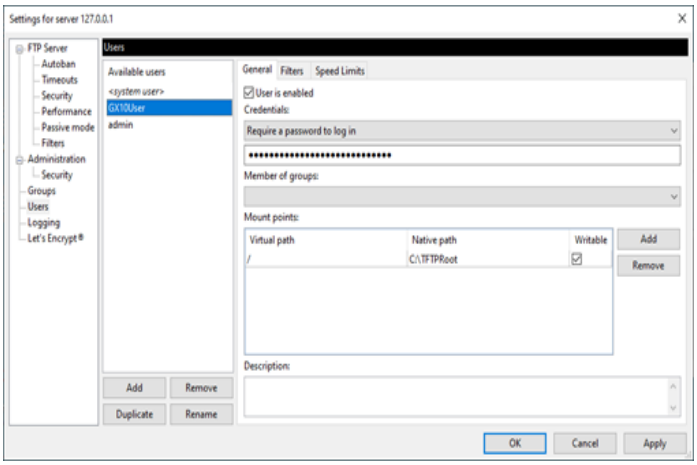
7. On the Settings for Server screen go to **Users** and click **Add** to add the GNX device generic **GX10User** user as follows:
   - Select Credentials as **Require a password to log in**.
   - Set the username as: **GX10User**
   - Set the password as: **secur1ty**
   - Under **Mount points** add a virtual path to **/** and the Native path to **C:\TFTPRoot** writable.
   - Click **Apply** to add the new user.

   The Username and Password can be customized to the customer needs.

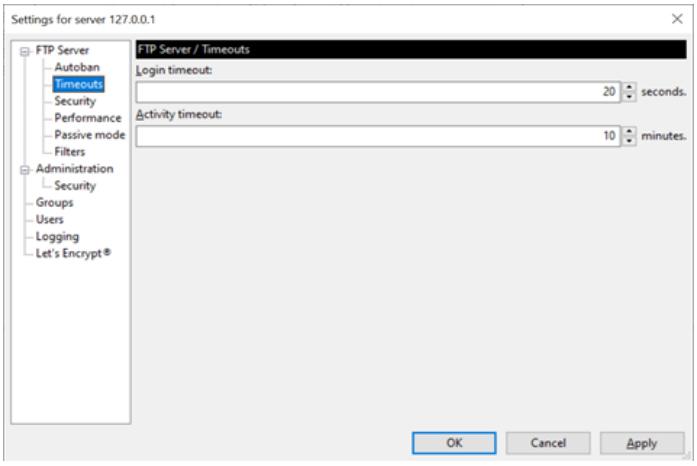
In addition to the GNX Device account, you should create an FTP account for the server administrator to add/remove and manage configuration files. The admin account should be created using the same process as for the GX10User, but using a different user name. The administrator should have Read/Write permissions and access to the C:\TFTPRoot folder and all its subdirectories.

If the administrator decides not to deploy an TFTP Server, the FileZilla FTP server should have an additional “anonymous” user created in order for a GNX device to deposit JLog data.

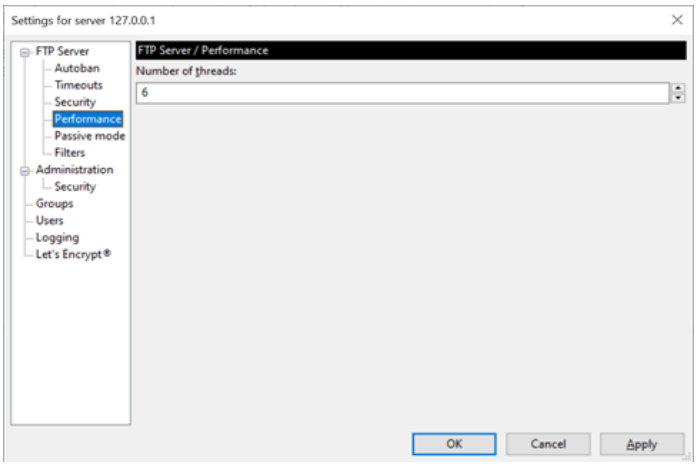
The “anonymous” user should have credentials set to **Do not require a password to log in** and its access should be restricted to the **C:\TFTPRoot\debug** folder in the **Mount points** section with Write access.



It is recommended that the FTP server has defined Login and Activity timeouts as shown below:

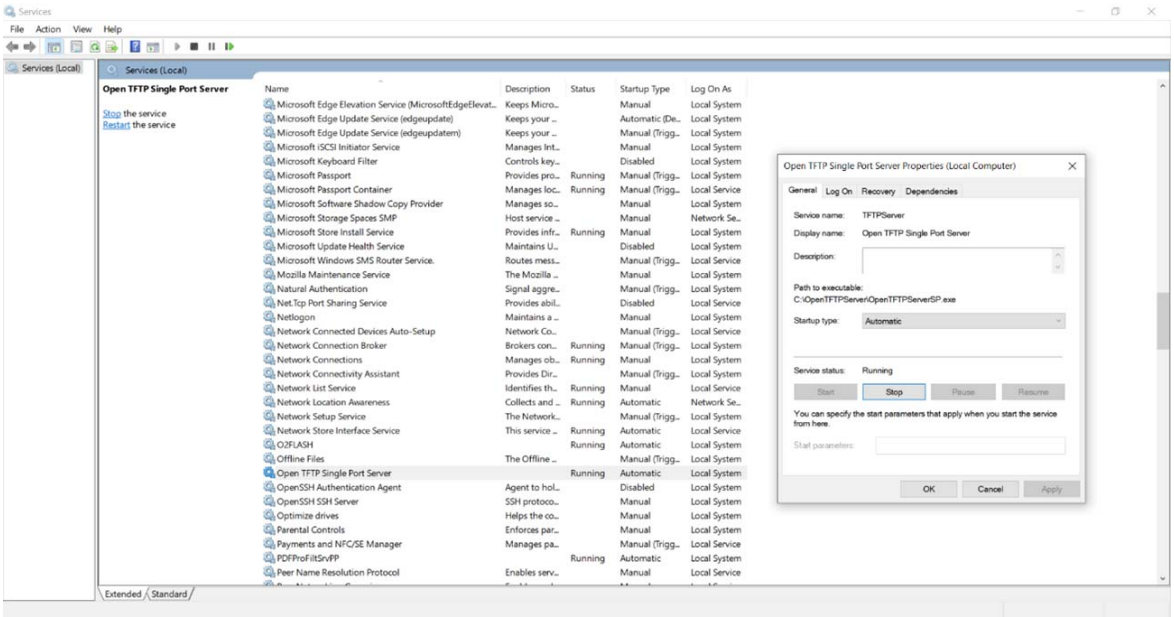


Depending on the numbers of units needing service from the FTP server, the number of threads can be adjusted to improve performance as shown below:

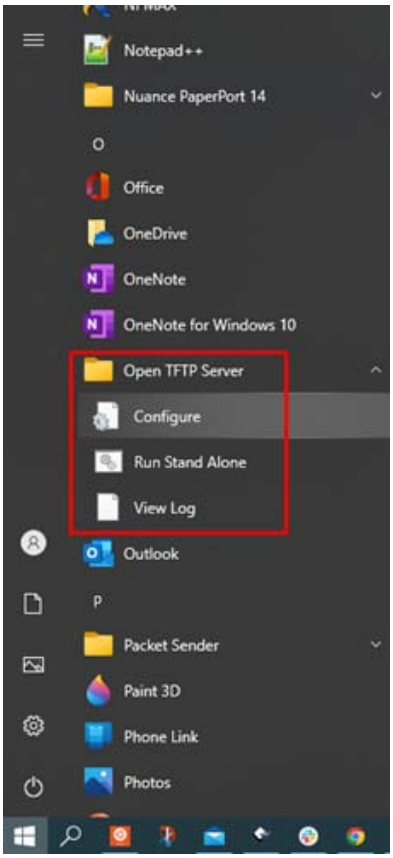


Open TFTP Server Configuration

The Open TFTP Server Installation will automatically install the **Open TFTP Single Port Server** service. This service can be stopped and started from the Windows Services application.



The Open TFTP Server can be configured by modifying the **OpenTFTPServerSP.ini** file. This file can be opened from the **Open TFTP Server** shortcut or it can be found at C:\OpenTFTPServer. The TFTP Server logs can be found in the C:\OpenTFTPServer\log folder, and this folder can also be opened from the **Open TFTP Server** shortcut in the Windows Start Menu.

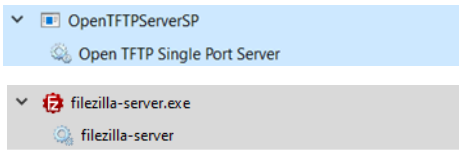


The Open TFTP Server should be configured by editing the OpenTFTPServerSP.ini file and setting the [HOME] section to the TFTP home directory, in this case to C:\TFTPRoot, and is recommended that the [TFTP-OPTIONS] blksize is set to the maximum value 65464, optionally the [LOGGING] level can be set to 'all'.

The “Open TFTP Single Port Server” service should be restarted after making changes to the the **OpenTFTPServerSP.ini** configuration file.

Verifying Operation

You can verify the FileZilla FTP server and the Open TFTP Server services are running by looking at the Task Manager:



Now GNX can make FTP/TFTP connections to the servers and download configuration and FW upgrade files. GNX can use the TFTP server and the FTP server simultaneously, because both protocols are supported by the GNX firmware.

GNX can also be configured to use TFTP or FTP as the default protocol for commands where the VIATFTP/VIAFTP option is not available, such as RESYNCNOW.

To have GNX default to a specific protocol, set the CONFIGURATION_MODE as follows in the GNX device:

- `SETPARAM CONFIGURATION_MODE=4;  // TFTP`
- `SETPARAM CONFIGURATION_MODE=64;  // FTP`

4: GNX Configuration Server Core Services

GNX Device Configuration

GNX Device configurable settings

The GNX device contains more than user 500 configurable settings. Some settings are intended to configure the core functionality of the GNX device such as CAN,1-Wire and Tracking. Other settings are intended to configure report settings, and some settings are intended for device administration.

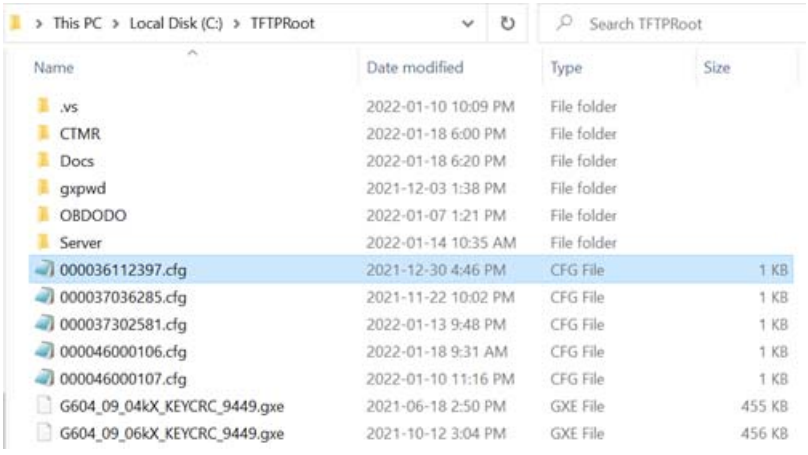
All the configurable settings can be modified via a UART connection and a computer terminal, but this manual process can be very time consuming and not always possible once GNX devices are deployed in the field, away from the device administrator. To overcome this problem, GNX is capable of using its over-the-air network capabilities to download and parse configuration settings from ASCII files located in predefined FTP/FTPT servers.

GNX Configuration Server

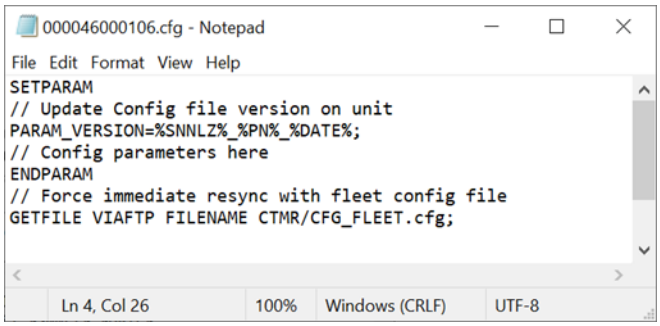
The GNX Configuration Server is an FTP/TFTP server that a customer deploys in order to send configuration and FW files to GNX devices requesting them (See Server Startup and Configuration).

Root (device) Configuration Files

A GNX configuration file is an ASCII files with a .cfg extension; a root configuration file is the first .cfg file a GNX device will request when accessing the server for the first time. The root configuration files must be placed in the root of the FTP/TFTP folder **C:\TFTPRoot**. There is only one root configuration file per GNX unit, and this file must be named after the GNX device's serial number:

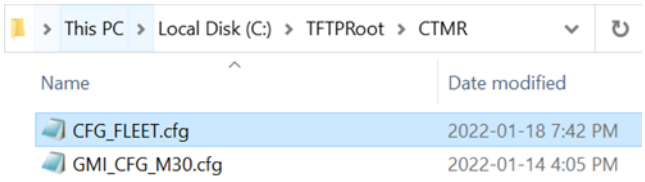


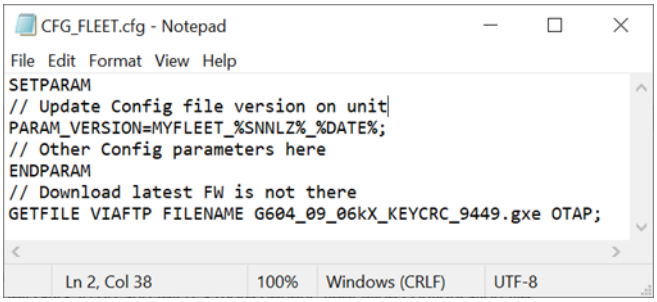
A configuration file can include all the configuration information the requesting GNX device needs, or it can simply tell GNX to fetch a broader fleet-wide configuration file from a directory dedicated to that customer.



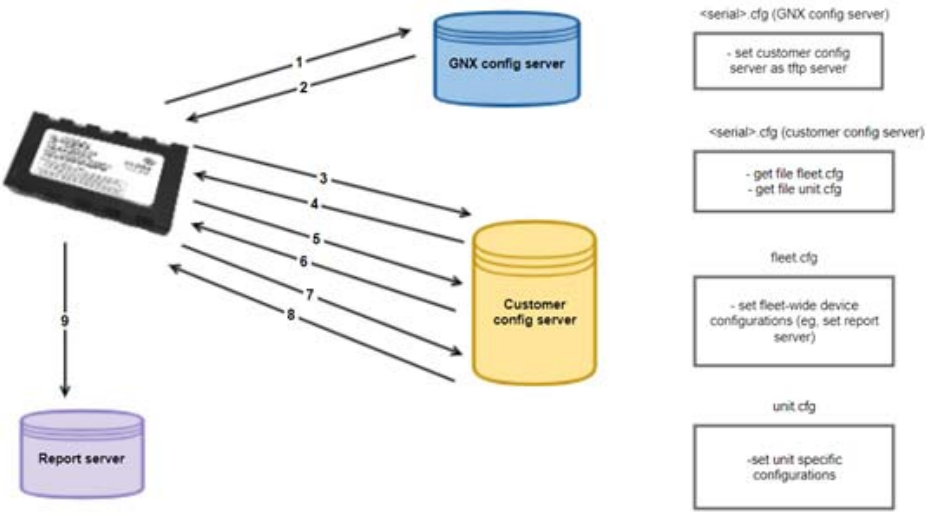
Fleet Configuration Files

Fleet configuration files are usually grouped inside a folder designated for a particular customer or fleet of devices. Many root files can point to a single fleet-wide configuration file, which allows the administrator to configure a fleet of devices without having to edit every serial.cfg file in the root directory. An example for the customer CTMR is shown below:





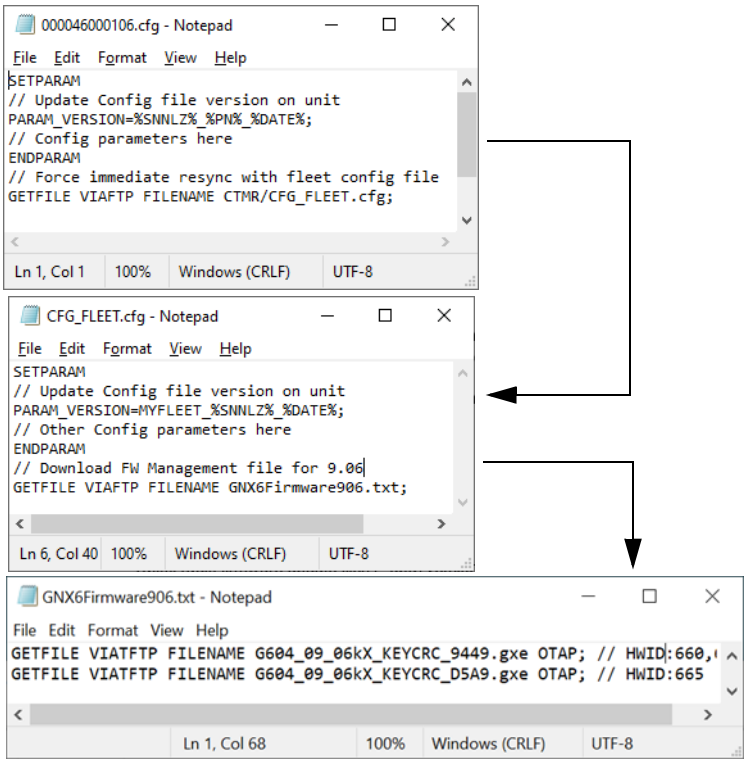
The downloaded config files set device parameters and can instruct the device to download more config files, in a daisy chain manner. This allows users to apply fleet-wide, sub-fleet, or unit-specific configurations to a device.



GNX Firmware Update Files

GNX Device Firmware Update Files

Configuration files can be used to tell GNX to download a particular FW update file. When upgrading the firmware on a fleet of GNX units, it is recommended that the serial.cfg or fleet.cfg file tells GNX to fetch a firmware management text file from the server. The administrator can edit this firmware management text file to include commands to download the latest FW files to cover different GNX hardware variations. In this case the file daisy chain will be as follows:



To deposit firmware update files and maintain the firmware configuration files, the system administrator logs in to the GNX Configuration Server using the **admin** account.

GNX firmware update files (*.gxe) should be placed directly in the **C:\TFTPRoot** directory. If the administrator decides to use a firmware management text file, the text file should also be placed in the **C:\TFTPRoot** directory.

GNX Radio Firmware Update Files

GNX is capable of updating the firmware on its radio module. This process is usually handled by the micro code in the HL7x radio module itself with minimum intervention from GNX, but some GNX devices are populated with the Ublox LARA-R202 module. To update the firmware on this radio module, GNX needs to make an FTP connection to the server and download the FW update file for the Ublox module.

Ublox radio firmware update files (*.upd) version 30.44 and under should be placed directly in the **C:\TFTPRoot** directory.

Ublox radio firmware update files (*.upd) version 30.55 and over should be placed in the **C:\TFTPRoot\radiofw** directory.

VIN Server

The VIN server is a service provided by the standalone DOS application **OBDOdoServer.exe**. This application runs when the server powers up and listens on the UDP port specified in the **config.txt** file.

The VIN server application receives the data produced by the command **DIAG SERNUM PARAMS=568,554,557** from a GNX device as it attempts to read the vehicle's odometer.

The VIN server uses the VIN number (param 568) provided by GNX as a primary key. After a search on the odometer lookup table (OBDOdoVINLookup.txt) it evaluates whether a GETFILE command can be sent back to GNX to instruct it to download a VIN-specific configuration file that GNX will use to read proprietary odometers.

The parameters GNX sends to the VIN server are the following:
- PARAM_VBUS_VIN (568): Vehicle VIN - Primary Key for OBDOdoVINLookup.txt
- PARAM_OBD_ODO_ADDRESS (554): request/response CAN OBD address
- OBD_ODO_PARSE_FORMAT (557): bytes to extract from response for ODO.

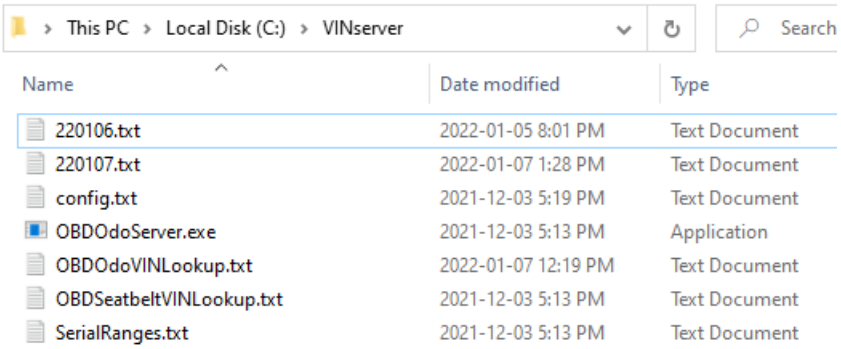
The **OBDOdoVINLookup.txt** file is a lookup table that cross-references VIN prefix and year to a configuration file that configures the requesting GNX device to read the vehicle's proprietary data.

The **SerialRanges.txt** file allows whitelisting or blacklisting of GNX serial numbers or serial number ranges in case specific customers wish to opt out of this service.

The **OBDOdoServer.exe** application also generates daily log files recording the serial number and VIN of GNX devices that have requested proprietary configuration.

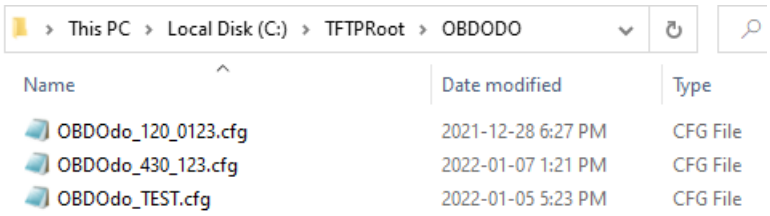
The VIN Server folder should contain all the VIN-specific database files and VIN Server application:
- OBDOdoVINLookup.txt
- OBDSeatbeltVINLookup.txt
- SerialRanges.txt
- OBDOdoServer.exe

A folder named VINserver containing all the required application files should be placed in the root of the hard disk **C:\VINserver** in the GNX Configuration Server.



OBDODO Configuration Files

The configuration files used to read proprietary odometers (OBDOdo files) are to be provided by Sierra Wireless. Because those files will be made available via the FTP server, they must be placed in the **C:\TFTPRoot\OBDODO** directory.



CAN Diagnostics (JLOG)

The JLog feature of GNX is basically available as a debugging service. The customer can use the CAN data collected by the JLogs to debug their system.

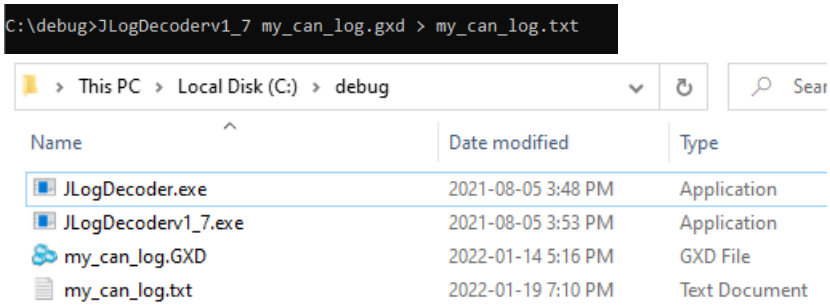
After CAN data has been collected by a JLog command (STARTJLOG3 or STARTJLOG7), the user can request GNX to read the memory window where the JLog data was deposited and send that data via TFTP/FTP to the IP of the GNX Configuration Server. It is recommended that the JLog data is sent to a **debug** folder at the root of the TFP/FTP server.

For example:

```
AT!GXDIAG MEMREADRAW 30080000 4000 VIATFTP XX.XX.XX.XX FILENAME
debug\filename.gxd;
```

The produced **filename.gxd** contains hex data. The application JLogDecoderv1_7.exe is necessary to decode the JLog files and convert them to human readable ASCII files.

The JLogDecoderv1_7.exe applications may reside in the debug folder and can be executed as follows:

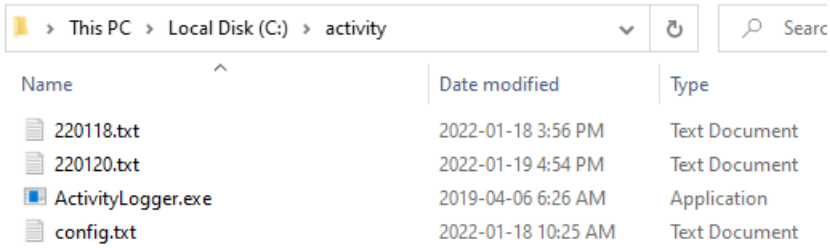


Activity Logger

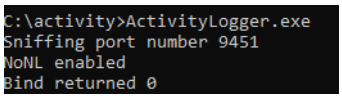
The Activity Logger is not a core or essential service to operate the GNX Configuration Server, but it can be very useful for tracking what FW version GNX devices are running. The ActivityLogger.exe application runs when the server powers up. It listens to UDP port 9451 for GNX records that are triggered by the following events:

- DIAG HARDWARE is sent whenever a GNX device is factory/NV reset. This allows us to track firmware versions on the GNX.
- DIAG USAGE when they hit their data usage limit. This allows tracking of units that may be misconfigured or may not be receiving acknowledgments from the customer data servers.
- OTAP_START, OTAP_END when a GNX device starts and finishes an OTAP file download.

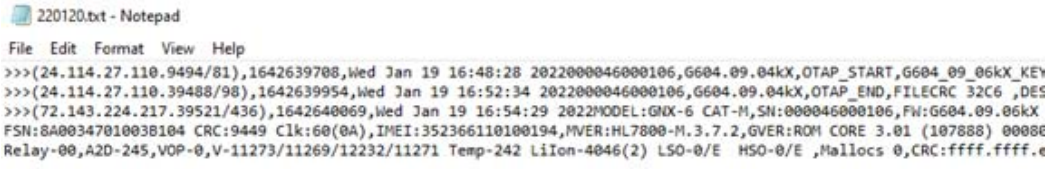
The Activity Logger application is traditionally placed in a directory named **activity** in the root of the hard disk **C:\activity**.



It is recommended that the ActivityLogger.exe application be started with the server, but it can also be started manually as follows:



The Activity Logger application will generate dated log files containing the date and time of the events it is listening to:



Configuring Applications

Standalone applications like the VIN server and Activity Logger can be configured with the following parameters included in their config.txt files.

See Table 4-1 for parameter definitions.

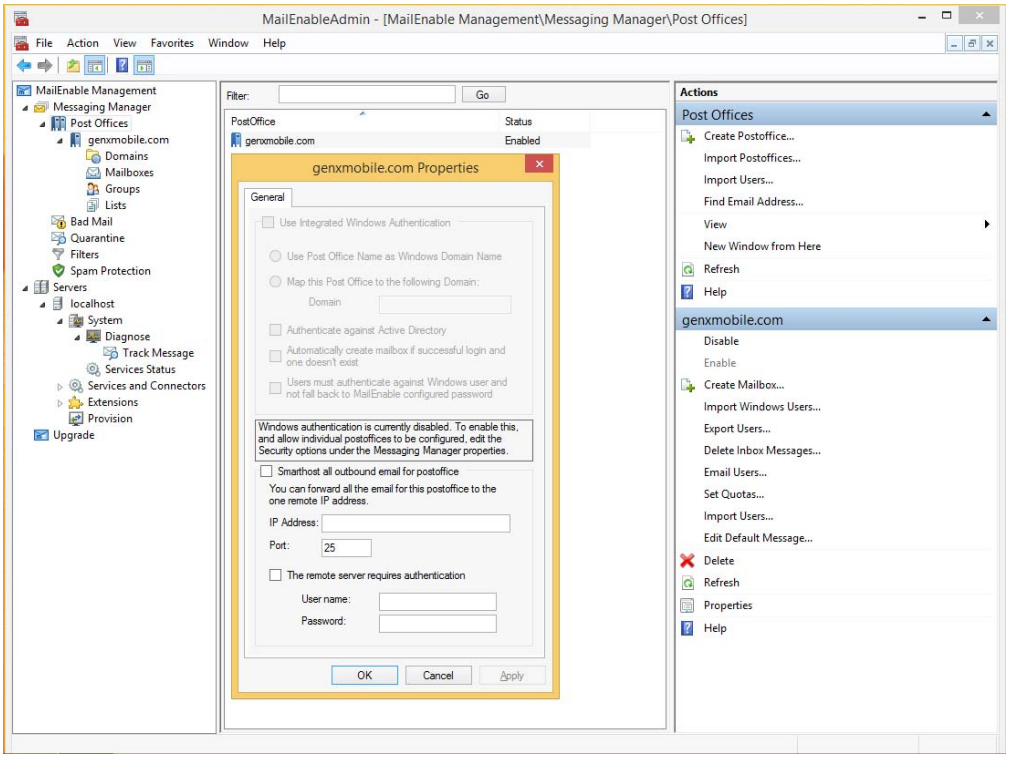
Table 4-1: Configuration Parameters

Parameter example	Description
LISTEN_PORT=9451	Port where the application is listening for GNX data.
ACK_TYPE=UDPACK	Ack type to GNX
NONL	Define to replace New Line with Comma when writing log.
DAILYLOG	Define to create a new log file per day.
FORWARD_OOS=NO	Deprecated parameter
SERVER_IP=45.79.93.94.x4C.x2D.45.79.93.94.x4C.x32	Optional—data server IP to replicate log data.
ODOGET=GETFILE VIATFTP 24.66.228.120 FILENAME OBDODO\	AT parameter specifying how GNX will download the Odometer Configuration file.

SMTP Server

GNX can send Alerts and Reports via email. By default, and after a factory reset, the SMTP mail server address will be **genxmobile.com**, which resolves to Sierra Wireless address 192.119.178.51 (port 25), username: GX10User, password: secur1ty.

Once the Sierra Wireless GNX config server is decommissioned, you must set up your own MailEnable SMTP Server (shown below) or any desired SMTP server to continue using this feature. The new SMTP server name can be configured using GNX parameter SMTP_SERVER_NAME(49). For more information, see Reference on page 29.


MailEnableAdmin - [MailEnable Management\Messaging Manager\Post Offices]
File Action View Favorites Window Help
MailEnable Management
Messaging Manager
Post Offices
genxmobile.com
Domains
Mailboxes
Groups
Lists
Bad Mail
Quarantine
Filters
Spam Protection
Servers
localhost
System
Diagnose
Track Message
Services Status
Services and Connectors
Extensions
Provision
Upgrade
Filter:
Go
PostOffice
Status
genxmobile.com
Enabled
genxmobile.com Properties
General
Use Integrated Windows Authentication
Use Post Office Name as Windows Domain Name
Map this Post Office to the following Domain:
Domain
Authenticate against Active Directory
Automatically create mailbox if successful login and one doesn't exist
Users must authenticate against Windows user and not fall back to MailEnable configured password
Windows authentication is currently disabled. To enable this, and allow individual postoffices to be configured, edit the Security options under the Messaging Manager properties.
Smarthost all outbound email for postoffice
You can forward all the email for this postoffice to the one remote IP address.
IP Address:
Port:
25
The remote server requires authentication
User name:
Password:
OK
Cancel
Apply
Actions
Post Offices
Create Postoffice...
Import Postoffices...
Import Users...
Find Email Address...
View
New Window from Here
Refresh
Help
genxmobile.com
Disable
Enable
Create Mailbox...
Import Windows Users...
Export Users...
Delete Inbox Messages...
Email Users...
Set Quotas...
Import Users...
Edit Default Message...
Delete
Refresh
Properties
Help

5: GNX Config Redirect (Optional)

GNX Configuration Server Destination

Background

Currently each customer has been provided with an FTP/TFTP account dedicated and limited to access only their **Customer Name** folder under **D:\TFTProot**; for example, **D:\TFTPRooot\Customer**

When new GNX devices are purchased and registered on the GNX Configuration Server, Sierra Wireless generates a basic configuration file and places it at the root of the TFTP/FTP folder **D:/TFTPRoot**. This file has instructions to redirect the identified GNX devices to a specific, customer controlled, fleet configuration file located in the customers directory.

Thousands of serial.cfg files at TFTPRoot level can point to a single fleet configuration file. Customers can customize the configuration files in their directories to meet their needs.

GNX devices, if set up to do so, will RESYNC with the GNX Configuration Server and download the config file every hour/day/week depending on the value in PARAM_RESYNC_TIME(501).

Objective

The goal is to retire the Sierra Wireless GNX Configuration Server hosted at IP address 192.119.178.51 and to have customers host their own private GNX Configuration Servers.

To accomplish the hand-over from the Sierra Wireless GNX Configuration Server to a customer's private GNX Configuration Server, the customer must have a GNX Configuration Server deployed as described in Server Startup and Configuration on page 11.

The intention is that GNX customers who want to continue configuring their devices via a TFTP/FTP server have their devices reprogrammed to replace the factory default Sierra Wireless IP 192.119.178.51 with the IP of their private configuration server.

To have the GNX devices redirected to the new server, it is necessary to replace the root serial.cfg files at the **D:\TFTPRoot** level in the current server so syncing GNX devices will be reprogrammed to redirect to the new server from there on. After that, it is expected that these GNX devices will not attempt to sync on the default IP 192.119.178.51 unless they are factory reset.

Redirect Strategy

The following steps describe the proposed strategy to redirect GNX units to a deployed TFTP/FTP server on the customer site:

Step 1: Group Serial Numbers per Customer

1. The customer should provide a list of all the serial numbers of GNX devices they intend to redirect to their server. The list should be in a file called **redirectserial.txt**.
2. The customer should provide the name of the directory hosted on 192.119.178.51 that they own and want to transfer.
3. It is recommended that the customer generates a spreadsheet of deployed GNX serial numbers and SIM phone numbers to access GNX devices via SMS as a backup recovery mechanism.

Step 2: ZIP Customer's Configuration Files and Backup

Sierra Wireless will copy the customer's .cfg files listed in **redirectserial.txt** along with any directories they requested, and make that into a ZIP or TAR file. The file will be sent to the customer to verify.

The customer shall archive a copy of the ZIP or TAR file and unzip the provided file at the root of their TFTP/FTP virtual folder **C:\TFTPRoot**.

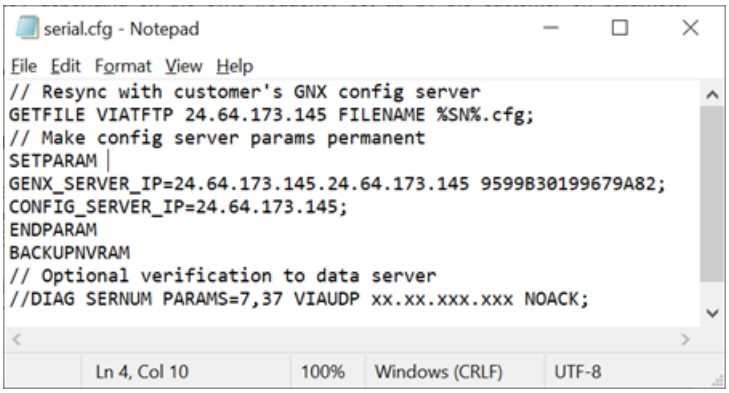
Step 3: Replace Serial Number files with Redirect Template

On the Sierra Wireless GNX config server there should be a script to replace all serial.cfg files in **D:\TFTPRoot** listed in **redirectserial.txt** with a redirect template config file. The files to be replaced are only those in **redirectserial.txt**. The replaced files should not be deleted but instead be moved to a backup directory.

The redirect script should take as input the serial numbers in **redirectserial.txt**, the IP and DNS (optional) of the new GNX config server and the GNX admin password for the week. Optionally the user may provide the IP of their data server for confirmation.

From the sample redirect template config file below:

- 24.64.173.145: IP address of new GNX config server provided by the customer.
- 9599B30199679A82: Weekly password the script gets by calling gxpwd.exe
- serial.cfg: should be an actual serial number from redirectserial.txt file.
- xx.xx.xxx.xxx: Data server IP hosted by the customer.



The template redirect file will accomplish the following on a GNX device when downloaded from the Sierra Wireless configuration server:

1. Update the GNX device with the config file parameters in the customer-deployed GNX config server - original parameters.
2. Replace the CONFIG_SERVER_IP (7), CONFIG_SERVER_NAME (31) (optional), and GENX_SERVER_IP (37) values to the IP of the GNX config server hosted by the customer.
3. Save all values to non-volatile memory.
4. Optional: If requested by a customer, it can send a UDP message to their data server listing the updated parameters.

Verification

GNX Devices Sync with Redirect Template

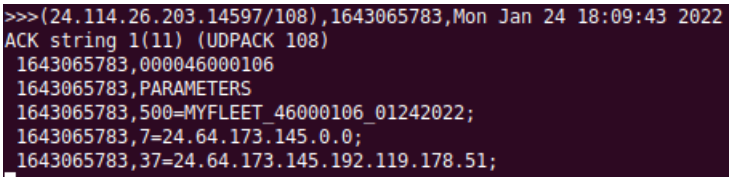
Eventually GNX devices will sync with the GNX Configuration Server IP at 192.119.178.51, depending on the sync frequency on parameter PARAM_RESYNC_TIME (501). The customer should monitor their TFTP/FTP server logs to verify their GNX devices are checking in to download the .cfg files.

Optionally to get real-time feedback that the GNX device has updated its configuration server settings, the following command can be added at the end of the redirect template file:

```
AT!GXAPP DIAG SERNUM PARAMS=7,37 VIAUDP xx.xx.xxx.xxx NOACK;
```

This command will have GNX check in with the customer's data server located at IP xx.xx.xxx.xxx. It then reports the serial number and the value of the reprogrammed parameters CONFIG_SERVER_IP (7), CONFIG_SERVER_NAME (31) (optional), and GENX_SERVER_IP (37).

For this verification feature to work, the customer must provide the IP of their data server or the IP where a UDP Sniffer application can run.



Factory Reset Recovery

The parameters entered to redirect the GNX Configuration Server will be set back to default (hard coded Sierra Wireless IP 192.119.178.51) after a RESETGNX FACTORY or RESETALLPARAMS command.

To recover, send an SMS to the phone number of the GNX device to have it redirect to the customer's IP.

The SMS should have the following 2 commands

```
SETPARAM CONFIG_SERVER_IP=XX.XX.XXX.XXX;
BACKUPNVRAM;
```

This forces a resync with the new GNX config server at IP address XX.XX.XXX.XXX

After a factory reset, the configuration mode must be set to the protocol of the deployed server; the default protocol is TFTP (4).

```
SETPARAM CONFIGURATION_MODE=64
SETPARAM CONFIGURATION_MODE=4
```

Reference

Command Reference and Parameter Definitions for GNX Mobile Tracker - GNX-6/5P