

Liebert® IntelliSlot® Web Cards

User Manual—Liebert IntelliSlot Web Card, Liebert IntelliSlot Web Card-LB,
Liebert IntelliSlot Web Card-LBDS, Liebert IntelliSlot Web Card-L,
Liebert IntelliSlot Web Card-IPBML Modbus IP / BACnet IP, Liebert IntelliSlot Web Card-S,
Liebert IntelliSlot Web Card-IPBMS Modbus IP, Liebert IntelliSlot Web Card-X,
Liebert IntelliSlot Web Card-IPBMX Modbus IP, Liebert IntelliSlot Web/485 Card With Adapter

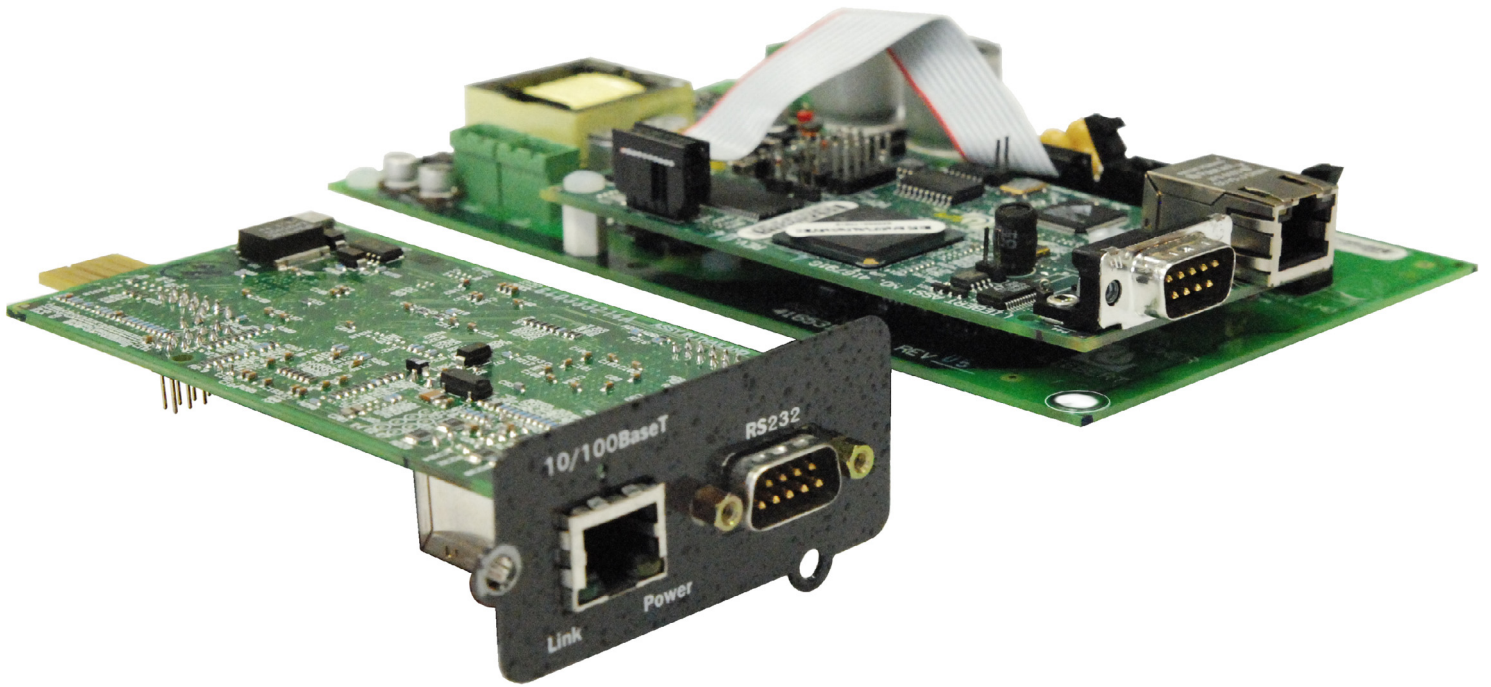


TABLE OF CONTENTS

IMPORTANT SAFETY INSTRUCTIONS	1
1.0 INTRODUCTION	2
COMPATIBILITY WITH OTHER EMERSON® PRODUCTS AND COMMUNICATION PROTOCOLS	3
1.1 Web Support	4
1.2 Password Protection	4
1.3 SNMP Support	4
1.4 Trellis® Support	4
1.5 Liebert Nform™ Support	4
1.6 Liebert MultiLink™ Support	4
1.7 Liebert SiteScan® Web With Modbus Support (<i>Units with IS-WEBADPT Only</i>)	5
2.0 INSTALLATION	6
2.1 Install a Liebert IntelliSlot Web Card—Non-Adapter Version	6
2.1.1 Connect the Cable	6
2.1.2 Prepare the Card for Configuration	6
2.2 Install a Liebert IntelliSlot Web/485™ Card With Adapter	7
2.2.1 Connect the Cable	7
2.2.2 Prepare the Card for Configuration	7
3.0 CONFIGURATION OVERVIEW	8
3.1 Guide to Configuration	8
3.2 Open the Terminal Emulation Interface - Serial Connection	9
3.3 Open the Terminal Emulation Interface - TCP/IP Connection	10
3.4 Open the Telnet Interface	11
3.5 Open the Web Interface	12
3.6 Saving Changes and Reinitializing the Web Card	13
4.0 EQUIPMENT INFORMATION	14
5.0 NETWORK SETTINGS	15
5.1 Boot/IP Settings	15
5.1.1 Boot/IP Settings (All Cards Except IS-WEBCARD)	15
5.1.2 Boot/IP Settings (IS-WEBCARD Only)	17
5.2 Domain Name Server (DNS) Settings	19
5.2.1 Domain Name Server (DNS) Settings (All Cards Except IS-WEBCARD)	19
5.2.2 Domain Name Server (DNS) Settings (IS-WEBCARD Only)	21
5.2.3 Domain Name Server (DNS) Test Settings (IS-WEB Card Only)	23

5.3	Management Protocol	24
5.3.1	SNMP Communications Menu	25
5.3.2	Display/Modify SNMPv1/v2c Communities	27
5.3.3	Display/Modify SNMPv1/v2c Trap Communities	29
5.3.4	Display/Modify SNMPv3 Settings (<i>Units with IS-WEBCARD Only</i>)	31
5.4	Web Server	33
5.4.1	Specify Web Server Settings	33
5.4.2	Install Security Certificates - Internet Explorer 6 or earlier	34
5.4.3	Install Security Certificates - Internet Explorer 7 or later	36
5.5	Telnet Server	38
5.6	Time (SNTP) Menu	39
5.7	Change Username / Password - Administrator and General User	40
5.8	Reset WEB Authentication to Factory Defaults (<i>Units with IS-WEBCARD, IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS, IS-WEBLB, IS-WEBX, IS-IPBMX Cards Only</i>)	41
6.0	MESSAGING	42
6.1	E-Mail Configuration	43
6.2	SMS Configuration	44
6.3	Customize Messages	45
7.0	FACTORY SETTINGS	46
7.1	Reset to Factory Defaults	46
7.2	Advanced Communication Settings	47
7.2.1	Local Node Settings for Multiple Cards	47
7.2.2	Managed Device Settings	48
7.2.3	Router Settings	48
7.3	Agent Event Log	49
7.4	Support Information	49
7.5	Realtime Information	50
7.6	Task Stack Usage	50
8.0	MONITOR AND CONTROL FUNCTIONS - WEB ONLY	51
8.1	Monitoring Liebert Equipment	51
8.2	Controlling Liebert Equipment	52
8.3	Event Log	53
8.4	Data/Logs Tab (<i>Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only</i>)	54
8.4.1	Downloads (<i>Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only</i>)	55
8.4.2	Event Log Agent (<i>Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only</i>)	56
8.4.3	Events and Parameters (<i>Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only</i>)	57

9.0	SUPPORT INFORMATION	58
9.1	View Web Card Information	58
9.2	Events and Parameters	59
10.0	BUILDING MANAGEMENT FUNCTIONS (<i>IS-IPBML, IS-IPBMS AND IS-IPBMX CARDS ONLY</i>)	60
10.1	Monitoring Data	60
10.2	Management Protocol Menu - Choose Modbus/TCP or BACnet/IP	61
10.3	Modbus/TCP Configuration Menu	62
	10.3.1 Select Modbus/TCP Security Mode Menu	63
	10.3.2 Supported Data List - Modbus/IP	64
10.4	BACnet/IP Server Menu	65
	10.4.1 Supported Data List - BACnet/IP	66
	APPENDIX A - FIRMWARE UPDATES	A1

FIGURES

Figure A1	Null connection	A11
-----------	---------------------------	-----

TABLES

Table 1	Compatibility With Liebert equipment	3
Table 2	Liebert IntelliSlot card communication protocols	3
Table 3	Communication settings	6
Table 4	Communication settings	7
Table 5	Configuration interfaces	8
Table 6	Guide to configuration details	8
Table 7	Communication settings	9
Table 8	Equipment Information identifiers	14
Table 9	Network Settings menu guide	15
Table 10	Boot/IP settings range (all cards except IS-WEBCARD)	15
Table 11	Boot/IP settings range (IS-WEBCARD only)	17
Table 12	Domain Name Server settings (all cards except IS-WEBCARD)	19
Table 13	Domain Name Server settings (all cards except IS-WEBCARD)	21
Table 14	Domain Name Server (DNS) Test settings (IS-WEBCARD only)	23
Table 15	Management protocol ranges	24
Table 16	SNMP communications menu	25
Table 17	Web server settings	33
Table 18	Time Server parameters	39
Table 19	Factory default passwords	40
Table 20	Username and password guidelines	40
Table 21	Factory default passwords	41
Table 22	Messaging menu guide	42
Table 23	E-mail configuration guide	43
Table 24	SMS configuration guide	44
Table 25	E-mail and SMS message guidelines	45
Table 26	Factory default addresses	47
Table 27	Control operations parameters—functions vary by Liebert unit	52
Table 28	Data/Logs tab features (<i>Units with IS-WEBL Cards Only</i>)	54
Table 29	Modbus/TCP Configuration Menu options	62
Table 30	BACnet/IP Server Menu options	65
Table A1	Overview of the upgrade process	A1
Table A2	Estimated Time for downloads	A1
Table A3	Communication settings	A2
Table A4	Firmware update settings - TFTP	A7
Table A5	Firmware update settings - Web	A9

IMPORTANT SAFETY INSTRUCTIONS

SAVE THESE INSTRUCTIONS



WARNING

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).



WARNING

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

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.

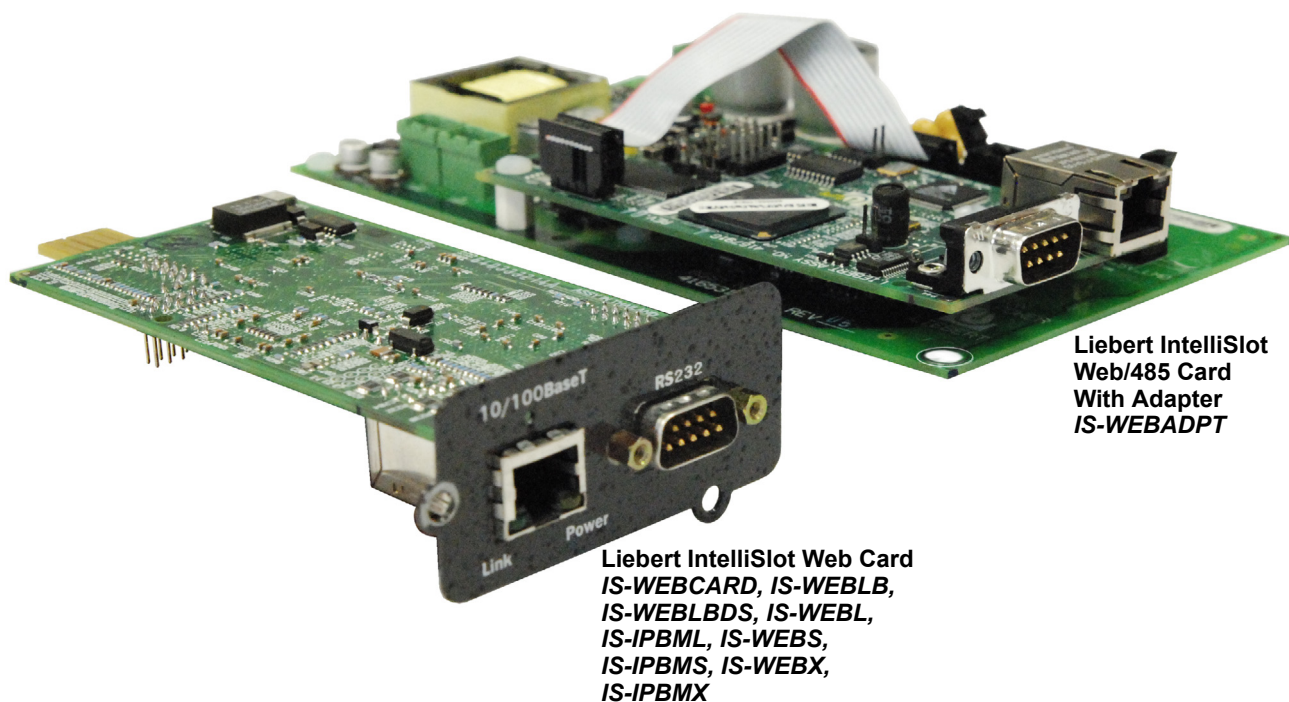
Check the circuits with a voltmeter before beginning installation.

1.0 INTRODUCTION

The Liebert IntelliSlot Web Card family delivers enhanced communications and control to Liebert UPS, AC Power and Thermal Management systems.

Liebert IntelliSlot Web cards bring SNMP, Telnet, Modbus IP, BACnet IP and Web-management capability to many models of Emerson Network Power's line of Liebert UPS, power and thermal management equipment. See **Table 1** for equipment supported and **Table 2** for communication protocols supported.

The cards employ an Ethernet network to monitor and manage a wide range of operating parameters, alarms and notifications.



COMPATIBILITY WITH OTHER EMERSON® PRODUCTS AND COMMUNICATION PROTOCOLS

The Liebert IntelliSlot Web Card family, formerly the OpenComms line, includes:

Table 1 Compatibility With Liebert equipment

Liebert IntelliSlot Card	Part Number	Compatible with:
Liebert IntelliSlot Web Card	IS-WEBCARD	• Liebert GXT™ • Liebert GXT3™ • Liebert GXT2U™ • Liebert PowerSure PSI™ • Liebert Nfinity® (prior to July 2008)
Liebert IntelliSlot Web Card-LB	IS-WEHLB	• Liebert Hinet™ • Liebert NX™
Liebert IntelliSlot Web Card-LBDS	IS-WEHLBDS	<i>Units with Liebert iCOM® Firmware prior to PA1.04.033.STD:</i> • Liebert Challenger 3000™ • Liebert DS™ • Liebert PeX™ • Liebert Challenger ITR™ • Liebert Deluxe System/3™ • Liebert XDC with Liebert iCOM • Liebert CW™ • Liebert XDF™
Liebert IntelliSlot Web Card-L Liebert IntelliSlot Web Card-IPBML Modbus IP / BACnet IP	IS-WEBL IS-IPBML	• Liebert APM™ (Modbus IP only) • Liebert CRV™ • Liebert HPC™ • Liebert HPM™ • Liebert XDP™ with Liebert iCOM <i>Units with Liebert iCOM Firmware PA1.04.033.STD or later:</i> • Liebert Challenger 3000 • Liebert DS • Liebert PeX • Liebert Challenger ITR • Liebert Deluxe System/3 • Liebert XDC with Liebert iCOM • Liebert CW
Liebert IntelliSlot Web Card-S Liebert IntelliSlot Web Card-IPBMS Modbus IP	IS-WEBS IS-IPBMS	<i>Units with Velocity v4 control only:</i> • Liebert FDC™ • Liebert PPC™ • Liebert RX™ • Liebert FPC™ • Liebert RDC™
IntelliSlot Web Card-X IntelliSlot Web Card-IPBMX Modbus IP	IS-WEBX IS-IPBMX	• Liebert NXL™ (SA, SR, SN, MM, CD) • Alber® BDSU™
IntelliSlot Web/485 Card with Adapter	IS-WEBADPT	For legacy device communication, contact Liebert Application Support at 1-800-222-5877 for compatibility.

The Web cards support the following protocols:

Table 2 Liebert IntelliSlot card communication protocols

Liebert IntelliSlot Card	Part Number	Communication Protocol								
		SNMP v1, v2c	SNMP v3	HTTP	HTTPS	EMAIL	SMS	TELNET	MODBUS IP/ BACNET IP	EMERSON PROTOCOL
Liebert IntelliSlot Web Card	IS-WEBCARD	✓	✓*	✓	✓	✓	✓	✓	—	—
Liebert IntelliSlot Web Card-LB	IS-WEHLB	✓	—	✓	✓	✓	✓	✓	—	—
Liebert IntelliSlot Web Card-LBDS	IS-WEHLBDS	✓	—	✓	—	—	—	✓	—	—
Liebert IntelliSlot Web Card-L	IS-WEBL	✓	—	✓	✓	✓	✓	✓	—	✓
Liebert IntelliSlot Web Card-S	IS-WEBS	✓	—	✓	✓	✓	✓	✓	—	✓
Liebert IntelliSlot Web Card-X	IS-WEBX	✓	—	✓	✓	✓	✓	✓	—	✓
Liebert IntelliSlot Web Card-IPBML Modbus IP / BACnet IP	IS-IPBML	—	—	✓	✓	—	—	✓	✓ Both	✓
Liebert IntelliSlot Web Card-IPBMS Modbus IP	IS-IPBMS	—	—	✓	✓	—	—	✓	✓** Modbus IP only	✓
Liebert IntelliSlot Web Card-IPBMX	IS-IPBMX	—	—	✓	✓	—	—	✓	✓** Modbus IP only	✓
IntelliSlot Web/485 Card with Adapter	IS-WEBADPT	✓	—	✓	—	—	—	✓	✓*** Modbus 485	—

* SNMP v3 available for Liebert GXT3 only

** Modbus IP only for IS-IPBMS and IS-IPBMX

*** Modbus 485 and BACnet IP for IS-WEBADPT

Liebert IntelliSlot Web cards support both 10Mbit and 100Mbit communication speeds and either half or full duplex.

**NOTE**

*See online demonstrations of Web cards installed in Liebert equipment at:
<http://demos.liebert.com>*

1.1 Web Support

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

1.2 Password Protection

Control and configuration capabilities are protected by a username and password combination. Optionally, status information can be password-protected. The default username is “Liebert” and the default password is also “Liebert.”

You can change the password using the terminal emulation, Telnet or Web interface. See **5.7 - Change Username / Password - Administrator and General User** for details.

**NOTE**

Change the username and password today to prevent unauthorized access.

1.3 SNMP Support

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

The Liebert Global Products MIB is included in this package on CD-ROM and supports both Microsoft® Windows™ and Unix file formats.

1.4 Trellis® Support

The Liebert IntelliSlot Web 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 Card communication interfaces.

For more information, visit the Trellis Solutions page at <http://www.emersonnetworkpower.com>

1.5 Liebert Nform™ Support

Utilizing the SNMP and Web technologies built into each of the Liebert IntelliSlot Web cards, Liebert Nform will centrally manage alarm notifications to provide you with an easy interface to access critical equipment information.

A downloadable edition is available online at:

nform.liebert.com

1.6 Liebert MultiLink™ Support

The Liebert IntelliSlot Web 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 MultiLink over the network, eliminating the need for serial cables.

For more information on MultiLink and a downloadable version of MultiLink software, visit the MultiLink page at:

multilink.liebert.com

1.7 Liebert SiteScan® Web With Modbus Support (*Units with IS-WEBADPT Only*)

The Liebert IntelliSlot Web/485 Card With Adapter integrates with Liebert SiteScan Web software using Modbus to monitor trends for analysis and maintenance to ensure high-availability operation of critical facilities.

For more information on SiteScan Web and Modbus integration, visit the SiteScan Web page at:

sitescan.liebert.com

2.0 INSTALLATION



WARNING

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

2.1 Install a Liebert IntelliSlot Web Card—Non-Adapter Version

Follow these steps to install a Liebert IntelliSlot Web card (non-adapter version—P/N IS-WEBCARD, IS-WEBLB, IS-WEBLBDS, IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS, IS-WE BX and IS-IPBMX).

1. Locate the Liebert IntelliSlot option bay on your Liebert equipment—You might need to remove a plastic cover.
2. Insert the Liebert IntelliSlot Web™ Card into the Liebert IntelliSlot bay.
3. Secure the card with the supplied screws.
4. Connect an Ethernet cable.

DHCP: The card ships with DHCP service enabled. The MAC address is on a sticker on the top of the card.

OR

Static IP: To assign a static IP address or hostname, use terminal emulation software to configure the card, as described in **Sections 2.1.1** and **2.1.2**.

2.1.1 Connect the Cable

- Connect a configuration cable (null modem) to the DB-9 port on the card and to a COM port on your PC. The configuration cable is available separately from Emerson (P/N LIEBNULL).

2.1.2 Prepare the Card for Configuration

- Use terminal emulation software, such as Microsoft® HyperTerminal, to open a connection to the card with the settings in **Table 3**.

Table 3 Communication settings

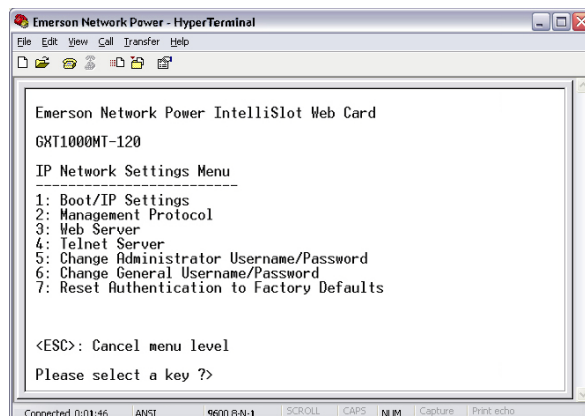
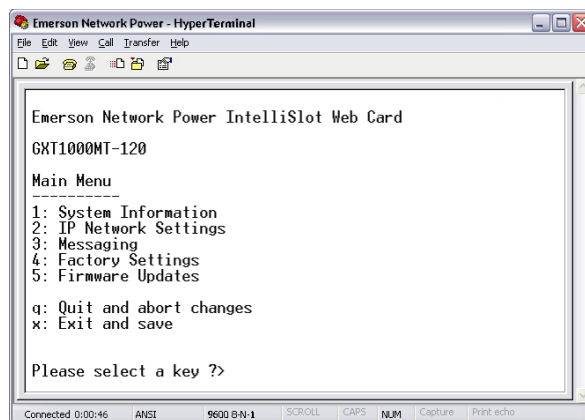
Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None

- Press the Enter key for the Main Menu, above right.
- Select **IP Network Settings**, then **Boot/IP Settings** and follow the instructions to enter an IP ADDRESS, NETMASK and GATEWAY.
- Press Esc to return to the Main Menu.
- Choose **Exit and Save** to save your changes and reboot the card.



NOTE

When installing the card in a Liebert NX, configure the communication port of the Liebert NX™ to 2400 baud. See the Liebert NX user manual for details.



2.2 Install a Liebert IntelliSlot Web/485™ Card With Adapter



WARNING

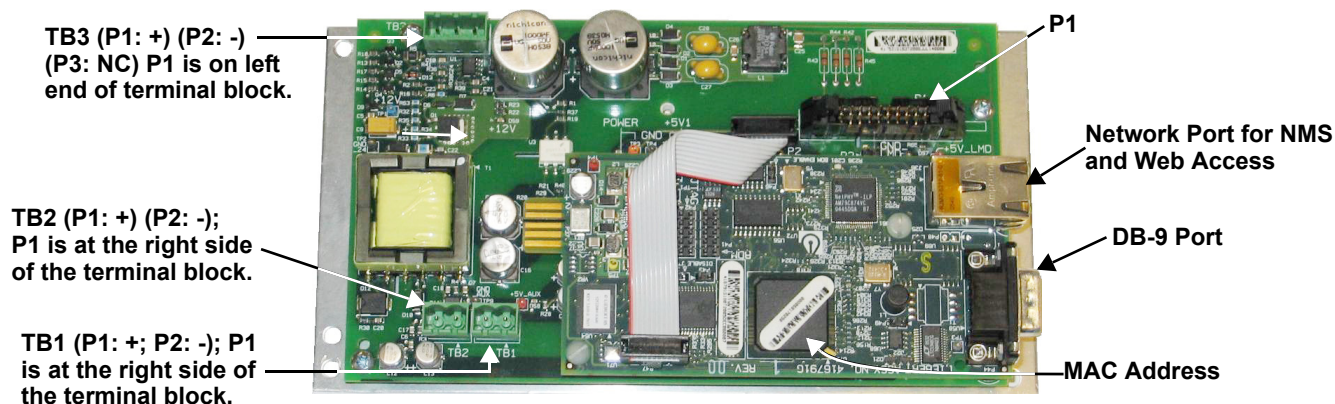
Risk of electric shock. Can cause equipment damage, injury or death.

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.

Check the circuits with a voltmeter before beginning installation.

Follow these steps to install a Liebert IntelliSlot Web/485 Card With Adapter (P/N IS-WEBADPT).

- Locate the adapter mounting location in your Liebert equipment.
- Secure the Liebert IntelliSlot Web/485 Card With Adapter with the supplied screws.
- Connect the equipment's communication cable to the TB1 terminal block or P1 on the card (see the user manual for the Liebert power or cooling unit for details).
- Connect a Modbus (RS-485) cable to the TB2 terminal block.
- Connect an input power supply cable to Pins 1 & 2 on the TB3 terminal block; Pin 1 is at the far left, and Pin 2 is the middle pin.



2.2.1 Connect the Cable

- Connect a configuration cable (null modem) to the DB-9 port on the card and to a COM port on your PC. The configuration cable is available separately from Emerson (P/N LIEBNULL).

2.2.2 Prepare the Card for Configuration

1. Use terminal emulation software, such as HyperTerminal, to open a direct connection to the card with the settings in **Table 4**.
2. Press the Enter key for the Main Menu.
3. Select **485 Network Settings** to access the communications settings.
4. Select **Enabled Application**.
5. Select **Modbus Server** to enable the Modbus application.
6. At the next screen, select **Server ID** (the default Server ID is 1, but may be any number up to 255).
7. Press Esc to return to the Main Menu.
8. Select **IP Network Settings**, then **Boot/IP Settings** and follow the instructions to enter an IP ADDRESS, NETMASK and GATEWAY.
9. Press Esc to return to the Main Menu.
10. Choose **Exit and Save** to save your changes and reboot the card.

Table 4 Communication settings

Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None






NOTE

When installing the card in a Liebert NX™, configure the communication port of the Liebert NX to 2400 baud. See the Liebert NX user manual for details.

3.0 CONFIGURATION OVERVIEW

You may use any of the following interfaces to configure the Web card:

Table 5 Configuration interfaces

Interface	Icon	Description	Available Functions	Connection Methods
Terminal Emulation (Serial or TCP/IP)		Use terminal emulation software—for example, HyperTerminal.	Configuration	Serial Cable or TCP/IP
Telnet		Use a command prompt—enter “telnet” and the IP address or hostname.	Configuration	TCP/IP
Web		Use a Web browser—for example, Microsoft® Windows® Internet Explorer®.	Configuration, Monitoring, Control	TCP/IP

Each configuration section provides instructions using the **Terminal Emulation (Serial or TCP/IP Connection) / Telnet Interface**, along with a brief description of how to access the same function through the **Web Interface**.



NOTE

The Terminal Emulation and Telnet interfaces present the same menus and choices.

3.1 Guide to Configuration

Refer to the following guide for details on configuration functions. **Sections 3.4 to 3.5** describe how to get started with each interface.

Table 6 Guide to configuration details

Topic	Section	Page:
Connecting to an interface	3.2 - Open the Terminal Emulation Interface - Serial Connection	9
	3.3 - Open the Terminal Emulation Interface - TCP/IP Connection	10
	3.4 - Open the Telnet Interface	11
	3.5 - Open the Web Interface	12
Saving configuration changes	3.6 - Saving Changes and Reinitializing the Web Card	13
Performing configuration functions	4.0 - Equipment Information	14
	5.0 - Network Settings	15
	6.0 - Messaging	42
	7.0 - Factory Settings	46
	Appendix A - - Firmware Updates	A1

3.2 Open the Terminal Emulation Interface - Serial Connection

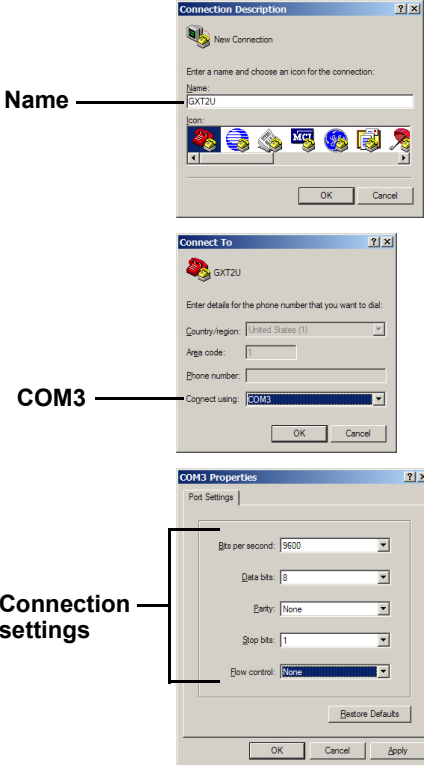
To access configuration using terminal emulation software with a serial connection to the Web card:

1. Open a terminal emulation application, such as HyperTerminal.
To do this:
 - Click the **Start** button, then **Programs, Accessories, Communications** and finally **HyperTerminal**.
2. In the Connection Description window, enter a name for the connection—for example, **GXT2U**—then click **OK**.
3. In the Connect To window:
 - Choose **COM3** from the Connect Using drop-down list.
 - Click **OK**.
4. In the COM3 Properties window, enter the communication settings shown in **Table 7**.

Table 7 Communication settings

Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None

5. When the message at right appears in the HyperTerminal window, press the Enter key.
6. In the Main Menu, enter the number that corresponds to your choice. Refer to **3.1 - Guide to Configuration** for details on each function.
7. After making changes, return to the Main Menu and choose **Exit and Save** to reboot the Web card and put your changes into effect (see **3.6 - Saving Changes and Reinitializing the Web Card**).



```
RTCS v2.96.00 Telnet server
Service Port Manager Active
<Esc> Ends Session
```

```
Main Menu
-----
1: Equipment Information
2: IP Network Settings
3: Messaging
4: Factory Settings
5: Firmware Updates

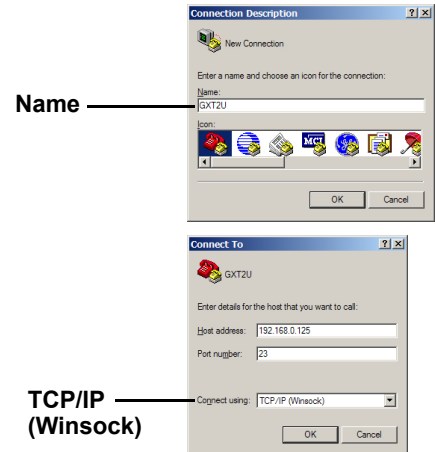
q: Quit and abort changes
x: Exit and save

Please select a key ?>
```

3.3 Open the Terminal Emulation Interface - TCP/IP Connection

To access configuration using terminal emulation software with an Ethernet connection to the Web card:

1. Open a terminal emulation application, such as HyperTerminal.
To do this:
 - Click the **Start** button, then **Programs, Accessories, Communications** and finally **HyperTerminal**.
2. In the Connection Description window, enter a name for the connection—for example, **GXT2U**—then click **OK**.
3. In the Connect To window:
 - Choose **TCP/IP (Winsock)** from the Connect Using drop-down list.
 - Enter the IP address or hostname of the Web card—for example, **192.168.0.125**—in the Host Address box, then click **OK**.



4. When the message at right appears in the HyperTerminal window, press the Enter key.
5. Enter the Administrator username and password (both are case-sensitive):
 - a. **Login** (username—default is *Liebert*)
 - b. **Password** (default is *Liebert*)

```
RTCS v2.96.00 Telnet server
Service Port Manager Active
<Esc> Ends Session
```

```
Login: Liebert
Password: *****
```

 **NOTE**

For security, change the default username and password (see 5.7 - Change Username / Password - Administrator and General User).

6. In the Main Menu, enter the number that corresponds to your choice. Refer to **3.1 - Guide to Configuration** for details on each function.
7. After making changes, return to the Main Menu and choose **Exit and Save** to reboot the Web card and put your changes into effect (see **3.6 - Saving Changes and Reinitializing the Web Card**).

```
Main Menu
-----
1: Equipment Information
2: IP Network Settings
3: Messaging
4: Factory Settings
5: Firmware Updates

q: Quit and abort changes
x: Exit and save

Please select a key ?>
```

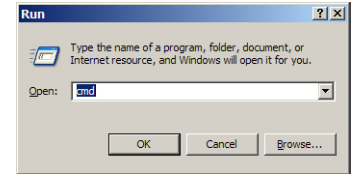

3.4 Open the Telnet Interface

To access configuration using Telnet:

1. Open a Telnet connection on a computer with an Ethernet connection to the Liebert unit.

To do this:

- Open a command prompt window—click the **Start** button, then **Run**.
- Enter **cmd** and click **OK**.
- In the command prompt window that opens, enter **telnet** followed by a space and the IP address or hostname of the Web card—for example:



telnet 192.168.0.125

2. When the message at right appears in the command prompt window, press the Enter key.
3. Enter the Administrator username and password (both are case-sensitive):
 - a. **Login** (username—default is *Liebert*)
 - b. **Password** (default is *Liebert*)

```
C:>telnet 192.168.0.125
```

```
RTCS v2.96.00 Telnet server
Service Port Manager Active
<ESC> Ends Session
```

```
Login: Liebert
Password: *****
```



NOTE

*For security, change the default username and password (see 5.7 - **Change Username / Password - Administrator and General User**).*

4. In the Main Menu, enter the number that corresponds to your choice. Refer to **3.1 - Guide to Configuration** for details on each function.
5. After making changes, return to the Main Menu and choose **Exit and Save** to reboot the Web card and put your changes into effect (see **3.6 - Saving Changes and Reinitializing the Web Card**).

```
Main Menu
-----
1: Equipment Information
2: IP Network Settings
3: Messaging
4: Factory Settings
5: Firmware Updates


q: Quit and abort changes
x: Exit and save

Please select a key ?>
```

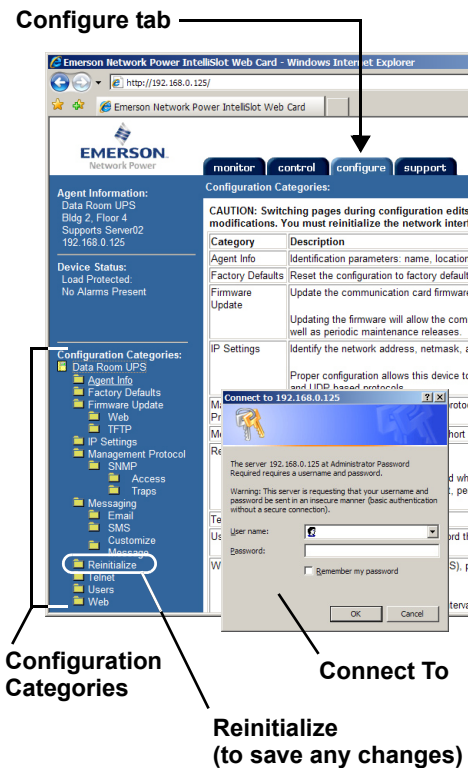
3.5 Open the Web Interface

To access configuration using the Web interface:

1. Open a Web browser such as Internet Explorer, then enter the IP address or hostname of the Web card in the address bar—e.g., **http://192.168.0.125**.
2. Click on the **Configure** tab, shown at right. Configuration Categories appear in the left panel, organized with folder icons.
3. Click on any configuration category, and the Connect To box opens.
4. Enter the Administrator username and password (both case-sensitive):
 - a. **User Name** (default is *Liebert*)
 - b. **Password** (default is *Liebert*)

 **NOTE**
 For security, change the default username and password (see 5.7 - **Change Username / Password - Administrator and General User**).

5. Click **OK**.
6. Refer to 3.1 - **Guide to Configuration** for details on each function.
7. After making changes, click the **Save** button, then click on **Reinitialize** to reboot the Web card and put your changes into effect (see 3.6 - **Saving Changes and Reinitializing the Web Card**).



3.6 Saving Changes and Reinitializing the Web Card

Follow the applicable steps for your interface to save configuration changes and reinitialize the Web card. Changes will not take effect until these steps are completed.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

- After each change is made, a reminder appears (shown at right).
- Return to the Main Menu, then choose **Exit and Save**. A message appears and remains until the card is reinitialized, followed by a message that the process was successful.

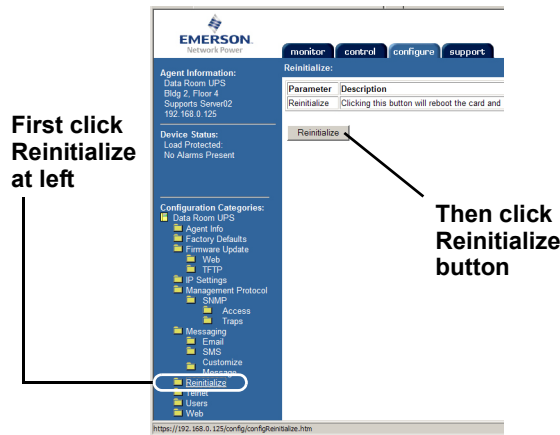
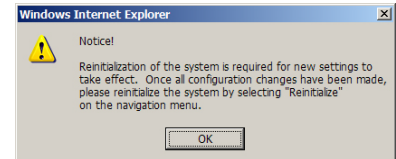
New Settings will take effect when saved
GO TO MAIN MENU AND DO 'EXIT AND SAVE' TO SAVE YOUR CHANGES!

Exiting and saving...
Configuration saved successfully

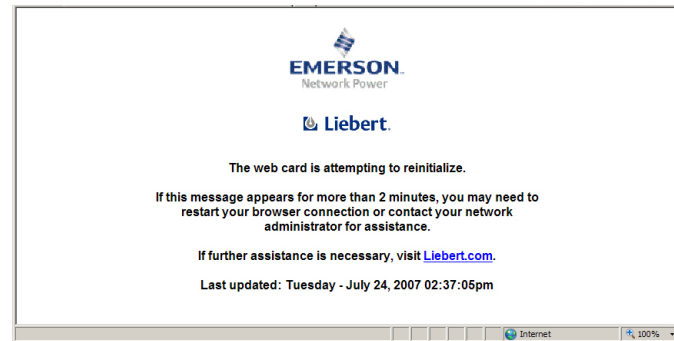


Web Interface

- After making each change, click the **Save** button. A reminder appears each time you make a change (shown at right).
- Without leaving the Configure tab window (below left), click **Reinitialize** in the left panel, then click the **Reinitialize** button at right to reboot the Web card and put your changes into effect.



Progress message window



- A message window appears, shown above right, and remains until the card is reinitialized.

4.0 EQUIPMENT INFORMATION

Equipment Information is optional and identifies the Liebert unit, its location, a contact person and other information about the unit. The default value of each field is “Uninitialized.”

```

Equipment Information Menu
-----
1: Name           Uninitialized
2: Contact        Uninitialized
3: Location       Uninitialized
4: Description    Uninitialized

<ESC>: Cancel menu level
Please select a key ?>
    
```



NOTE

This information also configures the SNMP parameters sysName, sysContact, sysDescr, and sysLocation available using RFC-1213 MIB II.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To edit any field in this category:

1. From the Main Menu, choose **Equipment Information**.
2. Enter the number that corresponds to your choice, then enter the identifying information, using the following as a guide.

Table 8 Equipment Information identifiers

Item	Description	Maximum Length*
Name	A name for the Liebert unit	255 characters
Contact	A contact person or department responsible for maintenance and operation of the Liebert unit	64 characters
Location	The location of the Liebert unit	64 characters
Description	Other useful information about the unit for quick reference	64 characters

* Valid characters include spaces and other printable characters except double quotes (").



Web Interface

To access Equipment Information through the Web interface:

- Click on the **Configure** tab, then **Equipment Information** in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

Configure tab

5.0 NETWORK SETTINGS

The IP Network Settings Menu is used to enable network communications with the Web card.

Refer to the following sections for detailed step-by-step instructions on each item from this menu:

Table 9 Network Settings menu guide

Menu item	Refer to:
5.1 - Boot/IP Settings	page 15
5.2 - Domain Name Server (DNS) Settings	page 19
5.3 - Management Protocol	page 24
5.4 - Web Server	page 33
5.5 - Telnet Server	page 38
5.6 - Time (SNTP) Menu	page 39
5.7 - Change Username / Password - Administrator and General User	page 40
5.8 - Reset WEB Authentication to Factory Defaults (Units with IS-WEBCARD, IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS, IS-WEBLB, IS-WEBX, IS-IPBMX Cards Only)	page 41

```

IP Network Settings Menu
-----
1: Boot/IP Settings
2: Domain Name Server (DNS) Settings
3: Management Protocol
4: Web Server
5: Telnet Server
6: Time (SNTP)
7. Change Administrator Username/
   Password
8: Change General Username/Password
9: Reset WEB Authentication to Factory
   Defaults

Option 9 above applies only to
the following cards:
• IS-WEBCARD
• IS-WEBL
• IS-IPBML
• IS-WEBS
• IS-IPBMS
• IS-WEBLB
• IS-WEBX
• IS-IPBMX

<ESC>: Cancel menu level
Please select a key ?>
    
```

5.1 Boot/IP Settings

5.1.1 Boot/IP Settings (All Cards Except IS-WEBCARD)

The Boot/IP Settings Menu is used to set parameters for network access to the Web card. Consult your network administrator for these settings.

```

Boot/IP Settings Menu
-----
1: Speed/Duplex Auto
2: Boot mode Static
3: IP Address
   192.168.0.125
4: Netmask 255.255.255.0
5: Default Gateway
   192.168.0.1
6: DNS Server 0.0.0.0
<ESC>: Cancel menu level
Please select a key ?>
    
```

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To change any parameter:

1. Choose **IP Network Settings** from the Main Menu, then **Boot/IP Settings**.
2. Select an option to change—for example, **Speed/Duplex**, then enter settings according to the following guide.

Table 10 Boot/IP settings range (all cards except IS-WEBCARD)

Parameter	Description & Valid Settings*
Speed/ Duplex	Speed and duplex configuration of the Ethernet port. <ul style="list-style-type: none"> • Auto (default—use this setting if unknown) • 10Mbs/Half Duplex • 10Mbs/Full Duplex • 100Mbs/Half Duplex • 100Mbs/Full Duplex
IPv4 Mode	<ul style="list-style-type: none"> • IPv4 Mode - DHCP • IP Address - Network address for the Liebert unit. Four numbers (0-255) separated by periods (.)—for example, 10.0.0.5 • Netmask - Network mask that divides your network into manageable segments. Four numbers (0-255) separated by periods (.)—e.g., 255.255.255.0 • Gateway - IP address of the gateway for network traffic to other networks or subnets. Four numbers (0-255) separated by periods (.)—e.g., 10.0.0.1
Boot Mode	Startup mode enabling the Web card to be a network-ready device. <ul style="list-style-type: none"> • Static - Fixed network addresses and other parameters • DHCP - Central management using dynamic network addresses • BootP - Older mechanism for central management of network addresses
DHCP/BootP Server	Device on a network that assigns IP addresses that are not static. Four numbers (0-255) separated by periods (.)—for example, 192.168.0.5
DNS Server	IP address of the Domain Name Server for the network. Four numbers (0-255) separated by periods (.)—e.g., 10.0.0.1

* Consult your network administrator for proper settings.

Web Interface

To access Boot/IP Settings through the Web interface:

- Click on the **Configure** tab, then **Network Settings** in the left panel and finally **Edit** beneath the table of parameters and descriptions. After making changes, click **Save**.

The screenshot shows the web interface for the Emerson Network Power IntelliSlot Web Card. The browser title is "Emerson Network Power IntelliSlot Web Card - Mozilla Firefox". The interface has a top navigation bar with tabs: "monitor", "control", "configure", "event log", and "support". The "configure" tab is selected. On the left side, there is a "Configuration Categories" tree with "Network Settings" selected. The main content area is titled "Network Settings" and contains a table of parameters:

Parameter	Description
Speed/Duplex:	Speed and duplex configuration of the ethernet port. Note: Typically, the value should be set to Auto, che
Boot Mode:	Mode the card boots into in order to be a network re <ul style="list-style-type: none"> ◊ Static: Directly specifies the network parame ◊ DHCP: Allows central management of networ ◊ BootP: Older mechanism for central manager configuration
IP Address*:	Network address for the interface.
Subnet Mask*:	Network mask for the interface which divides your ne
Default Gateway*:	IP address of the gateway for network traffic destine
	The value should be obtained from your network adr Acceptable values consists of 4 numbers, ranging fr character. As an example "10.0.0.1".

Below the table, there are input fields for "Speed/Duplex:" (set to "Auto"), "Boot Mode:" (with radio buttons for "Static", "BootP", and "DHCP", where "DHCP" is selected), "IP Address:" (192.168.0.25), "Subnet Mask:" (255.255.255.0), and "Default Gateway:" (192.168.0.1). There are "Edit" and "Reset" buttons. Annotations with arrows point to the "Configure" tab, "Network Settings" in the left menu, and the "Edit" button.

5.1.2 Boot/IP Settings (IS-WEBCARD Only)

The Boot/IP Settings Menu is used to set parameters for network access to the Web card. Consult your network administrator for these settings.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

1. Choose IP Network Settings from the Main Menu, then Boot/IP Settings.
2. Select an option to change—for example, Speed/Duplex, then enter settings according to the following guide.

```

Boot/IP Settings Menu
-----
1: Speed/Duplex      Auto
2: IPv4 Settings
3: IPv6 Settings
4: Ping Settings
<ESC>: Cancel menu level
Please select a key ?>

```

Table 11 Boot/IP settings range (IS-WEBCARD only)

Parameter	Description & Valid Settings*
Speed/Duplex	Speed and duplex configuration of the Ethernet port. Note: Typically, the value should be set to Auto; check with your network administrator
IPv4 Boot Mode	Method the card uses to configure an IPv4 address. <ul style="list-style-type: none"> • Static: Directly specifies the network parameters • BootP - Older mechanism for central management of network addresses and device configuration • DHCP - Allows central management of network addresses • Unconfigured - Do not configure an IPv4 address
IPv4 Address	Internet protocol version 4 address for the interface
Subnet Mask	Network mask for the address which divides your network into manageable segments
Default Gateway*	IPv4 address of the gateway for network traffic for other networks or subnets.
*	The value should be obtained from your network administrator. Acceptable values consist of 4 numbers, ranging from 0 to 255, separated with a *.* character. As an example, "10.0.0.1"
IPv6 Boot Mode	Method the card uses to configure an IPv6 address. <ul style="list-style-type: none"> • Static + Auto: Directly specifies the network parameters and allows central management of network addresses and device configuration • Auto - Allows central management of network addresses and device configuration • Unconfigured - Provides support for the link-local IPv6 address only
IPv6 Address	Internet protocol version 6 address for the interface
Prefix Length	Prefix length for the address divides your network into manageable segments. Acceptable values range 0-128.
Default Gateway**	IPv6 address of the gateway for network traffic desired for other networks or subnets.
**	The value should be obtained from your network administrator. Acceptable IPv6 values consist of 8 hexadecimal numbers ranging from 0 to ffff, separated by colons. A double colon can be used to eliminate the need to list consecutive zeroes within the address. As an example "2001:0db8::8a2e:030:7334"

Web Interface

To access Boot/IP Settings through the Web interface:

Click on the **Configure** tab, then **Network Settings** in the left panel and finally **Edit** beneath the table of parameters and descriptions. After making changes, click **Save**.

The screenshot displays the Liebert web interface for network configuration. On the left is a navigation menu with categories like 'Agent Information', 'Device Status', and 'Configuration Categories'. The 'Network Settings' option is selected. The main area shows a table of parameters with descriptions and a configuration form below it.

Parameter	Description
Gateway**	The value should be obtained from your network administrator. Acceptable values consists of 4 numbers, ranging from 0 to 255, separated with a "." character. As an example "10.0.0.1".
IPv6 Boot Mode	Method the card uses to configure an IPv6 address. <ul style="list-style-type: none"> Static + Auto: Directly specifies the network parameters and allows central management of network addresses and device configuration Auto: Allows central management of network addresses and device configuration Unconfigured: Provides support for the link-local IPv6 address only.
IPv6 Address**	Internet protocol version 6 address for the interface.
Prefix Length	Prefix length for the address which divides your network into manageable segments. Acceptable values range 0-120.
Default Gateway**	IPv6 address of the gateway for network traffic destined for other networks or subnets.
**	The value should be obtained from your network administrator. Acceptable IPv6 values consists of 8 hexadecimal numbers ranging from 0 to ffff, separated by colons. A double colon can be used to eliminate the need to list consecutive zeros within the address. As an example "2001:0db8:85a3:8a2e:0370:7334".

Below the table are 'Save' and 'Reset' buttons. The configuration form includes:

- Speed/Duplex: Auto (dropdown)
- IPv4 Mode: Static BootP DHCP Unconfigured
- IPv4 Address: 126.4.20.96
- Subnet Mask: 255.255.255.0
- Default Gateway: 126.4.20.1
- IPv6 Mode: Static + Auto Auto Unconfigured
- Auto: IPv6 Address: [text box], Default Gateway: [text box]
- Static: IPv6 Address: [text box], Prefix Length: 0, Default Gateway: [text box]

5.2 Domain Name Server (DNS) Settings

5.2.1 Domain Name Server (DNS) Settings (All Cards Except IS-WEBCARD)

The Domain Name Server settings menu configures the servers the Web card will use for hostname resolution. When configured, host addresses for SNMP, Network Time and Email/SMS can be specified in either full Domain Name format or in host-only format, provided that the appropriate Domain Name Suffix is used.

The DNS menu is used to set parameters for network access to the Web card. Consult your network administrator for these settings.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To change any parameter:

1. Choose **IP Network Settings** from the Main Menu, then **Domain Name Server (DNS) Settings**.
2. Select an option to change—for example, **DNS Mode**, then enter settings according to the following guide.

Table 12 Domain Name Server settings (all cards except IS-WEBCARD)

Parameter	Description & Valid Settings ¹
Disabled	DNS server addresses will not be obtained or assigned.
Obtain DNS server addresses automatically	Use DHCP/BootP-provided DNS server addresses. Note: This option is available only when the network Boot Mode is either DHCP or BootP.
Use the following DNS server addresses	Manually enter DNS addresses
Primary Domain Name Server (DNS)*	Primary IP address of the name server for the network, which should be obtained from your network administrator.
Secondary Domain Name Server (DNS)*	Secondary IP address of the name server for the network, which should be obtained from your network administrator.
DNS Resolve Interval	Interval to resolve DNS addresses from a network name to an IP Address.
DNS Naming	
*	Acceptable IPv4 DNS Server values consists of 4 numbers, ranging from 0 to 255, separated by periods (.) For example, "10.0.0.1" Acceptable IPv6 DNS Server values consist of 8 hexadecimal numbes ranging from 0 to ffff, separated by colons. A double colon can be used once to eliminate the need to list consecutive zeroes within the address. For example, "2001:0db8;85a3::0370:7334"

1. Consult your network administrator for proper settings.

Web Interface

To access the DNS menu through the Web interface:

- Click on the **Configure** tab, then **DNS** in the left panel under Network Settings and finally **Edit** beneath the table of parameters and descriptions. After making changes, click **Save**.

Configure tab

Click Edit to change settings

Obtain address automatically

Specify address

How long card retains resolved addresses

DNS

To access the DNS Test menu through the Web interface:

- Click on the **Configure** tab, then **Test** in the left panel under DNS in the Network Settings group.
- Choose the Type of DNS from the drop-down list—**Hostname**, **Fully Qualified Domain Name** or **IP Address**. In the Question box, enter a value for the DNS to answer.
- Click on the **Query** button. The DNS response will appear adjacent to the Last Query Response.

Configure tab

Test

Parameter	Description
Type	Type of DNS query
Question	Value for the domain name server (DNS) to answer.
Last Query Response:	Response from a domain name server (DNS) to the last query.

Domain Name Server (DNS) Test:

Type: Fully Qualified Domain Name

Question: _____

Last Query Response: _____

Query...

5.2.2 Domain Name Server (DNS) Settings (IS-WEBCARD Only)

The Domain Name Server settings menu configures the servers the Web card will use for hostname resolution. When configured, host addresses for SNMP, Network Time and Email/SMS can be specified in either full Domain Name format or in host-only format, provided that the appropriate Domain Name Suffix is used.

The DNS menu is used to set parameters for network access to the Web card. Consult your network administrator for these settings.

IPv4 and IPv6 Are Identical

```
Domain Name Server (DNS) Settings Menu
-----
1: Resolve Interval      24 hours
2: Domain Name Suffix
3: DNS Tests
4: IPv4 DNS Settings
5: IPv6 DNS Settings

<ESC>: Cancel menu level
Please select a keyv?> 2
Enter a domain name suffix (Max 64 chars) ?>
```



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To change any parameter:

1. Choose **IP Network Settings** from the Main Menu, then **Domain Name Server (DNS) Settings**.
 - Select an option to change—for example, **DNS Mode**, then enter settings according to the following guide.

Table 13 Domain Name Server settings (all cards except IS-WEBCARD)

Parameter	Description & Valid Settings ¹
DNS Server	
Disabled	DNS server addresses will not be obtained or assigned
Obtain DNS Server addresses automatically	Use DHCP/BootIP provided DNS server addresses. Note: This option is only available when the network Boot Mode is either DHCP or BootIP.
Use the following DNS server addresses	Manually enter DNS addresses.
Primary Domain Name Server (DNS) *	Primary IP address of the name server for network, which should be obtained from your network administrator.
Secondary Domain Name Server (DNS) *	Secondary IP address of the name server for network, which should be obtained from your network administrator.
DNS Resolve Interval	Interval to resolve DNS addresses from a network name to an IP Address.
DNS Naming	
Domain Name Suffix	Domain suffix. If specified, only the hostname(s) need to be entered rather than the fully qualified domain name (FQDN) for network names in other configuration fields.
*	Acceptable IPv4 DNS Server values consist of 4 numbers, ranging from 0 to 255, separated with a *.* character. As an example "10.0.0.1". Acceptable IPv6 DNS Server values consist of 8 hexadecimal numbers ranging from 0 to ffff, separated by colons. A double colon can be used once to eliminate the need to list consecutive zeroes within the address. As an example "2001:0db8:85a3::8a2e:0307:7334"

Web Interface

To access DNS Settings through the Web interface:

- Click on the **Configure** tab, then **Network Settings** in the left panel and **DNS** to alter DNS settings or on **Test** to test DNS entry. After making changes, click **Save**.



The screenshot displays the Emerson Liebert Network Server web interface. The top navigation bar includes tabs for monitor, control, configure, event log, and support. The left sidebar shows a tree view of configuration categories, with 'Network Settings' > 'DNS' selected. The main content area shows the DNS configuration page with the following sections:

addresses	
Primary Domain Name Server (DNS):	Primary IP address of the name server for network, which should be obtained from your network administrator.
Secondary Domain Name Server (DNS):	Secondary IP address of the name server for network, which should be obtained from your network administrator.
DNS Resolve Interval:	Interval to resolve DNS addresses from a network name to an IP Address.
DNS Naming	
Domain Name Suffix:	Domain suffix. If specified only the hostname(s) need to be entered rather than the fully qualified domain name (FQDN) for network names in other configuration fields.
<small>Acceptable IPv4 DNS Server values consists of 4 numbers, ranging from 0 to 255, separated with a "." character. As an example "10.0.0.1". Acceptable IPv6 DNS Server values consists of 8 hexadecimal numbers ranging from 0 to fff, separated by colons. A double colon can be used once to eliminate the need to list consecutive zeros within the address. As an example "2001:0db8:85a3:0000:0000:8a2e:0370:7334".</small>	

Below the table is an **Edit** button and the following configuration fields:

- Resolve Interval:** 24 hour
- Domain Name Suffix:** [Empty text box]
- IPv4 DNS Server:**
 - Disabled
 - Obtain DNS server addresses automatically
 - Use the following DNS server addresses
 - Primary Domain Name Server (DNS): 10.203.52.131
 - Secondary Domain Name Server (DNS): 10.20.64.11
- IPv6 DNS Server:**
 - Disabled
 - Obtain DNS server addresses automatically
 - Use the following DNS server addresses
 - Primary Domain Name Server (DNS): [Empty text box]
 - Secondary Domain Name Server (DNS): [Empty text box]

5.2.3 Domain Name Server (DNS) Test Settings (IS-WEB Card Only)

The DNS Test options allow you verify whether the DNS name entered under the DNS options can be reached by the DNS Server. The DNS server will return the Fully Qualified Domain Name, Host Name or IP Address that if found in response to the Question entered.

```
Domain Name Server (DNS) Settings Menu
-----
1: Resolve Interval      24 hours
2: Domain Name Suffix
3: DNS Tests
4: IPv4 DNS Settings
5: IPv6 DNS Settings
<ESC>: Cancel menu level
Please select a key ?> 2
Enter domain name suffix (Max 64
chars) ?>
```

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To change any parameter:

1. Choose **IP Network Settings** from the Main Menu, then **Domain Name Server (DNS) Settings**, then **DNS Tests**.
 - Select an option to change—for example, **Test Type (Type)** or **DNS Test String (Question)**, then enter settings according to the following guide.

```
DNS Tests Menu
-----
1: Test Type      Fully Qualified Domain Name
2: DNS Test String

<ESC>vCancel menu level
Please select a key ?> 1
1: Host Name
2: Fully Qualified Domain Name
3: IP Address
?>
```

Table 14 Domain Name Server (DNS) Test settings (IS-WEBCARD only)

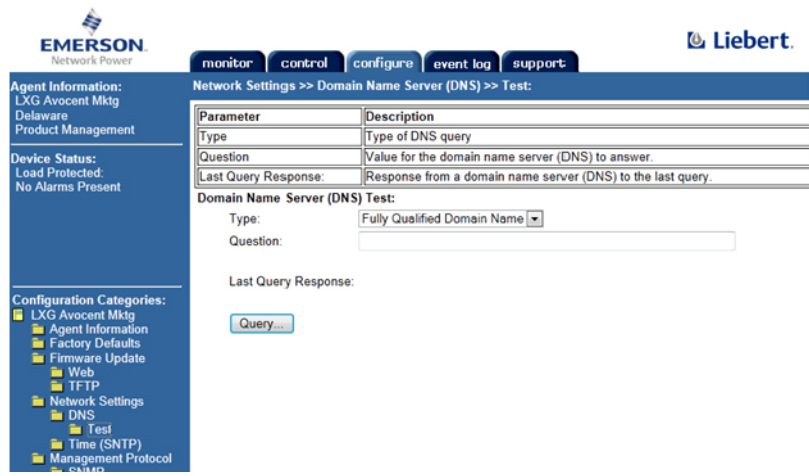
Parameter	Description & Valid Settings
Type ¹	Type of DNS Query
Question ²	Value for the domain name server (DNS) to answer.
Last Query Response	Response from a domain name server (DNS) to the last query
Domain Name Server (DNS) Test:	
Type	Fully Qualified Domain Name

1. Telnet shows Test Type
2. Telnet shows DNS Test String

Web Interface

To access DNS Test through the Web interface:

- Click on the **Configure** tab, then **Network Settings** in the left panel and **DNS** then **Test** to alter DNS Test settings.
- After making changes, click **Save**.



5.3 Management Protocol

The Management Protocol Menu allows you to enable or disable SNMPv1/v2c and SNMPv3 and configure management protocols. Consult your network administrator for these settings.



NOTE

SNMP v3 is available for IS-WEBCARD (HID9) only.

See Section 10 for Management Protocol options for BACnet and Modbus.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To change any parameter:

1. Choose **IP Network Settings** from the Main Menu, then **Management Protocol**.
2. Select an option to change, then use the following guide to make changes.

```
Management Protocol Menu
-----
1: SNMPv1/v2c Protocol   enabled
2: SNMPv3 Protocol      enabled
3: SNMP Communications
<ESC>: Cancel menu level
Please select a key ?>
```

Table 15 Management protocol ranges

Parameter	Description & Telnet Menus	
SNMP Protocol	Enable or disable SNMPv1/v2c or SNMPv3 for remote management.	<pre>Enable SNMPv1/v2c Protocol? [y/n] ?> Enable SNMPv3 Protocol? [y/n] ?></pre>
SNMP Communications	<p>The SNMP Communications Menu (shown at right) allows you to set up access privileges and configure the Web card to send traps for SNMPv1/v2c and SNMPv3.</p> <p>Refer to 5.3.1 - SNMP Communications Menu and Table 16 in that section for details and additional references to more information on these options.</p>	<pre>SNMP Communications Menu ----- 1: Authentication Traps yes 2: RFC-1628 (UPS) MIB enabled 3: - Traps enabled 4: Liebert Global Products MIB enabled 5: - Condition Traps enabled 6: - System Notify Trap enabled 7: Heartbeat Trap Interval 24 hours 8: Display/Modify SNMPv1/v2c Communities 9: Display/Modify SNMPv1/v2c Trap Communities A: Display/Modify SNMPv3 Settings B: Support Information <ESC>: Cancel menu level Please select a key ?> 1</pre>



Web Interface

To access SNMP Protocol settings through the Web interface:

- Click on the **Configure** tab, then **SNMP** (under **Management Protocol**) in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

The screenshot shows the Liebert web interface. At the top, there are navigation tabs: 'monitor', 'control', 'configure', 'event log', and 'support'. The 'configure' tab is active. On the left, there is a sidebar with 'Configuration Categories' including 'Monitoring Marketing', 'Agent Information', 'Factory Defaults', 'Firmware Update', 'Web', 'TFTP', 'Network Settings', 'DNS', 'Test', 'Time (SNTP)', 'Management Protocol', and 'SNMP'. The 'SNMP' category is selected. The main content area is titled 'Management Protocol:' and contains a table with two rows: 'v1/v2c Protocol' and 'v3 Protocol'. Both have checkboxes for 'enabled' which are checked. Below the table is an 'Edit' button. An arrow points from the text 'Click on Edit' to the 'Edit' button. At the bottom, the 'SNMP Agent:' section shows 'v1/v2c Protocol: [checked] enabled' and 'v3 Protocol: [checked] enabled Engine ID: 0000063000000a17e04145c'.

5.3.1 SNMP Communications Menu

Use the SNMP Communications Menu to enable authentication traps and view or change communities and trap communities, events and parameters.

Refer to **Table 16** for details on each menu option, as well as the following sections:

- **Section 5.3.2 - Display/Modify SNMPv1/v2c Communities**
- **Section 5.3.3 - Display/Modify SNMPv1/v2c Trap Communities**
- **Section 5.3.4 - Display/Modify SNMPv3 Settings (Units with IS-WEBCARD Only)**
- **Section 9.2 - Events and Parameters**
(for details on viewing Support Information)

```

SNMP Communications Menu
-----
1: Authentication Traps                yes
2: RFC-1628 (UPS) MIB                 enabled
3:   - Traps                          enabled
4: Liebert Global Products MIB        enabled
5:   - Condition Traps                enabled
6:   - System Notify Trap             enabled
7: Heartbeat Trap Interval             24 hours
8: Display/Modify SNMPv1/v2c Communities
9: Display/Modify SNMPv1/v2c Trap Communities
A: Display/Modify SNMPv3 Settings
B: Support Information

<ESC>: Cancel menu level
Please select a key ?> 1

```

Table 16 SNMP communications menu

Parameter	Description & Telnet Menus
Authentication Traps	Enables authentication traps to receive security alerts when the Web card detects a request with an invalid community string.
RFC-1628 (UPS) MIB	Enables the RFC-1628 (UPS specific information) MIB on the Web card for querying of information in that MIB. This can be enabled or disabled independently of the Liebert Global Products MIB.
• Traps	This option enables the RFC-1628 traps to be sent when an alarm event occurs on the device. The parent option must be enabled for this to also be enabled.
Liebert Global Products MIB	Enables the Liebert Global Products MIB (Enterprise Specific) for querying of information in that MIB. This option can be enabled or disabled independently of the RFC-1628 MIB.
• Condition Traps	Enables event condition traps to be sent per the LGP MIB. The parent option must be enabled for this to also be enabled.
• System Notify Trap	Enables system traps to be sent per the LGP MIB. The parent option must be also enabled for this to be enabled.
Heartbeat Trap Interval	Specifies how often a heartbeat trap will be sent to show that the device is online and functioning normally.
Display/Modify SNMPv1/v2c Communities	View devices that have permission to access the Web card, identified by IP address or hostname, read/write permission and community string. Up to 20 devices may be configured for access. See 5.3.2 - Display/Modify SNMPv1/v2c Communities .
Display/Modify SNMPv1/v2c Trap Communities	View devices that are configured to receive notifications from the Web card, identified by IP address or hostname, trap listen port and community string. Up to 20 devices may be configured to receive traps. See 5.3.3 - Display/Modify SNMPv1/v2c Trap Communities .
Display/Modify SNMPv3 Settings	View devices that have permission to access the Web card, identified by IP address and other parameters. See 5.3.4 - Display/Modify SNMPv3 Settings (Units with IS-WEBCARD Only) .
Support Information	View a list of all supported events and parameters for the Liebert equipment through any interface. Depending on the Liebert IntelliSlot Web™ Card, the list might include SNMP, Modbus or BACnet. See 9.2 - Events and Parameters .

Web Interface

To access SNMP Communications settings (for Authentication Traps, RFC-1628 (UPS) MIB, Liebert Global Products MIB and Heartbeat Trap Interval options) through the Web interface:

- Click on the **Configure** tab, then **SNMP** in the left panel (under **Management Protocol**) and finally **Edit** in the right panel. After making changes, click **Save**.
- Note the options vary according to the type of equipment. RFC-1628 MIB features are available for UPS/Power equipment only—not for Thermal Management and other equipment, as shown at bottom in the examples below.

Configure tab

Management Protocol

Click on Edit to enable any options

Interval choice sets the frequency of Heartbeat Traps

Category	Description
Access	Configure SNMP access parameters.
Traps	Configure SNMP trap targets.
Parameter	Description
Authentication Trap	If enabled, a SNMP Authentication Trap will be sent to all trap targets. Note: Typically this feature is enabled as a security measure to alert a management station that unintended/unauthorized requests are being received.
Heartbeat Trap Interval	A periodic "Heartbeat" trap will be sent at the selected interval to the trap targets that have been configured to receive heart beat traps. To select targets to receive heartbeat traps click here . Note: Receipt of a heartbeat trap indicates the source device is operating properly and has the expected connectivity.
RFC-1628 MIB	Enable or disable support for the retrieval of data from the RFC-1628 MIB objects. RFC-1628 is an IETF proposed standard for UPS information. Note: For proper operation of Multi-Link and Nform this feature must be enabled.
RFC-1628 MIB Traps	Enable or disable support for the sending of RFC-1628 MIB traps. RFC-1628 is an IETF proposed standard for UPS information. Note: For proper operation of Multi-Link and Nform this feature must be enabled.
Liebert Global Products (LGP) MIB	Enable or disable support for retrieval of data using the Liebert Global Products (LGP) MIB objects.
Liebert Global Products (LGP) MIB Traps	Enable or disable support for the Liebert Global Products (LGP) MIB Traps. Note that if a heart beat trap is enabled for a trap target and this (LGP) feature is disabled the heart beat trap will still be sent.
Liebert Global Products (LGP) System Notify Trap	Enable or disable support for the LGP System Notification Trap. This is a single trap that is sent each time a condition (alarm/warning) is added or removed from the conditions table. A varbind in this trap will contain a text description of the condition.

Edit

Authentication Traps: enabled

Heartbeat Trap Interval: 24 hours

RFC-1628 MIB: enabled

Traps: enabled

Liebert Global Products (LGP) MIB: enabled

Traps: enabled

System Notify Trap: enabled

OPTIONS FOR UPS/POWER EQUIPMENT
(includes RFC-1628 MIB features—retrieving data from RFC-1628 MIB objects and sending RFC-1628 MIB traps)

OPTIONS FOR THERMAL MANAGEMENT/OTHER EQUIPMENT
(does NOT include RFC-1628 MIB features)

Edit

Authentication Traps: enabled

Heartbeat Trap Interval: 24 hours

Liebert Global Products (LGP) MIB: enabled

Traps: enabled

System Notify Trap: enabled

5.3.2 Display/Modify SNMPv1/v2c Communities

View or modify devices that have permission to access the Web card, identified by IP address or hostname, read/write permission and community string. Choose **IP Network Settings** from the Main Menu, then **Management Protocol**.

Up to 20 devices may be configured for access.

EXAMPLE

Entry #	IP address	Access (read/write)	Community string
1:	10.0.0.5	write	public1
2:	10.0.0.6	write	public1

Codes for editing → `<a>dd <d>elete <e>dit`
Complex lines allowed. e.g. `<a 198.1.1.1 write public ?>`

Each device is identified by:

- **Entry Number** - use the entry number (1-20) to edit or delete an entry
- **IP address or Hostname** - the address of the device with access (MultiLink server, Nform server, Network Management System)
- **Access (read/write)** - **read** allows users to view but not change data; **write** allows full permission for configuration, control and viewing
- **Community string** - the community string used by the IP host for this Entry Number (case-sensitive, up to 32 characters)

To make changes:

- Add a device** (see example at right to enter all parameters in one line): **Example**
- Enter **a** to add an entry, then press Enter. *a 10.0.0.5 write public1*
 - Enter the IP address or hostname of the device to be added, then press Enter. (then press Enter)
 - Enter **1** for read or **2** for write access for this device, then press Enter.
 - Enter the community string, then press Enter.

- Edit a device** (see example at right to enter all parameters in one line): **Example**
- Enter **e** to edit an entry, then press Enter. *e 2 10.0.0.7 read public2*
 - Type the Entry Number, then press Enter. (then press Enter)
 - Enter the new IP address or hostname, then press Enter.
 - Enter **1** for read or **2** for write access for this device, then press Enter.
 - Enter the new community string, then press Enter.

- Delete a device** (see example at right to enter parameters in one line): **Example**
- Enter **d**, then press Enter. No confirmation message will appear. *d 2*
 - Type the Entry Number, then press Enter. (then press Enter)



NOTE

Avoid the following setting—it permits access by any host and may pose a security risk:

- IP address = 0.0.0.0
- Access = write
- Community = public

Web Interface

To access SNMPv1/v2c Communities settings through the Web interface:

- Click on the **Configure** tab, then **Access** or **V1 Access** (under **Management Protocol**) in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

Configure tab

EMERSON Network Power | Liebert.

Management Protocol >> SNMP >> V1 Access:

Parameter	Description
Entry	Entry number of the access source.
Network Name	Configure network hosts interested in device information access. The host can be identified as either a ip address or the network name of the host. <small>Note: Setting: Network name= 0.0.0.0, Access = write, and Community = public, allows write access by any host, this may be a security risk to consider.</small>
Access	Configure read and write access for network hosts.
Community	String identifying a "secret" known only by those hosts that are trusted for access. <small>Note: The maximum length of the entry is 32 characters.</small>
Clear	Clear the values of the parameters.

Edit ← Click on Edit

Entry	Network Name	Access	Community	
1	10.161.113.235	<input checked="" type="radio"/> read <input type="radio"/> write	LiebertEM	Clear
2	10.161.113.19	<input type="radio"/> read <input checked="" type="radio"/> write	public	Clear
3	126.4.203.125	<input type="radio"/> read <input checked="" type="radio"/> write	LiebertEM	Clear
4	0.0.0.0	<input checked="" type="radio"/> read <input type="radio"/> write	public	Clear
5	1.2.3.4	<input checked="" type="radio"/> read <input type="radio"/> write	test	Clear
6	10.161.113.25	<input checked="" type="radio"/> read <input type="radio"/> write	LiebertEM	Clear
7		<input checked="" type="radio"/> read <input type="radio"/> write		Clear

V1 Access

Configure up to 20 devices for read/write access



NOTE

Avoid the following setting—it permits access by any host and may pose a security risk:

- Network Name = 0.0.0.0
- Access = write
- Community = public

5.3.3 Display/Modify SNMPv1/v2c Trap Communities

View or modify devices that are configured to receive notifications from the Web card, identified by IP address or hostname, trap listen port and community string.

Up to 20 devices may be configured to receive traps.

EXAMPLE

Trap Communities			
Entry #	IP address	Port to receive traps	Community string
1:	10.0.0.5	162	public1
2:	10.0.0.6	162	public1

Codes for editing → `<a>dd <d>elete <e>dit`
Complex lines allowed. e.g. `<a 198.1.1.1 162 public> ?>`

Each device is identified by:

- **Entry Number** - use the entry number (1-20) to edit or delete an entry
- **IP address or hostname** - the address or name of the device to receive traps (MultiLink server, Nform server, Network Management System)
- **Port** - the Trap Listen Port where traps will be sent; use **162** if the host computer uses standard ports (161/162)
- **Community string** - the community string used by the IP host for this Entry Number (case-sensitive, up to 32 characters)

To make changes:

Add a device (see example at right to enter all parameters in one line): **Example**
a 10.0.0.5 162 public1
 (then press Enter)

- Enter **a** to add an entry, then press Enter.
- Enter the IP address or hostname of the device to be added, then press Enter.
- Enter the port number (default is **162**), then press Enter.
- Enter the community string, then press Enter.

Edit a device (see example at right to enter all parameters in one line): **Example**
e 2 10.0.0.7 162 public2
 (then press Enter)

- Enter **e** to edit an entry, then press Enter.
- Type the Entry Number, then press Enter.
- Enter the new IP address or hostname, then press Enter.
- Enter the port number (default is **162**), then press Enter.
- Enter the new community string, then press Enter.

Delete a device (see example at right to enter parameters in one line): **Example**
d 2
 (then press Enter)

Web Interface

To access SNMPv1/v2c Trap Communities settings through the Web interface:

- Click on the **Configure** tab, then **Traps** or **V1 Traps** (under **Management Protocol**) in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

The screenshot shows the Liebert web interface for configuring SNMP Traps. The left sidebar contains a navigation tree with 'Traps' selected under 'SNMP'. The top navigation bar has tabs for 'monitor', 'control', 'configure', 'data/logs', and 'support'. The main content area is titled 'Management Protocol >> SNMP >> Traps:' and contains a table of parameters and a configuration table.

Parameter	Description
Entry	Entry number of the trap target.
Network Host	Configure network hosts interested in alert notifications (i.e. SNMP Traps). The host can be identified as either an ip address or the network name of the host. Note: Typically notifications are sent to Network Management Systems (NMSs) and other hosts running Liebert MultiLink software for graceful operating system shutdown due to power outages.
Port	Port to send the notification to at the network host identified.
Community	String identifying a "secret" known only by those hosts that want to be notified of device status changes. Note: The maximum length of the entry is 32 characters.
Heartbeat Target	If checked the host will be sent a heartbeat trap. Note: Click the "Test Heartbeat" button to send a heartbeat test trap.
Clear	Clear the values of the parameters.

Entry	Network Host	Port	Community	Heartbeat	
1	126.4.20.80	162	LiebertEM	<input checked="" type="checkbox"/> enable	Clear
2		162		<input type="checkbox"/> enable	Clear
3		162		<input type="checkbox"/> enable	Clear
4		162		<input type="checkbox"/> enable	Clear
5		162		<input type="checkbox"/> enable	Clear
6		162		<input type="checkbox"/> enable	Clear
7		162		<input type="checkbox"/> enable	Clear
8		162		<input type="checkbox"/> enable	Clear
9		162		<input type="checkbox"/> enable	Clear
10		162		<input type="checkbox"/> enable	Clear

Annotations in the image include: 'Configure tab' pointing to the 'configure' tab; 'Traps' pointing to the 'Traps' menu item; 'Click on Edit' pointing to the 'Edit' button; 'Test Heartbeat Trap' pointing to the 'Test Heartbeat Trap' button; and 'Configure up to 20 devices to receive traps' pointing to the configuration table.

5.3.4 Display/Modify SNMPv3 Settings (Units with IS-WEBCARD Only)

View or modify SNMPv3 devices that have permission to access the Web card, identified by IP address and other parameters.

Up to 20 devices may be configured for access.

```
Display/Modify SNMPv3 Settings Menu
-----
Engine ID: 00000063000000a17e04145c
1: Display/Modify SNMPv3 Users
<ESC>: Cancel menu level
Please select a key ?> 1
```

EXAMPLE

```
Display/Modify SNMPv3 Users
-----
Num Enbl User Name Auth Priv R W N Access Addresses Notify Addresses
-----
1: YES Monitoring M MD5 DES Y Y Y 126.4.20.77 126.4.20.77
<ESC>: Cancel menu level
<a>dd <d>elete <e>dit <s>how <h>elp
Expert mode entry supported. Select <h>elp for details...
Make Selection: ?>
```

Codes for editing →

Each device is identified by these fields—numbers in parentheses correspond to field numbers in the **EDITING USER DATA** screen where data may be edited (shown below):

- **Num** (automatically generated) - use this entry number (1-20) to edit or delete an entry
- **Enbl** (1) - Shows whether SNMPv3 is enabled (*YES/NO*)
- **User Name** (2) - name of user (*Monitoring Marketing*)
- **Auth** (3) - type of authorization (*MD5/SHA-1/None*)
- **Priv** (4) - type of privacy (*DES/None*)
- **R** (5) - Read access allowed (*YES/NO*); permission to view but not change data
- **W** (6) - Write access allowed (*YES/NO*); full permission for configuration, control and viewing
- **N** (7) - Notifications access allowed (*YES/NO*)
- **Access Addresses** (8) - IP address of the device with read/write access as specified
- **Notify Addresses** (9) - IP address of the target device to receive notifications

```
EDITING USER DATA
1: User Record Enabled... YES
2: User..... Monitoring
Marketing
3: Auth Type..... MD5
4: Priv Type..... DES
5: Read Allowed..... YES
6: Write Allowed..... YES
7: Notifications Allowed: YES
8: Access Sources..... 126.4.20.77
9: Notification Targets.: 126.4.20.77
10: Auth Secret..... LiebertLiebert
11: Priv Secret..... LiebertLiebert
12: Notification Port.... 162
13: Enable Heartbeat Trap: YES
Enter # of field to edit, '0' to commit
edits, or <ESC>: to discard edits ?>
```

Other fields that may be edited in the **EDITING USER DATA** screen shown above are:

- **Auth Secret** (10) - Password (8-64 characters) for Get SNMPv3 request (e.g., *LiebertLiebert*)
- **Priv Secret** (11) - Password (8-64 characters) for Get SNMPv3 request (e.g., *LiebertLiebert*)
- **Notification Port** (12) - the Trap Listen Port where traps will be sent (*162* is standard port)
- **Enable Heartbeat Trap** (13) - notifications that the device is functioning normally (*YES/NO*)

To make changes:

Add a device (see example at right):

- Enter **a** to add an entry, then press Enter.
- The **EDITING USER DATA** screen appears (shown above right). Enter the field number of each item to be edited and make changes as needed.
- When finished, enter 0 (zero) to save changes (or Esc to exit without saving).

Example
a (press Enter)

Edit a device (see example at right):

- Enter **e** to edit an entry, then press Enter.
- Type the Num (entry number) of the entry to be edited, then Enter.
- The **EDITING USER DATA** screen appears (shown above right). Enter the field number of each item to be edited and make changes as needed.
- When finished, enter 0 (zero) to save changes (or Esc to exit without saving).

Example
e (press Enter)
2 (press Enter)

Delete a device (see example at right):

- Enter **d**, then press Enter. No confirmation message will appear.
- Type the Num (entry number) of the entry to be deleted, then Enter.

Example
d (press Enter)
2 (press Enter)



NOTE

Avoid the following setting—it permits access by any host and may pose a security risk:

- Access Sources (IP address) = 0.0.0.0
- Write Allowed = YES
- Auth Secret = LiebertLiebert
- Priv Secret = LiebertLiebert

Web Interface (Units with IS-WEBCARD Only)

To access SNMPv3 settings through the Web interface:

- Click on the **Configure** tab, then **V3 Settings** (under **Management Protocol**) in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

The screenshot shows the Emerson Liebert web interface. On the left, the 'Configure' tab is selected, and the 'V3 Settings' option is highlighted under the 'Management Protocol' category. An arrow points from this menu item to the main configuration area. The main area displays a table of parameters for 'SNMP >> V3 Setup'. Below this table, there are 'Save' and 'Reset' buttons. An arrow points from the 'Save' button to the text 'Click on Edit, then Save when finished'. Below the 'Save' buttons, there are two configuration sections for devices, each with fields for 'Enable', 'User Name', 'Access' (Read/Write), 'Notify', 'Heartbeat', 'Port', 'Authentication' (none, MD5, SHA-1), and 'Privacy' (none, DES). A 'Clear' button is present for each section.



NOTE

Avoid the following setting—it permits access by any host and may pose a security risk:

- Sources = 0.0.0.0
- Access = Write
- Authorization = none
- Privacy = none

5.4 Web Server

Use the Web Server Menu to configure access to the card through the Web interface. Consult your network administrator if needed.

```

Web Server Menu
-----
1: Web Server Mode           HTTP (Not Secure)
2: HTTP Transport Port      80
3: Password Protect Site    'disabled'
4: Configuration/Control    'enabled'
5: Refresh Rate             30 seconds
<ESC>: Cancel menu level
Please select a key ?>
    
```

5.4.1 Specify Web Server Settings

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To change any parameters:

1. Choose **IP Network Settings** from the Main Menu, then **Web Server**.
2. Select an option to change, then use the following guide to make changes.

Table 17 Web server settings

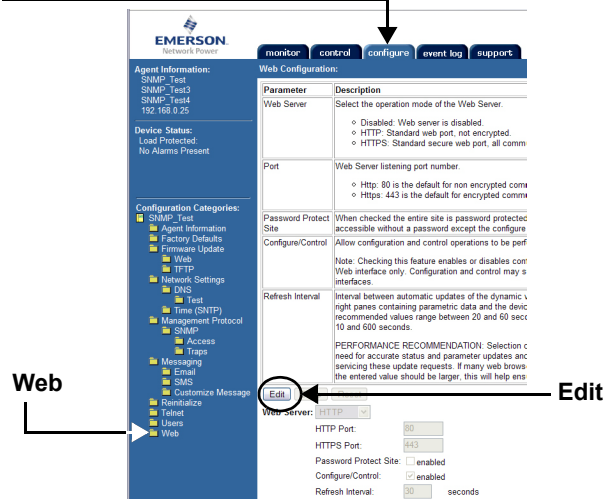
Parameter	Description & Valid Settings
Web Server Mode	Select the operation mode of the Web server. <ul style="list-style-type: none"> • Disabled - Web server is disabled • HTTP - Standard Web port, not encrypted • HTTPS - Standard secure Web port, all communication is encrypted
HTTP Transport Port	Web Server listening port number. <ul style="list-style-type: none"> • For HTTP mode (non-encrypted communications), the default port is 80. • For HTTPS mode (encrypted communications), the default port is 443. For HTTPS, you must also install a security certificate for Internet Explorer. Refer to the appropriate section for your version of Internet Explorer: <ul style="list-style-type: none"> • 5.4.2 - Install Security Certificates - Internet Explorer 6 or earlier • 5.4.3 - Install Security Certificates - Internet Explorer 7 or later
Password Protect Site	When enabled, the entire site is password-protected. (If disabled, all pages are accessible without a password except configure and control functions.)
Configuration/Control	Enable or disable the use of a Web browser to perform configuration and control operations. Note: This feature affects configuration and control operations from the Web interface only. If disabled, these functions may still be available using other system interfaces.
Refresh Interval	The interval in seconds (10 to 600 seconds) between automatic updates of dynamic Web pages—parametric data and device status in the right panel. RECOMMENDATION: Consider whether frequent updates will slow down the system. If many users will access the device simultaneously, select a larger value to best serve all users. Recommended values range from 20 to 60 seconds.

Web Interface

To access Web Server settings through the Web interface:

- Click on the **Configure** tab, then **Web** in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

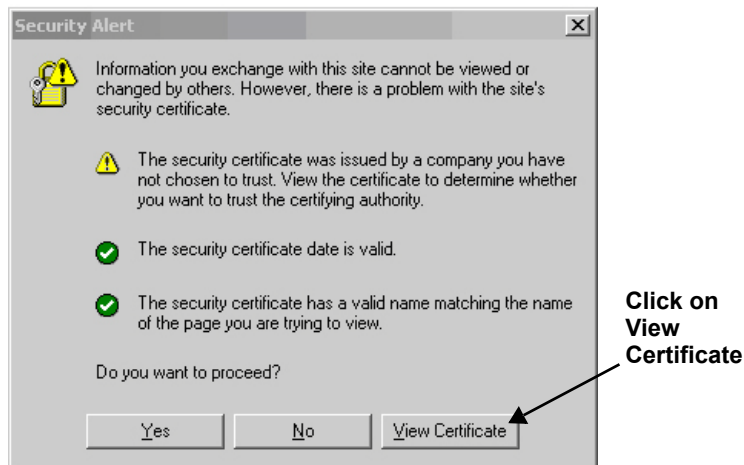
Configure tab



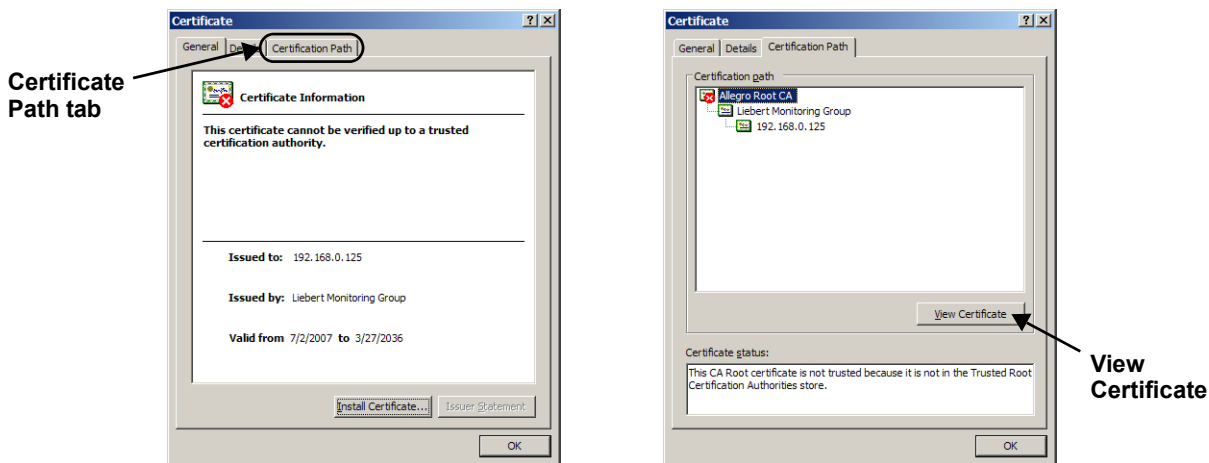
5.4.2 Install Security Certificates - Internet Explorer 6 or earlier

If you use Internet Explorer 6 or an earlier version and select **HTTPS** as the operation mode of the Web server (see 5.4.1 - **Specify Web Server Settings**), follow these instructions to install a security certificate.

- Open Internet Explorer and enter **https://** followed by the IP address or hostname of the Web card—for example, **https://192.168.0.125**—in the address bar. The following message appears.

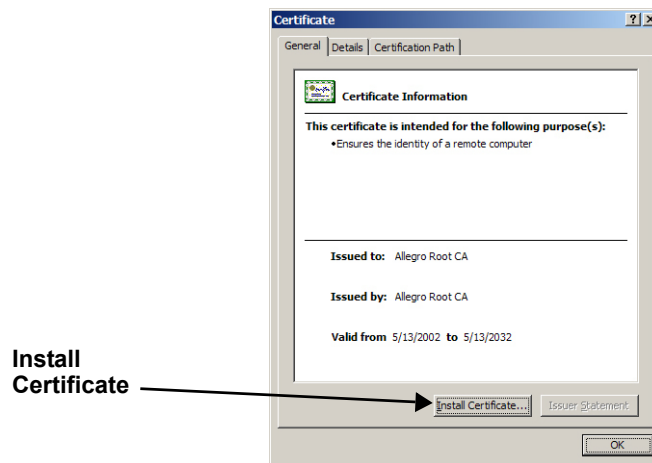


- Click the **View Certificate** button. This opens the Certificate window.

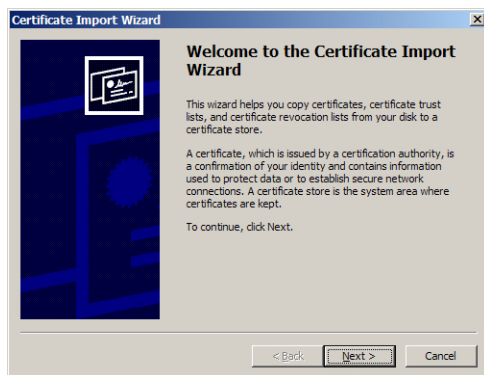


- In the Certificate window, above left, click the **Certificate Path** tab.
- In the Certificate Path tab, above right, click on **Allegro Root CA**, then on **View Certificate**.

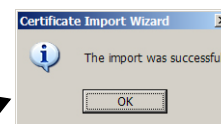
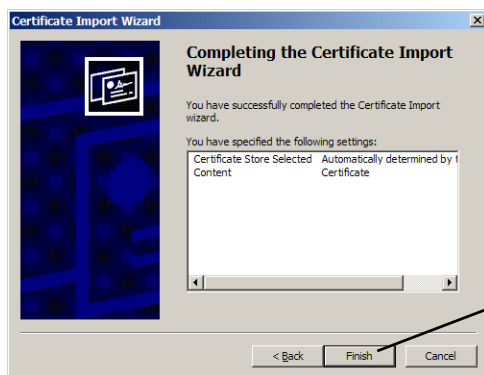
- In the Certificate window, click the **Install Certificate** button, as shown below.



- The Certificate Import Wizard opens. Click **Next**.



- Click on **Automatically select the certificate store based on the type of certificate**, then click **Next**.



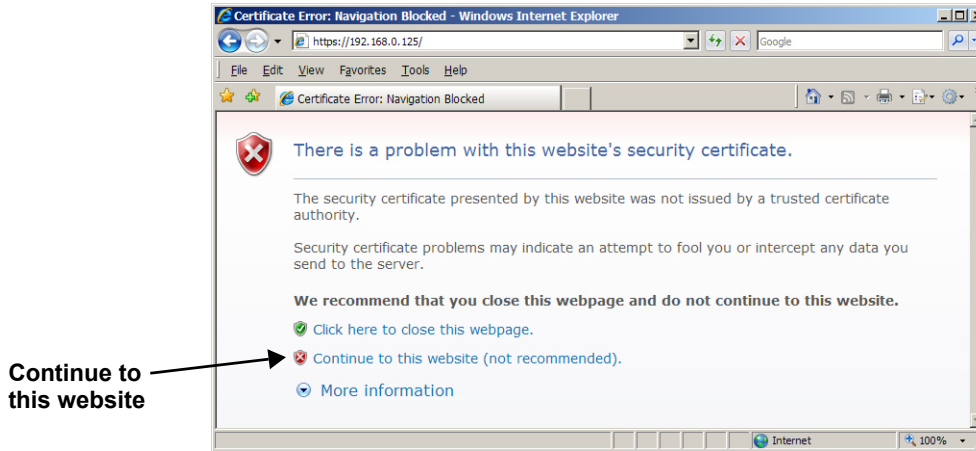
- The final Wizard window appears with a message that the process is complete. Click **Finish**.
- A confirmation box appears with a message that the import was successful. Click **OK**.

5.4.3 Install Security Certificates - Internet Explorer 7 or later

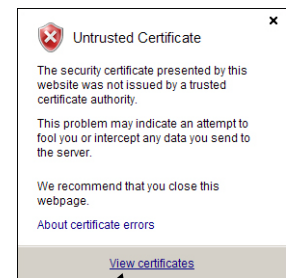
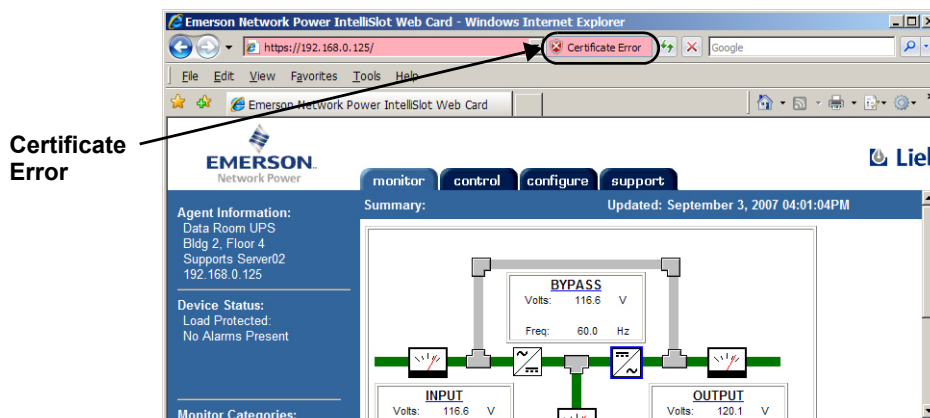
If you use Internet Explorer 7 or later and select **HTTPS** as the operation mode of the Web server (see 5.4.1 - Specify Web Server Settings), follow these instructions to install a security certificate.

To do this:

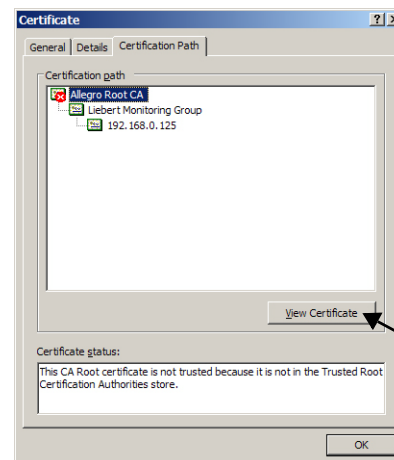
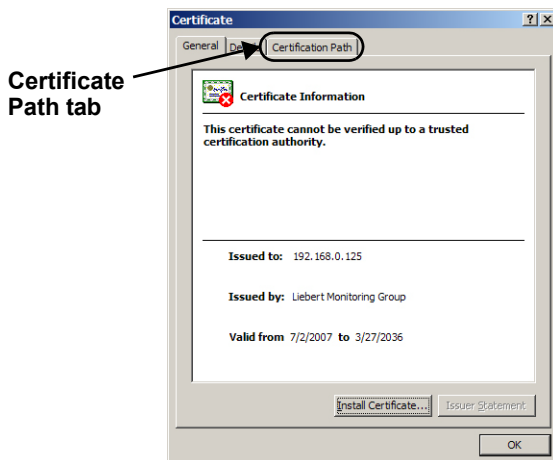
- Open Internet Explorer and enter **https://** followed by the IP address or hostname of the Web card—for example, **https://192.168.0.125**—in the address bar. The following message appears.



- Click on **Continue to this website (not recommended)** to open a connection to the Web card.

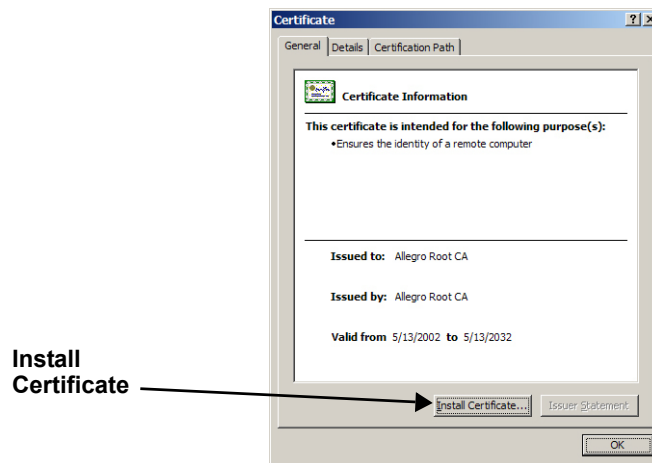


- Click the **Certificate Error** box next to the address bar, shown above left.
- In the window that pops up, shown next above right, click the **View Certificates** link. This opens the Certificate window.

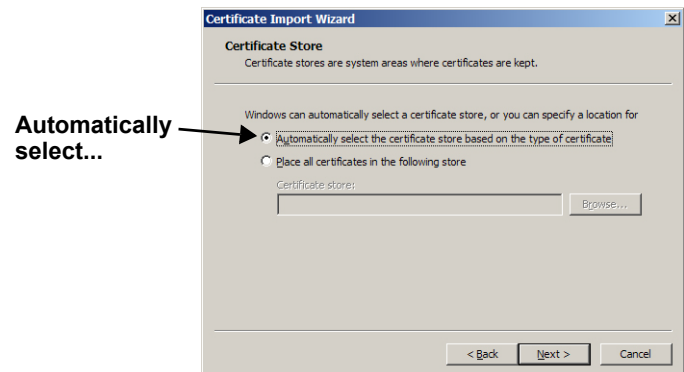
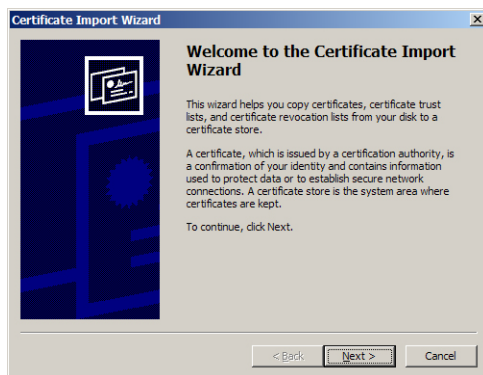


- In the Certificate window, above left, click the **Certificate Path** tab.
- In the Certificate Path tab, above right, click on **Allegro Root CA**, then on **View Certificate**.

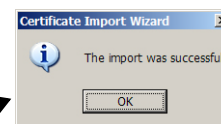
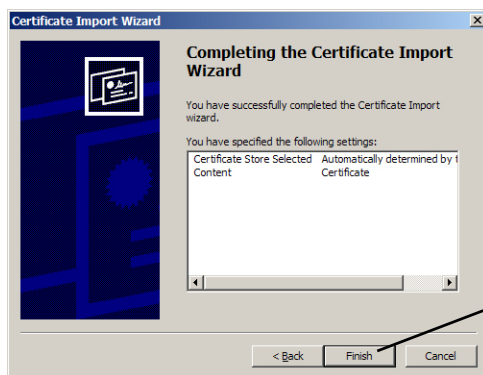
- In the Certificate window, click the **Install Certificate** button, as shown below.



- The Certificate Import Wizard opens. Click **Next**.



- Click on **Automatically select the certificate store based on the type of certificate**, then click **Next**.



- The final Wizard window appears with a message that the process is complete. Click **Finish**.
- A confirmation box appears with a message that the import was successful. Click **OK**.

5.5 Telnet Server

Use the Telnet Server Menu to enable or disable access to the Web card through a Telnet interface.

```
Telnet Server Menu
-----
1: Telnet Server      'enabled'
<ESC>: Cancel menu level
Please select a key ?>
```

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

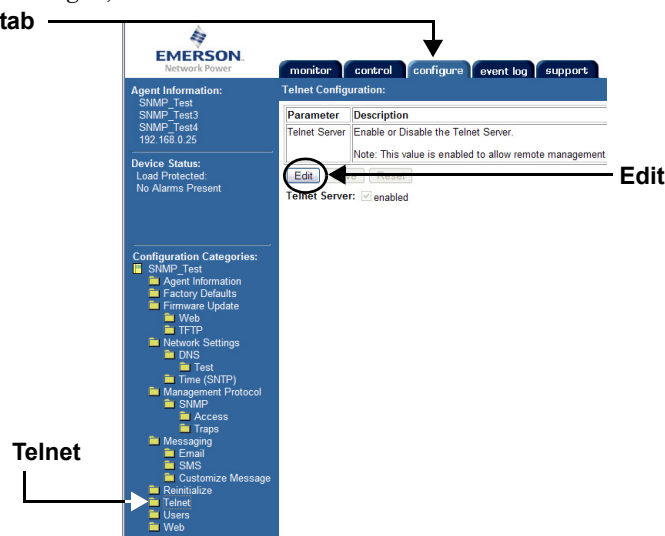
To change this setting:

1. Choose **IP Network Settings** from the Main Menu, then **Telnet Server**.
2. Choose Telnet Server, then specify:
 - **Enabled** to permit Telnet access
 - **Disabled** to block access via Telnet

Web Interface

To access Telnet settings through the Web interface:

- Click on the **Configure** tab, then **Telnet** in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.



5.6 Time (SNTP) Menu

This permits setting time options—how often the Web card synchronizes with the Time Server, which Time Server to use for synchronization and which the Time Zone the Web card is operating in.

```

Time Server Menu
-----
1: SNTP Time Sync Rate   Hourly
2: Time Server           time.nist.gov
3: Time Zone             (GMT) UTC
<ESC>: Cancel menu level
Please select a key ?>
    
```

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To change this setting:

1. Choose **IP Network Settings** from the Main Menu, then **Time (SNTP)**.
2. Choose SNTP Time Synch Rate, then specify:
 - Hourly
 - Daily
3. Choose Time Server, then specify the new time server, if desired.
4. Choose Time Zone, select a region from the list and then select a time zone.

Table 18 Time Server parameters

Parameter	Description & Telnet Menus
SNTP Time Sync Rate	This is how often the card will attempt to synchronize its internal clock with the specified time server.
Time Server	This is the server that will be used for synchronization. This can be either an IP address or a hostname, provided that the DNS options are configured.
Time Zone	This is the local Time Zone that will be used to correctly adjust the time provided by the server for the locale where the Web Card is being used.

Web Interface

To access Time (SNTP) settings through the Web interface:

Click on the **Configure** tab, then **Network Settings** in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

Configure tab

Click on Edit to choose options

Time Server list

Time Servers must be entered manually

Time zones available from list

5.7 Change Username / Password - Administrator and General User

The Web card is designed for two types of access, each with a default user name and password. For security, be sure to change the default password.

Table 19 Factory default passwords

Type of User	Factory Default		Description
Administrator	Username	Liebert	Full access to configuration and control functions, as well as viewing privileges
	Password	Liebert	
General User	Username	User	Viewing privileges only—no access to configuration or control functions
	Password	User	

Follow these guidelines to change the user name and password.

Table 20 Username and password guidelines

Maximum length	32 characters (6 or more characters recommended)
Valid characters	Any printable character EXCEPT colon, tab, double quote, question mark
Upper/lowercase	Case-sensitive—letters must be uppercase or lowercase as entered
Tips	Avoid common names, words and phrases as passwords



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To change the Administrator or General user name or password:

- Choose **IP Network Settings** from the Main Menu, then choose either:
 - **Change Administrator Username/Password** or
 - **Change General Username/Password**
- Enter a user name—the current user name is shown in brackets.

```
Enter Administrator Username, press enter for [Liebert]: (Max 32 chars) ?>
```

- Enter a password, then verify by typing the password again.

```
Enter New Password: (Max 32 chars) ?> *****
Verify Password: ?> *****
```



Web Interface

To access usernames and passwords through the Web interface:

- Click on the **Configure** tab, then **Users** in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

The screenshot shows the Emerson Network Power web interface. At the top, there are tabs for 'monitor', 'control', 'configure', and 'support'. The 'configure' tab is active. On the left, there is a navigation tree with 'Users' selected. In the main content area, the 'User Configuration' section is visible. It includes a table with 'Parameter' and 'Description' columns. Below the table, there are input fields for 'Administrator' and 'General User' usernames and passwords. The 'Administrator' fields show 'Username: Liebert' and 'Password: *****'. The 'General User' fields show 'Username: User' and 'Password: ****'. An 'Edit' button is circled in the right panel, and an arrow points to it from the 'Users' section in the left pane.

5.8 Reset WEB Authentication to Factory Defaults (*Units with IS-WEBCARD, IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS, IS-WEBLB, IS-WEBX, IS-IPBMX Cards Only*)

You may reset the Administrator and General User usernames and passwords to the factory defaults. This option applies only to the following cards:

- IS-WEBCARD
- IS-WEBL
- IS-IPBML
- IS-WEBS
- IS-IPBMS
- IS-WEBX
- IS-IPBMX
- IS-WEBLB

If you forget your username or password, you may reset them using a serial configuration cable connection (see Section 2.1.1 or 2.2.1 - **Connect the Cable**), which provides direct access to the card without a username or password. To enter a new username and password, see 5.7 - **Change Username / Password - Administrator and General User**.

Table 21 Factory default passwords

Type of User	Factory Default		Description
Administrator	Username	Liebert	Full access to configuration and control functions, as well as viewing privileges
	Password	Liebert	
General User	Username	User	Viewing privileges only—no access to configuration or control functions
	Password	User	



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To reset the usernames and passwords to the factory defaults:

1. Choose **IP Network Settings** from the Main Menu, then **Reset WEB Authentication to Factory Defaults**.
2. Enter **y** to reset the Administrator and General User usernames and passwords to the default settings.

```
IP Network Settings Menu
-----
1: Boot/IP Settings
2: Domain Name Server (DNS) Settings
3: Management Protocol
4: Web Server
5: Telnet Server
6: Time (SNTP)
7: Change Administrator Username/
  Password
8: Change General Username/Password
9: Reset WEB Authentication to Factory
  Defaults

<ESC>: Cancel menu level
Please select a key ?>9

Reset WEB Authentication to Factory
Defaults? [y/n] ?>
```



Web Interface



NOTE

This feature is not available through the Web interface.

6.0 MESSAGING

The Messaging menu is used to set up e-mail and text message notifications from the Web card.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To access these options:

1. Choose **Messaging** from the Main Menu.
2. Select an option, then use the following guide to make changes.

```

Messaging Menu
-----
1: Email  'disabled'
2: SMS    'disabled'
3: Email Configuration
4: SMS Configuration

<ESC>: Cancel menu level
Please select a key ?>
    
```

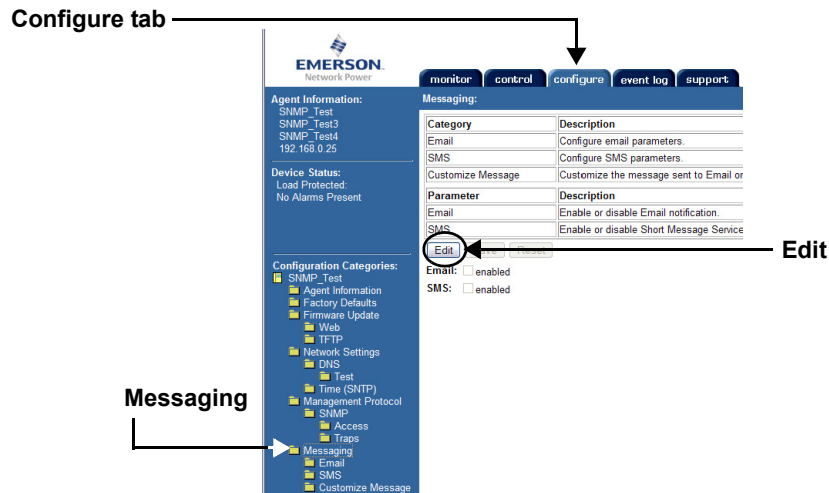
Table 22 Messaging menu guide

Menu item	Refer to:
E-Mail Configuration	page 43
SMS Configuration	page 44
Customize Messages (E-Mail and SMS)	page 45

Web Interface

To access Messaging settings through the Web interface:

- Click on the **Configure** tab, then **Messaging** in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.



6.1 E-Mail Configuration

Setting up event notifications to be sent via e-mail involves two steps: enabling the function, then specifying the parameters.

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To activate and set up e-mail messages:

1. Choose **Messaging** from the Main Menu, then **Email**.

```
Enable Email? [y/n] ?>
```

2. To enable the e-mail feature, enter **y** (yes) at the prompt.
3. Choose **Email Configuration** from the Messaging Menu, then select an option and use the following guide to make changes.

```

Email Configuration Menu
-----
1: Email From 'Uninitialized'
2: Email Message Recipients
3: Email Subject
4: Email Customize Message
5: SMTP Server 'Uninitialized'
6: Port 25
7: Test Email
8: View Test Email Log File

<ESC>: Cancel menu level
Please select a key ?>
    
```

Table 23 E-mail configuration guide

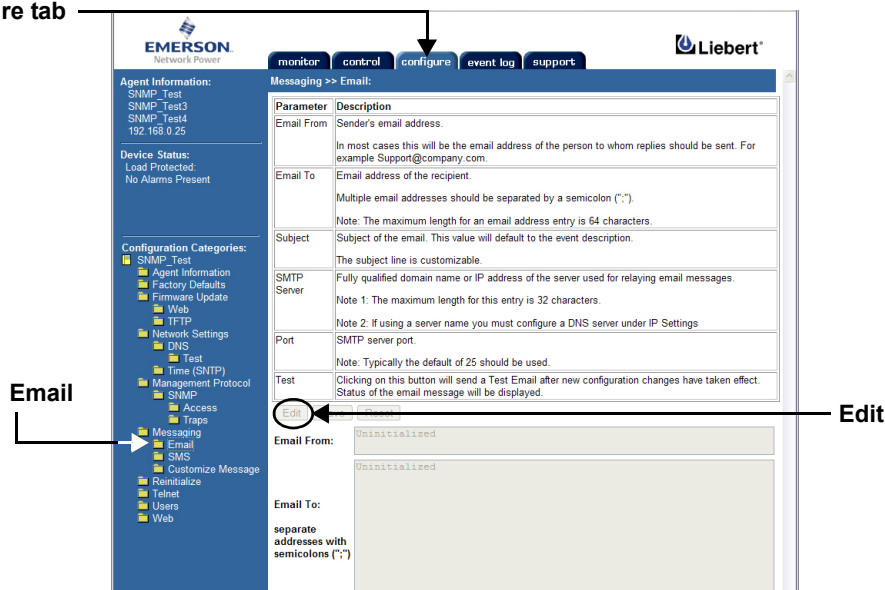
Parameter	Description	Maximum
Email From	The e-mail address of the sender—for example, <i>support@company.com</i> —typically, the address where replies should be sent.	64 characters
Email Message Recipients	The e-mail will be sent to this list of addresses. To add an e-mail address, use the format a jsmith@abc.com . Multiple addresses must be added individually. Changes may be made by entering d to delete an entry or e to edit an entry. NOTE: To specify multiple recipients of the e-mail message in the Web interface, use a semicolon (;) to separate addresses in the Email To box.	64 characters
Email Subject	The subject line of the e-mail. By default, this is the event description—e.g., <i>AlarmOnBypass</i> —but it may be customized.	120 characters
Email Customize Message	The text of the message sent to e-mail recipients. Choose from a list of items to include in the message. For details, see 6.3 - Customize Messages .	—
SMTP Server	The IP address or domain name of the SMTP e-mail server that sends messages.	32 characters
Port	SMTP server port—typically the default port, 25.	—
Test Email	After saving changes to e-mail parameters, send a test e-mail message to verify the settings are correct. The message status will be displayed.	—
View Test Email Log File	Choose this option to display a log showing the results of test e-mails.	—

Web Interface

To access E-Mail Configuration through the Web interface:

- Click on the **Configure** tab, then **Email** in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

Configure tab



The screenshot shows the Liebert web interface. At the top, there are tabs for 'monitor', 'control', 'configure', 'event log', and 'support'. The 'configure' tab is active. On the left, a navigation menu shows 'Email' selected under the 'Messaging' category. The main content area is titled 'Messaging >> Email:'. It contains a table with parameters and their descriptions:

Parameter	Description
Email From	Sender's email address. In most cases this will be the email address of the person to whom replies should be sent. For example Support@company.com.
Email To	Email address of the recipient. Multiple email addresses should be separated by a semicolon (";"). Note: The maximum length for an email address entry is 64 characters.
Subject	Subject of the email. This value will default to the event description. The subject line is customizable.
SMTP Server	Fully qualified domain name or IP address of the server used for relaying email messages. Note 1: The maximum length for this entry is 32 characters. Note 2: If using a server name you must configure a DNS server under IP Settings.
Port	SMTP server port. Note: Typically the default of 25 should be used.
Test	Clicking on this button will send a Test Email after new configuration changes have taken effect. Status of the email message will be displayed.

 Below the table, there are input fields for 'Email From:' and 'Email To:'. The 'Email From:' field contains 'Uninitialized'. The 'Email To:' field contains 'Uninitialized'. At the bottom left of the form area, there is an 'Edit' button circled in red.

6.2 SMS Configuration

Setting up event notifications for SMS text messages involves two steps: enabling the function, then specifying the parameters.

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To activate and set up SMS messages:

1. Choose **Messaging** from the Main Menu, then **SMS**.

```
Enable SMS [y/n] ?>
```

2. To enable the SMS feature, enter **y** (yes) at the prompt.
3. Choose **SMS Configuration** from the Messaging Menu, then select an option and use the following guide to make changes.

```
SMS Configuration Menu
-----
1: SMS From      'Uninitialized'
2: SMS Message Recipients
3: SMS Subject
4: SMS Customize Message
5: SMTP Server  'Uninitialized'
6: Port         25
7: Test SMS
8: View Test SMS Log File

<ESC>: Cancel menu level
Please select a key ?>
```

Table 24 SMS configuration guide

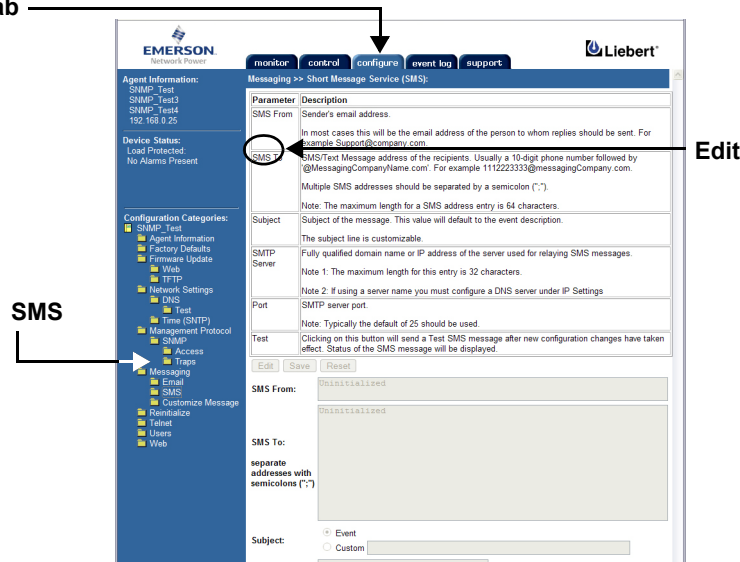
Parameter	Description	Maximum
SMS From	The e-mail address of the sender—for example, <i>support@company.com</i> —typically, the address where replies should be sent.	64 characters
SMS Message Recipients	The message will be sent to this list of addresses. The SMS/Text Message address is usually a 10-digit phone number followed by @____.com (where ____ might be a company name). To add an SMS address, use the format a 1112223333@abc.com . Multiple addresses must be added individually. Changes may be made by entering d to delete an entry or e to edit an entry. NOTE: To specify multiple recipients of the SMS message in the Web interface, use a semicolon (;) to separate addresses in the SMS To box.	64 characters
SMS Subject	The subject line of the message. By default, this is the event description—e.g., <i>AlarmOnBypass</i> —but it may be customized.	120 characters
SMS Customize Message	The text of the message sent to e-mail recipients. Choose from a list of items to include in the message. For details, see 6.3 - Customize Messages .	—
SMTP Server	The IP address or domain name of the SMTP e-mail server that sends messages.	32 characters
Port	SMTP server port—typically the default port, 25.	—
Test SMS	After saving changes to SMS parameters, send a test SMS message to verify the settings are correct. The message status will be displayed.	—
View Test SMS Log File	Choose this option to display a log showing the results of test messages.	—

Web Interface

To access SMS Configuration through the Web interface:

- Click on the **Configure** tab, then **SMS** in the left panel and finally **Edit** in the right panel. After making changes, click **Save**.

Configure tab



The screenshot shows the Emerson Liebert web interface. The top navigation bar includes 'monitor', 'control', 'configure', 'event log', and 'support'. The 'configure' tab is active. On the left, a tree view shows 'Configuration Categories' with 'SMS' selected. The main content area is titled 'Messaging >> Short Message Service (SMS)'. It contains a table with columns 'Parameter' and 'Description'. Below the table are input fields for 'SMS From', 'SMS To', 'Subject', 'SMTP Server', and 'Port'. There is a 'Test' button and 'Edit', 'Save', and 'Reset' buttons at the bottom. An arrow labeled 'Edit' points to the 'Edit' button.

6.3 Customize Messages

Both e-mail and SMS text messages may be customized to include items such as the IP address or hostname, event name and a link to the Web card in the body of the message.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

1. Choose **Messaging** from the Main Menu, then **Email Configuration** (or **SMS Configuration**).
2. Choose **Email** (or **SMS**) **Customize Message** from the Configuration menu.
3. Choose an option from the Email (or SMS) Customize Message Menu, then enter **y** (yes) at the prompt to confirm your choice. Repeat for each item to be included in messages. Refer to the following guidelines to make changes:

```

Email/SMS Customize Message Menu
-----
1: IP Address                'enabled'
2: Event                    'enabled'
3: Event Date & Time        'disabled'
4: Name                     'enabled'
5: Contact                  'enabled'
6: Location                 'enabled'
7: Description              'enabled'
8: Web link & Port          'disabled'
9: Event Consolidation      'enabled'
A: Consolidation Time Limit (seconds) 60
B: Consolidation Event Limit   30

<ESC>: Cancel menu level
Please select a key ?>
    
```

Table 25 E-mail and SMS message guidelines

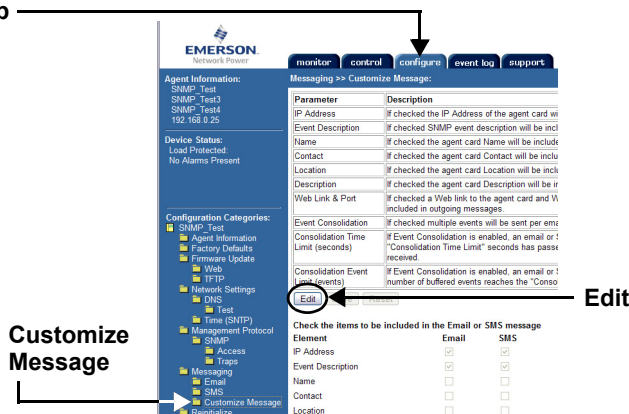
Parameter	Description—if enabled, outgoing messages will include:	Defined in:
IP address or hostname	The IP Address or Hostname of the Web card	5.1 - Boot/IP Settings
Event	Description of the SNMP event	9.0 - Support Information
Event Date & Time	The date & time when the SNMP event occurred	—
Name	The name for the Liebert unit	4.0 - Equipment Information
Contact	The contact person or department	
Location	The location of the Liebert unit	
Description	Other information about the Liebert unit	
Web Link & Port	A clickable link to the Web card through the Web interface The port number of the SMTP server port	5.1 - Boot/IP Settings
Event Consolidation	Enable or disable consolidation of events for e-mail/SMS notification	6.1 - E-Mail Configuration 6.2 - SMS Configuration
Consolidation Time Limit (seconds)	Duration (in seconds) to consolidate events before sending a notification. Notification will be sent when this threshold is reached, regardless of event limit. Range: 10 to 120.	Message Consolidation Time Limit on page 45
Consolidation Event Limit	Number of events to consolidate before sending a notification. Notification will be sent when this threshold is reached, regardless of time limit. Range: 1 to 50.	Message Consolidation Time Limit on page 45

Web Interface

To access Customize Message settings through the Web interface:

- Click on the **Configure** tab, then **Customize Messages** in the left panel and finally **Edit** in the right panel. Choose the items to include in each type of message in the Email and SMS columns.
- After making changes, click **Save**.

Configure tab



Message Consolidation Time Limit

Message Consolidation Time Limit allows adjusting the duration the card will wait for additional events before sending a notification E-mail. Consolidation event limit allows adjusting the number of events each E-mail will contain.

7.0 FACTORY SETTINGS

The Factory Settings menu allows you to restore factory default settings and offers other options that may vary by the Liebert unit where the card is installed. Refer to the following sections for details:

- 7.1 - Reset to Factory Defaults *
- 7.2 - Advanced Communication Settings *
- 7.3 - Agent Event Log *
- 7.4 - Support Information *
- 7.5 - Realtime Information *
- 7.6 - Task Stack Usage *

* Units with IS-WEBL, IS-WEBX, IS-IPBMX, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only

7.1 Reset to Factory Defaults

Factory default values may be restored for all configuration settings. This step:

- Replaces all user-defined settings described in this manual (see **3.0 - Configuration Overview** through **6.0 - Messaging**)
- Restores DHCP service, the factory default, replacing a static IP address or hostname, if configured during installation (see **2.0 - Installation**)



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To restore the factory default settings:

1. Choose **Factory Settings** from the Main Menu, then choose **Reset to Factory Defaults**.

```
Reset to factory defaults? [y/n] ?>
```

2. Enter **y** (yes) at the prompt to confirm your choice. To cancel, enter **n** (no).
3. A message appears until the process is complete.

```
Resetting card to factory defaults...
```

```
Factory Settings Menu
-----
1: Reset to Factory Defaults
2: Agent Card Information
<ESC>: Cancel menu level
Please select a key ?>
```



Web Interface

To restore the factory default settings through the Web interface:

- Click on the **Configure** tab, then **Factory Defaults** in the left panel and finally **Reset to Factory Defaults** in the right panel.

The screenshot shows the Emerson Network Power web interface. At the top, there are tabs for 'monitor', 'control', 'configure', 'event log', and 'support'. The 'configure' tab is active. On the left, there is a navigation pane with 'Factory Defaults' selected. The main content area displays 'Factory Defaults' with a table:

Parameter	Description
Reset To Factory Defaults	Clicking this button and confirming the action defaults

Below the table is a button labeled 'Reset To Factory Defaults'. Arrows point from the 'Configure tab' label to the 'configure' tab, from 'Factory Defaults' to the left navigation pane, and from 'Reset to Factory Defaults' to the button.

7.2 Advanced Communication Settings

The Advanced Communication Settings menu offers the following options:

- 7.2.1 - Local Node Settings for Multiple Cards
- 7.2.2 - Managed Device Settings
- 7.2.3 - Router Settings

7.2.1 Local Node Settings for Multiple Cards

If you install two Liebert IntelliSlot cards of the same type—two Web cards or two 485 cards—in a Liebert unit, you will need to change the default address of one card. Each type of card has a default MAC address and Node ID, as shown in **Table 26**.

Table 26 Factory default addresses

Type of Liebert IntelliSlot Card	Default MAC Address	Default Node ID
Web card	0x01	1
485 card	0x02	2

```
Factory Settings Menu
-----
1: Advanced Communication
   Settings
2: Reset to Factory Defaults
<ESC>: Cancel menu level
Please select a key ?>
```

```
Advanced Communication Settings
Menu
-----
1: Local Node Settings
2: Managed Device Settings
3: Reset to Default
<ESC>: Cancel menu level
Please select a key ?>
```



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To access local node settings:

1. Choose **Factory Settings** from the Main Menu.
2. Choose **Advanced Communication Settings** from the Factory Settings Menu.
3. Choose **Local Node Settings** from the Advanced Communication Settings Menu.
4. Choose **Node ID** from the Local Node Settings Menu, then use the following guide and **Table 26** to make changes.

If the Liebert unit has two Liebert IntelliSlot cards of the same type—Web or 485—change the address of one card:

- The default address for a Web card is **1**. Set the address of the second Web card to **2**.
- The default address for a 485 card is **2**. Set the address of the second 485 card to **1**.

```
Local Node Settings Menu
-----
1: Node ID: 1
2: Communication Rate: 38400
3: Maximum Master Address: 3
4: Maximum Retry Count: 5
5: Retry Interval(sec): 5
<ESC>: Cancel menu level
Please select a key ?>
```

7.2.2 Managed Device Settings

Units with IS-WEBL, IS-WEBX, IS-IPBMX, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only

Use the Managed Device Settings menu for connection settings for Liebert units with IS-WEBL, IS-WEBX, IS-IPBMX, IS-IPBML, IS-WEBS or IS-IPBMS cards (see **Table 1**).



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To specify connection settings for these units:

1. Choose **Factory Settings** from the Main Menu.
2. Choose **Advanced Communication Settings** from the Factory Settings Menu.
3. Choose **Managed Device Settings** from the Advanced Communication Settings Menu.
4. Choose **LAN Type** from the Local Node Settings Menu, then specify which communication port the card will use:
 - Choose **MS/TP** for 485 communications using the Liebert IntelliSlot 485 connection port.
 - Choose **BN/IP** for Ethernet communications using the Ethernet RJ45 connection port.
5. Choose **Network Number** from the Local Node Settings Menu, then specify the number of the network the card is connected to.
6. Choose **Node ID** from the Local Node Settings Menu, then specify the ID number of the server the card is communicating with.

```
Factory Settings Menu
-----
1: Advanced Communication
  Settings
2: Agent Event Log
3: Reset to Factory Defaults
4: Support Information
5: Realtime Information
6: Task Stack Usage
<ESC>: Cancel menu level
Please select a key ?>
```

```
Advanced Communication Settings
Menu
-----
1: Local Node Settings
2: Managed Device Settings
3: Router Settings
4: Reset to Default
<ESC>: Cancel menu level
Please select a key ?>
```

```
Managed Device Settings Menu
-----
1: Session Timeout(sec): 60
2: LAN Type: MS/TP
3: Network Number: 0
4: Node ID: 5
<ESC>: Cancel menu level
Please select a key ?>
```

7.2.3 Router Settings

Units with IS-WEBL, IS-WEBX, IS-IPBMX, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only

Use this menu to change router settings for Liebert units with IS-WEBL, IS-IPBML, IS-WEBS or IS-IPBMS cards (see **Table 1**).



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To specify router settings for these units:

1. Choose **Factory Settings** from the Main Menu.
2. Choose **Advanced Communication Settings** from the Factory Settings Menu.
3. Choose **Router Settings** from the Advanced Communication Settings Menu.
4. Choose **Router Enabled**, then turn the Protocol IP router on or off by choosing:
 - **Yes** to turn the router On (enable).
 - **No** to turn the router Off (disable).
5. Choose 485 Network Number, then specify the appropriate number.
6. Choose IP Network Number, then specify the appropriate number.

```
Factory Settings Menu
-----
1: Advanced Communication
  Settings
2: Agent Event Log
3: Reset to Factory Defaults
4: Support Information
5: Realtime Information
6: Task Stack Usage
<ESC>: Cancel menu level
Please select a key ?>
```

```
Advanced Communication Settings
Menu
-----
1: Local Node Settings
2: Managed Device Settings
3: Router Settings
4: Reset to Default
<ESC>: Cancel menu level
Please select a key ?>
```

```
Router Settings Menu
-----
1: Router Enabled: Yes
2: 485 Network Number: 1001
3: IP Network Number: 1000
<ESC>: Cancel menu level
Please select a key ?>
```

7.3 Agent Event Log

Units with IS-WEBL, IS-WEBX, IS-IPBMX, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only

Use this menu to enable or disable the event log for Liebert units with IS-WEBL, IS-IPBML, IS-WEBS or IS-IPBMS cards (see **Table 1**).



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To enable or disable the event log for these units:

1. Choose **Factory Settings** from the Main Menu.
2. Choose **Agent Event Log** from the Factory Settings Menu.
3. Choose **Agent Card Log** from the Advanced Communication Settings Menu, then choose:
 - **Enabled** to activate the event log.
 - **Disabled** to deactivate the event log.

```
Factory Settings Menu
-----
1: Advanced Communication
   Settings
2: Agent Event Log
3: Reset to Factory Defaults
4: Support Information
5: Realtime Information
6: Task Stack Usage
<ESC>: Cancel menu level
Please select a key ?>
```

```
Agent Event Log Menu
-----
1: Agent Card Log:      disabled
<ESC>: Cancel menu level
Please select a key ?>
```

7.4 Support Information

Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only

Use this menu to display support information for Liebert units with IS-WEBL, IS-IPBML, IS-WEBS or IS-IPBMS cards (see **Table 1**).



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To view Web card information for these units:

1. Choose **Factory Settings** from the Main Menu, then choose **Support Information**.
2. The Web card information appears, as shown in the following example. Press the Enter key to return to the previous menu.

```
MAC Address      00-00-68-18-8E-27
Network Card Model IntelliSlot Web Card
Network Card Part # IS-WEBCARD
Manufacture Date  MAY 10, 2008
Serial Number    416791G704T2008MAY100143
Boot Version     0.000.0
Boot Label       IS-WEBX_HID7_0.000.0_43860
App Version      3.410.0
App Label        IS-WEBX_HID7_3.410.0_047539
Hardware Version  7
CPU Speed        50 MHZ
Flash Usage      6367 Out of 8388 KByte
GDD Version      1
FDM Version      2014
OID1             2
OID2            10

Hit Enter to Exit
```

```
Factory Settings Menu
-----
1: Advanced Communication
   Settings
2: Agent Event Log
3: Reset to Factory Defaults
4: Support Information
5: Realtime Information
6: Task Stack Usage
<ESC>: Cancel menu level
Please select a key ?>
```

7.5 Realtime Information

Units with IS-WEBL, IS-WEBX, IS-IPBMX, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only

Use this menu to display realtime information for Liebert units with IS-WEBL, IS-IPBML, IS-WEBS or IS-IPBMS cards (see **Table 1**).



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To view realtime information for these units:

1. Choose **Factory Settings** from the Main Menu, then choose **Realtime Information**.
2. The information appears, as shown in the example at right. Press the Enter key to return to the previous menu.

```
Factory Settings Menu
-----
1: Advanced Communication
   Settings
2: Agent Event Log
3: Reset to Factory Defaults
4: Support Information
5: Realtime Information
6: Task Stack Usage
<ESC>: Cancel menu level
Please select a key ?>
```

```
=====
                    Realtime Information
=====
Feb 5 2009 14:11:29 <EST>
System Running Time: 3 Hour
                    42 Minute 48 Second
Flash Usage:       27%
Heap Usage:        18%
CPU Usage:         59%
```

7.6 Task Stack Usage

Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only

Use this menu to display task stack usage for Liebert units with IS-WEBL, IS-IPBML, IS-WEBS or IS-IPBMS cards (see **Table 1**)



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To view task stack usage information for these units:

1. Choose **Factory Settings** from the Main Menu, then choose **Task Stack Usage**.
2. The information appears, as shown in the example at right. Press the Enter key to return to the previous menu.

```
Factory Settings Menu
-----
1: Advanced Communication
   Settings
2: Agent Event Log
3: Reset to Factory Defaults
4: Support Information
5: Realtime Information
6: Task Stack Usage
<ESC>: Cancel menu level
Please select a key ?>
```

```
-----TASK STACK USAGE-----
Interrupt stack,76%
_mqx_idle_task,66%
Main,39%
Timer Task,12%
System Watchdog,47%
Service Port Manager,47%
HTTP Server,22%
Enp2ClientProcess,41%
Agent Log Server,43%
Velocity Startup Task,21%
Email Client,33%
SMS Client,33%
Telnet Task,55%
Telnet Server,29%
TCP/IP,27%
DNS Resolver,29%
TimeSync Startup,33%
workItemTask_101,33%
E2CacheMgr,11%
Device EventLog Task,2%
SNMP Agent,8%
Service Port Manager,58%
Service Terminal,26%
Hit Enter to Exit
```


8.0 MONITOR AND CONTROL FUNCTIONS - WEB ONLY

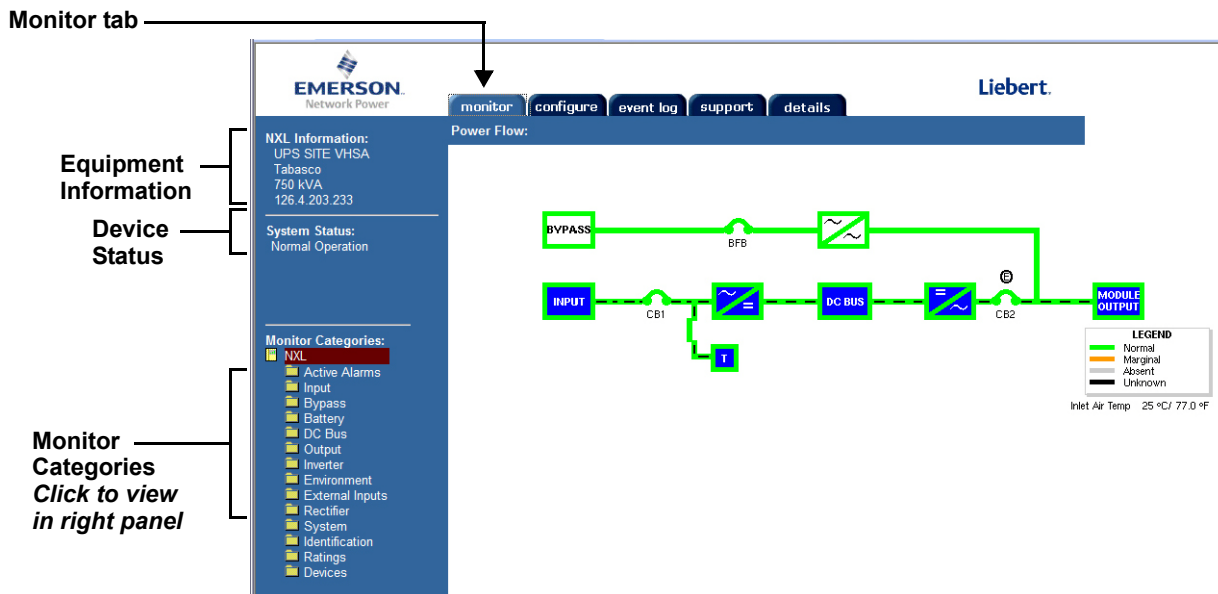
Web Interface Only

The Web interface allows you to monitor and control the Liebert equipment where the Web card is installed, in addition to configuration capabilities presented in previous sections.

8.1 Monitoring Liebert Equipment

To view monitoring data through the Web interface:

- Open the Web interface (if needed, see 3.5 - **Open the Web Interface**).
- Click on the **Monitor** tab if needed. This is always the opening view after connecting to the Web interface, as shown in the following example.



- The top portion of the left panel displays information that appears on all pages:
 - **Equipment Information** - name, contact, location and description of the Liebert unit (as defined in 4.0 - **Equipment Information**)
 - **Device Status** - current status of the Liebert unit and whether any alarms are active (if so, the most recent alarm is listed)
- **Monitor Categories** appear at bottom left, organized with folder icons and showing the available Monitoring functions.
- Click on a category to view parametric data in the right panel. The example above shows a graphic representation of the current state of a Liebert UPS. Other categories show data in table format. The information will vary according to the type of Liebert unit.



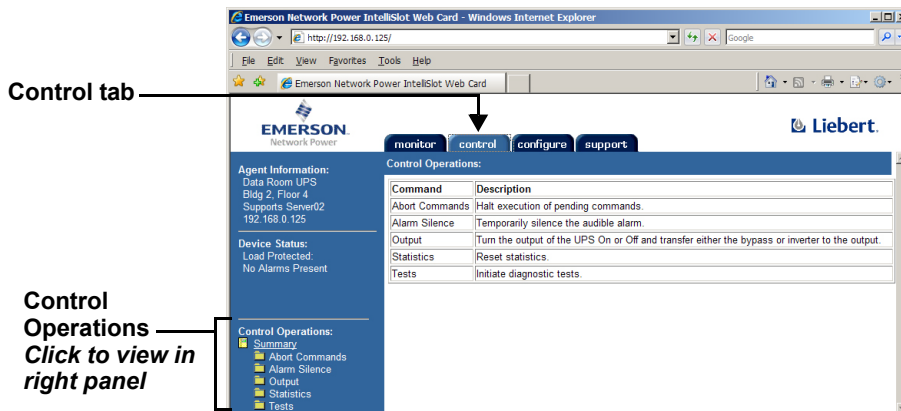
NOTE

*If any alarms are currently active, they are listed below the graphic in the opening window. Click on the **Active Alarms** category to view more details about any alarms that are active.*

8.2 Controlling Liebert Equipment

To perform Control operations through the Web interface:

- Open the Web interface (if needed, see 3.5 - Open the Web Interface).
- Click on the **Control** tab, as shown in the following example.



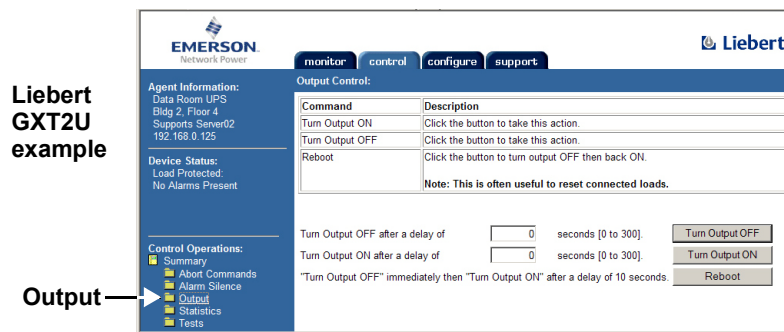
- **Control Operations** categories appear at bottom left, organized with folder icons and showing the available Control functions. Clicking on a category changes the view in the right panel. The example above shows the summary page.

The following guide is a partial list of Control operations—these vary by the type of Liebert unit.

Table 27 Control operations parameters—functions vary by Liebert unit

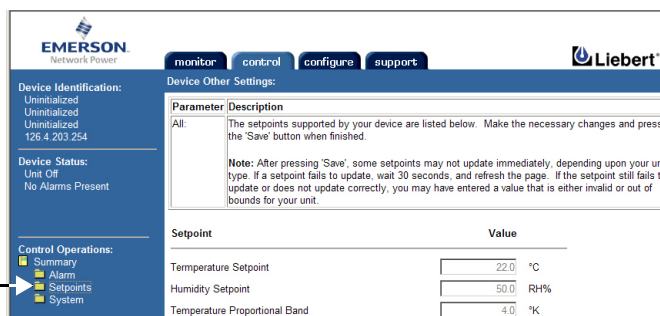
Command	Description
Abort Commands	Prevent any pending commands from being completed.
Alarm Silence / Alarms	Temporarily silence an audible alarm that is active. Reset or acknowledge alarms
Output / System	Turn the Liebert unit On or Off; reboot the unit.
Statistics	Reset statistics—for example, battery or power statistics
Tests	Initiate diagnostic tests on the Liebert unit.
Setpoints	Change setpoints for the Liebert unit.

- To perform an operation, click on a Control Operations category at left, then click on the appropriate button in the right panel. The example below shows control operations for two Liebert units.



Liebert DS example

Setpoints



8.3 Event Log



NOTE

For Liebert units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS, IS-WEBX or IS-IPBMX cards (see **Table 1**), the Web interface has a Data/Logs tab instead of the Event Log tab. For details, refer to 8.4 - **Data/Logs Tab (Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only)**.

The Event Log tab allows viewing events stored in the Web card's history. This history is gathered only when the Web card is installed and communicating properly with the device. The history is stored in descending chronological order; Page 1 Item 1 contains the most recent event.

The list of events includes:

1. The time and date of the event—This is either the local time and date (if the network time synchronization is working properly) or the time-delta from when the card was first powered on (if no network time synchronization has taken place).
2. The event ID—This is the index number given to events since the start of the history.
3. The event text—Text stating the type of event and how the card reacted.

Event Log Controls

<<-: Scroll directly to Page 1 of the history (most recent events)

<-: Scroll left one page in the history

->: Scroll right one page in the history

->>: Scroll directly to the last page of the history (oldest events)

Download Links

The Agent Event Log at the top of the page includes two links, **(.txt)** and **(.csv)**.

- The **txt** link will download the entire event history in unformatted text.
- The **csv** link will download the entire event history in comma-separated format, which can then be imported into an application such as Microsoft Excel®.

The screenshot shows the Liebert Web interface with the 'Event Log' tab selected. The interface includes the Emerson Network Power and Liebert logos. Navigation tabs are labeled 'monitor', 'control', 'configure', 'event log', and 'support'. The 'event log' tab is active, showing 'Agent Event Log (.txt) (.csv)' and 'Updated: June 24, 2008 09:55:13AM'. Below this are navigation buttons: '<<', '<', 'Page 1 of 1', '>', '>>', and 'Refresh'. A table displays event logs with columns for Time, ID, and Event.

Time	ID	Event
0:00:34 (SysUpTime)	2	Sent SNMP Trap IgpSysEventNotifications:Message:System Return to Normal to Trap Recipient List
0:00:34 (SysUpTime)	1	Sent SNMP Trap IgpSysEventNotifications:IgpSysNormal to Trap Recipient List

8.4 Data/Logs Tab (Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only)

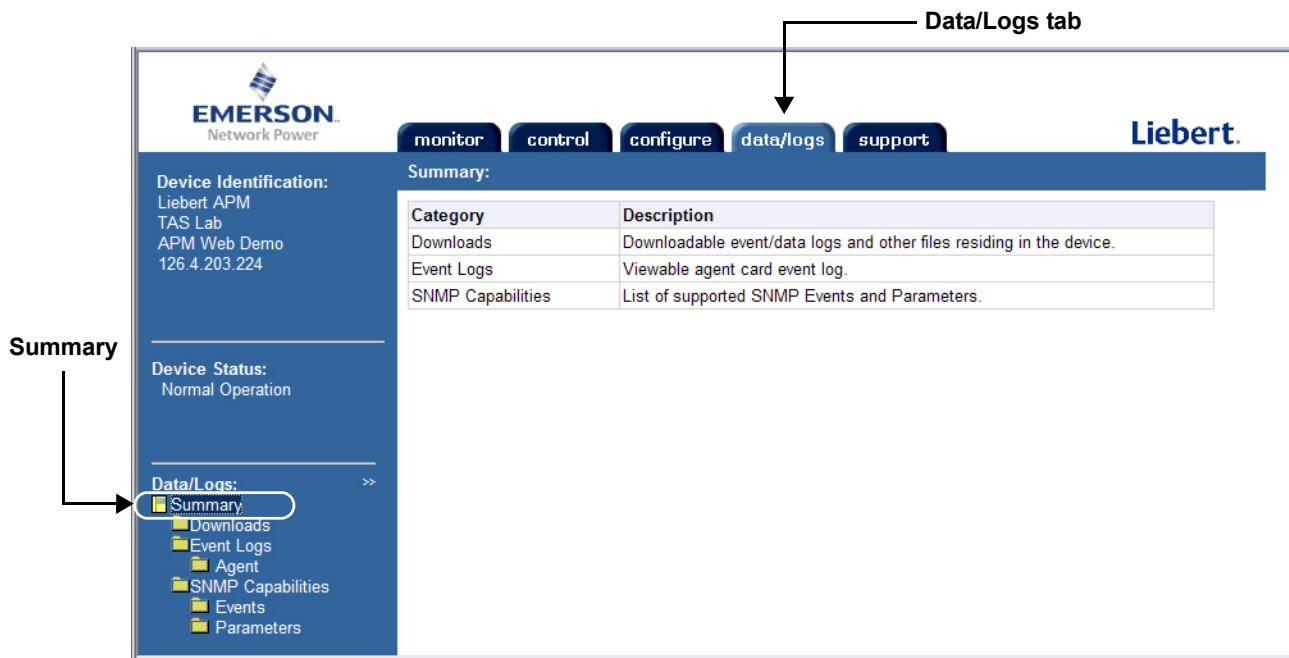
The Data/Logs tab offers the following features for Liebert units with IS-WEBL cards (see Table 1).

Table 28 Data/Logs tab features (Units with IS-WEBL Cards Only)

Feature	Description	For details, see:
Downloads	Event logs, data logs and other files that may be downloaded from the Liebert unit	8.4.1 - Downloads (Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only)
Agent	Log of events for the card	8.4.2 - Event Log Agent (Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only)
SNMP Capabilities	Events and parameters available for this Liebert unit	8.4.3 - Events and Parameters (Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only)

To view this list of features:

- Click on the **Data/Logs** tab at the top of the window.
- Click on **Summary** in the left panel.

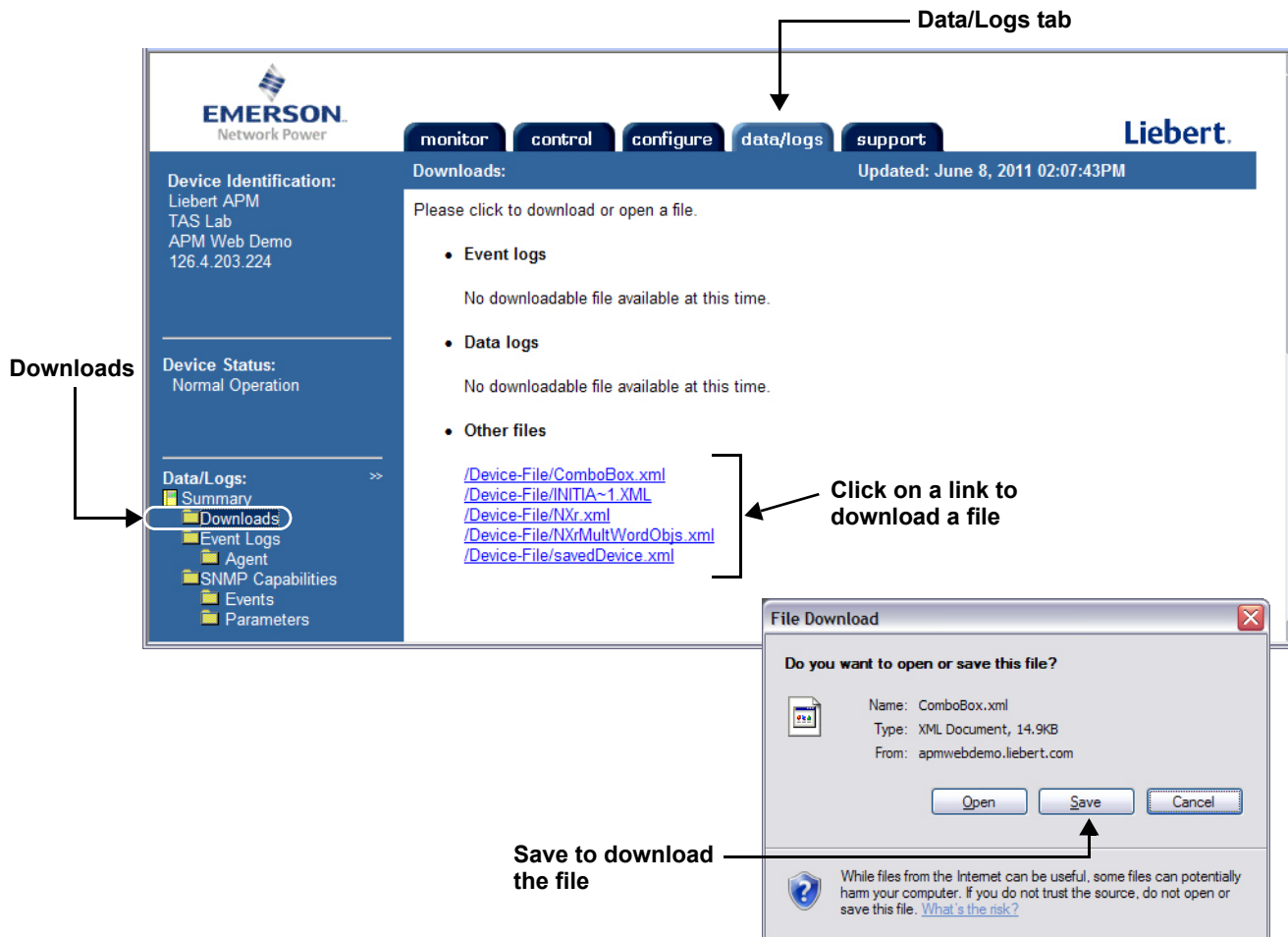


8.4.1 Downloads (Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only)

You may download event logs, data logs and other files stored in the Liebert unit.

To download or view a file:

- Click on the **Data/Logs** tab at the top of the window.
- Click on **Downloads** in the left panel.
- Downloadable files are listed as hyperlinks in the right panel in three categories: Event logs, Data logs and Other files.
- Click on a link to open the File Download dialog box, then click **Save** to download the file (or **Open** to view it). To complete the download, specify the file name and location where you wish to save it.



8.4.2 Event Log Agent (Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only)

The Event Log Agent allows viewing events stored in the Web card's history. This history is gathered only when the Web card is installed and communicating properly with the device. The history is stored in descending chronological order; Page 1 Item 1 contains the most recent event.

The list of events includes:

1. The time and date of the event—This is either the local time and date (if the network time synchronization is working properly) or the time-delta from when the card was first powered on (if no network time synchronization has taken place).
2. The event ID—This is the index number given to events since the start of the history.
3. The event text—Text stating the type of event and how the card reacted.

Event Log Controls

<<-: Scroll directly to Page 1 of the history (most recent events)

<-: Scroll left one page in the history

->: Scroll right one page in the history

->>: Scroll directly to the last page of the history (oldest events)

Download Links

The Agent Event Log at the top of the page includes two links, (.txt) and (.csv).

- The **txt** link will download the entire event history in unformatted text.
- The **csv** link will download the entire event history in comma-separated format, which can then be imported into an application such as Microsoft Excel.

To view this data:

- Click on the **Data/Logs** tab at the top of the window.
- Click on **Agent** in the left panel under **Event Log**.

The screenshot shows the web interface for the Liebert device. At the top, there are navigation tabs: monitor, control, configure, data/logs, and support. The 'data/logs' tab is active. Below the tabs, there is a header for 'Agent Event Log (.txt) (.csv)' with a 'Refresh' button and a page indicator 'Page 1 of 98'. A table of events is displayed below the header. The table has three columns: Time, ID, and Event. The events listed are:

Time	ID	Event
Oct 6 2009 09:51:00(EDT)	4477	Sent SNMP Trap IgpSysEventNotifications:Message:Firmware Update Successful to Trap Recipient List
Oct 6 2009 09:51:00(EDT)	4476	Sent SNMP Trap IgpAgentEventNotifications:IgpAgentFirmwareUpdateSuccessful to Trap Recipient List
Oct 2 2009 16:45:40(EDT)	4475	Sent SNMP Trap IgpSysEventNotifications:Message:Device Communication Lost to Trap Recipient List
Oct 2 2009 16:45:40(EDT)	4474	Sent SNMP Trap IgpAgentEventNotifications:IgpAgentDeviceCommunicationLost to Trap Recipient List
Oct 2 2009 13:12:56(EDT)	4473	Sent SNMP Trap IgpEventConditionEntryAdded:IgpConditionChilledWaterOverTemperature to Trap Recipient List
Oct 2 2009 13:12:56(EDT)	4472	Sent SNMP Trap IgpSysEventNotifications:Active:Alarm: Supply Chilled Water Over Temp to Trap Recipient List
Sep 30 2009 10:16:28(EDT)	4471	Sent SNMP Trap IgpEventConditionEntryAdded:IgpConditionHighHumidityReturnAir to Trap Recipient List
Sep 30 2009 10:16:26(EDT)	4470	Sent SNMP Trap IgpSysEventNotifications:Active:Alarm: High Return Humidity to Trap Recipient List
Sep 30 2009 08:51:06(EDT)	4469	Sent SNMP Trap IgpEventConditionEntryAdded:IgpConditionHighHumidityReturnAir to Trap Recipient List
Sep 30 2009 08:51:06(EDT)	4468	Sent SNMP Trap IgpSysEventNotifications:Active:Alarm: High Return Humidity to Trap Recipient List

8.4.3 Events and Parameters (Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only)

You may view a list of all supported SNMP events and parameters for the Liebert equipment through the Web interface.

To view this data:

- Click on the **Data/Logs** tab at the top of the window.
- Click on **Events** (or **Parameters**) in the left panel under **SNMP Capabilities**.
- The events or parameters are listed in the right panel. The example below shows a list of Events.

The screenshot displays the Emerson Liebert web interface. At the top, there are navigation tabs: monitor, control, configure, data/logs, and support. The 'data/logs' tab is selected. On the left side, there is a sidebar menu with sections: Device Identification, Device Status, and Data/Logs. Under Data/Logs, there are sub-items: Summary, Event Log, Agent, SNMP Capabilities, Events, and Parameters. The 'Events' item is highlighted. The main content area shows a list of SNMP Events under the heading 'SNMP Events:'. The list includes various event names and their corresponding IP addresses and ports. An arrow points to the 'Data/Logs tab' at the top right. Another arrow points to the 'Events (or Parameters)' label on the left sidebar. A third arrow points to the list of events in the right panel, labeled 'Listing in right panel'.

EMERSON
Network Power

Liebert.

monitor control configure **data/logs** support

Device Identification:
Uninitialized
Uninitialized
Uninitialized
126.4.100.78

Device Status:
Normal Operation

Data/Logs:
Summary
Event Log
Agent
SNMP Capabilities
Events
Parameters

SNMP Events:

[SNMP Events]
coldStart,1.3.6.1.6.3.1.1.5.1
IgpAgentDeviceCommunicationLost,1.3.6.1.4.1.476.1.42.2.3.0.1
IgpAgentFirmwareUpdateSuccessful,1.3.6.1.4.1.476.1.42.2.3.0.5
IgpAgentFirmwareCorrupt,1.3.6.1.4.1.476.1.42.2.3.0.6
IgpAgentHeartbeat,1.3.6.1.4.1.476.1.42.2.3.0.7
IgpAgentDnsLookupFailure,1.3.6.1.4.1.476.1.42.2.3.0.8
IgpConditionCompressor1LowSuctionPressure,1.3.6.1.4.1.476.1.42.3.2.1.10.1
IgpConditionStandbyGlycoolPumpOn,1.3.6.1.4.1.476.1.42.3.2.1.13
IgpConditionCompPumpDownFailure,1.3.6.1.4.1.476.1.42.3.2.1.130
IgpConditionChilledWaterLowWaterFlow,1.3.6.1.4.1.476.1.42.3.2.1.131
IgpConditionHumidifierRunHrsExceeded,1.3.6.1.4.1.476.1.42.3.2.1.134.10
IgpConditionDehumidifierRunHrsExceeded,1.3.6.1.4.1.476.1.42.3.2.1.134.11
IgpConditionFanRunHrsExceeded,1.3.6.1.4.1.476.1.42.3.2.1.134.12
IgpConditionComp1RunHrsExceeded,1.3.6.1.4.1.476.1.42.3.2.1.134.2
IgpConditionElectricalHeater1RunHrsExceeded,1.3.6.1.4.1.476.1.42.3.2.1.134.5
IgpConditionUnitOn,1.3.6.1.4.1.476.1.42.3.2.1.136
IgpConditionUnitOff,1.3.6.1.4.1.476.1.42.3.2.1.137
IgpConditionWaterUnderFloor,1.3.6.1.4.1.476.1.42.3.2.1.14
IgpConditionSystemOnStanby,1.3.6.1.4.1.476.1.42.3.2.1.140
IgpConditionHighTemperatureSupplyAir,1.3.6.1.4.1.476.1.42.3.2.1.142.10
IgpConditionHighTemperatureReturnAir,1.3.6.1.4.1.476.1.42.3.2.1.142.11
IgpConditionHighTemperatureDigitalScroll1,1.3.6.1.4.1.476.1.42.3.2.1.142.2
IgpConditionLowTemperatureSupplyAir,1.3.6.1.4.1.476.1.42.3.2.1.143.7
IgpConditionHighHumidityReturnAir,1.3.6.1.4.1.476.1.42.3.2.1.144.2
IgpConditionLowHumidityReturnAir,1.3.6.1.4.1.476.1.42.3.2.1.145.2
IgpConditionPeerNetworkNoMaster,1.3.6.1.4.1.476.1.42.3.2.1.146

9.0 SUPPORT INFORMATION

Support data includes identifying information for the Web card, as well as events and parameters available for the Liebert equipment.

9.1 View Web Card Information

Identifying information for the Web card may be viewed through any interface and includes the MAC address, model and part number, serial number and firmware version.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To view Web card information:

1. Choose **Factory Settings** from the Main Menu, then choose **Agent Card Information**.
2. The Web card information appears, as shown in the following example. Press the Enter key to return to the previous menu.

```

MAC Address          00-00-68-16-82-C1
Network Card Model  IntelliSlot web Card
Network Card Part # OCWEBCARD
Manufacture Date    APR 28, 2004
Serial Number       416701G105T2004APR280074
Boot Version        2.300.0
Boot Label          OCWEBCARD_HID3_2.300.0_034380
App Version         2.300.0
App Label           OCWEBCARD_HID3_2.300.0_035191
Hardware Version    3
CPU Speed           50 MHZ
Flash Usage         4327 Out Of 8388 KByte

Hit Enter to Exit
  
```

```

Factory Settings Menu
-----
1: Reset to Factory Defaults
2: Agent Card Information
<ESC>: Cancel menu level
Please select a key ?>
  
```



Web Interface

To view Web card information through the Web interface:

- Click on the **Support** tab, then **Summary** in the left panel. The Web card information appears in the right panel.

The screenshot shows the EMERSON Network Power web interface. At the top, there are tabs for 'monitor', 'control', 'configure', and 'support'. The 'support' tab is selected. On the left side, there is a navigation menu with 'Support' expanded to show 'Summary', 'Capabilities', 'Events', and 'Parameters'. The 'Summary' option is selected. The main content area displays a table of support information.

Support tab points to the 'support' tab in the top navigation bar.

Listing in right panel points to the table of support information.

Summary points to the 'Summary' option in the left navigation menu.

Item	Value
System Name	Data Room UPS
Location	Bldg 2, Floor 4
Description	Supports Server02
Contact	Network Svcs x100
Manufacturer	Liebert Corporation
Agent Model	IntelliSlot Web Card
Agent Part Number	OCWEBCARD
Agent App Firmware Version	2.300.0
Agent App Firmware Label	OCWEBCARD_HID3_2.300.0_035191
Agent Boot Firmware Version	2.300.0
Agent Boot Firmware Label	OCWEBCARD_HID3_2.300.0_034380
Agent Hardware ID	3
Agent Serial Number	416701G105T2004APR280074
Agent Manufacture Date	APR 28 2004
Agent Ethernet MAC Address	00-00-68-16-82-C1
Device Model	GXT2-700RT120
Device Firmware Version	GXT2MR10
Device Serial Number	0031300060AF011
Device Manufacture Date	08NOV00
Manufacturer support	Liebert.com

9.2 Events and Parameters

You may view a list of all supported events and parameters for the Liebert equipment through any interface. Depending on the Liebert IntelliSlot Web card, the list might include SNMP and Modbus.

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To view this data:

- Choose **IP Network Settings** from the Main Menu.
- Choose **Management Protocol**, then **SNMP Communications**.
- Choose **Support Information** from the SNMP Communications Menu to display the menu at right.

The menu displays:

- the number of events
 - the number of parameters
 - the total number of objects (sum of events and parameters)
- Choose **Display Events** to view a list of supported events for the Liebert unit, as shown in the example at right. These events may vary according to the Liebert unit where the card is installed.
- Choose **Display Parameters** to view a list of supported parameters for the Liebert unit, as in the example at right. These parameters vary according to the Liebert unit where the card is installed.

```
SNMP Communications Menu
-----
1: Authentication Traps 'no'
2: Display/Modify Communities
3: Display/Modify Trap
   Communities
4: Support Information
<ESC>: Cancel menu level
Please select a key ?>
```

```
Support Information Menu
-----
1: Display Events
2: Display Parameters
   Total Events: 40
   Total Parameters: 141
   Total Objects: 181
<ESC>: Cancel menu level
Please select a key ?>
```

```
Display Events (Example)
-----
AlarmOnBypass,1.3.6.1.2.1.33.
  1.6.3.9
IgpAgentDeviceCommunicationLost,
  1.3.6.1.4.1.476.1.42.2.3.0.1
Hit any key to continue...
```

```
Display Parameters (Example)
-----
sysDescr,1.3.6.1.2.1.1.1.0
sysObjectID,1.3.6.1.2.1.1.2.0
Hit any key to continue...
```

Web Interface



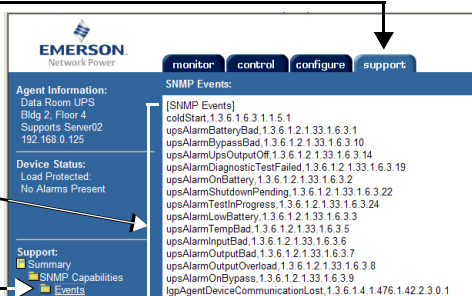
NOTE

For Liebert units with IS-WEBL cards (see **Table 1**), these features are available in the **Data/Logs** tab of the Web interface. For details, refer to **8.4.3 - Events and Parameters (Units with IS-WEBL, IS-IPBML, IS-WEBS, IS-IPBMS Cards Only)**.

To view events and parameters through the Web interface:

- Click on the **Support** tab, then **Events** (or **Parameters**) in the left panel. The events or parameters are listed in the right panel. The example below shows a list of Events.

Support tab →



The screenshot shows the EMERSON Network Power web interface. At the top, there are tabs for 'monitor', 'control', 'configure', and 'support'. The 'support' tab is selected. On the left side, there is a navigation menu with 'Support' expanded to show 'Events' and 'Parameters'. An arrow points from the 'Events' option to the right panel. The right panel displays a list of SNMP Events, including:

- [SNMP Events]
- coldStart,1.3.6.1.6.3.1.1.5.1
- upsAlarmBatteryBad,1.3.6.1.2.1.33.1.6.3.1
- upsAlarmBypassBad,1.3.6.1.2.1.33.1.6.3.10
- upsAlarmUpsOutputOff,1.3.6.1.2.1.33.1.6.3.14
- upsAlarmDiagnosticTestFailed,1.3.6.1.2.1.33.1.6.3.19
- upsAlarmOnBattery,1.3.6.1.2.1.33.1.6.3.2
- upsAlarmShutdownPending,1.3.6.1.2.1.33.1.6.3.22
- upsAlarmTestInProgress,1.3.6.1.2.1.33.1.6.3.24
- upsAlarmLowBattery,1.3.6.1.2.1.33.1.6.3.3
- upsAlarmTempBad,1.3.6.1.2.1.33.1.6.3.5
- upsAlarmInputBad,1.3.6.1.2.1.33.1.6.3.6
- upsAlarmOutputBad,1.3.6.1.2.1.33.1.6.3.7
- upsAlarmOutputOverload,1.3.6.1.2.1.33.1.6.3.8
- upsAlarmOnBypass,1.3.6.1.2.1.33.1.6.3.9
- IgpAgentDeviceCommunicationLost,1.3.6.1.4.1.476.1.42.2.3.0.1
- IgpConditionOutputToLoadOff,1.3.6.1.4.1.476.1.42.3.2.1.102

Annotations in the image include:

- 'Support tab' with an arrow pointing to the 'support' tab.
- 'Listing in right panel' with an arrow pointing to the list of events.
- 'Events (or Parameters)' with an arrow pointing to the 'Events' option in the left navigation menu.

10.0 BUILDING MANAGEMENT FUNCTIONS (IS-IPBML, IS-IPBMS AND IS-IPBMX CARDS ONLY)

This information in this section provides details on Modbus IP and BACnet IP functions that apply only to these cards:

- Liebert IntelliSlot Web Card-IPBML Modbus IP or BACnet IP (IS-IPBML)
- Liebert IntelliSlot Web Card-IPBMS Modbus IP (IS-IPBMS)

For other functions, see the appropriate section in this manual.

10.1 Monitoring Data



Web Interface

To view monitoring information through the Web interface:

- Click on the **Monitor** tab. The following example shows Device Model Number and Device Status.

Monitor tab

Item	Description
Device Model Number	BDSU Linker
Device Status	StartUp

10.2 Management Protocol Menu - Choose Modbus/TCP or BACnet/IP

The Management Protocol menu allows you to enable or disable Modbus/TCP or BACnet/IP and configure settings for that protocol. Consult your network administrator as needed for these settings.

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To activate Modbus/TCP or BACnet/IP:

1. Choose **IP Network Settings** from the Main Menu.
2. Choose **Management Protocol** from the IP Network Settings Menu.
3. Choose **Select Managed Protocol** from the Management Protocol Menu, then specify the protocol and refer to the following sections for more options:
 - **Modbus/TCP** to activate the Modbus TCP server (**10.3 - Modbus/TCP Configuration Menu**)
 - **BACnet/IP** to activate the BACnet IP server (**10.4 - BACnet/IP Server Menu**)

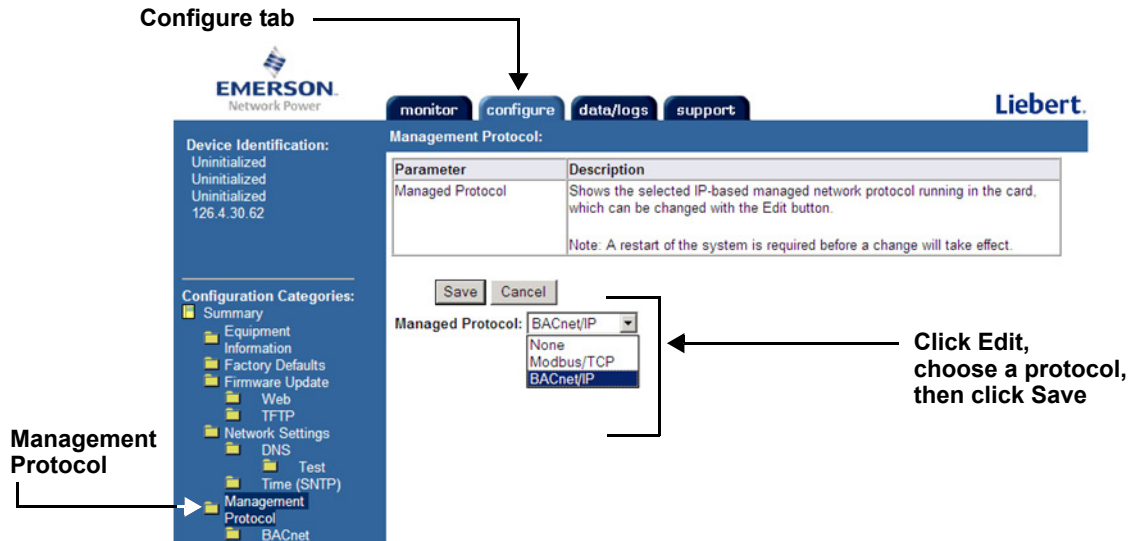
```
Management Protocol Menu
-----
1: Select Managed Protocol
<ESC>: Cancel menu level
Please select a key ?>
```

To deactivate a protocol that has been enabled, choose Modbus/TCP or BACnet/IP from the Management Protocol Menu, then choose **Disabled**.

Web Interface

To activate or deactivate Modbus/TCP or BACnet/IP through the Web interface:

- Click on the **Configure** tab, **Management Protocol** in the left panel, then **Edit** at right.
- Choose a protocol from the Managed Protocol drop-down list—**Modbus/TCP** or **BACnet/IP**—to activate (or choose **None** to deactivate). After making changes, click **Save**.



Configure tab

Management Protocol

Parameter	Description
Managed Protocol	Shows the selected IP-based managed network protocol running in the card, which can be changed with the Edit button. Note: A restart of the system is required before a change will take effect.

Save Cancel

Managed Protocol: BACnet/IP

None
Modbus/TCP
BACnet/IP

Click Edit, choose a protocol, then click Save

10.3 Modbus/TCP Configuration Menu

Once Modbus/TCP is activated (as described in **Section 10.2**), the Management Protocol menu displays Modbus/TCP as enabled and provides access to the Modbus/TCP Configuration menu.

The Modbus/TCP Configuration menu allows you to specify Modbus/TCP protocol settings for the Web card.

```
Management Protocol Menu
-----
1: Modbus/TCP          enabled
2: Modbus/TCP Configuration
<ESC>: Cancel menu level
Please select a key ?>
```

```
Modbus/TCP Configuration Menu
-----
1: Modbus/TCP Port      502
2: Modbus Write Access  Enabled
3: Modbus/TCP Security Mode Open
4: Supported Data List  9539
<ESC>: Cancel menu level
Please select a key ?>
```

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To access the Modbus/TCP Configuration Menu:

1. Choose **IP Network Settings** from the Main Menu.
2. Choose **Management Protocol** from the IP Network Settings Menu.
3. Choose **Modbus/TCP Configuration**.
4. Choose an option from the Modbus/TCP Configuration menu:

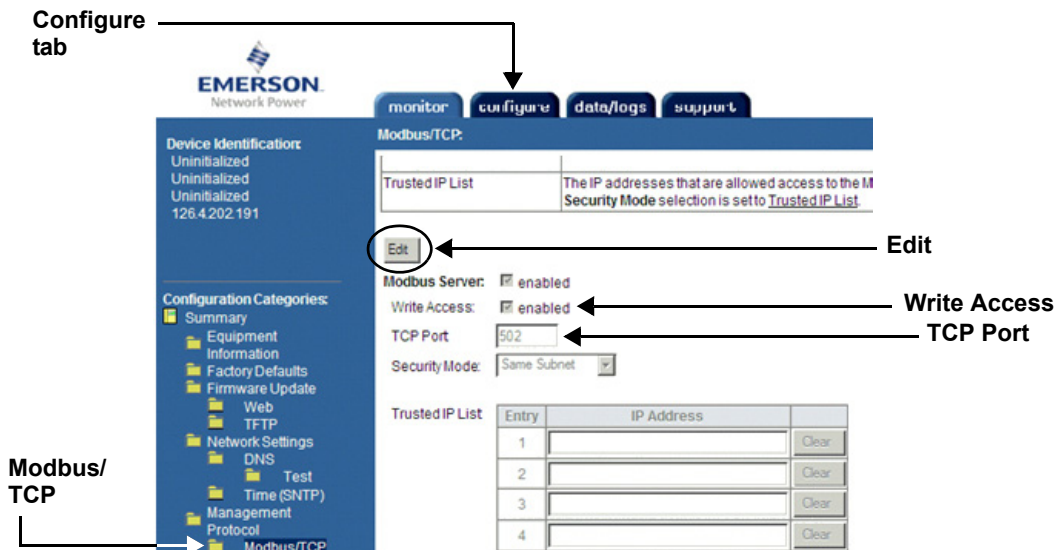
Table 29 Modbus/TCP Configuration Menu options

Feature	Description
Modbus/TCP Port	The TCP port used by the Modbus server to listen for Modbus protocol requests and respond to those requests based on the Security Mode setting. The default port is 502.
Modbus Write Access	Allows write operations to be performed via the Modbus protocol if enabled (or prevents write operations if disabled). Note: This feature has no effect on write operations that may be available from other system interfaces.
Modbus/TCP Security Mode	For detailed instructions, see 10.3.1 - Select Modbus/TCP Security Mode Menu .
Supported Data List	For detailed instructions, see 10.3.2 - Supported Data List - Modbus/IP .

Web Interface

To configure Modbus/TCP through the Web interface:

- Click on the **Configure** tab, then **Modbus/TCP** in the left panel under **Management Protocol** and finally **Edit** at right. After making changes, click **Save**.



10.3.1 Select Modbus/TCP Security Mode Menu

The Select Modbus/TCP Security Mode menu is used to restrict or allow Modbus access to the Web card.

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

1. Choose **IP Network Settings** from the Main Menu.
2. Choose **Management Protocol** from the IP Network Settings Menu, then **Modbus/TCP Configuration**.
3. Choose **Modbus/TCP Security Mode** from the Modbus/TCP Configuration menu.
4. Choose the security mode you wish to use from the Select Modbus/TCP Security Mode menu:
 - **Open** - allows any IP address to access the card Web page.
 - **Same Subnet** - allows any IP on the same Subnet as the card to access the card Web page.
 - **Trusted IPs** - allows a maximum of four IP addresses to access the card Web page.
5. If the Trusted IP option is selected, you may specify up to four IP addresses for access to the card Web page. To do this:
 - a. Choose **Modbus/TCP Trusted IP list** from the Modbus/TCP Configuration menu.
 - b. To add an address, enter **a** followed by a space and the IP address, then press Enter. For example:
a 126.4.230.111

Each entry will be numbered—either **1** or **2**, as shown at right. To make changes:

- To remove an address, enter **d** followed by a space and the number of the entry (**1** or **2**), then press Enter. For example:
d 2
- To edit an address, enter **e** followed by a space, the number of the entry (**1** or **2**), a space and the IP address, then press Enter. For example:
e 1 126.4.230.111

```
Management Protocol Menu
-----
1: Modbus/TCP          enabled
2: Modbus/TCP Configuration
<ESC>: Cancel menu level
Please select a key ?>
```

```
Modbus/TCP Configuration Menu
-----
1: Modbus/TCP Port          502
2: Modbus Write Access     Enabled
3: Modbus/TCP Security Mode Open
4: Supported Data List     9539
<ESC>: Cancel menu level
Please select a key ?>
```

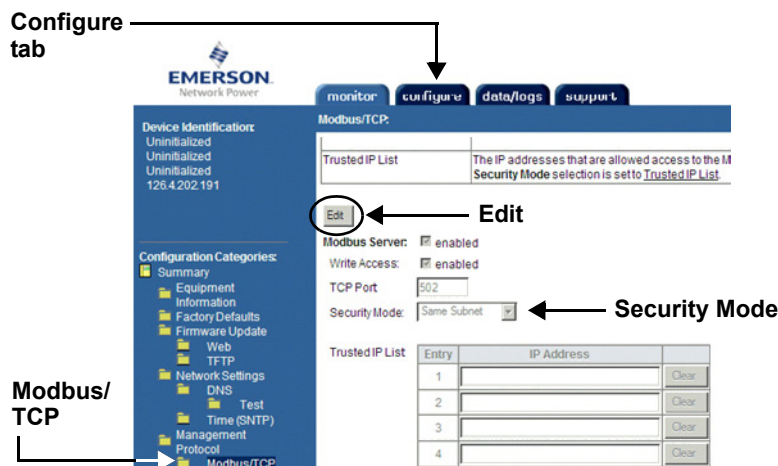
```
Select Modbus/TCP Security Mode
1. Open
2. Same Subnet
3. Trusted IPs
Select A Mode: ?>
```

```
Modbus/TCP Configuration Menu
-----
1: Modbus/TCP Port          502
2: Modbus Write Access     Enabled
3: Modbus/TCP Security Mode Trusted List
4: Supported Data List     9539
5: Modbus/TCP Trusted IP list 2
<ESC>: Cancel menu level
Please select a key ?> 5
1: 126.4.100.1
2: 126.4.100.2
3: 126.4.100.3
4: 126.4.100.4
<a>dd      <a xxx.xxx.xxx.xxx>
<d>delete <d n> or
<e>dit    <e n xxx.xxx.xxx.xxx>
```

Web Interface

To specify the Modbus/TCP security mode through the Web interface:

- Click on the **Configure** tab, then **Modbus/TCP** in the left panel and finally **Edit** at right. If you select **Trusted IP** as the Security Mode option, you may specify up to four IP addresses; click the **Clear** button to delete any entry. After making changes, click **Save**.



10.3.2 Supported Data List - Modbus/IP

The Supported Data List displays a listing of device data that may be accessed via the Modbus/IP protocol.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

1. Choose **IP Network Settings** from the Main Menu.
2. Choose **Management Protocol** from the IP Network Settings Menu, then **Modbus/TCP Configuration**.
3. Choose **Supported Data List**.
4. The listing displays the following details:

```

Modbus/TCP Configuration Menu
-----
1: Modbus/TCP Port           502
2: Modbus Write Access       Enabled
3: Modbus/TCP Security Mode  Same Subnet
4: Supported Data List     10404
<ESC>: Cancel menu level
Please select a key ?>
    
```

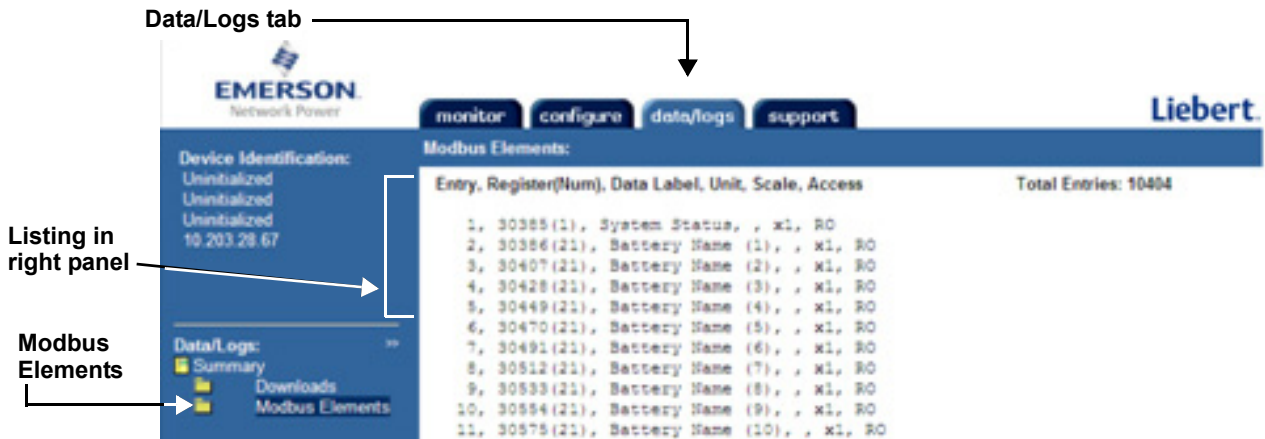
Entry	Register(Num)	Data Label	Unit	Scale	Access
1	30385(1)	System Status		x1	RO
2	30386(21)	Battery Name (1)		x1	RO
3	30407(21)	Battery Name (2)		x1	RO
4	30428(21)	Battery Name (3)		x1	RO
5	30449(21)	Battery Name (4)		x1	RO
6	30470(21)	Battery Name (5)		x1	RO
7	30491(21)	Battery Name (6)		x1	RO
8	30512(21)	Battery Name (7)		x1	RO
9	30533(21)	Battery Name (8)		x1	RO
10	30554(21)	Battery Name (9)		x1	RO
11	30575(21)	Battery Name (10)		x1	RO

- **Entry** - automatically assigned sequential identification numbers for data points (1, 2, 3, etc.).
- **Register(Num)** - the Modbus input or holding register and number from 1 to 127—for example, 30385(1)
- **Data Label** - user-assigned data point name—e.g., *System Status* or *Battery Name (1)*
- **Unit** - measurement units for the data point—*deg F*, *deg C*, *% RH*
- **Scale** - number to use as multiplier for the Modbus value—*x10* = multiply by 10
- **Access** - Read Only (RO) or Write Only (WO)

Web Interface

To view the same Supported Data List information through the Web interface:

- Click on the **Data/Logs** tab at the top of the window, then **Modbus Elements** in the left panel. The data appears in the right panel.



10.4 BACnet/IP Server Menu

Once BACnet/IP is activated (as described in **Section 10.2**), the Management Protocol menu displays BACnet/IP as enabled and provides access to the BACnet/IP Configuration menu.

The BACnet/IP Server menu allows you to specify BACnet/IP protocol settings for the Web card.

```
Management Protocol Menu
-----
1: Select Managed Protocol  BACnet/IP
2: BACnet/IP Server
<ESC>: Cancel menu level
Please select a key ?>
```

Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To access the BACnet/IP Server Menu:

1. Choose **IP Network Settings** from the Main Menu.
2. Choose **Management Protocol** from the IP Network Settings Menu.
3. Choose **BACnet/IP Server**.
4. Choose an option from the BACnet/IP Server menu:

```
BACnet/IP Server Menu
-----
1: BACnet Write Access      Enabled
2: Device Instance Number  1130000
3: Device Object Name      Device1130000
4: APDU timeout            3000
5: APDU Retries            3
6: Supported Data List     Initializing
<ESC>: Cancel menu level
Please select a key ?>
```

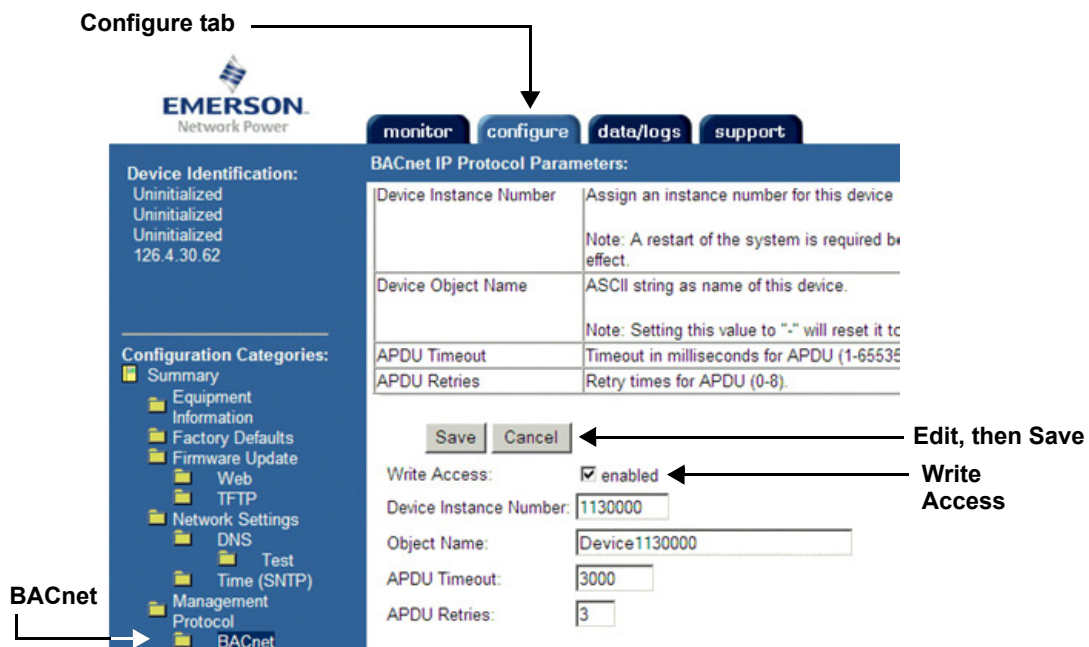
Table 30 BACnet/IP Server Menu options

Feature	Description
BACnet Write Access	Allows the BACnet server to write to the managed device. Note: Checking this feature enables or disables write operations by the BACnet interface only. Write operations may still be available from other system interfaces.
Device Instance Number	Assign an instance number for this device object (0-4194303). Note: A restart of the system is required before a change to this value will take effect.
Device Object Name	ASCII string as name of this device (32 characters maximum). Note: Setting this value to "-" will reset it to the factory default name.
APDU Timeout	Timeout in milliseconds for APDU (1-65535 ms).
APDU Retries	Retry times for APDU (0-8).
Supported Data List	For detailed instructions, see 10.4.1 - Supported Data List - BACnet/IP .

Web Interface

To configure BACnet/IP through the Web interface:

- Click on the **Configure** tab, then **BACnet** in the left panel under **Management Protocol** and finally **Edit** at right. After making changes, click **Save**.



Configure tab

EMERSON Network Power

monitor | **configure** | data/logs | support

Device Identification:
Uninitialized
Uninitialized
Uninitialized
126.4.30.62

Configuration Categories:
 Summary
 Equipment Information
 Factory Defaults
 Firmware Update
 Web
 TFTP
 Network Settings
 DNS
 Test
 Time (SNTP)
 Management Protocol
BACnet

BACnet

BACnet IP Protocol Parameters:

Device Instance Number	Assign an instance number for this device Note: A restart of the system is required before a change to this value will take effect.
Device Object Name	ASCII string as name of this device. Note: Setting this value to "-" will reset it to the factory default name.
APDU Timeout	Timeout in milliseconds for APDU (1-65535 ms).
APDU Retries	Retry times for APDU (0-8).

Save | Cancel

Write Access: enabled **Write Access**

Device Instance Number: 1130000

Object Name: Device1130000

APDU Timeout: 3000

APDU Retries: 3

Edit, then Save

10.4.1 Supported Data List - BACnet/IP

The Supported Data List displays a listing of device data that may be accessed via the BACnet/IP protocol.



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

1. Choose **IP Network Settings** from the Main Menu.
2. Choose **Management Protocol** from the IP Network Settings Menu, then choose **BACnet/IP Server**.
3. Choose **Supported Data List**.
4. The listing displays the following details:
 - **Entry** - automatically assigned sequential identification numbers for data points (1, 2, 3, etc.).
 - **Object ID** - the Object ID of the value being read from the equipment—for example, *AV-1*.
 - **Object Name** - the Object Name of the value being read from the equipment—e.g., *4097_1*.
 - **Description** - the text description of the value being read from the equipment—e.g., *System Input RMS A-B (Input)*.

```

BACnet/IP Server Menu
-----
1: BACnet Write Access      Enabled
2: Device Instance Number  1130000
3: Device Object Name      Device1130000
4: APDU timeout            3000
5: APDU Retries            3
6: Supported Data List     97

<ESC>: Cancel menu level
Please select a key ?>6
    
```

```

Entry, Object Id, Object Name, Description
1, AV-1, 4097_1, System Input RMS A-B (Input)
2, AV-2, 4099_1, System Input RMS B-C (Input)
3, AV-3, 4101_1, System Input RMS C-A (Input)
4, AV-4, 4113_1, System Input RMS Current Phase A (Input)
5, AV-5, 4114_1, System Input RMS Current Phase B (Input)
6, AV-6, 4115_1, System Input RMS Current Phase C (Input)
7, AV-7, 4105_1, System Input Frequency (Input)
8, AV-8, 4096_1, System Input RMS A-N (Input)
9, AV-9, 4098_1, System Input RMS B-N (Input)
10, AV-10, 4100_1, System Input RMS C-N (Input)
11, AV-11, 4116_1, System Input Power Factor Phs A (Input)
12, AV-12, 4117_1, System Input Power Factor Phs B (Input)
13, AV-13, 4118_1, System Input Power Factor Phs C (Input)
14, AV-24, 4128_1, Bypass Input Voltage RMS A-N (Bypass)
15, AV-25, 4129_1, Bypass Input Voltage RMS B-N (Bypass)
16, AV-26, 4130_1, Bypass Input Voltage RMS C-N (Bypass)
17, AV-27, 4131_1, Bypass Input Frequency (Bypass)
    
```

Web Interface

To view the same Supported Data List information through the Web interface:

- Click on the **Data/Logs** tab at the top of the window, then **BACnet Elements** in the left panel. The data appears in the right panel.

The screenshot shows the web interface for Emerson Network Power. At the top, there are navigation tabs: 'monitor', 'configure', 'data/logs', and 'support'. The 'data/logs' tab is selected. On the left side, there is a sidebar with 'Data/Logs' expanded to show 'BACnet Elements'. The main content area displays 'BACnet Elements' with a total of 97 elements. Below this, a table lists the elements with columns for Index, Object Id, Object Name, and Description. The table content is as follows:

Index	Object Id	Object Name	Description
1	AV-1, 4097_1	System Input RMS A-B	(Input)
2	AV-2, 4099_1	System Input RMS B-C	(Input)
3	AV-3, 4101_1	System Input RMS C-A	(Input)
4	AV-4, 4113_1	System Input RMS Current Phase A	(Input)
5	AV-5, 4114_1	System Input RMS Current Phase B	(Input)
6	AV-6, 4115_1	System Input RMS Current Phase C	(Input)
7	AV-7, 4105_1	System Input Frequency	(Input)
8	AV-8, 4096_1	System Input RMS A-N	(Input)
9	AV-9, 4098_1	System Input RMS B-N	(Input)
10	AV-10, 4100_1	System Input RMS C-N	(Input)
11	AV-11, 4116_1	System Input Power Factor Phs A	(Input)
12	AV-12, 4117_1	System Input Power Factor Phs B	(Input)
13	AV-13, 4118_1	System Input Power Factor Phs C	(Input)
14	AV-24, 4128_1	Bypass Input Voltage RMS A-N	(Bypass)
15	AV-25, 4129_1	Bypass Input Voltage RMS B-N	(Bypass)
16	AV-26, 4130_1	Bypass Input Voltage RMS C-N	(Bypass)
17	AV-27, 4131_1	Bypass Input Frequency	(Bypass)
18	AV-38, 4150_1	Battery Time Remaining	(Battery)
19	AV-39, 4155_1	Battery Volts for Cabinet	(Battery)
20	AV-40, 4156_1	Battery Temperature for Cabinet	(Battery)
21	AV-41, 4291_1	Inlet Air Temperature	(Battery)
22	AV-42, 4149_1	DC Bus Current	(Battery)
23	AV-53, 4385_1	System Output Voltage RMS A-N	(Output)
24	AV-54, 4386_1	System Output Voltage RMS B-N	(Output)
25	AV-55, 4387_1	System Output Voltage RMS C-N	(Output)

APPENDIX A - FIRMWARE UPDATES

A.1 INTRODUCTION

Liebert IntelliSlot cards may be updated to take advantage of the latest release of the firmware with enhanced features, compatibility with new units or service patches. Upgraded firmware may be downloaded with a browser, such as Internet Explorer. Emerson® maintains firmware upgrades on its Web site, www.liebert.com

Emerson manufactures various types of network cards for Liebert products. Before beginning any upgrade, determine the type of Liebert IntelliSlot card to be upgraded.

This identifying information—the type of card and firmware version currently installed—may be found in the documentation shipped with the card or by reading the card's support information through a terminal emulation, Telnet or Web interface, as described in **A.3.2 - Determine the Liebert IntelliSlot Card Type and Firmware Version**.



NOTE

Emerson recommends that users read all the instructions prior to attempting a firmware upgrade.

A.1.1 Overview

The firmware upgrade involves these steps:

Table A1 Overview of the upgrade process

Step	For details, see:
1. Decide which interface to use to connect to the Liebert IntelliSlot card	A.2 - Connect to the Card - Terminal Emulation, Telnet or Web Interface
2. Prepare for the upgrade	
<ul style="list-style-type: none"> • Make sure you have everything needed to perform the upgrade 	A.3.1 - Requirements to Update the Liebert IntelliSlot Card's Firmware
<ul style="list-style-type: none"> • Check the type of card and firmware version currently installed 	A.3.2 - Determine the Liebert IntelliSlot Card Type and Firmware Version
<ul style="list-style-type: none"> • Download the upgrade file from the Liebert Web site 	A.3.3 - Download the Firmware Upgrade File to the Computer
<ul style="list-style-type: none"> • Decide which method to use for the upgrade 	A.3.4 - Choose a Method to Install the Firmware Upgrade
3. Follow the step-by-step instructions to upgrade the firmware with the chosen method:	
<ul style="list-style-type: none"> • HTTP (Web) Method 	A.4 - Updating the Firmware - HTTP (Web) Method
<ul style="list-style-type: none"> • TFTP (HyperTerminal, Telnet, Web) Method 	A.5 - Updating the Firmware - TFTP (HyperTerminal, Telnet, Web) Method
<ul style="list-style-type: none"> • Xmodem (Serial) Method 	A.6 - Updating the Firmware - Xmodem (Serial) Method

A.1.2 Estimated Time to Download the Firmware Upgrade File

The amount of time required to download the firmware upgrade file depends on the upgrade method used. Refer to **Table A2** for estimated times for each method.

Table A2 Estimated Time for downloads

Upgrade Method	Expected Speed
HTTP (Web) Method (.bin file)	6-7 minutes (subject to network traffic)
TFTP (HyperTerminal, Telnet, Web) Method (.bin file)	5-6 minutes (subject to network traffic)
Xmodem (Serial) Method Xmodem 1K 115,200 bps	1st file 2 minutes
	2nd file 2 minutes
	3rd file 3-5 minutes

A.2 CONNECT TO THE CARD - TERMINAL EMULATION, TELNET OR WEB INTERFACE

Upgrading the firmware requires connecting to the card with one of these interfaces.

A.2.1 Open the Terminal Emulation Interface - Serial Connection

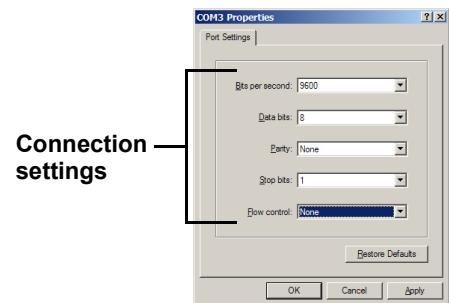
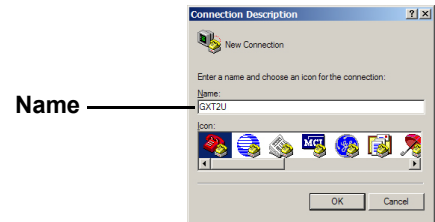
To connect to the card using terminal emulation software with a serial connection to the Web card:

1. Open a terminal emulation application, such as HyperTerminal.
To do this:
 - Click the **Start** button, then **Programs, Accessories, Communications** and finally **HyperTerminal**.
2. In the Connection Description window, enter a name for the connection—for example, **GXT2U**—then click **OK**.
3. In the Connect To window:
 - Choose **COM3** from the Connect Using drop-down list.
 - Click **OK**.
4. In the COM3 Properties window, enter the communication settings shown in **Table A3**.

Table A3 Communication settings

Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None

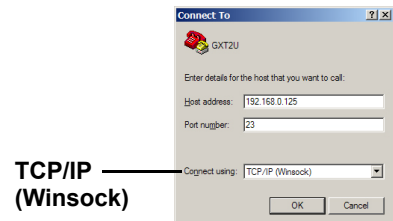
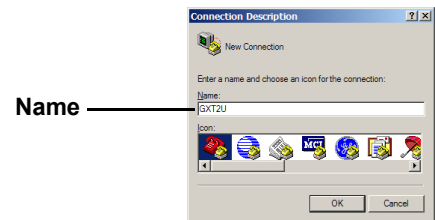
5. When the message at right appears in the HyperTerminal window, press the Enter key.



A.2.2 Open the Terminal Emulation Interface - TCP/IP Connection

To connect to the card using terminal emulation software with an Ethernet connection to the Web card:

1. Open a terminal emulation application, such as HyperTerminal.
To do this:
 - Click the **Start** button, then **Programs, Accessories, Communications** and finally **HyperTerminal**.
2. In the Connection Description window, enter a name for the connection—for example, **GXT2U**—then click **OK**.
3. In the Connect To window:
 - Choose **TCP/IP (Winsock)** from the Connect Using drop-down list.
 - Enter the IP address of the Web card—for example, **192.168.0.125**—in the Host Address box, then click **OK**.
4. When the message at right appears in the HyperTerminal window, press the Enter key.
5. Enter the Administrator username and password (both are case-sensitive):
 - a. **Login** (username—default is *Liebert*)
 - b. **Password** (default is *Liebert*)



```
RTCS v2.96.00 Telnet server
Service Port Manager Active
<Esc> Ends Session
```

```
Login: Liebert
Password: *****
```

A.2.3 Open the Telnet Interface

To connect to the card using Telnet:

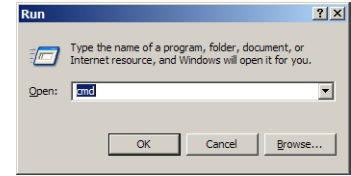
1. Open a Telnet connection on a computer with an Ethernet connection to the Liebert unit.

To do this:

- Open a command prompt window—click the **Start** button, then **Run**.
- Enter **cmd** and click **OK**.
- In the command prompt window that opens, enter **telnet** followed by a space and the IP address of the Web card—for example:

telnet 192.168.0.125

2. When the message at right appears in the command prompt window, press the Enter key.
3. Enter the Administrator username and password (both are case-sensitive):
 - a. **Login** (username—default is *Liebert*)
 - b. **Password** (default is *Liebert*)



```
C:>telnet 192.168.0.125
```

```
RTCS v2.96.00 Telnet server
Service Port Manager Active
<ESC> Ends Session
```

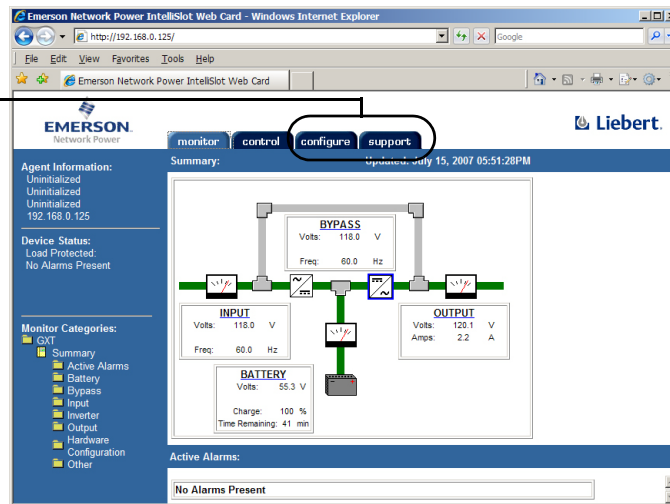
```
Login: Liebert
Password: *****
```

A.2.4 Open the Web Interface

To connect to the card using the Web interface:

1. Open a Web browser such as Internet Explorer.
2. Enter the IP address of the Web card in the address bar—e.g., **192.168.0.125**.
3. Click on a tab at the top of the window.

Configure and Support Tabs



A.3 PREPARING TO UPDATE LIEBERT INTELLISLOT FIRMWARE

A.3.1 Requirements to Update the Liebert IntelliSlot Card's Firmware

Make sure you have the following before starting the update:

- Firmware upgrade downloaded from the Liebert Web site (see **A.3.3 - Download the Firmware Upgrade File to the Computer**)
- A computer running Internet Explorer 5.5 or newer
- A Liebert IntelliSlot card
- A connection to the Liebert IntelliSlot card
 - Null modem cable—serial upgrade method
 - Ethernet connection—TFTP or HTTP upgrade method
- An Internet connection

A.3.2 Determine the Liebert IntelliSlot Card Type and Firmware Version

Each type of Liebert IntelliSlot card uses different firmware. Attempting to upgrade a card with the firmware for another type of card will fail and may damage the card.

To determine the type of card in your Liebert equipment:



Terminal Emulation (Serial or TCP/IP Connection) / Telnet

To view Web card information using terminal emulation or Telnet:

1. Open a connection to the Liebert IntelliSlot card (if needed, see instructions in **A.2.1 - Open the Terminal Emulation Interface - Serial Connection**, **A.2.2 - Open the Terminal Emulation Interface - TCP/IP Connection** or **A.2.3 - Open the Telnet Interface**).
2. Choose **Factory Settings** from the Main Menu, then choose **Agent Card Information**.
3. The Liebert IntelliSlot card model, part number and firmware version appear in the following example. Press the Enter key to return to the previous menu

```

Factory Settings Menu
-----
1: Reset to Factory Defaults
2: Agent Card Information
<ESC>: Cancel menu level
Please select a key ?>
    
```

```

MAC Address      00-00-68-16-82-C1
Network Card Model IntelliSlot Web Card
Network Card Part # OCWEBCARD
Manufacture Date APR 28, 2004
Serial Number    416701G105T2004APR280074
Boot Version     2.300.0
Boot Label      OCWEBCARD_HID3_2.300.0_034380
App Version      2.300.0
App Label       OCWEBCARD_HID3_2.300.0_035191
Hardware Version 3
CPU Speed        50 MHz
Flash Usage      4327 out of 8388 KByte
Hit Enter to Exit
    
```

Model and Part Number (points to Network Card Model and Network Card Part #)

Firmware Version (points to App Version)

Web Interface

To view Web card information using a Web browser:

1. Open a connection to the Liebert IntelliSlot card (if needed, see instructions in **A.2.4 - Open the Web Interface**).
2. Click on the **Support** tab, then **Summary** in the left panel. The Liebert IntelliSlot card model, part number and firmware version appear in the right panel.

Support tab

Summary

Item	Value
System Name	Data Room UPS
Location	Bldg 2, Floor 4
Description	Supports Server02
Contact	Network Svcs x100
Manufacturer	Liebert Corporation
Agent Model	IntelliSlot Web Card
Agent Part Number	OCWEBCARD
Agent App Firmware Version	2.300.0
Agent App Firmware Label	OCWEBCARD_HID3_2.300.0_035191
Agent Boot Firmware Version	2.300.0
Agent Boot Firmware Label	OCWEBCARD_HID3_2.300.0_034380
Agent Hardware ID	3

Model, Part Number and Firmware Version (points to Agent Model, Agent Part Number, and Agent App Firmware Version)

A.3.3 Download the Firmware Upgrade File to the Computer



NOTE

Turn off the power management on your PC or laptop before beginning the update to ensure that communication will not be disrupted during the process.

To download the upgrade file:

1. Open a Web browser, such as Internet Explorer (5.5 or newer).
2. Navigate to the Liebert Web site, www.liebert.com
3. Choose the firmware upgrade for your card from the selections on the Web page (see **A.3.2 - Determine the Liebert IntelliSlot Card Type and Firmware Version**).
4. Click on the link to download the file.
5. Save the file to your computer's hard drive.
Be sure to make a note of the location where the file is saved.

A.3.4 Choose a Method to Install the Firmware Upgrade

To install the firmware upgrade, choose one of these three methods and refer to the associated step-by-step directions:

- HTTP (Web) - see **A.4 - Updating the Firmware - HTTP (Web) Method**
- TFTP - see **A.5 - Updating the Firmware - TFTP (HyperTerminal, Telnet, Web) Method**
- Xmodem (Serial) - see **A.6 - Updating the Firmware - Xmodem (Serial) Method**

A.4 UPDATING THE FIRMWARE - HTTP (WEB) METHOD

Follow these steps to install the firmware upgrade using the HTTP (Web) method. This method is available through the Web interface only and requires an Ethernet connection to the Web card.

A.4.1 Install the Firmware Upgrade

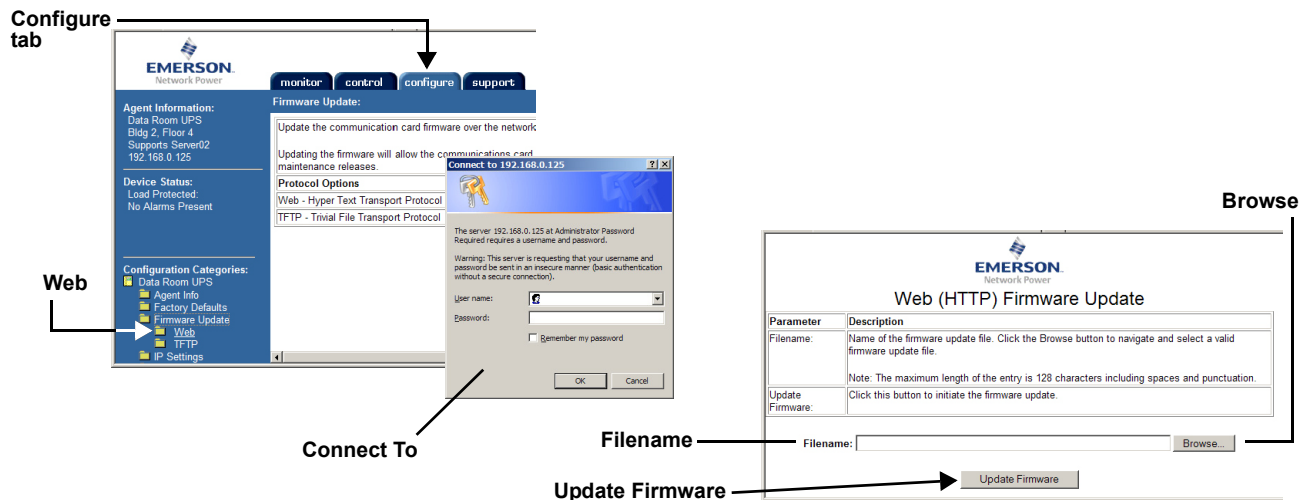


NOTE

Turn off the power management on your PC or laptop before beginning the update to ensure that communication will not be disrupted during the process.

To update the Liebert IntelliSlot card firmware using the HTTP (Web) method:

1. Open a connection to the Liebert IntelliSlot card (if needed, see instructions in **A.2.4 - Open the Web Interface**).
2. Click on the **Configure** tab, then click on **Web** (under Firmware Update) in the left panel. The Connect To box opens for you to enter the username and password.
3. Enter the Administrator username and password (both case-sensitive):
 - a. **User Name** (default is *Liebert*)
 - b. **Password** (default is *Liebert*)
4. Click **OK**. The Web (HTTP) Firmware Update window opens, as shown at right below.



5. Click on the **Browse** button to locate the upgrade file. This is the file with the extension “.bin” downloaded in **A.3.3 - Download the Firmware Upgrade File to the Computer**. Then click **Open** to return to the update screen.
6. When ready to begin the update, click the **Update Firmware** button.
A screen will appear, showing the firmware update progress.



NOTE

Do not refresh your browser or open another browser window. Wait until the firmware update has been completed before opening other applications or using the computer for other tasks.

7. A message appears indicating whether the update was successful.

After the firmware update is completed, the card will reinitialize and you may return to the Liebert IntelliSlot card’s Web interface.

Check the new firmware version if you wish (see **A.3.2 - Determine the Liebert IntelliSlot Card Type and Firmware Version**).

A.5 UPDATING THE FIRMWARE - TFTP (HYPERTERMINAL, TELNET, WEB) METHOD

Follow these steps to update the firmware using the TFTP method. This method is available through the terminal emulation, Telnet and Web interfaces with an Ethernet connection to the Web card.



NOTE

This method includes a time-sensitive operation requiring expeditious location of the upgrade files downloaded in A.3.3 - Download the Firmware Upgrade File to the Computer.

Read through this entire section before beginning the upgrade.

A.5.1 TFTP Method - Terminal Emulation / Telnet Interface

To update the Liebert IntelliSlot card firmware using the TFTP method with a terminal emulation or Telnet interface:

Open a Connection to the Card

1. Open a terminal emulation or Telnet connection to the Liebert IntelliSlot card (if needed, see instructions in A.2.2 - Open the Terminal Emulation Interface - TCP/IP Connection or A.2.3 - Open the Telnet Interface).
2. Choose **Firmware Updates** from the Main Menu.
3. Choose **TFTP Update** from the Firmware Updates menu, shown at right.

```
Firmware Updates Menu
-----
1: TFTP Update
```

Specify TFTP Server and Upgrade Filename

4. The TFTP Update Menu, shown at right, displays the TFTP server's IP address and listening port, along with the name of the firmware update file.
5. Select options as needed and refer to the following guide to change any settings.

```
TFTP Update Menu
-----
1: IP Address  0.0.0.0
2: Port       69
3: Filename   Uninitialized
4: Initiate TFTP Firmware Update

<ESC>: Cancel menu level
Please select a key ?>
```

Table A4 Firmware update settings - TFTP

Parameter	Description
Server	The IP address of the TFTP server—for example, 192.168.0.125 .
Port	Port that the TFTP server is using, typically 69 .
Filename	Name of the firmware update file—128 characters maximum, including spaces and punctuation. This is the file with the extension “.bin” downloaded in A.3.3 - Download the Firmware Upgrade File to the Computer .

6. After making changes, press the Escape key twice to return to the Main Menu.
7. Choose **Exit and Save** to save your changes and reboot the card.

Reconnect to the Card

8. Connect to the Liebert IntelliSlot card again (if needed, see A.2.3 - Open the Telnet Interface or A.2.1 - Open the Terminal Emulation Interface - Serial Connection).
9. Choose **Firmware Updates** from the Main Menu.
10. Choose **TFTP Update** from the Firmware Updates menu, shown at right.

```
Firmware Updates Menu
-----
1: TFTP Update
```

Begin the Upgrade Process

11. When ready to begin the update, choose **Initiate TFTP Firmware Update**.
12. Open the TFTP application and start TFTP. Ensure that all settings are ready to transfer the file, including the location of the upgrade file. Refer to your TFTP user manual for more details.
13. Return to the terminal emulation/Telnet screen. At the confirmation message prompt, enter **y** (yes) to confirm your choice. (To cancel, enter **n** for no.)
14. A message appears, as shown at right, showing the progress by percent complete.
15. When the progress screen shows 100% complete, the card will be rebooted. Press Enter when this is finished.
16. Press the Escape key to return to the Main Menu, then choose **Exit and Save**.

The upgrade is now complete.

Check the new firmware version if you wish (see **A.3.2 - Determine the Liebert IntelliSlot Card Type and Firmware Version**).

```
TFTP Update Menu
-----
1: IP Address 192.168.0.125
2: Port      69
3: Filename  OCWEBCARD_HID3_2.300.0_035780_AppFwUpdt.bin
4: Initiate TFTP Firmware Update

<ESC>: Cancel menu level
Please select a key ?>
```

```
All Code In Flash Will Be Rewritten, Confirm? [y/n]
```

```
TFTP Update initiated

The firmware on this card is currently being updated.
This operation may take 6 or more minutes depending
on network traffic and other factors. The card will be
rebooted upon successful completion of the process OR
control will be returned to this terminal session upon
failure so another firmware update attempt can be made.

Firmware update in process... Percent Complete(0%)
```

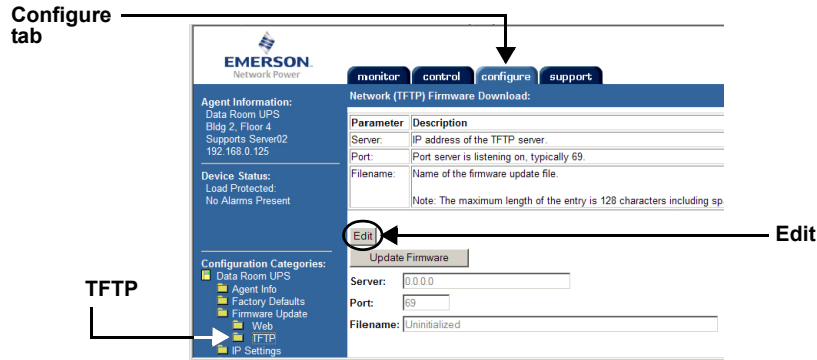
```
Main Menu
-----
1: System Information
2: IP Network Settings
3: Messaging
4: Factory Settings
5: Firmware Updates
q: Quit and abort changes
x: Exit and save
Please select a key ?>
```


A.5.2 TFTP Method - Web Interface

To update the Liebert IntelliSlot card firmware using the TFTP method with a Web interface:

Open a Connection to the Card

1. Open a connection to the Liebert IntelliSlot card (if needed, see instructions in **A.2.4 - Open the Web Interface**).
2. Click on the **Configure** tab, then **TFTP** in the left panel.



3. Enter the Administrator username and password (both are case-sensitive):
 - a. **Login** (username—default is *Liebert*)
 - b. **Password** (default is *Liebert*)

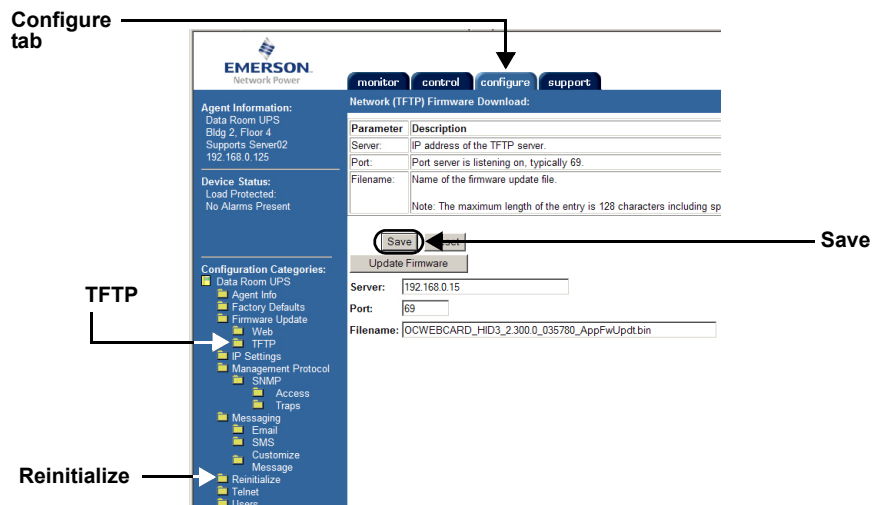
Specify TFTP Server and Upgrade Filename

4. Click the **Edit** button in the right panel.
5. Select options as needed and refer to the following guide to change any settings.

Table A5 Firmware update settings - Web

Parameter	Description
Server	The IP address of the TFTP server—for example, 192.168.0.125 .
Port	Port that the TFTP server is using, typically 69 .
Filename	Name of the firmware update file—128 characters maximum, including spaces and punctuation. This is the file with the extension “.bin” downloaded in A.3.3 - Download the Firmware Upgrade File to the Computer .

6. After making changes, click **Save**, then click **Reinitialize** in the left panel to reboot the card.

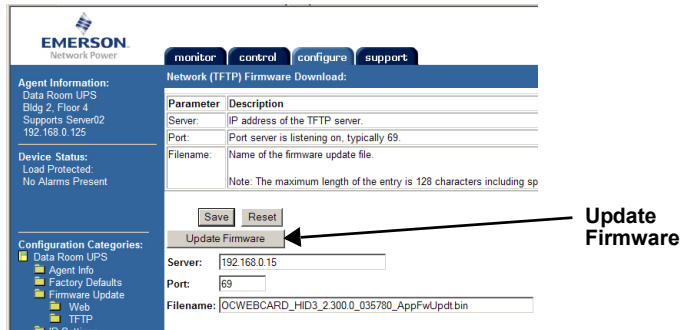


Reconnect to the Card

7. Click the **Configure** tab, then **TFTP** and enter the username and password (**Steps 2 and 3**) to return to the TFTP screen as shown above.

Begin the Upgrade Process

8. Open the TFTP application and start TFTP. Ensure that all settings are ready to transfer the file, including the location of the upgrade file. Refer to your TFTP user manual for more details.
9. Return to the Web interface.
10. When ready to begin the download, click the **Update Firmware** button.



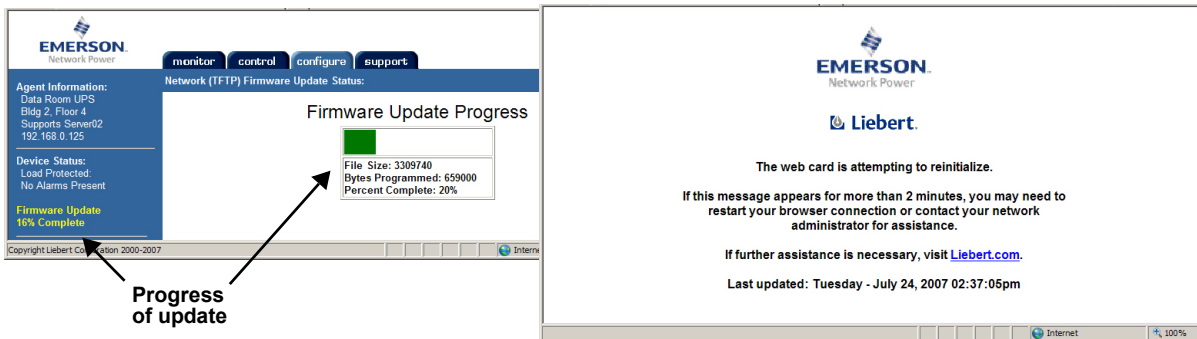
11. During the update, the window displays a progress bar, as shown below left.



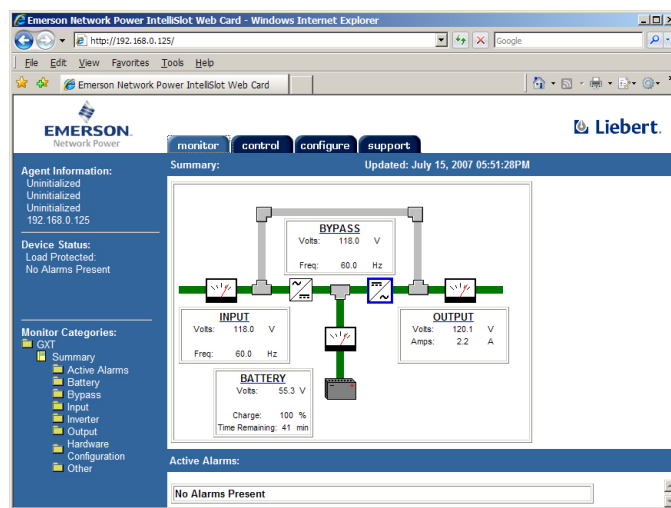
NOTE

Do not close the Web browser during this process or the update will abort.

After the firmware update is completed, the card will reinitialize automatically. A reboot message, as shown below right, remains until the rebooting is finished.



When the rebooting is complete, the Web browser window returns to the default opening view. The upgrade is now complete.



Check the new firmware version if you wish (see A.3.2 - Determine the Liebert IntelliSlot Card Type and Firmware Version).

A.6 UPDATING THE FIRMWARE - XMODEM (SERIAL) METHOD

Follow these steps to update the firmware using the Xmodem (serial) method. This method works through the Web card's serial port, employing terminal emulation software, such as HyperTerminal.



NOTE

This method includes a time-sensitive operation requiring expeditious location of the upgrade files downloaded in A.3.3 - Download the Firmware Upgrade File to the Computer. Read through this entire section before beginning the upgrade.

Connect a Cable to the Serial Ports

1. Connect one end of a DB-9 null modem or file transfer cable to the Web card's serial port and the other to the computer's serial port.

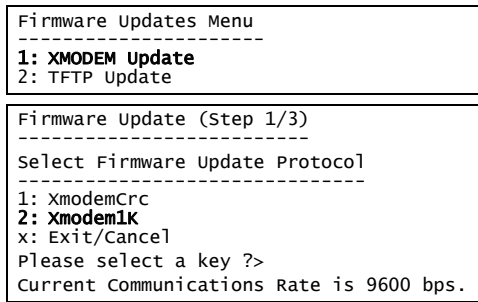
The correct cable will have, at a minimum, Pins 2 and 3 crossed at the ends, as shown in **Figure A1**. The configuration cable is available separately from Emerson® (P/N LIEBNULL).

Figure A1 Null connection



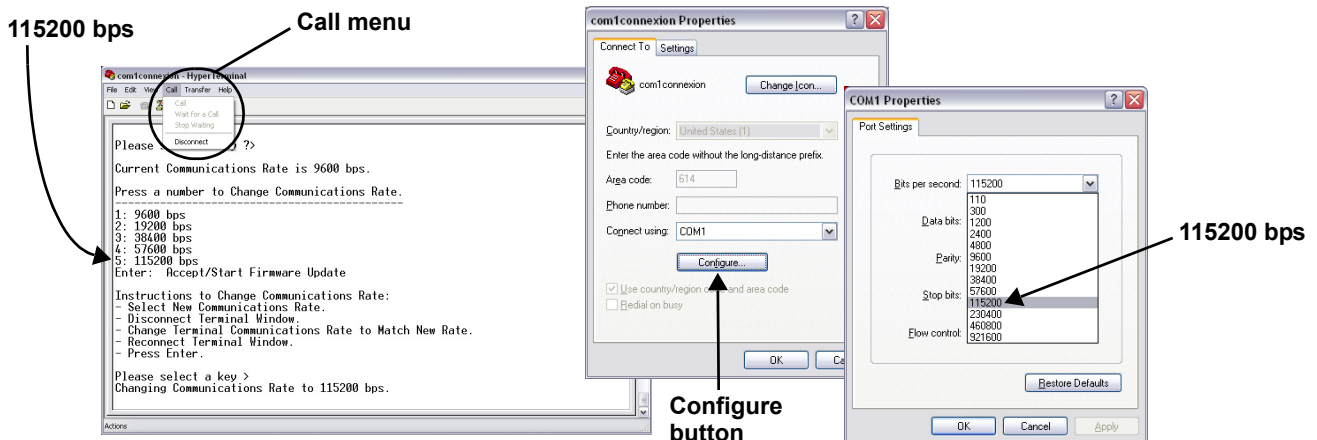
Open a Terminal Emulation Connection

2. Open a connection to the Liebert IntelliSlot card (if needed, see instructions in A.2.1 - Open the Terminal Emulation Interface - Serial Connection).
3. Choose **Firmware Updates** from the Main Menu.
4. Choose **XMODEM Update** from the Firmware Updates menu, seen at right, and enter **y** (yes) to confirm your choice.
5. Choose **Xmodem1K** from the Select Firmware Update Protocol, as shown at right.



Change the Baud Rate to 115200

6. Choose **115200 bps** from the menu, shown below left.
7. From the HyperTerminal menu, click on **Call**, then choose **Disconnect** (this will not close the HyperTerminal connection to the card).
8. In the HyperTerminal menu bar, click on **File**, then choose **Properties**.
9. Click on the Connect To tab and click the **Configure** button. This opens Port Settings tab in the COM1 Properties window, as shown below right.
10. Choose **115200** from the Bits Per Second drop-down list and click **OK**, then click **OK** to close the Properties window.
11. In the HyperTerminal menu bar, click on **Call**, then choose **Call** from the drop-down menu and press the Enter key.



Download the First Firmware Update File

12. After changing the communication rate to 115200 bps, press Enter to resume the firmware update.

After you press Enter, HyperTerminal displays Cs as it counts down the time remaining to locate and begin transferring the upgrade files.



NOTE

After you begin the initialization process in **Step 12**, you must complete **Steps 13 through 15** within 60 seconds. Before beginning, check to ensure that you know the location of the firmware files and read through the following steps to understand what needs to be done.

This 60-second limit also applies to downloading the second and third upgrade files.

13. In the HyperTerminal menu, click on **Transfer**, then **Send File**.

The image shows a HyperTerminal window with a menu open. An arrow points to the 'Send File' option with the label 'Browse to locate upgrade file'. Another arrow points to the '1K Xmodem' option in the protocol list with the label 'Choose 1K Xmodem'. A third arrow points to the 'Enter' key on the keyboard with the label 'Press Enter to start firmware update'. To the right, a 'Select File to Send' dialog box is shown with three files selected. An arrow points to the 'Open' button with the label 'Progress window shows elapsed time...'. A fourth arrow points to the 'Elapsed' and 'Remaining' time fields in the progress window with the label '... and remaining time'.

14. Click the **Browse** button to locate an upgrade file. Select the files in order—the filename ending in FILE1 for the first download, then FILE2, and finally FILE3—then click **Open**.

15. In the Send File window, choose **1K Xmodem** from the Protocol drop-down list and click **Send**.

A progress window opens, showing the elapsed time and amount of time remaining for the first file to be downloaded to the Liebert IntelliSlot card. The window closes after the first file is downloaded.



NOTE

Do not press any keys while the progress window remains open or the download will abort.

Download the Second and Third Firmware Update Files

16. When the progress window closes, enter **y** (yes) in HyperTerminal to continue the upgrade.

17. Choose **Xmodem1K** in the Select Firmware Update Protocol menu.

18. The screen shows that the communication rate is 115200. This does not need to be changed.

19. Press Enter to continue.

20. Repeat **Steps 12 through 15** within the 60-second limit to browse to the second upgrade file and download it to the Liebert IntelliSlot card.

21. Wait for the Progress window to close after the second file is downloaded.

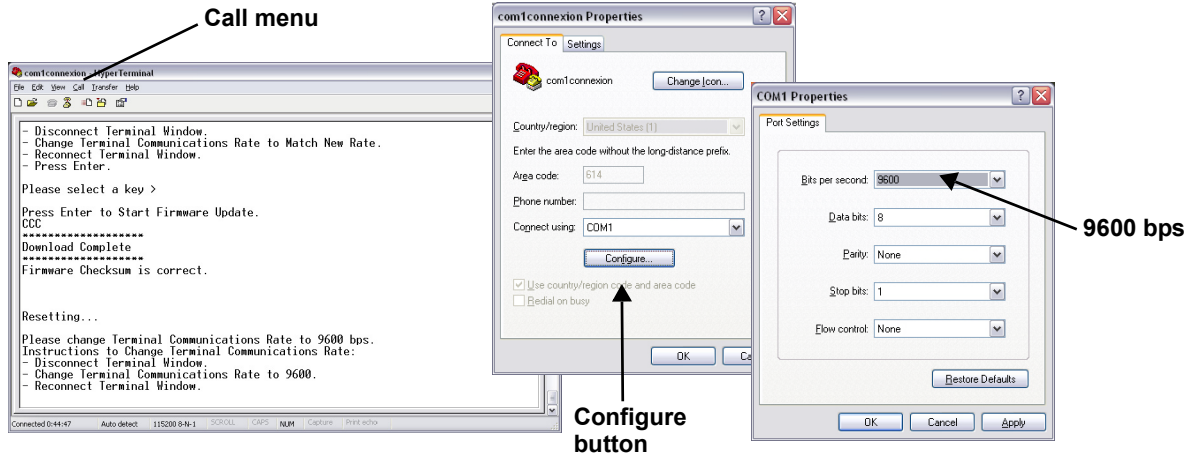
Then repeat **Steps 16 through 20** to download the third upgrade file. This file is the largest and may take 30 minutes or longer to download.

```

Would You Like to Continue (Y or N)?
Firmware Update (Step 2/3)
-----
Select Firmware Update Protocol
-----
1: XmodemCrc
2: Xmodem1K
X: Exit/Cancel
Please select a key ?>
Current Communications Rate is 115200 bps.
Press a number to Change Communications Rate.
-----
1: 9600 bps
2: 19200 bps
3: 38400 bps
4: 57600 bps
5: 115200 bps
Enter: Accept/Start Firmware Update
Please select a key >
Press Enter to Start Firmware Update.
    
```

Complete the Upgrade and Restore Communication Rate

22. Choose **9600 bps** from the menu, shown below left.
23. From the HyperTerminal menu, click on **Call**, then choose **Disconnect** (this will not close the HyperTerminal connection to the card).
24. In the HyperTerminal menu bar, click on **File**, then choose **Properties**.
25. Click on the Connect To tab and click the **Configure** button. This opens Port Settings tab in the COM1 Properties window, as shown below right.
26. Choose **9600** from the Bits Per Second drop-down list and click **OK**, then click **OK** to close the Properties window.
27. In the HyperTerminal menu bar, click on **Call**, then choose **Call** from the drop-down menu.
28. Press the Enter key.



29. Choose **Exit and Save** from the Main Menu to reboot the card. When rebooting is complete, the upgrade is finished.

Check the new firmware version if you wish (see **A.3.2 - Determine the Liebert IntelliSlot Card Type and Firmware Version**).

```

Main Menu
-----
1: System Information
2: IP Network Settings
3: Messaging
4: Factory Settings
5: Firmware Updates

q: Quit and abort changes
x: Exit and save

Please select a key ?> 5
    
```

Notes

Ensuring The High Availability Of Mission-Critical Data And Applications.

Emerson Network Power, a business of Emerson (NYSE:EMR), is the global leader in enabling *Business-Critical Continuity™* from grid to chip for telecommunication networks, data centers, health care and industrial facilities. Emerson Network Power provides innovative solutions and expertise in areas including AC and DC power and precision cooling systems, embedded computing and power, integrated racks and enclosures, power switching and controls, infrastructure management, and connectivity. All solutions are supported globally by local Emerson Network Power service technicians. Liebert AC power, precision cooling and monitoring products and services from Emerson Network Power deliver Efficiency Without Compromise™ by helping customers optimize their data center infrastructure to reduce costs and deliver high availability.

While every precaution has been taken to ensure the accuracy and completeness of this literature, Liebert Corporation assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions.

© 2009 Liebert Corporation

All rights reserved throughout the world. Specifications subject to change without notice.

® Liebert is a registered trademark of Liebert Corporation.

All names referred to are trademarks or registered trademarks of their respective owners.

SL-52615_REV6_09-13

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

Environmental 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

29/F, The Orient Square Building

F. Ortigas Jr. Road, Ortigas Center

Pasig City 1605

Philippines

+63 2 687 6615

Fax: +63 2 730 9572

Emerson Network Power.

The global leader in enabling *Business-Critical Continuity™*

AC Power

Embedded Computing

Outside Plant

Connectivity

Embedded Power

Power Switching & Controls

DC Power

Infrastructure Management & Monitoring

Precision Cooling

EmersonNetworkPower.com

Racks & Integrated Cabinets

Services

Surge Protection