ProtoNode
FPC-N54
Start-up Guide

APPLICABILITY & EFFECTIVITY

Effective for all systems manufactured after March 2019.
Technical Support

Please call us for any technical support needs related to the FieldServer product.

Sierra Monitor Corporation
1991 Tarob Court
Milpitas, CA 95035
Website: www.sierramonitor.com

U.S. Support Information:
+1 408 964-4443
+1 800 727-4377
Email: support@sierramonitor.com

EMEA Support Information:
+31 33 808 0590
Email: support.emea@sierramonitor.com
TABLE OF CONTENTS

1 Introduction .............................................................................................................................................. 6

2 Equipment Setup .................................................................................................................................... 6
  2.1 Mounting ........................................................................................................................................... 6
  2.2 Physical Dimensions .......................................................................................................................... 7
  2.3 DIP Switch Settings ............................................................................................................................. 8
  2.3.1 Bias Resistors ................................................................................................................................. 8
  2.3.2 Termination Resistor ...................................................................................................................... 9

3 Installing the ProtoNode .......................................................................................................................... 10
  3.1 Connecting the R1 Port ....................................................................................................................... 10
  3.1.1 Wiring ............................................................................................................................................ 10
  3.2 Power-Up ProtoNode ........................................................................................................................... 11

4 Connect the PC to the ProtoNode ............................................................................................................. 12
  4.1 Connecting to the ProtoNode via Ethernet......................................................................................... 12
  4.1.1 Enable Access Through the Local Browser .................................................................................. 12
  4.1.1.1 Changing the Subnet of the Connected PC .............................................................................. 12
  4.1.1.2 Changing the IP Address of the ProtoNode with FieldServer Toolbox ................................ 13

5 Network Settings ................................................................................................................................... 14
  5.1 Using FS-GUI to Input Network Settings ......................................................................................... 14

6 Configure the ProtoNode ........................................................................................................................ 16
  6.1 Retrieve the Sample Configuration File ............................................................................................ 16
  6.2 Change the Configuration File to Meet the Application .................................................................. 16
  6.3 Load the Updated Configuration File ................................................................................................ 17
  6.3.1 Using the Toolbox Application to Load a Configuration File ..................................................... 17
  6.3.2 Using the FS-GUI to Load a Configuration File .......................................................................... 18
  6.3.3 Retrieve the Configuration File for Modification or Backup ...................................................... 19
  6.4 Test and Commission the ProtoNode ............................................................................................... 20

Appendix A Useful Features ....................................................................................................................... 21
  Appendix A.1 SSL/TLS for Secure Connection ....................................................................................... 21
    Appendix A.1.1 Configuring FieldServer as a SSL/TLS Server ............................................................. 21
    Appendix A.1.1.1 Simple Secure Server Configuration ....................................................................... 21
    Appendix A.1.1.2 Limiting Client Access ............................................................................................. 22
    Appendix A.1.1.3 Upload the Authority File to the FieldServer ........................................................... 22
    Appendix A.1.1.4 Certificate Validation Options .................................................................................. 23
    Appendix A.1.1.5 Set up Server Certificate ......................................................................................... 23
    Appendix A.1.2 Configuring FieldServer as SSL/TLS Client ............................................................... 24
      Appendix A.1.2.1 Simple Secure Client Configuration ....................................................................... 24
      Appendix A.1.2.2 Limit Server Access ............................................................................................... 24
      Appendix A.1.2.3 Certificate Validation Options ................................................................................ 24
      Appendix A.1.2.4 Set up Client Certificate ......................................................................................... 24

Appendix B Troubleshooting ..................................................................................................................... 25
  Appendix B.1 Lost or Incorrect IP Address ............................................................................................ 25
  Appendix B.2 Viewing Diagnostic Information ....................................................................................... 26
  Appendix B.3 Checking Wiring and Settings ......................................................................................... 27
  Appendix B.4 LED Functions ................................................................................................................... 28
  Appendix B.5 Taking a FieldServer Diagnostic Capture ....................................................................... 29
    Appendix B.5.1 Using the FieldServer Toolbox .................................................................................. 29
    Appendix B.5.2 Using FS-GUI .............................................................................................................. 32
  Appendix B.6 Factory Reset Instructions ............................................................................................... 33
  Appendix B.7 Update Firmware .............................................................................................................. 33
  Appendix B.8 Securing ProtoNode with Passwords ................................................................................ 34
Appendix C Reference..................................................................................................................................................35
  Appendix C.1 Specifications ......................................................................................................................................35
  Appendix C.2 Compliance with UL Regulations .......................................................................................................36
Appendix D Limited 2 Year Warranty....................................................................................................................................37
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DIN Rail</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>ProtoNode FPC-N54 Dimensions</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>Bias Resistor DIP Switches</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>Termination Resistor DIP Switch</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>R1 &amp; R2 Connection Ports</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>Required Current Draw for the ProtoNode</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>Power Connections</td>
<td>11</td>
</tr>
<tr>
<td>8</td>
<td>Ethernet Port Location</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>FS-GUI Page</td>
<td>14</td>
</tr>
<tr>
<td>10</td>
<td>FS-GUI Navigation Panel</td>
<td>14</td>
</tr>
<tr>
<td>11</td>
<td>FS-GUI Network Settings</td>
<td>15</td>
</tr>
<tr>
<td>12</td>
<td>FS-GUI File Transfer</td>
<td>16</td>
</tr>
<tr>
<td>13</td>
<td>FS-GUI Loading Files</td>
<td>18</td>
</tr>
<tr>
<td>14</td>
<td>Retrieve Configuration File</td>
<td>19</td>
</tr>
<tr>
<td>15</td>
<td>FS-GUI Connections Screen</td>
<td>20</td>
</tr>
<tr>
<td>16</td>
<td>Ethernet Port Location</td>
<td>25</td>
</tr>
<tr>
<td>17</td>
<td>Error Messages Screen</td>
<td>26</td>
</tr>
<tr>
<td>18</td>
<td>Diagnostic LEDs</td>
<td>28</td>
</tr>
<tr>
<td>19</td>
<td>Ethernet Port Location</td>
<td>29</td>
</tr>
<tr>
<td>20</td>
<td>FS-GUI Passwords Page</td>
<td>34</td>
</tr>
<tr>
<td>21</td>
<td>Password Recovery Page</td>
<td>34</td>
</tr>
<tr>
<td>22</td>
<td>Specifications</td>
<td>35</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

ProtoNode is a high performance, cost effective building and industrial automation multi-protocol gateway providing protocol translation between serial and Ethernet, devices and networks.

**NOTE:** For troubleshooting assistance refer to Appendix B, or any of the troubleshooting appendices in the related driver supplements. Check the [Sierra Monitor website](#) for technical support resources and documentation that may be of assistance.

The ProtoNode is cloud ready and connects with Sierra Monitor’s SMC Cloud. See the SMC Cloud note in Section 6.4 for further information.

2 EQUIPMENT SETUP

2.1 Mounting

The ProtoNode can be mounted using the DIN rail mounting bracket on the back of the unit.

![DIN Rail Bracket](image.png)

*Figure 1: DIN Rail*
2.2 Physical Dimensions

Figure 2: ProtoNode FPC-N54 Dimensions
2.3 DIP Switch Settings

2.3.1 Bias Resistors

To enable Bias Resistors, move both the BIAS- and BIAS+ dip switches to the right in the orientation shown in Figure 3.

The ProtoNode bias resistors are used to keep the RS-485 bus to a known state, when there is no transmission on the line (bus is idling), to help prevent false bits of data from being detected. The bias resistors typically pull one line high and the other low - far away from the decision point of the logic.

The bias resistor is 510 ohms which is in line with the BACnet spec. It should only be enabled at one point on the bus (for example, on the field port were there are very weak bias resistors of 100k). Since there are no jumpers, many gateways can be put on the network without running into the bias resistor limit which is < 500 ohms.

NOTE: See www.ni.com/support/serial/resinfo.htm for additional pictures and notes.

NOTE: The R1 and R2 DIP Switches apply settings to the respective serial port.

NOTE: If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.
2.3.2 Termination Resistor

If the ProtoNode is the last device on the serial trunk, then the End-Of-Line Termination Switch needs to be enabled. To enable the Termination Resistor, move the TERM dip switch to the right in the orientation shown in Figure 4.

Termination resistor is also used to reduce noise. It pulls the two lines of an idle bus together. However, the resistor would override the effect of any bias resistors if connected.

NOTE: The R1 and R2 DIP Switches apply settings to the respective serial port.

NOTE: If the gateway is already powered on, DIP switch settings will not take effect unless the unit is power cycled.
3 INSTALLING THE PROTONODE

3.1 Connecting the R1 Port

For the R1 Port only: Switch between RS-485 and RS-232 by moving the number 4 DIP Switch left for RS-485 and right for RS-232 (Figure 4).

The R2 Port is RS-485.

Connect to the 3-pin connector(s) as shown below.

The following baud rates are supported on the R1 and R2 Ports:
9600, 19200, 38400, 57600, 76800, 115000

NOTE: Not all baud rates listed are supported by all protocols. Check the specific protocol driver manual for a list of the supported baud rates.

3.1.1 Wiring

<table>
<thead>
<tr>
<th>RS-485</th>
<th>RS-232</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMS RS-485 Wiring</td>
<td>ProtoNode Pin Assignment</td>
</tr>
<tr>
<td>RS-485 +</td>
<td>TX +</td>
</tr>
<tr>
<td>RS-485 -</td>
<td>RX -</td>
</tr>
<tr>
<td>GND</td>
<td>GND</td>
</tr>
</tbody>
</table>

NOTE: Use standard grounding principles for GND.
3.2 Power-Up ProtoNode

Check power requirements in the table below:

<table>
<thead>
<tr>
<th>Power Requirement for ProtoNode External Gateway</th>
<th>Current Draw Type</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ProtoNode Family</td>
<td>12VDC</td>
<td>24V DC/AC</td>
</tr>
<tr>
<td>FPC – N54 (Typical)</td>
<td>250mA</td>
<td>125mA</td>
</tr>
</tbody>
</table>

**NOTE:** These values are ‘nominal’ and a safety margin should be added to the power supply of the host system. A safety margin of 25% is recommended.

Apply power to the ProtoNode as shown below in Figure 7. Ensure that the power supply used complies with the specifications provided in Appendix C.1.

- The ProtoNode accepts 12-24VDC or 24VAC on pins L+ and N-.
- Frame GND should be connected.

![Figure 6: Required Current Draw for the ProtoNode](image)

![Figure 7: Power Connections](image)

<table>
<thead>
<tr>
<th>Power to ProtoNode</th>
<th>ProtoNode Pin Label</th>
<th>Pin Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power In (+)</td>
<td>L+</td>
<td>V+</td>
</tr>
<tr>
<td>Power In (-)</td>
<td>N-</td>
<td>V-</td>
</tr>
<tr>
<td>Frame Ground</td>
<td>FG</td>
<td>FRAME GND</td>
</tr>
</tbody>
</table>
4 CONNECT THE PC TO THE PROTONODE

4.1 Connecting to the ProtoNode via Ethernet

First, connect a Cat-5 Ethernet cable (straight through or cross-over) between the local PC and ProtoNode.

![Figure 8: Ethernet Port Location](image)

4.1.1 Enable Access Through the Local Browser

There are two methods to enable access to the ProtoNode in the local browser, either by changing the subnet of the connected PC (Section 4.1.1.1) or using the FieldServer Toolbox to change the IP Address of the ProtoNode (Section 4.1.1.2).

**NOTE:** Only perform one method or the other.

4.1.1.1 Changing the Subnet of the Connected PC

The default IP Address for the ProtoNode is **192.168.1.24**, Subnet Mask is **255.255.255.0**. If the PC and ProtoNode are on different IP networks, assign a static IP Address to the PC on the 192.168.1.xxx network.

For Windows 10:

- Find the search field in the local computer’s taskbar (usually to the right of the windows icon) and type in “Control Panel”.
- Click “Control Panel”, click “Network and Internet” and then click “Network and Sharing Center”.
- Click “Change adapter settings” on the left side of the window.
- Right-click on “Local Area Connection” and select “Properties” from the dropdown menu.
- Highlight and then click the Properties button.
- Select and enter a static IP Address on the same subnet. For example:

  - Click the Okay button to close the Internet Protocol window and the Close button to close the Ethernet Properties window.
4.1.1.2 Changing the IP Address of the ProtoNode with FieldServer Toolbox

- Ensure that FieldServer Toolbox is loaded onto the local PC. Otherwise, download the FieldServer-Toolbox.zip via the Sierra Monitor website’s Software Downloads.

- Extract the executable file and complete the installation.

- Double click on the FS Toolbox Utility and click Discover Now on the splash page.

- Find the desired gateway and click the Configure Device button (gear icon) to the right of the gateway information.

**NOTE:** If connectivity status is green, then the IP Address doesn’t need to be changed (the ProtoNode is already on the same subnet). Skip the rest of the section and go to Section 6.

- Select Network Settings in the Configure Device window.

- Modify the IP Address (N1 IP Address field) of the gateway Ethernet port.
  - Change additional fields as needed

**NOTE:** If the gateway is connected to a router, the Default Gateway field of the gateway should be set to the IP Address of the connected router.

**NOTE:** Do not change the DHCP Server State (N1 DHCP Server State field).

**NOTE:** If DNS settings are unknown, set DNS1 to “8.8.8.8” and DNS2 to “8.8.4.4”.

- Click Update IP Settings, then click the “Change and restart” button to reboot the Gateway and activate the new IP Address. See the FieldServer Toolbox and GUI Manual for more information.
5 NETWORK SETTINGS

NOTE: To change network settings using the FieldServer Toolbox, follow the same instructions in Section 4.1.1.2.

5.1 Using FS-GUI to Input Network Settings

To navigate from the FS-GUI page to the Network Settings page follow the below instructions:

- Find the Navigation tree across the left side of the screen.
- Click the orange arrow next to the ProtoNode CN number and title to expand the tree.
- Click on the orange arrow next to Setup to expand the tree.
- Click on Network Settings.

![Figure 9: FS-GUI Page](image)

![Figure 10: FS-GUI Navigation Panel](image)
To change the IP Settings, follow these instructions:

- Enable DHCP to automatically assign IP Settings or modify the IP Settings manually as needed, via these fields: IP Address, Netmask, Default Gateway, and Domain Name Server1/2.

**NOTE:** If the FieldServer is connected to a router, the IP Gateway of the FieldServer should be set to the same IP Address of the router.

- Click Update IP Settings, then click on System Restart to restart the Gateway and activate the new IP Address.

**NOTE:** If the FS-GUI was open in a browser, the browser will need to be pointed to the new IP Address of the ProtoNode before the FS-GUI will be accessible again.
6 CONFIGURE THE PROTONODE

6.1 Retrieve the Sample Configuration File

The configuration of the ProtoNode is provided to the ProtoNode’s operating system via a comma-delimited file called "CONFIG.CSV".

If a custom configuration was ordered, the ProtoNode will be programmed with the relevant device registers in the Config.csv file for the first time start-up. If not, the product is shipped with a sample config.csv that shows an example of the drivers ordered.

- In the main menu of the FS-GUI screen, go to “Setup”, then “File Transfer”, and finally “Retrieve”.
- Click on “config.csv”, and open or save the file.

6.2 Change the Configuration File to Meet the Application

Refer to the FieldServer Configuration Manual in conjunction with the Driver supplements for information on configuring the ProtoNode.
6.3 Load the Updated Configuration File

6.3.1 Using the Toolbox Application to Load a Configuration File

- From the Toolbox main page, click on the setup icon (the gear picture).

- Select File Transfer.

- Browse and select the .csv file, open, then click "Update Config".

- Once download is complete, click the Restart Button (or simply cycle power to the ProtoNode) to put the new file into operation.

**NOTE:** It is possible to do multiple downloads to the ProtoNode before resetting it.
6.3.2 Using the FS-GUI to Load a Configuration File

- In the main menu of the FS-GUI screen, click “Setup”, then “File Transfer” and finally “Update”.
- Browse and select the .csv file, open, then click “Submit”.

Once download is complete, a message bar will appear confirming that the configuration was updated successfully.
- Click the System Restart Button to put the new file into operation.

**NOTE:** It is possible to do multiple downloads to the ProtoNode before resetting it.
6.3.3 Retrieve the Configuration File for Modification or Backup

- To get a copy of the configuration file for modifying or backing up a configuration on a local computer, do the following:

- In the main menu of the FS-GUI screen, click “Setup”, then “File Transfer”.

  Figure 14: Retrieve Configuration File

- Click the “config.csv” link under the “Retrieve” heading in the middle section of the screen.

- The file will automatically download to the web browser’s default download location.

- Edit or store the file as desired.

**NOTE:** Before using any backup configuration file to reset the configuration settings, check that the backup file is not an old version.
6.4 Test and Commission the ProtoNode

- Connect the ProtoNode to the third party device(s), and test the application.
- Click on the Diagnostic button to view to get to the FS-GUI.
- From the landing page of the FS-GUI click on View in the navigation tree, then Connections to see the number of messages on each protocol.

![FS-GUI Connections Screen](image)

**Figure 15: FS-GUI Connections Screen**

**NOTE:** For troubleshooting assistance refer to Appendix B, or any of the troubleshooting appendices in the related driver supplements and configuration manual. Sierra Monitor also offers a technical support on the Sierra Monitor website, which contains a significant number of resources and documentation that may be of assistance.

**NOTE:** The FieldPoP™ button (see Figure 15) allows users to connect to the SMC Cloud, Sierra Monitor’s device cloud solution for IIoT. The SMC Cloud enables secure remote connection to field devices through a FieldServer and its local applications for configuration, management, maintenance. For more information about the SMC Cloud, refer to the SMC Cloud Start-up Guide.
Appendix A Useful Features

Appendix A.1 SSL/TLS for Secure Connection

SSL/TLS (Secure Sockets Layer/Transport Layer Security) is a security technology for establishing an encrypted connection between a server and a client. This allows the secure transfer of data across untrusted networks.

Appendix A.1.1 Configuring FieldServer as a SSL/TLS Server

The following example sets the FieldServer to accept a secure Modbus/TCP connection on port 1502.

Appendix A.1.1.1 Simple Secure Server Configuration

Add TLS_Port parameter in the connections section of the configuration file and set to a port number between 1 – 65535.

<table>
<thead>
<tr>
<th>Connections</th>
<th>Adapter</th>
<th>Protocol</th>
<th>TLS_Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>N1</td>
<td>Modbus/TCP</td>
<td>1502</td>
<td></td>
</tr>
</tbody>
</table>

This configuration sets the FieldServer to accept any incoming connection but will not request a client's certificate for verification. This means that the FieldServer end point communication will be encrypted but not authenticated.

The FieldServer will send an embedded self-signed certificate if one is requested by a connecting client.

NOTE: If a remote client requires a certificate, then request the smc_cert.pem certificate from Sierra Monitor Technical Support and update the remote client’s authority as per vendor instructions.
Appendix A.1.1.2 Limiting Client Access

In addition to TLS_Port parameter also add Validate_Client_Cert in the connections section of the configuration file and set it to “Yes”.

<table>
<thead>
<tr>
<th>Connections</th>
<th>Adapter</th>
<th>Protocol</th>
<th>TLS_Port</th>
<th>Validate_Client_Cert</th>
</tr>
</thead>
<tbody>
<tr>
<td>N1</td>
<td>Modbus/TCP</td>
<td>1502</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

The configuration above sets the FieldServer to request and verify a client’s certificate against its internal authority file before accepting connection. By default, this means the FieldServer will only accept connections from other FieldServers.

In order to load an authority file so that the FieldServer will accept connections from a chosen list of remote clients, configure the FieldServer with the following connection settings:

<table>
<thead>
<tr>
<th>Connections</th>
<th>Adapter</th>
<th>Protocol</th>
<th>TLS_Port</th>
<th>Validate_Client_Cert</th>
<th>Cert_Authority_File</th>
</tr>
</thead>
<tbody>
<tr>
<td>N1</td>
<td>Modbus/TCP</td>
<td>1502</td>
<td>Yes</td>
<td>my_authorized_clients.pem</td>
<td></td>
</tr>
</tbody>
</table>

This configuration has the FieldServer accept connections from clients who have the correct certificate. The authority file is a collection of client certificates in PEM format. This file can be edited using any text file editor.

**NOTE:** Cert_Authority_File is useful only if Validate_Client_Cert is set to ‘Yes’.

Appendix A.1.1.3 Upload the Authority File to the FieldServer

1. Enter the IP address of the FieldServer into a web browser.
2. Choose the ‘Setup’ option in the Navigation Tree and Select ‘File Transfer’.
3. Choose the ‘General’ tab.
4. Click on the ‘Browse’ button and select the PEM file you want to upload.
5. Click on ‘Submit’.
6. When the message, “The file was uploaded successfully” appears, click on the ‘System Restart’ button.
Appendix A.1.1.4 Certificate Validation Options

If connections must be limited to only a particular domain (vendor devices), include Check_Remote_Host to specify the domain/host name.

<table>
<thead>
<tr>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter , Protocol , TLS_Port , Validate_Client_Cert , Cert_Authority_File , Check_Remote_Host</td>
</tr>
<tr>
<td>N1 , Modbus/TCP , 1502 , Yes , my_authorized_clients.pem , SMC</td>
</tr>
</tbody>
</table>

The configuration above tells the FieldServer to only accept connections that have the correct certification and is coming from the specified host.

The Check_Remote_Host value is synonymously known as common name, host name or domain etc. The common name can be obtained by the following methods:

- Ask the certificate issuer for the host name.
- Use online tools to decode the certificate (for example: [https://www.sslshopper.com/certificate-decoder.html](https://www.sslshopper.com/certificate-decoder.html)).
- If the program openssl is installed on the local PC, then run the following command to get the common name: openssl x509 -in certificate.pem -text -noout

Appendix A.1.1.5 Set up Server Certificate

Make sure the certificate is in PEM format. Otherwise, convert it to PEM format (reference the link below).

[support.ssl.com/Knowledgebase/Article](support.ssl.com/Knowledgebase/Article)

Configure the FieldServer to use a custom certificate as shown below:

<table>
<thead>
<tr>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter , Protocol , TLS_Port , Server_Cert_File</td>
</tr>
<tr>
<td>N1 , Modbus/TCP , 1502 , my_server_cert.pem</td>
</tr>
</tbody>
</table>
Appendix A.1.2 Configuring FieldServer as SSL/TLS Client

The following Node configurations set the FieldServer to open a secure Modbus/TCP connection to a Server at IP Address 10.11.12.13 on port 1502.

### Appendix A.1.2.1 Simple Secure Client Configuration

Add Remote_Node_TLS_Port parameter in the nodes section of the configuration file and set to a port number between 1 – 65535.

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Node_Name</th>
<th>Node_ID</th>
<th>Protocol</th>
<th>Adapter</th>
<th>IP_Address</th>
<th>Remote_Node_TLS_Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLC_11</td>
<td>11</td>
<td>Modbus/TCP</td>
<td>N1</td>
<td>10.11.12.13</td>
<td>1502</td>
<td></td>
</tr>
</tbody>
</table>

The above configuration sets the FieldServer to connect to a remote server but does not request a server's certificate for verification. This means that the FieldServer endpoint communication will be encrypted but not authenticated.

If requested by a remote server, the FieldServer will send an embedded self-signed certificate.

### Appendix A.1.2.2 Limit Server Access

Add the Validate_Server_Cert parameter to the client node section of the configuration.

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Remote_Node_TLS_Port</th>
<th>Validate_Server_Cert</th>
<th>Cert_Authority_File</th>
</tr>
</thead>
<tbody>
<tr>
<td>------</td>
<td>1502</td>
<td>Yes</td>
<td>my_authorized_servers.pem</td>
</tr>
</tbody>
</table>

The above configuration sets the FieldServer to request and verify the server's certificate against its own internal authority file before finalizing the connection. By default, this means the FieldServer will only establish connections to other FieldServers.

### Appendix A.1.2.3 Certificate Validation Options

Use the Check_Remote_Host element as described in Appendix A.1.1.4.

### Appendix A.1.2.4 Set up Client Certificate

Make sure the certificate is in PEM format. Otherwise, convert it to PEM format (reference the link below). [support.ssl.com/Knowledgebase/Article](support.ssl.com/Knowledgebase/Article)

Configure the FieldServer to use a custom certificate as shown below:

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Client_Cert_File</th>
</tr>
</thead>
<tbody>
<tr>
<td>------</td>
<td>my_client_cert.pem</td>
</tr>
</tbody>
</table>
Appendix B Troubleshooting

Appendix B.1 Lost or Incorrect IP Address

- Ensure that FieldServer Toolbox is loaded onto the local PC. Otherwise, download the FieldServer-Toolbox.zip via the Sierra Monitor website’s Software Downloads.
- Extract the executable file and complete the installation.

![Ethernet Port Location](image1)

- Connect a standard Cat-5 Ethernet cable between the user’s PC and ProtoNode.
- Double click on the FS Toolbox Utility and click Discover Now on the splash page.
- Check for the IP Address of the desired gateway.

![FieldServer Toolbox](image2)

- If correcting the IP Address of the gateway: click the settings icon on the same row as the gateway, then click Network Settings, change the IP Address and click Update IP Settings to save.
Appendix B.2 Viewing Diagnostic Information

- Type the IP Address of the ProtoNode into the web browser or use the FieldServer Toolbox to connect to the ProtoNode.
- Click on Diagnostics and Debugging Button, then click on view, and then on connections.
- If there are any errors showing on the Connection page, refer to Appendix B.3 for the relevant wiring and settings.

![Error Messages Screen](image)

Figure 17: Error Messages Screen
Appendix B.3 Checking Wiring and Settings

No COMS on the Serial side. If the Tx/Rx LEDs are not flashing rapidly then there is a COM issue. To fix this problem, check the following:

- Visual observations of LEDs on the ProtoNode (Appendix B.4)
- Check baud rate, parity, data bits, stop bits
- Check Serial device address
- Verify wiring
- Verify device is connected to the same subnet as the ProtoNode

No COMS on the Ethernet protocol. To fix this, check the following:

- Visual observations of LEDs on the ProtoNode (Appendix B.4)
- Check device address
- Verify wiring
- Verify device is connected to the same subnet as the ProtoNode
- Verify IP Address setting

NOTE: If the problem still exists, a Diagnostic Capture needs to be taken and sent to support. (Appendix B.5)
Appendix B.4 LED Functions

See the diagram below for ProtoNode FPC-N54 LED Locations.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS</td>
<td>The SS LED will light if the unit is not getting a response from one or more of the configured devices.</td>
</tr>
<tr>
<td>ERR</td>
<td>The SYS ERR LED will go on solid indicating there is a system error. If this occurs, immediately report the related “system error” shown in the error screen of the FS-GUI interface to support for evaluation.</td>
</tr>
<tr>
<td>PWR</td>
<td>This is the power light and should always be steady green when the unit is powered.</td>
</tr>
<tr>
<td>RX</td>
<td>The RX LED will flash when a message is received on the serial port on the 3-pin connector. <strong>If the serial port is not used, this LED is non-operational.</strong> RX1 applies to the R1 connection while RX2 applies to the R2 connection.</td>
</tr>
<tr>
<td>TX</td>
<td>The TX LED will flash when a message is sent on the serial port on the 3-pin connector. <strong>If the serial port is not used, this LED is non-operational.</strong> TX1 applies to the R1 connection while TX2 applies to the R2 connection.</td>
</tr>
</tbody>
</table>

*Figure 18: Diagnostic LEDs*
Appendix B.5 Taking a FieldServer Diagnostic Capture

When there is a problem on-site that cannot easily be resolved, perform a diagnostic capture before contacting support so that support can quickly solve the problem. There are two methods for taking diagnostic captures:

- **FieldServer Toolbox:**
  This method requires installation of the FS Toolbox program. A FS Toolbox diagnostic capture takes a snapshot of the loaded configuration files and a log of all the communications on the serial ports over a specified period of time. If the problem occurs over an Ethernet connection, then take a Wire Shark capture.

- **Gateway's FS-GUI Page:**
  This method doesn't require downloading software. The diagnostic capture utilities are embedded in the FS-GUI web interface. Starting a diagnostic capture takes a snapshot of the loaded configuration files and a log of all the communications over a specified period of time. This works for both serial and Ethernet connections.

**NOTE:** The information in the zipped files contains everything support needs to quickly resolve problems that occur on-site.

Appendix B.5.1 Using the FieldServer Toolbox

Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

- Ensure that FieldServer Toolbox is loaded onto the local PC. Otherwise, download the FieldServer-Toolbox.zip via the Sierra Monitor website's Software Downloads.

- Extract the executable file and complete the installation.

- Connect a standard Cat-5 Ethernet cable between the PC and FieldServer.
- Double click on the FS Toolbox Utility.
• **Step 1: Take a Log**
  - Click on the diagnose icon of the desired device
  - Ensure "Full Diagnostic" is selected (this is the default)

NOTE: If desired, the default capture period can be changed.
Click on “Start Diagnostic”

Wait for Capture period to finish, then the Diagnostic Test Complete window will appear

- **Step 2: Send Log**
  - Once the Diagnostic test is complete, a .zip file will be saved on the PC
    - Choose “Open” to launch explorer and have it point directly at the correct folder
    - Send the Diagnostic zip file to support@sierramonitors.com

![](image)
Appendix B.5.2 Using FS-GUI

Completing a Diagnostic Capture through the FieldServer allows network connections (such as Ethernet and Wi-Fi) to be captured.

Once the Diagnostic Capture is complete, email it to technical support. The Diagnostic Capture will accelerate diagnosis of the problem.

- Open the FieldServer FS-GUI page.
- Click on Diagnostics in the Navigation panel.

- Go to Full Diagnostic and select the capture period.
- Click the Start button under the Full Diagnostic heading to start the capture.
  - When the capture period is finished, a Download button will appear next to the Start button.

- Click Download for the capture to be downloaded to the local PC.
- Send the diagnostic zip file to support@sierramonitor.com.

NOTE: Diagnostic captures of BACnet MS/TP communication are output in a “.PCAP” file extension which is compatible with Wireshark.
Appendix B.6 Factory Reset Instructions

For instructions on how to reset a FieldServer back to its factory released state, see ENOTE - FieldServer Next Gen Recovery.

Appendix B.7 Update Firmware

To load a new version of the firmware, follow these instructions:

1. Extract and save the new file onto the local PC.
2. Open a web browser and type the IP Address of the FieldServer in the address bar.
   - Default IP Address is 192.168.1.24
   - Use the FS Toolbox utility if the IP Address is unknown (Appendix B.1)
3. Click on the “Diagnostics & Debugging” button.
4. In the Navigation Tree on the left hand side, do the following:
   a. Click on “Setup”
   b. Click on “File Transfer”
   c. Click on the “General” tab
5. In the General tab, click on “Choose Files” and select the web.img file extracted in step 1.
6. Click on the orange “Submit” button.
7. When the download is complete, click on the “System Restart” button.
Appendix B.8 Securing ProtoNode with Passwords

Access to the ProtoNode can be restricted by enabling a password on the FS-GUI Passwords page – click Setup and then Passwords in the navigation panel. There are 2 access levels defined by 2 account names: Admin and User.

- The Admin account has unrestricted access to the ProtoNode.
- The User account can view any ProtoNode information but cannot make any changes or restart the ProtoNode.

The password needs to be a minimum of eight characters and is case sensitive.

If the password is lost, click cancel on the password authentication popup window, and email the password recovery token to technical support to receive a temporary password from the customer support team. Access the ProtoNode to set a new password.

![FS-GUI Passwords Page](image)

![Password Recovery Page](image)
## Appendix C Reference

### Appendix C.1 Specifications

<table>
<thead>
<tr>
<th>Electrical Connections</th>
<th>ProtoNode FPC-N54&lt;sup&gt;1&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>One 3-pin Phoenix connector with:</td>
<td></td>
</tr>
<tr>
<td>RS-485/RS-232 (Tx+ / Rx- / gnd)</td>
<td></td>
</tr>
<tr>
<td>One 3-pin Phoenix connector with:</td>
<td></td>
</tr>
<tr>
<td>RS-485 (Tx+ / Rx- / gnd)</td>
<td></td>
</tr>
<tr>
<td>One 3-pin Phoenix connector with:</td>
<td></td>
</tr>
<tr>
<td>Power port (+ / - / Frame-gnd)</td>
<td></td>
</tr>
<tr>
<td>One Ethernet 10/100 BaseT port</td>
<td></td>
</tr>
</tbody>
</table>

| Power Requirements | Input Voltage: 12-24VDC or 24VAC  
| Max Power: 3 Watts | Current draw: 24VAC 125mA  
| 12-24VDC 250mA @12VDC |

<table>
<thead>
<tr>
<th>Approvals</th>
<th>CE and FCC Class B &amp; C Part 15, UL 60950, WEEE compliant, IC Canada, RoHS compliant</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Power Requirements</th>
<th>12-24VDC or 24VAC</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Physical Dimensions</th>
<th>4 x 1.1 x 2.7 in (10.16 x 2.8 x 6.8 cm)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Weight</th>
<th>0.4 lbs (0.2 Kg)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Operating Temperature</th>
<th>-20°C to 70°C (-4°F to 158°F)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Humidity</th>
<th>10-95% RH non-condensing</th>
</tr>
</thead>
</table>

> Figure 22: Specifications

“This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference
- This device must accept any interference received, including interference that may cause undesired operation.

**NOTE:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his expense. Modifications not expressly approved by Sierra Monitor could void the user's authority to operate the equipment under FCC rules”.

---

<sup>1</sup> Specifications subject to change without notice.
Appendix C.2 Compliance with UL Regulations

For UL compliance, the following instructions must be met when operating the ProtoNode.

- The units shall be powered by listed LPS or Class 2 power supply suited to the expected operating temperature range.

- The interconnecting power connector and power cable shall:
  - Comply with local electrical code
  - Be suited to the expected operating temperature range
  - Meet the current and voltage rating for the ProtoNode

- Furthermore, the interconnecting power cable shall:
  - Be of length not exceeding 3.05m (118.3”)
  - Be constructed of materials rated VW-1, FT-1 or better

- If the unit is to be installed in an operating environment with a temperature above 65 °C, it should be installed in a Restricted Access Area requiring a key or a special tool to gain access.

- This device must not be connected to a LAN segment with outdoor wiring.
Appendix D Limited 2 Year Warranty

Sierra Monitor Corporation warrants its products to be free from defects in workmanship or material under normal use and service for two years after date of shipment. Sierra Monitor Corporation will repair or replace any equipment found to be defective during the warranty period. Final determination of the nature and responsibility for defective or damaged equipment will be made by Sierra Monitor Corporation personnel.

All warranties hereunder are contingent upon proper use in the application for which the product was intended and do not cover products which have been modified or repaired without Sierra Monitor Corporation’s approval or which have been subjected to accident, improper maintenance, installation or application, or on which original identification marks have been removed or altered. This Limited Warranty also will not apply to interconnecting cables or wires, consumables or to any damage resulting from battery leakage.

In all cases Sierra Monitor Corporation’s responsibility and liability under this warranty shall be limited to the cost of the equipment. The purchaser must obtain shipping instructions for the prepaid return of any item under this warranty provision and compliance with such instruction shall be a condition of this warranty.

Except for the express warranty stated above, Sierra Monitor Corporation disclaims all warranties with regard to the products sold hereunder including all implied warranties of merchantability and fitness and the express warranties stated herein are in lieu of all obligations or liabilities on the part of Sierra Monitor Corporation for damages including, but not limited to, consequential damages arising out of/or in connection with the use or performance of the product.