Field Tools 3.18 Quick Start Guide

Energy and Transportation Solutions

EMERSON

Application & Device Safety Considerations

- ### Reading these Instructions
  Before operating a device or application, read these instructions carefully and understand their safety implications. In some situations, improper use may result in damage or injury. Keep this manual in a convenient location for future reference. Note that these instructions may not cover all details or variations in equipment or cover every possible situation regarding installation, operation, or maintenance. Should problems arise that are not covered sufficiently in the text, immediately contact Energy and Transportation Solutions (ETS) Customer Support for further information.

- ### Protecting Operating Processes
  The failure of a device or application – for whatever reason – may leave an operating process without appropriate protection and could result in possible damage to property or injury to persons. To protect against this, review the need for additional backup equipment or provide alternate means of protection (such as alarm devices, output limiting, fail-safe valves, relief valves, emergency shutoffs, emergency switches, etc.). Contact ETS for additional information.

- ### Using Qualified Personnel
  Installation, configuration, and any subsequent modifications to a device or application should only be performed by qualified, suitably trained personnel.

- ### System Training
  A well-trained workforce is critical to the success of your operation. Knowing how to correctly install, configure, program, calibrate, and troubleshoot your Emerson equipment provides your engineers and technicians with the skills and confidence to optimize your investment. ETS offers a variety of ways for your personnel to acquire essential system expertise. Our full-time professional instructors can conduct classroom training at several of our corporate offices, at your site, or even at your regional Emerson office. You can also receive the same quality training via our live, interactive Emerson Virtual Classroom and save on travel costs. For our complete schedule and further information, contact the ETS Training Department at 800-338-8158 or email us at *education@emerson.com*.

- ### Grounding Equipment
  Ground metal enclosures and exposed metal parts of electrical instruments in accordance with relevant safety standards. For the USA, refer to OSHA rules and regulations as specified in *Design Safety Standards for Electrical Systems*, 29 CFR, Part 1910, Subpart S, dated: May 16, 1981 (OSHA rulings are in agreement with the National Electrical Code). For international locations, refer to IEC 60364-4-41: PROTECTION AGAINST ELECTRIC SHOCK. You must also ground mechanical or pneumatic instruments that include electrically operated devices such as lights, switches, relays, alarms, or chart drives. The chassis (or earth ground) lug provides a safe connection point to a customer-designated ground location for ESD and transient voltage suppression. Do not use the chassis ground lug for signal, common, or return connections. **Do not connect the chassis ground lug directly to a lightning arrestor/lightning rod.** Do not run signal wiring in conduit or open trays with power wiring or near heavy electrical equipment. If shielded wiring is used, ground the shield of the signal wiring at any one point of the signal loop.

  Important: Complying with the codes and regulations of authorities having jurisdiction is essential to ensuring personnel safety. The guidelines and recommendations in this manual are intended to meet or exceed applicable codes and regulations. If differences occur between this manual and the codes and regulations of authorities having jurisdiction, those codes and regulations must take precedence.

- ### Protecting from Electrostatic Discharge (ESD)
  Any device contains sensitive electronic components which can be damaged by exposure to an ESD voltage. Depending on the magnitude and duration of the ESD, it can result in erratic operation or complete failure of the equipment. Ensure that you correctly care for and handle ESD-sensitive components.

- ### Ethernet Connectivity
  This automation device is intended to be used in an Ethernet network which **does not** have public access. The inclusion of this device in a publicly accessible Ethernet-based network is **not recommended**.

- ### Returning Equipment
  If you need to return any equipment to ETS, it is your responsibility to ensure that the equipment has been cleaned to safe levels, as defined and/or determined by applicable federal, state and/or local law regulations or codes. You also agree to indemnify ETS and hold ETS harmless from any liability or damage which ETS may incur or suffer due to your failure to ensure device cleanliness.

Contents

Chapter 1. Introduction

1.1 What is Emerson Field Tools?

Emerson Field Tools provides a single integrated package for connecting to and configuring ROC, FloBoss™, ControlWave™ flow computers and RTUs, FB1000/FB2000 Series Flow Computers, and FB3000 RTUs.

Field Tools supports either a direct serial connection or an IP connection to a controller or flow computer. You can also connect wirelessly with FB1000/FB2000 Series Flow Computers. In all these cases, you establish communications with the controller using Field Tools' Connection wizard.

In addition, if you install configuration tools for the controller (ROCLINK, TechView, and/or FBxConnect) Field Tools automatically launches the appropriate tool when you open a connection to a ROC, FloBoss, ControlWave device, an FB1000/FB2000 Series Flow Computer, or an FB3000 RTU.

Chapter 2. Installation

This chapter covers installation of Field Tools software.

2.1 Minimum System Requirements

For optimal performance, we recommend that your laptop PC meet the following minimum requirements:

- Intel® Core™2 Duo T7100 or similar specification Intel CPU (minimum)
- 2.5 GB available hard disk space to install the full software package
- 8 GB RAM
- 1366 x 768 or better resolution display (OS compatible)
- Microsoft® Windows 10 Professional, or Windows 11 Professional. Use with older Windows versions is **not** recommended.
- Network port can be either:
  - RS-232 Serial port or USB to RS-232 converter (See *Section 2.1.1*)
  - Ethernet port

For details on compatibility of Field Tools with particular hardware, software, and firmware, please refer to the *Field Tools Product Data Sheet* (D301735X012).

2.1.1 Notes on USB to Serial Converters

USB to RS-232 serial converters vary widely in quality and performance. Users report good results with the following converters:

- BlackBox IC199A
- IOGear® GUC232A
- CHIPI-X10

If you experience problems with your converter, see *Appendix A – Troubleshooting Tips*.

2.2 Before you Begin

Before you install Field Tools, there are several things you need to know:

Important

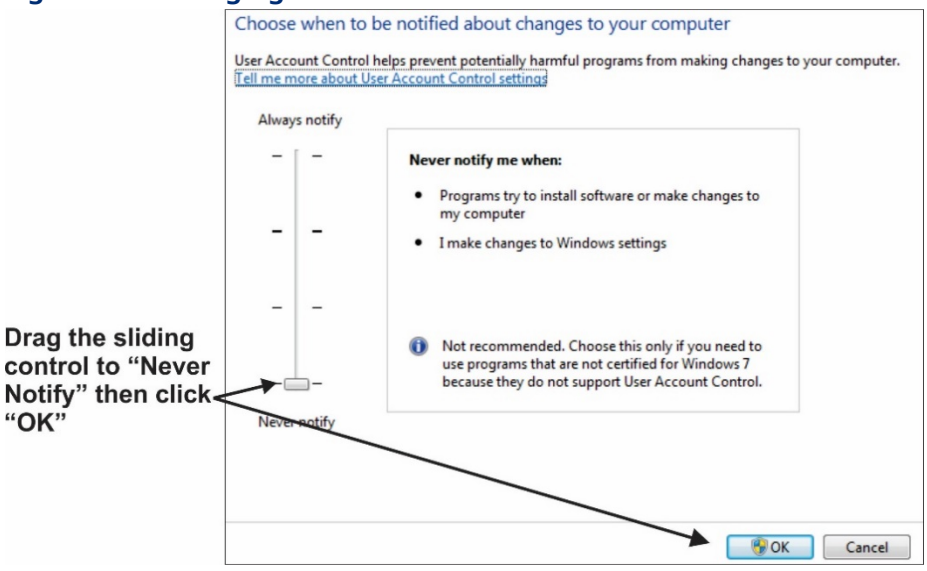
- Field Tools cannot reside on a computer running any components of OpenEnterprise 2.x, OpenEnterprise 3.x, OpenEnterprise Client/Server software, or ObjectServer.
- Field Tools includes components of BSI_Config (such as TechView) which are from OpenBSI version 5.9 Service Pack 3.
- Field Tools can co-exist on a computer running OpenBSI Network Edition 5.9 Service Pack 2 (or newer). It cannot be installed on a computer running OpenBSI versions older than 5.9 Service Pack 2.
- You must have administrative privileges to install Field Tools. The reason you need these privileges is because the Field Tools installer writes to certain folders on your PC that are normally hidden from regular users.
- Field Tools requires Internet access to communicate with RTUs and flow computers via Ethernet, and during installation and license registration. If your anti-virus software blocks Field Tools, you must follow instructions for that anti-virus program to"white list" Field Tools so it can communicate through the firewall.
- If installing TechView, close all other programs down before you begin installation. In particular Office 365 components must be closed because they can interfere with the Field Tools installer.
- You must disable User Account Control (UAC) prior to the installation (you can re-enable it after a successful installation). See *Section 2.2.1*.
- If you are using an Enterprise version of the Windows operating system and your administrative privileges do not include read/write access to \ProgramData\Emerson and its sub-folders, these privileges must be set manually by your system administrator.
- If you are using an Enterprise version of a Windows operating system with an application blocker, set any EXE files in \Program Files\Emerson to "trusted source."
- If installing Field Tools on a Citrix Server, you must disable virtualization of Field Tools for all Citrix Server users prior to the installation, and then reenable virtualization after Field Tools installation is successfully completed.
- For best results on a PC or laptop, set your Windows Control Panel display settings for smaller fonts (100% default). Larger fonts may cause some screen items to overlap or be cut off.
- For best results on a tablet, set your Windows Control Panel display settings for either smaller fonts (100%) or medium fonts (125% default). DPI should be 100.

2.2.1 Disabling User Account Control (UAC) in Windows

You must disable UAC prior to installing Field Tools. You can re-enable it after successful installation.

1. Click **Start > Control Panel** to open the Windows Control Panel.
2. Click **Action Center**.
3. Click **Change User Account Control** settings.
4. Drag the sliding control down to **Never notify** and click **OK**.

Figure 2-1. Changing User Account Control



2.2.2 Special Notes for BSI_Config/TechView Users

If you have BSI_Config 5.9 (which includes TechView) installed prior to installing Field Tools and it is a version older than 5.9 Patch A, the Field Tools installer automatically updates BSI_Config components on your PC to version 5.9 Service Pack 3 (which includes Patch A). If you subsequently reinstall BSI_Config 5.9, you'll need to manually copy the Field Tools installer version of TechView.exe to the proper installation path on your PC. If you used the default installation paths, you can use the following examples, assuming your PC hard disk is the C drive:

For 64-bit OpenBSI Users:

Copy C:\program files (x86)\emerson\openenterprise\bin\TechView.exe to C:\program files (x86)\bristol\openbsi\

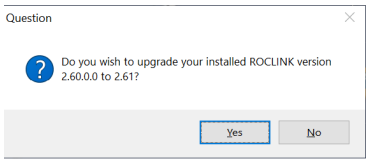
For 32-bit OpenBSI Users:

Copy C:\program files\emerson\openenterprise\bin\TechView.exe to C:\program files\bristol\openbsi\

2.2.3 Special Notes for OpenBSI Users

Field Tools includes components of OpenBSI's BSI_Config Version 5.9 Service Pack 3. OpenBSI Network edition version 5.9 Service Pack 2 (or newer) can co-exist with Field Tools. The Field Tools installer does not affect OpenBSI Network Edition. The two programs, however, are not linked together; you cannot for example, launch NetView from Field Tools.

2.2.4 Special Notes for ROCLINK Users



If you have a version of ROCLINK already installed that is older than the version included in the Field Tools installer, Field Tools prompts you to confirm the upgrade to the newer version. If you answer **Yes** the upgrade proceeds; if you answer **No** the installer leaves the existing version as is.

To preserve your existing files, always backup the device directory (which includes the ROC_USER.MDB file) before you install ROCLINK, and then copy it back after the installation completes. The device directory is the folder **\Program Files\ROCLINK800**.

You can only have three simultaneous ROCLINK connections to devices through Field Tools.

2.3 Installing Field Tools

Field Tools is available as a free download for registered Guardian users. The extracted executable follows the format FieldTools*buildnum*.exe where *buildnum* is the software version build number. See *Section 2.3.2* for instructions on validating the downloaded zip file.

Important

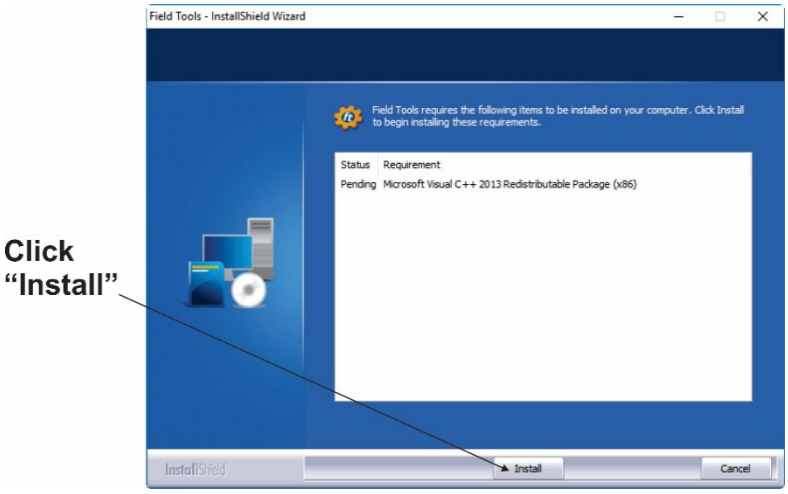
If you are not a registered Guardian user, activating a new Guardian account to obtain Field Tools software may take up to 24 hours to process.

If you are installing the Field Tools executable from a network drive, there may be a long delay while the installer extracts and uncompresses files onto the local PC.

1. Right-click on the Field Tools (.EXE) installation file and choose **Run as administrator** from the pop-up menu.

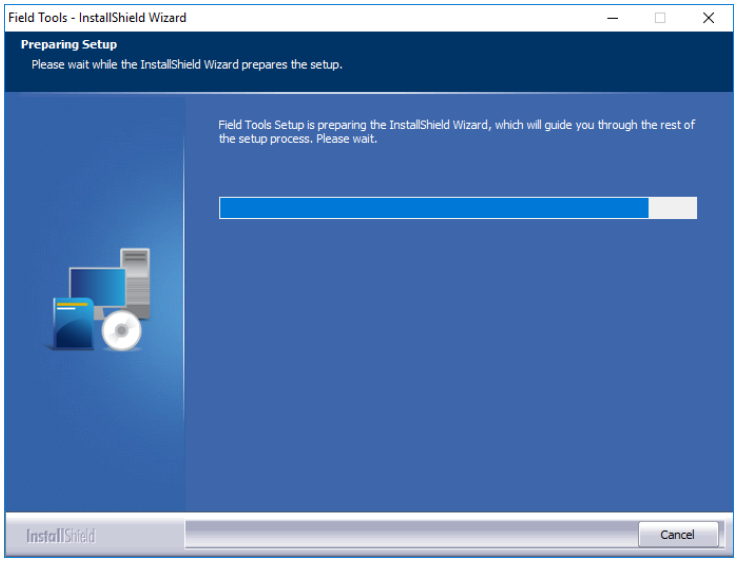
2. The installation process starts and checks whether certain necessary software components exist on the laptop, and if they are not present, the installation process prompts you to install them. Click **Install**. This process may take several minutes, and the installer may require you to reboot your PC.

Figure 2-2. Installshield Wizard



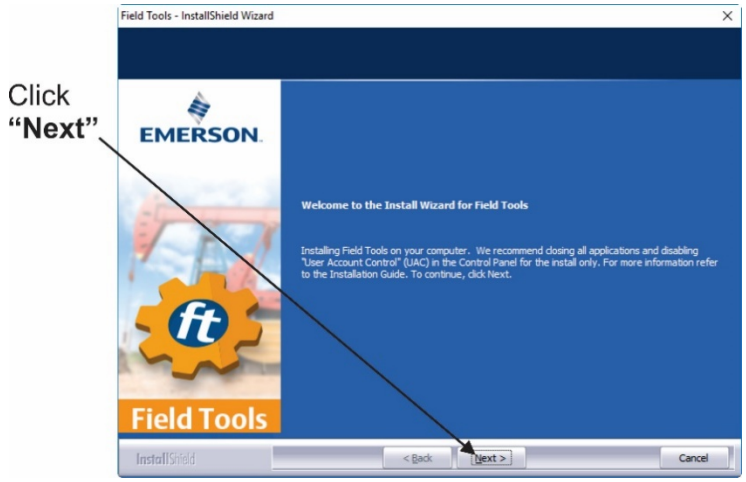
Once installation of the required components finishes, the Field Tools installation wizard starts:

Figure 2-3. InstallShield Wizard



3. Click **Next**.

Figure 2-4. Installer Welcome Screen

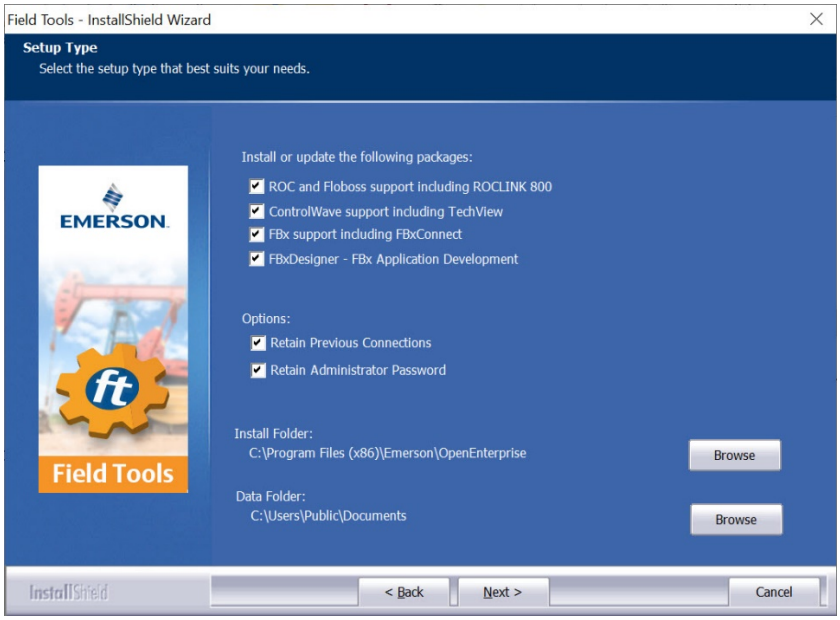


4. To proceed with the installation, click **I accept the terms of the license agreement** and then click **Next**.

Figure 2-5. License Agreement

5. Use the default installation folders for the program and data or click **Browse** to specify different locations. Then select the optional configuration packages you want to install and click **Next**.

Figure 2-6. Optional Package Selection

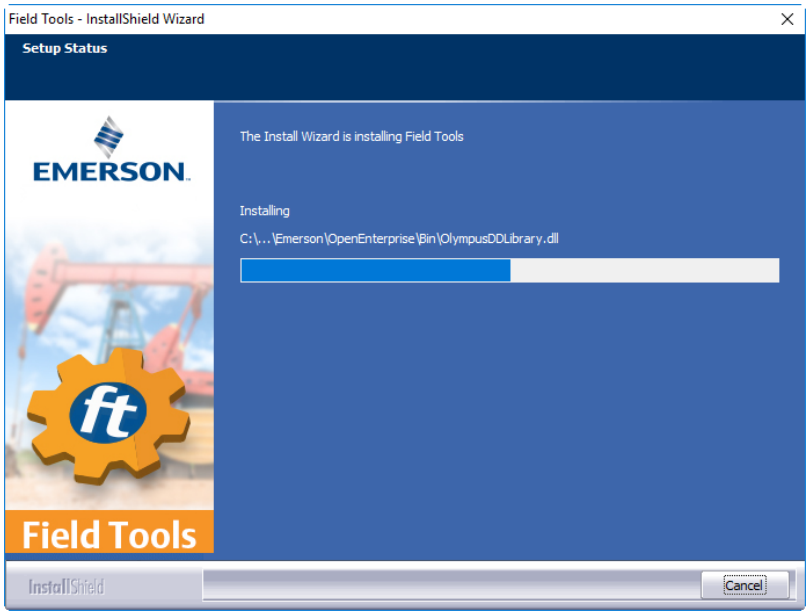


Notes

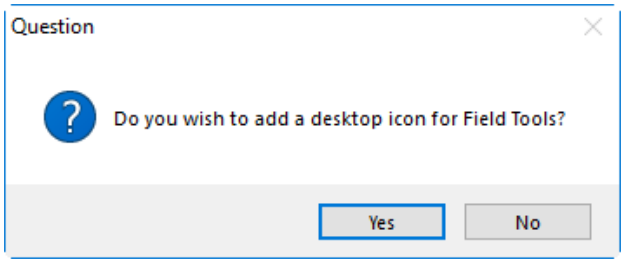
- You must purchase a license to use FBxDesigner; see the *FBxDesigner Quick Start Guide* (D301860X012) for more information on FBxDesigner. See *Chapter 6* for information on using the License Manager to license FBxDesigner. FB3000 users can purchase various features and applications. You license these from Emerson FBxConnect Licensing Tool. See *Section 2.4* for instructions on starting the Emerson FBxConnect Licensing Tool.
- If you are installing over an existing version of Field Tools, you have the option to preserve any saved connections by checking **Retain Previous Connections**, and to preserve the password for Field Tools software by checking **Retain Administrator Password.**

6. The installation proceeds. The installer program periodically reports which components are being installed. This may take several minutes:

Figure 2-7. Setup Status Screen

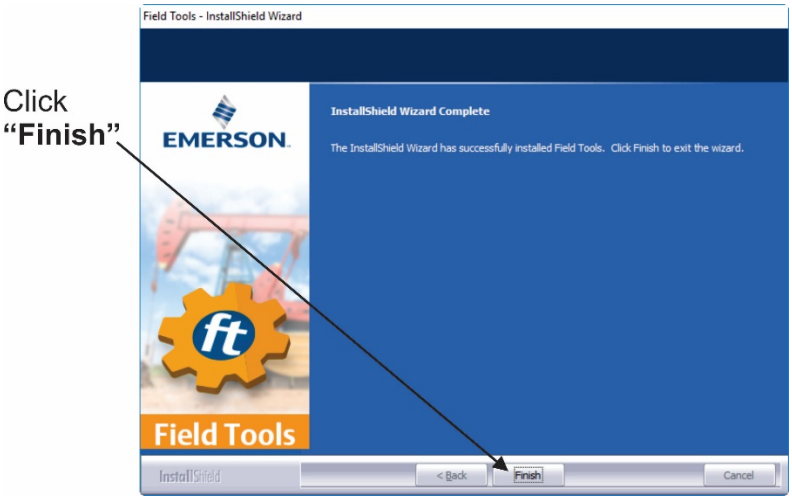


7. The software prompts you whether you want the installer to create a Field Tools desktop icon; click **Yes** if you want to start Field Tools from the desktop.



8. Click **Finish** to exit the installer.

Figure 2-8. Installshield Wizard Finish Screen



2.3.1 Custom Install/Upgrade without User Prompts

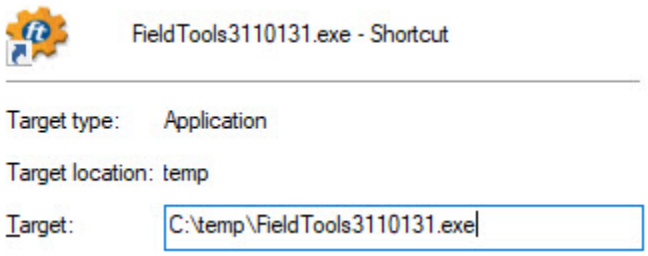
Some companies require software installations and upgrades to be handled by their Information Technology (IT) departments without user intervention.

To do this with Field Tools, you must create a custom setup file in a temporary folder that specifies which packages the installer should load.

The recommended way (and easiest way) to create the setup file is to create a desktop shortcut to the Field Tools installer, and then invoke the installer with the record option "**/r**" to save your installation choices to a file. Then you can use the file with the silent install "**/s**" option to install Field Tools for a user.

Recording an Installation Session to Create a Full Installation Setup File:

1. With the Field Tools installer in your temporary folder "C:\temp", right-click on it and choose Create shortcut and then examine the **Target** field in the properties of the resulting shortcut:



2. Edit the target line to set the record option "**/r**" along with the "**/f1**" option to specify the path and name of the setup file:

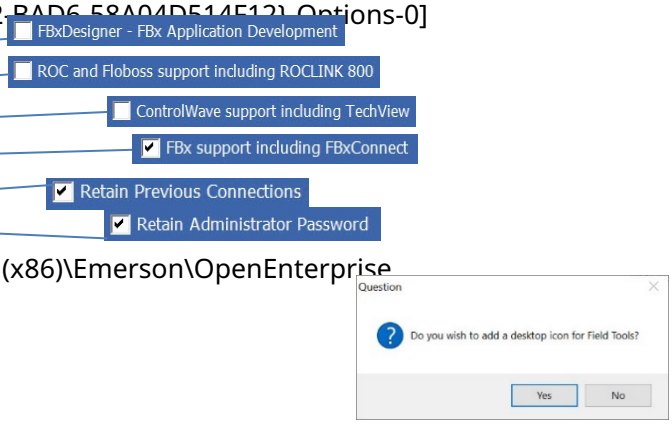
   C:\temp\FieldTools3110131.exe **/r /f1"C:\temp\full.iss"**

3. Click **OK** to exit the properties dialog box.

4. Right-click on the shortcut and choose **Run as administrator** to invoke the Field Tools installer and make your installation choices. See *Section 2.3* for information on what the different fields mean. When you click **Finish** to complete the installation, you should have a completed ISS file in the **C:\temp** folder that reflects the choices you made in the installer and looks similar to the file, below:

   [InstallShield Silent]
   Version=v7.00
   File=Response File
   [File Transfer]
   OverwrittenReadOnly=NoToAll
   [{A336A33B-40A8-4032-BAD6-58A04D514F12}-DlgOrder]
   Dlg0={A336A33B-40A8-4032-BAD6-58A04D514F12}-SdWelcome-0
   Count=5

```
Dlg1={A336A33B-40A8-4032-BAD6-58A04D514F12}-SdLicense2Rtf-0
Dlg2={A336A33B-40A8-4032-BAD6-58A04D514F12}-Options-0
Dlg3={A336A33B-40A8-4032-BAD6-58A04D514F12}-AskYesNo-0
Dlg4={A336A33B-40A8-4032-BAD6-58A04D514F12}-SdFinish-0
[{A336A33B-40A8-4032-BAD6-58A04D514F12}-SdWelcome-0]
Result=1
[{A336A33B-40A8-4032-BAD6-58A04D514F12}-SdLicense2Rtf-0]
Result=1
[{A336A33B-40A8-4032-BAD6-58A04D514F12}-Options-0]
Designer=0
ROCLink=0
TechTools=0
FBx=1
Connections=1
Password=1
Path=C:\Program Files (x86)\Emerson\OpenEnterprise
[Application]
Name=Field Tools
Version=3.11.0.131
Company=Emerson
Lang=0409
[{A336A33B-40A8-4032-BAD6-58A04D514F12}-AskYesNo-0]
Result=0
[{A336A33B-40A8-4032-BAD6-58A04D514F12}-SdFinish-0]
Result=1
bOpt1=0
bOpt2=0
```



The **bolded** items are portions you may choose to edit manually if you decide you want to change the setup file. *Table 2-1*, below, explains these items:

Table 2-1. Silent Install Options

Item	Set To:		
Designer	0	=	Do not install FBxDesigner
	1	=	Install FBxDesigner
ROCLink	0	=	Do not install ROCLINK
	1	=	Install ROCLINK
TechTools	0	=	Do not install TechView
	1	=	Install TechView
FBx	0	=	Do not install FBxConnect
	1	=	Install FBxConnect
Connections	0	=	Delete any existing connections

Item	Set To:		
	1	=	Preserve existing connections from previous installation
Password	0	=	Delete any existing Field Tools administrator password
	1	=	Preserve existing administrator password for Field Tools
Result	0	=	Do not create Field Tools desktop icon
	1	=	Create Field Tools desktop icon

Note

Once you complete the standard install you should save the **_users.bin** and **FieldToolsContainer.config** files from the **\Emerson\FieldTools\Application Data** folder. When you want to run an install/upgrade on a new PC, place these files in the same folder on the new PC **before** installing Field Tools because these files are only read at install/upgrade time.

Running Your Installation File:

1. Edit the target line for the shortcut you created for the installer, and change "**/r**" to "**/s**"

   C:\temp\FieldTools3110131.exe **/s** /f1"C:\temp\full.iss**"**

   Click **OK** to exit the properties dialog box.

2. Right-click on the shortcut and choose **Run as administrator** to invoke the Field Tools installer with your setup file.

3. The installer generates a log file – setup.log – in the C:\temp folder. If you see "Resultcode=0" you know the installation completed successfully.

Creating and Running an Upgrade Setup File:

When upgrading existing Field Tools installations, you need to create a separate setup file specific to the upgrade. Follow the same procedure of creating a shortcut and specifying a setup file path and filename with the "**/r**" and "**/f1**" options to record the upgrade; be sure to use a different name to avoid overwriting your existing setup file.

Then run the file in the same way by editing the shortcut using the "**/s**" and "**/f1**" options.

The file below shows a typical upgrade file:

[InstallShield Silent]
Version=v7.00
File=Response File

```
[File Transfer]
OverwrittenReadOnly=NoToAll
[{A336A33B-40A8-4032-BAD6-58A04D514F12}-DlgOrder]
Dlg0={A336A33B-40A8-4032-BAD6-58A04D514F12}-Options-0
Count=2
Dlg1={A336A33B-40A8-4032-BAD6-58A04D514F12}-SdFinish-0
[{A336A33B-40A8-4032-BAD6-58A04D514F12}-Options-0]
Designer=1
ROCLink=1
TechTools=1
FBx=1
Connections=1
Password=1
Path=C:\Program Files (x86)\Emerson\OpenEnterprise
[Application]
Name=Field Tools
Version=3.11.0.131
Company=Emerson
Lang=0409
[{A336A33B-40A8-4032-BAD6-58A04D514F12}-SdFinish-0]
Result=1
bOpt1=0
bOpt2=0
```

2.3.2 Validating the Field Tools Zip file Hash

The Field Tools ZIP file you download from Guardian has a calculated number associated with it called a “hash.” This number is visible in two .TXT files associated with the ZIP that are also available on Guardian. The hash number is generated based on the contents of the ZIP file, and so the hash should never change unless the file contents change. This is a security measure to ensure the file contents were not changed by a third party.

Once you download the zip file to your PC, make note of the folder where it resides so you can check the hash of the zip file as follows:

1. Type CMD to open a DOS command prompt.
2. Use the CD command to go to the folder where the ZIP file resides.
3. Type the following command and press enter.

   certutil -hashfile “FieldTools*xxxxxxx*_**signed.zip” MD5**

   Where *xxxxxxx* is the release number in the ZIP filename.

4. Compare the hash number you see with the one in the MD5 TXT file. If they do not match, it indicates the Field Tools zip file has been altered. See example, below:

```
>certutil -hashfile "FieldTools3130120_signed.zip" MD5
MD5 hash of FieldTools3130120_signed.zip:
f2b17bfb11b2af0dbe36db8178eb5cb0
CertUtil: -hashfile command completed successfully.
```

5. Type the following command and press enter.

   certutil -hashfile "FieldTools*xxxxxxx*_**signed.zip" SHA256**

   Where *xxxxxxx* is the release number in the ZIP filename.

6. Compare the hash number you see with the one in the SHA256 TXT file. If they do not match, it indicates the Field Tools zip file has been altered. See example, below:

```
>certutil -hashfile "FieldTools3130120_signed.zip" sha256
SHA256 hash of FieldTools3130120_signed.zip:
5184e909a99e944122d5d393822f8102c172e3115f3f155e2790549ec3c3ed72
CertUtil: -hashfile command completed successfully.
```

7. If either the MD5 hash or the SHA256 hash you generate from the ZIP file does not match the corresponding .TXT files for MD5 or SHA256, do **not** use the ZIP file. Contact Emerson for assistance.

2.4 Launching Licensing Tool

If you purchased licensed applications for use with the FB3000 RTU, you launch the licenses through the FBxConnect Licensing Tool. Licensing Tool is installed as part of Field Tools.

To launch Licensing Tool, click **Start** and select **Licensing Tool** from within the Emerson Field Tools group.

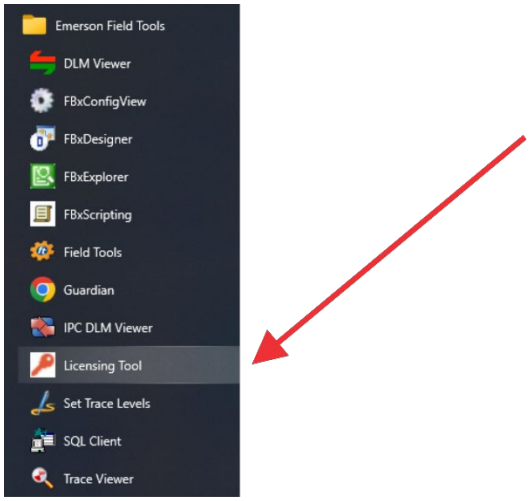
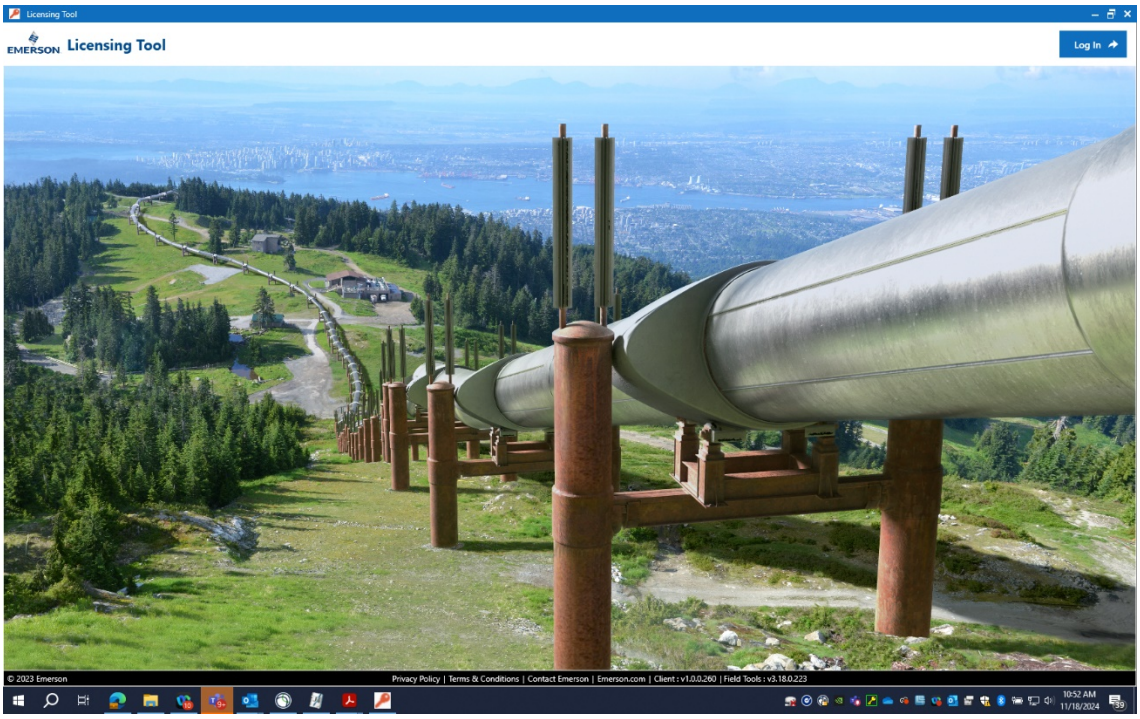


Figure 2-9. Licensing Tool Splash Screen



For details on using Licensing Tool, refer to the *Emerson FBxConnect Licensing Tool Software User Manual* (D301958X012).

Chapter 3. Communication Setup

This chapter covers initial communication setup with Field Tools.

3.1 Using Field Tools to Establish a Connection

Field Tools can communicate with a controller or flow computer using either a direct serial connection or through an IP network. FB1000/FB2000 Series Flow Computers also support wireless connections through FBxConnect.

⚠ CAUTION

When making multiple FBxConnect connections to the same device (as with a remote and a local connection), be aware that the changes one connection makes to the device may not be immediately visible to other connections and may even require the other connections to restart FBxConnect before changes become visible. For example, simple changes (such as changes to setpoints) may be immediately visible to all connections, but changing the number of meters, configuring I/O, adding/deleting menu items, or other major configuration changes may require re-establishing the connection using FBxConnect.

3.2 Before You Begin

- For serial connections, you would typically connect a serial cable between the laptop computer and a serial port on the controller or flow computer. Other options for serial connections could include a radio or modem.
- For IP connections, connect the laptop to the same IP network which includes the controller or flow computer.
- If you have an FBx-series device with the FBxWifi option, you can use a wireless IP connection. This option requires you know the connection key for the wireless network.
- For details on cabling/wiring, consult the hardware manual for your controller or flow computer.

Important
When using Field Tools for serial communication, you must plug into the Local Port. For ControlWave-series units, this is a port for which you've set the **_Pn_LOCAL_PORT** system variable TRUE in the ControlWave project running in

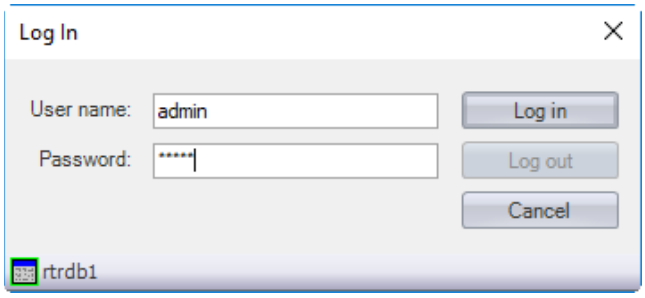
the unit. Local ports answer to requests sent to a BSAP local address of 1 which is what Field Tools requests. For Network 3000, this is a BSAP slave or pseudo-slave port. For a ROC or FloBoss, the Local Port is a specific port (the LOI port) which answers to the address of 240 and a group number of 240.

- For ControlWave/Network 3000 devices only, you need to know which TechView session (*.TVS) file is appropriate for your device so you can specify it when you establish your connection. If you installed TechView, a set of default TVS files resides on your hard disk in your \openbsi installation path. The Connection wizard opens that folder first when you specify your TVS file. For example, there is a CWaveEFM.TVS file to support the ControlWave EFM, a CWaveGFC.TVS file to support the ControlWave GFC, and so on. If you have a customized application with a customized TVS file, you should place it in that folder.

3.3 Starting Field Tools and Logging In

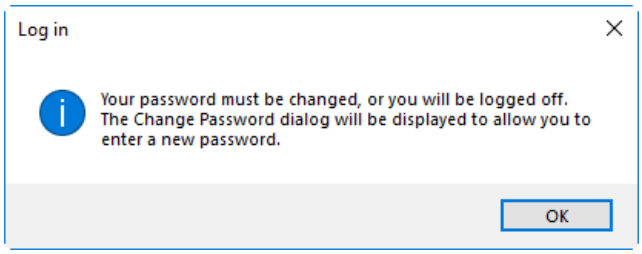
1. Start Field Tools either from the desktop icon or click: **Start > Programs > Emerson Field Tools > Field Tools**.
2. In the Log In dialog box, enter your **User name** and **Password** and click **Log in**.

Figure 3-1. Log in Dialog Box



Important

The very first time you log in, use **admin** for the **User name** and leave the **Password** field blank. Once you've logged in with these defaults, Field Tools prompts you to change your password:



3. The Field Tools main screen opens. Use it to establish a connection with the controller / flow computer.

Figure 3-2. Field Tools Main Screen

3.4 Changing the Password

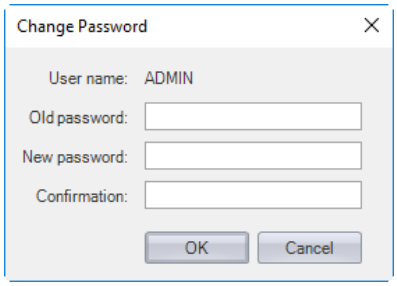
You can change the password for the currently logged on user at any time. .

1. Click **Security** > **Change password** from the menu bar. The Change Password dialog box opens.

Note

The very first time you start Field Tools, the default password for the ADMIN account is blank, and Field Tools forces you to define a new password; click **OK** to open the Change Password dialog box. Passwords are case sensitive.

Figure 3-3. Change Password Dialog Box



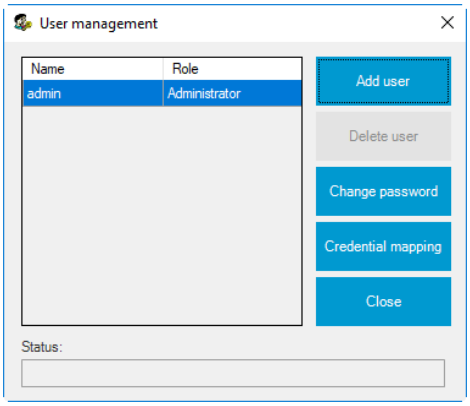
2. In the Change Password dialog box, enter the current password in the **Old password** field, then enter the new password in both the **New password** and **Confirmation** fields, then click **OK**. Your password is now changed.

3.5 Defining Users

The User Management dialog box lets you define Field Tools users, and also configure RTU login credentials for them.

To define the Field Tools users on this PC click **Security > User management** from the menu bar. This opens the User Management dialog box.

Figure 3-4. User management dialog box



3.5.1 Adding a User

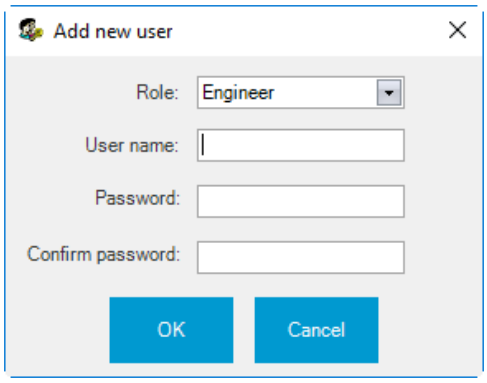
1. If the User Management dialog box is not already open, click **Security > User management** to open it.
2. Click **Add User**. Optionally choose a **Role** for the user. (Particular roles can have particular privileges associated with them.)
3. Enter a **User name** for the user.

Notes

- Usernames are case-insensitive and are stored in the database as lowercase.
- Do not create a user named Operator. This word is reserved for use internally by Field Tools.

4. Enter a password in the **Password** and **Confirm Password** fields.
5. Click **OK**.

Figure 3-5. Add new user Dialog Box

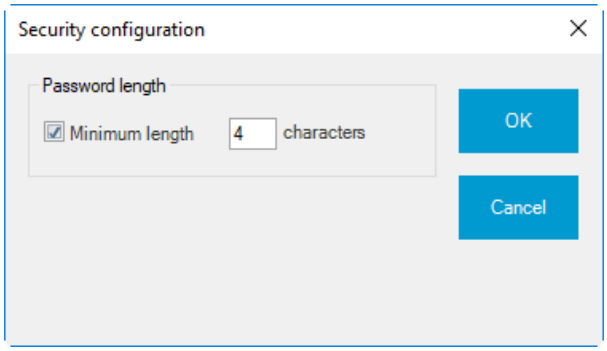


3.5.2 Setting a Minimum Password Length

You can enforce a minimum password length to increase the level of protection of your Field Tools passwords. Passwords can range from 1 to 32 characters. The longer the password length, the harder it is for an intruder to gain access to your system.

1. Click **Security > Security configuration** to open the Security configuration dialog box.

Figure 3-6. Security configuration dialog box



2. Enter the minimum number of characters required for a valid password and click **OK**.

From this point on, all users you define must have a password of this length or longer. Existing users created previously with passwords shorter than this number are unaffected.

3.5.3 Deleting a User

1. If the User Management dialog box is not already open, click **Security > User management** to open it.
2. Click the name of the user you want to delete.
3. Click **Delete user**.
4. Click **Yes** when prompted to confirm the deletion.

3.5.4 Assigning RTU Login Credentials

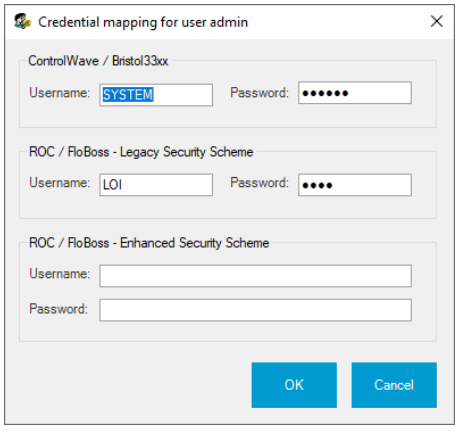
Note
Beginning with Field Tools Version 3.12, a separately licensed credential management utility can be used for this process. See *Chapter 5* for details.

Note

Login credentials for the FB1000/FB2000 Series Flow Computer and the FB3000 RTU default to the login credentials used for Field Tools; for this reason, the Device Credentials dialog box is not relevant for those devices.

1. If the User Management dialog box is not already open, click **Security > User management** to open it.
2. Click the name of the user for which you want to define RTU login credentials then click **Credentials mapping**. The Credentials mapping dialog box opens.

Figure 3-7. Device credentials dialog box



3. Enter a **Username** and **Password** for accessing the particular RTU type(s). If your system includes a mixture of different ROC/FloBoss devices in which some use the enhanced security scheme and others use the legacy security scheme, you should enter appropriate usernames and passwords for both schemes.

Note

ROC/FloBoss devices with newer firmware support either the legacy security scheme (shorter usernames and passwords); or the enhanced scheme, but once upgraded to the enhanced scheme, they no longer support the legacy scheme. Devices with older firmware only support the legacy scheme. Refer to *Table 3-1* to determine which ROC/FloBoss devices support the enhanced security scheme.

Table 3-1. ROC/FloBoss/DL8000 Firmware Revisions Supporting Enhanced Security

Device	Minimum Firmware Revision
ROC 800 Series	3.90 (for additional cybersecurity enhancements, use 3.91 or newer)
FloBoss 107	1.70 (for additional cybersecurity enhancements, use 1.71 or newer)
DL8000	2.60

4. Click **OK**.

3.6 Connections List

The left pane of the Field Tools main screen displays the Connections list tree. This shows connections you've previously saved or used, and also lets you create new connections. w

Figure 3-8. Connections List

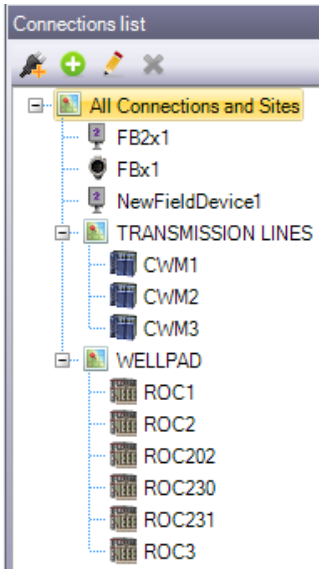
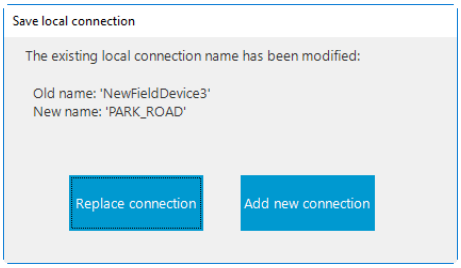


Table 3-2. Connections List Pane and Context Menus Icons

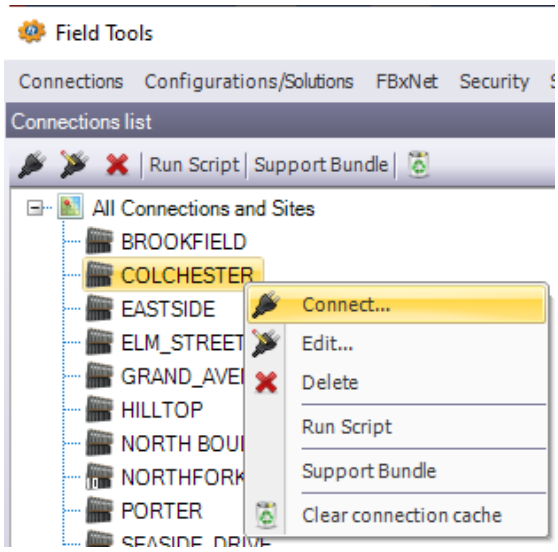
Icon	Description
	Identifies a previously configured connection to an FB1100 Flow Computer. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Identifies a previously configured connection to an FB1200 Flow Computer. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Identifies a previously configured connection to an FB2100 Flow Computer. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Identifies a previously configured connection to an FB2200 Flow Computer. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Identifies a previously configured connection to an FB3000 RTU. The name of the device appears next to the icon. Double-click the icon to re-start the connection.

Icon	Description
	Identifies a previously configured connection to a ROC, DL8000, or FloBoss. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Identifies a previously configured connection to a ControlWave or Network 3000 (33xx) controller. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Shows on top of a controller/flow computer icon when its connection is active. Beginning with Field Tools 2.0, you can have multiple simultaneous active connections.
	Site - A site is just a name underneath which you can group one or more connections. It could represent a geographical area, a department, or any other logical grouping you need. The Connections list comes with a default site name called “All Connections and Sites” which you can rename and/or add additional sites underneath. Although you can rename it, you cannot delete the “All Connections and Sites” site.
	Add Connection. Click to launch the Connection wizard. You can find this icon in the Connections list toolbar and in the context menu when you right click on a site.
	Edit Connection. Click to change the connection parameters for the selected connection. You **cannot** edit an active connection. **Note**: If you change the connection name, when you save, Field Tools prompts you to decide whether you want to save the connection as a new connection under the new name **(Add new connection)**, or to just rename the existing connection **(Replace connection)**. 
	Connect. Click to activate the selected connection.
	Delete. Click to delete the selected connection or site. You can delete connections underneath a site. If you try to delete a site that has connections underneath it, Field Tools prompts you to confirm that you want to delete the site and its connections. It is not possible to delete a site with connections underneath it without also deleting the connections at the same time.
	Add Site. Click this context menu item to add a site underneath the currently selected site.
	Rename Site. Click this context menu item to call up the Modify Site dialog box and rename the currently selected site.

Icon	Description
⊞	Expand branch. Click to expand this branch of the Connections tree.
⊟	Hide branch. Click to hide the portion of the Connections tree underneath.
	Clear Connection Cache. If you encounter a problem with a connection, try disconnecting, then clear the connection cache, and reconnect. This may resolve the issue.
	Apply Pin. Click to display only the portion of the tree below the current position of the cursor. This is useful if you have a large Connections list tree with many items and you only want to see a portion of it.
	Remove Pin. Click to turn off the Apply Pin option and display the entire Connections list tree.

3.7 Starting an Existing Connection

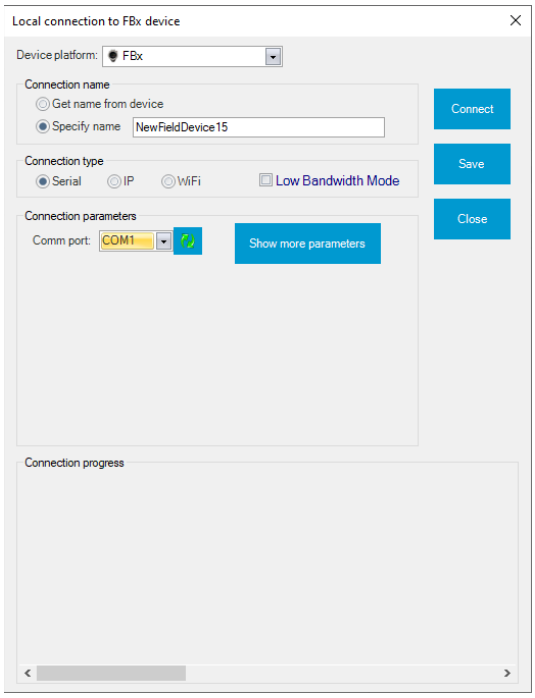
1. If you have previously established connections from this laptop, Field Tools displays them in the Connections list pane (see *Figure 3-8*).
2. To activate a connection, double-click on its icon and Field Tools activates that connection and automatically launches the appropriate configuration tool (ROCLINK, TechView, or FBxConnect). Alternatively, you can right-click on the connection name, and choose **Connect** in the context menu:



3.8 Creating a New Connection to a Device (Controller/Flow Computer)

1. If the connection for the controller/flow computer you want to communicate with already exists in the Connections list just double-click on it – you're done. If no previous connection exists to this device, go to the next step.
2. If you want to associate the device with a particular site, first click the site name in the Connections list. (If you don't want to choose a site at this time, you can skip that – the connection will automatically belong to the All Connections site.)
3. Click the **Add connection** icon in the Connections pane toolbar. If the icon is not visible (because no site is selected) click **Connections > Add connection** from the menu bar. Either way, the Connection wizard opens.

Figure 3-9. Connection Wizard



4. Select the type of device to which you want to connect in the **Device platform** field. The choices are: **FloBoss/ROC/DL8000, ControlWave/33xx**, or **FBx** (for the FB1000/FB2000 Series Flow Computers or FB3000 RTU).

Note
"33xx" refers to Network 3000 devices (for example, DPC 3330, DPC 3335, RTU 3310).

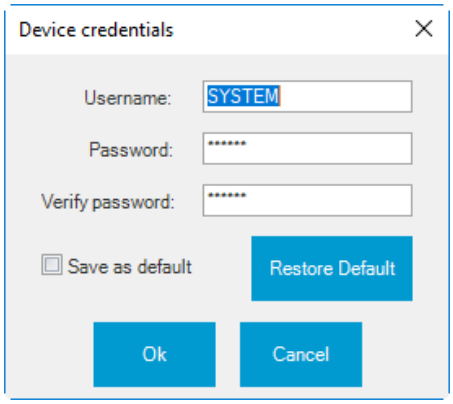
5. Enter the name of the field device in the **Specify name** field. For FBx devices, click the **Get name from device** button and Field Tools obtains the device name from the device (if it exists). If no name exists in the device, Field Tools uses the name "Default."

Note

Make connection names alpha-numeric; you can also include dashes, underscores, or spaces. Connection names cannot include special characters such as single or double quotation marks, commas, slashes, periods, colons, or asterisks. There is no pre-set maximum length for connection names.

6. For a ROC/FloBoss or ControlWave, if you want to define a default username/password combination for this device click **Device credentials** in the Connection page to open the Device credentials dialog box, enter a valid **Username** and **Password** combination for access to this controller/flow computer, and re-enter the password in the **Verify Password** field; this username/password combination will be used for this controller/flow computer throughout this Field Tools session. If you want to use this username/password combination as the default for this RTU for all subsequent connection sessions check the **Save as default** box. Click **OK** to finish and close the dialog box. Once you have saved the defaults, you can reload the default username and password when creating subsequent connections by clicking **Restore Default**.

Figure 3-10. Device credentials dialog box



Note

For FB1000/FB2000 Series Flow Computers or the FB3000 RTU, Field Tools uses the Field Tools Username and Password by default. If that username/password combination is not correct for the device, you can enter the correct ones, when prompted, and Field Tools then stores them with the connection details for that device. For that reason, there is no Device Credentials option for these devices.

7. Check **Low Bandwidth Mode** box in situations where communication infrastructure is slower and data cannot be moved as quickly as normal. Low bandwidth mode reduces

the amount of data transmitted by using a zipped solution file (*.ZSL) you have **previously** saved locally rather than uploading it again at the start of the connection. All process data is still transmitted normally. **Note**: Certain FBxConnect menu items are unavailable in low bandwidth mode.

Note

If you do not currently have a ZSL file for the connection on your PC but you want to use low bandwidth mode, you must connect to the device normally (without low bandwidth) and upload the solution running in the device to your PC. Then close the connection and create a new connection and select low bandwidth mode and when prompted, select the ZSL file you uploaded from the device.

8. Choose a **Connection type**. Choices include either **Serial**, **IP**, or **WiFi** (if you have an FB1000/FB2000 Flow Computer). Proceed to Step 9 for serial communication; skip to Step 10 for IP communication; skip to Step 11 for Wi-Fi communication.
9. For **serial** communication:

Figure 3-11. Serial Connection Settings – FB1000/FB2000 Series Flow Computers & FB3000 RTU

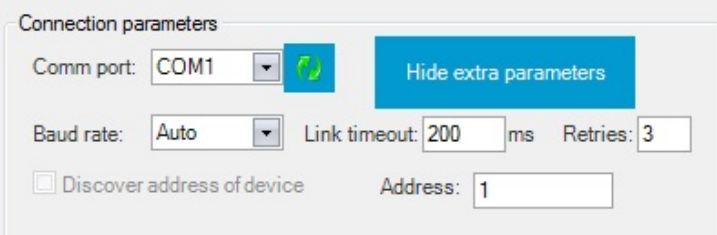


Figure 3-12. Serial Connection Settings – ROC/FloBoss

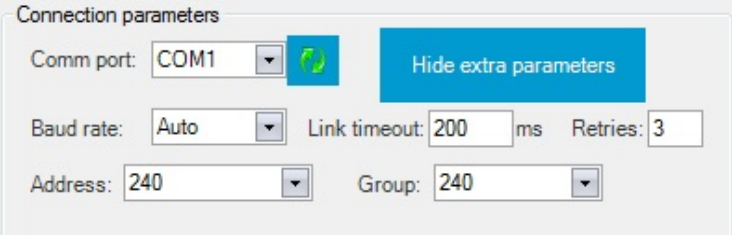
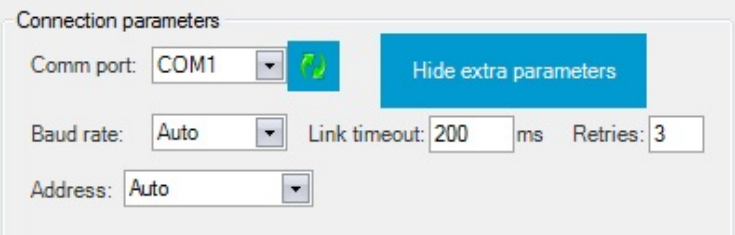


Figure 3-13. Serial Connection Settings – ControlWave/33xx



- Select the PC communication port in the **Comm port** drop down menu, otherwise leave it at the **Auto** default which causes the Connection wizard to cycle through the various ports until it finds the correct one. You can refresh the port selections by clicking the refresh ( ) button.
- The Wizard hides certain parameters to simplify configuration using default values; while this is useful in some situations, we recommend you enter the **Baud rate** and **Address** if you know them, rather than letting Field Tools attempt to auto-discover them. Most other parameters may be left at default values. Click **Show more parameters** to specify additional parameters as follows.
- If you know the baud rate for communicating with the field device, you can specify it in the **Baud rate** drop-down field. Otherwise use the **Auto** default which causes the Connection Wizard to cycle through the supported baud rates (9600, 19200, 38400, 57600, and 115200) until it finds the correct one.
- Optionally specify the **Link Timeout** for this connection. That value defines the period of time (in milliseconds) Field Tools waits for a response from the RTU or flow computer before declaring a communication failure. If you enter **0**, Field Tools uses a default of 200 milliseconds. Optionally, you can change the **Retries** parameter, which sets the total number of attempts to send a communication message before declaring an error.
- Specify the **Address** and the **Group** according to the following table:

Table 3-3. Specifying Address and Group for a Serial Connection

Device Type	Address	Group	Description
FB1000/FB2000 Series Flow Computers, FB3000 RTU	Default: 1 Range: 0-254	Not applicable	If you don't know the address, check the **Discover address of device** box.
ROC/FloBoss	Default: 240 Range: 0-255	Default: 240 Range: 0-255	Normally you should leave both of these at the default of 240 for local connections on the LOI port.
ControlWave	Default: Auto-detect Range: 1-127	Not applicable	If you are not connected to the local port or BSAP slave port (as specified in the ControlWave project or ACCOL load, respectively) but you know the BSAP local address for the field device, you can specify it in the **Address** drop-down field. Otherwise leave it at the **Auto** default which causes the

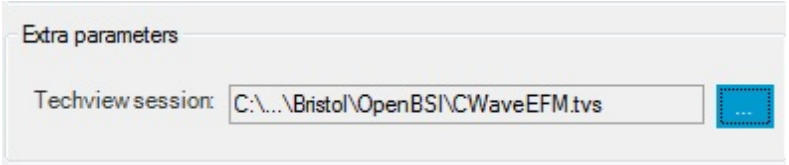
Device Type	Address	Group	Description
			Connection wizard to try each address in the range (1 to 127) until it finds the correct one.

- **For ROC/FloBoss only:** Under Extra Parameters use the **[...]** button to specify the ROC/FloBoss **.800 Configuration file** to associate it with this connection when ROCLINK launches. The .800 file must reside on this laptop PC.

Figure 3-14. Specifying the ROC Configuration File

- For **ControlWave/Network 3000 units only**: Under Extra Parameters use the **[...]** button to specify the **TechView session file** you want to use with this connection when TechView launches. The TechView session file must reside on this laptop PC.

Figure 3-15. Specifying the TechView Session File



Tips

- The **Auto** options are useful if you do not know the communication port, baud rate, or (for ControlWave/33xx only) the local address. If you leave all of these fields at **Auto**, however, it could take considerable time to establish the connection since the system must successively try each port, each of the five supported baud rates, and for ControlWave/33xx each of 127 possible local addresses.
- The maximum number of connection attempts if all fields are left at **Auto** for a ROC/FloBoss is (# of serial ports) * 5.
- The maximum number of connection attempts if all fields are left at **Auto** for a ControlWave/33xx is (# of serial ports) * 635.

When you've completed this step, go to Step12.

For **IP** communication:

Figure 3-16. IP Connection Settings – FB1000/FB2000 Series Flow Computers & FB3000 RTUs

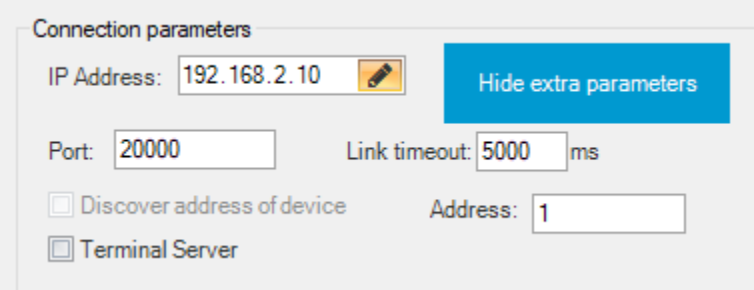


Figure 3-17. IP Connection Settings – ROC/FloBoss

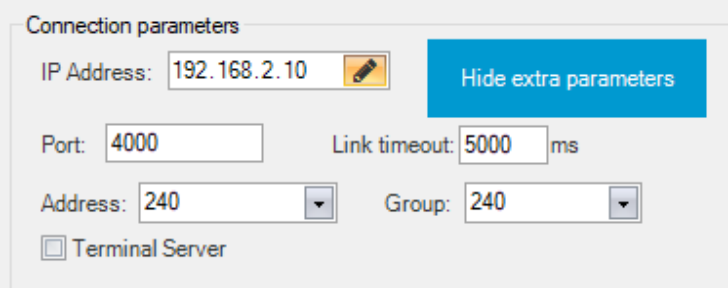
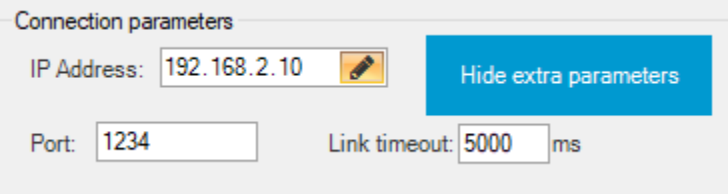


Figure 3-18. IP Connection Settings – ControlWave/33xx



Notes

- If you make an invalid entry in one of the Connection Wizard fields, a warning icon blinks, and you must correct the invalid entry.
- To view/modify hidden parameters, click **Show more parameters**.

- Specify the **IP address** of the RTU or flow computer. Position your cursor in the left-most digit position of the **IP address** field, enter the value for that position and use the tab key to move to the next position and so on until you enter the complete IP address. If you want to highlight the entire address to type over it, click the icon.
- Specify the port (IP socket number) used by this connection. The following table shows the default ports:

Table 3-4. Default Port (IP Socket Number) for connection

Device Type	Default Port (socket)
ROC/FloBoss	4000

Device Type	Default Port (socket)
FBx	20000
ControlWave	1234

Note

Field Tools only supports a **single** active IP connection to one ControlWave device at a time on a given default port. If more than one ControlWave device shares the same default port, only one of those ControlWave devices can have an active IP connection at any one time. If you attempt to start a second connection, Field Tools posts the message "An IP connection to a Bristol device already exists. Only one such connection is allowed." To make the new connection you must manually close down the existing active connection and then you can start the new connection.

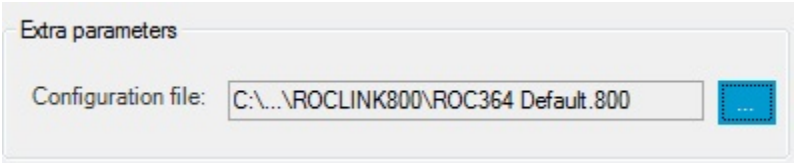
- Optionally specify the **Link Timeout** for this connection. That is the period of time (in milliseconds) Field Tools waits for a response from the RTU or flow computer before declaring a communication failure. If you enter **0** Field Tools uses a default of 5000 milliseconds.
- Specify the **Address** and **Group** according to the following table:

Table 3-5. Specifying Address and Group for an IP Connection

Device Type	Address	Group	Description
FBx	Default: 1 Range: 0-254	Default: 0 Range: 0 to 254	If you don't know the address, select the **Discover address of device** option.
ROC/FloBoss	Default: 240 Range: 0-255	Default: 240 Range: 0-255	Normally you should leave both of these at the default of 240 for local connections on the LOI port.
ControlWave	Not applicable	Not applicable	

- If the connection is through a terminal server, select the **Terminal Server** checkbox and set the **IP address** and **Port** (socket) to be the IP address and port of the terminal server. You should also select the **Terminal Server** checkbox if this device only supports a single IP connection on a port at one time, since Field Tools already uses one IP connection. For example, if you connect via Field Tools and then you activate another connection (such as ROCLINK on a ROC or FB107 device) if **Terminal Server** is unchecked, ROCLINK cannot communicate with the device.
- For ROC/FloBoss only: Under Extra parameters use the **[...]** button to specify the ROC/FloBoss **.800 Configuration file** in order to associate it with this connection when ROCLINK launches. The .800 file must reside on this laptop PC.

Figure 3-19. Specifying the ROC Configuration File



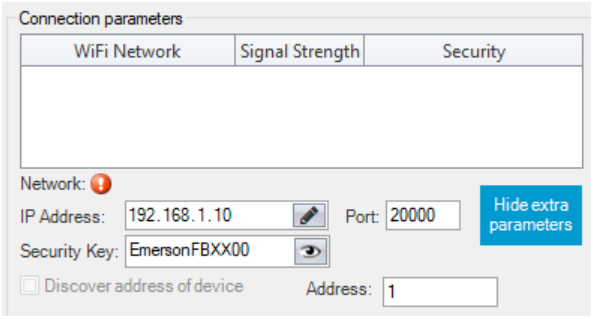
- For ControlWave/Network 3000 units only: Under Extra parameters use the [...] button to specify the **TechView session file** you want to use with this connection. The TechView session file must reside on this laptop PC.

Figure 3-20. Specifying the TechView Session File

When finished, skip to Step 12.

10. For **Wi-Fi** communication (FB1000/FB2000 Flow Computers only):

Figure 3-21. WiFi Connection Parameters

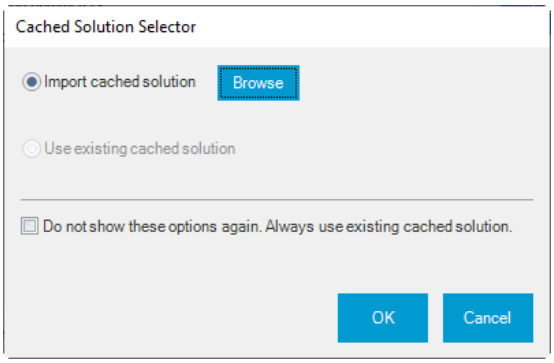


- Wi-Fi networks that your laptop detects are shown onscreen. For this type of connection to work, the laptop must first detect the **WiFi Network** to which the device belongs. The default WiFi Network follows the format FB*xxxx_serialnumber*.
- Specify the **IP address** of the RTU or flow computer as described in *Table 3-5*. Position your cursor in the left-most digit position of the IP address field, enter the value for that position and use the tab key to move to the next position and so on until you enter the complete IP address. If you want to highlight the entire address to type over it, click the icon. The default IP address for FB1000/FB2000 Flow Computers when they ship from the factory is **192.168.1.10**. If you do not know the address, check the **Discover address of device** box.
- Specify the **Port** (IP socket number) of the RTU or flow computer. The default port is 20000.

- Enter the **Security Key** for the wireless network. To see it as you type it, click the eyeball icon. The default security key for FB1000/FB2000 Flow Computers when they ship from the factory is **EmersonFBXX00**. Be sure to change it to something only your organization knows when you place the device in service.
- If the connection is through a terminal server, select the **Terminal Server** checkbox and set the **IP address** and **Port** (socket) to be the IP address and port of the terminal server. You should also select the **Terminal Server** checkbox if this device only supports a single IP connection on a port at one time, since Field Tools already uses one IP connection. For example, if you connect via Field Tools and then you activate another connection (such as ROCLINK on a ROC or FB107 device) if **Terminal Server** is unchecked, ROCLINK cannot communicate with the device.

If you don't want to activate the connection right now, but just want to save your configuration entries, you can click **Save**; this saves your entries in the Connection list, and exits the wizard. If you want to connect right now, click **Connect** and the wizard attempts to establish the connection.

Note



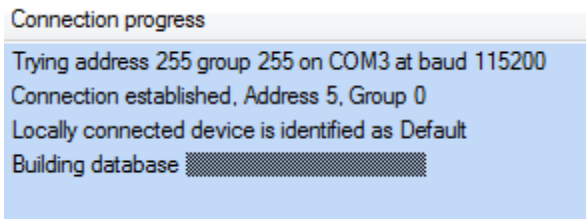
If this is an FB3000 RTU or an FB1000/FB2000 series flow computer for which you selected **Low Bandwidth Mode** and Field Tools prompts you regarding cached solutions, you can do one of two things:

1. If you previously specified the zipped solution file to use, you can select **Use existing cached solution** to proceed. Optionally, you additionally may also select **Do not show these options again. Always use cached solution** and going forward, Field Tools will always use the cached solution for this particular connection.
2. If, however, **Use existing cached solution** is grayed out, and **Import cached solution** is already chosen, it means you have not specified the zipped solution (*.ZSL) file yet and you must do so now to proceed. Click **Browse** and navigate to the correct solution file. If when you select, a mismatch is reported between the solution currently in the FB3000, and the cached solution, we recommend you exit **Low Bandwidth Mode** and

recreate the connection at the regular bandwidth speed (no low bandwidth) and upload the solution running in the FB3000 to your PC, then select that newly uploaded file as your cached solution so that the solutions in both locations match. Alternatively, you can proceed with the mismatch but data from some object instances may not be available.

Field Tools reports details of the connection progress in the Connection progress pane.

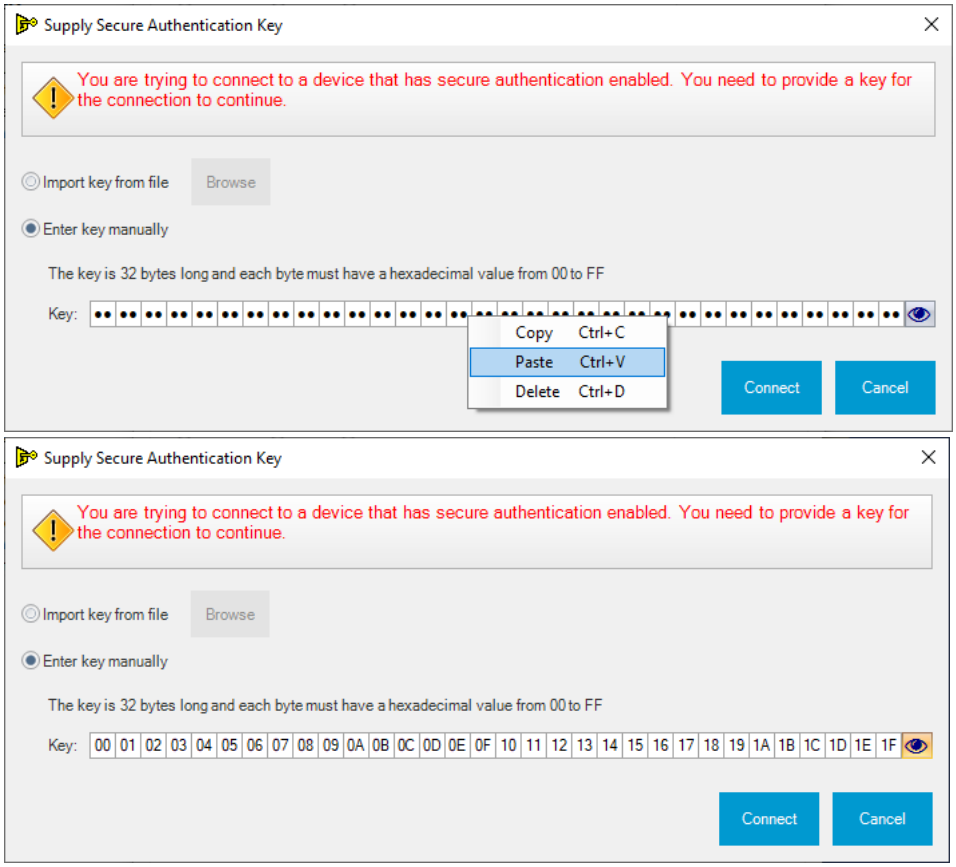
Figure 3-22. Connection in Progress



If the connection is successful, the Active connection pane of the Field Tools main screen shows an icon for the newly connected device and its toolbar populates with icons appropriate to the device type.

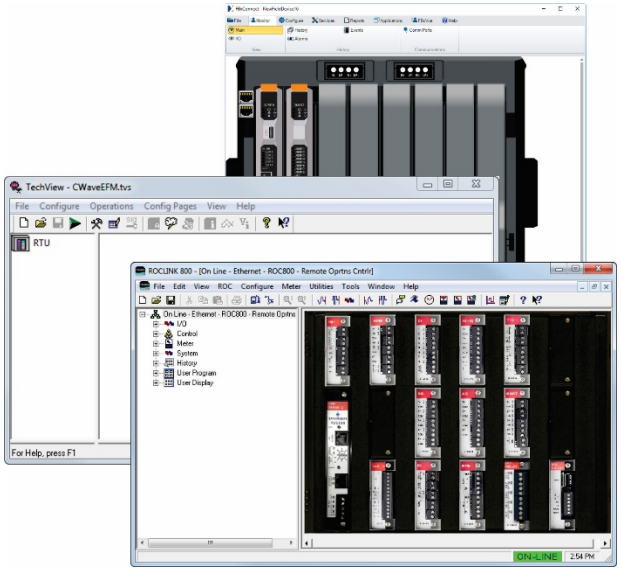
If the device has SAv5 secure authentication enabled, and Field Tools does not have the key, you must provide it. You can import the key by clicking **Import key from file** and **Browse** for the ZCF file (zipped connection file) containing the key; select the file and provide the file password when prompted. Alternatively, you can type in the key manually, or right-click in the field and paste the key if you copied it from another file. To see the key, click the eye icon . In either case, once you provide the key, click **Connect**.

Figure 3-23. Supply Secure Authentication Key



In addition, Field Tools automatically launches the configuration tool (ROCLINK, TechView, or FBxConnect) appropriate for the device platform.

Figure 3-24. RTU Configuration Tools – FBxConnect, TechView, ROCLINK

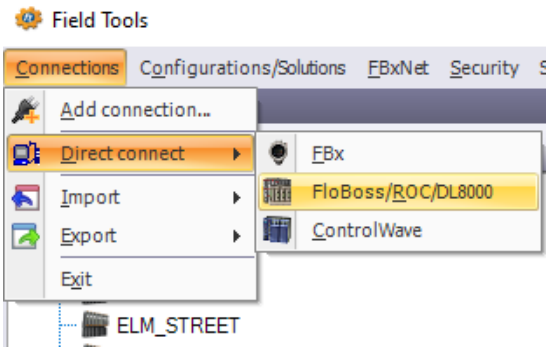


3.9 Making a Direct Connection

The term **direct connection** refers to a direct **serial** connection to a device.

Click **Connections > Direct Connect** and select the type of device from the options presented. Field Tools attempts to establish a local serial connection by sequentially trying each serial port using the default settings for that device type.

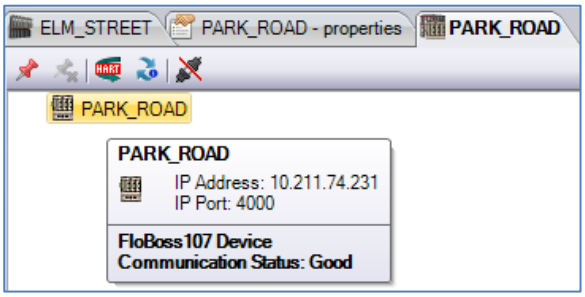
Figure 3-25. Direct Connection



3.10 Active Connection pane

The Active Connection pane shows details for the currently active connection and allows you to launch certain other tools for use with the device(s).

Figure 3-26. Active Connection Pane



The Active Connection pane includes a separate tab for each active connection. Click on the tab to see details about a particular connection.

To see information about a device (RTU, flow computer), move the cursor over that device and a small status box opens that shows details based on the type of device. This could include its address, or certain status information.

To disconnect an active connection, right click on the icon for the device and choose **Disconnect**. To disconnect all connections, click **Connections > Close all connections**.

Table 3-6. Icons Used in Active Connection Pane

Icon	Description
	Identifies a previously configured connection to an FB1100 Flow Computer. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Identifies a previously configured connection to an FB1200 Flow Computer. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Identifies a previously configured connection to an FB2100 Flow Computer. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Identifies a previously configured connection to an FB2200 Flow Computer. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	Identifies a previously configured connection to an FB3000 RTU. The name of the device appears next to the icon. Double-click the icon to re-start the connection.
	ROC or FloBoss controller connection.
	ControlWave or Network 3000 controller connection.
	Device icon(s). **Note**: The devices' device descriptor (DD) files provide the device icons. Consequently, depending upon the type of HART or WirelessHART device, you may see different device icons.
	Expand branch. Click this to expand the branch of the tree.
	Hide branch. Click this to hide the portion of the tree underneath.
	Apply Pin. Click to display only the portion of the tree below the cursor's current position. This is useful if you have a large tree with many items and you want to see only a portion of the tree.
	Remove Pin. Click to turn off the Apply Pin option and display the entire tree.
	Failure. Indicates some sort of failure associated with this device.
	Terminate Connection. Click to shut down the active connection in this device tab. Field Tools prompts you to confirm this action.

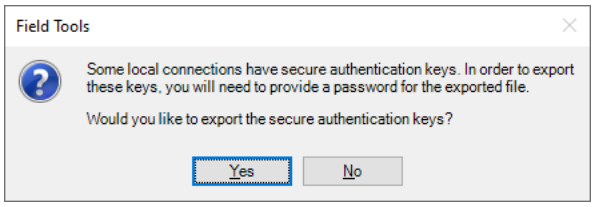
3.11 Exporting/ Importing Connections

If you have configured a group of connections, you can save the connection configuration details in a file. You can then transfer that file to another PC/laptop running Field Tools, so that you don't need to re-create the connections on that PC, you can just click on them to start the connection.

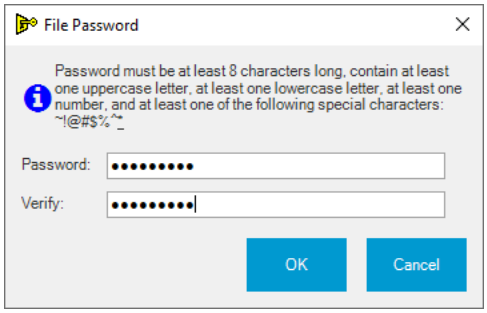
3.11.1 Exporting Connections

1. Click **Connections > Export > Export to file**.
2. Specify a name for the file. Its extension must be ZCF (for zipped connection file).

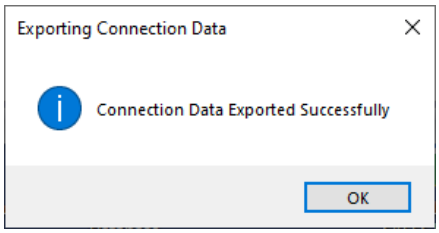
   If one or more of the connections include DNP3 security keys for communication with DNP3 SAv5 enabled FB1000/FB2000/FB3000 devices, Field Tools asks whether you want export the keys. If you choose **No**, skip to step 5. If you choose **Yes**, proceed to step 3.



3. To export DNP3 security keys, you must assign a password to the file. Enter it in the **Password** and **Verify** fields and click **OK**.

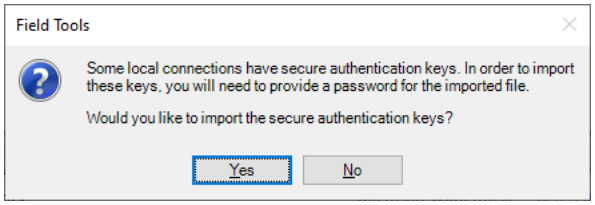


4. Field Tools exports the file. Click **OK**. You can import this file on other Field Tools PCs to bring in the connections.

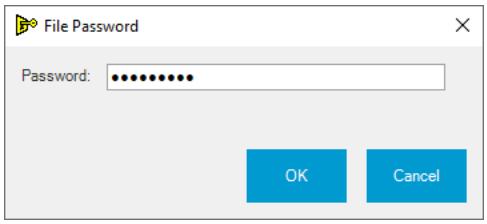


3.11.2 Importing Connections

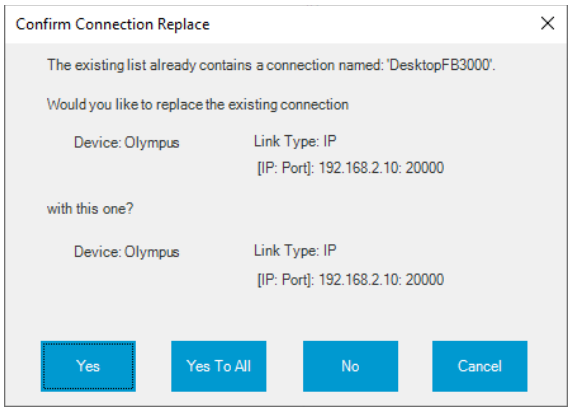
1. Click **Connections > Import > Import from file**.
2. Navigate to the file that contains the connection information and click **Open**.
3. If the connection file includes secure authentication keys, Field Tools prompts you to confirm whether you want to import the keys. If you click **Yes**, you must provide the password for the connection file. If you choose **No**, skip to step 5.



4. When prompted, enter the password for the connection file.



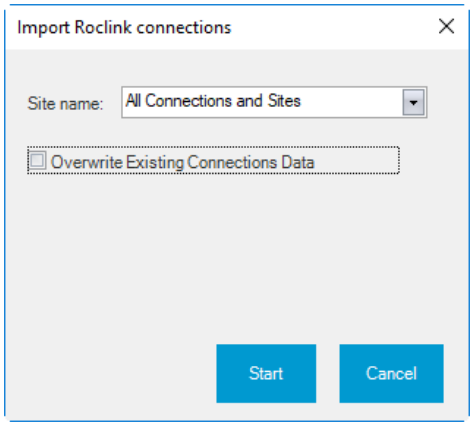
5. If there are duplicate connection names, Field Tools prompts you to confirm that you want to replace the the connection details for connections that already exist.



3.11.3 Importing ROCLINK Connections

If you had previously created connections within ROCLINK without Field Tools, you can import those connections into Field Tools.

1. Click **Connections > Import > Connections from ROCLINK**. The Import ROCLINK connections dialog box opens.



2. In the Import ROCLINK Connections dialog box, choose the site name which contains the ROCLINK connections you want to import.
3. If you want to overwrite existing ROCLINK connections, select the **Overwrite Existing Connections Data** option.
4. Click **Start** to import the connections.

3.12 Settings

Click **Settings** in the menu bar to open the Settings dialog box. The Settings dialog box lets you pre-configure certain items for FBxConnect or Field Tools.

General

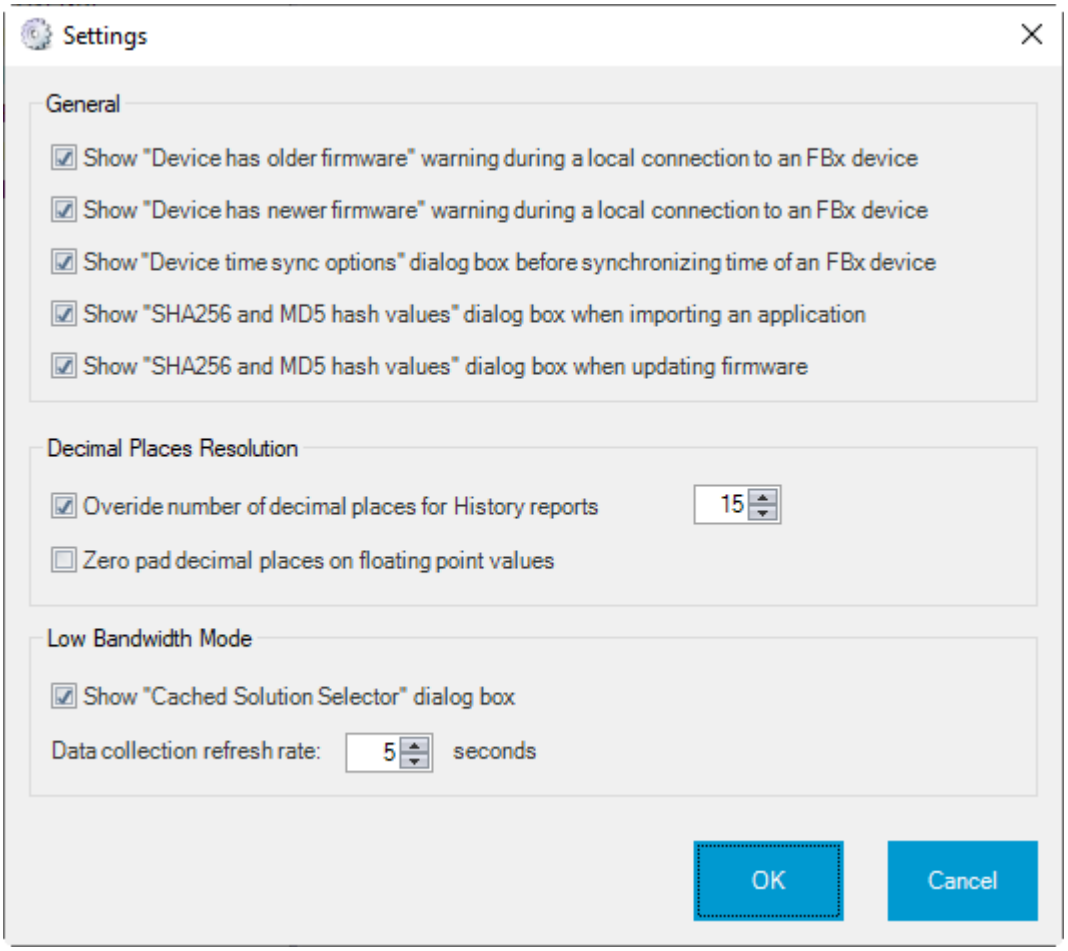
If you want to see firmware revision warnings when you connect to an FB1000/FB2000 Flow computer or FB3000 RTU, ensure the **Show "Device has older firmware"** and "**Show Đevice has newer firmware"** check boxes are selected.

If you want the system to prompt operators whether to override the time zone of an FBx device when a time synchronization message comes in, select the Show **"Override device time zone" dialog box before synchronizing time of an FBx device**.

Select **Show "SHA256 and MD5 hash values" when importing an application** if you want to compare those values with the original published values for the application available on Guardian. If the hash values displayed on import do not match the hash values on Guardian, you know the application has been modified from its original released version. This could indicate malicious or unauthorized modifications to the code.

Select **Show "SHA256 and MD5 hash values" when updating firmware** if you want to compare those values with the original published values for the firmware available on Guardian. If the hash values displayed when updating firmware do not match the hash values on Guardian, you know the firmware has been modified from its original released version. This could indicate malicious or unauthorized modifications to the code.

Figure 3-27. Settings dialog box



Decimal Places Resolution

The number of decimal places to the right of the decimal point for values displayed on a history or EFM report is normally configured on the Engineering Units display in FBxConnect. You can override that resolution by checking the **Override number of decimal places for History reports** then specifying a different resolution for this Field Tools connection, from 1 to 15 decimal places. If you uncheck this box, the value stored is zero, and there is no override during this Field Tools connection.

If you want to pad decimal places on the end of floating-point values, check the **Zero pad decimal places on floating point values**. For example, if the number of decimal places to the right of the decimal point is configured as 10, and the value to display is 28.4375, checking this box results in 28.4375000000 being displayed. This feature allows columns of figures in history or EFM reports to line up uniformly.

Low Bandwidth Mode

Low bandwidth mode is used in situations where communication infrastructure is slower and data cannot be moved as quickly as normal. Low bandwidth mode reduces the

amount of data transmitted by saving certain data structures from the solution in cached memory to avoid having to resend them. All process data is still transmitted normally.

Click **Show "Cached Solution Selector" dialog box** if you want to specify the cached solution file used for this connection.

Specify the desired **Data Collection Refresh Rate** in seconds.

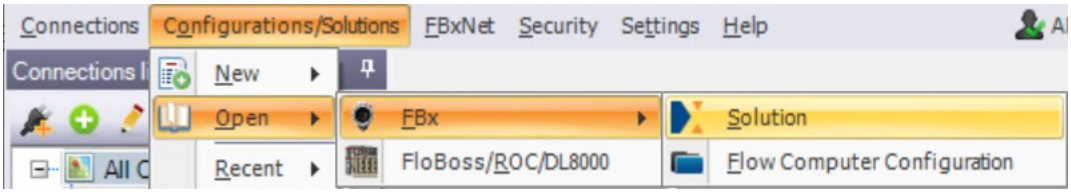
Click **OK** to save your changes to the settings.

3.13 Offline Configurations/Solutions Menu

The Configurations/Solutions menu bar item lets you view/create solution files for an FB1000/FB2000 Series Flow Computer or FB3000 Series RTU offline– without an active connection to the device. You can also create/view a configuration file for a ROC/DL8000 or FloBoss device.

For a ROC or FloBoss device, see the ROCLINK online help for more information.

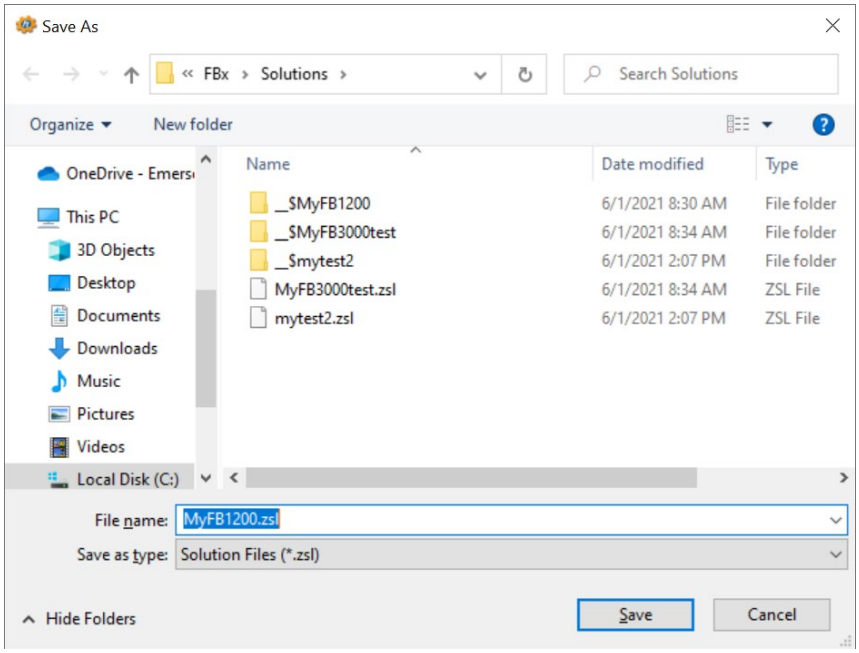
Figure 3-28. Offline Configurations



3.13.1 Creating a New Solution File for a Flow Computer (FB1000/FB2000 Series)

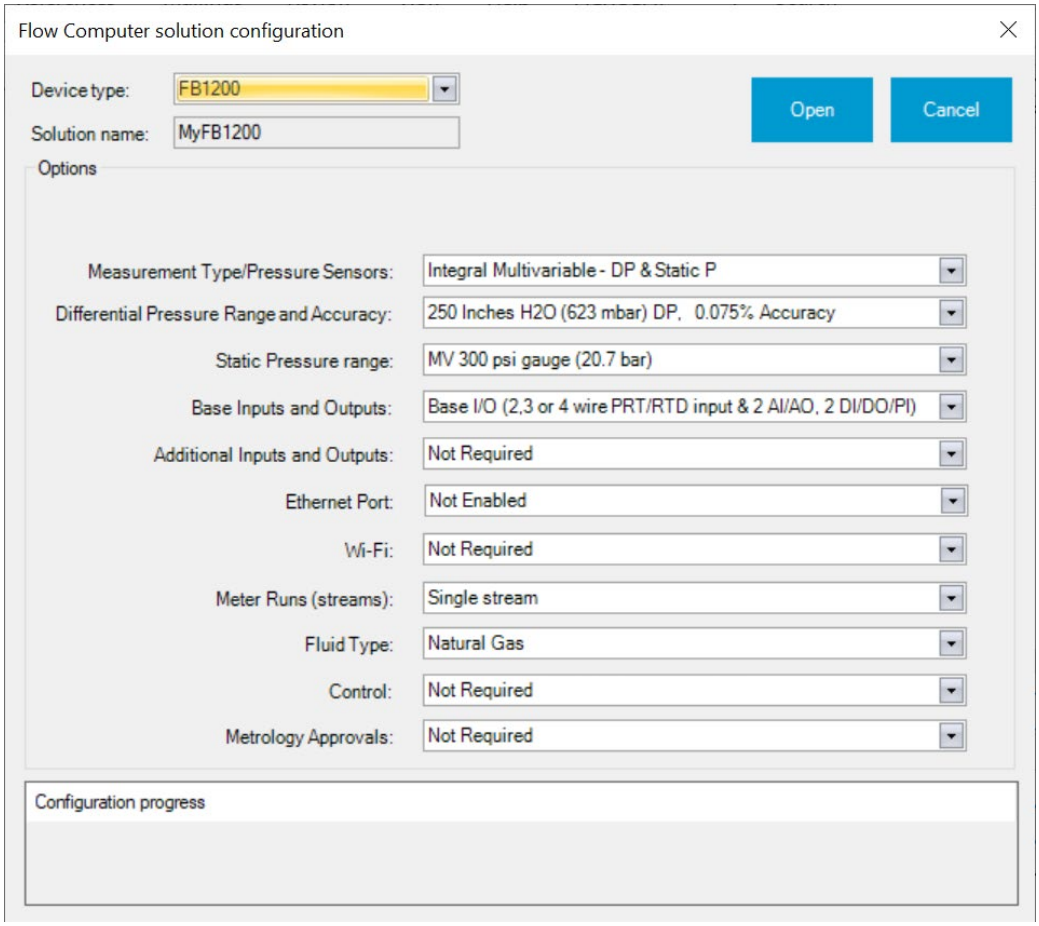
1. Click **Configurations/Solutions > New > FBx > Flow Computer**.
2. Specify a name for the solution file (*.zsl) and click **Save**.

Figure 3-29. Specifying the name of the solution file



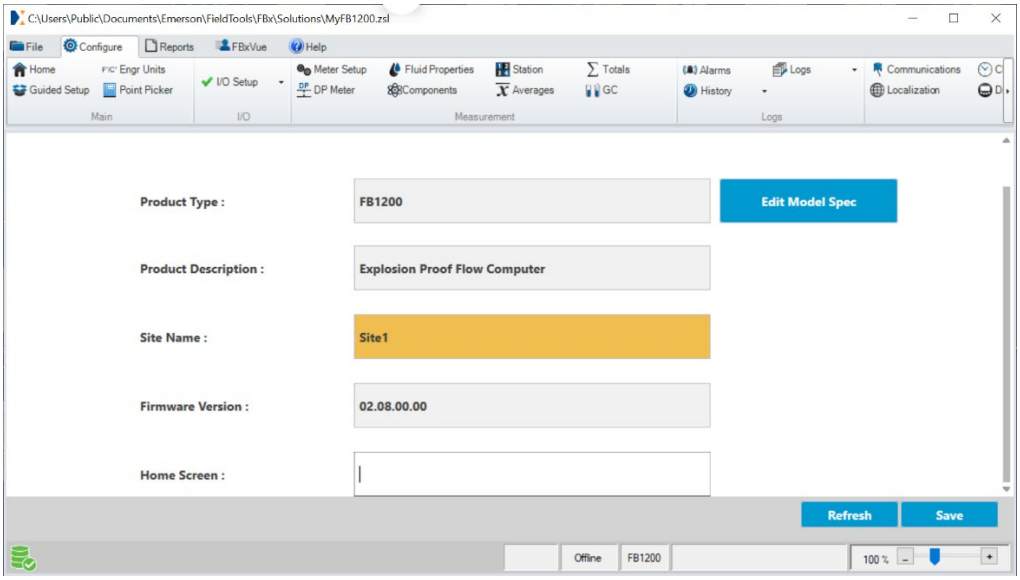
3. Select the correct **Device type** for your flow computer, and then select the correct configuration characteristics for sensor types, ranges, and so on. Finally, click **Open**.

Figure 3-30. Specifying the characteristics of the solution



4. You can now optionally configure various features through the FBxConnect toolbar. (See *D301850X012 - FBxConnect Configuration Software User Manual for the FB1000-FB2000 Series* for details on configuring features in FBxConnect.) You can specify an associated **Site** for the flow computer. If you created a custom FBxVue display for the flow computer which you would like to appear when starting an FBxConnect connection instead of the default, specify it in the **Home screen** field. Optionally you can go back to change the characteristics by clicking **Edit Model Spec**.
5. When you are finished with all entries, click **Save** to save your offline solution file. At a later time, you can download the solution file to the flow computer.

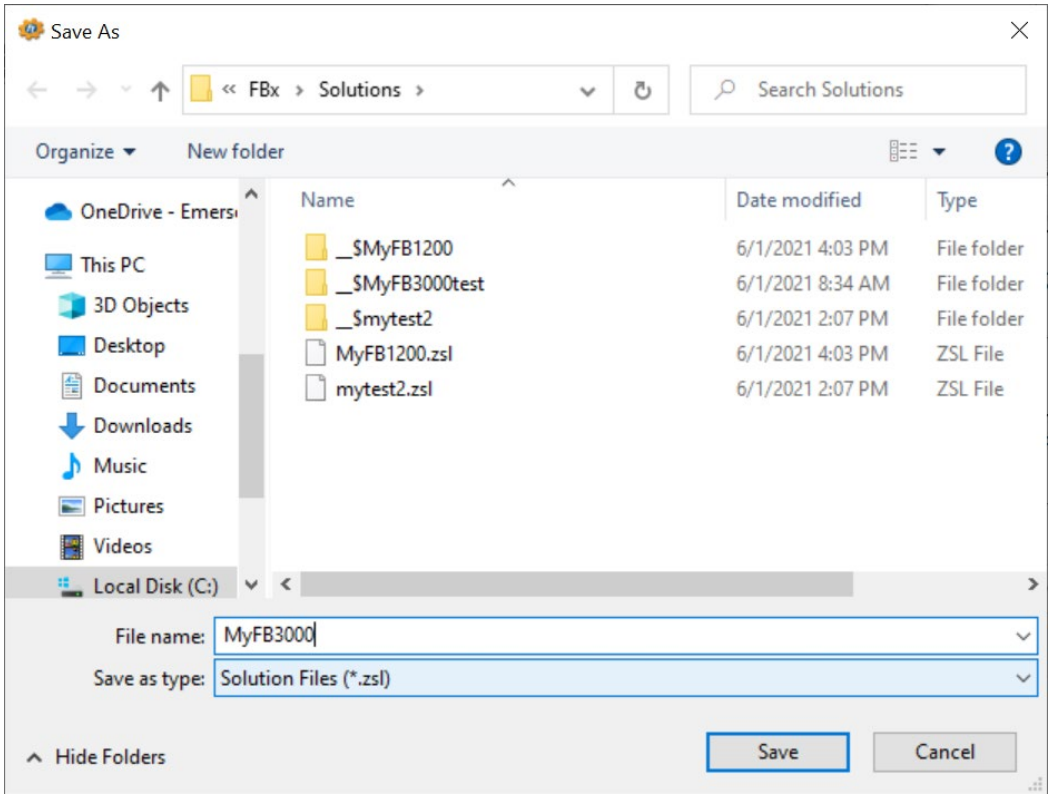
Figure 3-31. Saving the Offline Solution File



3.13.2 Creating a New Solution File for an RTU

1. Click **Configurations/Solutions > New > FBx > RTU**.
2. Specify a name for the solution file (*.zsl) and click **Save**.

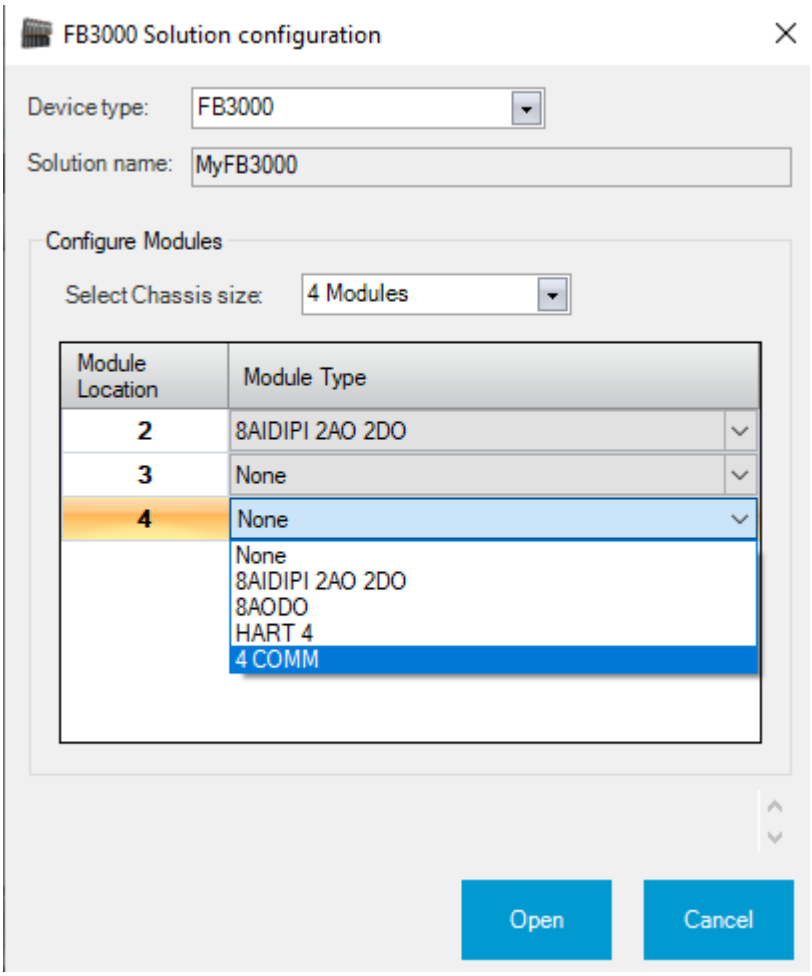
Figure 3-32. Specifying the name of the solution file



3. First, select the **Device type**. If this is an FB3000 RTU with the 3CPU16 CPU installed, choose **FB3000**. If this is an FBxRemote I/O rack with the 3IOCPU installed, choose **FBRIO**.

4. Depending upon whether or not your FB3000 includes one or more extension chassis, choose the appropriate number of chassis in the **Select Chassis size** field. You can then select the type of module in each slot using the **Module Type** selection box. Finally, click **Open**. **Note**: Slot 1 is always reserved for the CPU module so you cannot make selections for that **Module Location**.

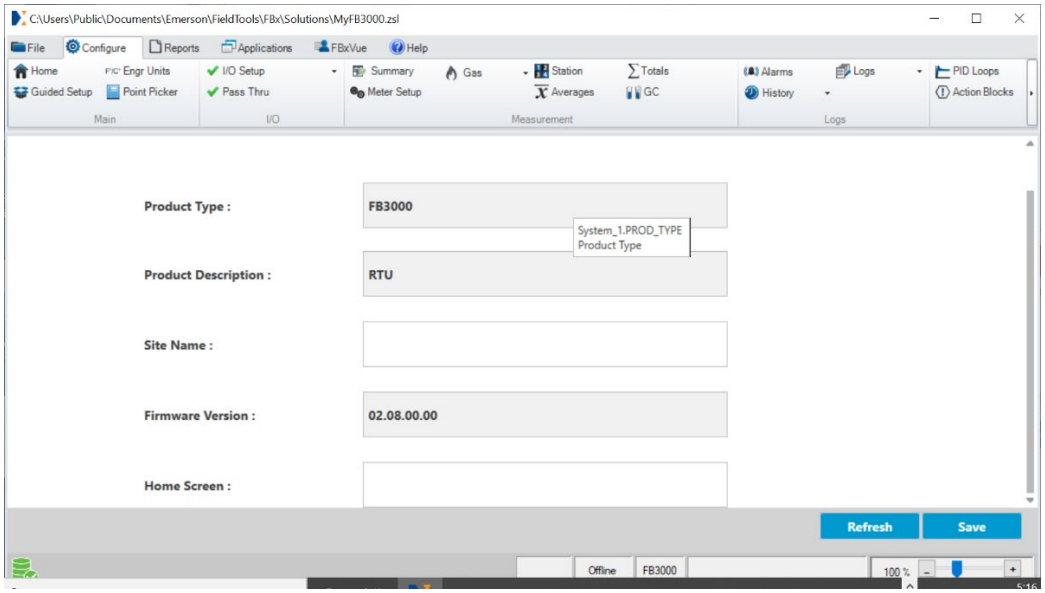
Figure 3-33. Specifying Modules for the FB3000



5. You can now optionally configure various features through the FBxConnect toolbar. (See *D301882X012 - FBxConnect Configuration Software User Manual for the FB3000* for details on configuring features in FBxConnect.) You can specify an associated **Site** for the RTU. If you created a custom FBxVue display for the RTU which you would like to appear when starting an FBxConnect connection instead of the default, specify it in the **Home screen** field.

When you are finished with any entries, click **Save** to save your offline solution file. At a later time, you can download the solution file to the FB3000.

Figure 3-34. Saving the Offline Solution File



3.13.3 Opening an existing Solution File

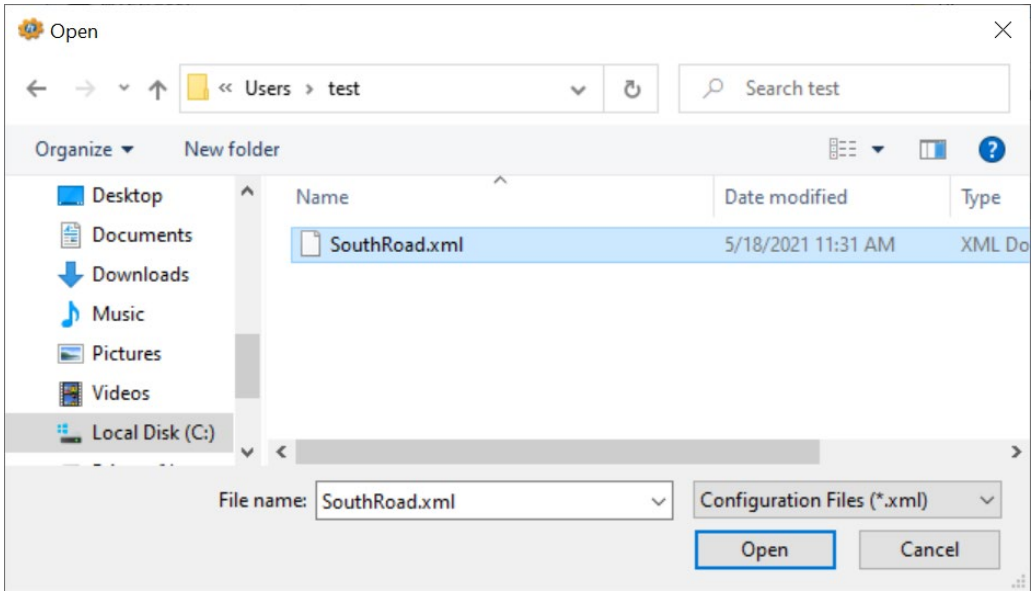
1. Click **Configurations/Solutions > Open > FBx > Solution**.
2. Select the solution file (*.zsl) and click **Open**. You can now edit the solution as desired.

3.13.4 Converting a Flow Computer Configuration (*.xml) to a Solution File

Going forward, Field Tools requires FB1000/FB2000 Series flow computers use solution files **similar** to those used in the FB3000. You can convert an existing flow computer configuration file to a solution file. The advantage of using solution files is they allow you to download an FBxVue display to the flow computer and they also allow easier reuse of user data descriptions and the DNP3 map file, etc. instead of only the configuration details.

1. Click **Configurations/Solutions > Open > FBx > Flow Computer Configuration**.
2. Navigate to the xml file and click **Open**.

Figure 3-35. Navigating to the Configuration (xml) File

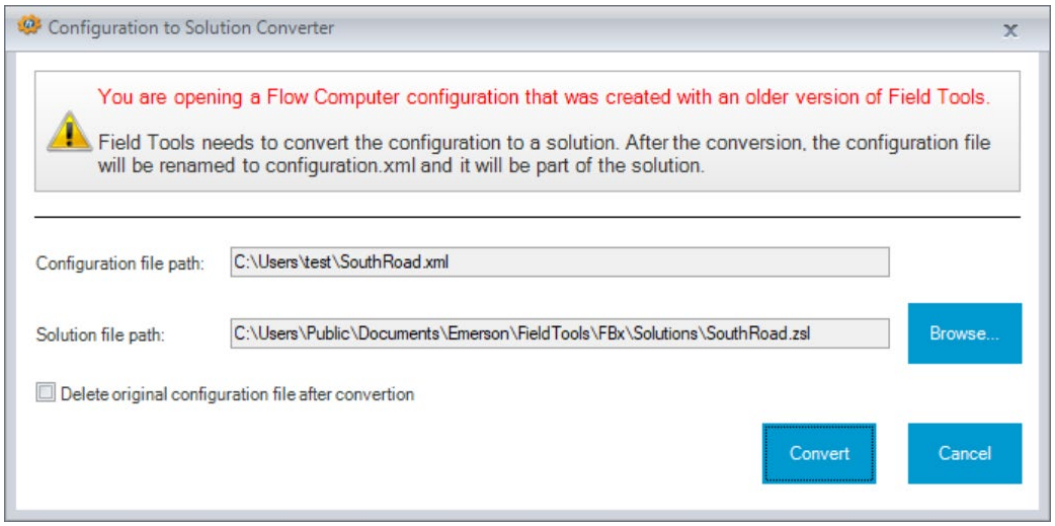


3. Field Tools prompts you to convert the XML file to a solution file.

   You can optionally specify that you want Field Tools to delete the original XML after conversion by clicking **Delete original configuration file after conversion**. If you don't select that, the original file remains unchanged after the conversion.

   Click **Convert** to generate a solution file from the XML file.

Figure 3-36. Converting a Configuration XML file to a Solution File



3.14 Launching a Script from Within Field Tools

Note

For information on running a special script to collect diagnostic information from FB1000/FB2000/FB3000 series devices and store it in a support bundle which you can forward to our technical support group for analysis, see *Section A.1* in *Appendix A*.

You can launch a script you created with FBx Script Developer from within the Field Tools tree. (See the *FBx Script Developer User Manual (D301953X012)* for details on creating scripts.)

1. Right-click on the device on which you want to run the script, and select **Run Script**. (Alternatively, you can single click on the device to highlight it and then click the **Run Script** button.)

Note

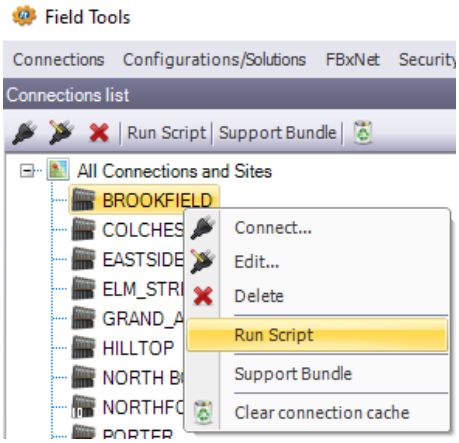
If a serial connection has already been established, the **Run Script** and **Support Bundle** context menu items are disabled.

For an active IP connection, these context menu items are enabled.

Note

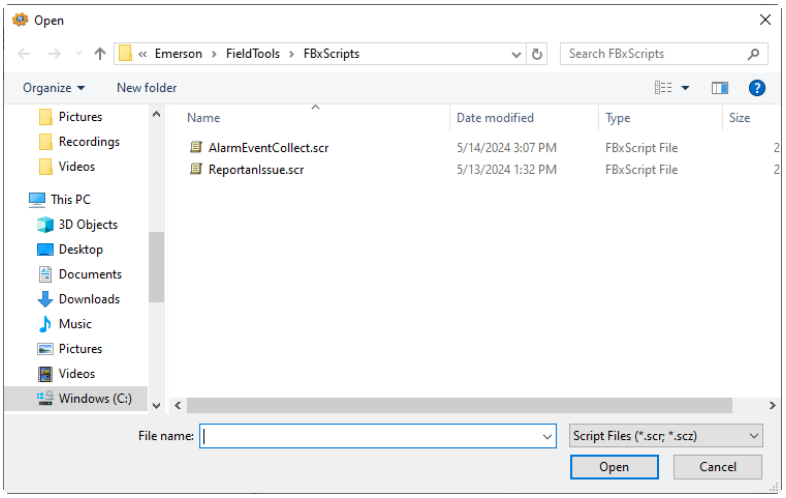
If your script includes a “CONNECT {$A1}” command, the connection name is automatically passed to the script to fill in the A1 parameter.

Figure 3-37. Launching a Script within Field Tools



2. Select the script file you want to run.

Figure 3-38. Selecting a Script File



3. Click **Open** and FBxScriptRunner launches the script.

Chapter 4. FBxNet™

You launch FBxNet from within Field Tools.

4.1 What is FBxNet?

FBxNet is a peer-to-peer communication network for exchanging data between Emerson RTUs and flow computers over Ethernet connections.

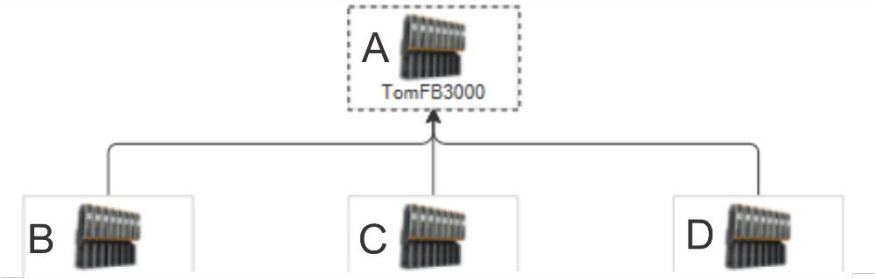
A **subscriber** device in the network must be an Emerson FB3000 RTU with a firmware revision that supports FBxNet.

Publisher devices in the network can be any mixture of Emerson FB3000 RTUs, Emerson FB1200 Flow Computers, or Emerson FB2200 Flow Computers with firmware revisions which support FBxNet.

FBxNet transfers data between the subscriber and its publishers according to **parameter** definitions. Each parameter definition specifies a correspondence between a tag in the publisher and a tag in the subscriber. These two tags exchange data using FBxNet.

The graphic, below, shows a peer-to-peer network with a single subscriber (A) and three publishers (B, C, and D).

Figure 4-1. FBxNet – Subscriber and Publisher Devices



4.2 Licensing FBxNet

If you start Field Tools and do not see the **FBxNet** menu bar item, it means FBxNet is not currently licensed on your PC. When you purchased FBxNet, you should have received a **License Id** and **Password** to access the licensing website and license FBxNet on your PC.

Note
If you install Field Tools on a server, you should purchase a Multi-User Server license so multiple users can log in from remote PCs and use FBxNet.

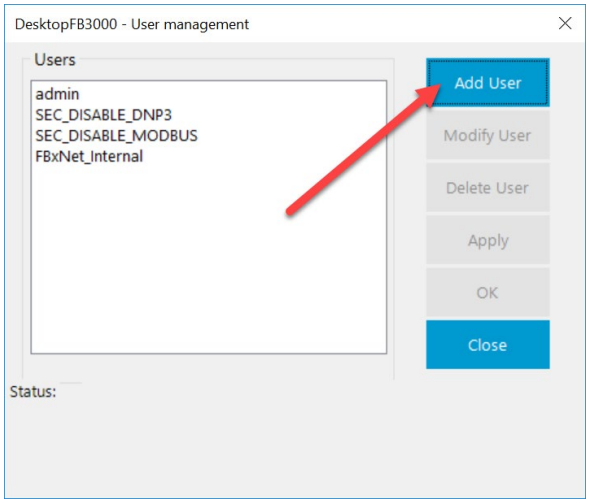
To License FBxNet, from the Field Tools menu bar click **Help> Licensing>Field Tools Licensing** and follow the instructions in *Chapter 6*.

4.3 How do I configure FBxNet?

FBxNet configuration is a multi-step process:

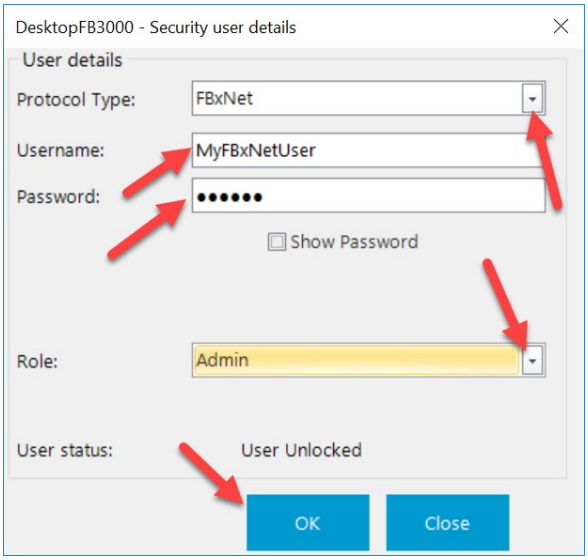
1. In FBxConnect, click **Configure > FBxNet** and use the FBxNet display to configure one or more Ethernet ports on your FB3000 Subscriber device to use FBxNet. (See the FBxConnect online help for details). If you do not see the FBxNet option, it means FBxNet is not licensed for that device. (See *Licensing FBxNet*.)
2. Each device in your FBxNet network must have an identical user with the same login credentials. In FBxConnect, click **Services > User Management**.
3. In the User Management screen, click **Add User**.

Figure 4-2. Adding a User



4. For the user details:
   - Select FBxNet as the Protocol Type.
   - Specify a **Username** and **Password** combination. All FBxNet users you define on your network must share this same username/password combination.
   - Specify the **Role** for the user; **Admin** provides the most access; **Auditor** provides the least access.

Figure 4-3. Defining User Details



5. Click **OK** to save your changes, and **OK** to exit the User Management screen.
6. Launch Field Tools and start FBxNet. (See *Starting FBxNet*.)
7. Create one or more sites and specify an RTU to hold CSV files for the site. (Sites are just a way to organize subscribers.) (See *Creating a Site*.)
8. Specify one or more subscribers for each site. The subscriber is an FB3000. (See *Creating a Subscriber Directly in FBxNet*.)
9. Specify one or more publishers for each subscriber. A publisher is an FB1200, FB2200, or FB3000. (See *Adding a Publisher*.)
10. Specify parameters which define which data should be transferred between the publisher(s) and the subscriber. (See *Adding a New Parameter*.)
11. Download the CSV file to the subscriber device. (See *Downloading CSV Files*.)

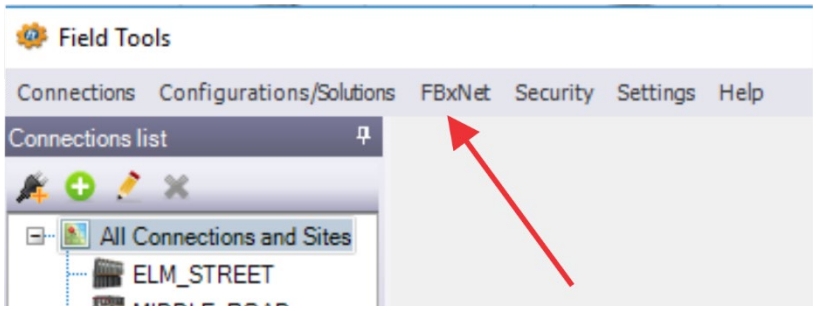
4.4 Starting FBxNet

Note

Unless you manually create them ahead of time, the first time you start FBxNet it notifies you that it cannot find subscriber CSV files. You can create them directly in FBxNet or create them manually in Excel or a text editor.

1. Launch Field Tools.
2. From the Field Tools menu bar, click **FBxNet.**

Figure 4-4. Starting FBxNet

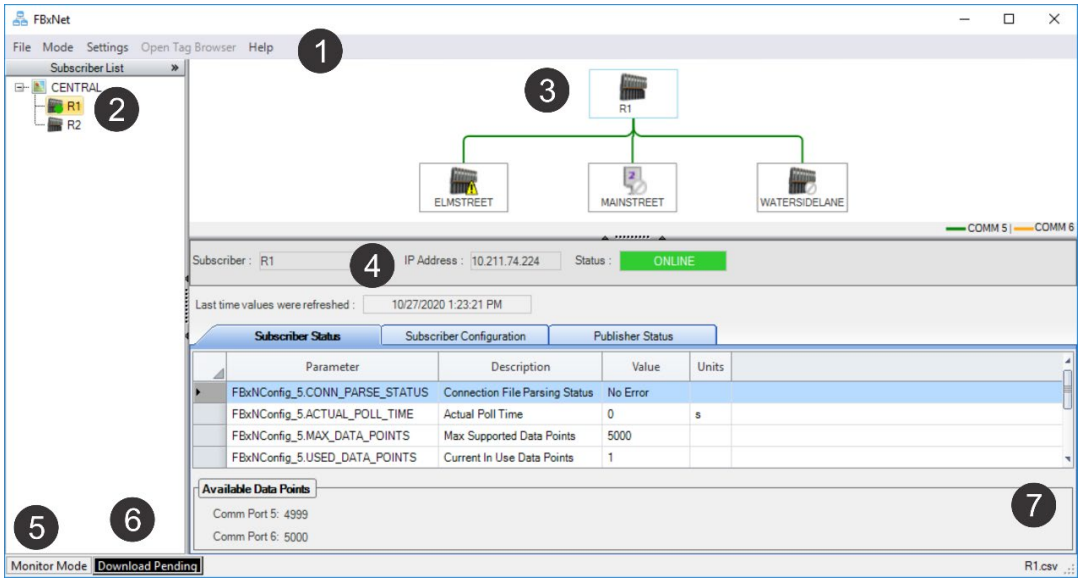


Important

If the FBxNet item is not visible in the menu bar of Field Tools, it means you have not licensed FBxNet on this PC. See *Licensing FBxNet*.

3. FBxNet opens and reads the subscriber CSV file(s) and based on them, creates a list of the subscribers, and generates a graphical network tree for the selected subscriber and its associated publishers. FBxNet displays the lines connecting the publishers in colors to differentiate between the communication ports used.

Figure 4-5. FBx Main Screen



1 Menu Bar

2 Subscriber List (the subscriber icon includes a green dot if the connection is active)

3 Network Pane (use mouse wheel to zoom in/zoom out)

4 Status Pane

5 Mode Indicator (Monitor or Configuration)

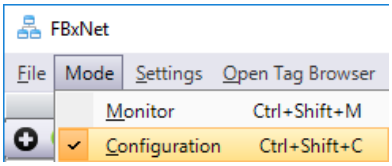
6 Messages

7 Name of current CSV file

4. In the FBxNet Subscriber List, click the name of the subscriber you want to view; the Network pane updates with a graphical tree for that subscriber and its publishers.

4.5 Switching Between Monitor and Configuration Mode

FBxNet displays the current mode in the Mode Indicator at the lower left of the screen. (See Item 5 in *Figure 4-12*.) You can also see the currently active mode by clicking **Mode** in the menu bar; FBxNet shows a check next to the current mode of operation.



The two FBxNet modes are:

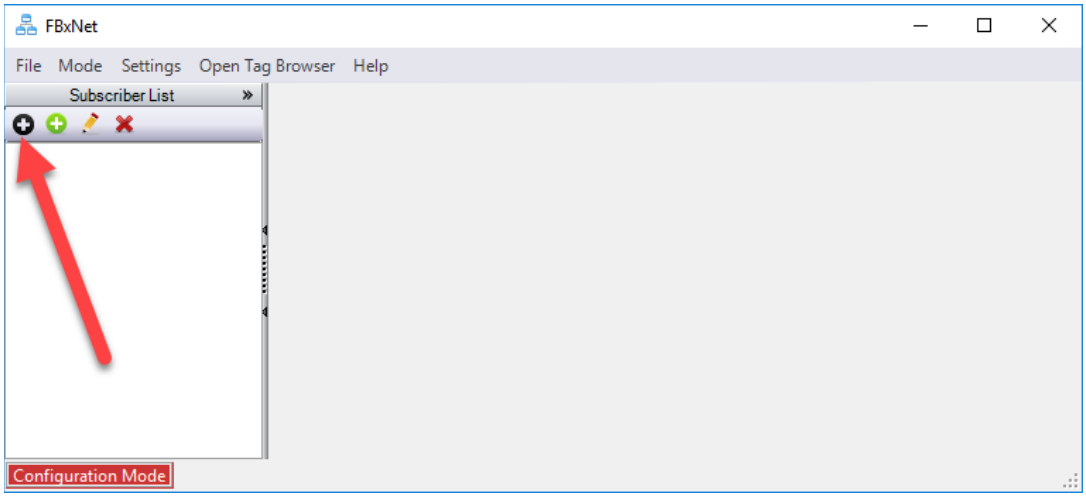
- Monitor Mode lets you view data and parameters for each subscriber and publisher. You can also change FBxNet subscriber configuration parameters. To open Monitor Mode, click **Mode > Monitor**.
- Configuration Mode lets you edit/change publisher and subscriber tag names for a particular subscriber. To open Configuration Mode, click **Mode > Configuration**.

4.6 Creating a Site

A site is a name under which you can group one or more subscribers. It could represent a geographical area, a department, or any other logical grouping you need.

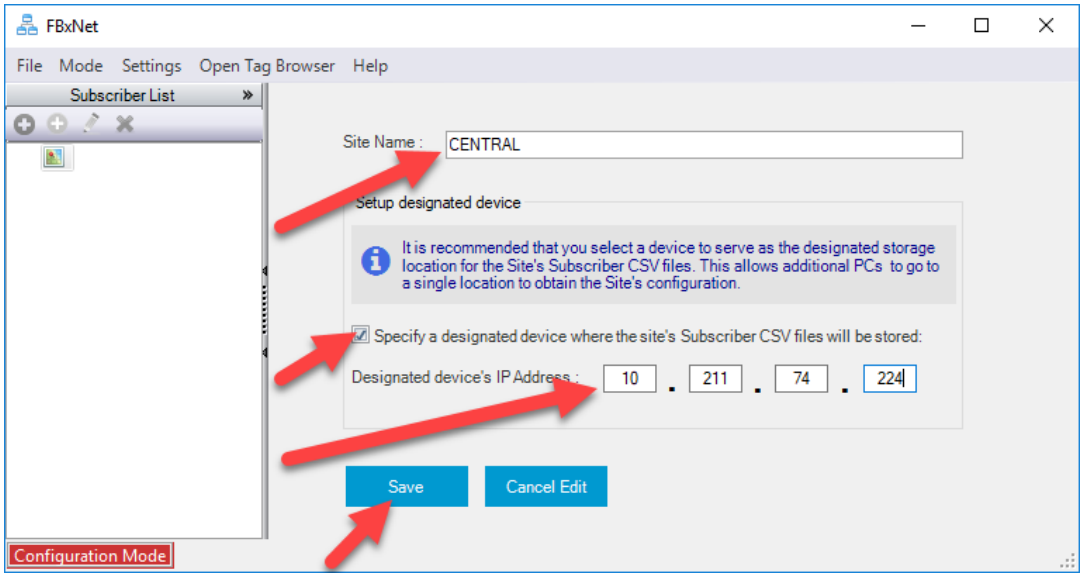
1. In Configure Mode, click the Add Site icon.

Figure 4-6. Adding a Site



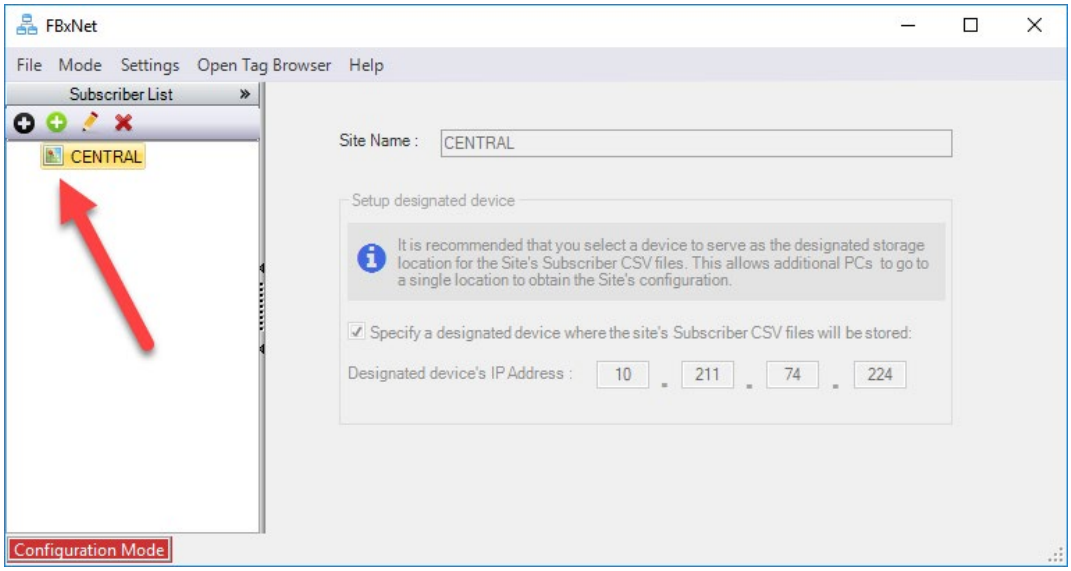
2. Now enter the name of the site in **Site Name.** The **Setup designated device** section defines a device where FBxNet stores CSV files for the subscribers associated with this site. This provides other PCs a place to locate FBxNet configuration details for the site. Check the **Specify a designated device...** box, and enter the **Designated device's IP Address**.

Figure 4-7. Defining the Site

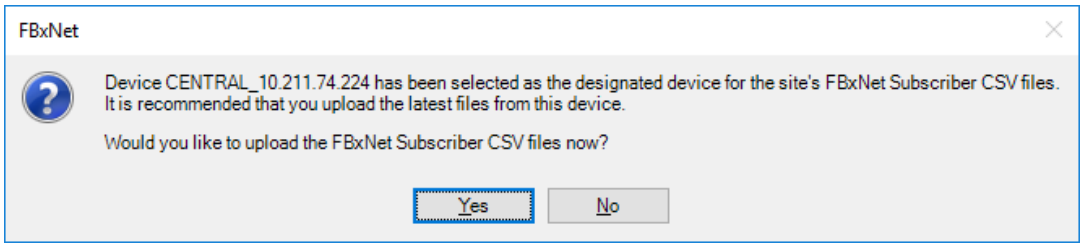


3. Click **Save**. The Subscriber List pane updates to show the newly defined **Site Name**.

Figure 4-8. Site Defined



4. FBxNet then prompts you to decide whether it should upload CSV files from the device to your PC.

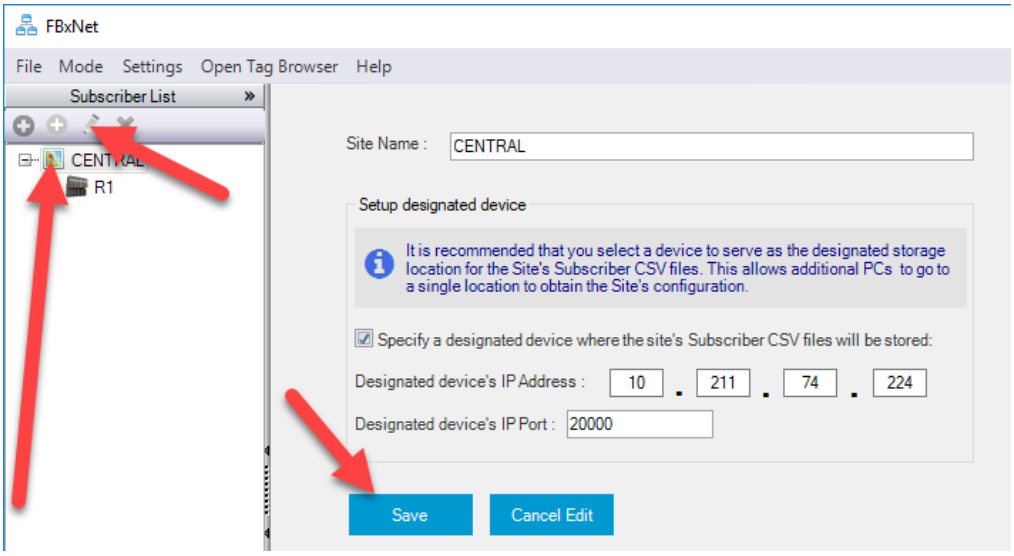


5. If you answer **Yes** FBxNet connects with the designated device and then notifies you if the version of CSV files on the designated device is newer, older, or the same as those on your PC. You can decide what you want to do. Typically, you would want to upload is the CSV files on the designated device are **newer** than the CSV files on the PC.

4.6.1 Editing the Site

After entering Configure Mode, click on the site in the Subscriber List pane and click and you can edit the site. Click **Save** to save your edits and update the CSV file or **Cancel Edit** to discard your edits.

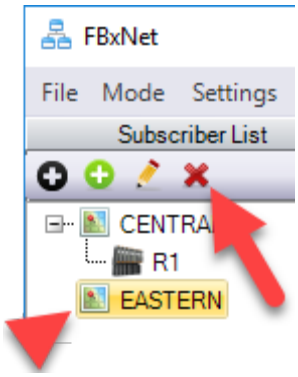
Figure 4-9. Editing a Site



4.6.2 Deleting a Site

You can only delete a site if it has no subscribers; once a site has subscribers you cannot delete it unless you first delete its subscribers.

In Configure Mode, click on the site name in the Subscriber List pane, then click the delete icon.



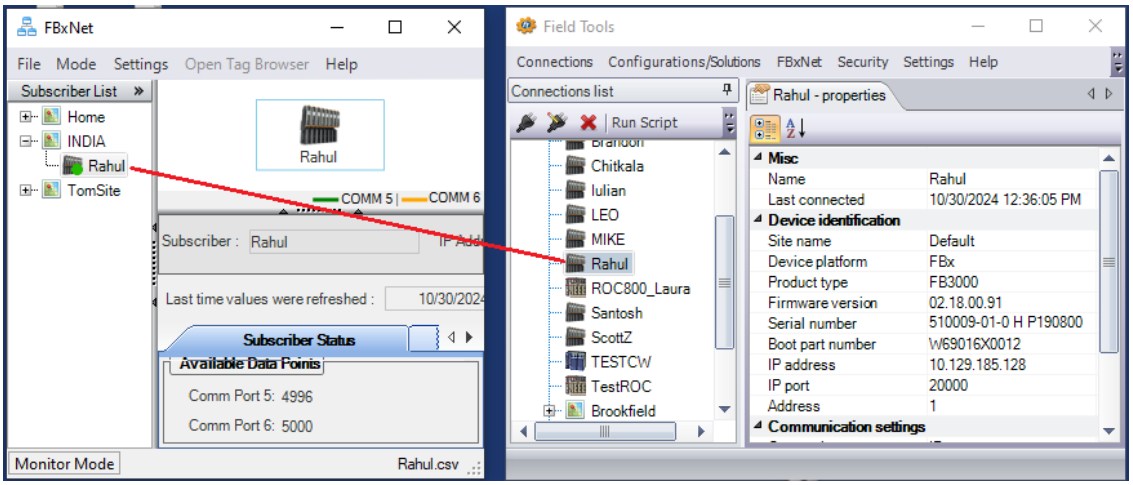
4.7 Creating a Subscriber Directly in FBxNet

Subscriber information is stored in CSV file(s). Each subscriber has its own CSV file that lists the name and IP address of the subscriber device as well as the names and IP addresses of all its publisher devices. The file also includes details on each publisher's parameters. The parameters define the source and destination tags for data to be exchanged between the publisher and subscriber over FBxNet.

You can create a subscriber's CSV file directly in FBxNet as described, below. Alternatively, you can create a CSV file manually in a text editor or Microsoft® Excel (See *Manually Creating the Subscriber CSV File*.)

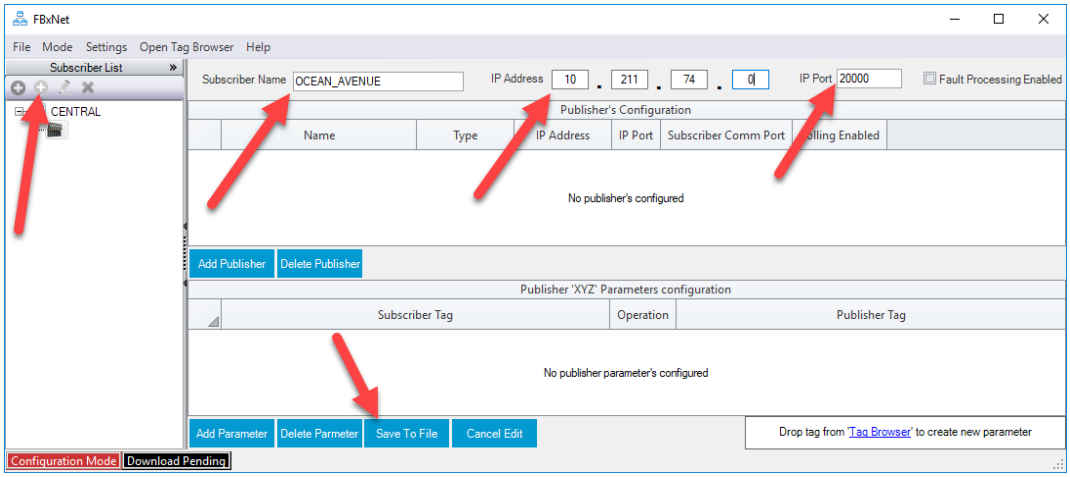
Note

If a subscriber device has SAv5 enabled, its name must be identical to its connection name in the Field Tools Connection list (visible in the tree) and that connection must have the correct SAv5 key for the FBxNet connection to work.



1. In Configure Mode, click in the Subscriber List pane on the site in which you want to add a subscriber, then click the Add Subscriber icon.
2. Specify the **Subscriber Name**, its **IP Address**, and **IP Port**.

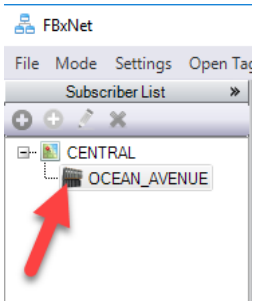
Figure 4-10. Adding a Subscriber



3. You can add publishers for this subscriber. (See *Adding a Publisher*.)
4. You can add publisher parameters and specify associated subscriber parameters for data exchange through FBxNet. (See *Adding a New Parameter*.)

5. Click **Save To File** to save your edits to the subscriber CSV file and FBxNet adds the name to the subscriber list.

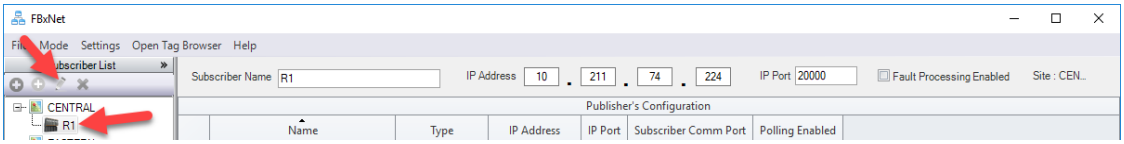
Figure 4-11. Subscriber Added



Alternatively, you could click **Cancel Edit** to cancel the operation.

4.7.1 Editing a Subscriber

After entering Configure Mode, select the subscriber, and click and you can edit the subscriber fields. Click **Save To File** when you finish to update the CSV file.

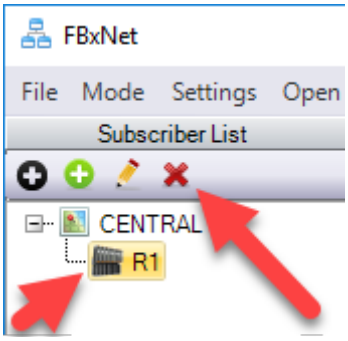


4.7.2 Deleting a Subscriber

Important

Once you delete a subscriber, you delete its associated CSV file. You **cannot undo** this deletion. Because of this, you may, instead want to remove the subscriber files from the device, through the Remove Subscriber button on the FBxNet display in FBxConnect. This removes the files at the device, but does not affect those stored at the PC, so you could re-download them to the device later if you decide you want to recreate the subscriber at the device.

In Configure Mode, click on the subscriber in the Subscriber List pane, then click the delete icon. You will be prompted to confirm the deletion.



4.8 Adding a Publisher

After entering Configure Mode, selecting a subscriber, and clicking you can add another publisher device for this subscriber:

1. In the Publisher's Configuration pane, click **Add Publisher** Add Publisher to add a new line to the grid.

	Name	Type	IP Address	IP Port	Subscriber Comm Port	Polling Enabled
1	New Publisher	FB3000	0.0.0.0	20000	5	☑

2. Enter the **Name** of the publisher, its device **Type** (FB3000, FB1200, or FB2200), its **IP Address**, **IP Port** (default is 20000), **Subscriber Comm Port** (5 or 6), and check **Polling Enabled** to allow communication to occur.
3. When you finish with all your edits on this page, click **Save To File** to update the CSV file.

4.8.1 Editing a Publisher

After entering Configure Mode, select a site and click on the subscriber, and click and you can edit the publishers under that subscriber. Click **Save To File** when you finish to update the CSV file.

	Name	Type	IP Address	IP Port	Subscriber Comm Port	Polling Enabled
1	MYPUB1	FB3000	0.0.0.0	20000	5	☑

4.8.2 Deleting a Publisher

Important
Exercise caution because once you delete a publisher, you cannot undo it. Deletion removes the publisher, its parameters, and all its tags from the CSV file.

After entering Configure Mode, selecting a subscriber, and clicking you can delete a publisher device from this subscriber:

1. In the Publisher's Configuration pane, use the scroll bar (if necessary) to locate the publisher you want to delete, and click on the line for it.
2. Click **Delete Publisher**. This deletes the publisher from the grid and from the CSV file.

4.9 Adding a New Parameter

After entering Configure Mode, selecting a site and subscriber, and clicking  you can add a new parameter.

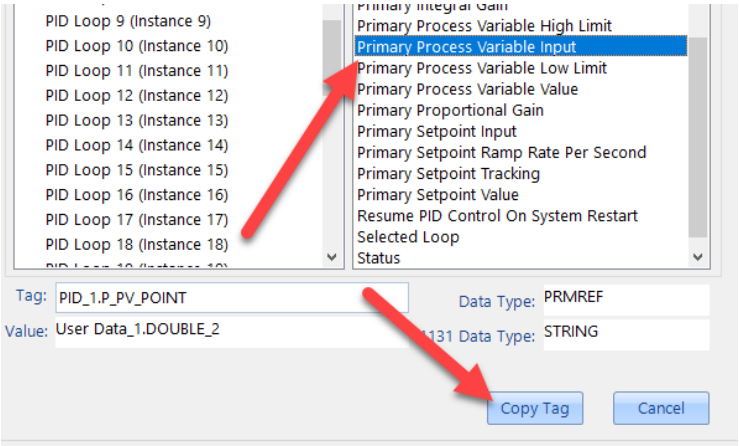
1. In the Publisher's Configuration pane, use the scroll bar (if necessary) to select the publisher for which you want to edit parameters, and click on its line.
2. In the Publisher Parameters Configuration pane you can see the existing parameters for this publisher. Use the scroll bar (if necessary) to locate the line below where you want to add the parameter and click on that line.
3. Click **Add Parameter** 

to add an empty line into which you can define the new parameter.

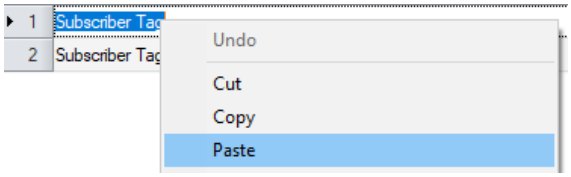
	Subscriber Tag	Operation	Publisher Tag
1	Subscriber Tag	READ	Publisher Tag

4. Launch the Tag Browser. For more information on using the Tag Browser, see *Working with the Tag Browser*.
5. Select the attribute whose tag you want as a **Subscriber Tag**, then click **Copy Tag**.

Figure 4-12. Copying a Tag



6. Go to the **Subscriber Tag** field in the empty line in the Publisher Parameters Configuration pane, right-click and choose **Paste** to paste in the tag. Repeat steps 5 and 6 to specify the **Publisher Tag**.



7. In the **Operation** field, choose **READ** or **WRITE**.
8. When you finish with all your edits on this page, click **Save To File** to update the CSV file.

Note
Instead of **Copy Tag** in Step 5, and **Paste** in Step 6, you can drag the attribute from the Tag Browser attribute pane into the desired Subscriber Tag or Publisher Tag field.

4.9.1 Editing Existing Publishing Parameters

After entering Configure Mode, selecting a subscriber, and clicking you can edit publisher parameters:

1. In the Publisher's Configuration pane, use the scroll bar (if necessary) to select the publisher for which you want to edit parameters, and click on its line.
2. In the Publisher Parameters Configuration pane, you can:
   - Click on the Publisher or Subscriber tag you want to edit, and proceed to edit the names as desired; press the **[Enter]** key when you're satisfied with your change.
   - Copy a tag name by clicking once on a tag and right clicking and selecting **Copy**; then you can click on a different field, right click and choose **Paste**.
   - Drag or paste in a tag name from the FBx Tag Browser. See *Working with the Tag Browser* for details.
3. Repeat for any other parameters you want to edit.
4. When you finish with all your edits on this page, click **Save To File** to update the CSV file.

Note
If you make a mistake in your edits, you can undo them by clicking **Cancel Edits**. Once you have saved the file, however, you cannot undo your changes.

4.9.2 Deleting a Parameter

Important
Exercise caution because once you delete a parameter, you cannot undo it.

After entering Configure Mode, selecting a subscriber, and clicking you can delete a parameter from this subscriber:

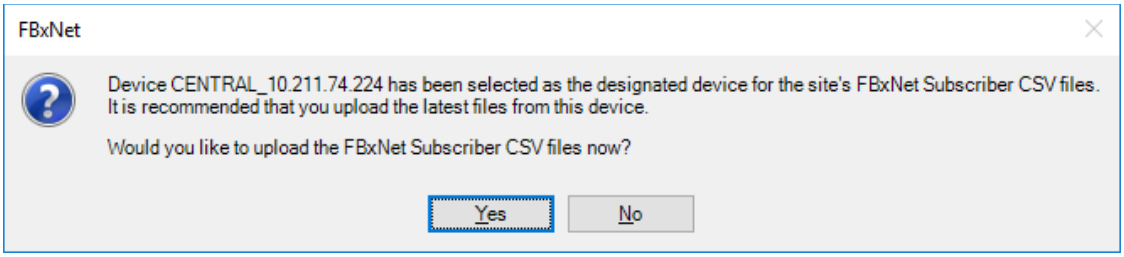
1. In the Publishers Configuration pane, use the scroll bar (if necessary) to locate the parameter you want to delete, and click on the line for it.
2. Click **Delete Parameter**. This deletes that line from the grid and from the CSV file.

Note
If you make a mistake in your edits, you can undo them by clicking **Cancel Edits**. Once you have saved the file, however, you cannot undo your changes.

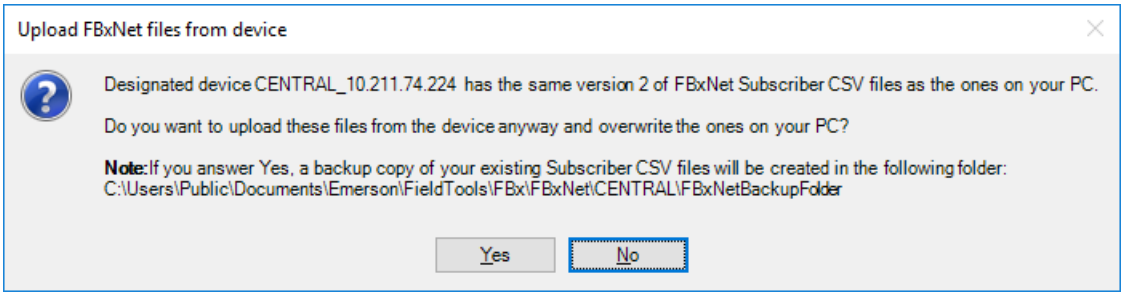
4.10 Synchronizing CSV Files

When you make changes to CSV files in FBxNet, FBxNet reminds you to download the changes by showing a **Download Pending** Download Pending message on the screen. You should then *download the CSV files*.

When you first create a site and specify a designated device to hold CSV files, FBxNet prompts you to synchronize files and if you agree, checks to see if CSV files on the designated device are newer, older, or the same as those on your PC. FBxNet also prompts you for this check when you click on a site name for the first time or expand the tree for a site the first time.



If you answer **Yes** FBxNet connects to the designated device and checks the CSV file versions and notifies you whether the CSV files on the designated device are newer, older or the same as CSV files on your PC. You can then choose whether or not you want to proceed with the upload. Typically, you would want to answer **Yes** to upload if the files on the designated device are newer than the ones on your PC.



4.11 Manually Creating the Subscriber CSV File

Subscriber information is stored in CSV file(s). Subscriber CSV files list the names and IP addresses of the subscriber device and all its publisher devices, as well as each publisher's parameters. The parameters define the source and destination tags for data to be exchanged between the publisher and subscriber over FBxNet.

Create one or more subscribers for each site. You can create subscribers directly in FBxNet as described in *Creating a Subscriber Directly in FBxNet*.

Alternatively, you can create a CSV file manually in a text editor or Microsoft® Excel If you have multiple subscriber devices, you must create a separate CSV file for each one. For example, if you have three subscribers, you must create three CSV files – one for each subscriber.

If you have many subscribers or many publishers, you may want to create your first subscriber or publisher directly in FBxNet, and then manually edit the resulting CSV file to add additional publishers, or copy the CSV file and use it as a basis for defining another subscriber and set of associated publishers.

4.11.1 Subscriber File Format

In the subscriber file, bolded entries must appear exactly as shown. Italicized entries must be modified to reflect details on the subscriber and publishers and associated tags.

The first line, which is bolded, provides a guide to the meaning of entries on the second line. The second line entries define the subscriber device.

The third line and fourth line (both bolded) provide a guide to the meaning of entries for the subscriber devices, defined on subsequent lines.

From line five to the end of the file are definitions of individual publisher devices, and their associated parameters. Lines that describe the actual tags begin with a comma ",".

SubscriberName,SubscriberIPAddress,SubscriberIPPort

SubscriberDeviceName, SubscriberIPAddress,SubscriberIPPort

PublisherName,PublisherType,PublisherIPAddress,PublisherIPPort,SubscriberCommPort,Enabled

,SubscriberTag,Operation,PublisherTag,FaultMode,FixedFaultValue,FBxNDataInstance

PublisherName:*PublisherDeviceName1,PublisherType1,PublisherIPAddress1,PublisherIPPort1, CommPortNumber1, EnableFlag1*

,SubscriberTag1, Operation1, PublisherTag1,FaultMode1,FixedFaultValue1,FBxNDataInstance1

,SubscriberTag2, Operation2, PublisherTag2,FaultMode2,FixedFaultValue2,FBxNDataInstance2

: :

,SubscriberTagx, Operationx, PublisherTagx,FaultModex,FixedFaultValuex,FBxNDataInstancex

PublisherName:*PublisherDeviceName2,PublisherType2,PublisherIPAddress2,PublisherIPPort2, CommPortNumber2 EnableFlag2*
,SubscriberTag1,Operation1,PublisherTag1,FaultMode1,FixedFaultValue1,FBxNDataInstance1
,SubscriberTag2,Operation2,PublisherTag2,FaultMode2,FixedFaultValue2,FBxNDataInstance2
: :
,SubscriberTagy,Operationy,PublisherTagy,FaultModey,FixedFaultValuey,FBxNDataInstancey
: :
PublisherName:*PublisherDeviceNamew,PublisherTypew, PublisherIPAddressw, PublisherIPPortw, CommPortNumberw EnableFlagw*
,SubscriberTag1,Operation1,PublisherTag1,FaultMode1,FixedFaultValue1,FBxNDataInstance1
,SubscriberTag2,Operation2,PublisherTag2,FaultMode2,FixedFaultValue2,FBxNDataInstance2
: :
,SubscriberTagz,Operationz,PublisherTagz,FaultModez,FixedFaultValuez,FBxNDataInstancez

Where:

Table 4-1. Subscriber File Parameters

Parameterr	Description
SubscriberDeviceName	Is the name of the subscriber (client) device. Although not required, we recommend you use the name of the FB3000 as defined in Field Tools.
SubscriberIPAddress	Is the IP address of the subscriber device. This is the IP address used by Field Tools to connect to the subscriber.
SubscriberIPPort	Is the TCP/IP port number of the subscriber device. If not specified, FBxNet uses a default of 20000. **Note**: Do not enter **9009** for this number; it is reserved by FBxNet.
PublisherName:*Publisher DeviceName*	Marks the beginning of a publisher (server) device definition. The keyword **PublisherName**: is required followed by the name of the publisher. Publisher names must be unique within the file; FBxNet ignores any duplicate publisher names
PublisherType	Specifies the type of device. Valid values are FB1200, FB2200, and FB3000. If not specified, FBxNet assumes a default of FB3000.
PublisherIPAddress	Is the IP address of this publisher device.
PublisherIPPort	Is the TCP/IP port number of this publisher device. If not specified, FBxNet assumes a default of 20000. (RESERVED FOR FUTURE USE)
CommPortNumber	Is the subscriber communication port number. This is either **5** or **6**.

Parameterr	Description	
EnableFlag	Is set **TRUE** to turn on polling for this publisher device, or **FALSE** to turn off polling for this publisher device.	
,SubscriberTag	Specifies the name of a database parameter in the subscriber device for which you want to transfer its value via peer-to-peer communication.	
Operation	is set to **READ** if the subscriber should read from this publisher or **WRITE** if the subscriber should write to this publisher.	
PublisherTag	Specifies the name of a database parameter in the publisher device whose value the subscriber wants to read from or write to.	
FaultMode	(This field is Optional, but if you include it you must also include the related *FixedFaultValue* and *FBxNDataInstance* fields) – Specify how FBxNet handles a communication failure or other error from this publisher. Choices are:	
	LIVE	Disables fault handling.
	FAULT	Switch to a pre-defined value, as specified in the FixedFaultValue field.
	LAST_GOOD	Show the last good value received.
FixedFaultValue	(This field is Optional, but if you include it you must also include the related *FaultMode* and *FBxNDataInstance* fields.) When Fault Mode is set to FAULT, specifies an override value to be used when a communication error or other fault occurs.	
FBxNDataInstance	(This field is Optional, but if you include it you must also include the related *FaultMode* and *FixedFaultValue* fields.) This field specifies the name of a fault handling database object and registers it in the FB3000 database. You can specify any unused FBxNDataInstance object number; they follow the format: **//FBXNData_x//** Where x is any integer between 1 and 10000. Once registered in the FB3000 database to belong to a particular publisher tag, this object instance stores any data quality or parameter "health" code received about a fault. This data can then be logged and may be viewed in the FBxConnect diagnostic report.	

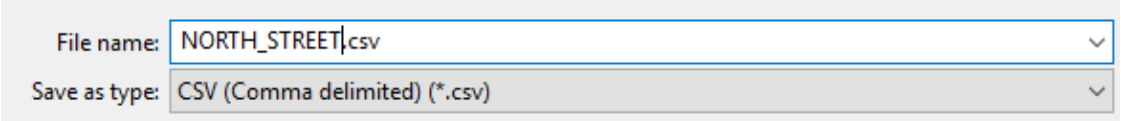
4.11.1 Subscriber File Example – Created in Excel

Below is an example subscriber file created in Microsoft® Excel. Typically, a subscriber file could refer to dozens of devices. The figure, below, shows a subscriber named NORTH_STREET with two publishers named ELM_STREET and SEASIDE_DRIVE. ELM_STREET has three data points to be transferred, and SEASIDE_DRIVE has four data points to be transferred. Both publishers use the default IP port of 20000, so the PublisherIPPort field may be left blank.]

Figure 4-13. . Subscriber CSV File in Excel

	A	B	C	D	E	F	G	H
1	SubscriberName	SubscriberIPAddress	SubscriberIPPort					
2	NORTH_STREET	10.211.74.221	20000					
3								
4	PublisherName	PublisherType	PublisherIPAddress	PublisherIPPort	SubscriberCommPort	Enabled		
5		SubscriberTag	Operation	PublisherTag	FaultMode	FixedFaultValue	FBxNDataInstance	
6								
7	PublisherName:ELM_STREET	FB3000	10.208.015.122		5	TRUE		
8		User Data_1.FLOAT_5	READ	User Data_1.FLOAT_5	FAULT	106	FBxNData_1	
9		User Data_1.DOUBLE_1	READ	User Data_1.DOUBLE_1	LAST_GOOD	0	FBxNData_2	
10		User Data_1.DOUBLE_2	READ	User Data_1.DOUBLE_2	FAULT	33.33	FBxNData_3	
11								
12	PublisherName:SEASIDE_DRIVE	FB1200	10.208.015.125		6	TRUE		
13		User Data_1.DOUBLE_3	READ	User Data_1.DOUBLE_3	FAULT	45.23	FBxNData_4	
14		User Data_1.DOUBLE_4	READ	User Data_1.DOUBLE_4	FAULT	32.13805556	FBxNData_5	
15		User Data_1.DOUBLE_5	READ	User Data_1.DOUBLE_5	FAULT	36.81988889	FBxNData_6	
16		User Data_1.DOUBLE_6	READ	User Data_1.DOUBLE_6	FAULT	41.50172222	FBxNData_7	
17								

Although not required, the base name of the file should be the name of the subscriber device and when you save the file, you must save it as type CSV (Comma separated variable) (*.csv) so that the required commas are included in the file.



4.11.2 Subscriber File Example – Created in a Text Editor

Below is a simple example subscriber file created in a text editor. Although not required, the base name of the file should be the name of the subscriber device and the extension must be CSV.

Typically, a subscriber file could refer to dozens of devices, but the simple example below, shows a subscriber named MYFB3000 with three publishers named MyPublisher1, MyPublisher2, and MyPublisher3. Each of the publishers have three data points to be transferred, and they all use the default IP port of 20000, so that field can be left blank, delimited by commas.

SubscriberName,SubscriberIPAddress,SubscriberIPPort
MyFB3000,10.208.15.82,20000

PublisherName,PublisherType,PublisherIPAddress,PublisherIPPort,SubscriberCommPort,Enabled

,SubscriberTag,Operation,PublisherTag

PublisherName: MyPublisher1,FB1200,10.208.15.83,,5,TRUE

,User Data_5.FLOAT_1,READ,User Data_5.FLOAT_1

,User Data_2.LONG_7,WRITE,User User Data_1.LONG_1

,User Data_1.SHORT_1,READ,User Data_1.SHORT_1

PublisherName: MyPublisher2,FB1200,10.208.15.84,,5,TRUE

,User Data_5.FLOAT_1,READ,User Data_5.FLOAT_1

,User Data_2.LONG_7,WRITE,User User Data_1.LONG_1

,User Data_1.SHORT_1,READ,User Data_1.SHORT_1

PublisherName: MyPublisher3,FB2200,10.208.15.85,,5,FALSE

,User Data_5.FLOAT_1,READ,User Data_5.FLOAT_1

,User Data_2.LONG_7,WRITE,User User Data_1.LONG_1

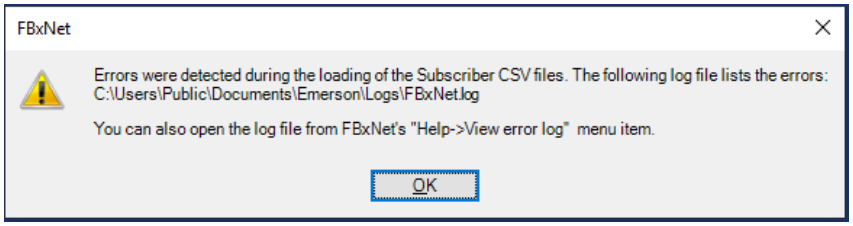
,User Data_1.SHORT_1,READ,User Data_1.SHORT_1

Other than the CSV extension (which is required), the name of the subscriber file is irrelevant but for good practices it should be the name of the subscriber device (for example MyFB3000.csv).

4.12 CSV File Validation

Field Tools performs a complete validation of the format and data of CSV files you create:

- If there are errors in subscriber data, FBxNet ignores that subscriber file.
- If there are errors in publisher data, FBxNet ignores that publisher section.
- If there are errors in the peer-to-peer data for a parameter, FBxNet ignores that parameter.
- If FBxNet can apply a default in order to continue it will. For example, if the file specifies an invalid operation, FBxNet applies a default of READ.
- If FBxNet detects errors as it loads CSV files, it creates a log file of those errors and reports this message:



You should open the log file and try to correct the errors, and then re-download the files and restart FBxNet so it loads the corrected files.

4.13 FBxNet Authentication

Every FB1200, FB2200, or FB3000 device that exists in an FBxNet network must have an identical FBxNet user configured. Each such user in the network must share identical login credentials. In FBxConnect, go to **Services > Users Management** to configure the FBxNet user.

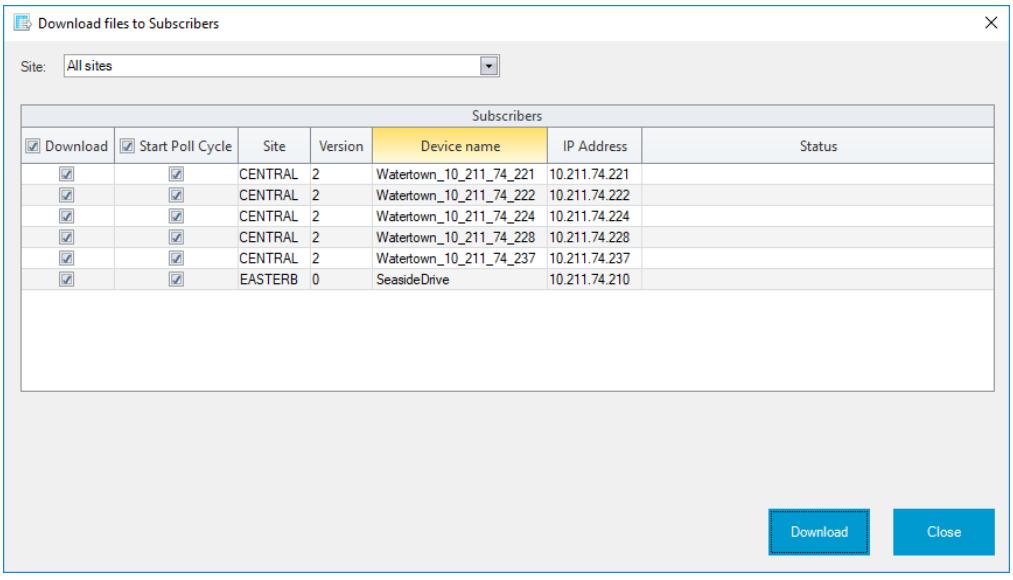
4.14 Downloading CSV Files

FBxNet first reads the subscriber CSV files to generate the network tree. FBxNet also processes the files and generates publisher-specific files for the connections and parameter mapping (map file) for each publisher device. You must download the CSV files for the FBxNet network to function.

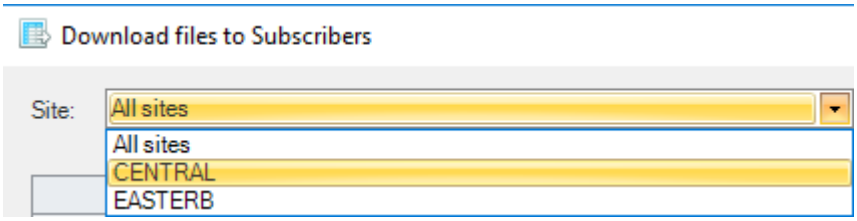
1. In Monitor Mode, click **File > Download files.**
2. The Download files to Subscribers screen shows a list of subscriber devices, showing the **Site**, **Device name** and **IP Address** of each FB3000 subscriber device.

Note
You will only see FB3000 devices in the list because only an FB3000 can serve as a subscriber

Figure 4-14. Download Files to Subscribers



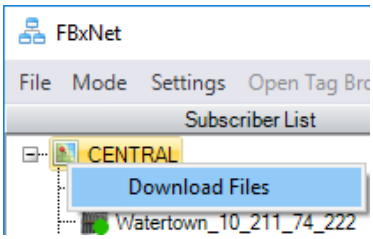
3. By default, the screen shows subscribers for all sites. To only download the subscribers for a specific site, select the desired site from the **Site** selection box.



4. To download CSV files for all subscribers, select the **Download** check box. If you only want to download CSV files to certain subscribers, de-select the **Download** check box, and then check the boxes for only those subscribers to which you want to download CSV files.
5. To start polling all subscribers automatically after the download completes, select the **Start Poll Cycle** checkbox. If you do not want polling for all subscribers to occur, de-select that and only check those devices for which you want polling to occur.
6. Click the **Download** button. FBxNet downloads CSV files to the selected subscriber(s) and starts polling for any that have **Start Poll Cycle** selected. The **Status** field shows any error messages that occur during the download for particular subscribers.

4.14.1 Downloading CSV Files for a Single Site

If you only want to download files for a single site, in Monitor Mode right click on the site name in the Subscriber List pane and choose **Download files**.



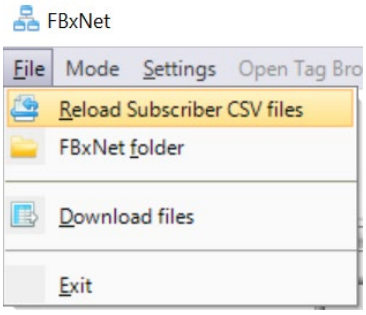
This opens the Download files to subscribers dialog box for that subscriber only. Click **Download** to proceed.

4.15 Making Changes to Your CSV Files

If you need to change your CSV file(s) after you download them, you can edit them directly in Configure Mode, or you can edit the CSV files manually in Microsoft Excel® or a text editor.

4.15.1 Making Edits Manually in Microsoft® Excel or a Text Editor

To edit CSV files manually click **File > FBxNet folder** and double-click on the folder for the site that contains the CSV file you want to edit. Use Excel or a text editor to modify the file, then save it. Make sure you save it with an extension of CSV. You must reload files modified by this method. To do this, click **File > Reload Subscriber CSV files.**



As part of the reload process:

- Previous connections are shut down.
- FBxNet clears previous CSV files from its memory.
- FBxNet validates the new CSV files and loads them into memory.
- FBxNet connects to the first subscriber in the list.

4.15.2 Making Edits Directly in FBxNet

To edit CSV files in Configure Mode, click **Mode > Configuration** and click on the name of the subscriber you want to edit, then click the edit icon. Make your changes and click **Save To File**.

4.15.3 Downloading the Modified CSV Files to Subscribers

No matter which way you make your edits, once you finish you must re-download the CSV files by clicking **File > Download files**. See *Downloading the CSV Files* for more information.

4.16 Restoring the Backup of Previous CSV Files at the PC

If you upload files from a site's designated device to the PC, FBxNet first creates a separate backup file for the existing subscriber CSV files on the PC for that site (FBxNetFilesBackup.ZIP).

If, for some reason, you accidentally overwrite the CSV file for a site, you can restore the previous version from that site's FBxNetFilesBackup.ZIP file.

1. Close FBxNet.
2. Ensure that you have a FBxNetFilesBackup.ZIP file in the folder:

   \Users\Public\Public Documents\Emerson\FieldTools\FBx\FBxNet*sitefolder***\FBxNetBackupFolder**

   where *sitefolder* is the name of the site.
3. Delete the existing CSV files in the folder:

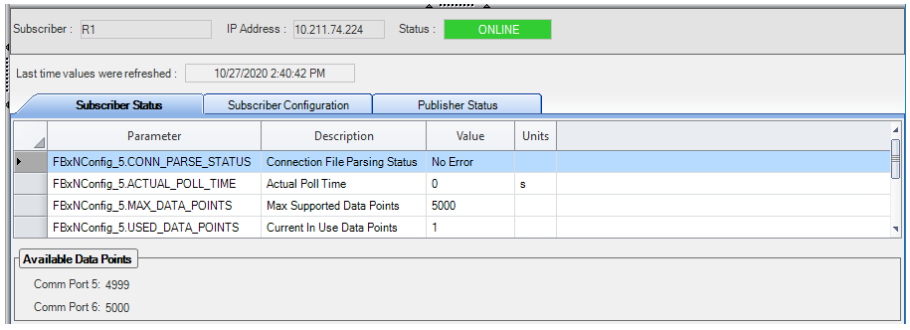
   \Users\Public\Public Documents\Emerson\FieldTools\FBx\FBxNet*sitefolder*****
4. Unzip the FBxNetFilesBackup.ZIP file, then copy the unzipped CSV files to:

   \Users\Public\Public Documents\Emerson\FieldTools\FBx\FBxNet*sitefolder*****
5. Restart FBxNet.

4.17 Viewing Status of the Subscriber Device

1. In Monitor Mode, select the subscriber device you want to see in the Subscriber List.
2. In the Network pane, click on the subscriber device (the top node in the tree) to open the Subscriber Status tab.

Figure 4-15. FBxNet – Subscriber Status tab visible



The Status pane displays the following information:

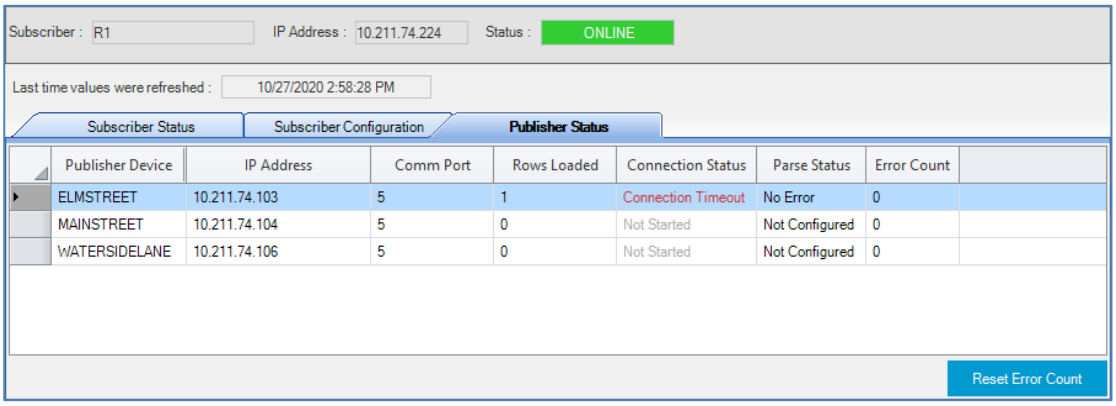
Field	Description
Subscriber	The name of the subscriber device.
IP Address	The IP address of the subscriber device.
Status	The status of the connection between FBxNet and the subscriber device.
Last time values were refreshed	The timestamp showing when status fields were last updated.

Field	Description
Parameter	This column shows the name of the database tag(s) in the subscriber device that provide status information.
Description	This column provides a textual description of the parameter to provide greater detail than the parameter name.
Value	This column shows the value of the database tag.
Units	This column shows engineering units for the value, if appropriate.
Available Data Points	Shows a list of the communication ports connected to this subscriber, and the number of data points on each port that FBxNet could potentially collect.

4.18 Viewing Status of the Publisher Devices

In Monitor Mode, click the **Publisher Status** tab.

Figure 4-16. FBxNet – Publisher Status tab visible



Field	Description
Subscriber, IP Address, Status, Last time values were refreshed	See *Section 4.17.*
Publisher Device	This column shows names of the publisher (server) devices.
IP Address	This column shows IP addresses of the publisher devices.
Comm Port	This column shows the communication port numbers used by the publisher devices. This is either 5 or 6.
Rows Loaded	This column shows the number of parameter mapping file rows that were successfully parsed from the publisher device. For example, if you have 5 parameters you are transferring between a publisher and the subscriber, this

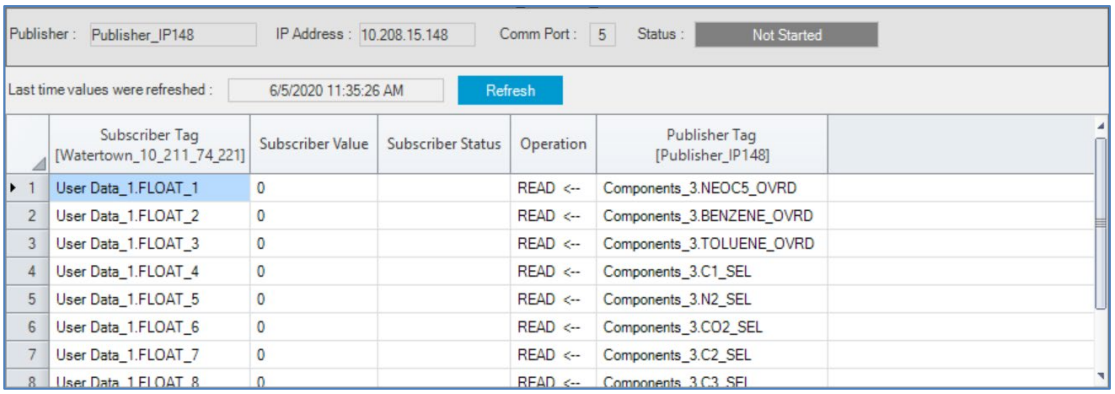
Field	Description	
	number should be 5. If Rows Loaded is less than the number of parameters you are transferring, this indicates FBxNet could not parse one or more of the parameter lines in your CSV file, and you should check the file for errors.	
Connection Status	This column shows the current connection status of the publisher device. Possible status messages include:	
	Not Started	FBxNet not setup for the device (no parameter mapping file for the publisher) or polling not started.
	Connecting	The subscriber is attempting to establish a TCP connection to the publisher.
	Resolving	The subscriber is resolving all the tags to be read/written as well as the fault handling instructions.
	Online	System is communicating with no issues found.
	Offline	Publisher is disabled in the device connection file.
	Invalid	Publisher's parameter mapping file is invalid, or the response received from the publisher is invalid. This is a critical error - the system will attempt to recover.
	Connection Timeout	Subscriber could not connect to the publisher. TCP connection request failed.
	Transmission Error	Subscriber could not send message to the publisher. Transmission of the data failed.
	Response Timeout	No response received. Subscriber timed out waiting for response from the publisher.
	Resolving Failure	Critical error occurred while resolving the parameter map.
	Read Failure	Critical error occurred while reading the parameters from the publisher.
	Disabled	Device is disabled.

Field	Description	
	Online with Parameter Error(s)	System transferring data but there are errors - see subscriber diagnostic file for details.
	No Account Found	There is no FBxNet user account on the subscriber.
	Authentication Failed	There is a mismatch between the FBxNet user accounts (username and password) on the subscriber and the publisher. If this happens, you must stop communications between the subscriber and publisher, use FBxConnect to modify the FBxnet user account usernames and/or passwords in the subscriber and publisher so they are identical in both devices, and then restart communications. **Note**: If the user account is locked out you must either wait for the lock out to expire, or a security administrator must temporarily disable the lockout in FBxConnect, then re-enable it when you finish.
	Authenticating	The subscriber is attempting authentication with the publisher.
Parse Status	This column shows the current parsing status of the publisher device's parameter mapping file. Possible status messages include:	
	No Error	Parse was successful.
	File Open Fail	Could not find or open the publisher map file.
	Column Mismatch	Column of the map file is invalid.
	Missing Required Column	Missing required column header in the map file.
	Exceeded Max Data Points	Map file number parameters exceed the maximum allowed.
Error Count	This shows the total number of errors for connections to each publisher. You can zero-out this number by clicking **Reset Error Count**.	

4.19 Viewing Details on a Single Publisher

In Monitor Mode In the network pane, click the icon for the publisher you want to view and the status pane updates with details on that publisher.

Figure 4-17. Details on Single Publisher



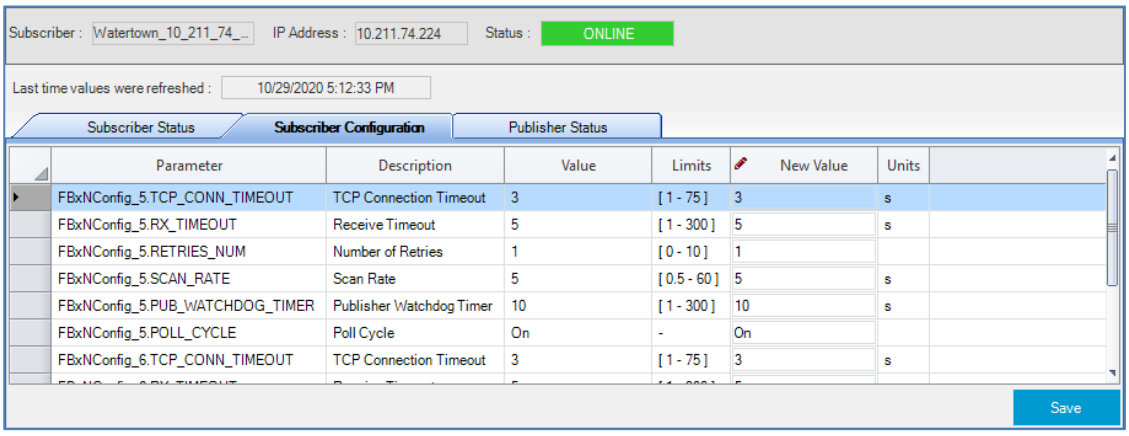
Field	Description
Publisher	This shows the name of the selected publisher device.
IP Address	This shows the IP address of the publisher device.
Comm Port	This column shows the communication port number used by the publisher device. This is either 5 or 6.
Status	Shows the status of the connection to this publisher.
Last time values were refreshed	Shows the last time the values were updated in the Status pane. Click **Refresh** to force an update.
Subscriber Tag	This column shows the names of database parameters in the subscriber device for which you want to transfer values using peer-to-peer communication. The heading for the column shows the subscriber device name.
Subscriber Value	This column shows the value of the subscriber parameter.
Subscriber Status	In this column, if FBxNet could not collect the value, it shows an error code. The most typical error is “Tag name is not valid. Error code:1307” which occurs when a parameter does not exist.
Operation	This column shows **READ** if the subscriber should read from this publisher or **WRITE** if the subscriber should write to this publisher.
Publisher Tag	This column specifies the names of database parameters in the publisher whose values the subscriber wants to read from or write to. The heading for the column shows the publisher’s device name.

Click **Refresh** to update the Status pane with the latest values from the publisher

4.20 Modifying FBxNet Configuration Parameters

In Monitor Mode, click the **Subscriber Configuration** tab.

Figure 4-18. Subscriber Configuration tab



The Subscriber Configuration tab updates to show configuration parameters for each port on the subscriber device. The **Parameter** names begin with the name FBxNConfig_x where x is the port number. The **Description** field provides a textual description for the parameter and the **Value** field shows the current value of the parameter. The **Limits** field shows the range of valid values for that parameter.

See *Section 4.9* for details on the read-only fields.

You can select a **Parameter** and then enter its new value in the **New Value** field. The **Units** field shows the engineering units (if applicable). To finish and write the new value(s) to the subscriber, click **Save**.

The configuration parameters are:

Parameter	Description
TCP_CONN_TIMEOUT	The number of seconds the subscriber waits for a response from a connection request before a timeout occurs.
RX_TIMEOUT	The number of seconds the subscriber waits for a response from the publisher after the connection has been established.
RETRIES_NUM	The number of retry attempts when a timeout occurs.
SCAN_RATE	The frequency at which the subscriber polls its publishers.
POLL_CYCLE	Enables/disables polling for this port.

4.21 Enabling/Disabling Fault Processing

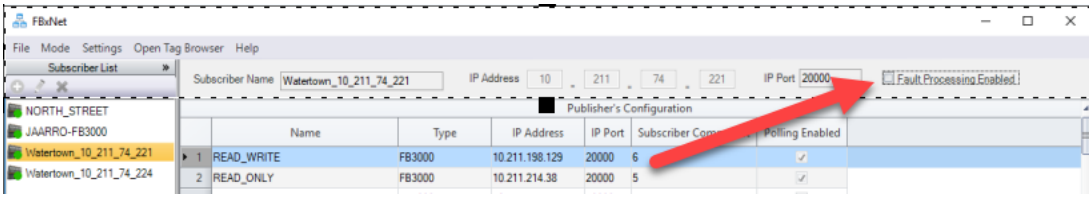
Optionally, you can specify a database object to process a fault in FBxNet communications. For example, you can specify that if communications fail during transmission of a particular parameter, you could use its last good value, or a pre-configured fixed fault value. Fault processing also captures any error code generated from the fault, allowing it to be logged in the FBxConnect Diagnostic Report.

To enable fault processing, in Configure mode click **Fault Processing Enabled**

Important

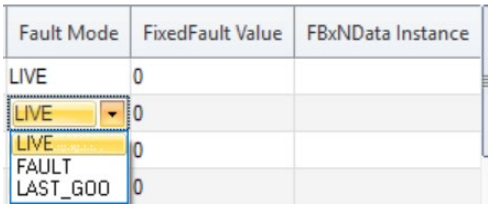
For I/O points, built-in hardware fault handling and user-configured fault handling in FBxConnect supersedes FBxNet fault processing because the hardware/firmware fault handling is more feature-rich

Figure 4-19. Enabling Fault Processing



Once enabled, FBxNet adds three additional columns to the Publisher Parameters Configuration screen. You must configure all three for fault processing to work.

Figure 4-20. Fault Handling Columns



Note

If after you configure the fault handling columns you de-select Enable Fault Handling, FBxNet deletes those columns and the entries you made from the configuration and your CSV file.

Column	Description	
FaultMode	Use the selection box to specify how FBxNet handles a communication failure or other error from this publisher. Choices are:	
	LIVE	Disables fault handling.
	FAULT	Switch to a pre-defined value, as specified in the FixedFaultValue field.

Column	Description
	LAST_GOOD Show the last good value received.
FixedFaultValue	When Fault Mode is set to FAULT, specifies an override value to be used when a communication error or other fault occurs.
FBxNDataInstance	This field specifies the name of a fault handling database object and registers it in the FB3000 database. You can specify any unused FBxNDataInstance object number; they follow the format: **//FBxNData_y//** where y is any integer between 1 and 10000. Once registered in the FB3000 database to belong to a particular publisher tag, this object instance stores any data quality or parameter "health" code received about a fault. This data can then be logged and may be viewed in the FBxConnect diagnostic report.

4.22 Troubleshooting Tips

- Do your devices have firmware that supports FBxNet? If not, FBxNet will not work.
- Did you put your CSV files in the correct folder? They must be in **\Users\Public\Public Documents\Emerson\FieldTools\FBx\FbxNet**
- If you edited your CSV file(s) in Excel, did you remember to save them in the CSV format? They must be CSV files, not XLS files.
- Check the Rows Loaded, Connection Status, and Parse Status entries on the Publisher Status tab. This can help you identify where problems might exist.

4.23 FBxNet Settings

Click **Settings** to open the FBxNet Options dialog box. You can decide whether you want FBxNet to display a dashed line on the screen for one or both communication line connections to publishers. Check the desired box(es) and click **OK**.

Figure 4-21. FBxNet Options dialog box

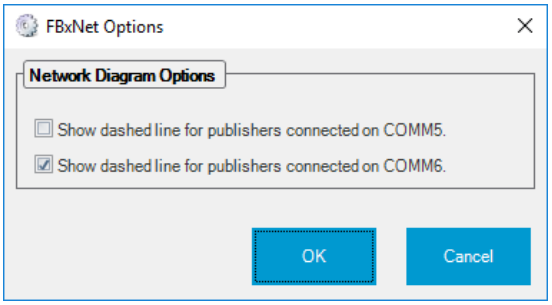
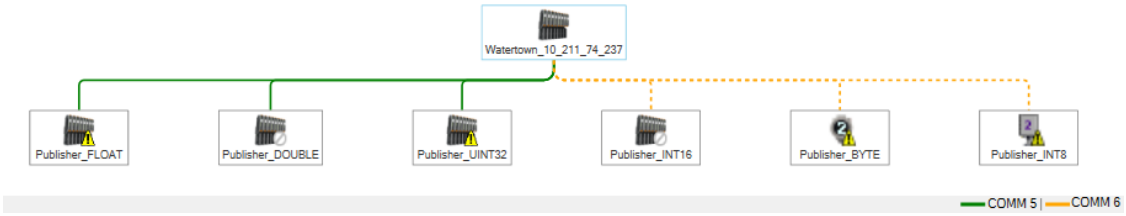


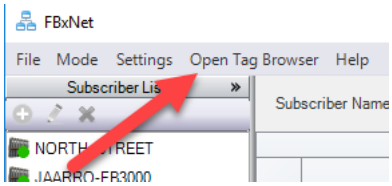
Figure 4-22. Effect on Network Diagram

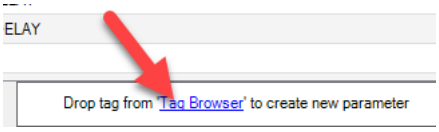


4.24 Working with the Tag Browser

The Tag Browser lets you examine all the database objects and their associated attributes for a selected FB3000 RTU.

1. Either click **Open Tag Browser** in the FBxNet menu bar, or click **Tag Browser** from the link in Publisher Parameters Configuration pane; either one opens the Tag Browser.



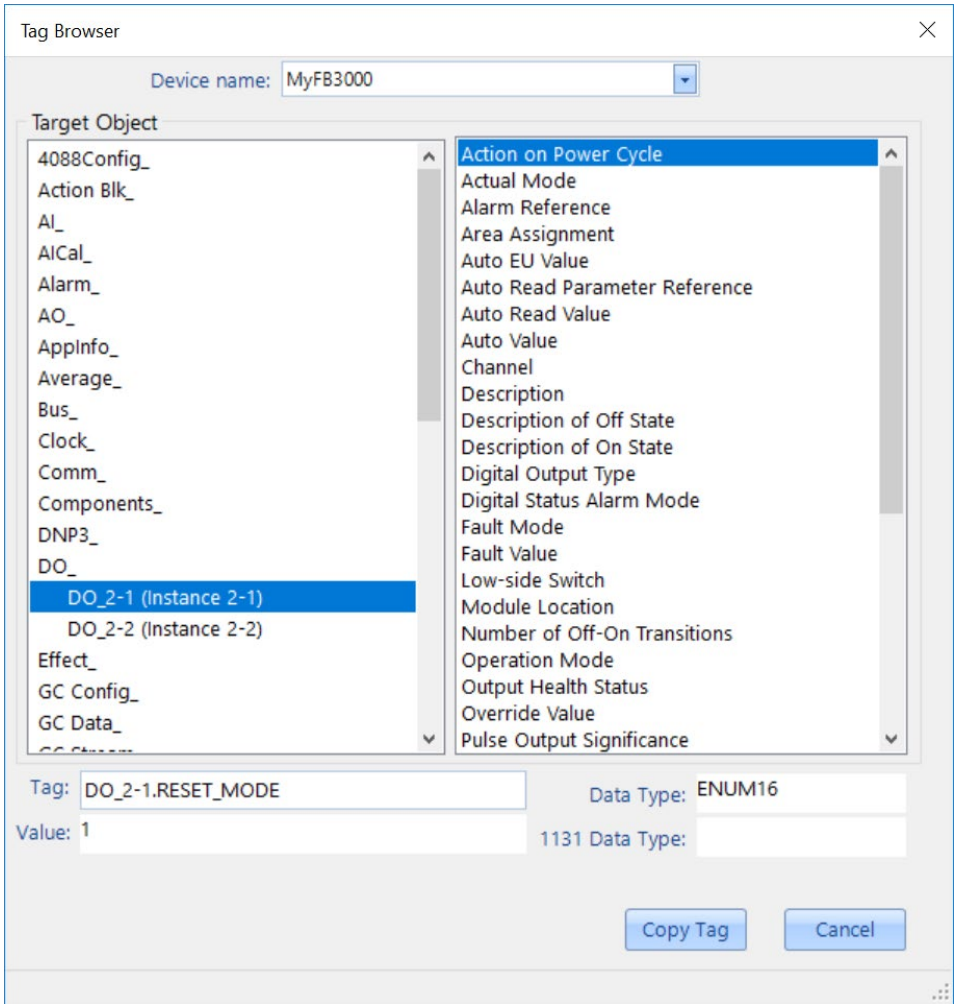


2. In the Tag Browser, select the **Device name** of the RTU or flow computer from which you want to view tags; once you make your selection, the Tag Browser populates the **Target Object** pane.

   Each database object shown in the **Target Object** pane corresponds to a particular feature or component that you configure in FBxConnect. For example, if you install a mixed I/O module in the device, there will be a database object for each type of input or output you configure in FBxConnect.

   So, for an I/O module that has two (2) digital outputs, there will be two instances (or copies) of the digital output (DO) object – one for each DO.

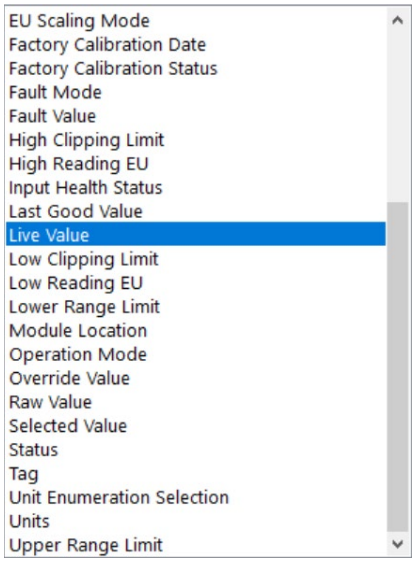
Figure 4-23. Tag Browser



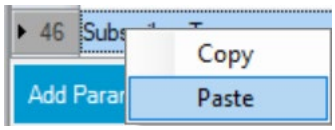
3. Select the desired **Target Object** instance. Once you click on it, the rightmost pane updates with the attributes for that object instance.

   Each object typically also has one or more attributes. For example, for an analog input (AI), you could choose the raw value from the I/O point, the live value scaled for the applied engineering units, the tag name, or many other things.

Figure 4-24. Attribute Pane Showing Attributes of a Target Object Instance



4. Click the attribute of interest. Tag Browser updates the **Tag**, **Data Type**, **Value**, and **1131 Data Type** (if applicable) for the selected tag.
5. You can click **Copy Tag** to store the tag name associated with that attribute in the clipboard, and then right click and **Paste** it into any field that accepts a publisher or subscriber tag.



Or you can drag the name of the attribute from the attribute pane and release your cursor in the field where you want it; FBxNet pastes in the associated tag name.

Chapter 5. Device Security Management

This chapter covers the Device Security Management tool in Field Tools.

5.1 Device Compatibility

Device Security Management's DNP3 License Keys feature tab works with:

- FB1100, FB1200, FB2100, and FB2200 flow computers with firmware 2.13 or newer.
- FB3000 RTU with firmware 2.13 or newer.

Device Security Management's Credential Manager tab (if present) works with:

- FB1100, FB1200, FB2100, and FB2200 flow computers
- FB3000 RTU
- ControlWave devices with version 2.0 or newer firmware.
- ROC and FloBoss devices that support either the legacy username/password scheme using PT 57 Parameter 0 (3-character user id) and Parameter 4 (4-character password), or the enhanced username/password scheme with longer usernames and passwords. Contact Technical Support for exact firmware revisions for the legacy scheme.

5.2 Starting Device Security Management

Click **Security > Device Security Management**

5.3 DNP3 Security Keys tab

In a communication network using Distributed Network Protocol 3 (DNP3) Secure Authentication Version 5 (SAV5) verifies that a message from a device (RTU or flow computer) has arrived intact, without any alteration.

To implement SAV5, both the devices and the SCADA system must support SAV5.

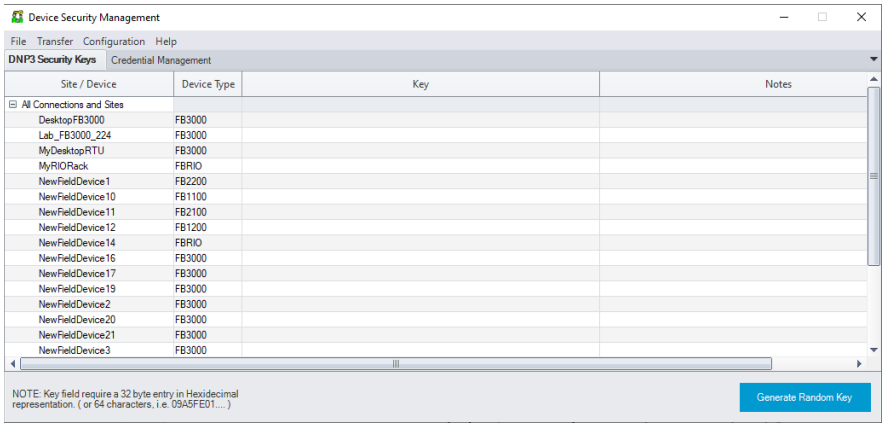
When the message arrives the protocol performs an operation on the message using a **DNP3 security key** - that must be known at both the source and destination - to tell that the message is valid .

A DNP3 security key is a 32-btye string, consisting of 64 hexadecimal characters. Hexadecimal characters are the integers 0 through 9, and the letters A, B, C, D, E, and F.

Device Security Management allows you to:

1. Create DNP3 security keys for FB1000/2000 Series Flow Computers and the FB3000 RTU that communicate via DNP3 protocol using SAV5. (See *Section 5.3.1*).
2. Save the keys for those RTUs with their associated Field Tools connections. (See *Section 5.3.3*).
3. Create a security target file (*.STF) for each RTU containing its DNP3 security key. (See *Section 5.3.4*).
4. Load the security target file in the device.

Figure 5-1. DNP3 Security Keys tab

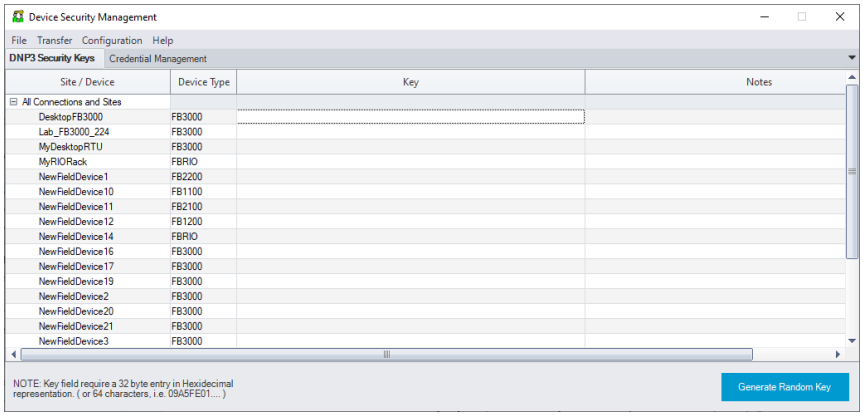


5.3.1 Creating DNP Security Keys

You could make up your own DNP3 keys, but you would need to type them in yourself which could result in an error. An easier way to create the key is to let Device Security Management generate the key:

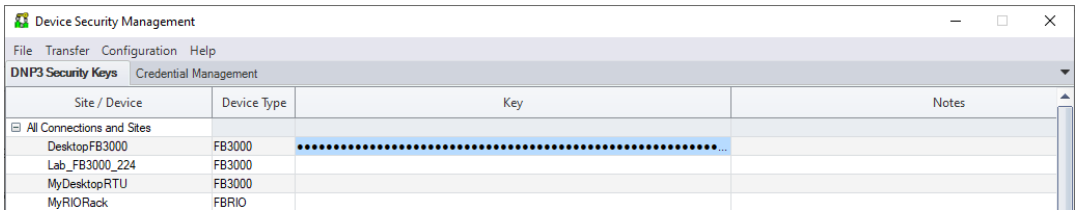
1. On the **DNP3 Security Keys** tab, click in the **Key** column for a particular device (or site).

Figure 5-2. Creating DNP Security Keys



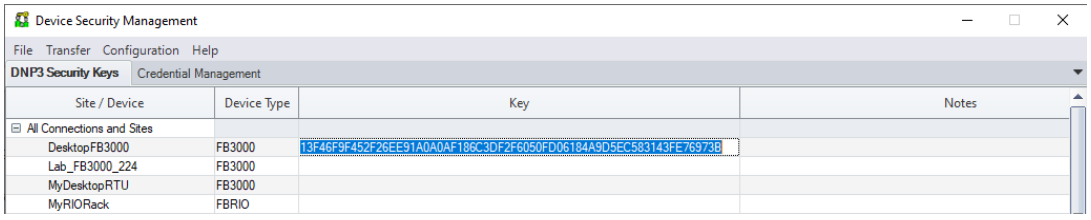
2. Click **Generate Random Key**. Device Security Management generates a DNP3 key in the **Key** column.

Figure 5-3. Generating a Random Key



3. By default, the screen hides the **Key** entry, but you can click on it to view the actual key in plain text:

Figure 5-4. Viewing the Key in Plain Text



4. You can optionally enter descriptive text in the **Notes** field such as an asset tag number. **Do not copy the key text into this field**.

5. Repeat this process to generate a key for each device.

5.3.2 Transferring DNP3 Keys to Field Tools

Once you finish generating DNP Security Keys, you need to transfer them to Field Tools, otherwise once SAV5 is enabled on an RTU, Field Tools would be unable to connect to it.

In Device Security Management, click: **Transfer > Transfer DNP3 Keys to FieldTools**

Now Field Tools **on this PC** will be ready to communicate with those RTUs once their SAv5 keys are loaded.

5.3.3 Transferring DNP3 Keys to other PCs running Field Tools

If you have other PCs running Field Tools that also need to be able to communicate with the same RTUs you created keys for on this PC, you must export the connection(s) to those devices, and then load the connection file on the other PCs. See *Section 3.11* for details.

5.3.4 Creating a DNP3 Security Target File for a Device

Each RTU implementing DNP3 SAV5 security must be loaded with a security target file (*.STF) containing the individual DNP Security key you created for it.

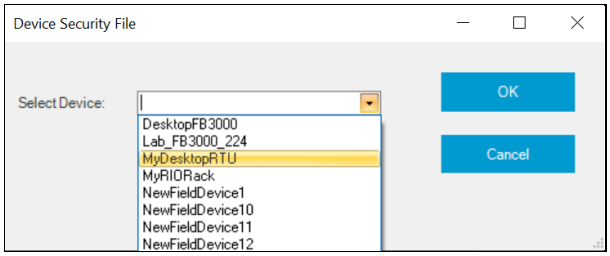
To create the target file:

1. In Device Security Management, click **Transfer > Create Security File for Target Device.** This opens the Device Security File dialog box.

Figure 5-5. Device Security File dialog box

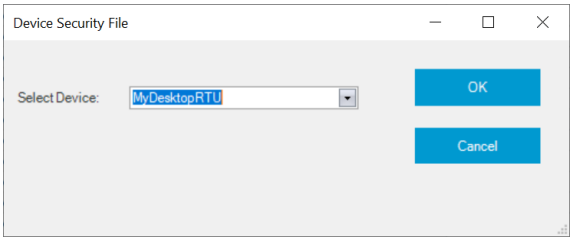
2. In the Device Security File dialog box, use the **Select Device** field to choose the device for which you want to create a target file. You can choose from any device present in the Field Tools tree.

Figure 5-6. Choosing the Device for which you want to create a target file



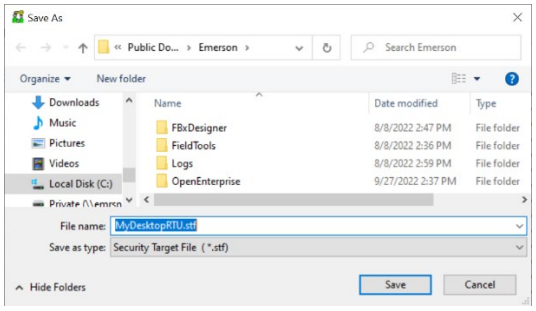
3. Click **OK.**

Figure 5-7. Confirming the selection



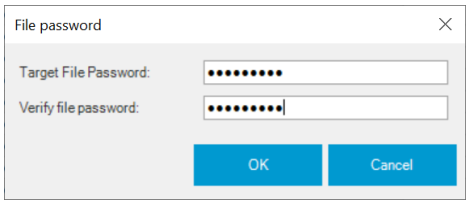
4. By default, the security target file name matches the device name. Although you can optionally change it, we recommend you keep the matching name to avoid confusion among multiple STF files. Navigate to the location where you want to save the STF file and click **Save.**

Figure 5-8. Saving the STF File

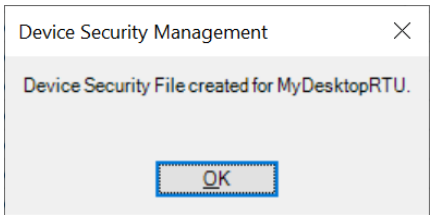


5. Device Security Management prompts you to supply a password for the STF file. Enter it in both the **Target File Password** and **Verify file password** fields and click **OK**.

Figure 5-9. Assigning a password to the Target File



6. Click **OK** when the message box confirms creation of the STF file.



7. Repeat this process for each and every RTU that requires DNP3 security keys.

5.3.5 Loading the Security Target File into the Device

Important

Once you load a DNP security key into the device, there is no way to communicate on the DNP port with that device without the key. If you should accidentally delete the connection containing the key, and if you do not have the STF file or if you forget the password for the STF file, you will not be able to communicate with the device via DNP. IN THIS SITUATION, THE DEVICE REQUIRES A FACTORY RESET. IF YOU HAVE FIRMWARE REVISION 2.17 OR NEWER YOU CAN PERFORM THE FACTORY RESET PROCEDURE DESCRIBED IN THE INSTRUCTION MANUAL FOR THE DEVICE. IF YOU HAVE OLDER FIRMWARE YOU MUST DISCONNECT THE DEVICE AND RETURN IT TO EMERSON FOR REPAIRS. To avoid this situation, ensure you save the STF file in a safe place, and that you do not lose the password for the file. Also, ensure that you

export your connections with their keys to a zipped connection file (*.ZCF) and do not lose the password for the file.

⚠ DANGER

EXPLOSION HAZARD - MAY CAUSE DEATH

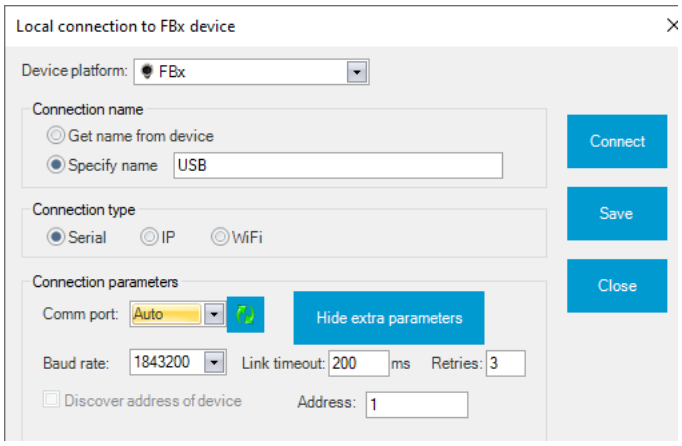
Connect or disconnect only in a non-hazardous area.

1. Connect a cable between your Field Tools laptop and the device:
   - For an FB3000 RTU, connect a USB cable between the laptop and the **USB port** on the CPU module.
   - For an FB1000 or FB2000 Series Flow Computer, connect a serial cable (or USB to serial converter cable) between the laptop and **COM1** on the flow computer.
2. In Field Tools, click **Connections > Add Connection.**
3. Create a local serial connection with the device.

   FB3000 RTU:

   - Choose **FBx** as the **Device platform**.
   - We chose a name of “USB” for the **Connection name.**
   - Set the **Connection type** to **Serial.**
   - Set the **Baud rate** and **Link timeout** as shown in *Figure 5-10*.
   - Set the correct local **Address** of the RTU.
   - If you know which COM port on your laptop is the USB port, select it in the **Comm port** field; if you do **not** know which port is the USB port, choose **Auto**, and Field Tools will cycle through the ports to find the USB port when it connects.

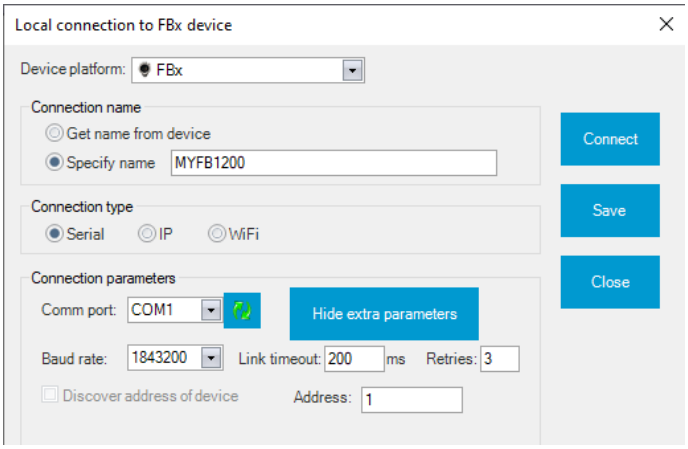
Figure 5-10. Creating a Connection to the RTU



FB1100, FB1200, FB2100, FB2200 Flow Computer:

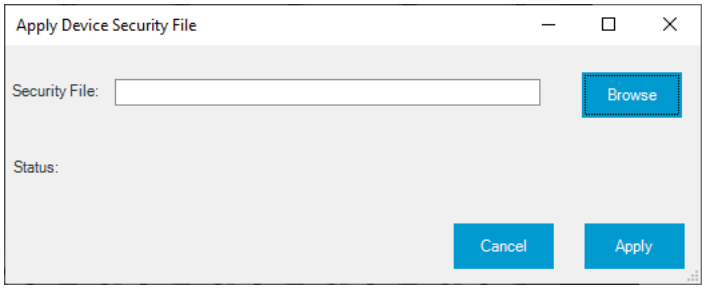
- Choose **FBx** as the **Device platform.**
- Specify a **Connection name** of your choice.
- Set the **Connection type** to **Serial.**
- Set the **Baud rate** and **Link timeout** as shown in *Figure 5-11*.
- Set the correct local **Address** of the RTU.
- **Comm port** must be **COM1.**

Figure 5-11. Creating a Connection to the Flow Computer



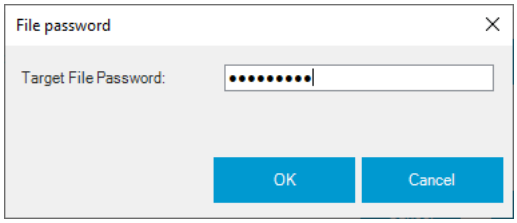
4. Click **Connect**. Field Tools initiates the connection with the device and launches FBxConnect.
5. In FBxConnect, click: **Services > Apply Security File**
6. In the Apply Security File dialog box, click **Browse** to locate the STF file for the device.

Figure 5-12. Apply Device Security File



7. Enter the **Target File Password** for your STF file and click **OK.**

Figure 5-13. Entering the Target File Password



8. Click **Apply**. FBxConnect now loads the STF file containing the DNP3 security key into the device. You should see the message “Device has been updated with the Security Key.”

Important

We recommend you do not leave Field Tools and Device Security Management running on a computer that is unattended. If you need to step away from the computer, you should save your work and shut down Field Tools and restart it when you return. This is to prevent an unauthorized user from modifying the security master file. This is similar to closing your browser after an online banking session.

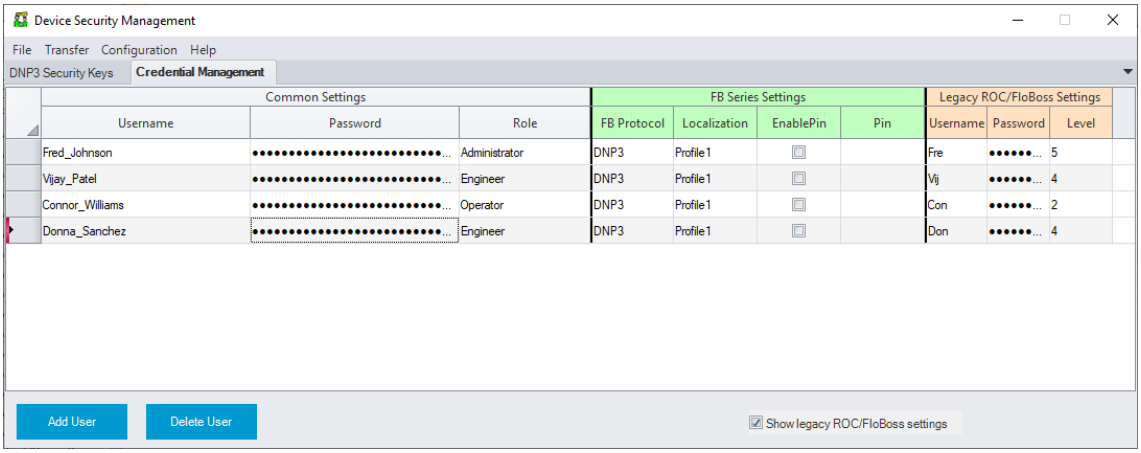
5.3.6 Disabling SAv5 in the Target RTU

1. Connect to the RTU or flow computer in the same way you would to load the key. (See *Section 5.1.5*)
2. In FBxConnect, click **Services > Disable SAv5**.

5.4 Credential Management Tab

If you purchased Credential Manager, (a licensed utility option within Field Tools) you can define users for one or more RTUs and save their access credentials in an encrypted file called the security master file. Then you can transmit that file to the RTUs in a single batch operation that updates each RTU with the same set of users and access credentials. This simplifies the task of updating multiple RTUs when you need to add or remove a user; you can just edit a single file and then update all the selected RTUs with the new file.

Figure 5-14. Credential Management Tab



Note

If you do not see the Credential Manager tab, it means you do not have the Credential Manager license for Field Tools on this PC. Normally you will only have this license if you have the role of Administrator. If you are an Administrator and purchased Credential Manager see *Chapter 6* for details on how to license the option in License Manager.

5.4.1 Security Master Files

A security master file (*.smf) is a password-protected encrypted file that holds the usernames, passwords, and associated credentials you define using Device Security Management. They make it easier to manage security information for your FB1000, FB2000, FB3000, ControlWave, ROC, and FloBoss devices. When you make security changes, you can transmit the file out to its associated RTUs and flow computers. If you have multiple geographic locations with different sets of users, you might want to have a separate security master file for each location.

Important

For an additional level of protection, we recommend you store security master files on an encrypted disk. There are numerous encryption tools available to accomplish this such as VeraCrypt, DiskCryptor, or GnuPG.

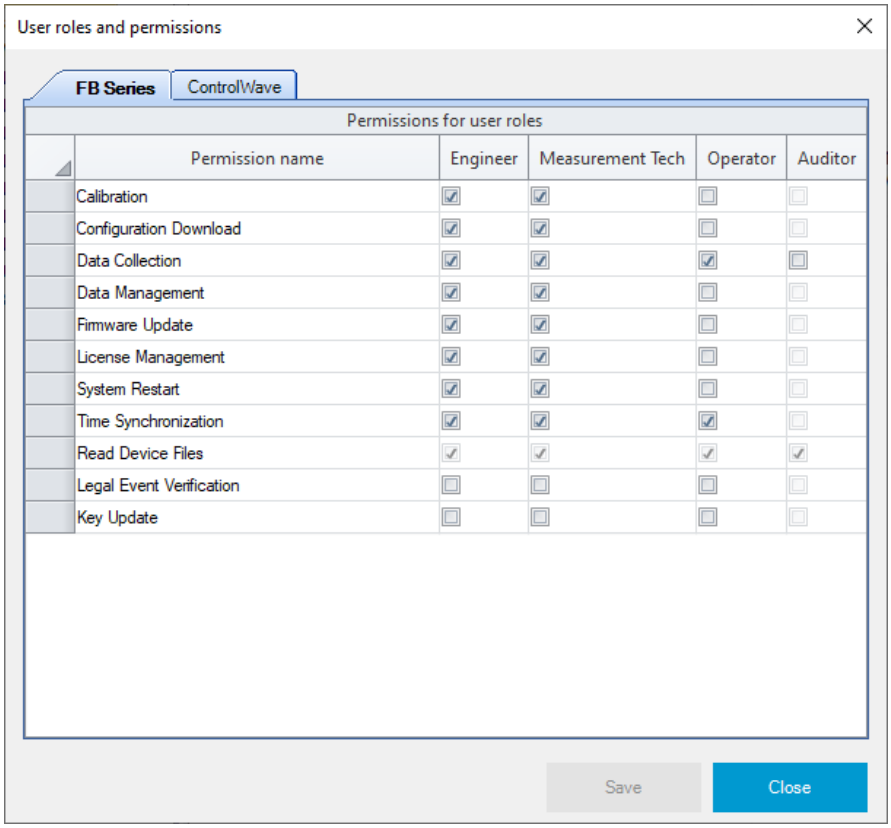
5.4.2 Defining Permissions for Different User Roles

Every user has one of five assigned roles (Administrator, Engineer, Operator, Measurement Tech, or Auditor). Administrators, by definition, have permission to perform any operation, so typically you would only have a small number of Administrators, and they would be high-level managers, and their Field Tools license would include Device Security Management. The other four roles have whatever permissions the Administrator assigns to those roles.

Only Administrators can change passwords; other roles (Engineer, Operator, etc.) cannot change their own passwords.

1. Click **Configuration > User roles and permissions** to open the User roles and permissions page.

Figure 5-15. User roles and permissions-FB1000/FB2000/FB3000 & ROC/FloBoss devices with Enhanced Security



2. For FB1000/FB2000 flow computers, the FB3000 RTU, or ROC/FloBoss devices with enhanced security, select the **FB Series** tab and assign permissions for each role. For ControlWave series RTUs, select the **ControlWave** tab and assign permissions for each role.
3. On the **FB Series** tab, in each column representing a role (Engineer, Measurement Tech, Operator, Auditor) check the boxes in the rows that correspond to permissions you want to assign to users with that role. So, for example, if you want operators to have permissions for Data Collection, Time Synchronization, and Read Device Files, check those boxes in the Operator column that are in the same row as those permission names. See *Table 5-1* for explanations of the permissions.

Table 5-1. FB1000/FB2000/FB3000 Permissions

Permission Name	Description
Calibration	Allows you to calibrate an input, verify a calibration, reset a calibration, set zero shift, and perform a plate change.
Configuration Download	Allows you to download a configuration to the device.
Data Collection	Allows you to create history, alarm, and event reports from the device.
Data Management	Allows you to create diagnostic reports and clear alarm, event, and history data from the device.
Firmware Update	Allows update the firmware on the device.
License Management	Allows you to add product licenses to and remove product licenses from the device.
System Restart	Allows you to perform a warm start or cold start of the device.
Time Synchronization	Allows you to adjust the clock on the device.
Read Device Files	Allows you read-only access to files on the device.
Legal Event Verification	Allows you to verify the configuration of the device.
Key Update	Allows you to update DNP3 security keys or disable SAv5 through FBxConnect.

4. On the **ControlWave** tab, in each column representing a role (Engineer, Measurement Tech, Operator, Auditor) check the boxes in the rows that correspond to permissions you want to assign to users with that role. So, for example, if you want auditors to have permissions for Read Data Value, Read Historical Data, and Read Stat/Diag Info Data, check those boxes in the Auditor column that are in the same row as those permission names. See *Table 5-2* for explanations of the permissions.

Figure 5-16. User roles and permissions-ControlWave

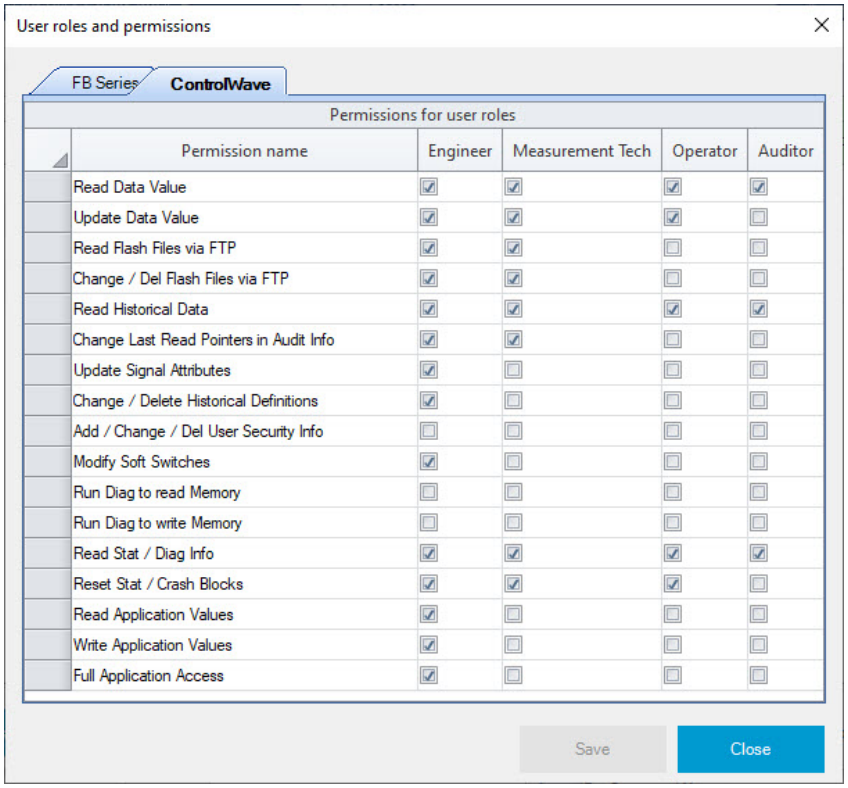


Table 5-2. ControlWave Permissions

Permission Name	Description
Read Data Value	Allows this user to read data values from this controller.
Update Data Value	Allows this user to change data values in this controller.
Read Flash Files via FTP	Allows this user read access (via File Transfer Protocol) to files stored in this ControlWave's flash memory. This could include the ControlWave boot project, source files (*.ZWT), etc.
Change / Del Flash Files via FTP	Allows this user (via File Transfer Protocol) to add, change or delete files stored in the ControlWave's flash memory. This could include the ControlWave boot project, source files (*.ZWT), etc.
Read Historical Data	Allows this user to view historical data (Audit / Archive information) from the controller, either via web pages, or OpenBSI DataView.
Change Last Read Pointers in Audit Info	Allows the user to delete Audit Trail data from the controller.
Update Signal Attributes	Allows this user to modify the status of inhibit / enable flags in the controller.
Change / Delete Historical Definitions	Allows this user to add, change or delete historical definitions via the Flash Configuration Utility.

Permission Name	Description
Add / Change / Del User Security Info	Allows this user to add, change, or delete security configuration information via the Flash Configuration Utility.
Modify Soft Switches	Allows this user to change soft switch values on the soft switches page of the Flash Configuration Utility.
Run Diag to read Memory	Allows this user to run diagnostics to read memory at the controller.
Run Diag to write Memory	Allows this user to run diagnostics to write to memory at the controller.
Read Stat / Diag Info	Allows this user to view communication statistics and other information on the Statistics web pages.
Reset Stat / Crash Blocks	Allows this user to reset statistics and crash block areas on the Statistics web pages.
Read Application Values	Allows this user to read values using the ControlWave Designer OPC Server.
Write Application Values	Allows this user to modify values using the ControlWave Designer OPC Server.
Full Application Access	Allows this user full privileges to perform debugging operations in ControlWave Designer.

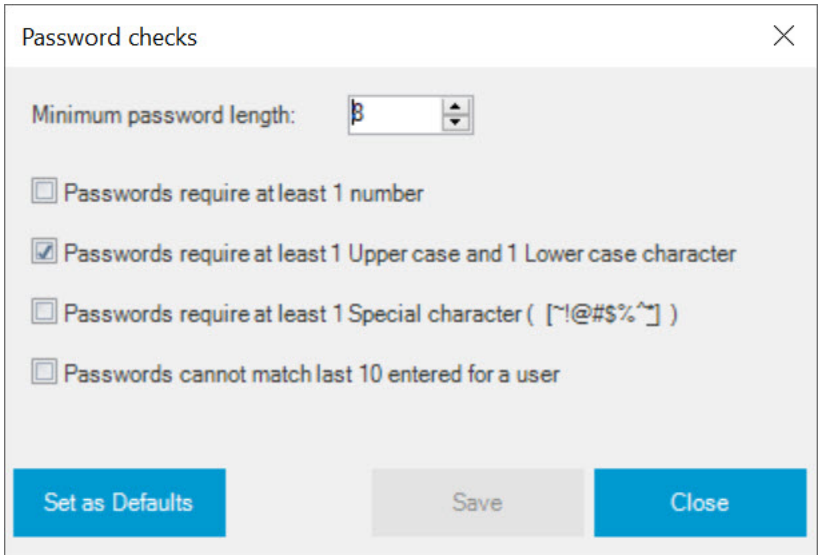
5. Click **Save** to update the permissions assigned for the roles.

5.4.3 Applying Rules for Password Creation

One way to increase your security is to make sure that you create passwords that are more complex. Credential manager supports some rules that you can choose to enforce for password creation.

1. Click **Configuration > Password Checks** to open the Password checks dialog box.

Figure 5-17. Password checks dialog box



2. You can define the **Minimum password length**. Longer passwords are more secure. The password length for FB1000, FB2000, and FB3000 devices, as well as ROC/FloBoss devices using enhanced security can range from 8 to 32 characters. ControlWave passwords can range from 8 to 16 characters; any additional characters are not read. Some security certification organizations recommend you use at least 12 characters.
3. Other password rules you can enforce:
   - **Passwords require 1 number** means that passwords must include at least one number from 0 to 9.
   - **Passwords require 1 Upper case and 1 Lower case character** means the password must include at least one UPPER CASE and at least one lower case character.
   - **Passwords require 1 Special character** means that the password must include at least one of the following characters: ~!@#$%^*
   - **Passwords cannot match last 10 entered for a user** requires that the password defined cannot match any of the last 10 passwords that were defined for this user.
4. When you complete your choices, click **Set as Defaults** to indicate that choices will be used as defaults for future smf files you create.
5. Click **Save** to save your choices in the smf file and exit the dialog box, or **Close** or **Cancel** to discard your selections and exit the dialog box.

5.4.4 Adding Users

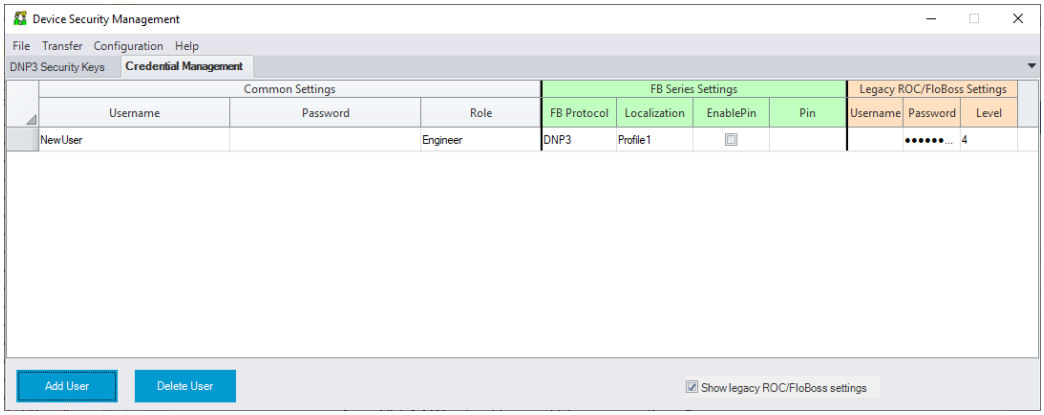
As an Administrator, after you specify what permissions you want to assign to particular roles (*Section 5.4.2*) and you decide what kinds of passwords you want to allow (*Section 5.4.3*), you can start adding users.

Note

While you define passwords or pins for any device type, you can click see the plain text while you type it in. At all other times, the text is blacked out.

1. On the Credential Management tab, click **Add User** to add a row which you can configure.

Figure 5-18. Adding Users



2. Click on “new user” in the **Username** column, and type in the name for the user. Usernames for FB1000/FB2000/FB3000 devices as well as ROC/FloBoss devices using enhanced security can be up to 30 characters. Usernames for ControlWave devices can be up to 16 characters; any additional characters are not read. Usernames cannot include spaces.
3. Click in the **Password** column and enter the password this user will use when logging into the RTU. Passwords for FB1000/FB2000/FB3000 as well as ROC/FloBoss devices using enhanced security support up to 32 characters. Passwords for ControlWave devices can be up to 16 characters; any additional characters are not read. If you saved password rules as defaults in the Password checks dialog box (*Section 5.4.3*) the tool enforces those rules in a later step when you save your entries.
4. Click in the **Role** column and use the drop down to select the desired role (Administrator, Engineer, Measurement Tech, Operator, or Auditor). The permissions associated with each role are configured in the User roles and permissions page (*Section 5.4.2*).

5. When communicating with an FB1000/FB2000 flow computer, you can specify parameters used when someone connects to the device through the local HMI display:
   - **Protocol –** Click and use the dropdown to select the communication protocol used for a local connection to the device. Choices include DNP, FBxNet, ROC, or BSAP protocol. (This field also applies to FB3000 devices.)
   - **Localization** – Select the desired localization profile which sets the language used in the HMI display. (Future)
   - **Enable pin** – Check this to require that someone using the HMI display on the flow computer must enter a four digit pin.
   - **Pin –** Type the pin this user must enter when using the local HMI display.
6. For legacy ROC/FloBoss devices or newer ROC 800, FB107, DL8000 devices not yet configured for enhanced security, ensure the **Show legacy ROC/FloBoss settings** box is checked. Define credentials as follows:
   - **Username –** Usernames for these devices are three characters long. This column displays the first three characters of the full username defined in Step 2. You cannot change it without changing the full username.
   - **Passwords** – Passwords must be numbers. You can use 1 to 4 digits to represent the number. If after you enter the password you want to edit it, be sure to click so the entire field is selected – then you can enter a new password.
   - **Level** – Select the level from the dropdown (0 to 5). The higher the number, the greater the level of access allowed. Repeat these steps for each user you want to create. When finished save the user information. **Note**: Changing the Role on the FB Series tab changes this number, but you can change it back in this field.

5.4.5 Deleting an Existing User

1. Click in the row for a user so that the entire row for that user is selected and there is a little arrow pointing at the username. If you want to delete multiple users, hold down the **Ctrl** key while you select additional users.
2. Click **Delete User**.
3. Click **Yes** to confirm that you want to delete the user(s), or click **No** to keep the user(s).

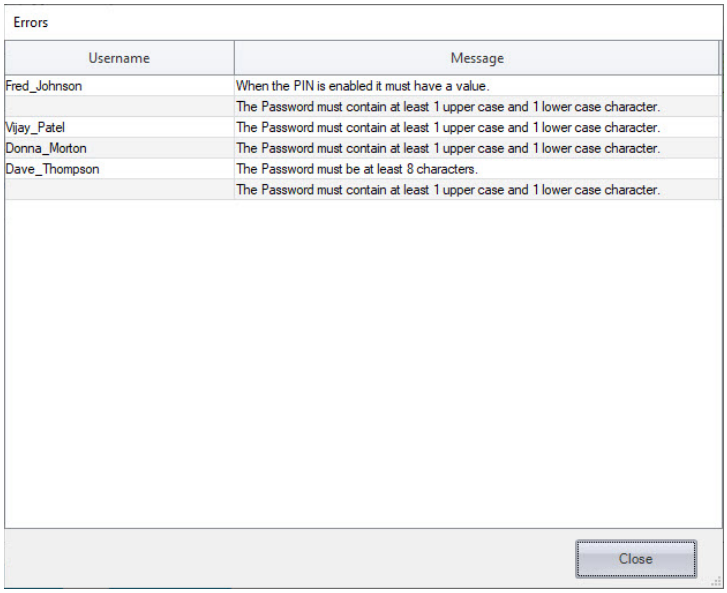
5.4.6 Saving Your Usernames, Passwords, and Credentials in a Security Master File

Once you finish adding users, you must save them in a security master file (*.smf).

1. Click **File > Save**.

Note
If an error window opens, it means the password rules selected earlier detected a problem with the password associated with the listed username. Review the error message(s), then close the error window and correct the passwords for those usernames so it conforms to the chosen rules.

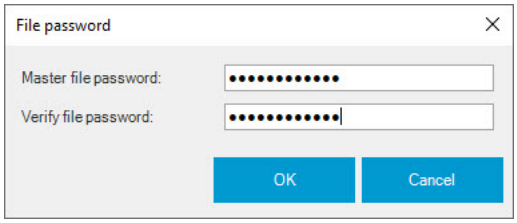
Figure 5-19. Error Messages



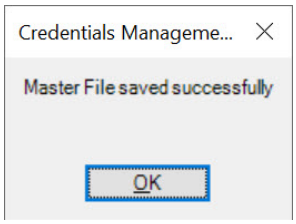
2. Navigate to the location on the PC where you want to store the security master file, and specify a name for the file.
3. In the File password dialog box, specify a master password for the security master file in the **Master file password** field, and then enter it again in the **Verify file password** field.

Important
If you forget your master password, there is no way to retrieve the information in the security master file.

Figure 5-20. File password dialog box



4. Click **OK** when finished, or **Cancel** to return to the credential manager.
5. When you save the file, you will see a confirmation message; click **OK** at the prompt.



Important

We recommend you do not leave Field Tools and credential manager running on a computer that is unattended. If you need to step away from the computer, you should save your work and shut down Field Tools and restart it when you return. This is to prevent an unauthorized user from modifying the security master file. This is similar to closing your browser after an online banking session.

5.4.7 Opening an Existing Security Master File

1. Click **File > Open**.
2. Navigate to the location on your PC where you store security master files, click on the filename, then click **Open**.
3. Enter the master file password for that file, and click **OK**. You can now view/edit the file.

5.4.8 Saving a Copy of the current Security Master File under a different name

1. Click **File > Save As**.
2. Navigate to the location on the PC where you want to store the new security master file and specify a name for the file.
3. In the File password dialog box, specify a master password for the security master file and repeat it in the verify field. If you need to edit the password after you type it, be sure to highlight the entire field before you start typing.

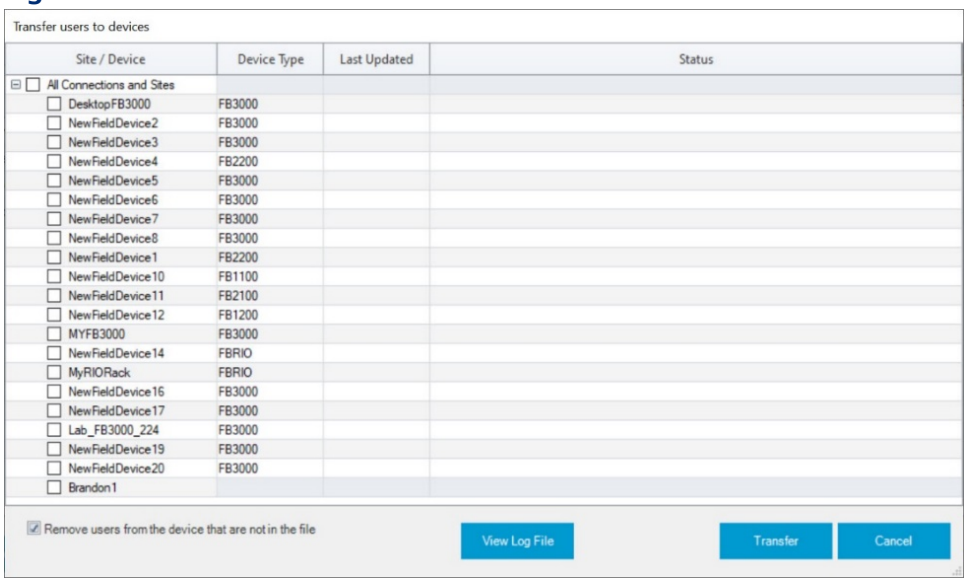
4. Click **OK** when finished or **Cancel** to return to credential manager.
5. When you save the file, you will see a confirmation message; click **OK** at the prompt.

5.4.9 Transmitting the Security Master File to Your RTUs and Flow Computers

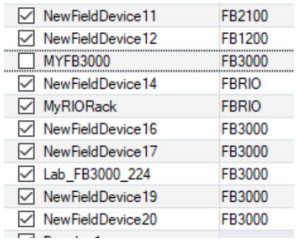
Once you open a completed security master file, you can transmit it to a selected group of RTUs and flow computers.

1. Click **File > Transfer to devices** to open the Transfer users to devices page.
2. In *Figure 5-21:*
   - The **Site/Device** column shows all the connections, sites, and devices in your current Field Tools configuration.
   - The **Device Type** field shows the type of RTU/flow computer.
   - The **Last Updated** field shows the last time this RTU/flow computer received an updated security master file.

Figure 5-21. Transfer users to devices



6. Select the devices to which you want to send the security master file. If you click on a site name, it automatically selects all the devices for that site. If you click on **All connections and sites**, it automatically selects every device. If you see a device selected that you do not want to update, un-check it.



7. If you want to delete users from devices if they are not defined in this security master file, select **Remove users from the device that are not in the file**. Those user accounts will be deleted from the devices.
8. When you finish making your selections, you can transmit the security master file to the selected RTUs and flow computers. Click **Transfer** to send the file.
9. The **Status** field shows the status of the file transmission to each of the selected RTUs and flow computers. You can click **View Log File** to see all status messages associated with the file transmission. Timestamps of the last transfer and error messages associated with the transfer are stored in the Field Tools database so they can be read and displayed the next time you invoke the tool.

Important

We recommend you do not leave Field Tools and Device Security Management running on a computer that is unattended. If you need to step away from the computer, you should save your work and shut down Field Tools and restart it when you return. This is to prevent an unauthorized user from modifying the security master file. This is similar to closing your browser after an online banking session.

Chapter 6. Using License Manager

6.1 Licensing Optional Components

If you purchase optional components such as FBxDesigner, FBxNet, or Credential Manager, you must license them through License Manager.

Important

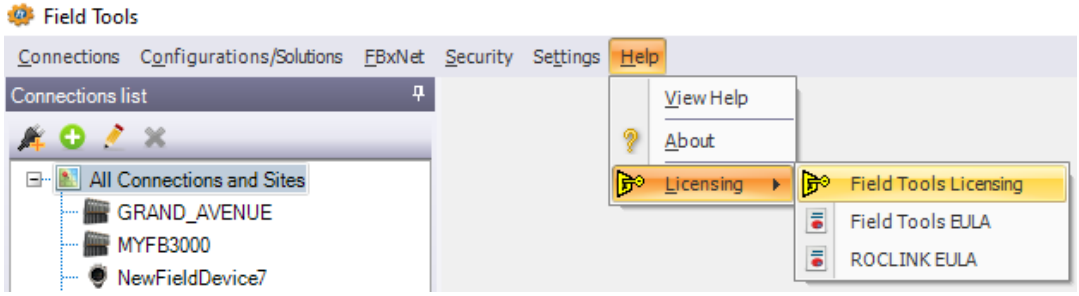
Do not confuse License Manager with the Emerson FBxConnect Licensing Tool. The Licensing Tool is for purchased applications that run on an **FB3000 RTU**. License Manager is for software that runs on the **Field Tools workstation**.

Note

If launching the Licensing Manager through a newer browser such as Edge, you must run the browser in IE mode.

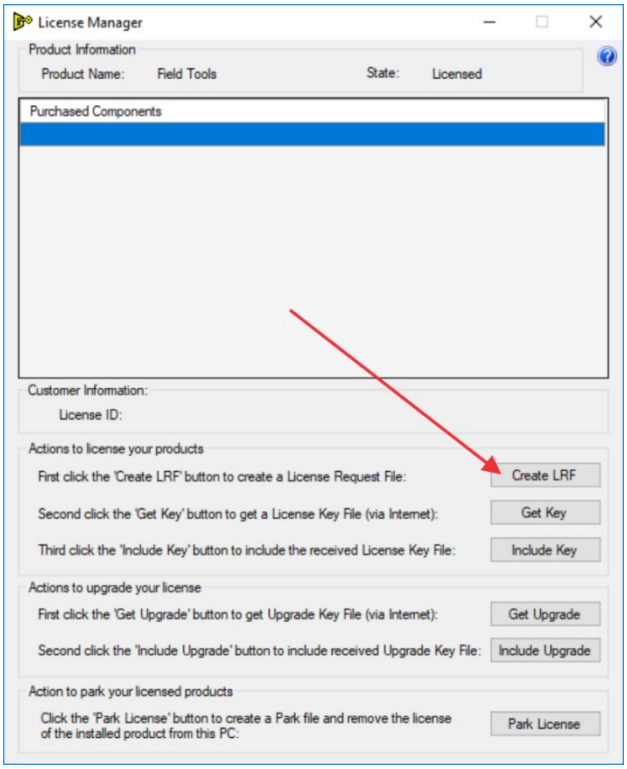
1. Within Field Tools, click **Help > Licensing > Field Tools Licensing**.

Figure 6-1. Calling Up the License Manager



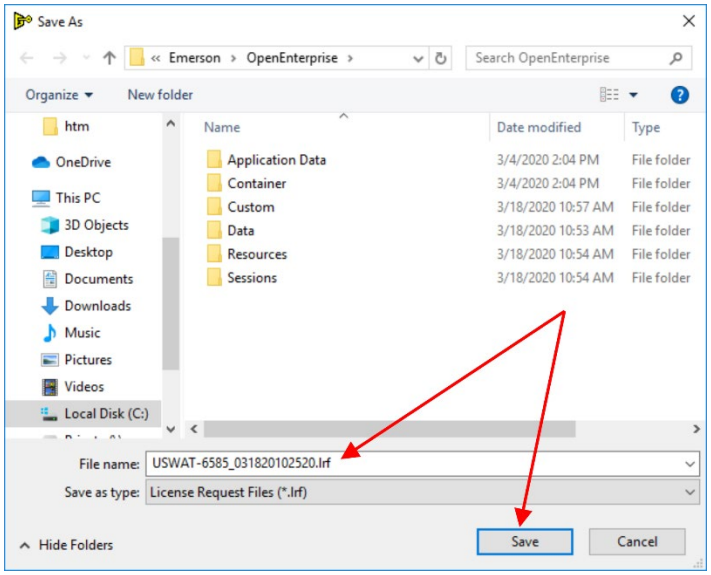
2. When the License Manager opens, click **Create LRF**.

Figure 6-2. Creating the LRF File



3. The License Manager prompts you to save the LRF file. (Make sure you make note of where you save it, before you click **Save** because you will need it later.

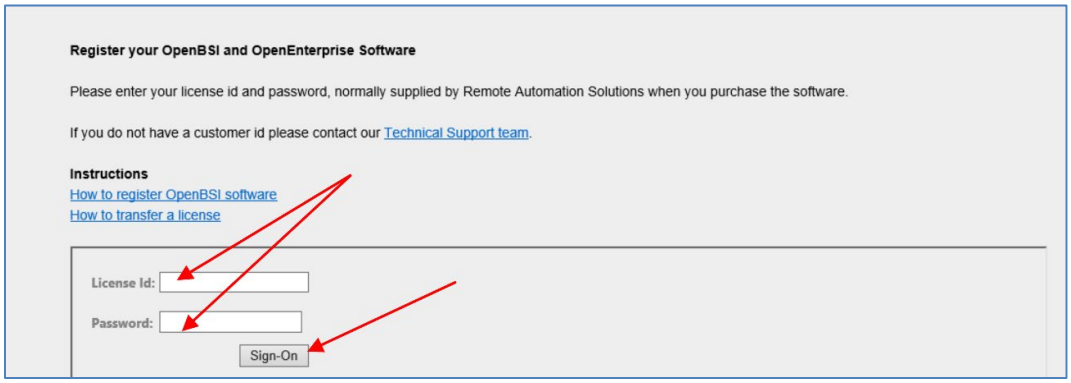
Figure 6-3. Saving the LRF File



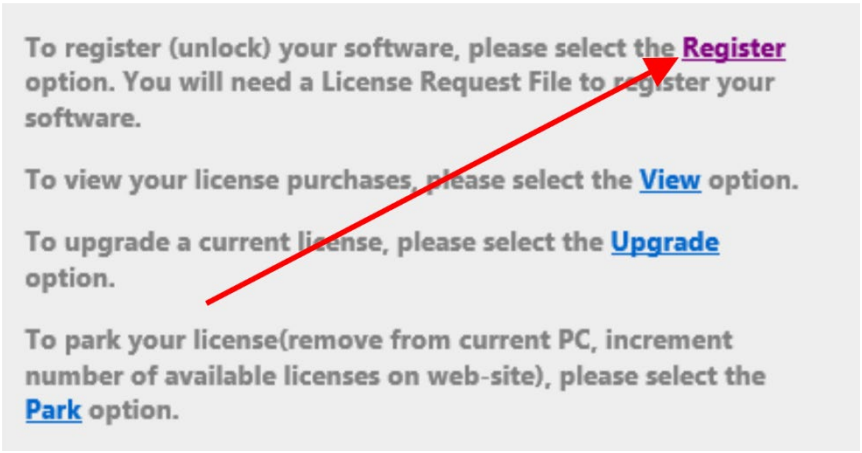
4. Now click **Get Key** in the License Manager.

5. On the registration page, enter your **License Id** and **Password** you received with your purchase and click **Sign-On**.

Figure 6-4. Signing on with your License Id and Password

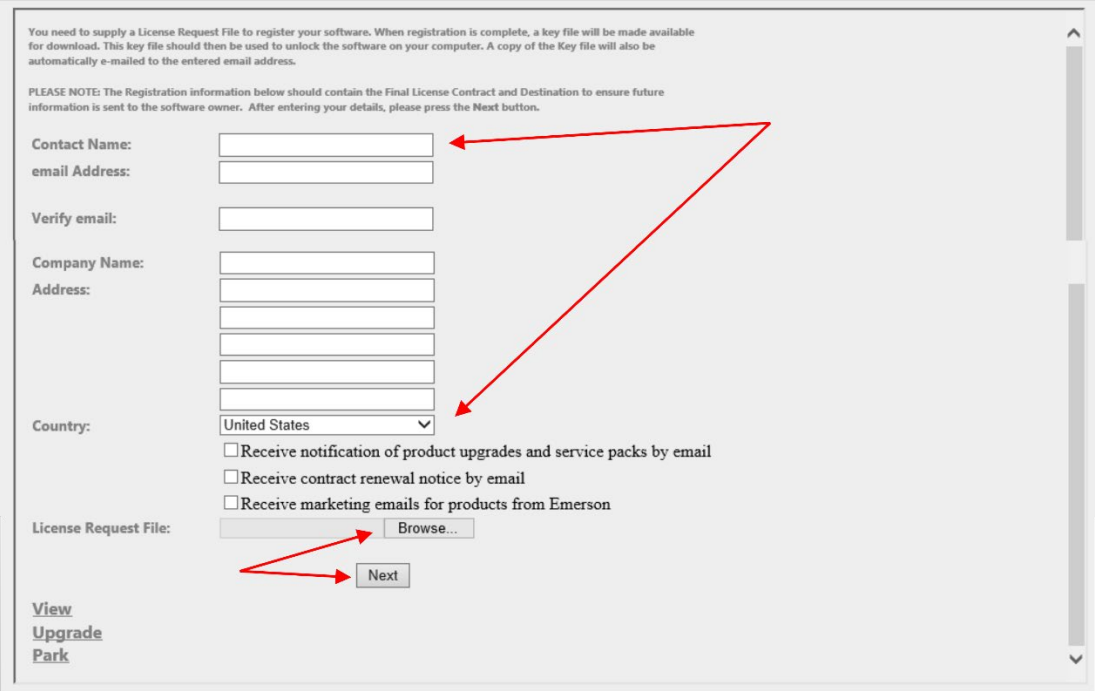


6. When you sign on successfully, click the **Register** link.



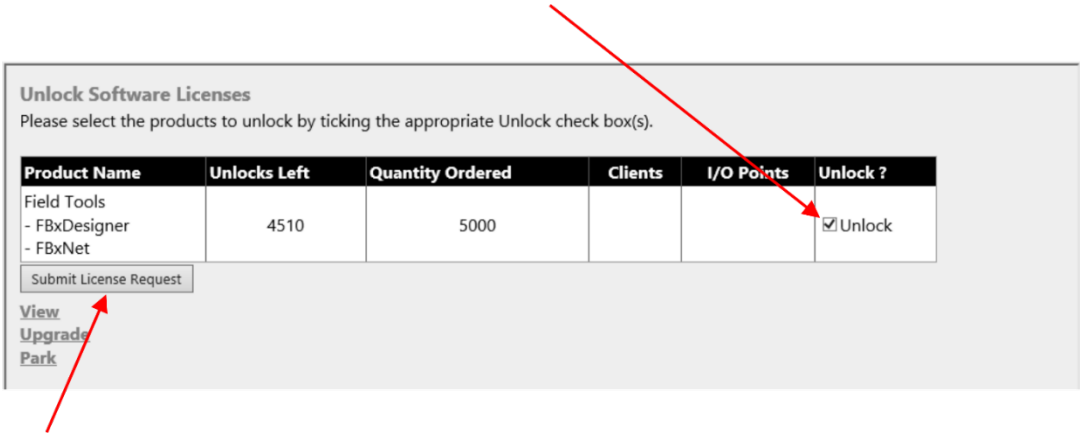
7. Now enter your contact information, email, and other details in the upper part of the page and use the scroll bar to reach the lower fields. Then click **Browse** to select the license request file (LRF) you saved in Step 3 and click **Next**.

Figure 6-5. Entering Contract Details and Selecting the LRF File



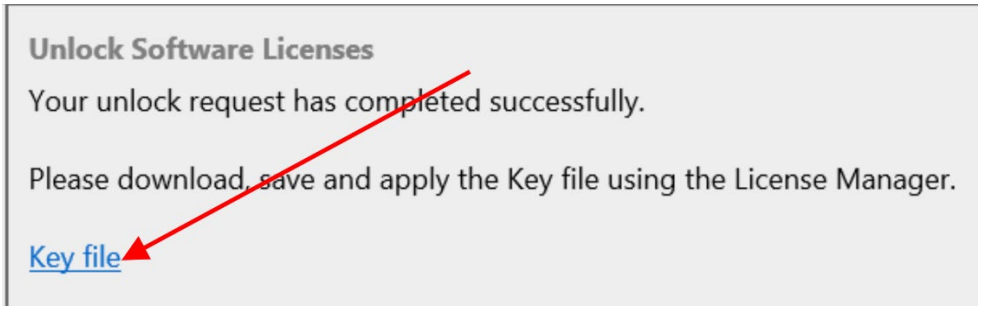
8. From the Unlock Software Licenses page, click **Unlock** for the item you want to unlock, then click **Submit License Request**.

Figure 6-6. Unlock Software Licenses and Submit License Request



9. A page opens with a Key file link from which you can download your key file. The website also sends a copy of the key file to the email address you specified with your contact information.

Figure 6-7. Download the Key File

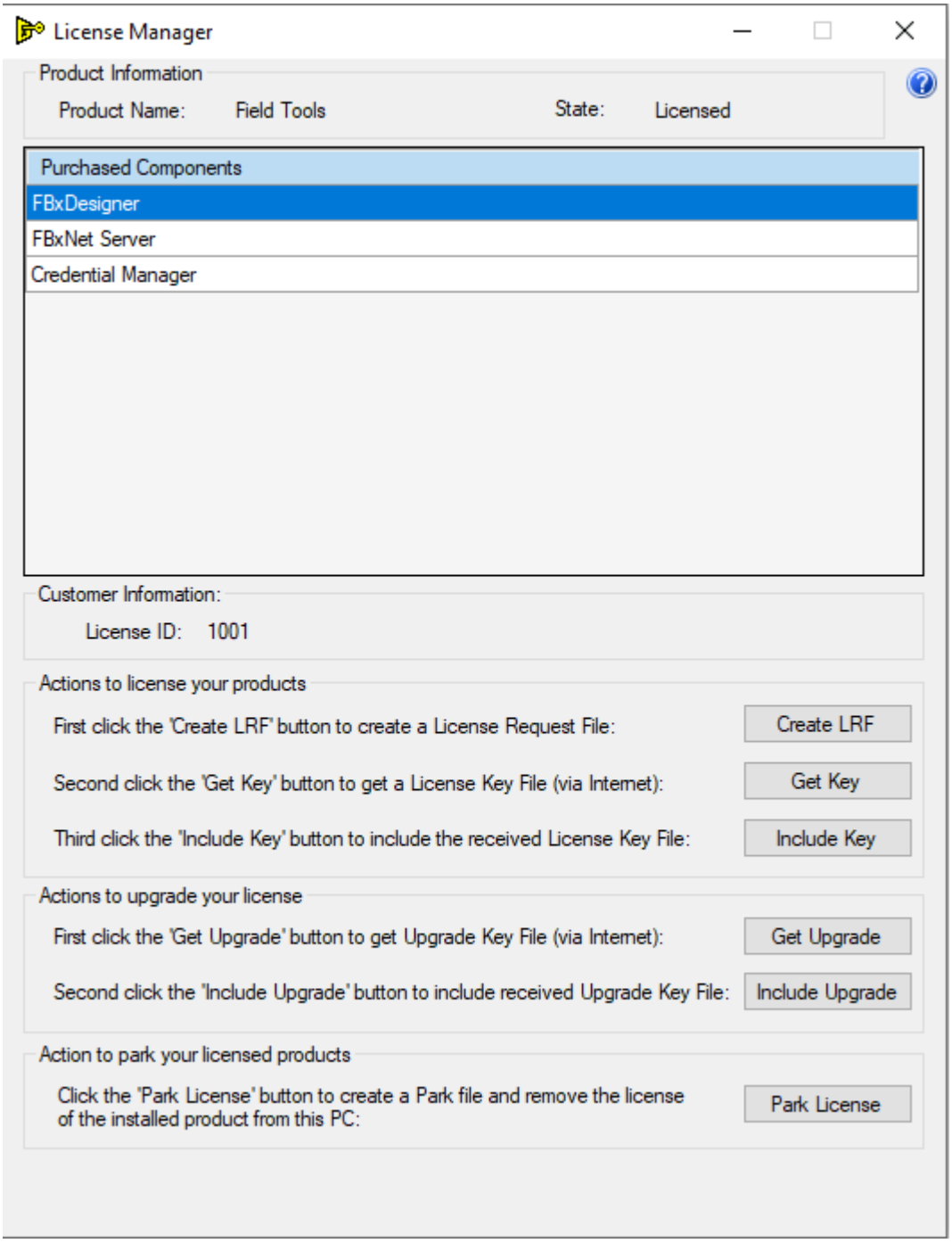


Important

- If you use Microsoft® Internet Explorer 9, it automatically saves your key file with a .TXT extension. License Manager handles the .TXT extension; do not change the extension or the file may become unusable.
- If you right-click on the Key File link and select the **Save Target** as context menu item, the key file is saved with an .XML extension.
- The e-mailed key file has an extension of .KEY.
- License Manager handles .KEY, .TXT, and .XML extensions.

10. To apply the license, click **Include Key** in the License Manager (see *Figure 6-2*). Browse to the location of your key file and click **Open** to apply the key file. Your purchased options are now licensed.

Figure 6-8. Licensed Components



6.1.1 Re-assigning a License to another PC (Parking a License)

If you license a component (FBxDesigner, Credential Manager, FBxNet, and so on) on a particular PC and then decide you want to re-assign the license to a different PC, you can

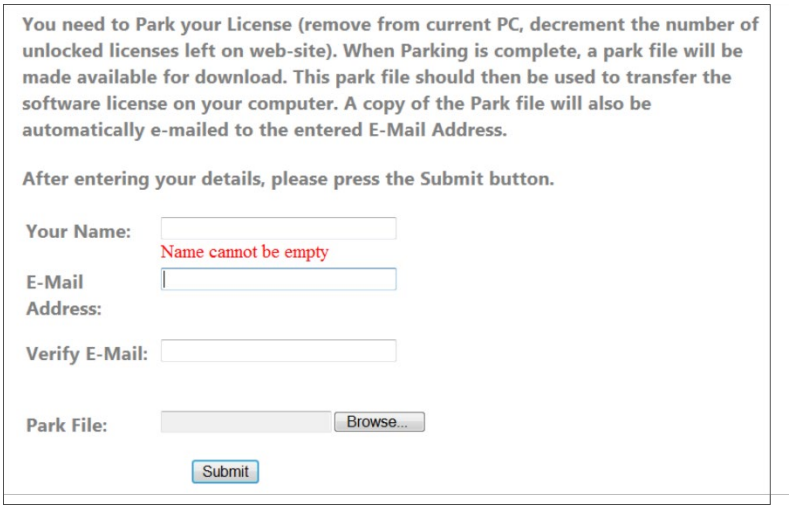
remove the license from the first PC and then temporarily “park” that license on the License Registration website. This restores the license to your total number of purchased licenses, and you can then assign it to the new PC through the normal license registration procedure.

Important

Once you park a license (which removes it from the original PC) **you cannot assign a new license to that same PC without first contacting our Technical Support personnel** for codes to restore the demo period for that PC. The technical support phone number in the U.S. is: 1-800-537-9313; for international numbers use this link: https://www.emerson.com/en-us/automation/guardian/technical-support-contact-information/ Alternately, log into Guardian at this link: https://guardian.emerson.com/login

1. To start the License Manager, either click **Help > Field Tools Licensing** from the menu bar in Field Tools.
2. Click **Park License** and save the PRK file. Make note of the location because you need to access the file in a later step.
3. Click **Get Key** to go to the License Registration website.
4. Enter your **License Id** and **Password** and then click **Sign-On**.
5. Click the **Park** option; this removes the license from the current PC.

Figure 6-9. Parking a License



6. Enter your name in the **Your Name** field; and enter your e-mail address in both the **E-Mail Address** and **Verify E-Mail** fields. This is the address to which the licensing website sends your key file.
7. Use the **Browse** button to locate the **Park File** you created in Step 2.

8. Click **Submit**. When the website accepts the park file, it shows the message **Park File Operation Completed Successfully**.

Exit the License Manager. You can now re-assign the license to a different PC by following the licensing procedure on the new PC.

Appendix A - Troubleshooting Tips

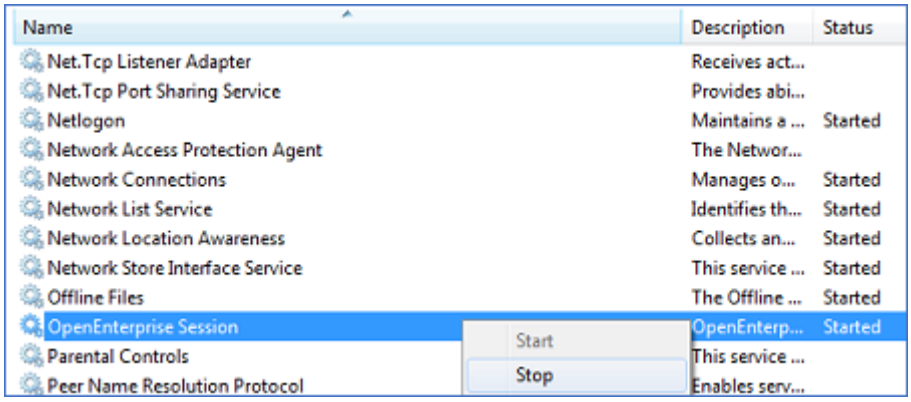
The following are some common problems that may occur and procedures for resolving them.

Message: *Failed to connect to Comm Manager*

You may see this message if something disrupts a communications connection. (Because they share some common code, Field Tools makes use of an OpenEnterprise session to communicate.) Stop and re-start the OpenEnterprise session using these steps:

1. In Windows Control Panel, double-click **Administrative Tools**.
2. Double-click **Services**.

Figure A-1. OpenEnterprise Services



3. Right-click on the OpenEnterprise Session and choose **Stop** from the menu.
4. Right-click on it again and choose **Start** from the menu.

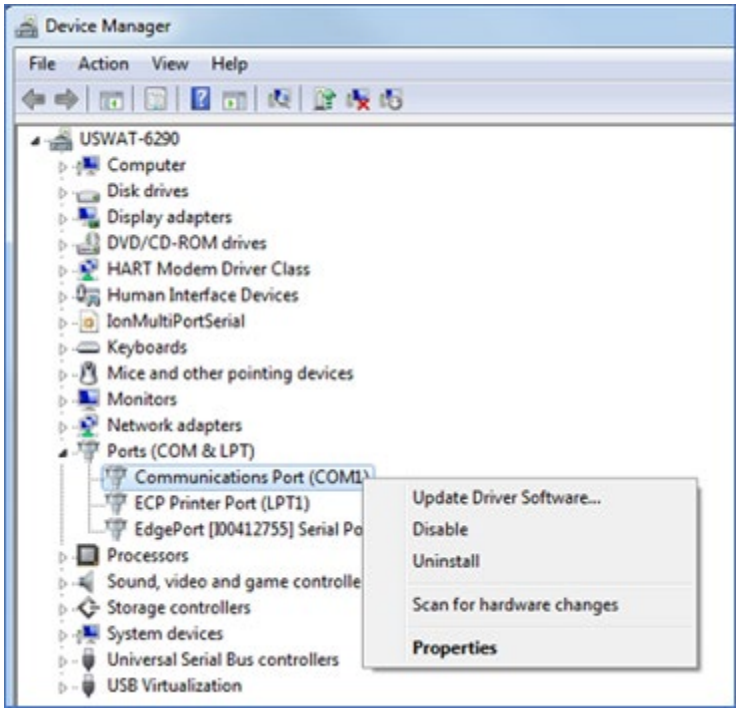
Communication Problem Causing Truncated Messages

If you use RTS/CTS with radios and encounter a problem where Field Tools can transmit but RTUs are unable to respond, it could be related to PC port configuration in Windows which results in messages being truncated.

If this problem occurs, follow these steps:

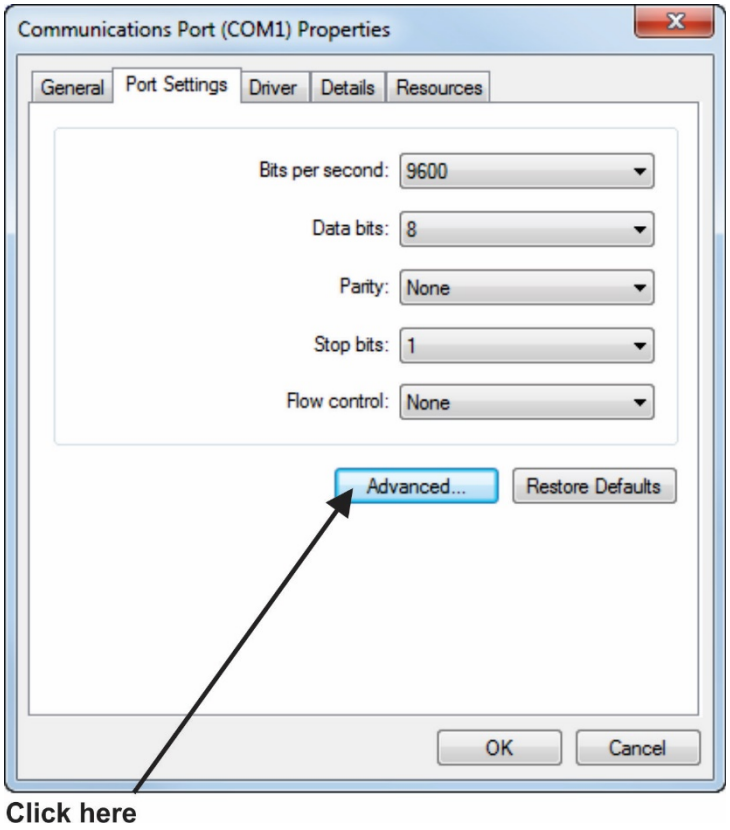
1. Open the Windows Control Panel.
2. Click **Device Manager.** The Device Manager dialog opens.

Figure A-2. Device Manager



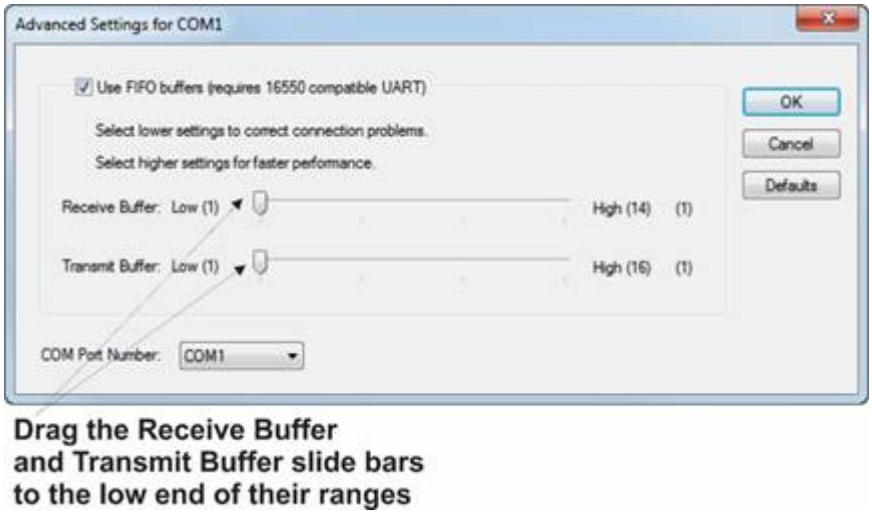
3. Expand the **Ports (COM & LPT)** selection to display a list of ports.
4. Right-click once on the port used for Field Tools communications and choose **Properties** from the pop-up menu. The Communications Port (COM1) Properties dialog box opens.

Figure A-3. Device Manager



5. Select the **Port Settings** tab, then click **Advanced** to display the Advanced Port Settings dialog box.

Figure A-4. Advanced Comm Port Settings Dialog



6. In the Advanced Port Settings dialog box, drag the Receive Buffer and Transmit Buffer slide bars to the low end of their ranges, and click **OK**.

7. Choose **OK** in the Communication Port Properties dialog box, and exit the Device Manager and Control Panel to save the settings.
8. Reboot your PC for the new settings to take effect.

USB to RS-232 Serial Connection Problems

USB to RS-232 serial converters vary widely in quality and performance. Other customers have reported good results with the following converters:

- BlackBox IC199A
- IOGear® GUC232A
- FDI's CHIPI-X10

If you experience problems with a particular USB to serial converter, there are a few things you can try:

- Make sure you installed the correct up-to-date software driver for your USB to serial converter. Sometimes a driver update can solve the problem.
- If the connection failure occurs after you unplug and plug back in, close the connections and unplug the USB from the PC. Then reconnect the USB and restart the connection.
- Some problems can occur from truncated messages. In Windows Device Manager, set FIFO transmit and receive buffers for the port to low as described above in Communication Problem Causing Truncated Messages. This may improve the USB connection.

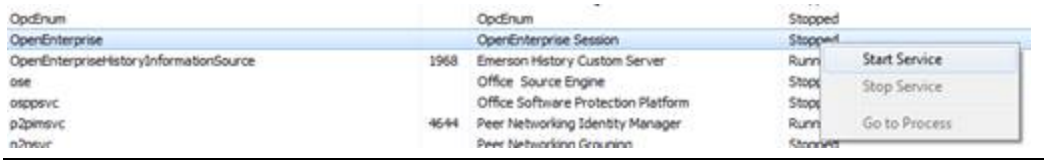
VPN Causes Certain Features to Fail

- When connecting to a virtual private network (VPN) certain features in Field Tools may fail to operate correctly.
- Connecting to a VPN shuts down certain Windows services that Field Tools uses. (Because they share some common code, Field Tools makes use of an OpenEnterprise service.) While some services can reconnect automatically, others may require you to restart the OpenEnterprise service. If you need to do this, follow these steps:

  1. Launch Windows Task Manager.
  2. Select the **Services** tab.

3. Right-click on the **OpenEnterprise** service and choose **Start Service**.

Figure A-5. Start Services



4. The OpenEnterprise service restarts; features should now operate correctly.

Overlapping or Truncated Screen Items

If display settings in Windows Control Panel are set for larger fonts, you may see certain text items truncated (cut off) on the screen, or there may be overlapping between text items.

To solve this, set display settings in Windows Control Panel to use smaller text sizes.

Cannot Communicate with Device After Configuration Download or Cold/Warm Start

In some cases, after you download a configuration or perform a cold/warm start, FBxConnect cannot communicate with the device because the device reboot takes longer than expected, resulting in a communications timeout. If these timeouts occur, you can increase the amount of time FBxConnect waits for communications to be established with the device following a reboot.

To do this, you need to edit the values for the BootTimeAfterConfigApply and BootTimeAfterColdWarmStart parameters. These parameters specify the amount of time (in minutes) FBxConnect waits after a device reboot before declaring a communications timeout failure.

These parameters are located in the FieldToolsContainer.config file located in the folder:

```
\ProgramData\Emerson\OpenEnterprise\Application Data\
```

In the example shown below, FBxConnect waits 5 minutes after a configuration download and waits 6 minutes after a cold or warm start before declaring a communication timeout.

```
 <appSettings>
       <clear />
       <add key="BootTimeAfterConfigApply" value="5" />
       <add key="BootTimeAfterColdWarmStart" value="6" />
</appSettings>
```

Incorrect Timestamp in FBxConnect Logs

Once you install Field Tools software, the software begins using the configured time zone in Windows when generating time stamps for historical data/logs. If you subsequently **change** the Windows time zone, you must **re-boot** your PC workstation for Field Tools to recognize the time zone change so it can be reflected in logs and historical data.

Wi-Fi connections Incompatible with FIPS

The encryption algorithm used for Wi-Fi passwords in Field Tools and FB1000/FB2000 Series Flow Computers is newer than the Federal Information Processing Standard (FIPS) standard and so is incompatible with it.

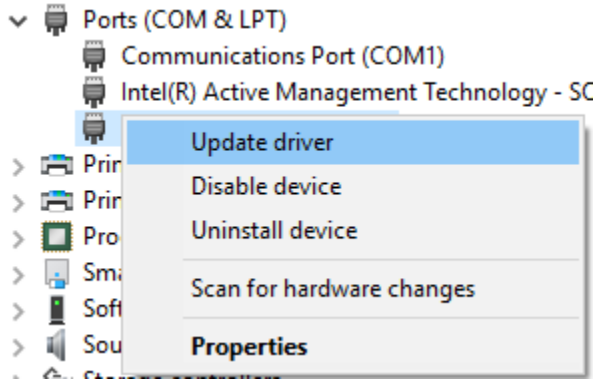
To prevent errors associated with this, you must disable (de-select) the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** option for the Local Security Policy of your laptop/PC workstation.

FBxConnect USB Driver Installation Issues

Sometimes the USB CDC driver does not install correctly. If that happens, follow these steps:

1. Launch the Windows Control Panel.
2. Click Device Manager.
3. Select Ports. Locate the CDC Serial Driver and right click on it, and choose **Update Driver**.

Figure A-6. Updating Driver

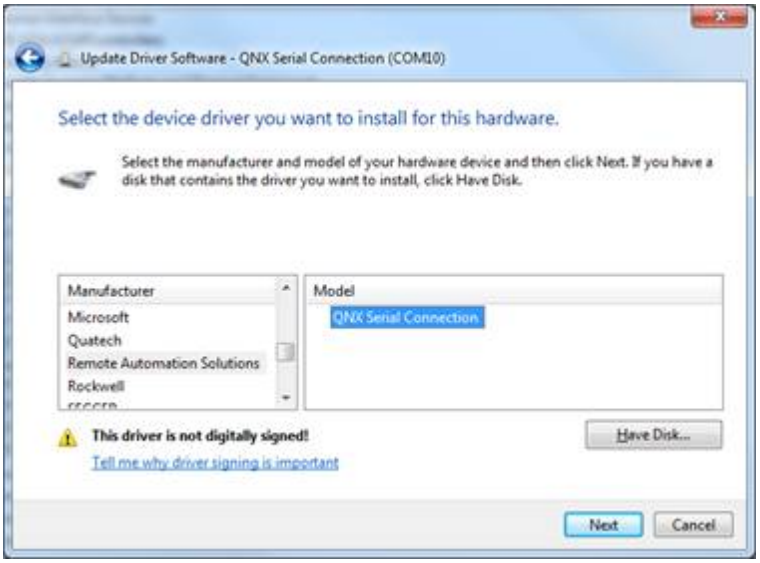


4. A new screen opens. Click **Browse my computer** for driver software.

5. From the next screen, choose **Let me pick from a list of available drivers on my computer**.

6. From the list presented, choose **Remote Automation Solutions** as the **Manufacturer** and **QNX Serial Converter** as the **Model**, then click **Next** and Windows reinstalls the driver.

Figure A-7. Updating Driver



Number of Supported ROCLINK Connections

Even though ROC devices support 6 active IP/TCP connections, launching ROCLINK from Field Tools limits the connections to 3. This is because one connection is made by Field Tools (to locally connect to the device and start ROCLINK) and the other connection is made by the ROCLINK application.

Message: *Comm Manager Connection Lost*

If the Connection Progress field on the Properties page for the connection reports this message, it may indicate a conflict between Field Tools and other software for the same TCP sockets. Edit the file **c:\Users\Public\Documents\Emerson\FieldTools\Application Data\CommManager.Config**

```
<appSettings>
  <clear />
  <add key="CCListenPort" value="40000" />
  <add key="DriverBaseListenPort" value="40010" />
  <add key="VPCListenPort" value="40001" />
  <add key="AmsGatewayListenPort" value="40004" />
  <add key="HartIdListenPort" value="40005" />
  <add key="AmsComListenPort" value="20001" />
  <add key="RasAdminTaskListenPort" value="40002" />
  <add key="DBBuildServer" value="40006" />
```

Change the **CCListenPort** value to 50000, the **DriverBaseListenPort** value to 50010, the **VPCListenPort** value to 50001, the **RasAdminTaskListenPort** value to 50002, and the **DBBuildServer** value to 50006.

To make the changes take effect, stop the OpenEnterprise Session, then re-start the OpenEnterprise Session. For information on how to do this, see the first troubleshooting tip in this appendix.

Note
If you subsequently reinstall Field Tools you must redo these changes.

A.1 Generating a Support Bundle for a Device

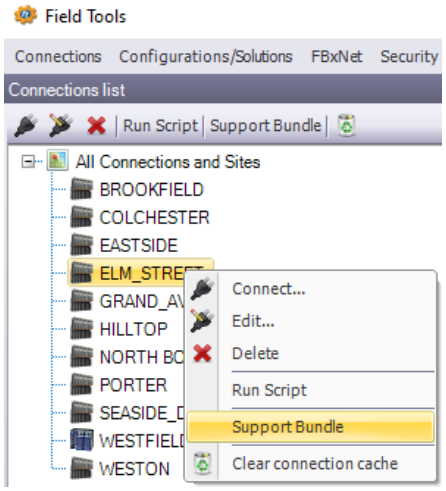
If you are experiencing problems with a particular FB1100/FB1200/FB2100/FB2200 or FB3000 device, a predefined script exists that you can use to gather diagnostic and system information in a ZIP file called a **support bundle** that you can forward to our technical support group for analysis.

Note

If a serial connection has already been established, the **Run Script** and **Support Bundle** context menu items are disabled. For an active IP connection, these context menu items are enabled.

1. Right-click on the device for which you want to gather support information and select **Support Bundle**. Alternatively, you can single click on the device to highlight it and click the **Support Bundle** button.

Figure 3-8. Generating a Support Bundle



2. The script launches to collect diagnostic information, memory dumps, alarm and event information and more.
3. The collected information is stored in a zip file. By default, the support bundle zip file is stored in the \Emerson\Logs folder:

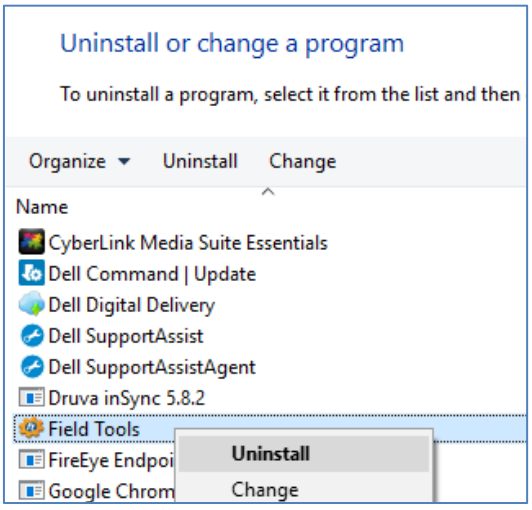
\Users\Public\Public Documents\Emerson\Logs*connection_name*_Issue_*timestamp*

Appendix B Field Tools Uninstallation Procedure

Normally, you can uninstall Field Tools like any other Windows application and just reboot your PC. Under certain circumstances such as a failed installation or some sort of file corruption, it may be necessary to take additional steps such as cleaning the installation folders and editing the Windows Registry.

Uninstalling from the Windows Control Panel

1. Navigate to **Control Panel > All Control Panel Items >Programs and Features**.
2. Right click on **Field Tools** from the **Uninstall** or **Change** a program list.
3. Choose **Uninstall** to start the installation wizard.



4. Choose **Remove** and click **Next**. Wait for the uninstall process to complete (this may take a few minutes), then click **Finish**, and reboot your PC.

Cleaning up and Deleting Installation Folders

1. Navigate to the **C:\Program Files (x86)\Emerson** folder.
2. Delete the **Emerson** folder.

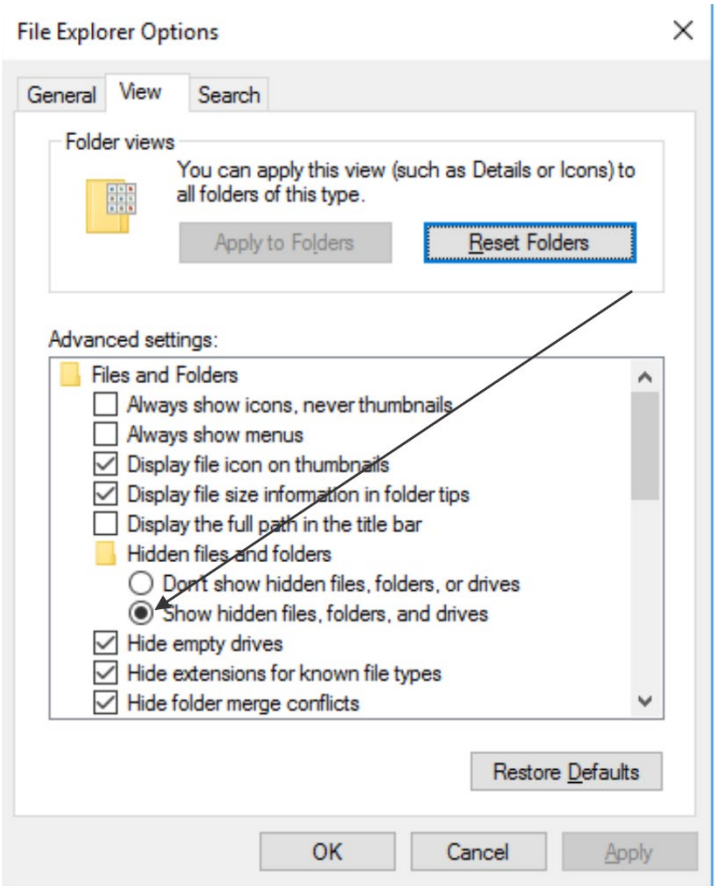
Note

If Windows prevents you from doing this, go to **Task Manager** and stop the **OpenEnterprise** and **Emerson.RuntimeDataService** services and under **Details**, end the **OEOPCDAServer.exe** task.

3. Navigate to the **C:\ProgramData\Emerson** folder.

Note

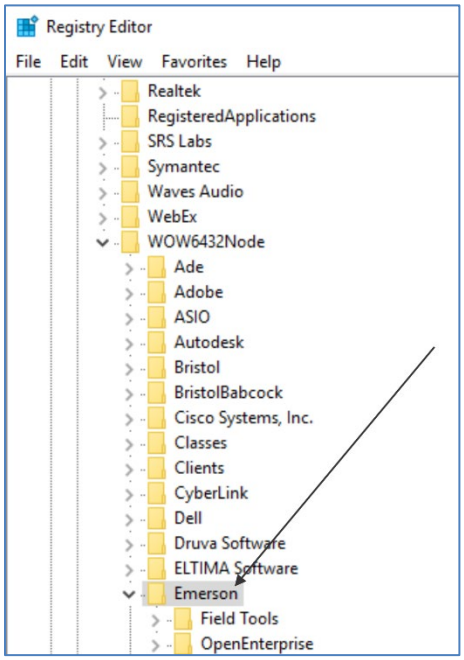
If the **ProgramData\Emerson** folder is not visible, go to Windows Control Panel, choose **File Explorer Options** and from the **View** tab, make sure **"Show hidden files, folders, and drives"** is selected.



4. Delete the **Emerson** folder.
5. Navigate to the **Users\Public\Public Documents** folder.
6. Delete the **Emerson** folder.
7. Navigate to the **Users***current user***Documents** folder.
8. Delete the **Emerson**, **MultiGrid** and **OpenEnterprise** folders.
9. Navigate to the **C:\ProgramData\Microsoft\Windows\Start Menu\Programs** folder.
10. Delete the **Emerson Field Tools** folder.
11. Reboot the PC.

Cleaning the Registry

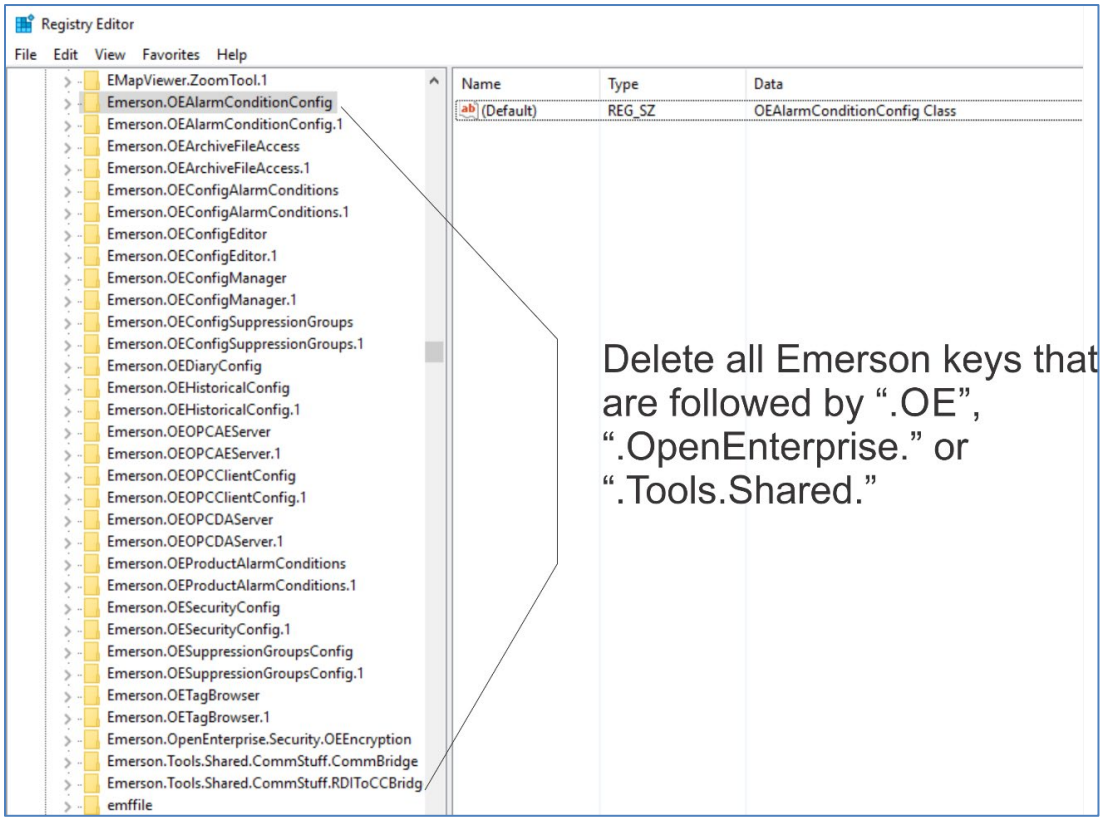
1. Click **Start > Run** and type **RegEdit** to launch the Windows Registry Editor.
2. Navigate to Computer \ HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node and delete the **Emerson** folder as shown below:



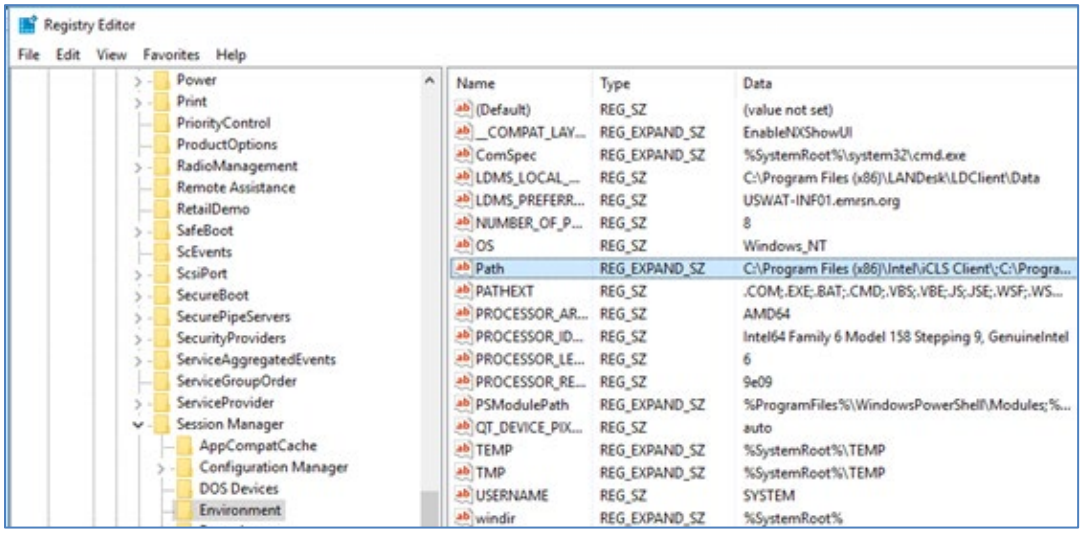
3. Exit the Registry Editor and reboot the PC.

Deep Cleaning the Registry (Usually Not Needed)

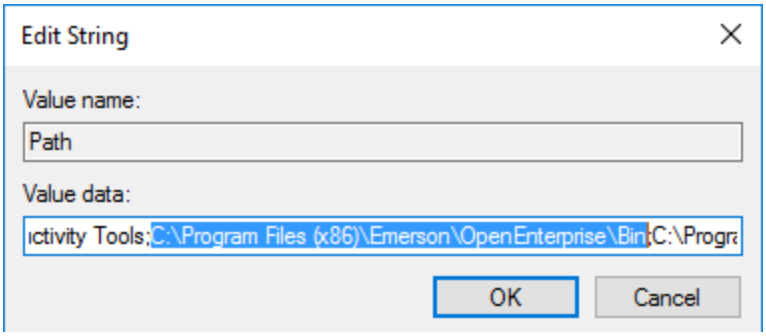
1. In RegEdit, navigate to Computer **\ HKEY_CLASSES_ROOT**
2. Delete all EMERSON keys that are followed by the text "**.OE**," "**.OpenEnterprise**," or "**.Tools.Shared**".



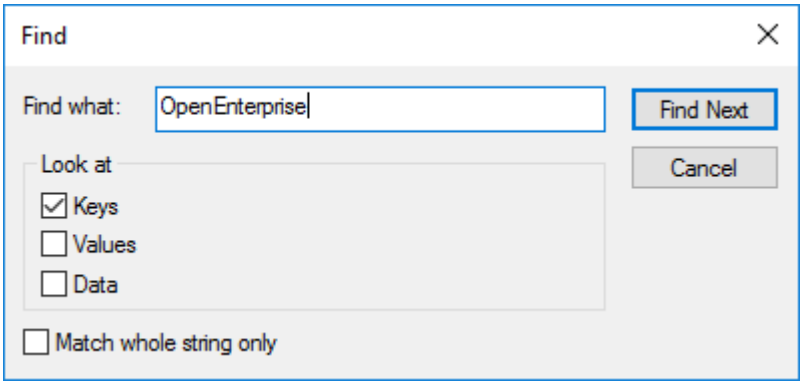
3. Navigate to:
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SessionManager\Environment



4. Double click on the Path string and then delete **the C:\Program Files (x86)\Emerson\OpenEnterprise\Bin**; path from the Edit String dialog box as shown below:



5. Click **OK** to close the dialog box.
6. Click **Edit >Find.** In the Find dialog box, make sure selections are made to look at **Keys.**
7. Type **OpenEnterprise** in the **Find wha**t edit field and click **Find Next.**



8. Delete each OpenEnterprise key and continue (use **F3** key to continue the search) until no OpenEnterprise keys can be found.
9. Exit RegEdit and reboot the PC.

Index

T

U

X

Field Tools Quick Start Guide

D301703X412

November 2024

For customer service and technical support, visit *Emerson.com/Guardian*.

North America and Latin America:
Emerson Energy and Transportation Solutions
6005 Rogerdale Road
Houston, TX 77072 U.S.A.
T +1 281 879 2699 | F +1 281 988 4445
Emerson.com/SCADAforEnergy

United Kingdom:
Emerson Process Management Limited
Fosse House, 6 Smith Way
Grove Park, Enderby
Leicester LE19 1SX UK
T +44 0 870 240 1978

Europe:
Emerson S.R.L
Regulatory Compliance Shared Services Department
Company No. J12/88/2006
Emerson 4 Street
Parcul Industrial Tetarom 11
Romania
T +40 374 132 000

Middle East/Africa:
Emerson Energy and Transportation Solutions
Emerson FZE
P.O. Box 17033
Jebel Ali Free Zone – South 2
Dubai U.A.E.
T +971 4 8118100 | F +971 4 8865465

Asia-Pacific:
Emerson Energy and Transportation Solutions
1 Pandan Crescent
Singapore 128461
T +65 6777 8211| F +65 6777 0947

Energy and Transportation Solutions

EMERSON