VERTIV.

Liebert®

IntelliSlot™ Unity™ Card

Installer/User Guide

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Refer to other local practices or building codes as applicable for the correct methods, tools, and materials to be used in performing procedures not specifically described in this document.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. Visit https://www.VertivCo.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

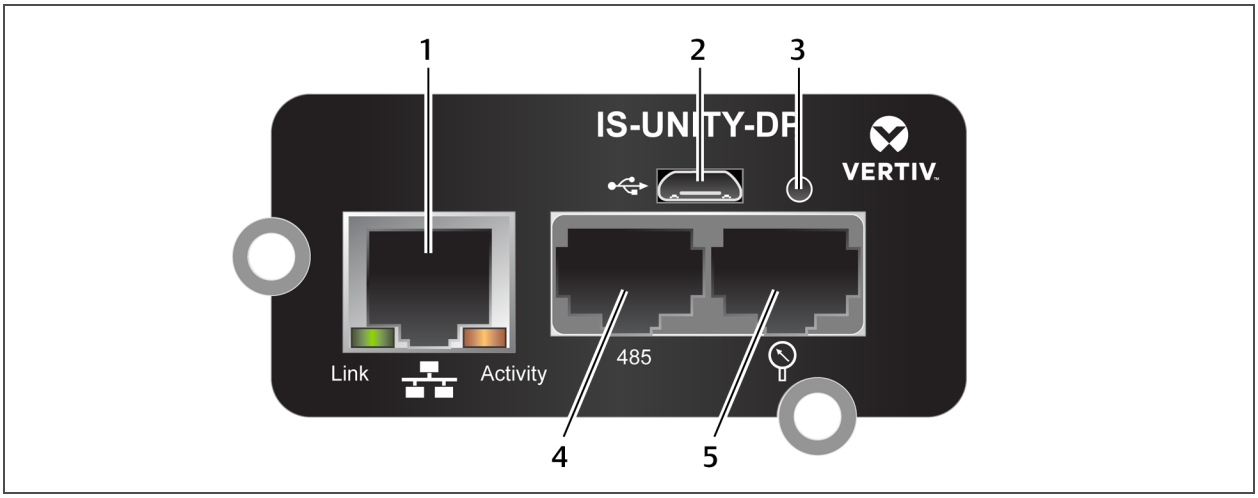
1 INTRODUCTION

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

The platform includes the IS-Unity-DP™, IS-Unity-SNMP™, and IS-Unity-LIFE™ cards.

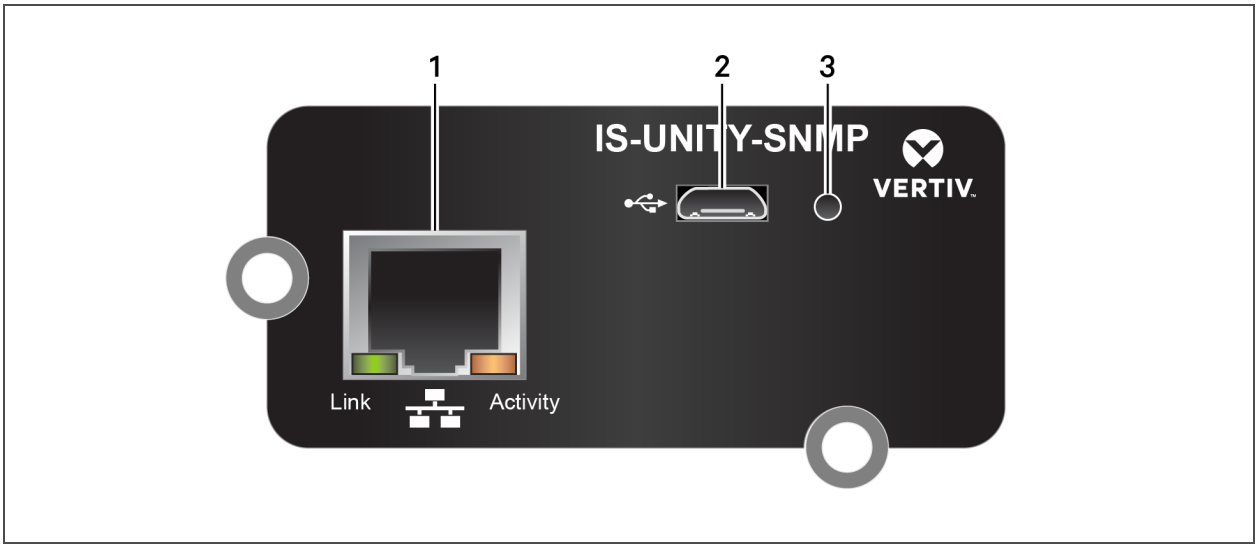
Each card employs the Velocity Protocol to monitor and manage a wide range of operating parameters, alarms, and notifications. The card communicates with Building Management Systems and Network Management Systems via BACnet, Modbus, SNMP, LIFE/Remote Services, and YDN23 protocols.

Figure 1.1 IS-Unity-DP Card Features



ITEM	DESCRIPTION
1	RJ-45 Ethernet port
2	Micro-USB port
3	Reset button, see Manually Resetting to Factory Defaults on page 67.
4	RS-485 port (BACnet/MSTP, Modbus RTU or YDN23. Only one may be used.)
5	Liebert sensor-network port (SN sensors only)

Figure 1.2 IS-Unity-SNMP Card Features



ITEM	DESCRIPTION
1	RJ-45 Ethernet port
2	Micro-USB port
3	Reset button, see Manually Resetting to Factory Defaults on page 67.

1.1 Support for Liebert SN Sensors

The Unity card monitors up to 10 Liebert SN modular and integrated sensors. Available sensor types include temperature, humidity, door closure, contact closure and leak detection. Sensor tab menus permit configuring sensors and putting them in user-configured order for easier checking of high-priority conditions. Sensor data is available via SNMP and the Web user interface. See Sensor Tab Menu on page 26.

2 INSTALLATION

⚠ **WARNING! Arc flash and electric shock hazard. Open all local and remote electric power supply disconnect switches, verify with a voltmeter that power is Off and wear personal protective equipment per NFPA 70E before working within the electrical control enclosure. Failure to comply can cause serious injury or death.**

⚠ **WARNING! Risk of electric shock. Can cause equipment damage, injury or death.**

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

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

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

NOTICE

Risk of improper installation. Can cause equipment damage.
Only a qualified service professional should install these products. We recommend that a Vertiv™ technician perform the installation in large UPS system. Contact Vertiv™ at https://www.vertivco.com/en-us/support/.

NOTICE

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

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

Each IntelliSlot card must have a unique node ID. This will not be a problem if only one card is installed on your system. Duplicate node IDs are easily averted with the procedure detailed in Installing Multiple Cards in a System on page 7.

2.1 Installing the Card

The Unity card may be installed at the factory or field-installed.

To perform a field installation:

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

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

3. Secure the card with the screws used for the cover plate.

4. Connect an Ethernet cable to the card's Ethernet RJ-45 port for IP communication interfaces.
5. Connect a serial cable to the card's 485 RJ-45 port for RS-485 communication interfaces, see Connecting an RS-485 Serial Cable on page 6.

2.1.1 Connecting Directly to Computer for Configuration

Before you can make any configuration changes like configuring the static-IP settings, you must access the card's web server via Ethernet.

To connect to the card:

1. Connect a computer running a Microsoft Windows operating system (Microsoft Windows® XP or later) to the card by plugging one end of a network cable into the Ethernet port on the computer and the other end into the Ethernet port on the Unity card, see **Figure 1.1** on page 1. Computer Automated Private IP addressing (APIPA) is normally enabled by default on computers running the Microsoft Windows operating system and will assign an Autoconfiguration IPv4 address when a DHCP server is not detected.

NOTE: This IP autoconfiguration process can take 1 to 3 minutes.

If necessary, use the Windows Command Prompt to verify the computer's IP-address settings:

- Press the Windows key+**R**, and enter **cmd**, and click *OK*.
- Type **ipconfig /all** and press Enter, then verify the following, see FIGURE:

  Autoconfiguration Enabled = Yes

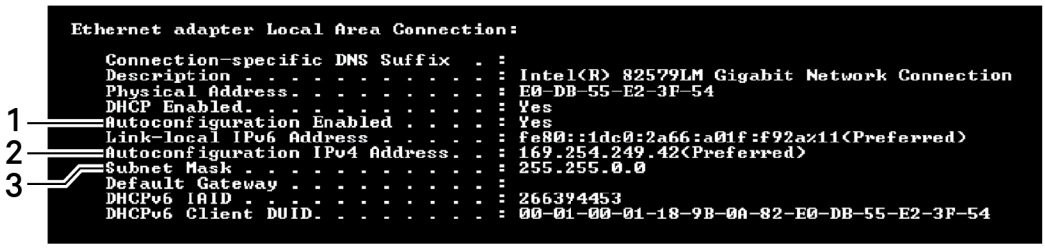
  Autoconfiguration IPv4 Address = 169.254.x.x

  Subnet Mask = 255.255.0.0

NOTE: Enter ipconfig /renew to for acquisition of an Autoconfiguration IPv4 Address if one is not listed.

2. On the computer, open a web browser session and enter 169.254.24.7 to connect to the card's web server.
   The Unity user interface opens.

Figure 2.1 Autoconfiguration Lines in the Command Prompt



ITEM	DESCRIPTION
1	Autoconfiguration Enabled
2	Autoconfiguration IPv4 Address
3	Subnet Mask

2.1.2 Determining the DHCP IP Address

The Unity card is factory-configured for DHCP. If a Static or BootP network configuration is required, change the Boot Mode as described in Assigning a Static IP Address below. For DHCP, connect an active Ethernet cable to the card, and it will receive an IP address from the DHCP server. Contact the DHCP administrator to obtain the IP address using the Unity card's MAC address. The MAC address is printed on the card's faceplate.

If the DHCP administrator is not available or if there is not a convenient way of determining the IP address assigned by the DHCP server, use a computer with a direct Ethernet connection to the card, and the Autoconfiguration IPv4 Address convention described in Connecting Directly to Computer for Configuration on the previous page, to access the card's Web page.

To see the card's last DHCP-assigned IP address:

1. Click the *Communications* tab, then on the left-side menu, select *Support* > *Active Networking*.
2. Check the Last DHCP/BOOTP Address field, which shows the last IP address assigned by the DHCP server. The card may retain that IP address when it reconnects to the DHCP network because most DHCP systems reuse the same IP address for the same device.

2.1.3 Assigning a Static IP Address

To assign a static IP address, use the direct Ethernet connection to configure the card. Proceed to Connecting Directly to Computer for Configuration on the previous page and Change User Names and Passwords Immediately on page 7.

2.1.4 Connecting an RS-485 Serial Cable

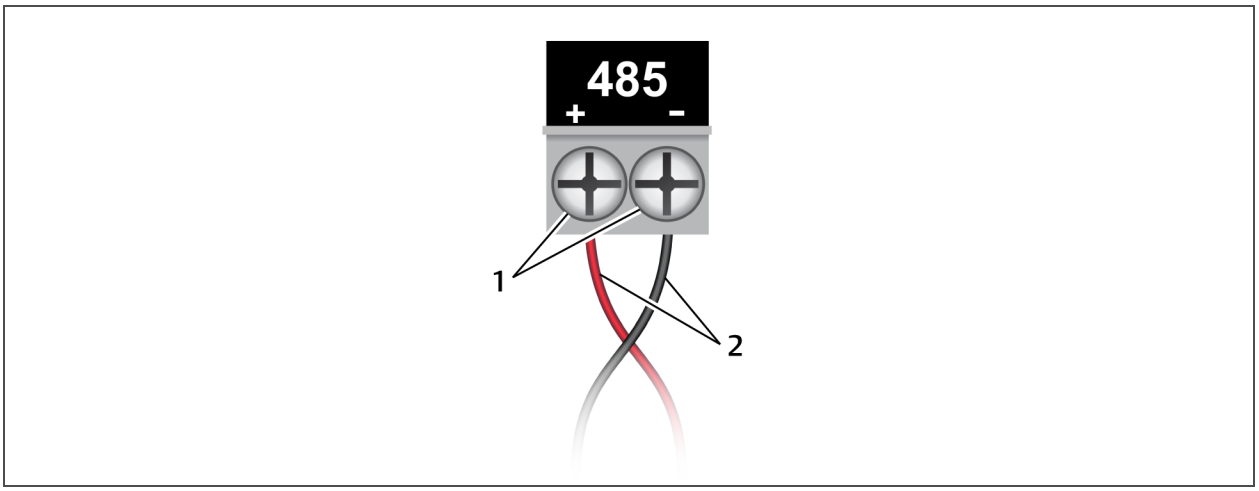
Unity cards come with an Adapter RJ-45-2POS Terminal Block. The adapter has two screw terminals to attach the ends of a RS-485 cable for communicating to a building management system.

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

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

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

Figure 2.2 Adapter terminal-block marks face up



ITEM	DESCRIPTION
1	Screws
2	Wires

4. Loosen the screw to the positive terminal and insert the red wire far enough into the terminal block to insert the bare wires under the screw, then tighten the screw using care not to break the wires.
5. Repeat Step 3 with the negative terminal and the black wire.
6. Plug the cable into the 485 RJ-45 port on the Unity card. See IS-Unity-DP Card Features on page 1, for the location of the port.

2.2 Change User Names and Passwords Immediately

NOTE: We recommend changing the user names and passwords of the factory-default Local Users with administrator and general access immediately to safeguard protected configuration and control areas of the Unity card.

The factory-default administrator user is "Local Users [1]" with the user name *Liebert* and default password *Liebert* (both case-sensitive).

The factory-default general user is "Local Users [2]" with the default password *Liebert* (case-sensitive).

To change the user names and passwords, see the steps in Local Users Folder on page 31.

2.3 Configure the Card

The Unity card requires minor configuration, to enable basic network connectivity. The default for IP/Web communication is IPv4, but this can be changed to IPv6 for greater security. Contact your network administrator to determine if it is compatible with your network.

1. On the Communications tab menu, select *Configuration* > *Network*.
2. Enable the protocol, IPv4 or IPv6, that will be used to communicate with the Unity card and with the Liebert equipment:
   a. Click *IPv4* or *IPv6*.
   b. Click *Edit*.
   c. When prompted, enter the Administrative user name and password.
      The default name and password are both "Liebert" (case-sensitive).
   d. Click to check *enabled*.
   e. Enter the assigned IP address along with the rest of the required networking information. Contact your system administrator if necessary.
3. Click *Save* to confirm the changes or *Cancel* to discard them.
   The changes take effect after the card is restarted.

2.4 Installing Multiple Cards in a System

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

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

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

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

The default node ID for a Unity card is 0, so the second card should use 1. A third card should use 2. A fourth card should use 100 to 127. Contact your system administrator about the proper node ID for the second card, then perform the following steps.

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

2.5 Security Best Practices

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

Table 2.1 on the facing page, provides a list of items to review. Each should be reviewed, configured based on the operational needs for managing the equipment, and verified that the settings support the desired operational functionality without adding unnecessary or unauthorized access to critical infrastructure equipment. A reference to the proper section in this document is provided for configuring each item.

Table 2.1 Settings to review and verify to reduce the risk of unauthorized access

ITEM	DESCRIPTION	REFERENCE
Accounts & Passwords	Change the admin and user account names and passwords immediately to eliminate default credential access.	Change User Names and Passwords Immediately on the previous page
IP Network Access	Enable/disable IPV4 and IPV6 network access to the Unity Card - disable unused network access.	Configure the Card on the previous page
Telnet and SSHv2 Access	Enable/disable telnet and SSHv2 access for diagnostic and configuration support - disable when not in use.	Network Folder on page 37
Web Service Protocol	Select HTTPS to use SSL encryption when accessing data through the web user interface.	Web Server Folder on page 39
SSL Certificates	When using HTTPS, install your own SSL Certificates from a trusted certificate authority or generate alternative self-signed certificates	Certificate Folder on page 41
Password Protect Web Access	Enable to require users to log in before any device information is displayed to the user.	Web Server Folder on page 39

Table 2.1 Settings to review and verify to reduce the risk of unauthorized access (continued)

ITEM	DESCRIPTION	REFERENCE
Remote Write Web Access	Disable to require all updates to the device and card be made through a local interface, via an Autoconfiguration connection with a PC directly connected to the Unity card or through the device's local user interface display (if available). ⚠ **WARNING! Only disable this if you are absolutely sure that you do not need to administer the managed device or the Unity card through a remote web browser session.**	Web Server Folder on page 39
Communication Protocols	Enable/disable BACnet, Modbus, SNMP, and YDN23 protocols - disable any that are unused.	Enable Communication Protocols on page 11
BACnet Settings	Set Managed Device Write Access to Read-Only to prevent changes to the device through the BACnet interface.	Enable BACnet Protocol on page 13
Modbus Settings	Set Managed Device Write Access to Read-Only to prevent changes to the device through the Modbus interface; Select the appropriate option for Limit Network Access Type to restrict which systems may request Modbus data from the device - access may be open to any system, limited to those on the same subnet as the device, or limited to only those from systems on a Trusted IP Address List.	Enable Modbus Protocol on page 11
SNMP Version Settings	Enable/disable the desired SNMP version(s); Consider using SNMPv3 with user authentication and encryption.	Configure SNMP Settings on page 15
SNMP Access Table Settings	For each SNMPv1/v2c Access table entry, set the SNMP Access Type to Read-Only to prevent changes to the device from the hosts identified in the table entry.	Configure SNMPv1/v2c Access Settings on page 17
SNMP Community Strings	Change the SNMP v1/v2c Trap and Access Community Strings from their default values.	Configure SNMPv1 Trap Settings on page 16 and Configure SNMPv1/v2c Access Settings on page 17
SNMPv3 Settings	Use the SNMPv3 Authentication and Privacy settings to make SNMPv3 communications more secure.	Configure SNMPv3 User Settings on page 16
YDN23 Settings	Set Managed Device Write Access to Read-Only to prevent changes to the device through the YDN23 interface.	YDN23 Folder on page 59
Velocity Protocol Settings	Enable/disable the Velocity Protocol which is used by Vertiv™ management applications to access device data.	Velocity Protocol Folder on page 47

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

Table 2.2 Ports used by the Unity card

NETWORK SERVICE		PORT USED	DEFAULT?	CAN BE MODIFIED?
Web	HTTP	TCP 80	Yes	Yes
	HTTPS	TCP 443	Yes	Yes
DNS		TCP & UDP 53	Yes	No
NTP		TCP & UDP 123	Yes	No
SMTP		TCP 25	Yes	Yes
SSHv2		TCP & UDP 22	Yes	No
Telnet		TCP 23	Yes	No
SNMP		UDP 161, 162	Yes	Only trap port 162 may be changed
Modbus TCP		TCP 502	Yes	Yes
BACnet IP		UDP 47808	Yes	Yes
Velocity Protocol		UDP 47808	Yes	No
LIFE		TCP 80	Yes	Yes

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

3 ENABLE COMMUNICATION PROTOCOLS

The Unity card communicates with equipment and 3rd-party systems over the following protocols:

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

NOTE: No more than two protocols may be enabled on one card. Only one version of BACnet may be selected: BACnet IP or BACnet MSTP. Only one version of Modbus may be selected: Modbus TCP or Modbus RTU. Only one of the chosen protocols can use the 485 port. Choosing two 485 protocols will cause conflicts.

NOTE: Some building-management systems (BMS) can be configured to send continuous updates for device setpoints, usually setting the same value. The BMS should be configured to send, on a sustained average, no more than two writes per second to the device. This will allow the device to catch up after a burst of updates when necessary, while allowing other communication with the device to proceed.

3.1 Enable Protocols

Protocols may be enabled after a card is installed and configured for basic network connectivity. After a protocol is enabled, it must be configured, which requires opening the folder for the desired protocol (*Communications* tab > *Protocols* > *(protocol to configure)*.

To enable two communication protocols:

1. On the Communications tab, select *Protocols*.
2. Click *Edit* and enter the administrator user name and password.
3. Click to check the box next to the protocols to use.
   - Only two protocols may be enabled.
   - Only one of the two can use the 485 port.
4. Click *Save* to confirm the changes or *Cancel* to discard them.
5. Configure the protocols selected. See Editing the Unity Card Configuration on page 29.
6. Restart the card:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

3.1.1 Enable Modbus Protocol

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

1. On the Communications tab, select *Protocols* > *Modbus*.
2. Click *Edit* and enter a user name and password.

3. Select the access level (*Read Only* or *Read/Write*).
4. Select the Modbus interface, (*Modbus TCP* or *Modbus RTU*).
5. Click *Save* to confirm the changes or *Cancel* to discard them.
6. Configure the Modbus interface chosen.
   See Configure Modbus TCP below or Configure Modbus RTU below.
   For descriptions of the settings, see Modbus Folder on page 54.

Configure Modbus TCP

1. On the Communications tab, select *Protocols* > *Modbus* > *Modbus TCP*.
2. Click *Edit*, and enter a user name and password if necessary.
3. Set the Limit Network Access Type by choosing from the drop-down list:
   - Open
   - Same Subnet
   - Trusted IP List

   See Modbus TCP Folder on page 55 for additional details.
4. Enter the Port that the Modbus server will use to listen-for and respond-to Modbus protocol requests based on the selected Limit Network Access Type.
5. Enter the Maximum Client Connection Count.
6. Click *Save* to confirm the changes or *Cancel* to discard them.
7. Restart the card:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

Configure Modbus RTU

1. On the Communications tab, select *Protocols* > *Modbus* > *Modbus RTU*.
2. Click *Edit*, and enter a user name and password if necessary.
3. Enter the Node ID and the Baud Rate.
   - The Node ID defaults to 1, but must have a value from 1 to 247 that is unique among devices connected through the RS-485 interface.
   - The default baud rate is 9600. 19200 and 38400 are also available.

   For additional description of the settings, see Modbus RTU Folder on page 55.

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

4. Click *Save* to confirm the changes or *Cancel* to discard them.
5. Restart the card:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

3.1.2 Enable BACnet Protocol

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

1. On the Communications tab, select *Protocols* > *BACnet*.
2. Click *Edit*, and enter a user name and password if necessary.
3. Select the Managed Device Write Access level: *Read Only* or *Read/Write*.
   This determines a user's ability to change settings in the Unity card.
4. Choose the BACnet interface: *BACnet IP* or *BACnet MSTP*.
5. Set the Device Object Instance Number.
6. Set the Device Object Name.
7. Set the APDU Timeout.
8. Set the APDU Retries.
9. Click *Save* to confirm the changes or *Cancel* to discard them.
10. Configure the BACnet interface chosen, see Configure BACnet IP Protocol below or Configure BACnet MSTP Protocol below.
    For description of the settings, see BACnet Folder on page 53.

Configure BACnet IP Protocol

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

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

   For descriptions of the settings, see BACnet IP Folder on page 54.
4. Click *Save* to confirm the changes or *Cancel* to discard them.
5. Restart the card:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

Configure BACnet MSTP Protocol

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

1. On the Communications tab, select *Protocols* > *BACnet* > *BACnet MSTP*.

2. Click *Edit*, and enter a user name and password if necessary.
3. Set the BACnet MSTP Node ID.
   - The Node ID defaults to 1, but must have a value from 0 to 127 that is unique among devices connected through the RS-485 interface.
4. Set the BACnet MSTP Data Rate.
5. Set the BACnet MSTP Max Master Address.
6. Set the BACnet MSTP Max Info Frames.

   For descriptions of the settings, see BACnet MSTP Folder on page 54.
7. Click *Save* to confirm the changes or *Cancel* to discard them.
8. Restart the card:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

3.1.3 Enable SNMP

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

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

   For descriptions of the settings, refer to SNMP Folder on page 56.
6. Click *Save* to confirm the changes or *Cancel* to discard them.
7. Restart the card:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

Global Products MIB for SNMP Integration

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

The Liebert Global Products MIB is available at https://www.vertivco.com/en-us/support/software-download/monitoring/management-information-bases-mibs-for-liebert-products/. It supports both Windows® (192436P1) and Unix (192435P1) file formats.

Configure SNMP Settings

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

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

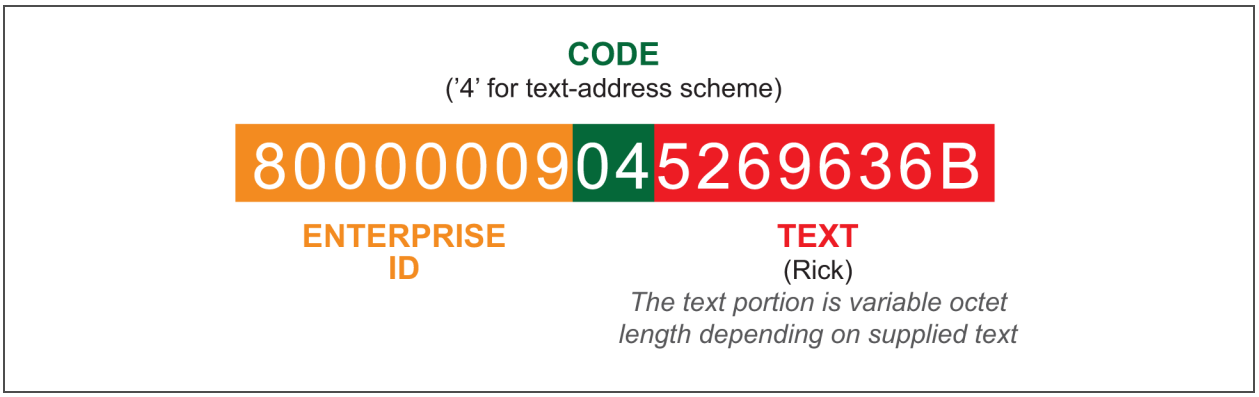
- SNMPv1 must have trap settings.
- SNMPv2c must have Access settings.
- SMPv3 users must have settings configured and the method for generating the Engine ID may be selected.
- the access settings for SNMPv1/v2c are separate from SNMPv1 trap settings.

Select SNMPv3 Engine ID Format

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

1. On the Communications tab, select *Protocols* > *SNMP*.
2. Click *Edit*, and enter a user name and password if necessary.
3. Edit the settings:
   Refer to SNMP Folder on page 56, for descriptions of the settings and options.
   - In SNMPv3 Engine ID Format Type, select *MAC Address* or *Text*.
   - If you selected Text, type the text on which the generated engine ID will be based.
   - Click *Save* to confirm the changes or *Cancel* to discard them.
     The new engine ID is not displayed until after rebooting the card in Step 4.
     The text-generated engine ID is a hexadecimal representation of ASCII characters similar to that shown in Figure 3.1 on the next page.

Figure 3.1 SNMP Engine ID generated using text-format scheme



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

4. Restart the card to activate the changes:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

Configure SNMPv3 User Settings

1. On the Communications tab, select *Protocols* > *SNMP* > *SNMPv3Users Setting 20)* > *SNMPv3 Users Setting (1)*.

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

2. Click *Edit*, and enter a user name and password if necessary.
3. Enter the information and set the permissions appropriate to the user.
   For descriptions of the settings and options, see SNMPv3 User Folder on page 57.
4. Click *Save* to confirm the changes or *Cancel* to discard them.
5. Repeat steps 1 through 4 for additional users.
6. Restart the card to activate the changes:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

Configure SNMPv1 Trap Settings

1. On the Communications tab, select *Protocols* > *SNMP* > *SNMPv1 Trap (20)*.

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

2. Click *Edit*, and enter a user name and password if necessary.
3. Enter the information and set the permissions appropriate to the user.
   For descriptions of the settings, see SNMPv1 Trap Folder on page 58.

4. Click *Save* to confirm the changes or *Cancel* to discard them.
5. Repeat 1 through 4 for any additional users.
6. Restart the card to activate the changes:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

Configure SNMPv1/v2c Access Settings

1. On the Communications tab, select *Protocols* > *SNMP* > *SNMPv1/v2c Access (20)* > SNMPv1/v2c Access (1).

NOTE: Selecting the SNMPv1/v2c Access folder, displays only the settings that are available for configuration.

2. Click *Edit*, and enter a user name and password if necessary.
3. Enter the information and set the permissions appropriate to the user.
   For description of the settings and options, see SNMPv1/v2c Access Folder on page 59.
4. Click *Save* to confirm the changes or *Cancel* to discard them.
   The card must be restarted before another user's settings may be changed.
5. Restart the card to activate the changes for this user:
   a. On the Communications tab, click *Support*.
   b. Click *Enable*.
   c. Click *Restart*.

3.2 Download Protocol Mappings

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

NOTE: The Liebert SN sensors are not supported via BACnet or Modbus.

To download a data mapping list:

Click the Managed Device tab, then *Summary* > *Downloads*.
The Data Mapping Files heading shows mapping files for each enabled protocol:

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

More information about BACnet and Modbus protocol mapping is available in the *Liebert IntelliSlot Modbus and BACnet Protocol Reference Guide* (SL-28170) at www.vertivco.com. The SNMP MIB files are also available for download from the site.

4 ENABLE CLOUD CLIENT FOR LIEBERT® MINI-MATE™

The Cloud Client is exclusively for the Mini-Mate Thermal Management System. The configuration menu for the Cloud Client is only displayed when the detected managed device is a Mini-Mate unit. For all other devices the Cloud Client configuration menu will NOT be displayed.

The Cloud Client updates a Cloud Server and make Mini-Mate status information available to a mobile app, providing remote-device monitoring for the Mini-Mate unit.

To configure the Cloud Client, start with Typical Configuration for Cloud-client Support (Prerequisites) below..

4.1 Typical Configuration for Cloud-client Support (Prerequisites)

Configuring the Cloud Client on an un-initialized Unity card requires the following:

- The Unity card must have a network address assigned and have access to the Cloud Service URL. The Cloud Service URL is typically https://icomcms.com.
- DNS must be configured and working appropriately because it is used to access the Cloud Service.
- The Unity card must have a System Name that is unique to the Organization. The Unity card "System Name" maps to the "Manager Name" in the Cloud Service.
- The managed device must be a Mini-Mate Thermal Management System. Otherwise, the Cloud Client folder is not available in the Unity Web UI menu.
- The following Cloud Client information must have been factory-configured or be configured by the customer using factory-supplied information:
  - Email Address – the customer email address associated with the Cloud Service Organization specific to the customer.
  - Registration Key – factory supplied
  - Cloud Service URL – typically https://icomcms.com
- The Cloud Client must be enabled.

With these items in place or staged, proceed to Registering with the Cloud Service Administration Portal to Allow Mobile-app Users Access on the facing page.

4.2 Registering with the Cloud Service Administration Portal to Allow Mobile-app Users Access

Thermal-management units must be registered to provide data to the cloud so that mobile-app users will receive the notifications from the cooling unit.

Units are registered based on domain portion of the organization's e-mail address. The domain is the part after the "@" symbol and is typically the name of the organization, for example: @company.com.

NOTE: Before attempting registration with the Mobile Cloud Service, the Unity card in the unit must be assigned network credentials on your corporate network to access the Cloud Service URL (https://icomcms.com).

NOTE: When registering the cooling unit, be sure to use an e-mail address with the correct domain of the organization. If you register using an e-mail address with an incorrect domain, un-register and contact the administrator for the correct address.

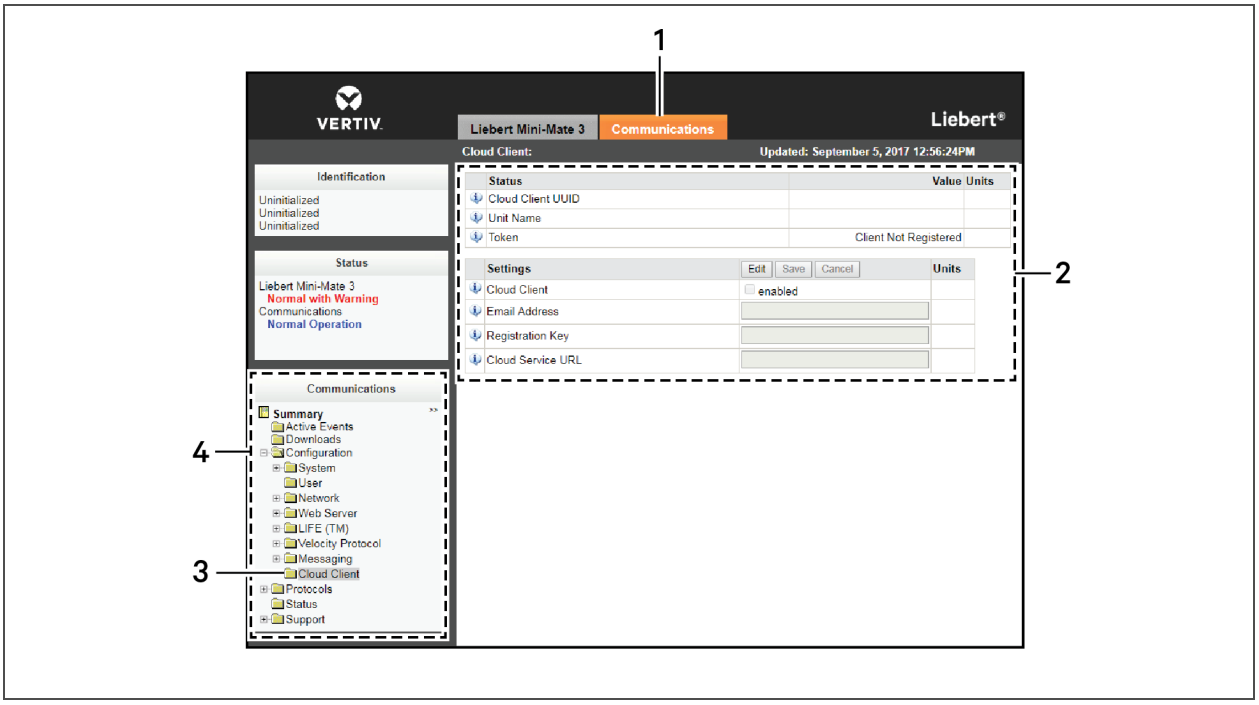
NOTE: The mobile app is available for download from the Apple Store or Google Play Store depending on your mobile device. Search for "iCOM CMS."

To register with the administration portal:

1. Use a CAT5 Ethernet cable to connect a computer/laptop to an Ethernet port on the Unity card.
2. On the connected computer, open a Web browser and enter the card's default address: 169.254.24.7 in the address bar.
   The Unity web user interface opens.
3. Configure the System Name before attempting to register the Mini-Mate unit:
   - On the Unity web UI, click the *Communications* tab.
   - In the Communications pane on the left-hand side, select *Configuration* > *System*.
   - Click *Edit*, and enter the default Username and Password, which is *Liebert* (case-sensitive) for both.
   - Enter a descriptive System Name for the Mini-Mate unit. This will identify the unit for management in the cloud client administration portal.
   - Enter the remaining system settings if needed, and click *Save*.
4. Restart the card for the changes to take effect:
   - Communications pane on the left-hand side, select *Support*.
   - In the Commands section, click *Enable*, and enter the default Username and Password, which is *Liebert* (case-sensitive) for both.
   - Click *Restart Card*.
5. Obtain an e-mail address with valid domain from the Unity administrator who manages mobile-app access for the organization.
6. On the Unity web UI, click the *Communications* tab, see Cloud Client Folder on page 52.
7. In the Communications pane on the left-hand side, select *Configuration* > *Cloud Client*.
8. Click *Edit*, and enter the default Username and Password, which is *Liebert* (case-sensitive) for both.

9. Click to check *enable* next to Cloud Client, and enter the following:
    - Email Address = Customer e-mail address associated with the customer's organization within the cloud service. The organization is based on the domain portion of the e-mail address.
    - Registration Key = Factory-configured, unique key that identifies the Mini-Mate/Unity card for the cloud service. They key cannot be shared between Unity cards.
    - Cloud Service URL = https://icomcms.com. The address for the cloud service administration portal, through which mobile-app users are managed.
10. Click *Save*.
11. Restart the card for the changes to take effect:
    - Communications pane on the left-hand side, select *Support*.
    - In the Commands section, click *Enable*, and enter the default Username and Password, which is *Liebert* (case-sensitive) for both.
    - Click *Restart Card*.
      The device is registered with the Cloud Client Administration Portal.

Figure 3.2 Cloud Client page



ITEM	DESCRIPTION
1	Communications tab
2	Cloud Client status and settings
3	Cloud Client folder
4	Communications folders

5 UNITY CARD WEB-PAGE LAYOUT

Default settings of the Unity card let you use it immediately after installation to monitor the equipment in which the card is installed. The Web interface customizes the information to ease equipment monitoring and troubleshooting problems. You can name the equipment, enter a location, set up email and text alerts and change equipment settings.

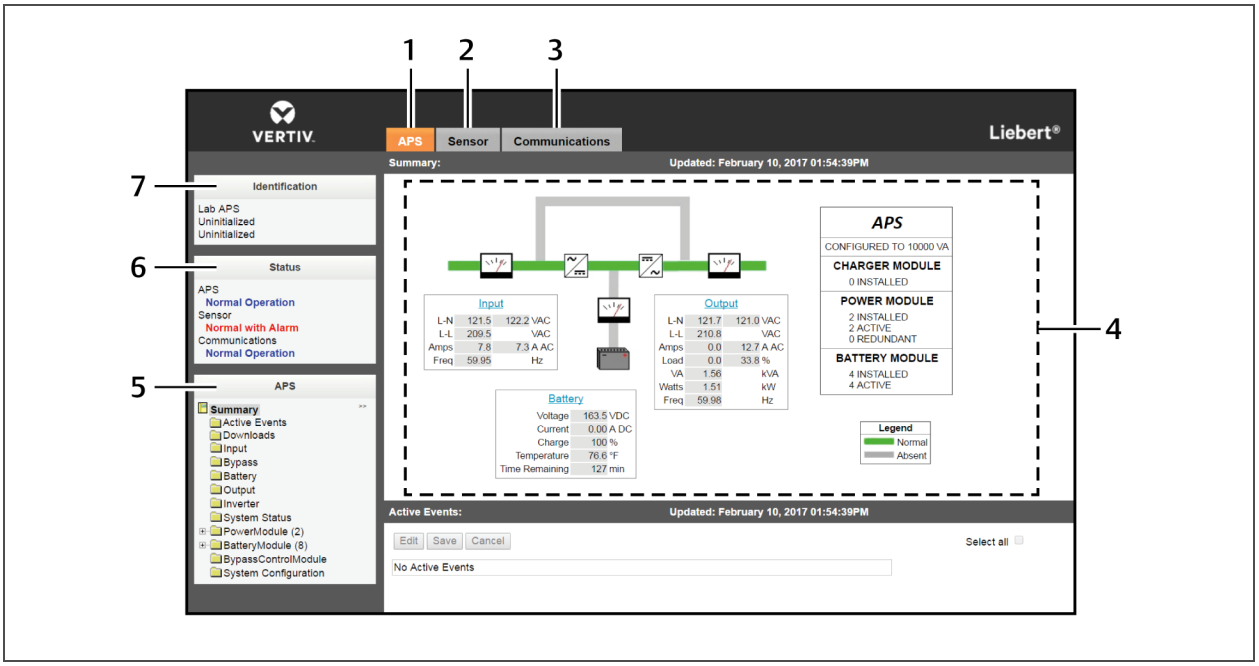
NOTE: The Edit button is grayed-out if the settings on a menu cannot be changed.

5.1 Web Page Sections

Each Unit card has a Web-page user interface (Web UI) with the following areas, see Figure 4.1 below.

- Identification panel
- Status panel
- Tab menu panel
- Detail area

Figure 4.1 Web page sections



ITEM	DESCRIPTION
1	Managed-device tab displays nformation about the monitored and controlled equipment. Refer to Managed Device Tab Menus on the facing page for details. The tab label names the type of Liebert unit in which the card is installed. For example, the Managed Device tab for a card installed in a Liebert APS UPS is labeled "APS" (see **Figure 4.1** on the previous page).
2	Sensor tab displays information about Liebert SN sensors, if installed, including status or data from each sensor and sensor-configuration settings. When sensors are connected to the card, the Sensor tab appears between the Managed Device tab and the Communications tab. The tab does not display when no sensors are connected to the card. Refer to Sensor Tab Menu on page 26 for details.
3	Communications tab displays information about the Unity card, such as the overall event status of the equipment and communication interface, logs of third-party information, communication settings, third-party protocol settings and system status. Refer to Communications Tab Menu on the facing page for details.
4	Details area displays detailed information about the device based on the menu selection made in the Tab Menu area. Edits to the device and its configuration are made in this section.
5	Selected-tab menu. By default, the Web UI always displays two tabs, the managed-device tab and the Communications tab. A third tab, the Sensor tab, appears if Liebert SN sensors have been installed.
6	Status panel displays the status of the monitored equipment, the Unity card, and any Liebert SN sensors connected to the card.
7	Identification panel displays the System Name, System Location, and System Description.

5.2 Help Text

Each Web page shown by the Unity card has informational text that is revealed by hovering the cursor over the icon to the left of the Status, Events or Settings row.

The Web UI may display any of the 6 icons described in the following table.

Table 4.1 Help text and icons

ICON	DESCRIPTION
	Event Normal
	Event Information
	Event Alarm
	Event Warning
	Event Critical
	Tool Tip

5.3 Managed Device Tab Menus

Menus on the Managed Device tab list only data that is relevant to the monitored equipment. For example, menus shown by a Unity card installed in a UPS differ from menus shown by a card installed in Thermal Management equipment. Selected menu items also display detailed information based on the equipment in which the card is installed. Power information is displayed in the Managed Device tab for a UPS, while environmental information is displayed for a thermal-management unit.

5.4 Communications Tab Menu

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

Table 4.2 Communication-tab menus

MENU	DESCRIPTION	SEE DETAILS:
Active Events	Displays the current event activity	Active Events Folder on page 29
Downloads • Agent (or Unity Card) Logs • Event Logs • Data Logs • Other files	Downloading files to text-accessible, comma-delimited or tab-delimited files ease troubleshooting.	Downloads Folder on page 29
Configuration • System • Users • Remote Authentication • Network • Web Server • LIFE • Remote Services • Velocity Protocol • Messaging	Displays information about the system setup, access, network connections, Velocity Protocol settings and whether email and SMS messaging are enabled	Configuration Folder on page 30
Protocols • Modbus • BACnet • SNMP • YDN23	Lists information and settings related to available third-party protocols employed to monitor equipment.	Protocols Folder on page 53

Table 4.2 Communication-tab menus (continued)

MENU	DESCRIPTION	SEE DETAILS:
Status • System Status • System Restart Required • LIFE™ device identity changed-LIFE™ needs to be reconfigured • RS-485 Port Conflict • Duplicate Velocity Protocol MSTP Node ID • Duplicate BACnet MSTP Node ID	Shows the overall condition of the system and whether a restart is needed to activate configuration changes; restart is performed only from the Support Folder	Status Folder on page 59
Support • Agent time and Date • Agent Model • Agent App Firmware Version • Agent App Firmware Label • Agent Boot Firmware Version • Agent Boot Firmware Label • Agent Serial Number • Agent Manufacture Date • Agent Hardware Version • GDD Version • FDM Version • Product Sequence ID • Restart Card • Reset Card to Factory Defaults (see NOTE below) • Generate and download diagnostic file • Firmware Update • Active Networking	Shows information needed for maintenance or troubleshooting and shortcuts to reboot the card, reset the Unity card to its factory defaults and to update the card's firmware.	Support Folder on page 60 (Firmware Update also on)

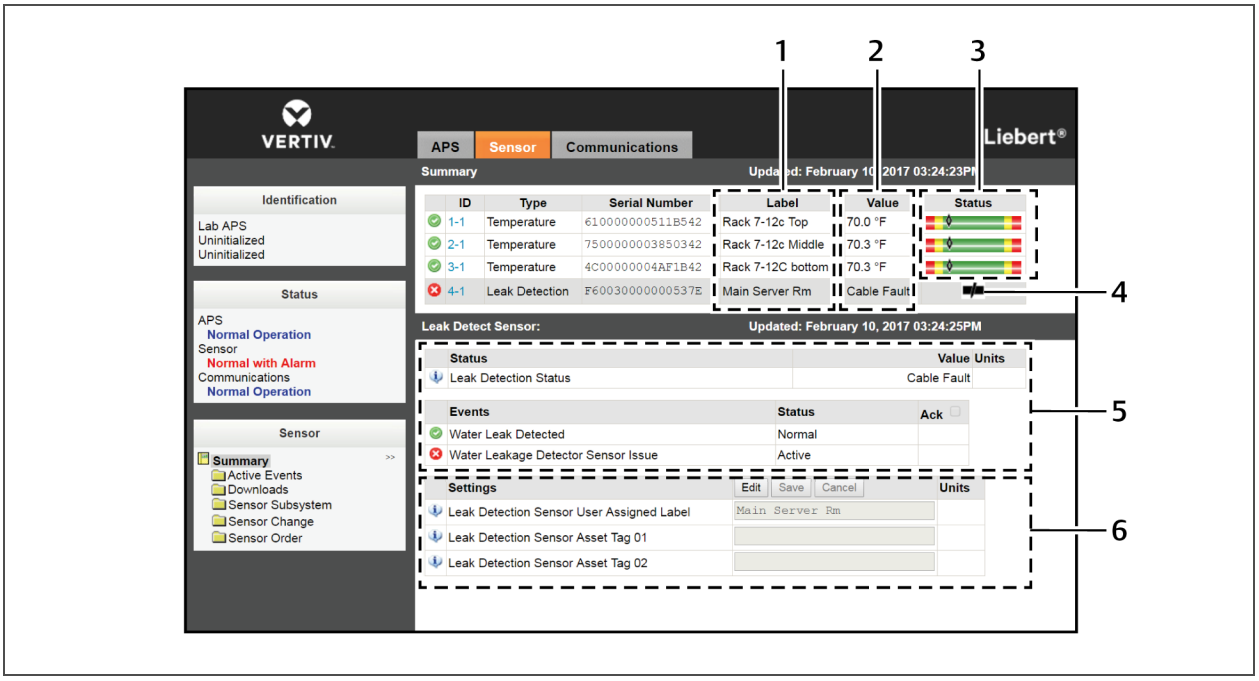
NOTE: The card may be reset to factory defaults manually using the reset button, see Manually Resetting to Factory Defaults on page 67.

5.5 Sensor Tab Menu

NOTE: Shown only if a sensor is connected.

When Liebert SN sensors are installed and connected to the sensor port on the Unity card, the Sensor tab appears.

Figure 4.2 Sensor-tab Summary page



ITEM	DESCRIPTION
1	User-assigned labels for sensor identification/location
2	Actual sensor-reading values
3	Graphs indicate sensor readings in relationship to thresholds.
4	Icons indicate sensor status readings for example: cable fault or door open/closed depending on sensor function.
5	Sensor details—data for sensor selected in the summary list.
6	Sensor settings—editable data/configuration for sensor selected in the summary list.

The Sensor menu contains folders showing an overview of the installed sensors, the event status of the sensors, download links for log files and sensor-configuration settings described in the following table.

Table 4.3 Sensor-tab menu folders

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

5.5.1 Sensor-tab Summary Page

The Sensor tab Summary Page shows the status of all installed sensors, details about selected sensor and a Setting pane that permits changing a sensor's label, thresholds if applicable, alarm configuration and acknowledging alarms and events. See Figure 4.2 on the previous page.

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

Events may also be acknowledged on this window.

5.5.2 Sensor-tab Summary Details Pane

The Details pane of the Sensor tab appears when the Summary folder is selected. The area shows the status of all connected sensors. See Figure 4.2 on the previous page.

Supported sensors include:

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

When a sensor is selected, the details for that sensor display in this pane. The content of the details section is specific to the type of sensor selected. For example, a temperature sensor shows the temperature readings and a door sensor shows whether or not the door is open.

The Unit of Measure used for temperature values is defined in the Display Temperature Units setting on the Communications tab. See System Folder on page 30.

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

5.5.3 Changing Sensor Order

Sensors are listed in the order they are installed. You can change the order to put sensors deemed more-important at the top of the list.

To change the order of the sensor list:

1. On the Sensor tab, click *Sensor Order*.
2. Click *Edit*, and enter the user name and password.
3. Select the radio button for the sensor to move.
4. Use the arrows at the right of the list to move the sensor up or down.
5. Click *Save*.

6 EDITING THE UNITY CARD CONFIGURATION

The Web UI can be used to configure the settings for the Unity card and for the monitored equipment. The following steps apply to making changes to all configuration settings.

To edit the configuration:

1. Open a Web browser and enter the card's IP address.
2. Click the Communications tab.
3. In the tab menu, select the folder that contains the configuration setting to change.
4. Click *Edit*, and enter a user name and password if necessary.
5. Change the settings.
6. Click *Save* to apply the changes or *Cancel* to discard them.

6.1 Communications Tab Menu Folders

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

- Active Events Folder below
- Downloads Folder below
- Configuration Folder on the next page
- Protocols Folder on page 53
- Status Folder on page 59
- Support Folder on page 60

6.2 Active Events Folder

The Active Events folder contains no configurable settings. The folder displays events that affect the Unity card.

6.3 Downloads Folder

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

6.4 Configuration Folder

The top level Configuration folder displays the System Model Number of the Unity card. This name is factory-set and cannot be changed. The Configuration folder contains the following subfolders:

- System Folder below
- Local Users Folder on the facing page
- Remote Authentication Folder on the facing page
- Network Folder on page 37
- Web Server Folder on page 39
- LIFE™ Folder on page 43
- Remote Services Folder on page 45
- Velocity Protocol Folder on page 47
- Messaging Folder on page 48
- Cloud Client Folder on page 52

6.4.1 System Folder

The System subfolder displays general information about the monitored and managed device. You can select the temperature units displayed, which is "Celsius" by default.

To edit the information displayed:

1. Click *Edit*, and enter a user name and password if necessary.
2. Make the changes, and click *Save*.

Time Service Settings

The System subfolder contains the Time Service folder. Each setting offers a menu of choices or an enable/disable check box.

Time Service setting options

External Time Source

The external source to use for time synchronization. Default = NTP Server.

Primary NTP Time Server

URL, Hostname, or IP address of the primary NTP time source. 64-character maximum.

Backup NTP Time Server

URL, Hostname, or IP address of the back-up NTP time source. 64-character maximum.

NTP Time Sync Rate

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

Time Zone

Time zone where the device is located.

Enable Auto-Sync to Managed Device

Enable automatic writing time to the managed device.

Managed Device Auto-Sync Rate

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

6.4.2 Local Users Folder

The Local Users subfolder offers up to 10 users and 3 access levels described in Table 5.1 below.

The default password for all users is *Liebert* (case-sensitive).

Table 5.1 User-access Levels

LEVEL NAME	ACCESS/ PERMISSION TYPE	DESCRIPTION
No Access	None	The No Access level is enforced when "Password Protected Site" is enabled.
General User	Read-only	Able to view all tabs, folders and sub-folders of the user-interface. A General User will only need to enter the assigned password if "Password Protected Site" is enabled, see Web Server Folder on page 39. By default, Local User [2] is *User* with the default password *Liebert* (both are case-sensitive). The Authorization (access type) for Local User [2] is "General User."
Administrator	Read/Write	Able to edit settings using the assigned password, which is always required to edit settings/configuration. By default, Local User [1] is *Liebert* with the default password *Liebert* (both are case-sensitive). The Authorization (access type) for Local User [1] is "Administrator." Be sure that you always have one administrator user, so you can access and modify configuration and other settings.

IMPORTANT! Record user names and passwords and save them in a secure place where they can be found if forgotten. A lost password cannot be retrieved from the IS-UNITY card. If the administrator password is lost, the card must be reset to factory defaults and reconfigured.

To change the user names and passwords:

NOTE: 30-character maximum. All printable characters are valid except: \ : ' < > ~ ? " #

1. On the Communications tab, select *Configuration* > *Local Users*, then select the folder of the user to configure.
2. Click *Edit* and enter the administrator user name and password, then click *OK*.
3. Enter a new user name and password.
4. Re-enter the password to confirm it.
5. In *Authorization for User*, select the type of access, see Table 5.1 above.
6. Click *Save* to confirm the changes or *Cancel* to discard them.

6.4.3 Remote Authentication Folder

The top level of the Remote Authentication subfolder displays the configured authentication type. The implementation provides authentication and authorization at the remote server.

The folder contains subfolders for authentications types:

- RADIUS Authentication below
- LDAP Authentication on the facing page
- TACACS+ Authentication on page 35
- Kerberos Authentication on page 37

RADIUS Authentication

Authentication and authorization is provided by the remote RADIUS server.

RADIUS Settings

[Enable/Disable selection]

Enables RADIUS authentication in the card.

Primary Authentication Server

IP address of primary authentication server.

Secondary Authentication Server

IP address of secondary authentication server.

Secret

The shared secret that serves as a password between the client and the server.

Timeout

Time in milliseconds between authentication retries. Range: 0 to 65535

Retries

Number of times to attempt contact before trying a different server.

Server Configuration Requirements for RADIUS Authentication

The value for **Filter-Id** must be

```
unity_group=unityadmin;
```

– or –

```
unity_group=unityuser;
```

- The attributes are in a config file or a GUI interface depend on the authentication server implementation.
- The **unity_group=unityuser;** can be used in the same manner as **unity_group=unityadmin;** .
- The **unity_group=unityadmin;** and **unity_group=unityuser;** string must be terminated with a semicolon.

LDAP Authentication

Authentication and authorization is provided by the remote LDAP server.

NOTE: If you are using an out-of-the-box Linux OpenLDAP installation, you must add the "Info" attribute to specify the Unity-group authorization, or the LDAP authorization will not work. See Adding "Info" Attribute to LDAP Schema for Linux OpenLDAP on the next page.

LDAP Settings

[Enable/Disable selection]

Enables LDAP authentication in the card.

LDAP Server

IP address of LDAP server.

LDAP Base

Base Distinguished Name, the path to the LDAP user accounts.

LDAP Secure

SSL mode.

Database UserName

Bind Distinguished Name, the service account used to access the LDAP server.

Database Password

Password for the service account that accesses the LDAP server.

Login Attributes

Account attribute that authenticates the user credentials, for example: CN.

Server Configuration Requirements for LDAP Authentication

The value for **info** must be

```
unity_group=unityadmin;
```

– or –

```
unity_group=unityuser;
```

- The attributes are entered into a config file or a GUI interface depending on the authentication server implementation.
- The **unity_group=unityuser;** can be used in the same manner as **unity_group=unityadmin;** .
- The **unity_group=unityadmin;** and **unity_group=unityuser;** string must be terminated with a semicolon.

Adding "Info" Attribute to LDAP Schema for Linux OpenLDAP

The Unity card obtains group authorization information from a remote LDAP server for an LDAP user via the “Info” attribute in the user’s remote LDAP user account. The “Info” attribute specifies group authorization using “unity_group=<x>;” where <x> is “unityadmin” or “unityuser”. However, the user account of an out-of-the-box Linux OpenLDAP installation does not provide the “Info” attribute so remote LDAP support will not work until support for the “Info” attribute is added to LDAP user accounts.

The LDAP schema for a Linux OpenLDAP installation is defined and exists at “/etc/ldap/schema.” The LDAP schema for a user account exists in the “nis.ldif” file and is specified in an objectClass named “posixAccount.”

Add the the “Info” attribute as a member of “posixAccount” MUST attribute so that it is always considered for specifying for a user. The “Info” attribute already exists in the LDAP schema, but it is not assigned to anything in the default schema.

To add the "Info" attribute on a brand new OpenLDAP installation:

Before starting OpenLDAP, refer to the following to edit the “nis.ldif” file:

Original “posixAccount” object schema:

- olcObjectClasses: (1.3.6.1.1.1.2.0 NAME 'posixAccount' DESC 'Abstraction of an account with POSIX attributes' SUP top AUXILIARY MUST (cn $ uid $ uidNumber $ gidNumber $ homeDirectory) MAY (userPassword $ loginShell $ gecos $ description))

Updated “posixAccount” object schema with the “Info” attribute added:

- olcObjectClasses: (1.3.6.1.1.1.2.0 NAME 'posixAccount' DESC 'Abstraction of an account with POSIX attributes' SUP top AUXILIARY MUST (cn $ uid $ uidNumber $ gidNumber $ homeDirectory $ Info) MAY (userPassword $ loginShell $ gecos $ description))

To add the "Info" attribute on an existing OpenLDAP installation:

Use “ldapmodify” or other LDAP administrator tool to add the “Info” attribute to the user accounts.

TACACS+ Authentication

Authentication and authorization is provided by the remote TACACS+ server.

TACACS+ Settings

[Enable/Disable selection]

Enables TACACS+ authentication in the card.

Primary Authentication Server

IP address of the primary TACACS+ server.

Secondary Authentication Server

IP address of the secondary TACACS+ server.

Secret

The shared secret that serves as a password between the client and the server.

Timeout

Time in milliseconds between authentication retries. Range: 0 to 65535

Retries

Number of times to attempt contact before trying a different server.

Version

Minor version.

Server Configuration Requirements for TACACS+ Authorization

The config file contains the **unity_group=unityadmin;** string in the **raccess** field.

```
user = tacacsAdmin {

service = raccess {

unity_group=unityadmin;

}

}
```

– or –

The config file contains the **unity_group=unityuser;** string in the **raccess** field.

```
user = tacacsAdmin {

service = raccess {

unity_group=unityuser;

}

}
```

- The attributes are in a config file or a GUI interface depend on the authentication server implementation.
- The **unity_group=unityuser;** can be used in the same manner as **unity_group=unityadmin;** .
- The **unity_group=unityadmin;** and **unity_group=unityuser;** string must be terminated with a semicolon.

Kerberos Authentication

Kerberos Settings

[Enable/Disable selection]

Enables Kerberos authentication in the card.

Server (Realm)

IP address of the Kerberos server.

Realm Domain Name

Name of the realm of systems that share the Kerberos database.

Domain Name

Domain where Kerberos database resides in the master system..

6.4.4 Network Folder

The top level of the Network subfolder displays the following:

Speed Duplex

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

Hostname

Identifies the network node. Default = UNITY-*serial_number_of_card*.

Domain Name Suffix List

Listing of domain name suffixes for resolution of host names. If it requires changing, contact the system administrator for the proper setting.

Telnet Server

Enables/Disables telnet access to the card to prevent unauthorized changes. The default setting disables telnet access.

SSHv2 Server

Enables/Disables SSHv2 (Secure SHell) access to the card to prevent unauthorized changes. The default setting disables SSHv2 access.

The Network folder also contains subfolders related to communication:

- IPv4 and IPv6 Folders on the next page
- Domain Name Server (DNS) Test Folder on page 39

IPv4 and IPv6 Folders

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

IPv4 Settings

IPv4 Protocol

Enables IPv4 in the card

IP Address Method

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

Static IP Address

Network address for the interface

Subnet Mask

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

Default Gateway

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

DNS Server Address Source

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

Primary DNS Server

Network address of the primary DNS server.

Secondary DNS Server

Network address of the secondary DNS server.

IPv6 Settings

IPv6 Protocol

Enables IPv6 in the card.

IP Address Method

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

Static IP Address

Network address for the interface.

Prefix Length

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

Default Gateway

IP address of the gateway for network traffic destined for other networks or subnets. Default = 64.

DNS Server Address Source

Source of DNS server identification (None, Automatic, Configured). Default = Automatic.

Primary DNS Server

Primary DNS Server

Secondary DNS Server

Secondary DNS Server

Domain Name Server (DNS) Test Folder

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

Domain Name Server (DNS) Test Settings

Last Query Response

Response from a domain name server (DNS) to the last query.

Example: *gxtwebdemo.liebert.com* resolved to *126.4.203.251*

Type of Query

Type of DNS query. (Hostname, IP Address)

Query Value

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

6.4.5 Web Server Folder

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

Web Server Settings

Web Server Protocol

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

HTTP Port

Standard web port not encrypted. Required if HTTP is enabled as Web Server Protocol. Default = 80.

HTTPS Port

Standard secure Web port; all communication is encrypted. Required if HTTPS is enabled as Web Server Protocol. Default = 443.

Password Protected Site

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

Remote Write Access

When enabled, all web browsers have write access to data on all Unity-card web pages when the user is logged-in with Administrator credentials. When disabled, write access is restricted to web browsers connected via IPv4 Auto-configuration address at 169.254.24.7. For additional information, see Connecting Directly to Computer for Configuration on page 4.

NOTE: When Remote Write Access is disabled, an indicator is displayed in the upper right corner of the web page as a reminder, shown in the following figure.

NOTE: Only disable remote-write access if you are absolutely sure that you do not need to administer the managed device or the Unity card through a remote web-browser session. A local direct connection to 169.254.24.7 is required to enable this setting.

Session Idle Timeout

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

Figure 5.1 Remote-write-access-disabled indicator

Certificate Folder

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

Selections in Certificate provide commands to Upload SSL Certificate PEM Files or Generate Self-Signed SSL Certificate.

Certificate Commands

Upload SSL Certificate PEM Files

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

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

Generate Self-Signed SSL Certificate

Generates and installs a new self-signed certificate based on the mode selected for Generate Self-Signed SSL Certificate Mode. See Generating a Self-signed SSL Certificate on page 43.

Certificate Settings

Generate Self-Signed SSL Certificate Mode

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

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

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

Common Name

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

Organization

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

Organizational Unit

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

City or Locality

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

State or Province

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

Country Code

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

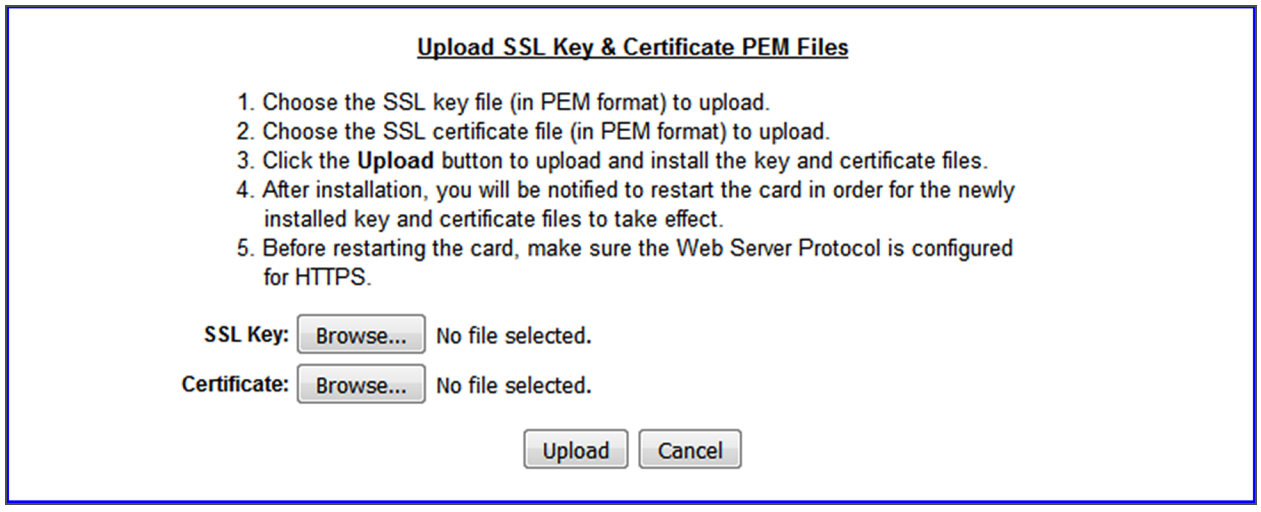
Email Address

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

Uploading SSL Certificate PEM Files

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

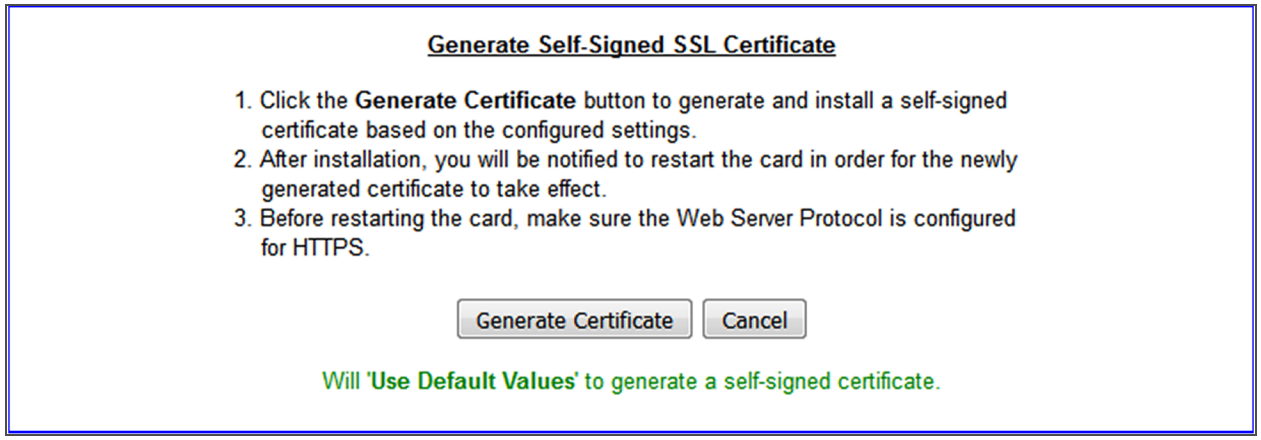
Figure 5.2 Upload SSL Key & Certificate PEM Files dialog



Generating a Self-signed SSL Certificate

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

Figure 5.3 Generate Self-Signed SSL Certificate dialog



6.4.6 LIFE™ Folder

The LIFE subfolder contains settings that affect use of the Vertiv™ LIFE Technology, a remote monitoring and diagnostic service for Vertiv™ units. The LIFE settings are for use by trained Vertiv™ personnel only and require no user changes. The following tables provide reference information about the LIFE settings.

Settings in this folder are managed by Vertiv™. A service contract is required.

For support, contact Vertiv™ Technical Support for LIFE Services at 1-800-435-7250, option 3.

Table 5.2 LIFE Status Settings

STATUS	DESCRIPTION
Connection Media	The LIFE Technology connection media
Enable Date and Time	The date and time that LIFE Technology support was enabled.
Settings	Description
LIFE Technology	Enable or disable the LIFE Technology
System Serial Number Override	When enabled, A user configured System Serial Number will override a Serial Number configured in the device ,

Table 5.2 LIFE Status Settings (continued)

STATUS	DESCRIPTION
System Serial Number	System serial number, obtained from the unit automatically
Site Equipment Tag Number	Site equipment tag number
Site Identifier	Site identifier, entered by the Service Technician
Answer Incoming Call	Enable answering of LIFE Watch Station incoming calls
Next Call Date and Time	Date and Time of next call to make to the LIFE Watch Station server
Call Interval Days	Days between routine calls to LIFE Watch Station
Call Interval Hours	Number of hours between LIFE Watch Station routine calls
Call Interval Minutes	Number of minutes between routine LIFE Watch Station calls. This value is used in conjunction with val_life_callInterval_hours.
Call Trials Number	The number of attempts to retry a call after it fails before rescheduling the call.

Table 5.3 LIFE UPS-state SMS Messaging Configuration

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

6.4.7 Remote Services Folder

The top level of the Remote Services subfolder offers options for remote-service connections.

Settings in this folder are managed by Vertiv™. A service contract is required.

For support, contact Vertiv™ LIFE Services at 1-800-435-7250, option 3.

The folder contains subfolders for connectivity and diagnostics:

- Remote Services Connectivity on the next page
- Remote Services Diagnostics on page 47

Remote Service Options and Settings

Serial number from device

Serial number obtained from the managed device. Identifies the device to the system unless *Device Serial Number Override* is enabled.

Reset Remote Services Config

Resets configuration of the remote service back to factory defaults.

NOTE: Does not reset the communication card configuration.

Remote Service

Enables/Disables remote-servcie connection.

Device Data Sampling

Enables/Disables, data sampling of the device.

Device Serial Number

Serial number used when *Device Serial Number Override* is enabled.

Device Serial Number Override

Enables/Disables use of the serial number obtained from the managed device.

Site Equipment Tag Number

Number from the site equipment tag.

Site Identifier

Site identification number.

Device Instance ID

Manufacturerer's device identification number.

Service Center Country

Country in which the device is serviced.

Remote Services Connectivity

Remote-service Connectivity Options and Settings

Connectivity Test Result

Result of most-recent connectivity test.

Test Connectivity

Initiates connectivity test.

Evaluate Remote Services Configuration

Attempt to connect to the remote service to verify the configuration.

Remote Service platform URL

URL address of the remote-service platform. Do not enter the "http://" or "https://" prefix.

Connection retry time

Length of time to attempt reconnection in the event of a communication failure. Range: 30 to 600 seconds.

Proxy Enable

Enables use of remote-service-platform URL to connect with a proxy server.

Proxy Authentication

Enables authentication of the proxy server.

Proxy Address

IP or URL address of the proxy server.

Proxy IP Port Number

Port number of the proxy server. Range: 1 to 65535.

Proxy User Name

User name of the proxy server.

Proxy User Password

Password of the proxy server.

Remote Service Cloud URL

URL address of the remote-service cloud. Do not enter the "http://" or "https://" prefix.

Remote Services Diagnostics

Remote-service Diagnostic Settings

Communication Status

Results of the most-recent transaction.

Communication Error Count

Number of communication errors since reboot.

Last communications error

Most-recent communication error message since reboot with date and time stamp.

Monitored Device Rule File Information

Details about the remote-service rule file in effect for the monitored device.

Remote Services Operating Status

Status of the remote service.

Managed Device Status

Status of managed device's communication with the card.

6.4.8 Velocity Protocol Folder

Velocity Protocol contains four sub-folders: Managed Device, MSTP, Ethernet and Internal. Velocity is the input protocol from a managed/monitored system.

NOTE: With the exception of changing the node ID when multiple cards are used or when disabling Velocity-Protocol IP access, the settings in the Velocity Protocol sub-folders should not be modified unless directed by a Vertiv™ representative.

NOTE: Liebert® Nform™ requires that IP access to Velocity be enabled.

Velocity Protocol options

Velocity Protocol IP Access

When disabled, prevents access from a remote, IP-based system using the Velocity Protocol. Default = Disabled.

6.4.9 Messaging Folder

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

Messaging options

Email

Is enabled to send email messages about events

SMS

Is enabled to send text messages about events

Email

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

Email Settings

Email From Address

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

Email To Address

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

Email Subject Type

Subject of the email. This value will default to the event description, unless customized by entering Custom Subject Text.

Custom Subject Text

The editable subject of the message. Defaults to event description if nothing is entered.

SMTP Server Address

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

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

SMTP Server Port

SMTP server port. Default = 25.

SMTP Connection

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

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

SMTP Authentication

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

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

SMTP Username

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

SMTP Password

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

Include IP Address in Message

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

Include Event Description in Message

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

Include Name in Message

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

Include Contact in Message

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

Include Location in Message

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

Include Description in Message

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

Include Web Link in Message

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

Enable Event Consolidation

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

Consolidation Time Limit

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

Consolidation Event Limit

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

SMS

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

SMS Settings

SMS From Address

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

SMS To Address

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

SMS Subject Type

Subject of the SMS. Defaults to the event description unless customized using Custom Subject Text.

Custom Subject Text

The editable subject of the message. Defaults to event description if nothing is entered.

SMTP Server Address

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

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

SMTP Server Port

SMTP server port. Default = 25.

SMTP Connection

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

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

SMTP Authentication

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

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

SMTP Username

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

SMTP Password

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

Include IP Address in Message

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

Include Event Description in Message

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

Include Name in Message

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

Include Contact in Message

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

Include Location in Message

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

Include Description in Message

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

Include Web Link in Message

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

Enable Event Consolidation

If checked multiple events will be sent per outgoing message.

Consolidation Time Limit

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

Consolidation Event Limit

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

Messaging Test

Tests the set up for email and SMS messages. If the test fails, incorrect settings should be changed to ensure that the Unity card sends proper notifications if an event should occur.

6.4.10 Cloud Client Folder

NOTE: The Cloud Client configuration is used exclusively by Liebert Mini-Mate Thermal Management Systems. The Cloud Client folder displays only when the device managed by the Unity card is a Mini-Mate unit.

The Cloud Client subfolder enables/disables remote device monitoring for a Liebert Mini-Mate unit by registering the device with the cloud client that manages device-status monitoring for Liebert iCOM CMS mobile-application users.

Cloud Client Status options

Cloud Client UUID

Unit identifier for the Unity card that associates the card and the cloud service. The identifier is internally generated, but displays here and in the cloud service administration portal.

Unit Name

Descriptive name for the Mini-Mate unit, populated based on the System Name. See System Folder on page 30, to configure the System Name and other device-specific information.

NOTE: The System Name must be configured before registering the unit with the cloud client.

Token

Unique identifier provided by the cloud service that confirms registration. If the unit is not registered, the field displays "Client Not Registered."

Cloud Client Settings options

Cloud Client Enable

Enables/Disables registration of the Mini-Mate unit with the cloud service.

Email Address

Customer e-mail address associated with the customer's organization within the cloud service. The organization is based on the domain portion of the e-mail address.

Registration Key

Unique key pre-programmed at the factory that identifies the Mini-Mate unit/Unity card for the cloud service.

Cloud Service URL

The address for the cloud service administration portal, through which mobile-app users are managed. The default URL is https://icomcms.com.

6.5 Protocols Folder

The Protocols folder displays the types of protocols that may be enabled for a Unity card to communicate with management systems such as BMS, NOC, and so on. Not all protocols are available at the same time, for example: Modbus RTU and BACnet MSTP cannot be used at the same time because there is one RS-485 port used for the output protocol. The card allows two third-party protocols to be enabled.

NOTE: To enable and configure the Vertiv™ Velocity protocol, see Velocity Protocol Folder on page 47.

Settings in each of the subfolders configure the selected protocols:

BACnet, See:

- BACnet IP Folder on the next page
- BACnet MSTP Folder on the next page

Modbus, see:

- Modbus TCP Folder on page 55
- Modbus RTU Folder on page 55

SNMP, see:

- SNMPv3 User Folder on page 57
- SNMPv1 Trap Folder on page 58
- SNMPv1/v2c Access Folder on page 59

YDN23, see YDN23 Folder on page 59.

6.5.1 BACnet Folder

BACnet Settings

Managed Device Write Access

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

BACnet Interface

BACnet server interface: BACnet IP or BACnet MSTP.

Device Object Instance Number

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

Device Object Name

The name of the BACnet server's device object.

APDU Timeout

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

APDU Retries

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

BACnet IP Folder

BACnet IP Settings

BACnet IP Port Number

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

Register as Foreign Device

Enable or Disable registration as a foreign device.

IP Address of BBMD

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

Foreign Device Time-to Live

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

BACnet MSTP Folder

BACnet MSTP Settings

Node ID

The BACnet server's MS/TP node ID (MAC). Must be unique for each node on the communication bus.

Data Rate

The BACnet MSTP communication rate (bits per second).

Max Master Address

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

Max Info Frames

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

6.5.2 Modbus Folder

Modbus Settings

Managed Device Write Access

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

Modbus Interface

Select the Modbus interface, either Modbus TCP or Modbus RTU

Modbus TCP Folder

The Modbus TCP permits connection to the card by:

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

Modbus TCP Settings

Limit Network Access Type

IP Access List

- Open
- Same Subnet
- Trusted IP List

Port

The TCP port used by the Modbus Server to listen for and respond to Modbus protocol requests. Default = 502.

Maximum Client Connection Count

Maximum number of simultaneous connections allowed. Range: 1 to 5.

Modbus RTU Folder

Modbus RTU Settings

Node ID

Modbus Server ID for the interface; obtain from network administrator. Must be unique for each node on the communication bus.

Baud Rate

Communication rate.

- 9600
- 19200
- 38400

Parity Check

The communication parity check.

- None
- Even
- Odd

6.5.3 SNMP Folder

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

SNMP Settings

SNMPv3 Engine ID

The generated SNMPv3 engine ID.

NOTE: The engine ID is based on the MAC address of the card by default.

SNMP v1/v2c Enable

Enable or Disable SNMP v1/v2c.

SNMP v3 Enable

Enable or Disable SNMPv3.

Authentication Traps

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

Heartbeat Trap Interval

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

RFC-1628 MIB

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

RFC-1628 MIB Traps

Enable or Disable support for sending RFC-1628 traps. The RFC-1628 MIB must be enabled for RFC-1628 traps to operate.

These traps apply only to UPS systems.

Liebert Global Products (LGP) MIB

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

LGP MIB Traps

Enable or Disable support for Liebert Global Products MIB traps. The LGP MIB must be enabled for LGP traps to operate.

LGP MIB System Notify Trap

Enable or Disable support for the LGP System Notification trap. This is a single trap sent each time an alarm or warning is added or removed from the conditions table. It provides a text description of the event in a varbind of the trap message. The LGP MIB must be enabled for LGP Notify traps to operate.

SNMPv3 Engine ID Format Type

Selects method to build the engine ID. Valid values:

- MAC Address (default) = Engine ID built from the Unity card's MAC address.
- Text = Engine ID built from text entered in SNMPv3 Engine ID Text. See Select SNMPv3 Engine ID Format on page 15.

SNMPv3 Engine ID Text

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

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

SNMPv3 User Folder

The Unity card supports up to 20 SNMPv3 users and offers advance security including authentication and encryption. The top-level page is a table with settings for all 20. The page displays a link to edit the table columns displayed for each SNMPv3 user. The same settings may be accessed by clicking on a folder for a user, such as SNMPv3 User [1].

To display the settings, click on any of the SNMPv3 User links. After making any changes, click **Save** to make the changes effective.

SNMPv3 User Settings

SNMPv3 User Enable

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

SNMPv3 Username

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

SNMPv3 Access Type

Read Only, Read/Write or Traps only

SNMPv3 Authentication

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

SNMPv3 Authentication Secret

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

SNMPv3 Privacy

Cryptographic algorithm used for encryption. Options are:

- None
- DES
- AES

SNMPv3 Privacy Secret

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

SNMPv3 Trap Target Addresses

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

SNMPv3 Trap Port

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

Editing the SNMPv3 Table

You can configure the amount of information displayed he table on the SNMPv3 User Settings [20] page.

1. Above the table, click *Click here to edit columns displayed in this table*.
2. Check the boxes next to the information to include in the table.
   The choices let you show the same information in this screen as that displayed when folder or link for a specific user is selected.

SNMPv1 Trap Folder

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

SNMPv1 Trap Settings

SNMP Trap Target Addresses

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

SNMP Trap Port

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

SNMP Trap Community String

String identifying a 'secret' known only by those hosts that want to be notified of device status changes. Default: public (case-sensitive).

SNMPv1/v2c Access Folder

This page contains settings for network hosts that access data using SNMPv1/v2c. Up to 20 access hosts can be enabled and configured. Port 161 is required as the default SNMP trap port to receive alarms. Like the SNMPv3 pages, the setting for each host may be reached by clicking the links in the data portion of the page or by clicking the folders for the access hosts. Also, data shown in the table may be changed by clicking the link above the table.

SNMPv1/v2c Access Settings

SNMP Access IP Address

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

SNMP Access Type

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

SNMP Access Community String

String identifying a 'secret' to allow read-only or write-only access. The default is read-only acciess: public (case-sensitive). Write-only access: private (case-sensitive).

6.5.4 YDN23 Folder

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

YDN23 Protocol settings

Managed Device Write Access

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

Device Address

YDN23 device address

Baud Rate

The communications rate in bps.

6.6 Status Folder

The Status folder contains no configurable items. It displays the System Status of the Unity card and a list of events that affect the card's status. Status is also indicated by the icons next to the items. See Help Text on page 23 for a description of the icons.

6.7 Support Folder

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

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

Support Folder Settings

Agent Date and Time

Date and time setting for the card.

Agent Model

The card's model (Unity Platform)

Agent App Firmware Version

The card's firmware version (2.0 or higher)

Agent App Firmware Label

The card's firmware label

Agent Boot Firmware Version

The card's Boot firmware version

Agent Boot Firmware Label

The card's boot firmware label

Agent Serial Number

The card's serial number

Agent Manufacture Date

The card's manufacture date

Agent Hardware Version

The card's hardware version

GDD Version

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

FDM Version

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

Product Sequence ID

The card's product sequence identifier

Commands

Enable/Cancel

Restart Card

Restart card and implement configuration changes

Reset Card to Factory Defaults

Reset the card's configuration to its factory defaults

Generate and download diagnostic file

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

6.7.1 Active Networking Folder

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

Active Networking Parameters

Ethernet MAC Address

Ethernet MAC Address for the Liebert IntelliSlot card

IPv4 Address

Presently used IPv4 network address

IPv4 Default Gateway

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

Primary DNS

Presently used IPv4 Primary DNS

Secondary DNS

Presently used IPv4 Secondary DNS

Last DHCP/BOOTP Address

Last known IPv4 address assigned by DHCP

Last DHCP Lease

Lease time of last known DHCP address

IPv6 Global Address

Shows if DHCPv6 or Static address is presently being used

StateLess Address AutoConfiguration

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

Link Local

Presently used IPv6 Link Local Address

IPv6 Default Gateway

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

Primary DNS Server

IPv6 Primary DNS

Secondary DNS Server

Presently used IPv6 Secondary DNS

Last DHCPv6

Last known IPv6 address assigned by DHCPv6

Last DHCPv6 Lease

Lease time of last known DHCPv6 address

6.7.2 Firmware Update Folder

The Unity card has two areas in flash memory for the firmware and the configuration. One area currently operates on the card. The other area is the previous firmware on the card and is considered to be an alternate image.

The folder supports updating the firmware of the Unity card or reverting to a previous version. If the firmware has not been updated, then the previous version/configuration is not available to revert.

NOTE: If downgrading firmware to a previous version, a reset to factory defaults occurs if there are feature in the current version that are not present in the older version. However, if downgrading using an alternate image, no reset occurs.

Firmware Update settings

Current Firmware Version

The version of the firmware running on the card

Current Firmware Label

The label of the firmware running on the card

Current Firmware Date

The build date of the firmware running on the card

Alternate Firmware Version

The version of the alternate (previous) firmware

Alternate Firmware Label

The label of the alternate (previous) firmware

Alternate Firmware Date

The build date of the alternate (previous) firmware

Firmware Commands

Run Alternate Firmware

Return the card's firmware to the alternate (previous) version.

Firmware Update

Update the card's firmware to a new/different version.

Updating the Card Firmware

For description of the field and folders used when updating, see Firmware Update Folder on the previous page.

To update the firmware on the Unity card:

1. On a computer, download the latest Unity-card firmware from https://www.vertivco.com/en-us/support/software-download/monitoring/liebert-intellislot-communications-interface-cards/.
   - If you know the card's IP address, type the IP address in a web browser.
   - If you do not know the IP address, connect the card to a computer with an Ethernet cable and open a web browser, see Connecting Directly to Computer for Configuration on page 4.
     The card has an Ethernet RJ-45 connector on the front, see Figure 1.1 on page 1.
     When directly connected, the card and computer automatically negotiate communications, which takes about 1 minute. When communication is established, open a web browser and enter the address *169.254.24.7*, which is the card's default Autoconfiguration IPv4 Address.
     The card's Web UI will open.
2. On the Communications tab, select *Support* > *Firmware Update* in the tab menu on the left panel.
3. Click *Edit* and enter the administrator user name and password.
4. Click *Web*.
   The firmware-update screen opens.
5. Browse to the firmware file that was downloaded in Step 1 to update, select it, and click *Update Firmware*.

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

Reverting to Alternate (Previous) Firmware

When a card's firmware is updated, the previous firmware and configuration are moved to the alternate area. You can restore the firmware version and configuration that are kept in the alternate area.

1. On the Communications tab, select *Support* > *Firmware Update* in the tab menu on the left panel.
2. Click *Edit* and enter the administrator user name and password.
3. Click *Run Alternate*.
   A confirmation dialog opens.
4. Click *OK*.
   The card reboots. After reboot, the card is running the previous version of the firmware and configuration. The replaced firmware and configuration are now stored in the alternate area.

6.7.3 Configuration Export/Import Folder

Unity configuration settings may be saved to a local disk or USB drive , and the saved files may be imported to restore the configuration is the card is reset/replaced and to transfer settings to another card.

Configuration Export/Import options

Export configuration file

Saves the Unity-card configuration, which may be edited and used to import common settings to other Unity cards. See Exporting and Modifying a Configuration File on page 66, and About the Exported Configuration File below.

Import configuration file

Loads the Unity-card configuration contained in a modified export file or a created file. The import file is typically used to deploy common card settings. See Importing a Configuration File on page 67.

About the Exported Configuration File

An exported configuration file contains all the configuration settings of the card's Communication tab. Managed-device settings, such as UPS or thermal-management system are not included.

Security Considerations

Passwords and other secrets are not exported. Protected values are shown as asterisks and the lines are commented-out. To use the file as a complete, importable back-up file, you must replace the asterisks (*) with your password/secret values and un-comment the lines. You can also reference the header of the export file for additional details.

NOTE: Do not import an un-modified export file from one card to another. This could cause a duplicate IP address or other unintended duplications.

NOTE: If you add sensitive data such as passwords to the file, we recommend that you use an HTTPS connection when importing to ensure that the file is encrypted when transmitted.

General Format

The exported file is self-describing using commented lines and includes the following format designations:

- # precedes comments.
- Settings and their values are not commented.
- A colon (:) separates the setting and value.
- Double quotes (") enclose all text-based values
- Numeric and enumerated values are not enclosed in double quotes
- Brackets ([ ]) indicate the folder that contains the settings
- User password and other secrets are hidden in the export file, and the line is commented to prevent inadvertent import. To import a new password or other secret, un-comment the line and enter the new password. Because this is a text string, it must be enclosed in double quotes (").

Figure 5.4 File-format Examples (example lines are bold)

Text

```
[System]
# System Name
# End user assigned name for the
system
# maximum length: 64
System Name: "GXT4"
# Contact Information
# End user assigned contact
information for the system
# maximum length: 50
Contact Information: "IT Manager"
```

Enumerated

```
[Time Service]
# External Time Source
# The external source to use for
time synchronization.
# 0: NTP Server
# 1: Modbus System
# 2: BACnet System
# 3: Velocity Management System
# 4: LIFE (TM) Watch Station
# 5: YDN23 System
# 6: Remote Services System
External Time Source: 0
```

Numeric

```
# Timeout
# The timeout for an
   authentication query to be
   answered.
# range: 0 to 65535 sec
Timeout: 3
# Retries
# The number of times a RADIUS
   server is tried   before another
   is contacted.
# range: 0 to 65535
Retries: 2
```

Secure

```
[Local User.1]
# User Name
# Case sensitive string containing
   printable ASCII characters
   excluding: \:'<>~?#, double
   quote, and space
# maximum length: 30
# minimum length if not blank*: 1
# *This setting can be cleared with
   a blank string.
User Name: "Liebert"
# User Password
# Case sensitive string containing
   printable ASCII characters
   excluding: \:'<>~?#, double
   quote, and space
# maximum length: 30
# minimum length if not blank*: 1
# *This setting can be cleared with
   a blank string.
# ** Protected value not displayed.
   Uncomment following line to
   import new value:
# User Password: "********"
# Authorization for User
# User access privilege level - No
   Access, General User,
   Administrator
```

Exporting and Modifying a Configuration File

The exported file is text format (.txt) saved to the default folder created by the web browser, which is typically the "Downloads" folder on MicroSoft Windows devices. The file is named with the prefix "config_" followed by MAC address, Year, Month, Day, and Time. This is included so that the file is uniquely identifiable. See About the Exported Configuration File on page 64, for security and format details.

1. On the Communications tab, select *Support* > *Configuration Export/Import*.
2. Click *Enable* and enter a user name and password.

3. Click *Export*.
   The .txt file is saved to the web browser's default down-load folder.
4. To prepare the file to use for import:
   - Save the file on a computer or network folder.
   - Open the file in a text editor, and un-comment the line containing password/secret data (remove #).
   - Delete the asterisks (*****), and replace with the password/secret value in double quotes (").
   - An imported file need only contain the data to add or update, and does not require comments. Remove (delete) the content that is not needed.
   - Save the edited file.

Importing a Configuration File

An imported configuration file is typically used to back-up the configuration of a card or to configure many cards for with a common configuration.

If the export file will be used as a back-up, all of the passwords and secrets must be manually restored.

NOTE: Do not import an un-modified file. This could cause a duplicate IP address or other unintended duplications.

In addition, the import file does not require comments, and needs only the date to update. For example, you can change only the system name or a network address by editing the configuration file to contain only those lines.

To import a configuration file:

1. On the Communications tab, select *Support* > *Configuration Export/Import*.
2. Click *Enable* and enter a user name and password.
3. Click *Import* and follow the instructions on the import dialog.

6.7.4 Manually Restarting the Card

1. Locate the small hole on the front of the card that contains the reset button, see Figure 1.1 on page 1.
2. Insert a straight, non-conductive tool into the small hole and press-and-hold for 5 seconds. The card restarts without resetting it to factory defaults. To reset to factory defaults, see Manually Resetting to Factory Defaults below.

6.7.5 Manually Resetting to Factory Defaults

1. Locate the small hole on the front of the card that contains the reset button, see Figure 1.1 on page 1.
2. Insert a straight, non-conductive tool into the small hole and press 5 times. Each press should be 1 to 2 seconds long and must be completed within 10 seconds.
   The card is reset to factory-default configuration.

CAUTION: Do not press-and-hold the button too long. Pressing and holding for 5 seconds restarts the card without resetting to factory defaults.

This page intentionally left blank


VERTIV.

VertivCo.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

SL-52645_REV11/590-1305-501E