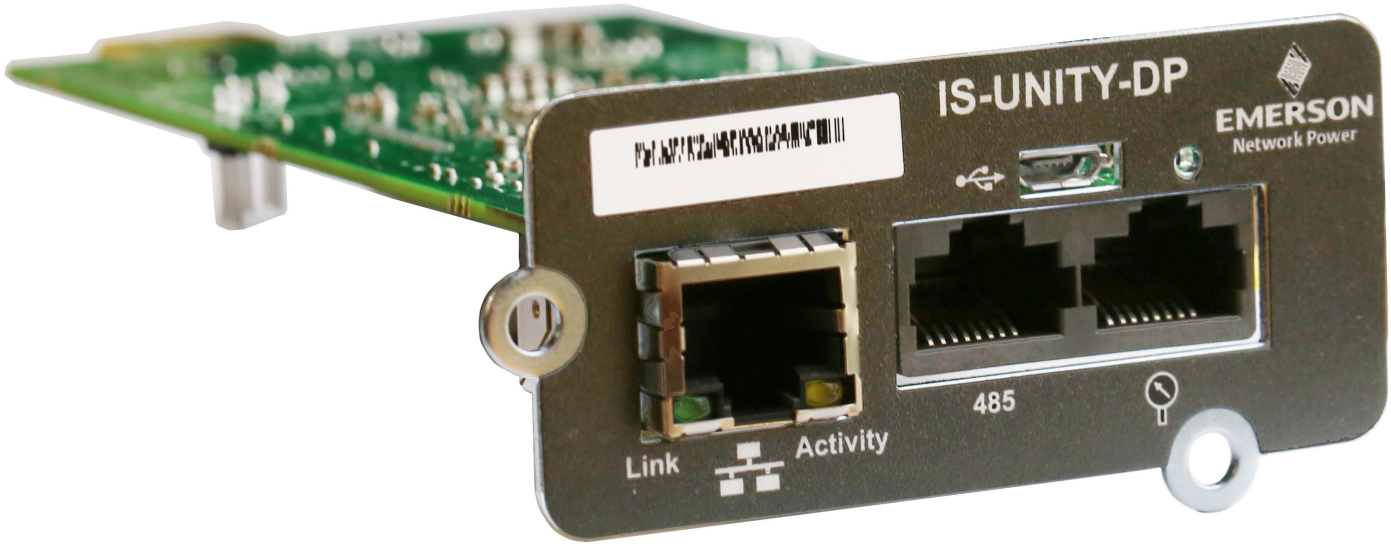
Liebert® IntelliSlot™ Unity™ Card

User Manual—Web, SNMP, Modbus, BACnet, YDN23



EMERSON
Network Power

Table of Content

List of Figures

List of Tables

Page intentionally left blank.

Important Safety Instructions

SAVE THESE INSTRUCTIONS

WARNING

Risk of arc flash and electric shock. Can cause injury or death.

Open all local and remote electric power supply disconnect switches, verify with a voltmeter that power is off and wear personal protective equipment per NFPA 70E before working within the electric control enclosure. Failure to comply can cause serious injury or death.

WARNING

Risk of electric shock. Can cause equipment damage, injury or death.

Open all local and remote electric power supply disconnect switches and verify with a voltmeter that power is off before working within any electric connection enclosures.

Service and maintenance work must be performed only by properly trained and qualified personnel and in accordance with applicable regulations and manufacturers' specifications.

Opening or removing the covers to any equipment may expose personnel to lethal voltages within the unit even when it is apparently not operating and the input wiring is disconnected from the electrical source.

NOTICE

Risk of improper installation. Can cause equipment damage.

Only a qualified service professional should install these products. Emerson recommends having an Emerson Network Power® Liebert Services representative perform the installation in large UPS's. Contact Liebert Services at 1-800-LIEBERT (1-800-543-2378).

Page intentionally left blank.

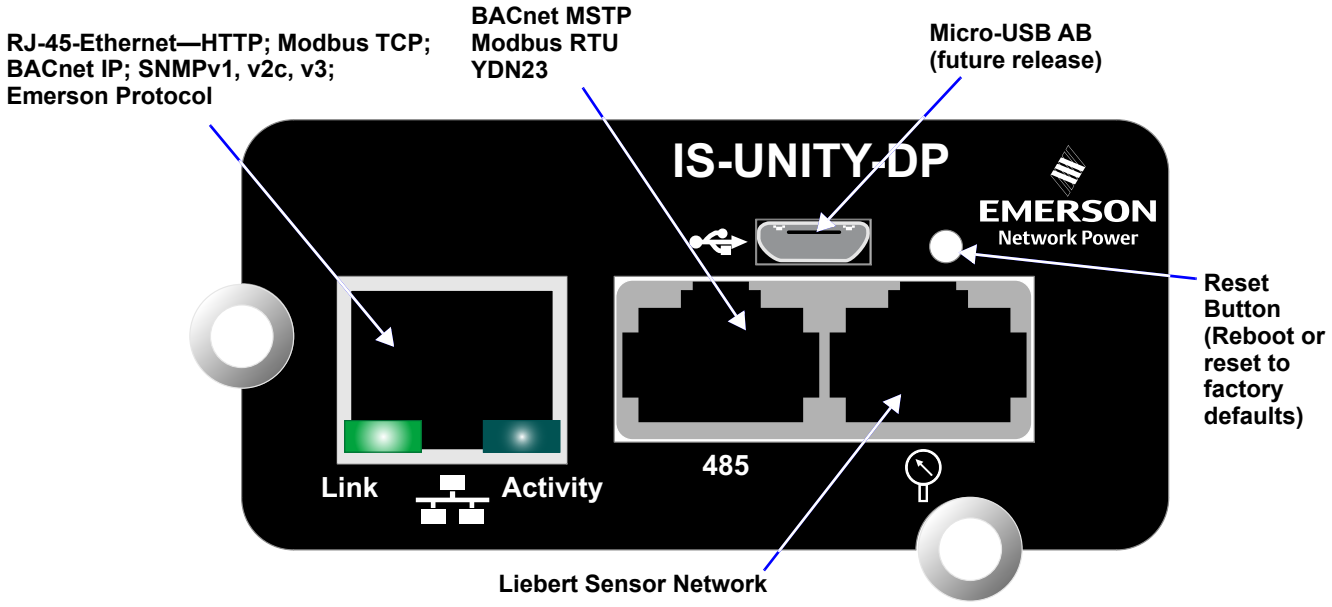
1.0 Introduction

This Liebert IntelliSlot Unity platform delivers enhanced communication and control of AC Power, Power Distribution and Thermal Management products. The platform communicates with Emerson Network Power® software tools and services, including Trellis®, LIFE™ Services, Liebert SiteScan Web™ and Liebert Nform®.

The platform includes the Liebert IntelliSlot Unity-DP™ and Liebert IntelliSlot Unity LIFE™ cards.

Each card employs the Emerson Protocol to monitor and manage a wide range of operating parameters, alarms and notifications about power, distribution and cooling equipment. The cards also communicate with Building Management Systems and Network Management Systems. Liebert IntelliSlot Unity cards support monitoring of sensors to improve system reliability and efficiency.

Figure 1-1 Liebert IntelliSlot Unity-DP card features



1.1 Protocols

Each card supports the Emerson Protocol, Remote Service Delivery Protocol and HTTP Web by default.

The Liebert IntelliSlot Unity-DP supports selecting two third-party protocols; the Liebert IntelliSlot Unity LIFE card supports the default protocols only (Emerson Protocol, Remote Service Delivery Protocol and HTTP Web).

Available protocols are

- BACnet IP—BACnet over Internet Protocol
- BACnet MSTP—BACnet Master-Slave/Token-Passing (MSTP) communications protocol over a RS-485 serial network (also known as BACnet MSTP RS-485)
- Modbus RTU—Modbus Remote Terminal Unit (RTU) communication protocol over a RS-485 serial network (also known as Modbus RTU RS-485)
- Modbus TCP—Modbus Transmission Control Protocol over Internet Protocol (also known as Modbus TCP/IP)
- SNMP
- YDN23 - YD-T-1363 specification protocol (also known as YD/T 1363)

1.2 Compatibility With Other Emerson Products and Communication Protocols

The Liebert IntelliSlot Unity platform includes:

Table 1-1 Compatibility with Liebert equipment

Liebert IntelliSlot Card	Compatible with:		
Liebert IS-UNITY-DP Liebert IS-UNITY-LIFE	Alber BDSU-50™	Liebert EPM™	Liebert NX™ 225-600 kVA
	Liebert APM™	Liebert EXC™	Liebert NXC™
	Liebert APS™	Liebert *e*XL™	Liebert NXL™ *
	Liebert Challenger 3000™	Liebert *e*XM™	Liebert NXR™
	Liebert CRV™	Liebert FDC™	Liebert PCW™/PDX™
	Liebert CW™	Liebert FPC™	Liebert PeX™ *
	Liebert DCL™	Liebert GXT3™	Liebert PPC™
	Liebert DCP™	Liebert GXT4™	Liebert RDC™
	Liebert Deluxe System/3™	Liebert HPC™	Liebert RX™
	Liebert DS™	Liebert HPC-S/M/R/W/Generic™	Liebert XDC™
	Liebert DSE™	Liebert HPM™	Liebert XDP™
			Liebert XDP-Cray™

The Liebert IntelliSlot Unity-DP platform supports the following protocols:

Table 1-2 Liebert IntelliSlot card communication protocols

Liebert IntelliSlot Card (Part #)	Communication Protocols Available								
	HTTP HTTPS	Emerson Protocol	Remote Service Delivery Protocol	Email	SMS	SNMP v1, v2c, v3	BACnet IP BACnet MSTP	Modbus TCP Modbus RTU	YDN23 *
Liebert IS-UNITY-DP (IS-UNITY-DP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Liebert IS-UNITY-LIFE (IS-UNITY-LIFE)	✓	✓	✓	✓	✓	—	—	—	—

* YDN23 applicable only to Liebert PeX and Liebert NXL.

The Liebert IntelliSlot Unity platform supports both 10Mbit and 100Mbit communication speeds and either half or full duplex.

Sensor Support

The Liebert IntelliSlot Unity platform supports these sensors: Liebert SN-2D, Liebert SN-3C, Liebert SN-L, Liebert SN-T, Liebert SN-TH, Liebert SN-Z01, Liebert SN-Z02 and Liebert SN-Z03.

Password Protection

Control and configuration capabilities are protected by an administrator's username and password combination. Optionally, status information can be password-protected. The default user name for the administrator is *Liebert* and the default password is also *Liebert.*

The user name and password can be changed with the Web interface. See **2.2 - Change User Names and Passwords Immediately** for details.

SNMP Support

The Liebert IntelliSlot Unity card enables SNMP management of Liebert equipment. To integrate the card into a SNMP implementation, import or compile the Liebert Global Products MIB on the network management station (NMS).

The Liebert Global Products MIB is available at Liebert's Web site (**www.liebert.com**); it supports both Windows® (192436P1) and Unix (192435P1) file formats.

Web Support

The Liebert IntelliSlot Unity card delivers Web management and control to Liebert equipment over HTTP and HTTPS. All authorized users on your network will be able to view status information.

Modbus TCP and Modbus RTU Support

The Liebert IntelliSlot Unity card supports Modbus TCP and Modbus RTU for the full range of information available from the managed device. The Modbus protocol mapping document, SL-28170, is available at Liebert's Web site: **www.liebert.com**

BACnet IP and BACnet MSTP Support

The Liebert IntelliSlot Unity card supports BACnet IP and BACnet MSTP for the full range of information available from the managed device. The BACnet protocol support in the IS_UNITY 6.0 release has been tested by the BACnet Testing Laboratories (BTL) and was found in conformance to the BACnet protocol standards. The BTLCertification listing for the Unity card on the BACnet International website can be found **here**. The BACnet protocol mapping document, SL-28170, and the BACnet Protocol Implementation Conformance Statement (PICS), SL-52647, are available at Liebert's Web site (**www.liebert.com**) as guides to implementing the BACnet protocol.

YDN23 Support

The Liebert IntelliSlot Unity card supports YD/T-1363 specification for the full range of information available from managed Liebert NXL™ or Liebert PeX™ units.

Trellis™ Support

The Liebert IntelliSlot Unity-DP card communicates a rich set of Emerson Protocol information to the Trellis DCIM platform.

Trellis can manage and control Liebert equipment using SNMP, Modbus or the Emerson Protocol. This allows monitoring all Liebert equipment using Liebert IntelliSlot Web, Liebert IntelliSlot 485, Liebert IntelliSlot IPBML, Liebert IntelliSlot Web ADPT or Liebert IntelliSlot Unity platform communication interfaces.

Liebert Nform® Support

Utilizing the Emerson Protocol or SNMP and Web technologies built into each Liebert IntelliSlot Unity card, Liebert Nform will centrally manage alarm notifications to provide an easy interface to access critical equipment information.

A downloadable version is available online at: **nform.liebert.com**

Liebert MultiLink® Support

The Liebert IntelliSlot Unity card integrates with Liebert's MultiLink software to provide unattended, graceful operating system shutdown of PCs, servers and workstations. The card can be monitored by Liebert MultiLink over the network, eliminating the need for serial cables.

For more information on Liebert MultiLink and a downloadable version of Liebert MultiLink software, visit **multilink.liebert.com**

1.3 Support for Liebert SN Sensors

The Liebert IntelliSlot Unity card supports connection and monitoring up to 10 Liebert SN modular and integrated sensors. Available sensor types include temperature, humidity, door closure, contact closure and leak detection. Sensor tab menus permit configuring sensors and putting them in order for easier checking of high-priority conditions. Sensor data is available via SNMP and the Web user interface.

2.0 Installation

WARNING

Risk of arc flash and electric shock. Can cause injury or death.

Open all local and remote electric power supply disconnect switches, verify with a voltmeter that power is off and wear personal protective equipment per NFPA 70E before working within the electric control enclosure. Failure to comply can cause serious injury or death.

WARNING

Risk of electric shock. Can cause equipment damage, injury or death.

Open all local and remote electric power supply disconnect switches and verify with a voltmeter that power is off before working within any electric connection enclosures.

Service and maintenance work must be performed only by properly trained and qualified personnel and in accordance with applicable regulations and manufacturers' specifications.

Opening or removing the covers to any equipment may expose personnel to lethal voltages within the unit even when it is apparently not operating and the input wiring is disconnected from the electrical source.

NOTICE

Risk of improper installation. Can cause equipment damage.

Only a qualified service professional should install these products. Emerson recommends having an Emerson Network Power® Liebert Services representative perform the installation in large UPS's. Contact Liebert Services at 1-800-LIEBERT (1-800-543-2378).

NOTICE

Risk of duplicate node IDs if two or more Liebert IntelliSlot cards are installed. Can cause network conflicts.

An internal networking conflict may occur within a device when multiple communication cards with duplicate Node IDs are installed in the device.

Each Liebert IntelliSlot card must have a unique node ID. This will not be a problem if only one card is installed on your system. Duplicate node IDs are easily averted with the procedure detailed in **2.4 - Installing Multiple Liebert IntelliSlot Unity Cards in a System**.

2.1 Installing the Liebert IntelliSlot Unity Card

The Liebert IntelliSlot Unity card may be installed at the factory or field-installed. To perform a field-installation:

1. Find the Liebert IntelliSlot bay on your Liebert equipment—It may have a plastic cover.
2. Insert the card into the Liebert IntelliSlot bay.

NOTE

The card will only fit one way in the Liebert IntelliSlot bay because the circuit board is not centered on the faceplate. The slot in the Liebert IntelliSlot bay also is not centered.

3. Secure the card with the screws supplied with the cover plate.

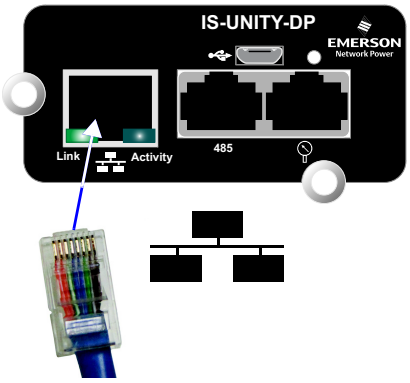
4. Connect an Ethernet cable to the card's Ethernet RJ-45 port for IP communication interfaces.
5. Connect a serial cable to the card's 485 RJ-45 port for RS-485 communication interfaces (see **2.1.3 - Connect an RS-485 Serial Cable**.

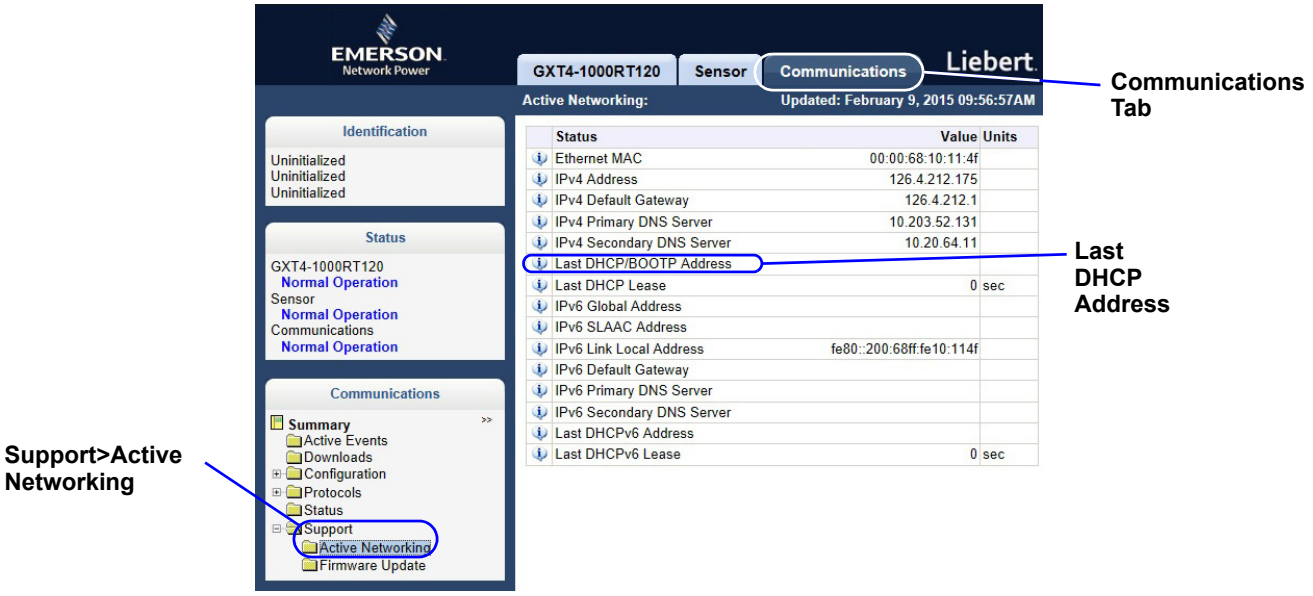
2.1.1 Assigning the Card's IP Address

2.1.1.1 DHCP

The Liebert IntelliSlot Unity card is factory-configured for DHCP. If a Static or BootP network configuration is required, change the Boot Mode as described in **Static IP on page 8**. Connect an RJ-45 cable to the card and it will receive an IP address from the DHCP server. Contact the DHCP administrator to obtain the IP address using the Liebert IntelliSlot Unity card's MAC address. The MAC address is printed on the card's faceplate.

If the DHCP administrator is not available or there is no way of determining the IP address assigned by the DHCP server, use a computer with a direct Ethernet connection to the Liebert IntelliSlot Unity card, and the Autoconfiguration IPv4 Address convention described in **2.1.2 - Connect an Ethernet Cable** to access the card's Web page and configure the card. To see the card's last DHCP-assigned IP address, click the *Communications* tab, then on the left side menu select *Support* > *Active Networking*. The table of information will show the last IP address assigned by the DHCP server. The card may retain that IP address when it reconnects to the DHCP network because most DHCP systems reuse the same IP address for the same device.





2.1.1.2 Static IP

To assign a static IP address, use the Ethernet connection to configure the card. Proceed to **2.1.2 - Connect an Ethernet Cable** and **2.2 - Change User Names and Passwords Immediately**.

2.1.2 Connect an Ethernet Cable

1. Connect a computer running a Microsoft Windows operating system (Microsoft Windows® XP with SP2 [64-bit] or SP3 [32-bit] or later) to the card by plugging a network cable into the RJ-45 port on the computer and the Liebert IntelliSlot Unity card.
2. Autoconfiguration, which is normally enabled on computers running Microsoft Windows operating systems, will automatically negotiate the communication settings. This takes about one minute.

NOTE

If the computer does not automatically connect, verify that autoconfiguration is enabled by:

Open the Command Prompt window from the computer's Start menu.

*Enter ipconfig/all to verify that Autoconfiguration is enabled on the computer and that an Autoconfiguration IPv4 Address has been assigned: Enabled = Yes (see **Figure 2-1**). An Autoconfiguration IPv4 Address begins with 169.254.)*

3. If the Ethernet adapter being used to attach to the card does not show an Autoconfiguration IPv4 Address, open a new Command Prompt and type *ipconfig/renew* and press Enter. This forces the computer to acquire an Autoconfiguration IPv4 Address.
4. When the computer has an Autoconfiguration IPv4 Address, open a browser window on the computer and type *169.254.24.7* (the card's default Autoconfiguration IPv4 Address) in the URL address field. The card's Web page will appear.

Figure 2-1 Command prompt access

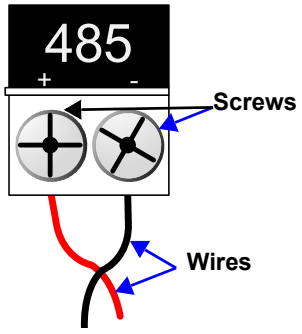
```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection
   Physical Address. . . . . . . . . : E0-DB-55-E2-3F-54
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1dc0:2a66:a01f:f92a%11(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.249.42(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 266394453
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-18-9B-0A-82-E0-DB-55-E2-3F-54
```

2.1.3 Connect an RS-485 Serial Cable

For Building Management Systems using serial network connections, an RS-485 serial cable connection will be used.

Liebert IntelliSlot Unity cards come with an Adapter RJ-45-2POS Terminal Block. The adapter has two screw terminals to attach the ends of a RS-485 cable for communicating to a building management system.

1. Find the serial cable from the building management system. If it already has an RJ-45 connector on the end, determine whether it uses the same pin-out as the Liebert IntelliSlot Unity card's connector. If the pin-out is the same as the Liebert IntelliSlot Unity card connector's pin-out, skip to **Step 7**.
2. Strip the ends of the positive (typically red) and negative (typically black) leads on the RS-485 cable so that enough bare wire is exposed for connection, about 1/4" (6mm).



NOTE

No bare wire should be exposed when the connection is completed.

3. Position the adapter so the side with the positive and negative marks is face up. The small markings are on the same side as the screw heads, as shown at right.

4. Loosen the screw to the positive terminal and insert the red wire far enough to insert the bare wires into the terminal block under the screw, then tighten the screw.
5. Be careful not to break the wires.
6. Repeat **Step 3** with the negative terminal and the black wire.
7. Plug the cable into the 485 RJ-45 port on the Liebert IntelliSlot Unity card.

2.2 Change User Names and Passwords Immediately

NOTE
*Emerson recommends changing the administrative and general user names and passwords **immediately** to safeguard protected configuration and control areas of the Liebert IntelliSlot Unity card.*

The administrative user name and password are set at the factory: *Liebert* and *Liebert* (case-sensitive). All printable characters are valid except \ : ' < > ~ ? " #

The general user name and password are also set at the factory: *User* and *User* (case-sensitive). The general user has access only to non-protected configuration and control areas of the Liebert IntelliSlot Unity card.

To change the user names and passwords:

1. Select the *Communications* tab > *Configuration* > *User*.
2. Click the *Edit* button and enter the factory-set administrator user name (*Liebert*) and password (*Liebert*).
3. Click *OK*.
4. Enter a new administrator user name and password.
5. Re-enter the administrator password to confirm it.
6. Enter a new general user name and password.

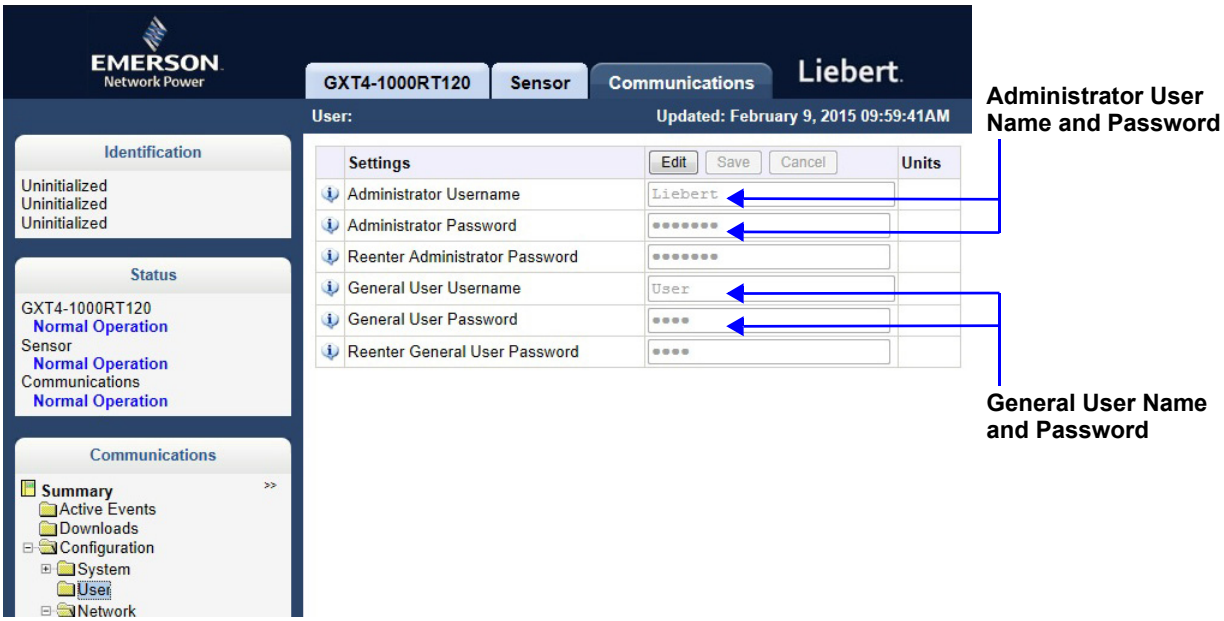
7. Re-enter the general user's password to confirm it.
8. Click *Save* button to confirm the changes or *Cancel* to discard them.

NOTE

Record the new user names and passwords and save them in a secure place where they can be found if forgotten.

A lost password cannot be retrieved. If the password is lost, the card must be reset to factory defaults and reconfigured.

Figure 2-2 Change administrator and general user names and passwords



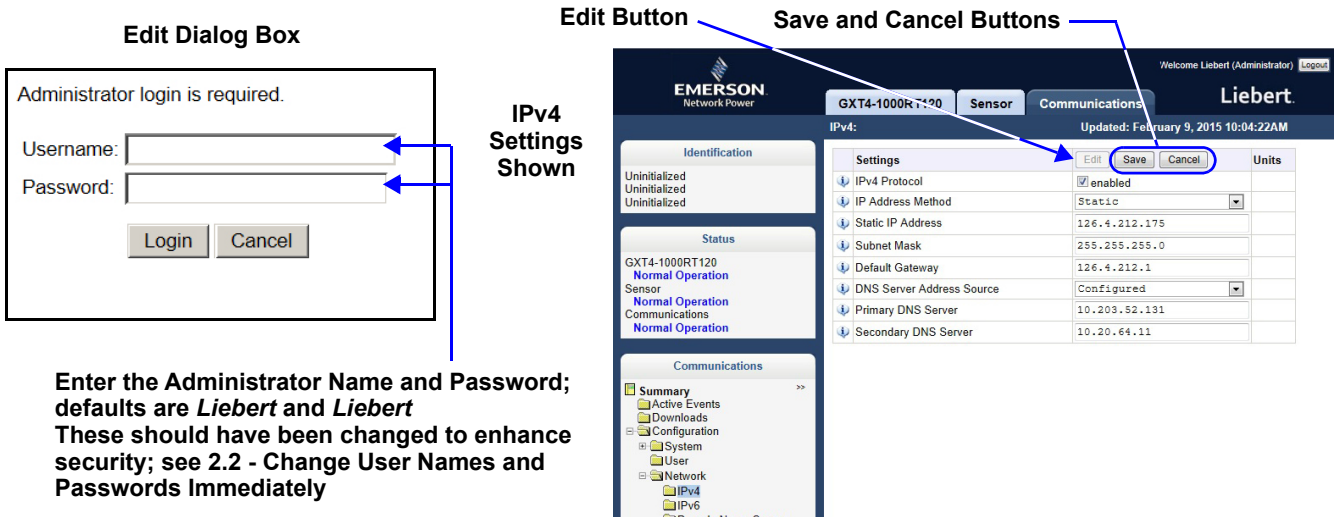
2.3 Configure the Card

The Liebert IntelliSlot Unity card requires minor configuration, such as choosing the IP/Web communication interface, serial RS-485 communication interface, or both. The default for IP/Web communication is IPv4, but this can be changed to IPv6 for greater security; contact your network administrator to determine whether it is compatible with your network. To choose the communication interface refer to **Figure 2-3**:

1. Select *Communications* tab > *Configuration* > *Network*.
2. Enable the protocol, either IPv4 or IPv6, that will be used to communicate with the Liebert IntelliSlot Unity card and with the Liebert equipment.
   a. Click either *IPv4* or *IPv6*.
   b. Click *Edit*.
   c. When prompted with a login display, enter the user name and password (the defaults are *Liebert* and *Liebert*).
   d. Click to check *enabled*.
   e. Enter the desired or assigned IP address along with the rest of the required networking information. Contact your system administrator if necessary.

3. Click *Save* to confirm the changes or *Cancel* to discard them.
   The changes take effect after the card is restarted.

Figure 2-3 Enabling the communication protocol—IPv4 or IPv6



2.4 Installing Multiple Liebert IntelliSlot Unity Cards in a System

More than one Liebert IntelliSlot card may be installed in a system, but circular routes and duplicate node IDs must be avoided during installation. The instructions below apply if the second card to be installed is a Liebert IntelliSlot Unity card. If the second card is not a Liebert IntelliSlot Unity card, follow instructions in the user manual for that card.

Before beginning installation of a second Liebert IntelliSlot card, verify that the first card functions properly.

If the first card is a Liebert IntelliSlot card, but not a Liebert IntelliSlot Unity card, and if both cards connect to the same Ethernet network, then you should disable the router function on the first card. This will avoid circular routes. Follow instructions in the user manual for the first card.

If the first and second cards are both Liebert IntelliSlot Unity cards, steps must be taken to avoid duplicate Emerson Protocol MSTP node IDs. By default, the two cards would use the same node ID, and one or both cards would report a duplicate node error and fail to communicate with the system.

The default node ID for a Liebert IntelliSlot Unity card is 0, so the second card should use 1 or 2 preferably, or 127 if necessary. Contact your system administrator about the proper node ID for the second card, then perform the steps below.

1. Open a Web browser and navigate to the second Liebert IntelliSlot Unity card.
2. Click *Communications* tab > *Configuration* > *Emerson Protocol* > *MSTP*.
3. Click *Edit* and enter a password and username if required.
4. Enter the new node ID.
5. Click *Save* to confirm the changes or *Cancel* to discard them.
6. Restart the card:
   a. Select the *Communications* tab > *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

2.5 Security Best Practices

The default settings on the Unity card support a fast installation and start-up to get basic communication services up and running quickly. Proper security of critical infrastructure equipment requires proper configuration of ALL communication services. This section summarizes the settings to examine to reduce the risk of unauthorized access to critical infrastructure equipment through a Unity card.

Table 2-1 provides a list of items to review. Each should be reviewed, configured based on the operational needs for managing the equipment, and verified that the settings support the desired operational functionality without adding unnecessary or unauthorized access to critical infrastructure equipment. A reference to the proper section in this document is provided for configuring each item.

Table 2-1 Settings to review and verify to reduce risk of unauthorized access to critical infrastructure equipment

Item	Description	Reference
Accounts & Passwords	Change the admin and user account names and passwords immediately to eliminate default credential access.	**2.2 - Change User Names and Passwords Immediately**
IP Network Access	Enable/disable IPV4 and IPV6 network access to the Unity Card - disable unused network access.	**2.3 - Configure the Card**
Telnet and SSH Access	Enable/disable telnet and SSH access for diagnostic and configuration support - disable when not in use.	**5.4.3 - Configuration—Network Folder**
Web Service Protocol	Select HTTPS to use SSL encryption when accessing data through the web user interface.	**5.4.4 - Configuration—Web Server Folder**
SSL Certificates	When using HTTPS, install your own SSL Certificates from a trusted certificate authority or generate alternative self-signed certificates	**5.4.4.1 - Certificate**
Password Protect Web Access	Enable to require users to login before any device information is displayed to the user.	**5.4.4 - Configuration—Web Server Folder**
Remote Write Web Access	Disable to require all updates to the device and card be made through a local interface, via an Autoconfiguration connection with a PC directly connected to the Unity card or through the device's local user interface display (if available). **WARNING!** - Only disable this if you are absolutely sure that you do not need to administer the managed device or the Unity card through a remote web browser session.	**5.4.4 - Configuration—Web Server Folder**
Communication Protocols	Enable/disable BACnet, Modbus, SNMP, and YDN23 protocols - disable any that are unused.	**3.0 - Enable Communication Protocols**
BACnet Settings	Set Managed Device Write Access to Read-Only to prevent changes to the device through the BACnet interface.	**3.1.2 - Enable BACnet Protocol**
Modbus Settings	Set Managed Device Write Access to Read-Only to prevent changes to the device through the Modbus interface; Select the appropriate option for Limit Network Access Type to restrict which systems may request Modbus data from the device - access may be open to any system, limited to those on the same subnet as the device, or limited to only those from systems on a Trusted IP Address List.	**3.1.1 - Enable Modbus Protocol**

Table 2-1 Settings to review and verify to reduce risk of unauthorized access to critical infrastructure equipment (continued)

Item	Description	Reference
SNMP Version Settings	Enable/disable the desired SNMP version(s); Consider using SNMPv3 with user authentication and encryption.	**3.1.3.1 - Configure SNMP Settings**
SNMP Access Table Settings	For each SNMPv1/v2c Access table entry, set the SNMP Access Type to Read-Only to prevent changes to the device from the hosts identified in the table entry.	**3.1.3.1.4 - Configure SNMPv1/v2c Access Settings**
SNMP Community Strings	Change the SNMP v1/v2c Trap and Access Community Strings from their default values.	**3.1.3.1.3 - Configure SNMPv1 Trap Settings** and **3.1.3.1.4 - Configure SNMPv1/v2c Access Settings**
SNMPv3 Settings	Use the SNMPv3 Authentication and Privacy settings to make SNMPv3 communications more secure.	**3.1.3.1.2 - Configure SNMPv3 User Settings**
YDN23 Settings	Set Managed Device Write Access to Read-Only to prevent changes to the device through the YDN23 interface.	**5.5.4 - Protocols—YDN23 Folder**
Emerson Protocol Settings	Enable/disable the Emerson Protocol which is used by Emerson Network Power management applications for accessing device data.	**5.4.6 - Configuration—Emerson Protocol Folder**

For added security, the local network firewall and gateway may be restricted to allow only the necessary traffic on the required network ports. The ports used by the Unity card are listed in **Table 2-2**. Some port settings may be changed by the administrator.

Table 2-2 Ports used by the Unity card

Network Service		Port Used	Default?	Can be Modified?
Web	HTTP	TCP 80	Yes	Yes
	HTTPS	TCP 443	Yes	Yes
DNS		TCP & UDP 53	Yes	No
NTP		TCP & UDP 123	Yes	No
SMTP		TCP 25	Yes	Yes
SSH		TCP & UDP 22	Yes	No
Telnet		TCP 23	Yes	No
SNMP		UDP 161, 162	Yes	Only trap port 162 may be changed
Modbus TCP		TCP 502	Yes	Yes
BACnet IP		UDP 47808	Yes	Yes
Emerson Protocol		UDP 47808	Yes	Yes
LIFE		TCP 80	Yes	Yes

Details for configuration of all options are provided in the remainder of this User Manual.

3.0 Enable Communication Protocols

The Liebert IntelliSlot Unity card will communicate with equipment and third-party systems over these protocols:

- BACnet IP
- BACnet MSTP
- Modbus TCP
- Modbus RTU
- SNMP
- YDN23

NOTE

No more than two protocols may be enabled on one card.

- *Only one version of BACnet may be selected, either BACnet IP or BACnet MSTP*
- *Only one version of Modbus may be selected, either Modbus TCP or Modbus RTU*
- *Only one of the protocols can use the 485 port; choosing two 485 protocols will cause conflicts.*

NOTE

Some Building Management Systems can be configured to send continuous updates for device setpoints, usually setting the same value. The BMS should be configured to send, on a sustained average, no more than two writes per second to the device. This will allow the device to catch up after a burst of updates when required while allowing other communication with the device to proceed.

3.1 Enable Protocols

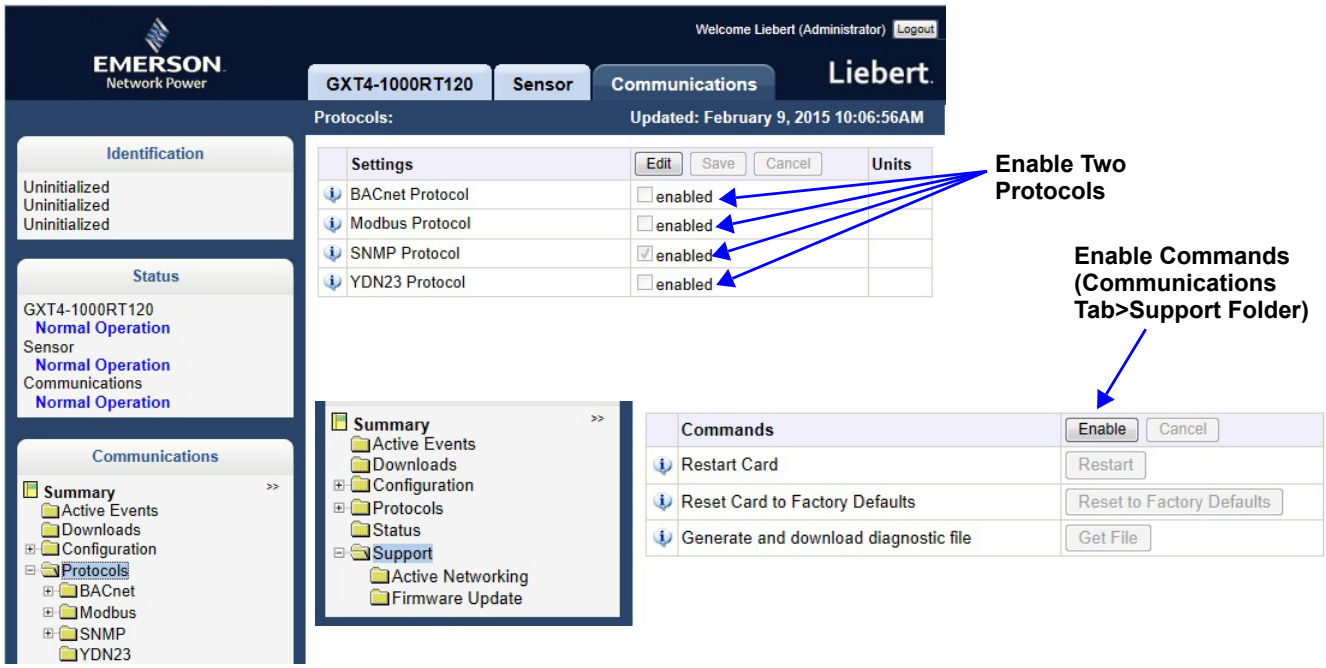
Protocols may be enabled after a card has been installed and configured. After a protocol is enabled, it must be configured, which requires opening that protocol's folder (*Communications* tab > *Protocols* > (desired protocol).

To enable two communication protocols:

1. Select *Communications* tab > *Protocols*.
2. Click *Edit* and enter the administrator user name and password.
3. Put a check mark next to the protocols to use—Only two may be enabled; only one of the two can use the 485 port.
4. Click *Save* to confirm the changes or *Cancel* to discard them.

5. Configure the protocols selected. See **5.0 - Editing the Liebert IntelliSlot Unity Card Configuration**.
6. Restart the card (See **5.7 - Communications—Support Folder**).
   a. Select *Communications* tab > *Support*.
   b. Enable the commands.
   c. Click *Restart*.

Figure 3-1 Enable protocols; enable commands



3.1.1 Enable Modbus Protocol

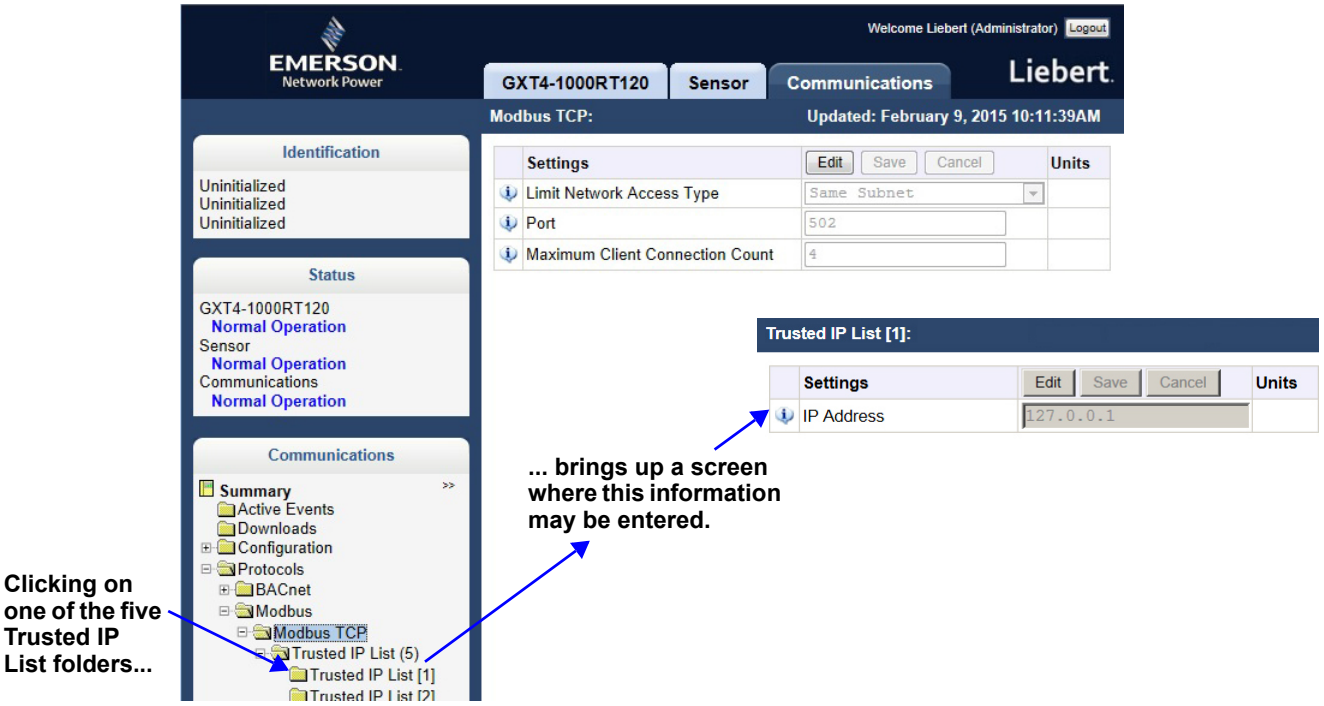
Protocols may be enabled after a card has been installed and configured.

1. Select *Communications* tab > *Protocols* > *Modbus*.
2. Click *Edit* and enter a User name and password.
3. Select the access level (**Read Only** or **Read/Write**).
4. Select the Modbus interface, (**Modbus TCP** or **Modbus RTU**).
5. Click *Save* to confirm the changes or *Cancel* to discard them.
6. Configure the Modbus interface chosen.
   See **3.1.1.1 - Configure Modbus TCP** or **3.1.1.2 - Configure Modbus RTU**.
   For descriptions of the settings, see **5.5.2 - Protocols—Modbus Folder**.

3.1.1.1 Configure Modbus TCP

1. Select the *Communications* tab > *Protocols* > *Modbus TCP*.
2. Click *Edit* and enter a User name and password if required.
3. Set the *Limit Network Access Type* by choosing from the drop-down list (**Open**/**Same Subnet**/**Trusted IP List**).
   Refer to **5.5.2.1 - Modbus TCP Folder** for additional details.
4. Enter the *Port* to be used by the Modbus Server to listen for and respond to Modbus protocol requests based on limit Network Access Type setting.
5. Enter the *Maximum Client Connection Count*.
6. Click *Save* to confirm the changes or *Cancel* to discard them.
7. Restart the card to confirm the changes.
   a. Select *Communications* tab > *Support*.
   b. Enable the commands.
   c. Click *Restart*.

Figure 3-2 Modbus TCP-Trusted IP List



3.1.1.2 Configure Modbus RTU

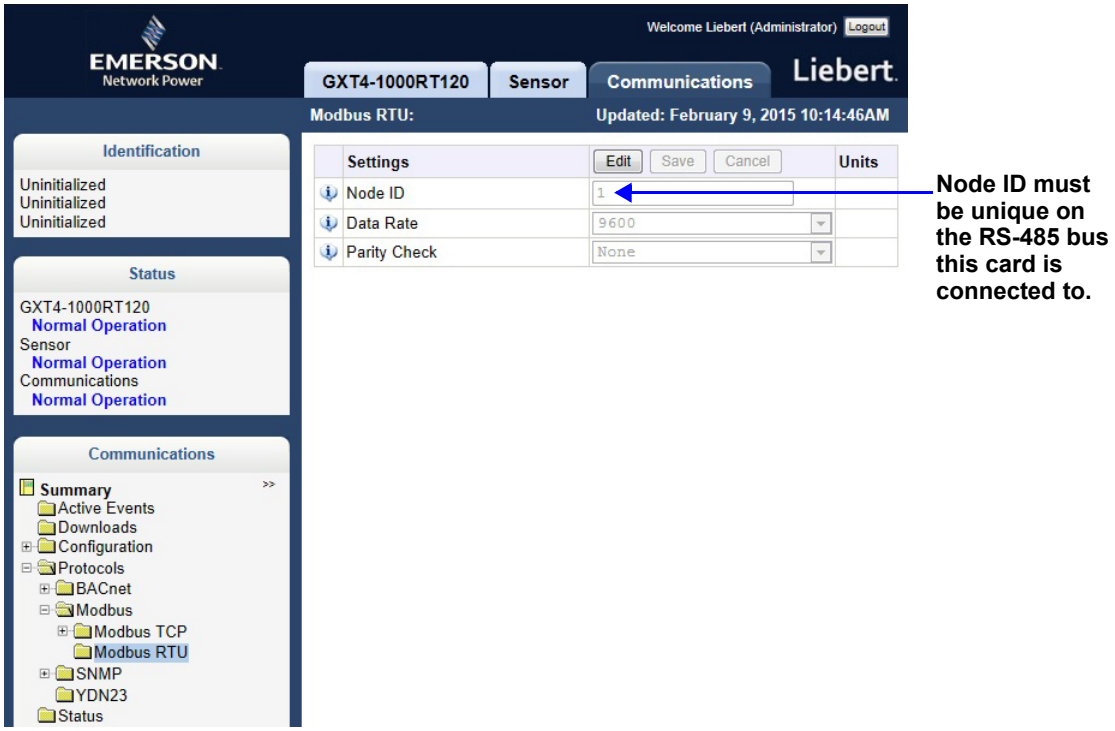
1. Select the *Communications* tab > *Protocols* > *Modbus RTU*.
2. Click *Edit* and enter a user name and password if required.
3. Set the *Node ID* and the *Baud Rate*.
   - The Node ID defaults to 1, but must have a value from 1 to 255 that is unique among devices connected through the RS-485 interface.
   - The default baud rate is 9600; 19200 and 38400 are also available.

   For additional description of the settings, see **5.5.2.2 - Modbus RTU Folder**.

NOTE
Contact your system administrator if you are uncertain about the settings.

4. Click *Save* to confirm the changes or *Cancel* to discard them.
5. Restart the card to confirm the changes.
   a. Select *Communications* tab > *Support*.
   b. Enable the commands.
   c. Click *Restart*.

Figure 3-3 Modbus-RS-485



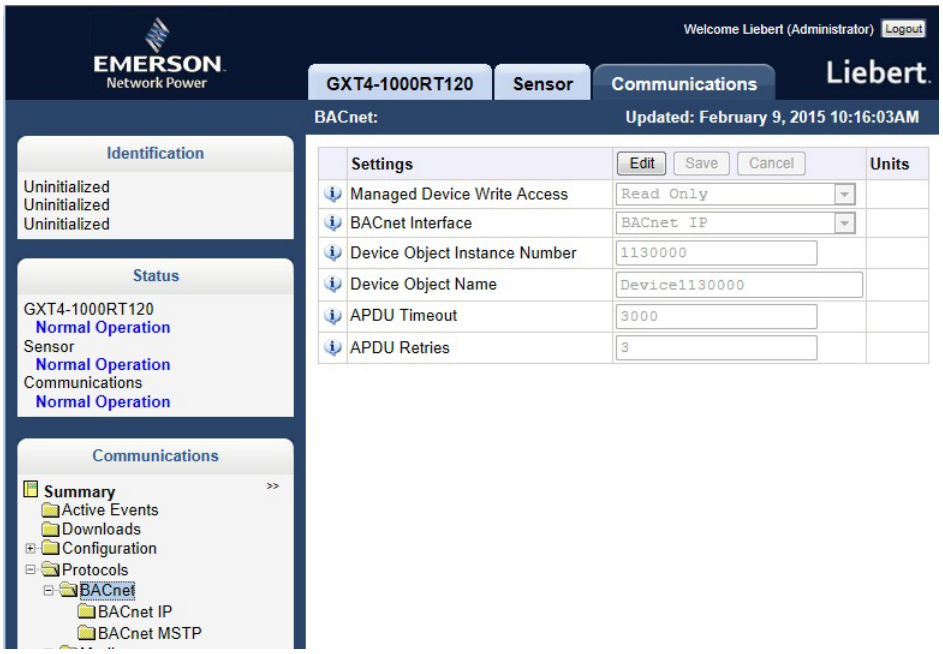
3.1.2 Enable BACnet Protocol

NOTE

Contact your system administrator or building management system administrator if you are uncertain about the settings.

1. Select *Communications* tab > *Protocols* > *BACnet*.
2. Click *Edit* and enter a user name and password if required.
3. Enter the *Managed Device Write Access level* (**Read Only** or **Read/Write**).
   This determines a user's ability to change settings in the Liebert IntelliSlot Unity card.
4. Choose the *BACnet interface*: **BACnet IP** or **BACnet MSTP**.
5. Set the *Device Object Instance Number*.
6. Set the *Device Object Name*.
7. Set the *APDU Timeout*.
8. Set the *APDU Retries*.
9. Click *Save* to confirm the changes or *Cancel* to discard them.
10. Configure the BACnet interface chosen, see **3.1.2.1 - Configure BACnet IP Protocol** or **3.1.2.2 - Configure BACnet MSTP Protocol**.
    For description of the settings, see **5.5.1 - Protocols—BACnet Folder**.

Figure 3-4 BACnet protocol settings



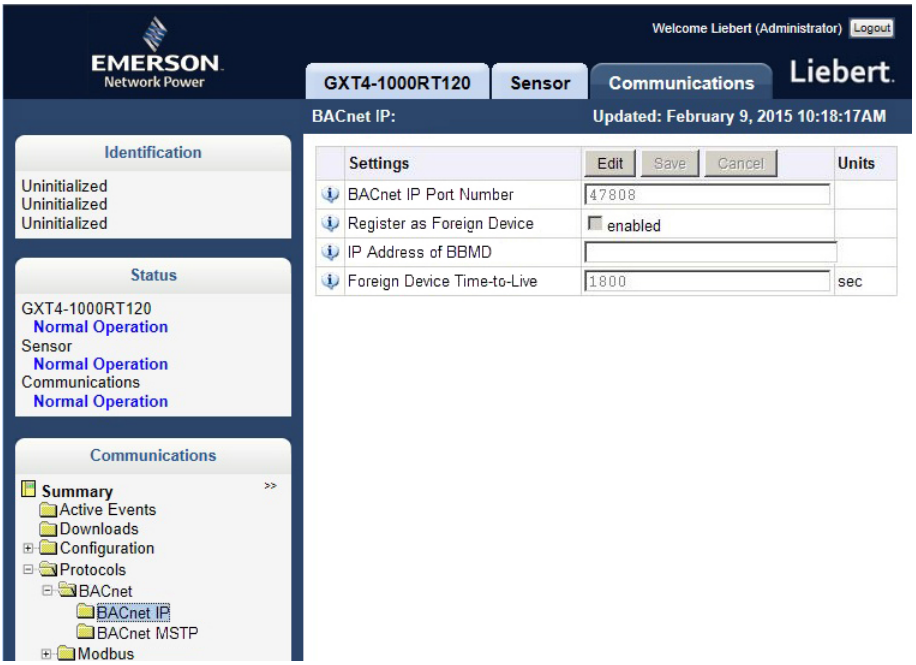
3.1.2.1 Configure BACnet IP Protocol

NOTE
Contact your system administrator if you are uncertain about the settings.

1. Select *Communications* tab > *Protocols* > *BACnet IP*.
2. Click *Edit* and enter a User name and password if required.
3. Set the *BACnetIP/Port Number*.
   If the Liebert IntelliSlot Unity card is on a different subnet (a possibility when the monitored units are part of a Liebert SiteScan network or other third-party monitoring service):
   a. Choose whether or not to enable *Register as Foreign Device*.
   b. Enter the *IP address of the BBMD* (BACnet Broadcast Management Device).
   c. Enter a time in seconds for *Foreign Device Time-to-Live*.

   For descriptions of the settings, see **5.5.1.1 - BACnet IP Folder**.
4. Click *Save* to confirm the changes or *Cancel* to discard them.
5. Restart the card to activate the changes.
   a. Select the *Communications* tab > *Support*.
   b. Enable the commands.
   c. Click *Restart*.

Figure 3-5 BACnet IP



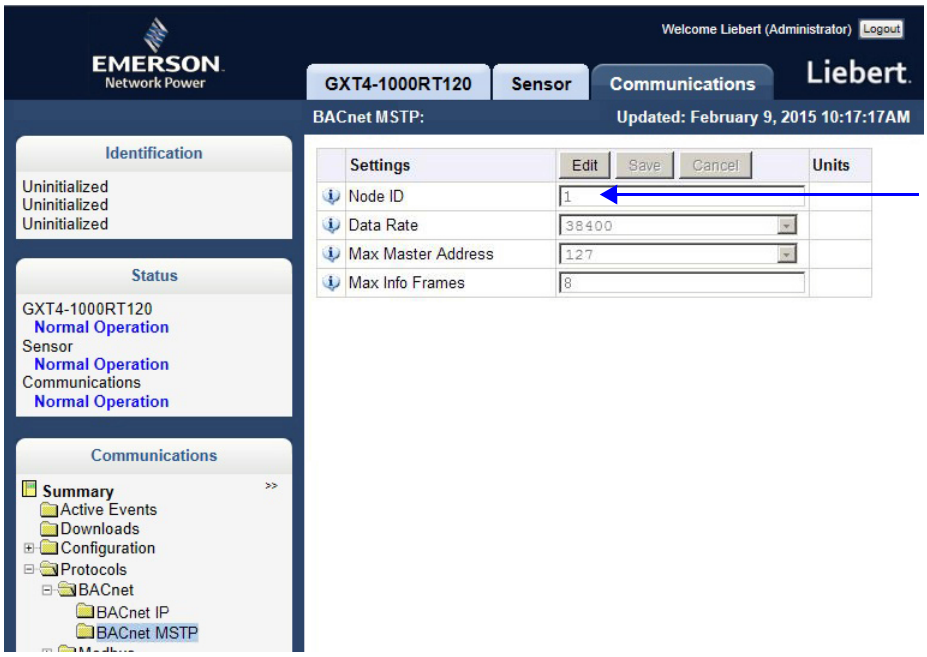
3.1.2.2 Configure BACnet MSTP Protocol

NOTE
Contact your system administrator if you are uncertain about the settings.

1. Select *Communications* tab > *Protocols* > *BACnet MSTP*.
2. Click *Edit* and enter a user name and password if required.
3. Set the BACnet MSTP *Node ID*.
   - The Node ID defaults to 1, but must have a value from 1 to 255 that is unique among devices connected through the RS-485 interface.
4. Set the BACnet MSTP *Data Rate*.
5. Set the BACnet MSTP *Max Master Address*.
6. Set the BACnet MSTP *Max Info Frames*.

   For descriptions of the settings, see **5.5.1.2 - BACnet MSTP Folder**.
7. Click *Save* to confirm the changes or *Cancel* to discard them.
8. Restart the card to activate the changes.
   a. Select *Communications* tab > *Support*.
   b. Enable the commands.
   c. Click *Restart*.

Figure 3-6 BACnet MSTP



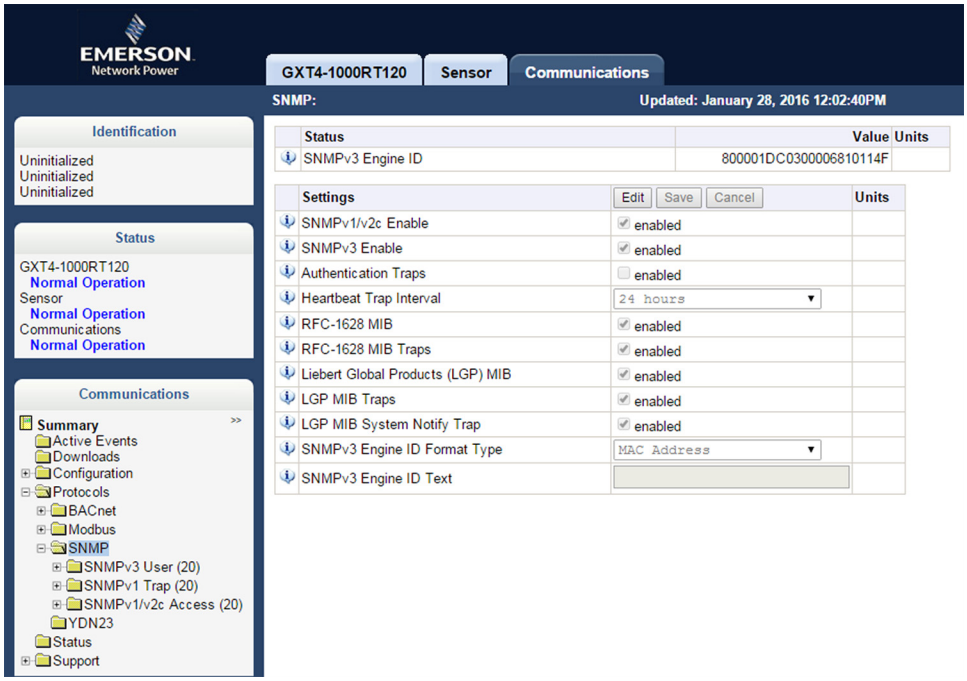
3.1.3 Enable SNMP

SNMPv1/v2c and SNMPv3 are enabled by default. The protocols may be configured or their default values may be accepted. Authentication Traps are not enabled by default. The default Heartbeat Trap interval is 24 hours; this can be disabled or the interval may be changed.

1. Select the *Communications* tab > *Protocols* > *SNMP*.
2. Click *Edit* and enter a User name and password if required.
3. To enable *Authentication Traps*, click to check mark the box.
4. To change the *Heartbeat Trap Interval*, choose a time from the drop-down list or choose **Disabled** to prevent any heartbeat traps from being sent.
   - The interval times offered are 5 minutes, 30 minutes, or 1, 4, 8, 12 or 24 hours.
5. For each trap, choose whether or not to disable or set the interval to one of the periods on the menu.

   For descriptions of the settings, refer to **5.5.3 - Protocols—SNMP Folder**.
6. Click *Save* to confirm the changes or *Cancel* to discard them.
7. Restart the card to activate the changes.
   a. Select the *Communications* tab > *Support*.
   b. Enable the commands.
   c. Click *Restart*.

Figure 3-7 SNMP



3.1.3.1 Configure SNMP Settings

SNMPv3 Users or SNMPv1/v2c Trap and Access settings must be made before SNMP access or notifications can occur. The Liebert IntelliSlot Unity card permits up to 20 SNMPv3 Users, up to 20 SNMPv1 Trap targets, and up to 20 SNMPv1/v2c Access addresses.

The required changes vary according to the type of SNMP protocol used:

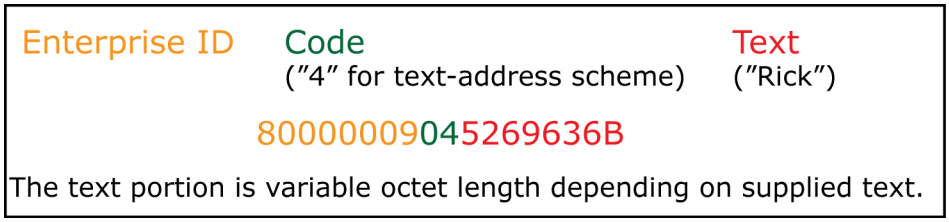
- SNMPv1 must have trap settings.
- SNMPv2c must have Access settings.
- SMPv3 users must have settings configured and the method for generating the Engine ID may be selected.
- the access settings for SNMPv1/v2c are separate from SNMPv1 trap settings.

3.1.3.1.1 Select SNMPv3 Engine ID Format

By default, the Engine ID is automatically generated using the MAC address. Optionally, you can select a text-based ID instead.

1. Select *Communications* tab > *Protocols* > *SNMP*.
2. Click *Edit* and enter a User name and password if required.
3. Edit the settings:
   Refer to **5.5.3**, **Protocols—SNMP Folder**, **page 60**, for descriptions of the settings and options.
   - In *SNMPv3 Engine ID Format Type*, select **MAC Address** or **Text**.
   - If you selected Text, type the text on which the generated engine ID will be based.
   - Click *Save* to confirm the changes, or click on *Cancel* to discard them.
     The new engine ID is not displayed until after rebooting the card in **Step 4**.
     The text-generated engine ID is a hexadecimal representation of ASCII characters similar to that shown in **Figure 3-8**.

Figure 3-8 SNMP Engine ID generated using text-format scheme



NOTE
If the format type or text for the Engine ID are incomplete or invalid, the Engine ID is generated based on the MAC Address.

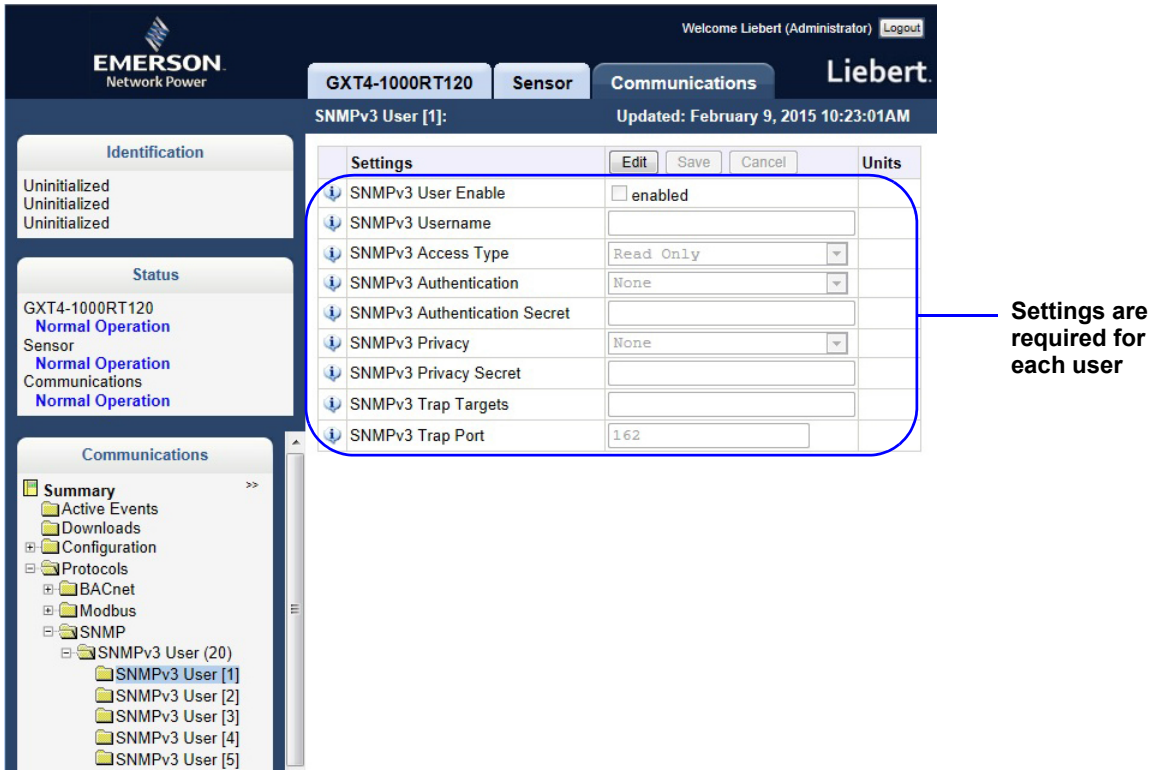
4. Restart the card to activate the changes.
   a. Select the *Communications* tab > *Support*.
   b. Enable the commands.
   c. Click *Restart*.

3.1.3.1.2 Configure SNMPv3 User Settings

The settings must be made for each user who will receive notifications.

1. Select *Communications* tab > *Protocols* > *SNMP* > *SNMPv3 Users Setting (20)* > *SNMPv3 Users Setting (1)*.
2. Click *Edit* and enter a User name and password if required.
3. Enter the information and set the permissions appropriate to the user, **Figure 3-9**.
   For descriptions of the settings and options, see **5.5.3.1**, **SNMPv3 User Folder**, **page 62**.
4. Click *Save* to confirm the changes, or click on *Cancel* to discard them.
5. Repeat **Steps 1** through **4** for additional users.
6. Restart the card to activate the changes.
   a. Select the *Communications* tab > *Support*.
   b. Enable the commands.
   c. Click *Restart*.

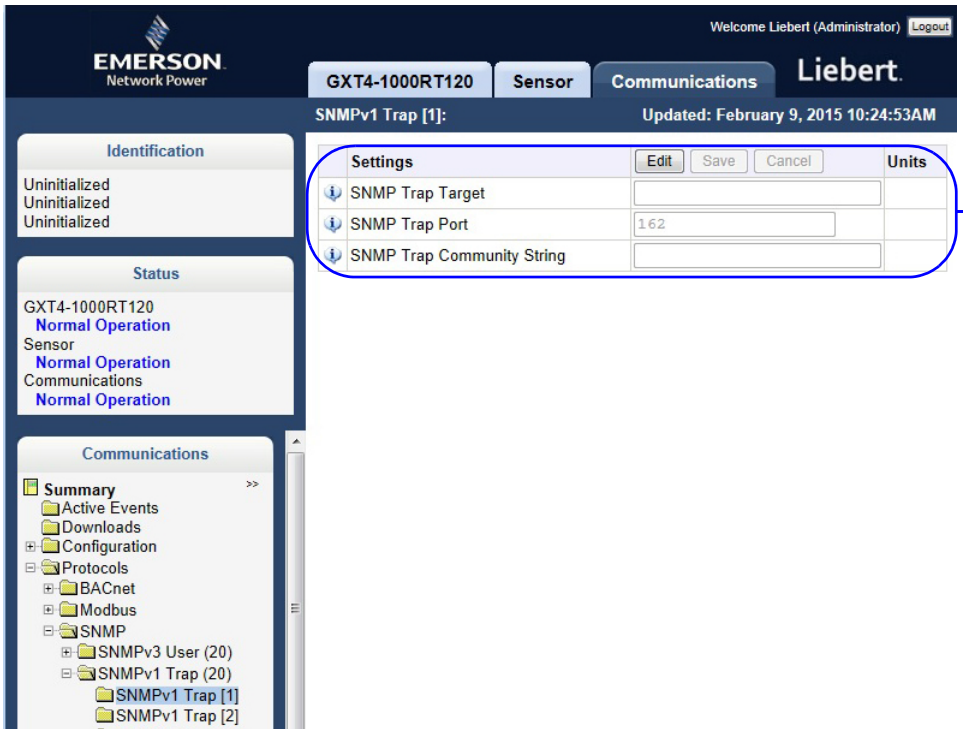
Figure 3-9 SNMPv3 user settings



3.1.3.1.3 Configure SNMPv1 Trap Settings

1. Select *Communications* tab > *Protocols* > *SNMP* > *SNMPv1 Trap (20)*.
2. Click *Edit* and enter a User name and password if required.
3. Enter the information and set the permissions appropriate to the user, **Figure 3-10**. For descriptions of the settings, see **5.5.3.3 - SNMPv1 Trap Folder**.
4. Click *Save* to confirm the changes or *Cancel* to discard them.
5. Repeat **Steps 1** through **4** for any additional users.
6. Restart the card to confirm the changes.
   a. Select the *Communications* tab > Support.
   b. Enable the commands.
   c. Click *Restart*.

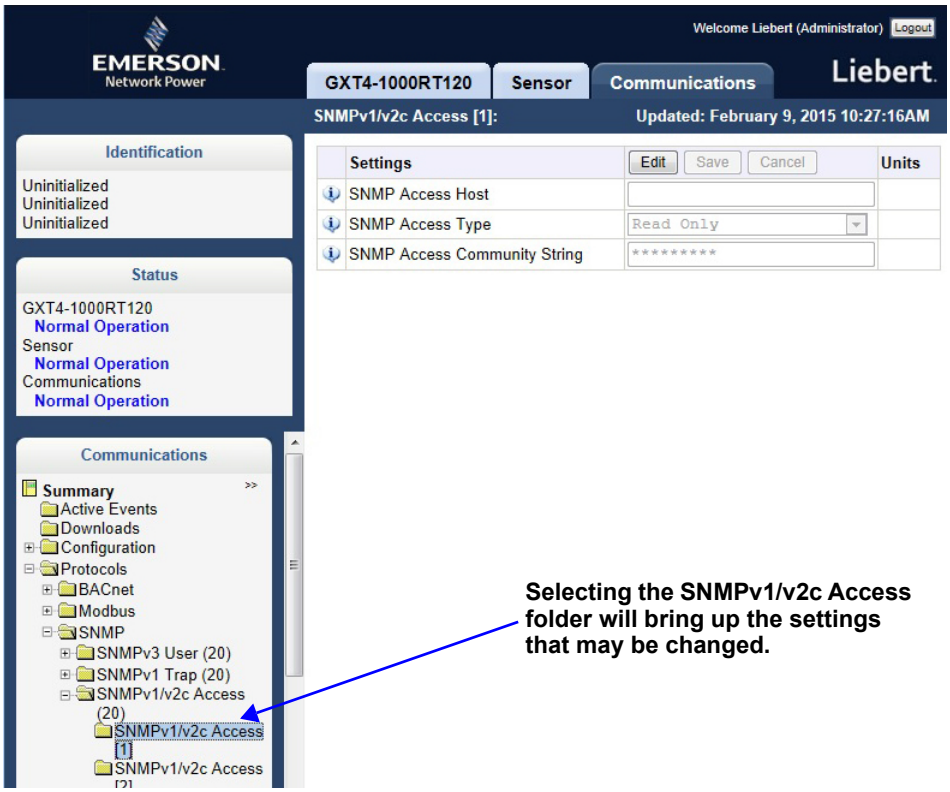
Figure 3-10 SNMPv1 trap settings



3.1.3.1.4 Configure SNMPv1/v2c Access Settings

1. Select *Communications* tab > *Protocols* > *SNMP* > *SNMPv1/v2c Access (20)* > *SNMPv1/v2c Access (1)*.
2. Click *Edit* and enter a User name and password if required.
3. Enter the information and set the permissions appropriate to the user, **Figure 3-10**.
   For description of the settings and options, see **5.5.3.4**, **SNMPv1/v2c Access Folder**, **page 66**.
4. Click *Save* to confirm the changes or *Cancel* to discard them.
5. Restart the card to confirm the changes.
   The card must be restarted before another user's settings may be changed.
   a. Select the *Communications* tab > *Support*.
   b. Enable the commands.
   c. Click *Restart*.

Figure 3-11 SNMPv1/v2c Access settings



3.2 Download Protocol Mappings

The Liebert IntelliSlot Unity Card's permits downloading files listing information available from a managed device for each enabled protocol. The listings identify the data available from the device and how that data will be represented, or mapped, into a particular protocol.

To download a data mapping list, click the *Managed Device* tab, then *Summary* > *Downloads*. The Data Mapping Files heading shows mapping files for each enabled protocol:

- *BACnetDataMap.txt* for BACnet IP and BACnet MSTP
- *ModbusDataMap.txt* for Modbus TCP and Modbus RTU
- *SNMP_Events.txt, SNMP_Parameters.txt, SNMP_upsMibEvents.txt*, and *SNMP_upsParams.txt* for SNMP v1/v2c/v3
- *Ydn23DataMap.txt* for YDN23

More information about BACnet and Modbus protocol mapping is available in the Liebert IntelliSlot Modbus RTU, Modbus TCP, BACnet MSTP and BACnet IP Reference Guide (SL-28170) at Liebert's Web site: **www.liebert.com**

The SNMP MIB files are also available for download from the Web site.

Page intentionally left blank.

4.0 Liebert IntelliSlot Unity Card Web Page Layout

Default settings in the Liebert IntelliSlot Unity card permit using it immediately after installation to monitor the equipment the card is installed in. The Web interface permits customizing the information to ease monitoring the equipment and troubleshooting problems. Users can name the equipment, enter a location, set up email and text alerts and change equipment settings.

NOTE
The Edit button will be grayed-out if the settings on a menu cannot be changed.

4.1 Web Page Sections

Each Web page displayed by the Liebert IntelliSlot Unity card has these main areas (see **Figure 4-1**):

- Identification
- Status
- Tab Menus
- Detail

Identification

Displays the System Name, System Location and System Description

Status

Displays the status of the monitored equipment, the Liebert IntelliSlot Unity card and any Liebert SN sensors connected to the card.

Tab Menus

The Liebert IntelliSlot Unity card has two tabs by default: the Managed Device tab, which will display the name of the monitored equipment, and the Communications tab. A third tab, the Sensor tab, appears if Liebert SN sensors have been installed. The tab selected determines the menu shown.

- **Managed Device tab**—Information pertaining to the equipment being monitored and controlled. Refer to **4.3 - Managed Device Tab Menus** for details. The tab label refers to the type of Liebert unit the card is installed in. For example, the Managed Device tab for a card installed in a Liebert GXT4-1000-RT120 UPS will be labeled GXT4-1000-RT120 (see **Figure 4-1** for this example). **Figure 4-2** shows a Web page for a Liebert IntelliSlot Unity card installed in a Liebert CRV.
- **Communications tab**—Information about the Liebert IntelliSlot Unity card, such as the overall event status of the equipment and communication interface, logs of third-party information, communication settings, third-party protocol settings and system status. Refer to **4.4 - Communications Tab Menus** for details.
- **Sensor tab**—Information about Liebert SN sensors, if any are installed, including status or data from each sensor and sensor configuration settings. When sensors are connected to the card, this tab appears between the Managed Device tab and the Communications tab. The tab is not shown when no sensors are connected to the card (see **Figure 4-3**). Refer to **4.5 - Sensor Tab Menus—Shown Only if a Sensor is Connected** for details.

Detail

Displays detailed information about the device based on the menu selection made in the Tab Menu area. Edits to the device and its configuration are made in this section.

Figure 4-1 Web page sections, UPS example

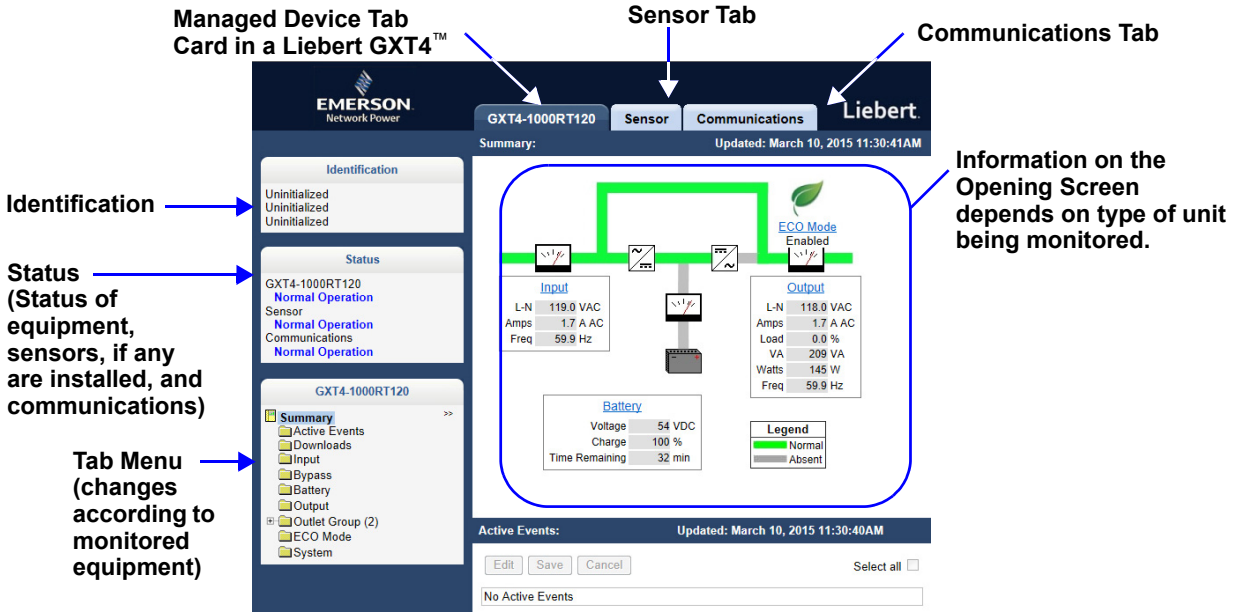


Figure 4-2 Web page sections, Thermal Management unit example

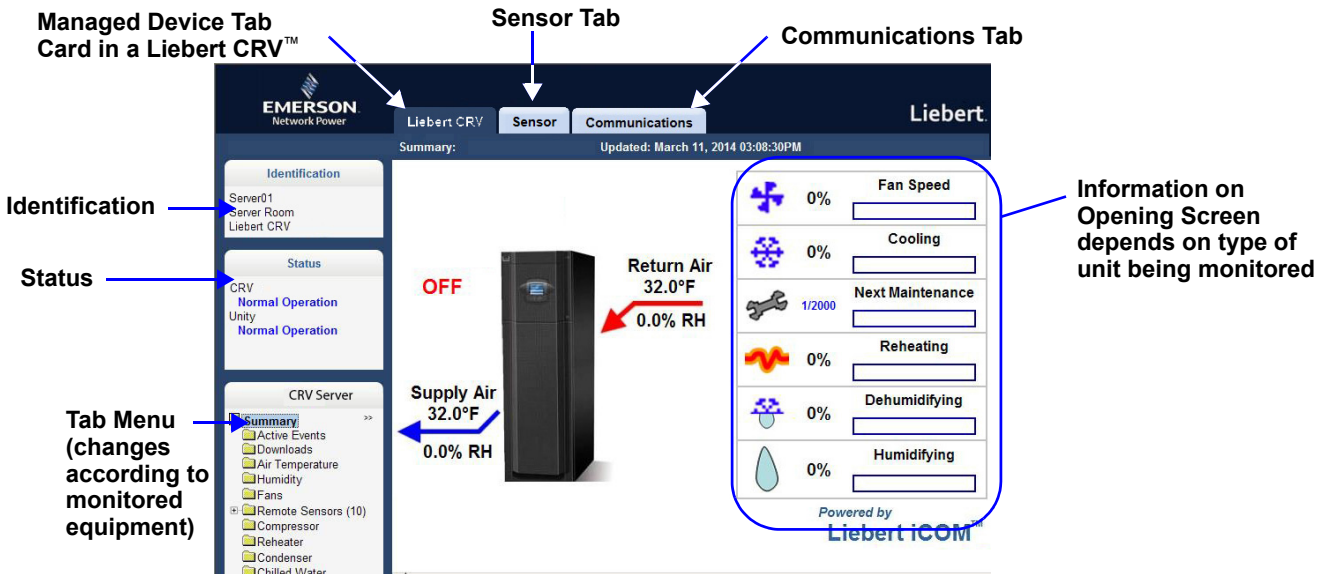
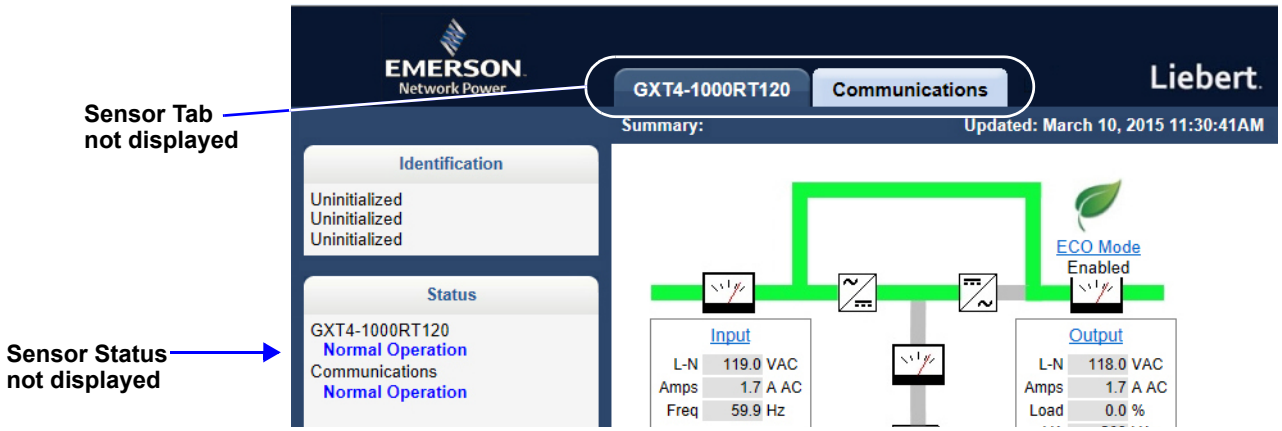


Figure 4-3 Managed Device Web page without sensors



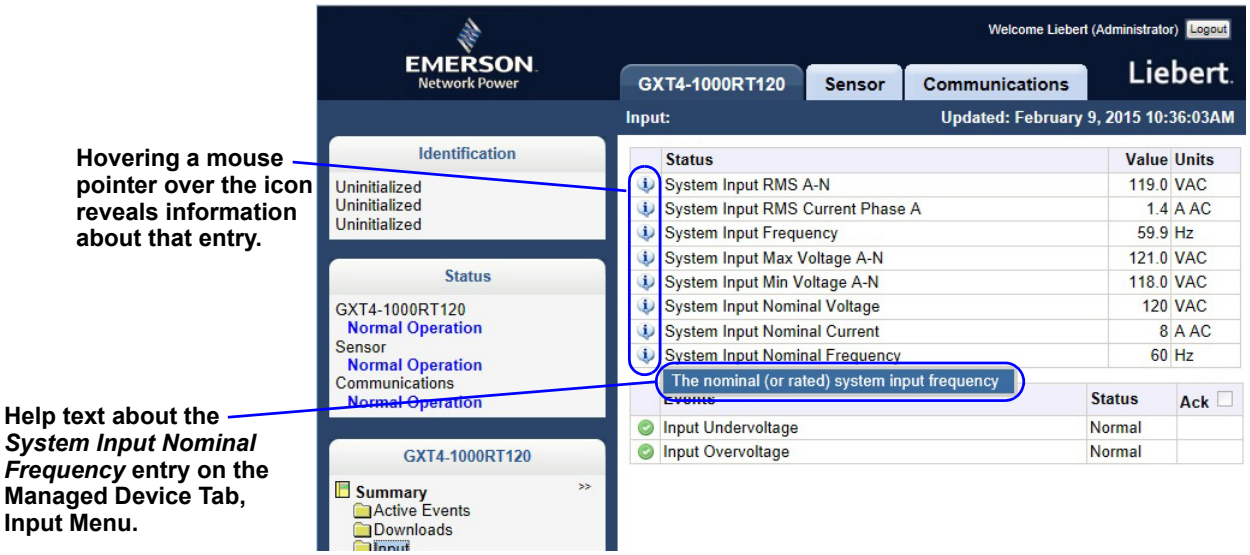
4.2 Help Text

Each Web page shown by the Liebert IntelliSlot Unity-DP card has informational text that is revealed by hovering a mouse pointer over the icon to the left of the Status, Events or Settings row, as shown below. The Web page may display any of six icons beside the Status, Events or Setting entry:

Table 4-1 Help text and icons

Icon	Description
	a check mark (?) on a green button (Event Normal)
	an **i** on a blue button (Event Information)
	an **x** on a red button (Event Alarm)
	an exclamation point (**!**) on a yellow shield (Event Warning)
	an exclamation point (**!**) on a red button (Event Critical)
	an **i** in a word balloon (Tool Tip).

Figure 4-4 Help text on mouse-over



4.3 Managed Device Tab Menus

Menus on the Managed Device tab list only data that is relevant to the equipment being monitored. For example, menus shown by a Liebert IntelliSlot Unity card installed in a UPS differ from menus shown by a card installed in Thermal Management equipment. Information on those menus will also differ depending on the equipment the card is installed in.

Figure 4-5 Managed Device tab examples, Liebert GXT4™ and Liebert CRV™

4.4 Communications Tab Menus

The Communications tab shows the overall event status of the equipment and communication interface. It contains logs of third party information, communications settings, third party protocol settings and system status information as detailed below.

Table 4-2 Communications tab menus

Communications tab Menus	Description	See Details:
Active Events	Displays the current event activity	page 40
Downloads Agent (or Unity Card) Logs Event Logs Data Logs Other files	Downloading files to text-accessible, comma-delimited or tab-delimited files ease troubleshooting.	page 40
Configuration System User Network Web Server LIFE Emerson Protocol Messaging	Displays information about the system setup, access, network connections, Emerson Protocol settings and whether email and SMS messaging are enabled	page 40
Protocols Modbus BACnet SNMP YDN23	Lists information and settings related to available third-party protocols employed to monitor equipment.	page 56
Status System Status System Restart Required LIFE™ device identity changed-LIFE™ needs to be reconfigured RS-485 Port Conflict Duplicate Emerson Protocol MSTP Node ID Duplicate BACnet MSTP Node ID	Shows the overall condition of the system and whether a restart is needed to activate configuration changes; restart is performed only from the Support Folder	page 68
Support Agent time and Date Agent Model Agent App Firmware Version Agent App Firmware Label Agent Boot Firmware Version Agent Boot Firmware Label Agent Serial Number Agent Manufacture Date Agent Hardware Version GDD Version FDM Version Product Sequence ID Restart Card Reset Card to Factory Defaults (see **Note** below) Generate and download diagnostic file Firmware Update Active Networking	Shows information needed for maintenance or troubleshooting and shortcuts to reboot the card, reset the Liebert IntelliSlot Unity card to its factory defaults and to update the card's firmware.	page 69 (Firmware Update also on page 75)

NOTE

The card may be reset to factory defaults manually by briefly pressing the reset button five times within 10 seconds.

Do not hold the reset button too long: Pressing the reset button and holding it for 5 seconds will restart the card without resetting it to factory defaults.

*To perform either function, insert a straight, non-conductive tool into the small hole on the front of the card (see **Figure 1-1** for the Reset Button's location).*

4.5 Sensor Tab Menus—Shown Only if a Sensor is Connected

When Liebert SN sensors are installed and connected to the sensor port on the Liebert IntelliSlot Unity card, the Sensor tab appears. It contains folders showing an overview of the installed sensors, the event status of the sensors, download links for log files and sensor configuration settings as detailed below.

Figure 4-6 Sensor tab menu

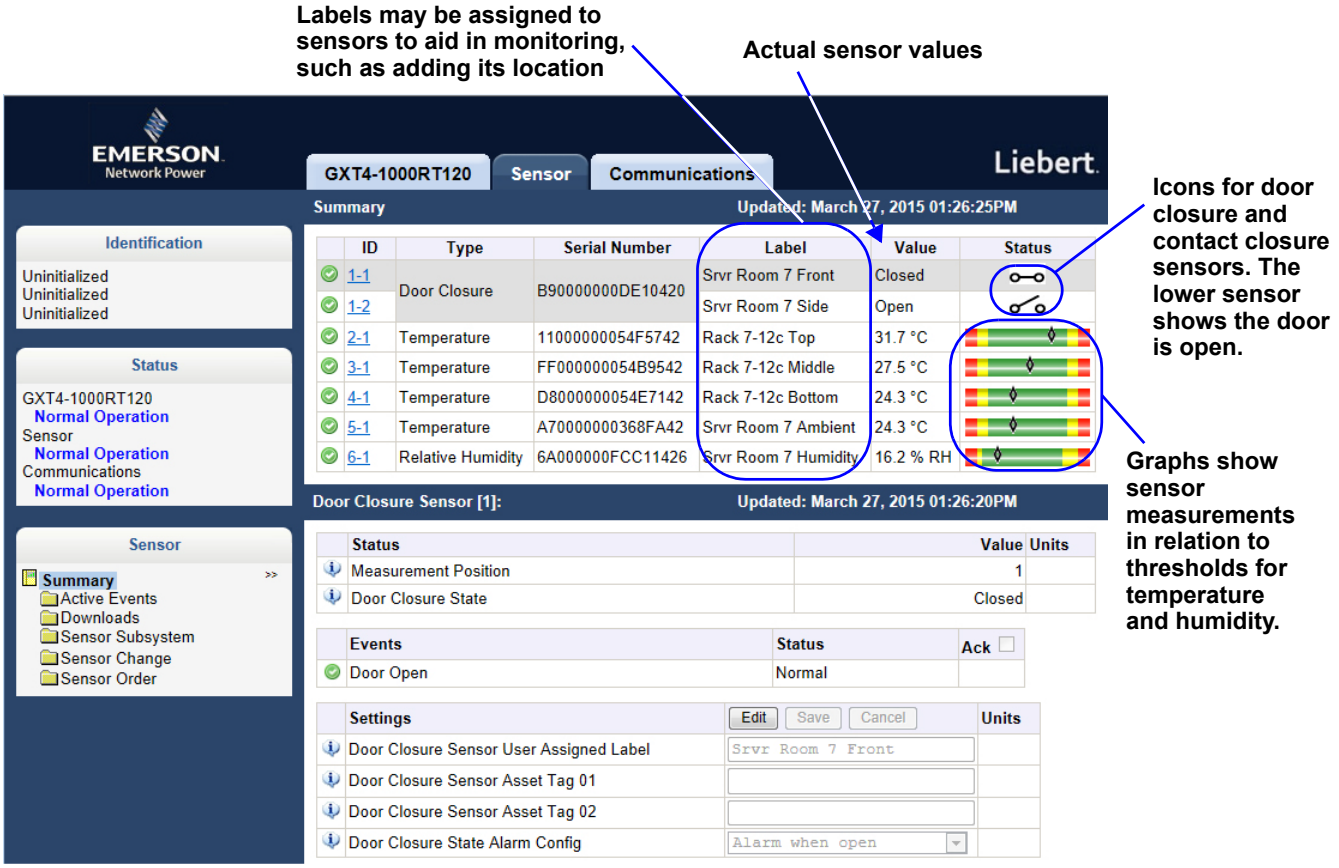


Table 4-3 Sensor tab folders

Sensor Tab Menus	Description
Summary	Displays a list of currently discovered sensors, with their status and values. Also displays a detail section about the sensor that is currently selected
Active Events	Displays a list of sensor events that are currently active.
Downloads	Displays a list of text files that can be downloaded. The files available are dependent on the current state of the card.
Sensor Server System Model Number System Status Too Many Sensors Slots Not Available Acknowledge Sensor Changes	Displays overall information about the sensors.
Sensor Change	Lists events showing sensors that have been added or removed. If the list has any entries, an Acknowledge button appears. Clicking the Acknowledge button clears the list. The Acknowledge button on this page has the same behavior as the Acknowledge button on the Sensor Server page.
Sensor Order	Displays a list of sensors, and allows setting the order in which the sensors are displayed on the Summary page.

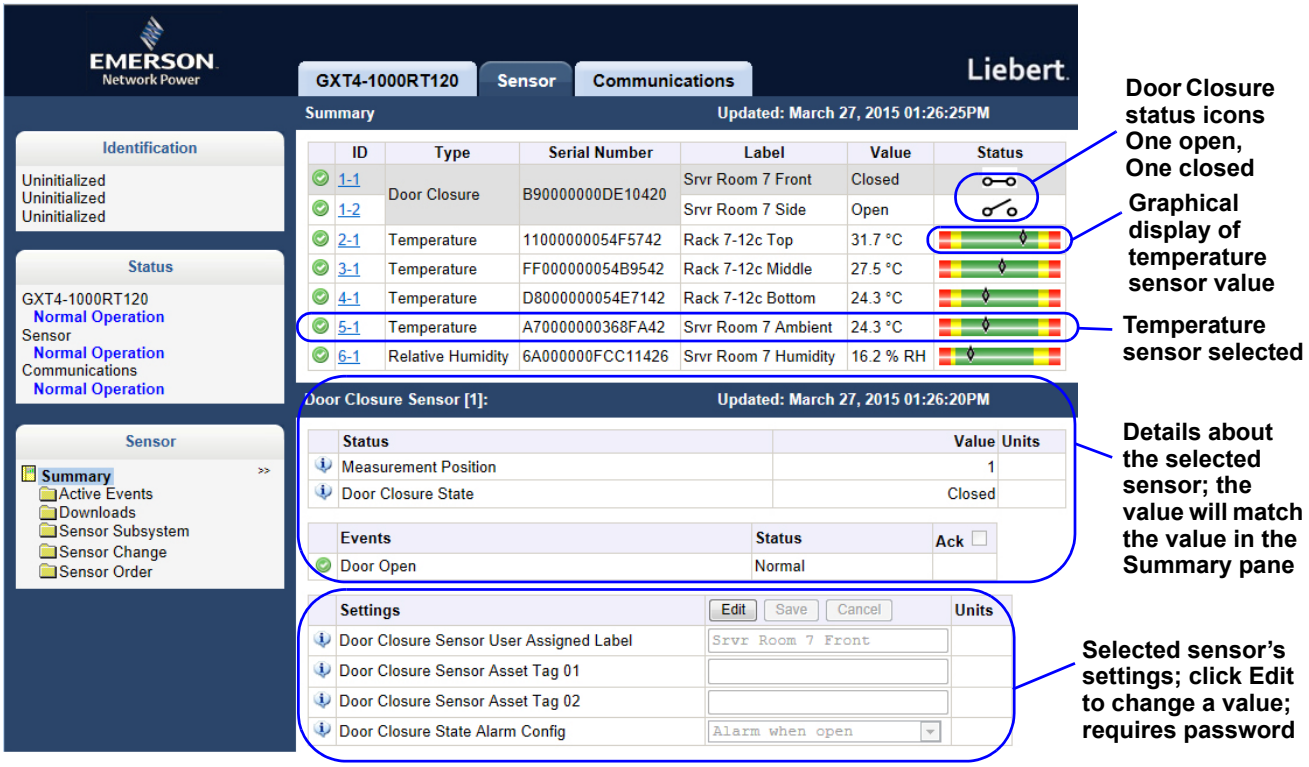
4.5.1 Sensor Tab Summary Page

The Sensor tab Summary Page shows the status of all installed sensors, details about any selected sensor and a Setting pane that permits changing a sensor's label, thresholds if applicable, alarm configuration and acknowledging alarms and events.

Selecting a sensor permits changing its settings at the lower part of the window.

Events may also be acknowledged on this window.

Figure 4-7 Sensor tab-Summary page layout



4.5.2 Sensor Tab Summary Page-Details Pane

The Details pane of the Sensor tab window appears when the Summary folder is selected. The area shows the status of all connected sensors (see **Figure 4-7**).

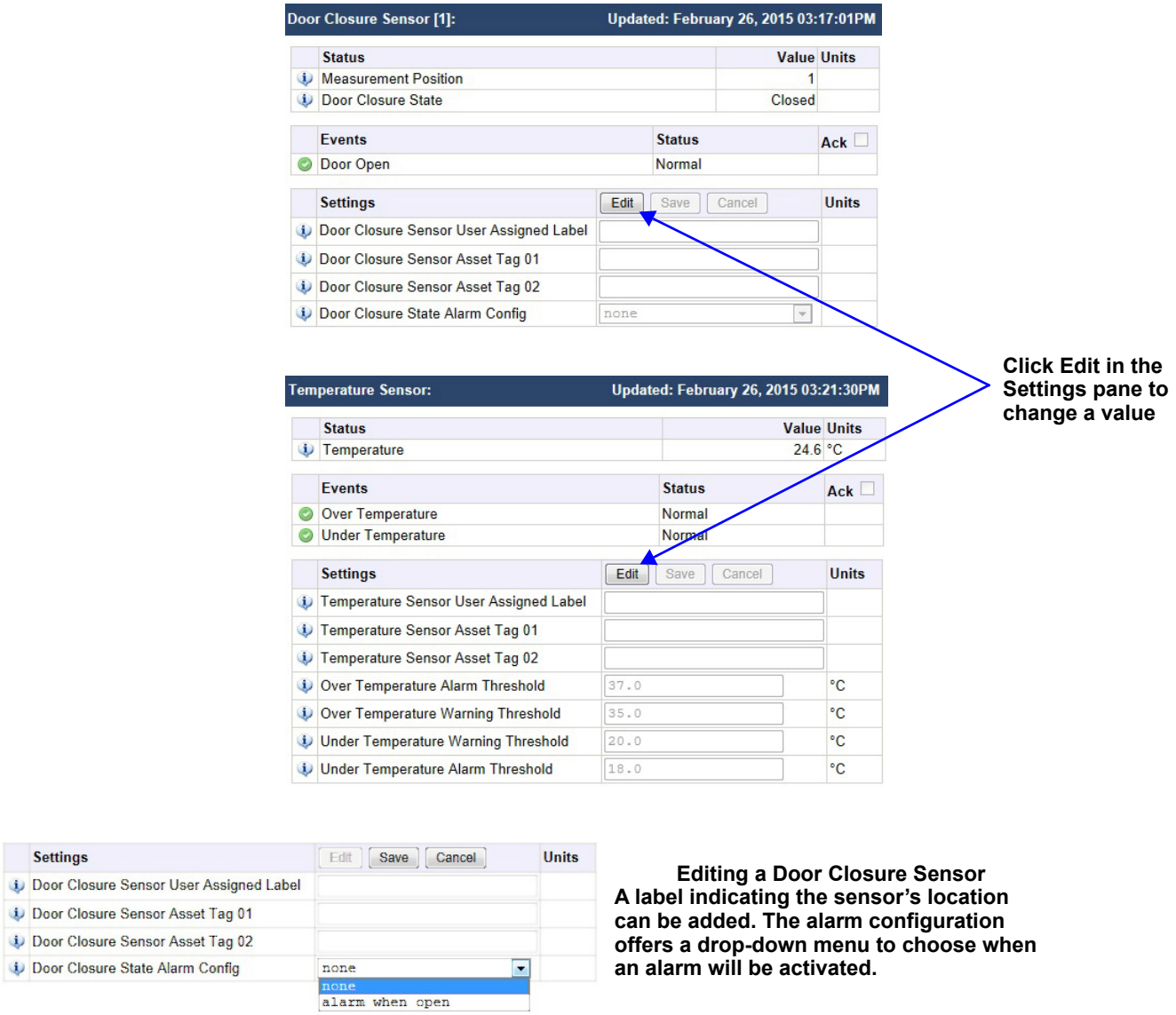
Supported sensors include:

- Temperature
- Humidity
- Door Closure
- Contact Closure
- Leak Detection

Selecting a sensor displays details for that sensor. The content of the details section is specific to the type of sensor selected. For example, a temperature sensor would show the temperature of the area where it is installed and a door sensor would show whether the door is open. The Unit of Measure used to display the temperature values is defined in the Display Temperature Units setting under *Communications* tab > *Configuration* > *System*. See **5.4.1 - Configuration—System Folder**.

Details for the sensors include the current state or reading, event status and whether the reading is above or below the threshold established in the Settings pane.

Figure 4-8 Sensor details—Door closure and temperature sensor examples



Editing a Door Closure Sensor
A label indicating the sensor's location can be added. The alarm configuration offers a drop-down menu to choose when an alarm will be activated.

4.6 Changing Sensor Order

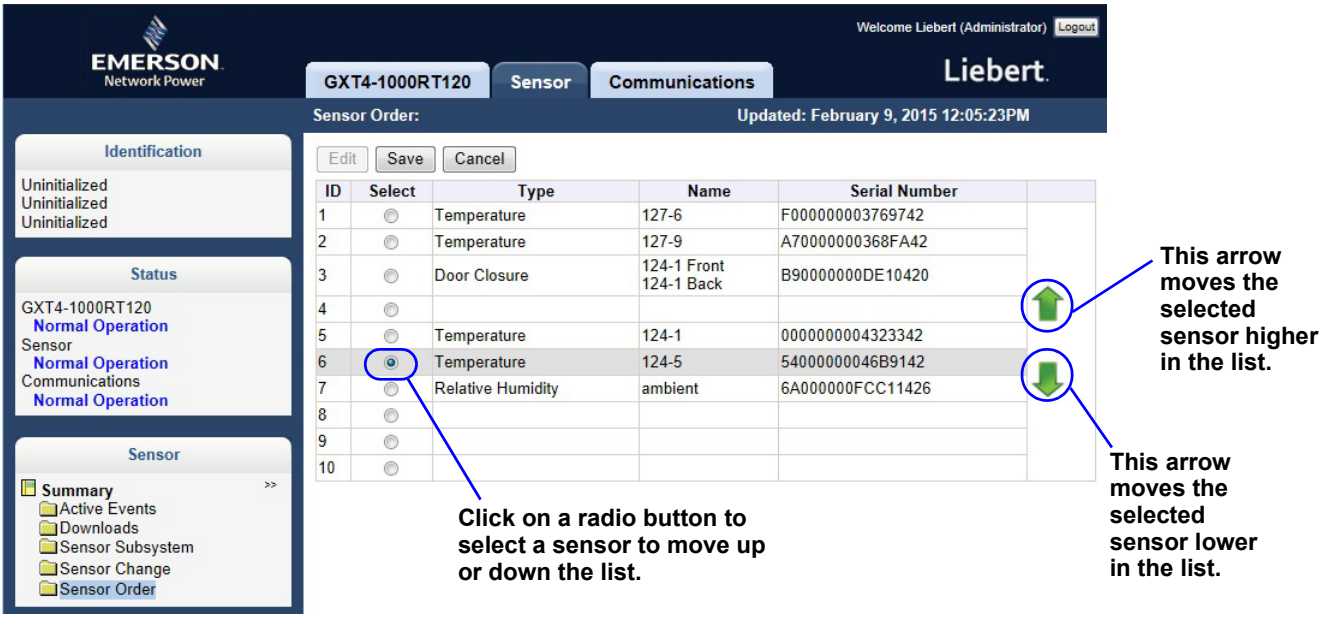
Sensors are listed in the order they are installed. The order can be changed to put sensors deemed more important at the top of the list.

To change the order of the sensor list:

1. Click *Sensor* tab > *Sensor Order*.
2. Click *Edit*.
3. Enter the user name and password.
4. Select the sensor to be moved higher or lower in the list.
   The radio button beside the sensor to be changed is highlighted.
5. Use the arrows at the right side of the list to move the sensor up or down.
6. Click *Save*.

Repeat the steps for any other sensors to be moved higher or lower in the list.

Figure 4-9 Changing sensor order



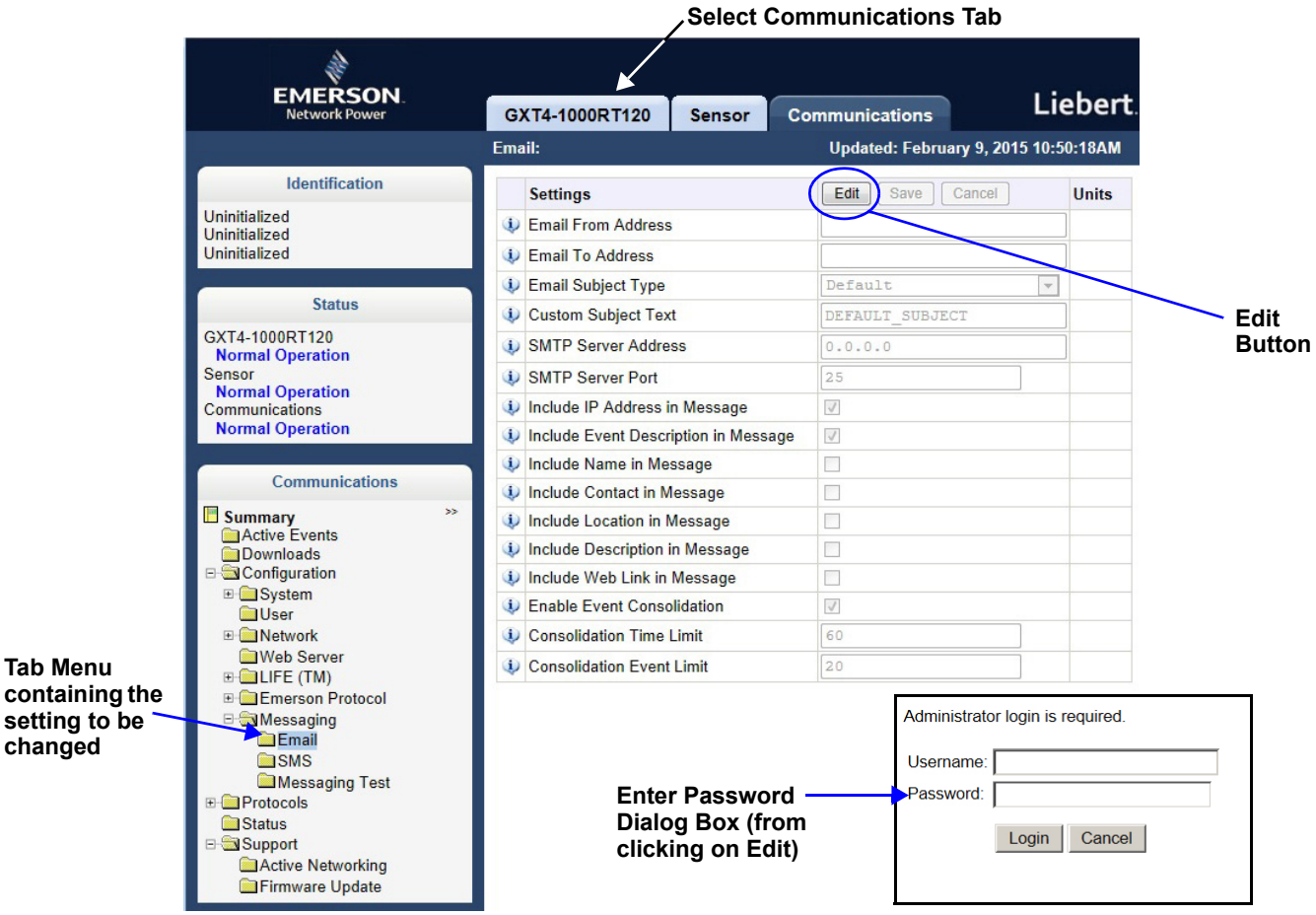
5.0 Editing the Liebert IntelliSlot Unity Card Configuration

The Web-based interface can be used to change settings for the Liebert IntelliSlot Unity card and for the monitored equipment. The following steps apply to making changes in all sections of the Liebert IntelliSlot Unity card.

To edit the configuration:

1. Open a Web browser and enter the card's IP address.
2. Click the *Communications* tab.
3. Select the menu in the Tab Menu area, **Figure 5-1**, that contains the configuration setting to be changed.
4. Click the *Edit* button near the top of the page.
5. Enter the administrator name and password for the Liebert IntelliSlot Unity card in the dialog box that opens (the default settings are *Liebert* and *Liebert).*
6. Click *OK*.
7. Change the settings.
8. Click *Save* to apply the changes or *Cancel* to discard them.

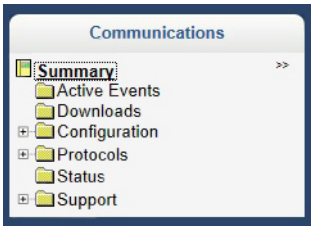
Figure 5-1 Editing configuration settings



5.1 Communications Tab Folders

The Communications tab of the web-based interface contains information about the overall event status of the equipment and communication interface. It presents logs of third-party information, communication settings, third-party protocol settings and system status information.

The Communications tab folders are shown at right.

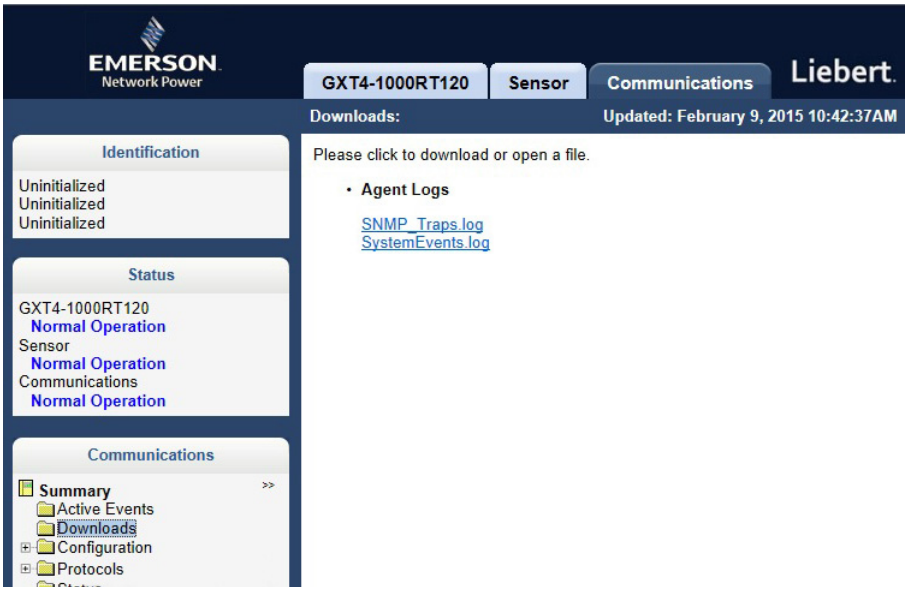


5.2 Communications—Active Events Folder

The Communications tab's Active Events folder contains no configurable settings. The folder displays events affecting the Liebert IntelliSlot Unity card.

5.3 Communications—Downloads Folder

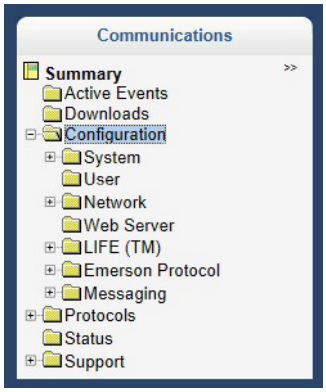
The Communications tab's Downloads folder contains no configurable settings. The folder displays links to download logs of third-party protocols that are enabled on the Liebert IntelliSlot Unity card. The logs help in configuring and troubleshooting communication between the Network Management or Building Management Systems being used to monitor the managed device.



5.4 Communications—Configuration Folder

The Configuration folder's top level displays the System Model Name of the Liebert IntelliSlot Unity card. This name is factory-set and cannot be changed (the **Edit** button is grayed out). The Configuration folder contains seven subfolders:

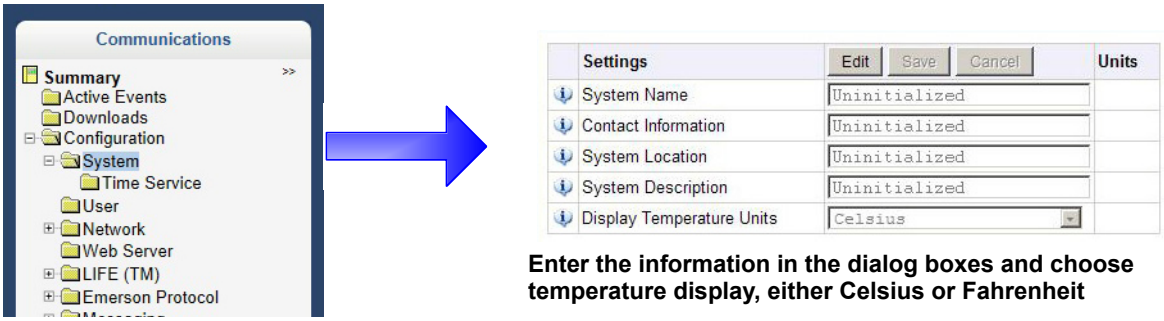
- System
- User
- Network
- Web Server
- LIFE™
- Emerson Protocol
- Messaging



5.4.1 Configuration—System Folder

The System subfolder displays general information about the monitored and managed device and the display of some data. Refer to **Figure 5-2**. The data displayed is set by the user and can assist in troubleshooting. To alter the information displayed, click on the **Edit** button, enter the administrator name and password and make changes. Click **Save** to save the changes; click **Cancel** to discard the changes.

Figure 5-2 Configuration folder, System subfolder

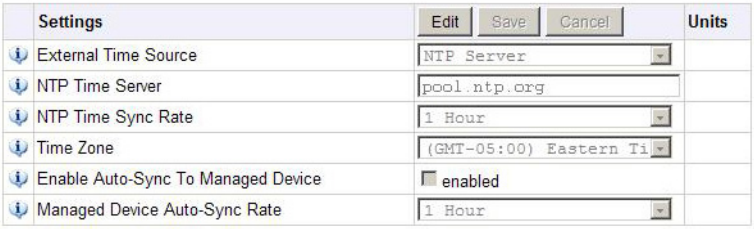


Enter the information in the dialog boxes and choose temperature display, either Celsius or Fahrenheit

5.4.1.1 Time Service Settings

The System Subfolder contains one folder: Time Service. Each setting offers either a menu of choices or an enable/disable check box. Users can set these parameters

Figure 5-3 Configuration folder, System subfolder, Time Service



Time Service setting options

External Time Source

The external source to be used for time synchronization.

NTP Time Server

Network Time Server (NTP) URL or IP address

NTP Time Sync Rate

The rate at which time will be synchronized with the Network Time Protocol server, if NTP is the external time source.

Time Zone

Time zone where the device is located.

Enable Auto-Sync to Managed Device

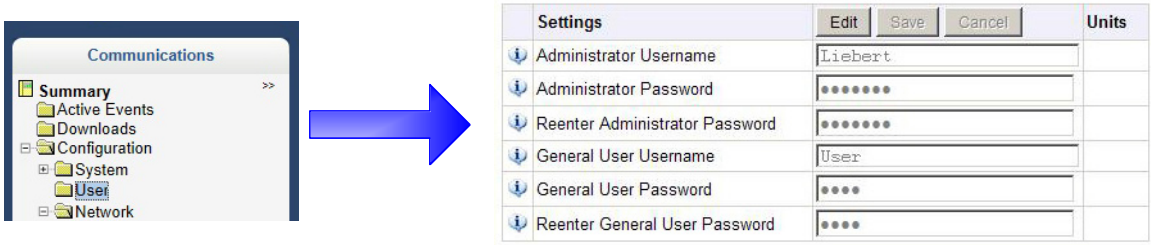
Enable automatic writing time to the managed device.

Managed Device Auto-Sync Rate

Rate at which time will be written to the managed device, if an external time source has been selected.

5.4.2 Configuration—User Folder

The User subfolder displays the administrator's and general user's name and password. Each can be changed. The default user name and password for the administrator are *Liebert* and *Liebert*. The defaults for the general user are *User* and *User*. To change either, click on **Edit**, enter the default username and password and enter the new information. Click on **Save** to accept the changes or click **Cancel** to discard the changes.



5.4.3 Configuration—Network Folder

The top level of the Network subfolder displays:

- Speed Duplex
- Domain Name Suffix List
- Telnet Server
- SSH Server

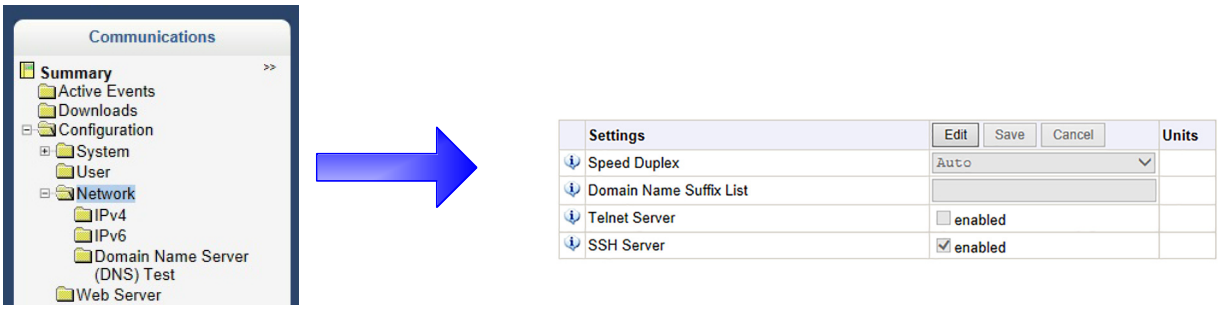
The Speed Duplex item selects the speed and duplex configuration of the card's Ethernet port. It is set to Auto by default. If it requires changing, contact the system administrator for the proper settings.

The Domain Name Suffix List is a listing of domain name suffixes for resolution of host names. If it requires changing, contact the system administrator for the proper setting.

The Telnet Server item allows disabling telnet access to the card to prevent unauthorized changes. The default setting disables telnet access.

The SSH Server item allows disabling SSH (Secure SHell) access to the card to prevent unauthorized changes. The default setting disables SSH access.

The Network subfolder contains three subfolders related to communication:

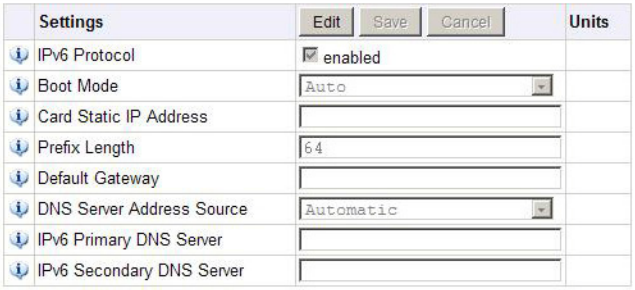


5.4.3.1 IPv4/IPv6

The IPv4 and IPv6 settings determine which Internet Protocol will be used for communication over the network connected to the Ethernet port. IPv4 and IPv6 networks will run in parallel (dual-stack network), but the protocols are different. See your network administrator to determine which protocol should be enabled and to determine the correct settings.

Figure 5-4 IPv4/IPv6 settings

IPv4 Settings



IPv6 Settings

IPv4 Settings

IPv4 Protocol

Enables IPv4 in the card

IP Address Method

Mode the card boots into to be a network ready device (Static, DHCP, BootP)

Static IP Address

Network address for the interface

Subnet Mask

Network mask for the interface which divides a network into manageable segments

Default Gateway

IP address of the gateway for network traffic destined for other networks or subnets

DNS Server Address Source

Source of DNS server identification (None, Automatic, Configured)

Primary DNS Server

Secondary DNS Server

IPv6 Settings

IPv6 Protocol

Enables IPv6 in the card.

IP Address Method

Mode the card boots into to be a network ready device (Static, Auto)

Static IP Address

Network address for the interface.

Prefix Length

Prefix length for the address that divides a network into manageable segments.

Default Gateway

IP address of the gateway for network traffic destined for other networks or subnets.

DNS Server Address Source

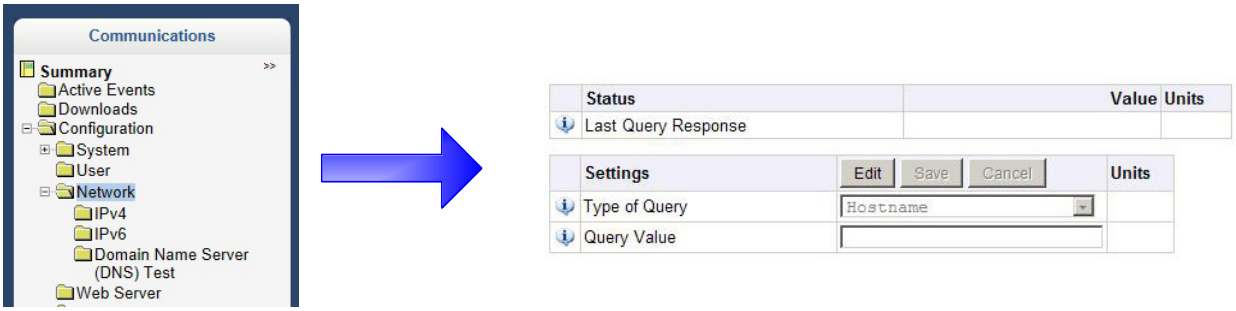
Source of DNS server identification (None, Automatic, Configured)

Primary DNS Server

Secondary DNS Server

5.4.3.2 Domain Name Server (DNS) Test

The Domain Name Server Test checks key points of a Domain Name Server (DNS) setup for a given domain.



Domain Name Server (DNS) Test Settings

Last Query Response

Response from a domain name server (DNS) to the last query.
Example: *gxtwebdemo.liebert.com* resolved to *126.4.203.234*

Type of Query

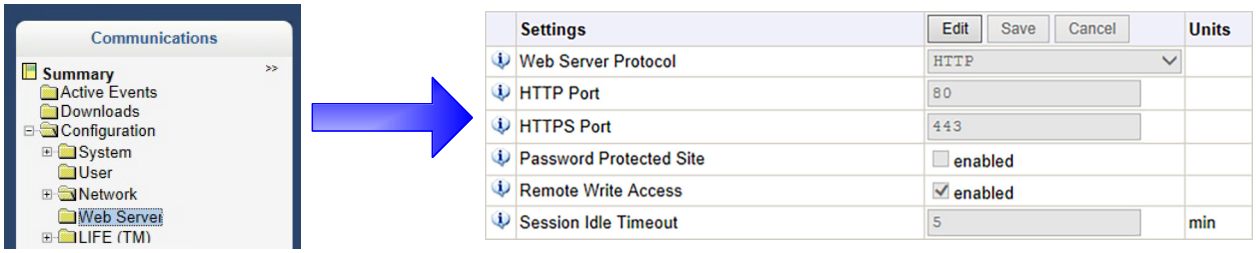
Type of DNS query. (Hostname, IP Address)

Query Value

Value for the domain name server (DNS) to resolve. Example: *gxtwebdemo.liebert.com*

5.4.4 Configuration—Web Server Folder

The Web Server Settings permits making some security settings, such as HTTP or HTTPS, and password enabling.



Web Server Settings

Web Server Protocol

Select the operation mode of the Web Server (HTTP, HTTPS)

HTTP Port

Standard web port not encrypted. Required if HTTP is enabled as Web Server Protocol.

HTTPS Port

Standard secure Web port; all communication is encrypted. Required if HTTPS is enabled as Web Server Protocol.

Password Protected Site

When enabled, a login session is required before any device information is displayed to the user. User level credentials will allow only viewing of device information. Administrator level credentials are required to make any changes.

Remote Write Access

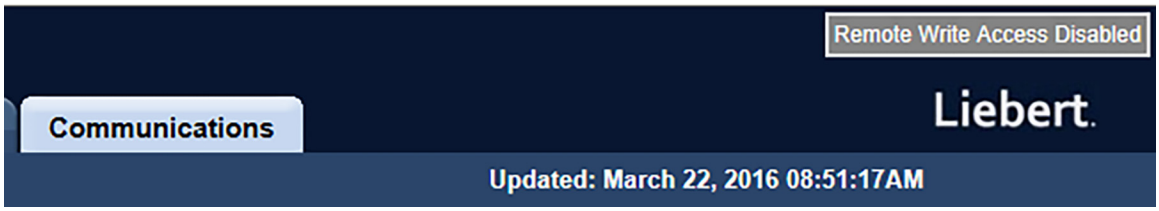
When enabled, all web browsers have write access to data on all Unity-card web pages when the user is logged-in with Administrator credentials. When disabled, write access is restricted to web browsers connected on an Autoconfiguration IPv4 address. An Autoconfiguration IPv4 address is of the form 169.254.x.x, and is negotiated automatically when a direct connection is made between the Ethernet port of your PC and the Ethernet port of the Unity card. For additional information, see **2.1.2 - Connect an Ethernet Cable**. Regardless of this setting, all web browsers always have read access to the web pages (subject to the setting of the Password Protected Site parameter), and the diagnostic information file can be generated when the user is logged-in with Administrator credentials (see **5.7 - Communications—Support Folder**).

Note: When Remote Write Access is disabled, an indicator is displayed in the upper right corner of the web page as a reminder, **Figure 5-5**.

NOTE

Only disable remote-write access if you are absolutely sure that you do not need to administer the managed device or the Unity card through a remote web-browser session.

Figure 5-5 Remote write access disabled indicator



Session Idle Timeout

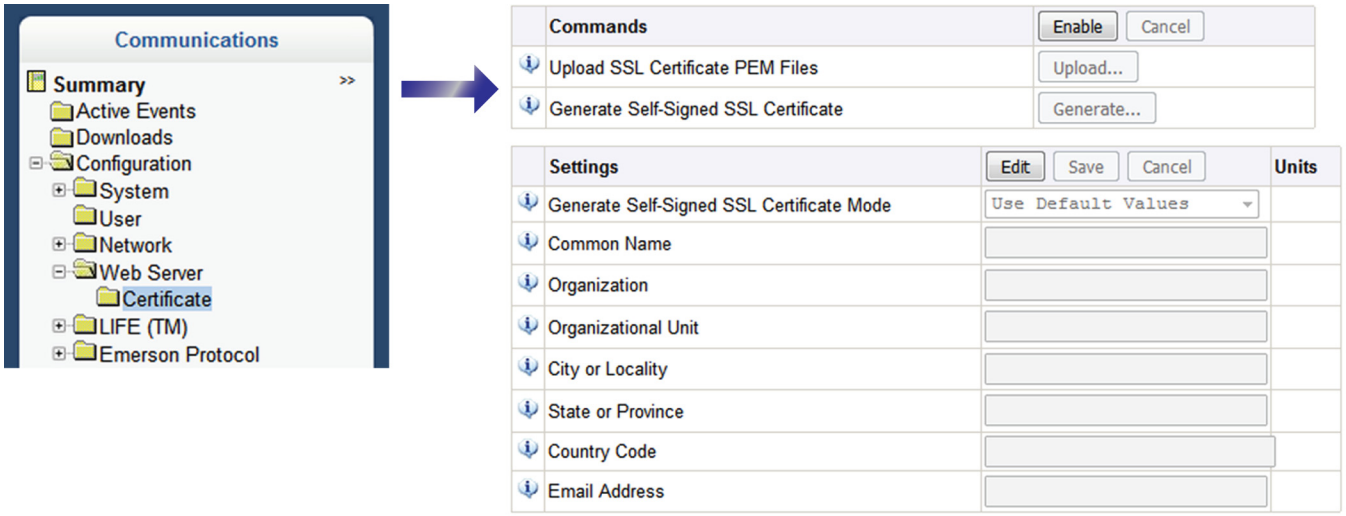
The interval the software will wait before logging off a user unless there is user activity (Default is 5 min.)

5.4.4.1 Certificate

When the Web Server Protocol is configured to use HTTPS communications, all web-server communication with all browsers is encrypted and validated based upon the security algorithms and validity checks specified in the SSL certificate that is currently-installed in the card. By default, the card generates its own unique, self-signed SSL certificate when it is first powered up. However, many installations want to install and use SSL certificate files that were generated by their own Certificate Authority (CA).

Selections in Certificate, **Figure 5-6**, provide commands to Upload SSL Certificate PEM Files or Generate Self-Signed SSL Certificate.

Figure 5-6 Certificate



Certificate Commands

Upload SSL Certificate PEM Files

Uploads and installs a PEM-encoded SSL key file and certificate file that were generated by a trusted Certificate Authority and that conform to the Apache *mod_ssl* module's SSL CertificateKeyFile and SSLCertificateFile directives. See **5.4.4.1.1**, **Uploading SSL Certificate PEM Files**, **page 48**.

Note: For more information on Apache's use of SSL certificates, see **http://httpd.apache.org/docs/2.4/mod/mod_ssl.html#sslcertificatefile**.

Generate Self-Signed SSL Certificate

Generates and installs a new self-signed certificate based on the mode selected for Generate Self-Signed SSL Certificate Mode. See **5.4.4.1.2**, **Generating a Self-signed SSL Certificate**, **page 48**.

Certificate Settings

Generate Self-Signed SSL Certificate Mode

Method used to generate a self-signed SSL certificate. Options are:

- Use Default Values = the values used in place of the user-configurable fields are the same as those used when the original SSL certificate was generated by the card on first power-up. The default values are not displayed.
- Use Configured Settings = the user-entered values in the configurable fields are used to generate the certificate.

Note: When using configured settings, all of the configurable fields, described below, must have an entry to successfully generate a certificate.

Common Name

Fully-qualified domain name that browser clients will use to reach the card's web server when it is running with the certificate generated with the name entered here.

Organization

Organization or company identified as the owner of the generated certificate.

Organizational Unit

Organizational unit or company division of the organization identified as the owner of the generated certificate.

City or Locality

City or locality of the organization identified as the owner of the generated certificate.

State or Province

State or province of the organization identified as the owner of the generated certificate.

Country Code

Country-code (2-letter abbreviation) of the organization identified as the owner of the generated certificate.

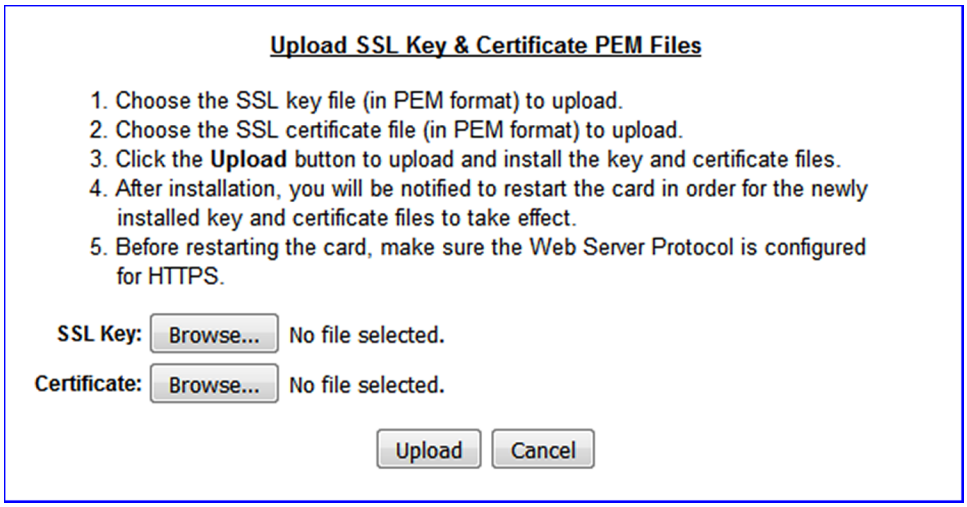
Email Address

Email-address of the contact within the organization identified as owner of the generated certificate.

5.4.4.1.1 Uploading SSL Certificate PEM Files

1. Select *Communications* tab > Configuration > Web Server > Certificate.
2. In Commands, click *Enable*, then click *Upload* next to *Upload SSL Certificate PEM Files*.
   The upload dialog, **Figure 5-7**, opens.
3. Follow the instructions in the dialog to select and upload the appropriate files.

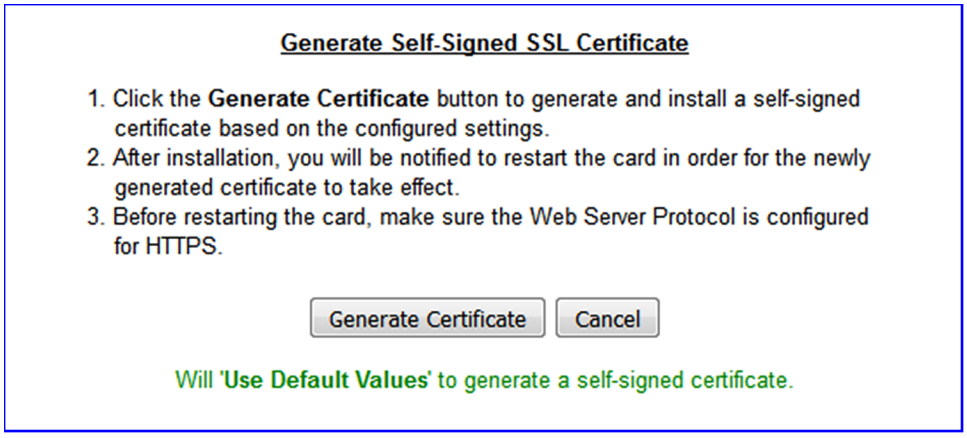
Figure 5-7 Upload SSL Key & Certificate PEM Files dialog



5.4.4.1.2 Generating a Self-signed SSL Certificate

1. Select *Communications* tab > *Configuration* > *Web Server* > *Certificate*.
2. In the Settings section:
   a. Click *Edit*.
   b. In *Generate Self-Signed SSL Certificate Mode*, select the mode to use.
   - If you select **User Configured Settings**, make entries in all of the configurable-value fields (required), then click *Save*.
3. In the Commands section, click *Enable*, then click *Generate* next to *Generate Self-Signed SSL Certificate*.
   The generate dialog, **Figure 5-8**, opens.
4. Follow the instructions in the dialog to generate and install the certificate.

Figure 5-8 Generate Self-Signed SSL Certificate dialog



5.4.5 Configuration—LIFE™ Folder

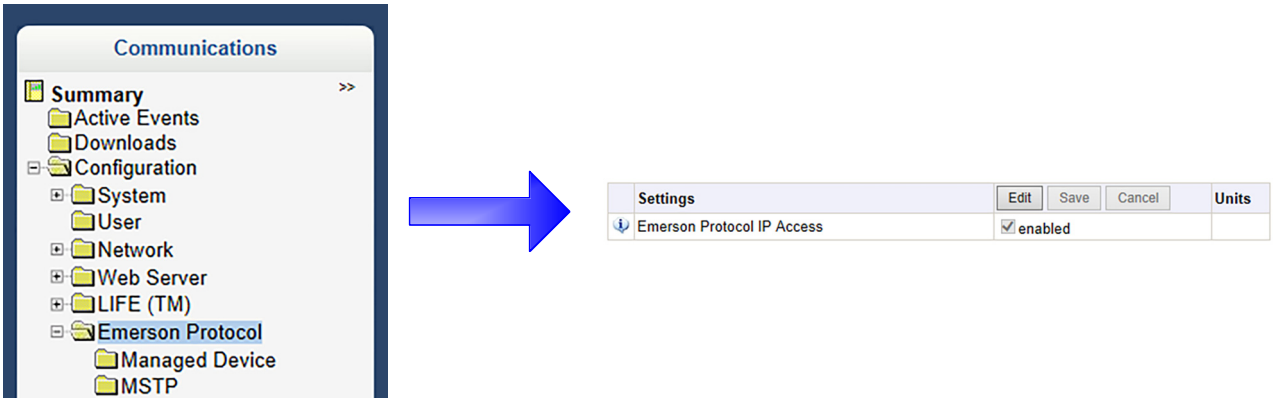
The LIFE subfolder contains settings that affect use of the Emerson® LIFE Technology, a remote monitoring and diagnostic service for Emerson Network Power units. The LIFE settings are for use by trained Emerson Network Power personnel only and require no user changes. For information about the LIFE settings, refer to **Appendix A - Configuration Folder—LIFE™ Sub Folder**.

5.4.6 Configuration—Emerson Protocol Folder

Emerson Protocol contains four subfolders: Managed Device, MSTP, Ethernet and Internal.

NOTE

With the exception of changing the node ID when multiple cards are used or when disabling Emerson-Protocol IP access, the settings in the Emerson Protocol subfolders should not be modified unless directed by an Emerson Network Power representative.



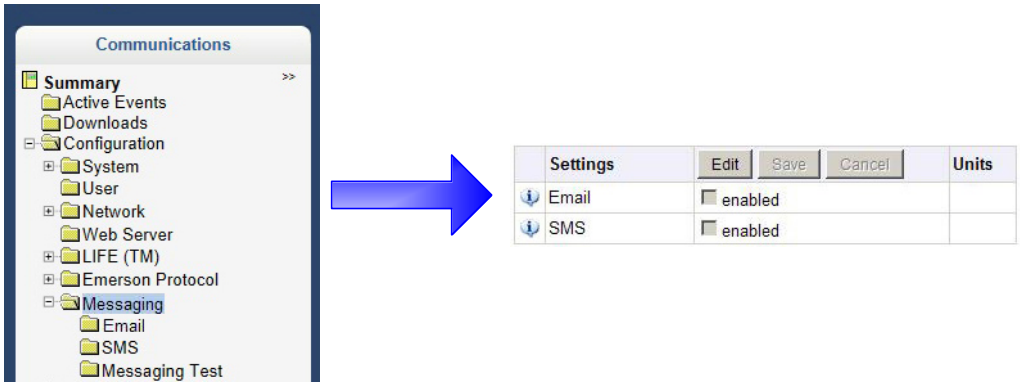
Emerson Protocol options

Emerson Protocol IP Access

When disabled, prevents access from a remote, IP-based system using the Emerson Protocol

5.4.7 Configuration—Messaging Folder

The Messaging subfolder permits enabling email and text messaging about events. The subfolder also contains a test to determine if email and text messages can be successfully sent. Settings for the two messaging methods permit specifying who gets the messages, the format or the messages and other details.



Messaging options

Email

May be enabled to send email messages about events

SMS

May be enabled to send text messages about events

5.4.7.1 Email

Selections in Email determine how the card sends emails about events.

Settings	Edit / Save / Cancel	Units
Email From Address		
Email To Address		
Email Subject Type	Default	
Custom Subject Text	DEFAULT_SUBJECT	
SMTP Server Address	0.0.0.0	
SMTP Server Port	25	
SMTP Connection	Clear	
SMTP Authentication	enabled	
SMTP Username		
SMTP Password		
Include IP Address in Message	☑	
Include Event Description in Message	☑	
Include Name in Message	☐	
Include Contact in Message	☐	
Include Location in Message	☐	
Include Description in Message	☐	
Include Web Link in Message	☐	
Enable Event Consolidation	☑	
Consolidation Time Limit	60	
Consolidation Event Limit	20	

Email Settings

Email From Address

Sender's email address. In most cases this will be the email address of the person to whom replies should be sent. Example *Support@company.com*

Email To Address

Email address of the recipient. Multiple email addresses should be separated by a semicolon.

Email Subject Type

Subject of the email. This value will default to the event description. The subject line can be customized.

Custom Subject Text

The subject of the email can be changed

SMTP Server Address

Fully qualified domain name or IP address of the server used for relaying email messages. If using a server name, a DNS server may need to be configured under Network Settings.

SMTP Server Port

SMTP server port.

SMTP Connection

SMTP server connection type. Determines the capabilities of the SMTP server. Options are:

- Clear = Do not use encryption
- SSL/TLS = Encryption using SSL/TLS connection
- STARTTLS = SSL/TLS encryption initiated using STARTTLS.

SMTP Authentication

Enable or disable email SMTP authentication. An email account must be provided for the SMTP service provider to authenticate.

NOTE

Some email servers may require account-configuration changes to allow communication with the Unity card. For example, Gmail only recognizes Google applications as being secure. However, they provide an account setting that allows authentication with what they consider "less-secure apps." Please see your network administrator or service provider for configuration details.

SMTP Username

Username of the email account to use when email SMTP authentication is enabled.

SMTP Password

Password for the email account to use when email SMTP authentication is enabled.

Include IP Address in Message

If checked, the IP Address of the agent card will be included in outgoing messages.

Include Event Description in Message

If checked, SNMP event description will be included in outgoing messages.

Include Name in Message

If checked, the agent card Name will be included in outgoing messages.

Include Contact in Message

If checked, the agent card Contact will be included in outgoing messages.

Include Location in Message

If checked the agent card Location will be included in outgoing messages.

Include Description in Message

If checked, the agent card Description will be included in outgoing messages.

Include Web Link in Message

If checked, a Web link to the agent card and Web Server listening port number will be included in outgoing messages.

Enable Event Consolidation

If checked, multiple events will be sent per outgoing message.

Consolidation Time Limit

If Event Consolidation is enabled, a message will be sent when 'Consolidation Time Limit' seconds has passed since the first buffered event was received.

Consolidation Event Limit

If Event Consolidation is enabled, a message will be sent when the number of buffered events reaches the 'Consolidation Event Limit.'

5.4.7.2 SMS

Selections in SMS determine how the card sends text messages about events.

	Settings	Edit / Save / Cancel	Units
	SMS From Address		
	SMS To Address		
	SMS Subject Type	Default	
	Custom Subject Text	DEFAULT_SUBJECT	
	SMTP Server Address	0.0.0.0	
	SMTP Server Port	25	
	SMTP Connection	Clear	
	SMTP Authentication	enabled	
	SMTP Username		
	SMTP Password		
	Include IP Address in Message		
	Include Event Description in Message		
	Include Name in Message		
	Include Contact in Message		
	Include Location in Message		
	Include Description in Message		
	Include Web Link in Message		
	Enable Event Consolidation		
	Consolidation Time Limit	60	
	Consolidation Event Limit	20	

SMS Settings

SMS From Address

Sender's SMS address. In most cases this will be the SMS address of the person to whom replies should be sent. For example: Support@company.com

SMS To Address

SMS address of the recipient. Multiple SMS addresses should be separated by a semicolon.

SMS Subject Type

Subject of the message, either Default or Custom.

Custom Subject Text

The subject of the message; can be customized by the customer

SMTP Server Address

Fully-qualified domain name or IP address of the server used for relaying SMS messages.

Note: If using a server name, a DNS server may need to be configured under Network Settings.

SMTP Server Port

SMTP server port.

SMTP Connection

SMTP server connection type. Determines the capabilities of the SMTP server. Options are:

- Clear = Do not use encryption
- SSL/TLS = Encryption using SSL/TLS connection
- STARTTLS = SSL/TLS encryption initiated using STARTTLS.

SMTP Authentication

Enable or disable SMS SMTP authentication. An SMS account must be provided for the SMTP service provider to authenticate.

NOTE

Some messaging servers may require account-configuration changes to allow communication with the Unity card. For example, Gmail only recognizes Google applications as being secure. However, they provide an account setting that allows authentication with what they consider "less-secure apps." Please see your network administrator or service provider for configuration details.

SMTP Username

Username of the SMS account to use when SMS SMTP authentication is enabled.

SMTP Password

Password for the SMS account to use when SMS SMTP authentication is enabled.

Include IP Address in Message

If checked the IP Address of the agent card will be included in outgoing messages.

Include Event Description in Message

If checked SNMP event description will be included in outgoing messages.

Include Name in Message

If checked the agent card Name will be included in outgoing messages.

Include Contact in Message

If checked the agent card Contact will be included in outgoing messages.

Include Location in Message

If checked the agent card Location will be included in outgoing messages.

Include Description in Message

If checked the agent card Description will be included in outgoing messages.

Include Web Link in Message

If checked a Web link to the agent card and Web Server listening port number will be included in outgoing messages.

Enable Event Consolidation

If checked multiple events will be sent per outgoing message.

Consolidation Time Limit

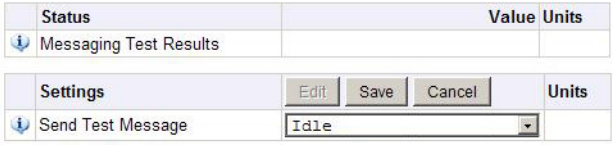
If Event Consolidation is enabled, a message will be sent when “Consolidation Time Limit” seconds has passed since the first buffered event was received.

Consolidation Event Limit

If Event Consolidation is enabled, a message will be sent when the number of buffered events reaches the “Consolidation Event Limit.”

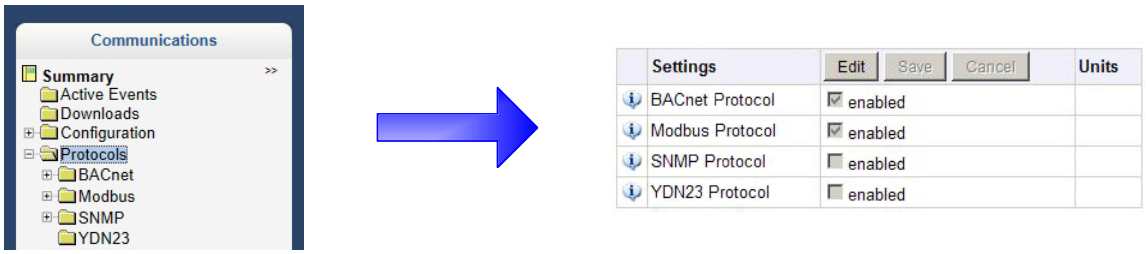
5.4.7.3 Messaging Test

Selections here permit testing the setup for email and SMS messages. If the test fails, incorrect settings should be changed to ensure that the Liebert IntelliSlot Unity card sends proper notifications if an event should occur.



5.5 Communications—Protocols Folder

The Protocols folder displays the types of protocols that may be enabled for a Liebert IntelliSlot Unity card. Not all protocols are available at the same time. Some protocols may not be available for some types of managed devices (see **1.2 - Compatibility With Other Emerson Products and Communication Protocols**). The Liebert IntelliSlot Unity card allows selecting two third-party protocols.

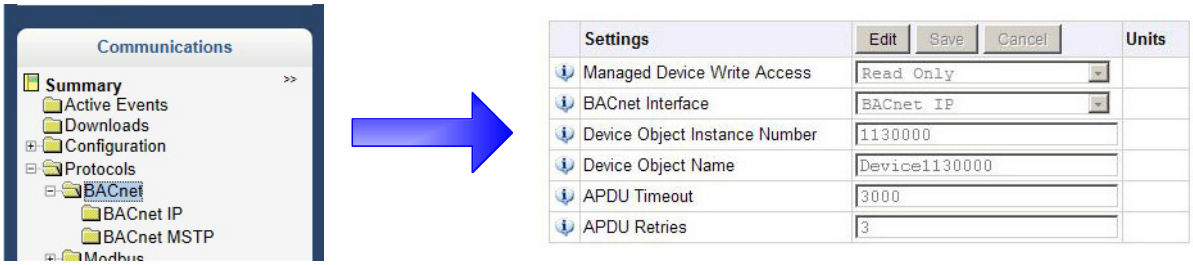


The folders contained by the Protocols folder are:

- **BACnet**
  - BACnet IP
  - BACnet MSTP
- **Modbus**
  - Modbus TCP
  - Modbus RTU
- **SNMP**
  - SNMPv3 User (20)
  - SNMPv1 Trap (20)
  - SNMPv1/v2c Access (20)
- **YDN23**

Settings in each permit configuring the protocols available on the Liebert IntelliSlot Unity card.

5.5.1 Protocols—BACnet Folder



BACnet Settings

Managed Device Write Access

Enable or Disable the BACnet server to write to the managed device.

BACnet Interface

BACnet server interface: BACnet IP or BACnet MSTP.

Device Object Instance Number

The instance number (0-4194302) of the BACnet server's device object.

Device Object Name

The name of the BACnet server's device object.

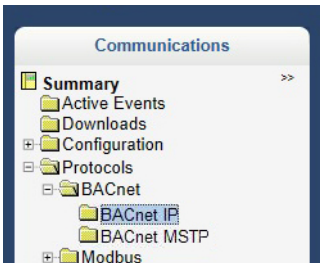
APDU Timeout

The timeout in milliseconds between APDU retries (1-65535).

APDU Retries

The number of times to retransmit an APDU after the initial attempt (0-8).

5.5.1.1 BACnet IP Folder



BACnet IP Settings

BACnet IP Port Number

The port for the BACnet server's UDP/IP connection.

Register as Foreign Device

Enable or Disable registration as a foreign device.

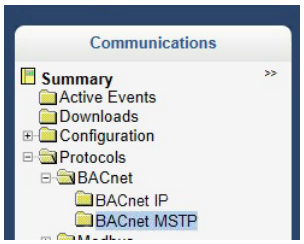
IP Address of BBMD

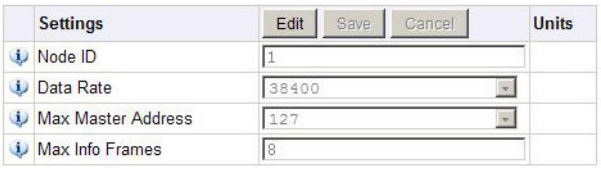
IP Address of the BACnet Broadcast Management Device (BBMD) to be accessed for Foreign Device Registration

Foreign Device Time-to Live

Time to remain in the BBMD Foreign Device table after registration.

5.5.1.2 BACnet MSTP Folder





BACnet MSTP Settings

Node ID

The BACnet server's MS/TP node ID (MAC).

Data Rate

The BACnet MSTP communication rate (bits per second).

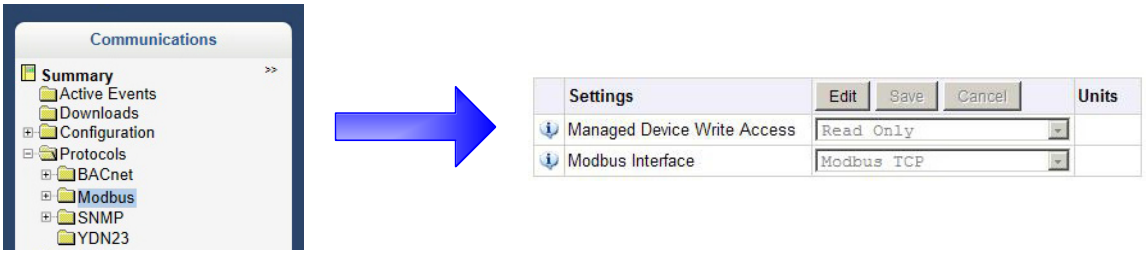
Max Master Address

The maximum node ID (MAC) in use on the MS/TP network.

Max Info Frames

Maximum number of information frames this node may send before it must pass the token.

5.5.2 Protocols—Modbus Folder



Modbus Settings

Managed Device Write Access

Enable or Disable the Modbus server to write to the managed device

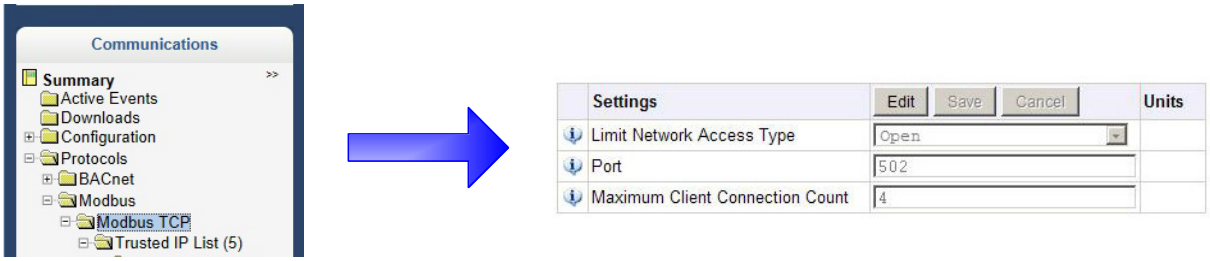
Modbus Interface

Select the Modbus interface, either Modbus TCP or Modbus RTU

5.5.2.1 Modbus TCP Folder

The Modbus TCP permits connection to the card by:

- any client (Open) permits communication by any IP address
- clients on the same subnet as the Liebert IntelliSlot Unity card
- clients with specific IP addresses (Trusted IP Lists); only five addresses are permitted



Modbus TCP Settings

Limit Network Access Type

IP Access List

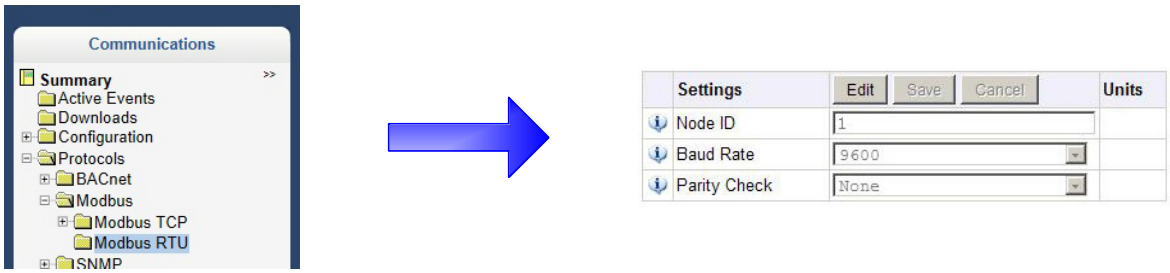
(Open, Same Subnet, Trusted IP List)

Port

The TCP port used by the Modbus Server to listen for and respond to Modbus protocol requests based on Limit Network Access Type setting.

Maximum Client Connection Count

5.5.2.2 Modbus RTU Folder



Modbus RTU Settings

Node ID

Modbus Server ID for the interface; obtain from network administrator.

Baud Rate

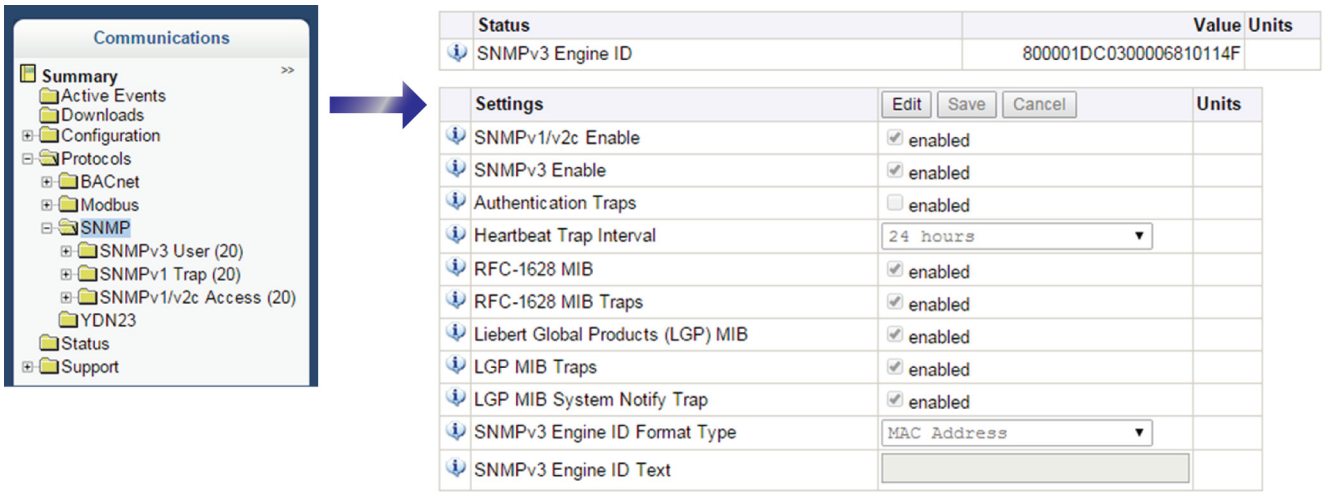
Communication rate (9600, 19200, 38400)

Parity Check

The communication parity check (None, Even, Odd)

5.5.3 Protocols—SNMP Folder

Folders and settings in this folder permit configuring the card for various types of SNMP communication, including access, traps and other user settings.



SNMP Settings

SNMPv3 Engine ID

Read-only. The generated SNMPv3 engine ID.

Note: A newly-generated ID appears only after rebooting the card.

SNMP v1/v2c Enable

Enable or Disable SNMP v1/v2c.

SNMP v3 Enable

Enable or Disable SNMPv3.

Authentication Traps

When enabled, an Authentication Trap is sent if an SNMP host tries to access the card via SNMP, but either the host address is not in the SNMP Access Settings or it is using the wrong Community String.

Heartbeat Trap Interval

Enable or Disable and set interval 5 minutes, 30 minutes, 1 hour, 4 hours, 8 hours, 12 hours and 24 hours.

RFC-1628 MIB

Enable or Disable support for retrieval of data from the RFC-1628 MIB objects.

Note: Required for proper operation of Liebert MultiLink® and applies only to managed UPS equipment.

RFC-1628 MIB Traps

Enable or Disable support for sending RFC-1628 traps.

Note: Required for proper operation of Liebert MultiLink and applies only to managed UPS equipment.

Liebert Global Products (LGP) MIB

Enable or Disable support for getting and setting data using the Liebert Global Products MIB.

LGP MIB Traps

Enable or Disable support for Liebert Global Products MIB traps.

Note: LGP traps will not be sent unless LGP MIB is enabled.

LGP MIB System Notify Trap

Enable or Disable support for the LGP System Notification trap. This is a single trap sent each time an alarm or warning is added or removed from the conditions table. It provides a text description of the event in a varbind of the trap message.

Note: LGP System Notify Traps will not be generated unless the LGP MIB is enabled.

SNMPv3 Engine ID Format Type

Selects method to build the engine ID. Valid values:

- MAC Address (default) = Engine ID built from the Unity card's MAC address.
- Text = Engine ID built from text entered in SNMPv3 Engine ID Text. See **3.1.3.1.1**, **Select SNMPv3 Engine ID Format**, **page 23**.

SNMPv3 Engine ID Text

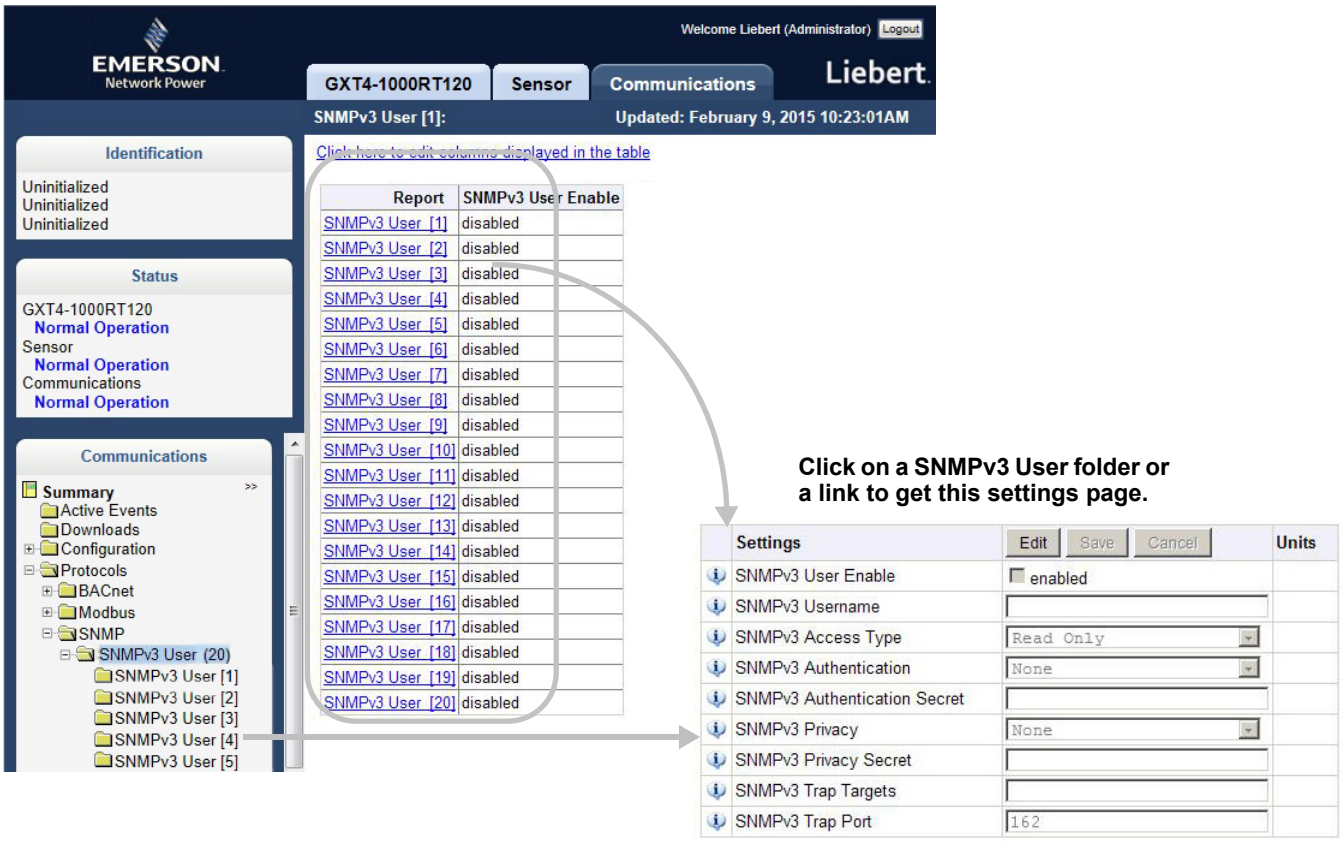
Text on which the engine ID is built when SNMPv3 Engine ID Format Type is **Text**.

Note: If this field is left blank, the engine ID is built from the Unity card's MAC address.

5.5.3.1 SNMPv3 User Folder

The Liebert IntelliSlot-Unity card supports up to 20 SNMPv3 users. The top level page has a table with settings for all 20. The page displays a link to edit the table columns displayed for each SNMPv3 user. The same settings may be accessed by clicking on a folder for a user, such as SNMPv3 User [1].

The Web page below shows the settings that can be changed for a SNMPv3 user. To display the settings, click on any of the SNMPv3 User links. After making any changes, click **Save** to make the changes effective; click **Cancel** to discard the changes.



SNMPv3 User Settings

SNMPv3 User Enable

Select to enable read, write or sending notifications with the user's credentials.

SNMPv3 Username

The User name the authentication and privacy settings apply to. This string can be composed of printable characters except colon, tab, double quote, and question mark.

SNMPv3 Access Type

Read Only, Read/Write or Traps only

SNMPv3 Authentication

Cryptographic algorithm used for authentication: None, MD5 or SHA-1

SNMPv3 Authentication Secret

Pass phrase or password used for SNMPv3 Get request. This string can be composed of printable characters with the exception of colon, tab, double quote, and question mark. Note: The entry must be 8 or more characters but not more than 64.

SNMPv3 Privacy

Cryptographic algorithm used for encryption. Options are:

- None
- DES
- AES

SNMPv3 Privacy Secret

Pass phrase or password used for SNMPv3 Get request. This string can be composed of printable characters with the exception of colon, tab, double quote, and question mark. Note: The entry must be 8 or more characters but not more than 64.

SNMPv3 Trap Target Addresses

Network hosts that will receive SNMPv3 traps, identified with either a network name or IP address. Multiple addresses must be separated by commas.

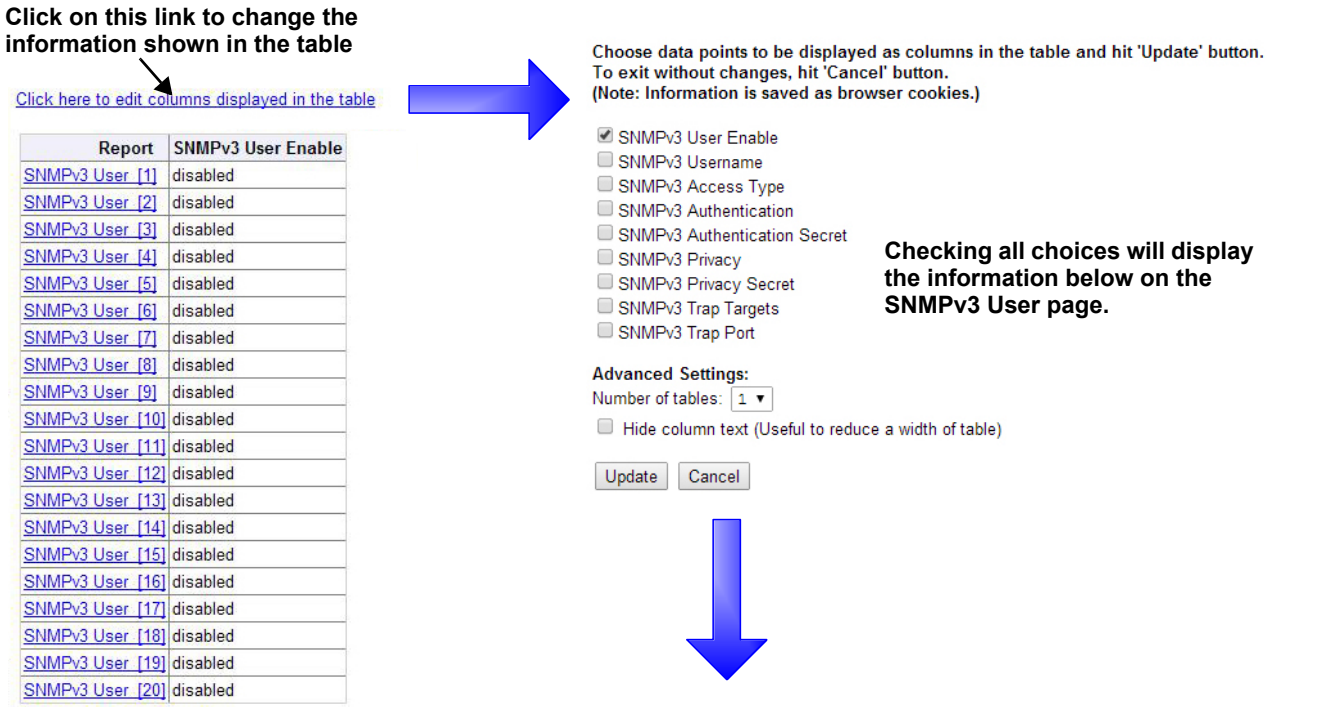
SNMPv3 Trap Port

Port used by the target host for receiving SNMPv3 traps; default is 162.

5.5.3.2 Editing the SNMPv3 Table

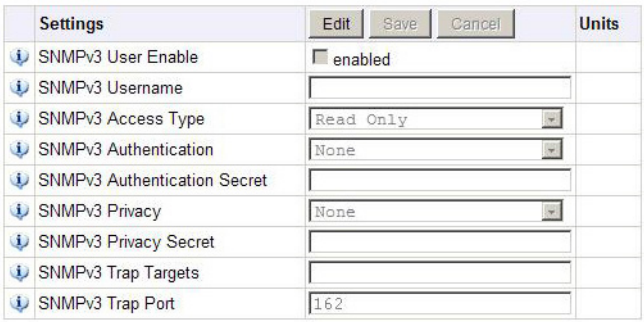
The table on the SNMPv3 User Settings [20] page may be altered to provide more or less information. To do so, click on the command above the table (Click here to edit columns displayed in this table). Put a check mark (✓) in the boxes beside the desired information (see **Figure 5-9**). The choices permit showing the same information in this screen that is displayed by clicking on a SNMPv3 User Settings folder or a SNMPv3 User Settings link.

Figure 5-9 Edit the SNMPv3 table



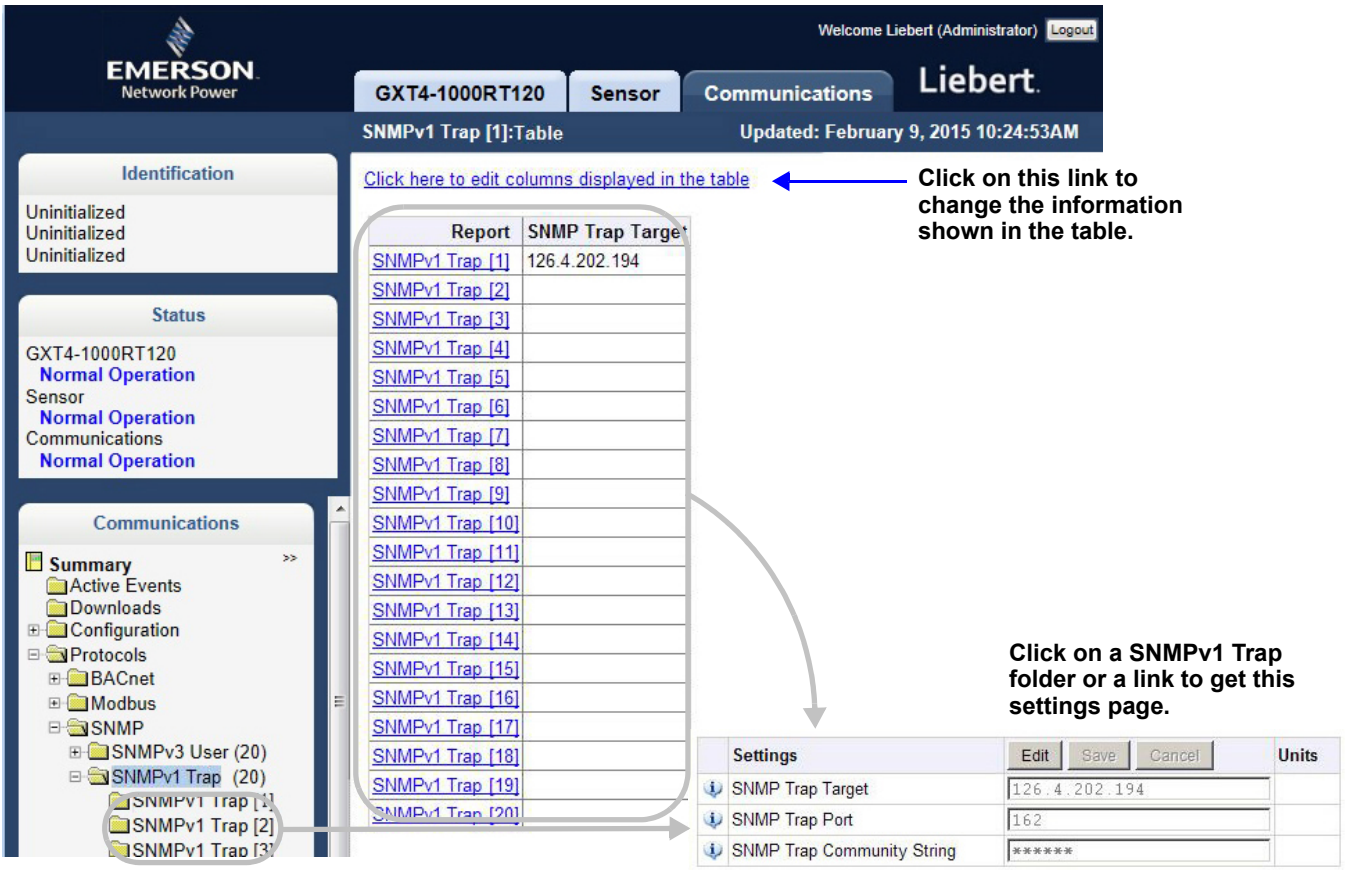
SNMPv3 User Enable	SNMPv3 Username	SNMPv3 Access Type	SNMPv3 Authentication	SNMPv3 Authentication Secret	SNMPv3 Privacy	SNMPv3 Privacy Secret	SNMPv3 Trap Targets	SNMPv3 Trap Port
disabled		Read Only	None		None			162

The information in the table for one user may be viewed by clicking on a SNMPv3 User Settings folder or a SNMPv3 User Settings link, as shown at right.



5.5.3.3 SNMPv1 Trap Folder

This page contains settings for network hosts that will receive SNMPv1 traps. Up to 20 trap recipients may be enabled and configured. Like the SNMPv3 pages, the settings for each target may be reached by clicking on the links in the **Detail** portion of the page or by clicking on the folders for the trap targets. Also, data shown in the table may be changed by clicking on the link above the table.



SNMPv1 Trap Settings

SNMP Trap Target Addresses

Configure network hosts that will receive alert notifications (i.e., SNMP Traps). The host can be identified as either an IP address or the host's network name.

SNMP Trap Port

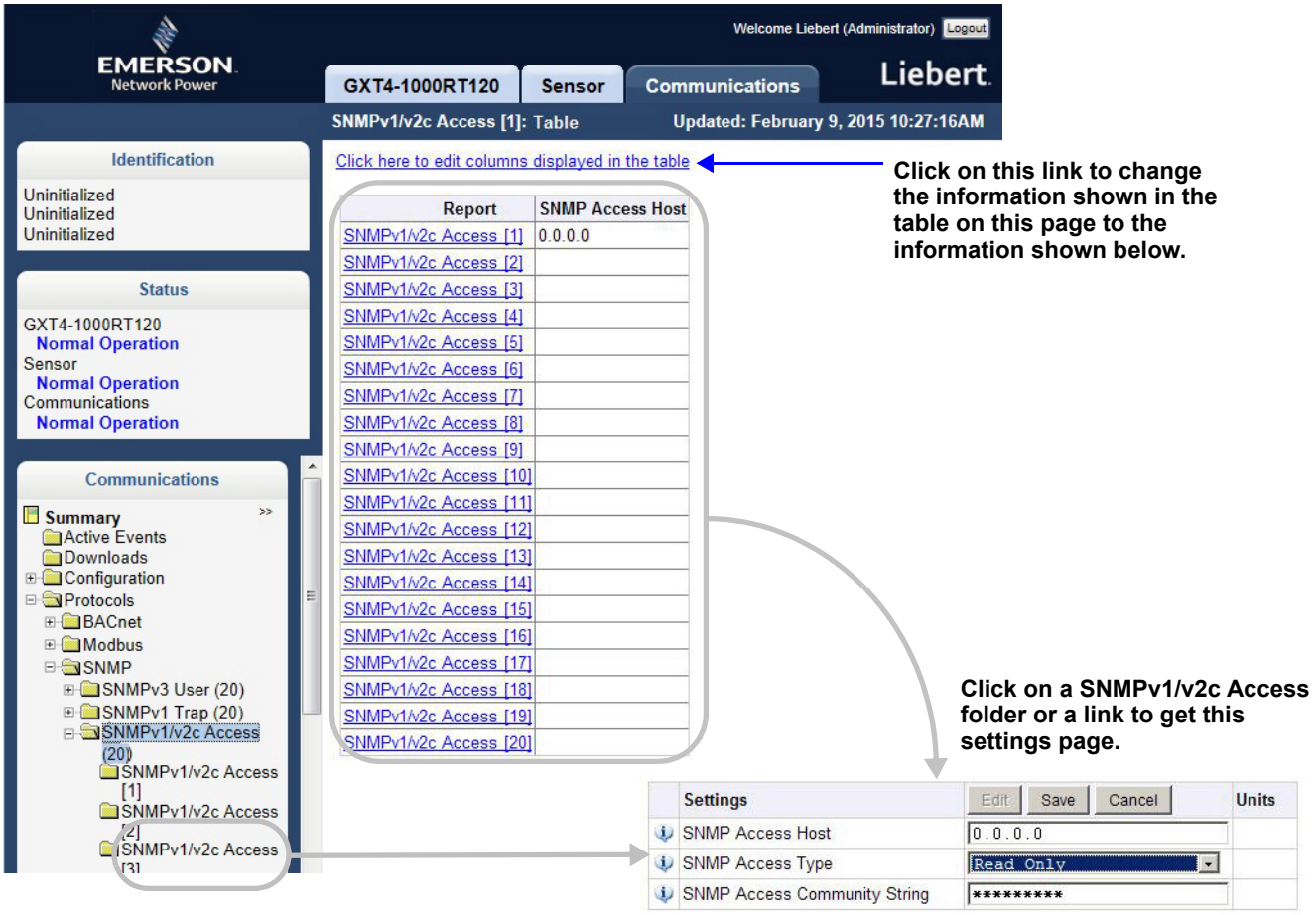
Port used by the target host for receiving notifications; default is 162.

SNMP Trap Community String

String identifying a 'secret' known only by those hosts that want to be notified of device status changes.

5.5.3.4 SNMPv1/v2c Access Folder

This page contains settings for network hosts that can access data using SNMPv1/v2c. Up to 20 access hosts can be enabled and configured. Like the SNMPv3 pages, the setting for each host may be reached by clicking on the links in the data portion of the page or by clicking on the folders for the access hosts. Also, data shown in the table may be changed by clicking on the link above the table.



SNMPv1/v2c Access Settings

SNMP Access IP Address

Configure network hosts interested in device information access. The host can be identified as either an IP address or the host's network name

SNMP Access Type

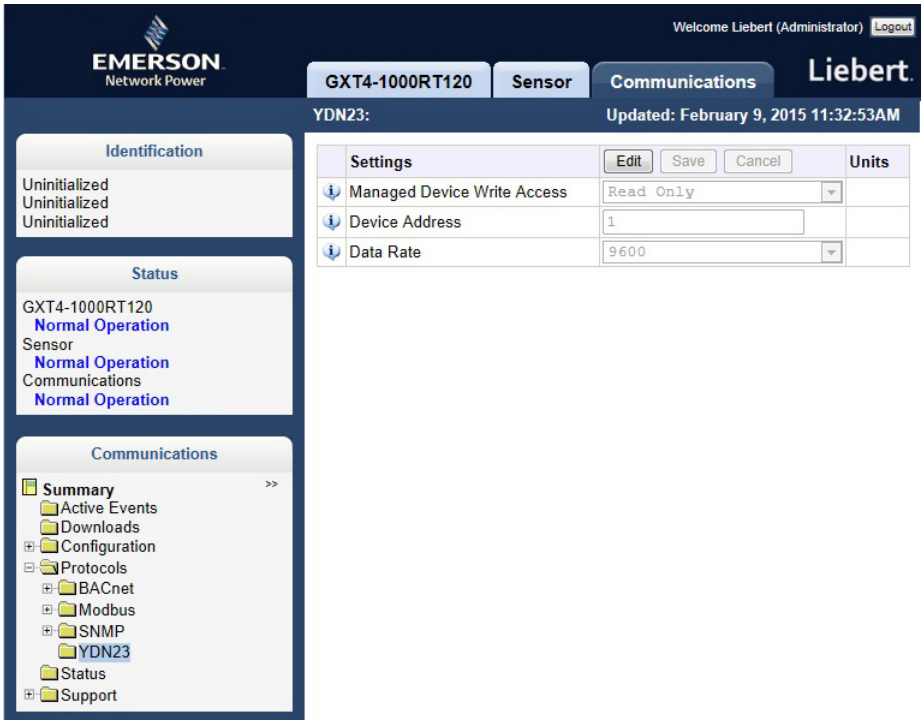
SNMPv1/v2C access type: Read Only or Read/Write

SNMP Access Community String

SNMP Community String

5.5.4 Protocols—YDN23 Folder

The YDN23 protocol supported is based on the YD-T-1363 specification using an RS-485 network connection.



YDN23 Protocol settings

Managed Device Write Access

Enable or Disable the YDN23 server to write to the managed device.

Device Address

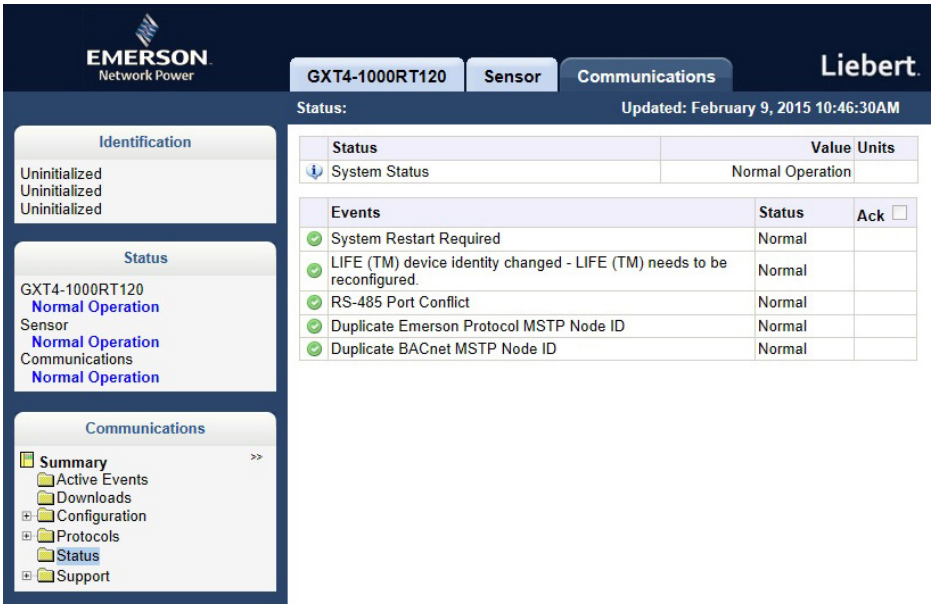
YDN23 device address

Baud Rate

The communications rate in bps.

5.6 Communications—Status Folder

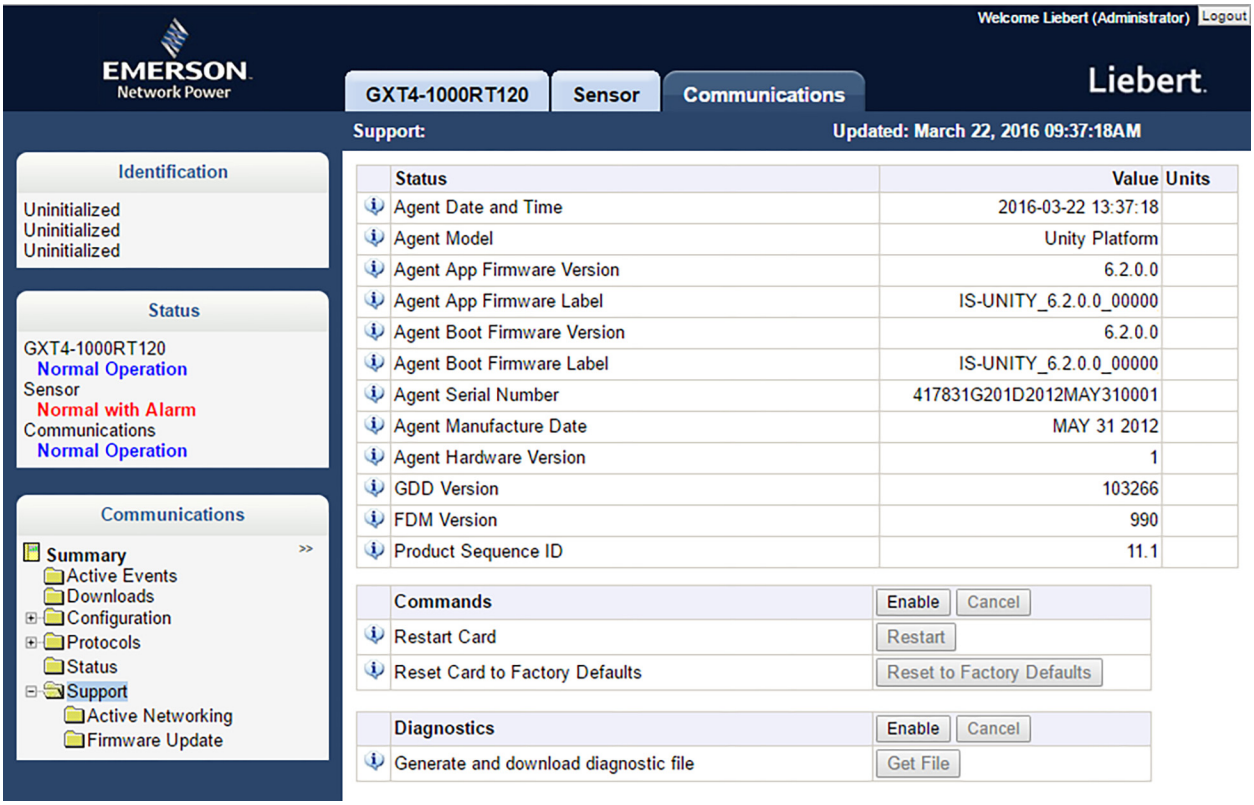
The Status folder contains no configurable items. It displays the System Status of the Liebert IntelliSlot Unity card and a list of events that affect the card's status. A green check mark (?) indicates the status is Normal, as shown in the Status column



5.7 Communications—Support Folder

The Support folder permits restarting the Liebert IntelliSlot Unity card, resetting the card to its factory defaults and updating the card's firmware. *Agent* refers to the Liebert IntelliSlot Unity card.

The folder also displays information about the card for help in troubleshooting, such as the card's firmware version, label, MAC address and related information.



Support Folder Settings

Agent Date and Time

Date and time setting for the card.

Agent Model

The card's model (Unity Platform)

Agent App Firmware Version

The card's firmware version (2.0 or higher)

Agent App Firmware Label

The card's firmware label

Agent Boot Firmware Version

The card's Boot firmware version

Agent Boot Firmware Label

The card's boot firmware label

Agent Serial Number

The card's serial number

Agent Manufacture Date

The card's manufacture date

Agent Hardware Version

The card's hardware version

GDD Version

The card's GDD version, current when the card's firmware was installed; the GDD is a proprietary reference document for device data.

FDM Version

The card's FDM version; the FDM is a data model document that defines data supported by devices that use the Emerson Protocol.

Product Sequence ID

The card's product sequence identifier

Commands

Enable/Cancel

Restart Card

Restart card and implement configuration changes

Reset Card to Factory Defaults

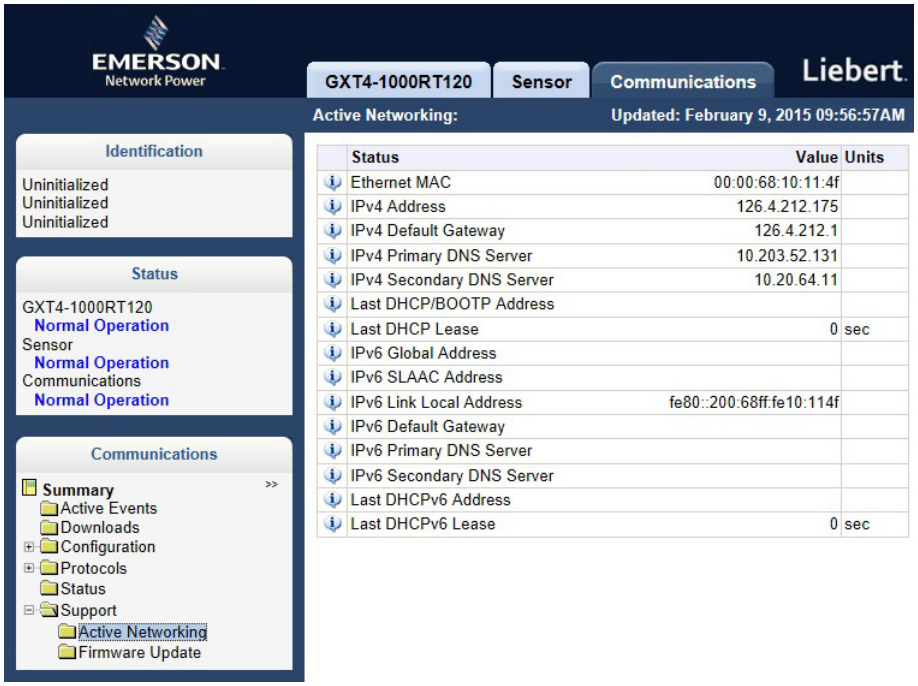
Reset the card's configuration to its factory defaults

Generate and download diagnostic file

Generate a file containing diagnostic information and download it with a Web browser.

5.7.1 Support—Active Networking Folder

Status of the currently active IP network settings for the Liebert IntelliSlot Unity card along with some previous values for troubleshooting IP communication issues.



Active Networking Settings

Ethernet MAC Address

Ethernet MAC Address for the Liebert IntelliSlot card

IPv4 Address

Presently used IPv4 network address

IPv4 Default Gateway

Presently used IPv4 network address of the gateway for network traffic destined for other networks or subnets

Primary DNS

Presently used IPv4 Primary DNS

Secondary DNS

Presently used IPv4 Secondary DNS

Last DHCP/BOOTP Address

Last known IPv4 address assigned by DHCP

Last DHCP Lease

Lease time of last known DHCP address

IPv6 Global Address

Shows if DHCPv6 or Static address is presently being used

StateLess Address AutoConfiguration

IPv6 SLAAC is assigned automatically from Router Advertisement, if “A” flag is set, combining Prefix with EUI-64 MAC

Link Local

Presently used IPv6 Link Local Address

IPv6 Default Gateway

Presently used IPv6 network address of the gateway for network traffic destined for other networks or subnets

Primary DNS Server

IPv6 Primary DNS

Secondary DNS Server

Presently used IPv6 Secondary DNS

Last DHCPv6

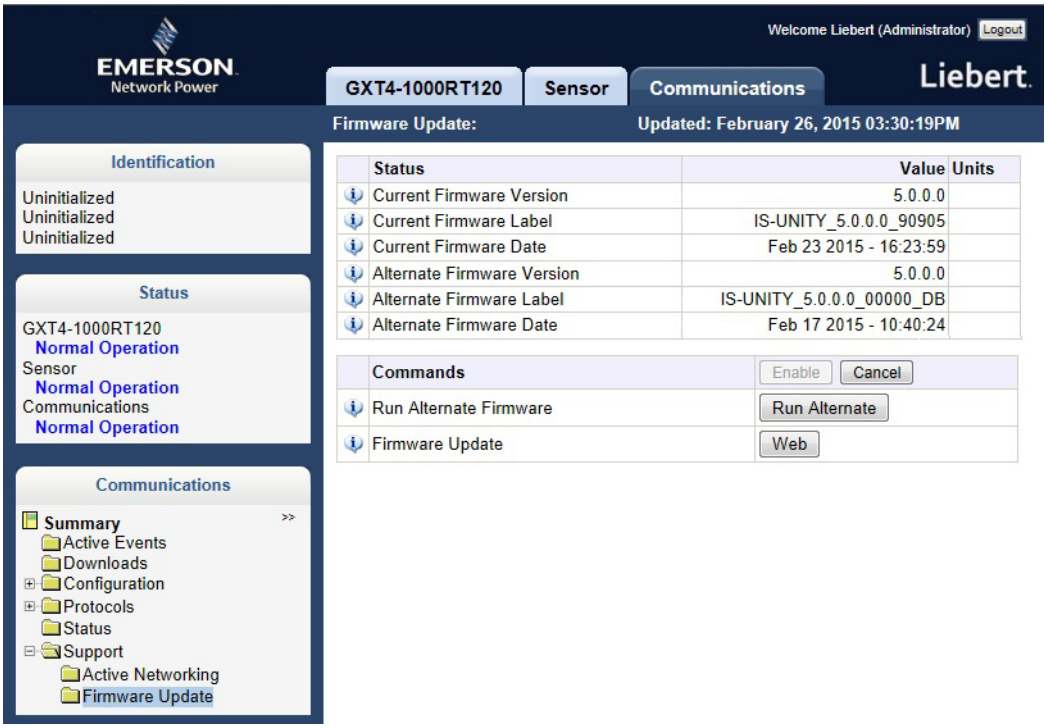
Last known IPv6 address assigned by DHCPv6

Last DHCPv6 Lease

Lease time of last known DHCPv6 address

5.7.2 Support—Firmware Update Folder

The Firmware Update folder supports updating the firmware of the Liebert IntelliSlot Unity card or reverting to an alternate firmware version and configuration (if the current firmware is not the initial load).



Firmware Update settings

Current Firmware Version

The version of the firmware running on the card

Current Firmware Label

The label of the firmware running on the card

Current Firmware Date

The build date of the firmware running on the card

Alternate Firmware Version

The version of the firmware in the alternate area

Alternate Firmware Label

The label of the firmware in the alternate area

Alternate Firmware Date

The build date of the firmware in the alternate area

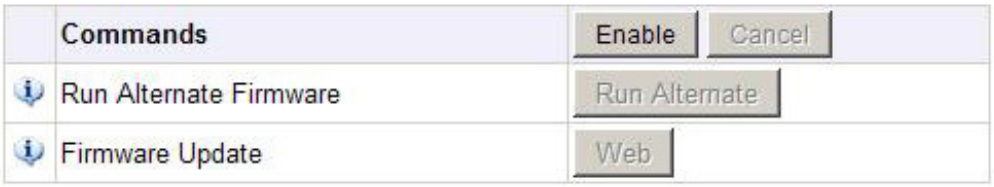
Firmware Commands

Run Alternate Firmware

Return the card's firmware to a version in the alternate area (the version in use before the most recent firmware update).

Firmware Update

Update the card's firmware to a new version



6.0 Firmware Updates

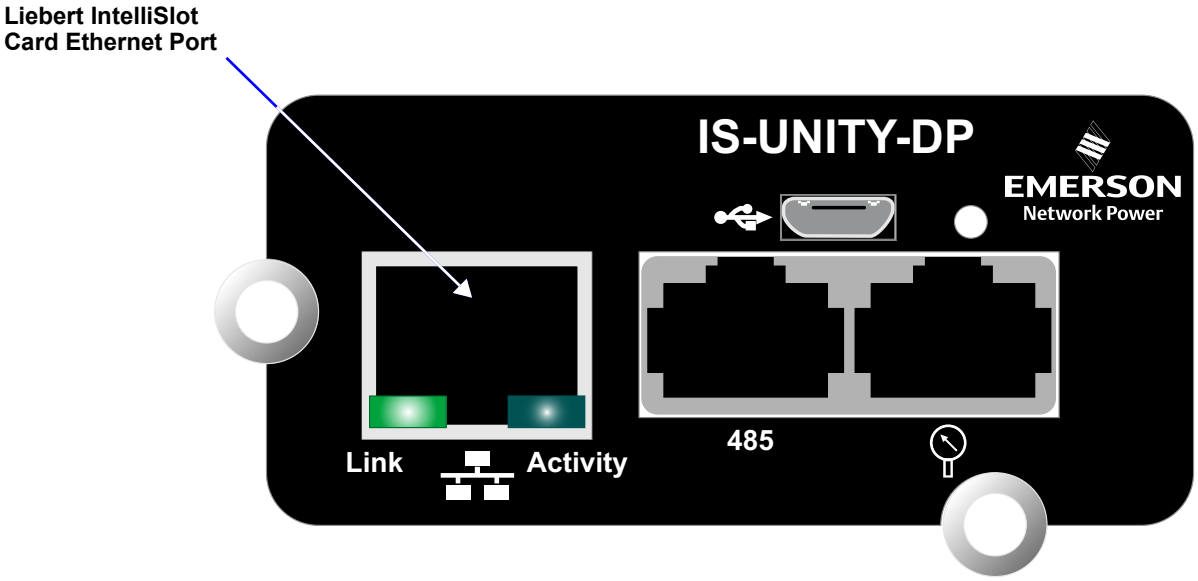
The Liebert IntelliSlot Unity card has two areas in flash memory for the firmware and the configuration. One area is currently operating on the card. The other area is the previous firmware on the card and is considered an alternate. For information on the alternate firmware, see **6.2 - Revert to Alternate Firmware**.

6.1 Updating the Liebert IntelliSlot Unity Card's Firmware

To update the Liebert IntelliSlot Unity card's firmware:

1. Download onto your computer the latest Liebert IntelliSlot Unity card firmware update from the Liebert software download Web site at **www.liebert.com**
2. If the card's DHCP or Static-IP address is known, type the IP address in the Web browser address window.
3. If the card does not have a known IP address and it is configured for DHCP, connect the card to a computer with an Ethernet cable and open a Web browser. The card has an Ethernet RJ-45 connector on the front (see **Figure 6-1**). The card and computer will automatically negotiate communications, which will take about one minute (for details on auto configuration, see **2.1.2 - Connect an Ethernet Cable**). When communication is established, open a Web browser and enter the address *169.254.24.7*, the card's default Autoconfiguration IPv4 Address. The card's Web page will appear.

Figure 6-1 Ethernet port

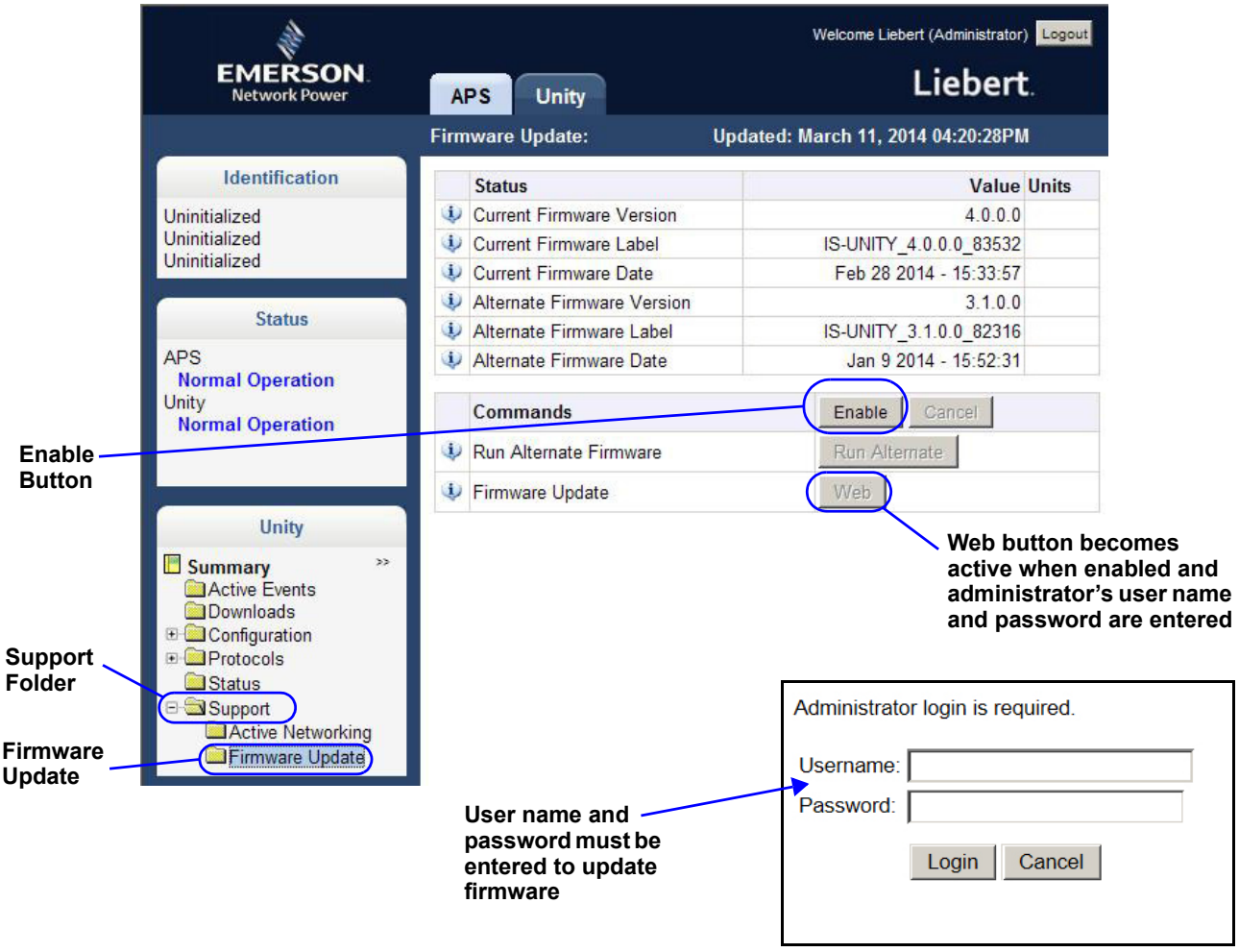


4. Select the *Communications tab* at the top of the screen, then the *Support* folder from the Communications folders on the left of the screen and then the *Firmware Update* folder.
5. Select the *Enable* button.
6. Enter the administrator user name and password selected previously (see **2.2 - Change User Names and Passwords Immediately**) in the security dialog box that appears.

7. Click the *Web* button.
   The firmware-update screen opens.
8. Browse to the firmware file to update, select it and click the *Update Firmware* button.

NOTE
Do not navigate away from the Firmware Update screen and do not close the browser once the update begins. Either action will interrupt the download.

Figure 6-2 Firmware update screen



6.2 Revert to Alternate Firmware

The Liebert IntelliSlot Unity card has two areas in flash memory for the firmware and the configuration. One area is currently operating on the card. The other area is considered an alternate.

When a card's firmware is updated, the previous firmware and configuration are moved to the alternate area. The Liebert IntelliSlot Unity card allows returning to the firmware version and configuration that are kept in the alternate area.

NOTE

Reverting to an alternate firmware version will not be possible if the currently operating firmware is the initial version loaded on the Liebert IntelliSlot Unity card. If the initially loaded firmware is still running on the card, the Alternate Version fields will be blank, and it will not be possible to revert to an alternate version.

1. Select the *Communications* tab at the top of the screen.
2. Select the *Support* folder, then the *Update Firmware* folder.
3. Select the *Enable* button.
4. Enter the user name and password in the security dialog box that appears; use the administrator user name and password from the user settings.
5. Click the *Run Alternate* button.
   A confirmation dialog opens.
6. Click *OK* on the confirmation dialog.

NOTE

The card will reboot. After the reboot, the card will be running the previous version of the firmware and configuration, which had been stored in flash memory. The previous firmware and configuration will have been moved to the alternate area.

Page intentionally left blank.

Appendix A - Configuration Folder—LIFE™ Sub Folder

The LIFE sub folder contains settings that affect use of the Emerson® LIFE Technology, a remote monitoring and diagnostic service for Emerson units. The LIFE settings are for use by trained Emerson Network Power personnel only and require no user changes.

Status	Description
Connection Media	The LIFE Technology connection media
Enable Date and Time	The date and time that LIFE Technology support was enabled.
Settings	**Description**
LIFE Technology	Enable or disable the LIFE Technology
System Serial Number	System serial number, obtained from the unit automatically
Site Equipment Tag Number	Site equipment tag number
Site Identifier	Site identifier, entered by the Service Technician
Answer Incoming Call	Enable answering of LIFE Watch Station incoming calls
Next Call Date and Time	Date and Time of next call to make to the LIFE Watch Station server
Call Interval Days	Days between routine calls to LIFE Watch Station
Call Interval Hours	Number of hours between LIFE Watch Station routine calls
Call Interval Minutes	Number of minutes between routine LIFE Watch Station calls. This value is used in conjunction with val_life_callInterval_hours.
Call Trials Number	The number of attempts to retry a call after it fails before rescheduling the call.

UPS State SMS Messaging Configuration

Settings	Description
Primary Mains Restored SMS	Send SMS when Primary Mains are restored
Primary Mains Restored SMS Value	Value sent via SMS when Primary Mains are restored
Primary Mains Failure SMS	Send SMS when Primary Mains fail
Primary Mains Failure SMS Value	Value sent via SMS when Primary Mains fail
Bypass Mains Fail SMS	Send SMS when Bypass Mains fail
Bypass Mains Failure SMS Value	Value sent via SMS when Bypass Mains fail
Load On Bypass SMS	LIFE Load on Bypass SMS Enable
Load On Bypass SMS Delay	The amount of time to delay sending an SMS after a Load is on Bypass if the condition still exists.

Gate Settings

Status	Description
HTTP Transport Result	HTTP Transport Result contains the result of the last HTTP transaction.
HTTP Transport Error Value	HTTP Transport Error value from the last HTTP transaction
HTTP Transport Reply Time	HTTP transport reply time
Connection Result	IP connection result
Bridge State	IP Bridge state machine state
Error Count	Gate connection error count
Settings	**Description**
Proxy Enable	Enable Gate proxy
Proxy Authentication	Enable Gate proxy authentication
Proxy IP Address	Gate proxy IP address
Proxy IP Port Number	Gate proxy IP port number
Proxy User Name	Gate proxy user name
Proxy User Password	Gate proxy user password
LIFE Gate IP Address	LIFE Gate IP address
LIFE Gate IP Port Number	LIFE Gate Port Number

Advanced

Status	Description
Device State	Whether the device is connected or unconnected
Connection Status	The connection status of the Remote Service Delivery application system interface. This is the interface by which Remote Service Delivery services communicates with the Unity system software.
Call Type	The type of call currently in progress with the LIFE™ Watch Station server.
Scheduled Call Delay Time	The delay time before the next call to the LIFE Watch Station server.
Heartbeat Status	Device status as determined by heartbeat traps
Date and Time (UTC) of Last Call	The date and time (in UTC) of the LIFE Watch Station that was retrieved when the last successful call was made. YY-MM-DD HH:MM:SS
Commands	**Description**
Make Manual Call	Sends all currently collected events
Reset Scheduled Call Delay Time	Forces a rescheduled call to be done immediately
Reset Activity and Data	Resets all LIFE in-progress activity and deletes all LIFE data
Settings	**Description**
Service Mode	Enable or Disable LIFE service Mode

Technical Support / Service

Web Site
www.liebert.com
Monitoring
liebert.monitoring@emerson.com
800-222-5877
Outside North America: +00800 1155 4499
Single-Phase UPS & Server Cabinets
liebert.upstech@emerson.com
800-222-5877
Outside North America: +00800 1155 4499
Three-Phase UPS & Power Systems
800-543-2378
Outside North America: 614-841-6598
Thermal Management Systems
800-543-2778
Outside the United States: 614-888-0246

Locations

United States
1050 Dearborn Drive
P.O. Box 29186
Columbus, OH 43229

Europe
Via Leonardo Da Vinci 8
Zona Industriale Tognana
35028 Piove Di Sacco (PD) Italy
+39 049 9719 111
Fax: +39 049 5841 257

Asia
7/F, Dah Sing Financial Centre
108 Gloucester Road, Wanchai
Hong Kong
852 2572220
Fax: 852 28029250

SL-52645_REV9_8-16
590-1305-501C

Emerson Network Power
www.emersonnetworkpower.com

EMERSON. CONSIDER IT SOLVED.™