



Liebert® IntelliSlot™ RDU120 Communications Card

Installer/User Guide

2.0.1

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 result from use of this information or for any errors or omissions.

Refer to local regulations and building codes relating to the application, installation, and operation of this product. The consulting engineer, installer, and/or end user is responsible for compliance with all applicable laws and regulations relation to the application, installation, and operation of this product.

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.vertiv.com/en-us/support/> for additional assistance.

TABLE OF CONTENTS

1 Introduction	1
1.1 Support for Environmental Sensors	2
2 Installation	3
2.1 Installing the Card	3
2.1.1 Connecting Directly to Computer for Configuration	4
2.1.2 Determining the DHCP IP Address	5
2.1.3 Assigning a Static IP Address	5
2.1.4 Connecting an RS-485 Serial Cable	5
2.2 Create Administrator Username and Password	6
2.3 Configure the Card	7
2.4 Installing Multiple Cards in a System	8
2.5 Cybersecurity Best Practices	8
2.6 Risk Assessment	11
2.6.1 Physical Security	11
2.6.2 Account Access	11
3 Enable Communication Protocols	13
3.1 Enable Protocols	13
3.1.1 Enable Modbus Protocol	13
3.1.2 Enable BACnet Protocol	14
3.1.3 Enable SNMP	15
3.2 Download Protocol Mappings	18
4 Vertiv™ Liebert® IntelliSlot™ RDU120 Card Web Page Layout	19
4.1 Web Page Sections	19
4.2 Help Text	20
4.3 Managed Device Tab Menus	21
4.4 Communications Tab Menu	21
4.5 Sensor Tab Menu	23
4.5.1 Sensor Tab Summary Page	24
4.5.2 Sensor Tab Summary Details Pane	24
4.5.3 Changing Sensor Order	25
5 Editing the Vertiv™ Liebert® IntelliSlot™ RDU120 Card Configuration	27
5.0.1 Communications Tab Menu Folders	27
5.1 Active Events Folder	27
5.2 Downloads Folder	27
5.3 Configuration Folder	28
5.3.1 System Folder	28
5.3.2 Network Folder	31

- 5.3.3 Local Authentication Folder34
- 5.3.4 Remote Authentication Folder 35
- 5.4 Protocols Folder 39
 - 5.4.1 BACnet Folder 39
 - 5.4.2 Modbus Folder 40
 - 5.4.3 SNMP Folder 42
 - 5.4.4 Web Server Folder 46
 - 5.4.5 Email Folder 50
 - 5.4.6 Cloud Service 52
 - 5.4.7 Managed Device Folder 55
- 5.5 Support Folder 57
 - 5.5.1 Active Networking Folder 59
 - 5.5.2 Firmware Update Folder 61
 - 5.5.3 Configuration Export/Import Folder 62
 - 5.5.4 Manually Restarting the Card 63
 - 5.5.5 Manually Resetting the Card 63
- 5.6 Status Folder 63
 - 5.6.1 Status 63
- Appendices 65**
- Appendix A: Technical Support and Contacts 65

1 Introduction

This Vertiv™ Liebert® IntelliSlot™ RDU120 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 Vertiv™ Environet™ Alert, Vertiv™ Power Insight, Vertiv™ Power Assist, and Remote Services.

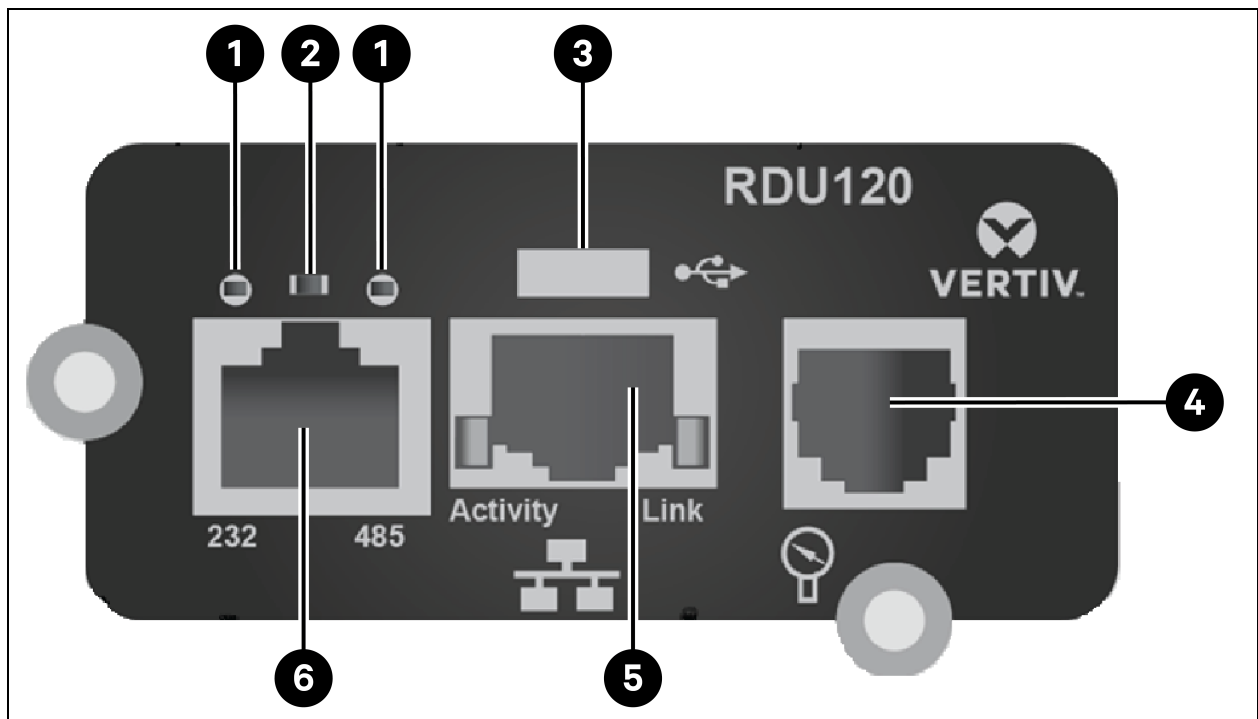
The RDU120 card firmware images are cybersecurity hardened via a secure boot implementation and also UL2900-1 Certified.

UL 2900-1: 12/13/2023

Standard for Safety for Software Cybersecurity for Network Connectable Products, Part 1: General Requirements, ANSI/CAN/UL 2900-1, Second Edition, Dated December 13, 2023.

The RDU120 is an optional card and is not required for the primary function of the host system to operate. The 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 (BMS) and network management systems (NMS) via BACnet, Modbus, SNMP, LIFE/Remote Services.

Figure 1.1 RDU120 Card Features



Item	Description
1	Status LED indicators, see Table 1.1 on the next page.
2	Reset button, see Manually Resetting the Card on page 63.
3	USB C port, see Firmware Update Folder on page 61.

Item	Description
4	Sensor network port, supported sensors are in Table 22 on page 10.
5	RJ-45 Ethernet port
6	RS-485 port (BACnet/MSTP, Modbus RTU. Only one may be used.) and RS-232.

1.1 Support for Environmental Sensors

The Vertiv™ Liebert® IntelliSlot™ RDU120 card monitors up to 16 Geist and Liebert 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 23.

Table 1.1 LED Indicators and Description

LED Indicators	Description
Green On	Full network connectivity, DHCP
Green Off	No network connectivity
Green Blinking	Link local address only
Red On	Web pages for the monitored device are unavailable (Vertiv™ Liebert® GXT5, for example).
Red Off	Web pages for the monitored device are available
Red blink fast	Web pages for the monitored device are initializing. Blink rate is 0.25 sec.
Red blink slow	Device not available. Blink rate is 1.50 sec.
Green and red toggling	Reset to Factory Defaults has been recognized.

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.vertiv.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 8.

2.1 Installing the Card

The Vertiv™ Liebert® IntelliSlot™ RDU120 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. Also, the card is hot swappable and can be installed while the managed system is powered up. This will not affect the end system operation.

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 5.

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 Vertiv™ Liebert® IntelliSlot™ RDU120 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 dynamic host configuration protocol (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:

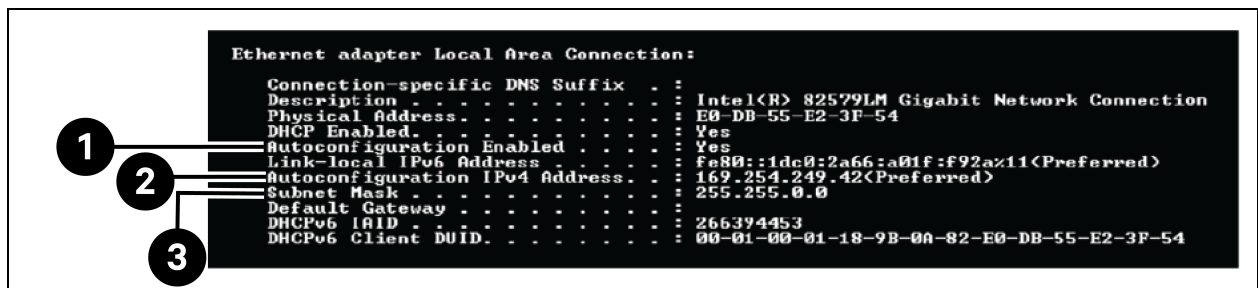
```
Autoconfiguration Enabled = Yes
Autoconfiguration IPv4 Address = 169.254.x.x
Subnet Mask = 255.255.0.0
See Figure 2.1 below.
```

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 Liebert® IntelliSlot™ RDU120 user interface opens. Alternatively, the card can be accessed at 192.168.123.123. Statically assign the laptop or PC to the 192.168.123.x subnet.

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 Vertiv™ Liebert® IntelliSlot™ RDU120 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 RDU120 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 usernames and passwords immediately. See **Figure 23** on page 7 for more details.

2.1.4 Connecting an RS-485 Serial Cable

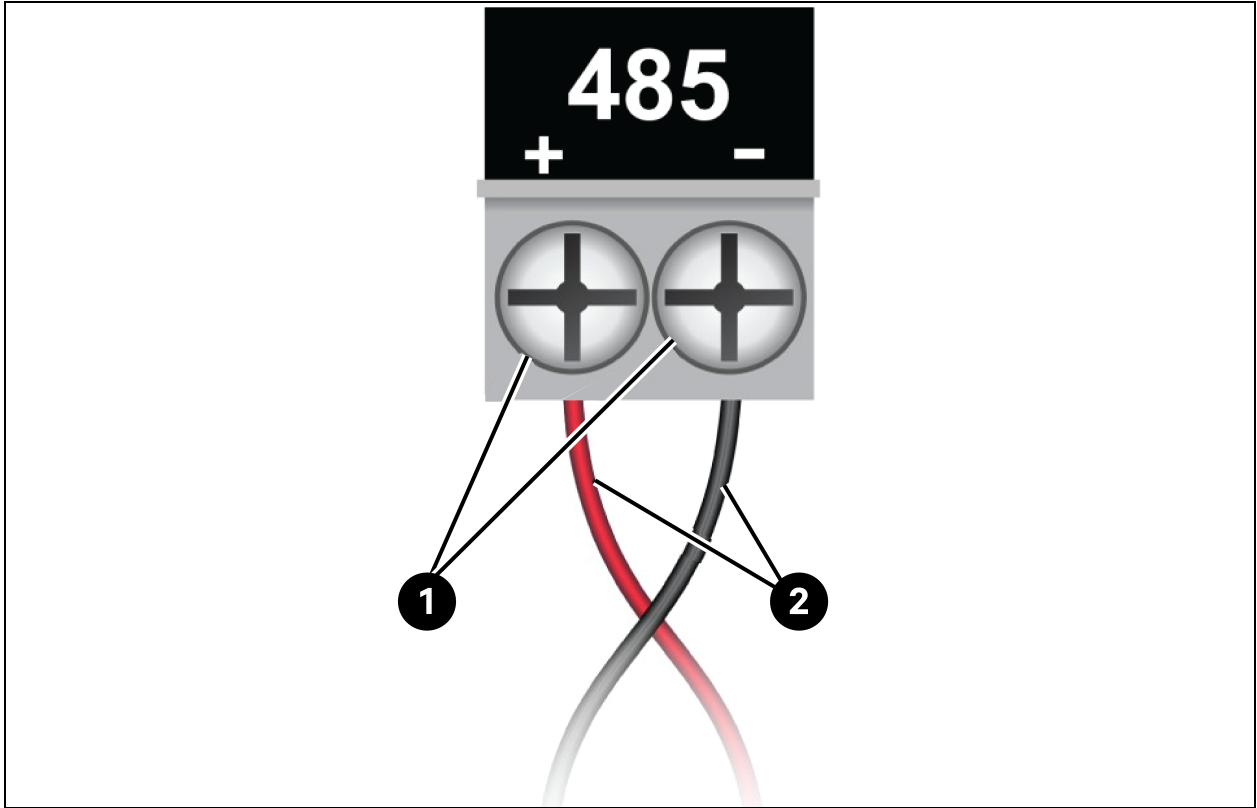
The Liebert® IntelliSlot™ RDU120 cards come with an Adapter RJ-45-2POS Terminal Block. The adapter has two screw terminals to attach the ends of a RS-485 cable for communicating to a building management system.

1. Find the serial cable from the building management system. If it already has an RJ-45 connector on the end, determine whether it uses the same pin-out as the Liebert® IntelliSlot™ RDU120 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 in **Figure 22** on the next page.

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 Vertiv™ Liebert® IntelliSlot™ RDU120 card. See **Figure 1.1** on page 1, for the location of the port.


2.2 Create Administrator Username and Password


The administrator user credentials must be setup on the initial access/power-up of the Liebert® IntelliSlot™ RDU120 card.


1. Create an Administrator account. See **Figure 2.3** on the facing page.
2. Please note the Username and Password requirements in the dialogue.


Figure 2.3 Login Page

Please Create an Administrator Level Account

Please hover over tool tips () to see Username and Password rules.

Username 

Password 

Confirm Password

Enable HTTP Access

Username Requirements: 2-30 characters, case-sensitive, printable ASCII excluding: \ '<>~?#, double quote, and space.

Password Requirements: 8-30 characters, case-sensitive, include upper/lower case, digits, and special characters (excluding : \ '<>~?#, double quote, space). Must not match the username.

3. Take careful note of the actual credentials that are entered in the Admin Account Setup dialogue shown **Figure 2.3** above.

NOTE: If the administrator credentials are lost or forgotten, the card must be reset to a factory default state to regain access.

2.3 Configure the Card

The Vertiv™ Liebert® IntelliSlot™ RDU120 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 Liebert® IntelliSlot™ RDU120 card and with the Liebert equipment:
 - a. Click *IPv4* or *IPv6*.
 - b. Click *Edit*.
 - c. When prompted, enter the Administrator username and password.
 - 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-

Click *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 Vertiv™ IntelliSlot™ RDU120 card. If the second card is not a Liebert® IntelliSlot™ RDU120 card, follow instructions in the user manual for that card.

Before beginning installation of a second Liebert® IntelliSlot™ RDU120 card, verify that the first card functions properly.

If the first card is an IntelliSlot™ card, but not a Liebert® IntelliSlot™ RDU120 card, and if both cards connect to the same Ethernet network, then you should disable the router function on the first card. This will avoid circular routes. Follow instructions in the user manual for the first card.

If the first and second cards are both Liebert® IntelliSlot™ RDU120 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 Liebert® IntelliSlot™ RDU120 card is 113, so the second card should use 114. A third card should use 115. A fourth card should use 115. 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 Liebert® IntelliSlot™ RDU120 card.
2. On the Communications tab, click *Configuration > Managed Device > Serial Interface*.
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-

Click *Cancel* to discard them.

2.5 Cybersecurity Best Practices

The configuration settings on the card support are defaulted for a secure configuration on deployment. Proper security of critical infrastructure equipment requires proper configuration of ALL communication services. This section summarizes the settings.

The Liebert® IntelliSlot™ RDU120 has been architected with cybersecurity as a primary consideration. Multiple features in the areas of Design, Security, and Management functions are offered in the Liebert® IntelliSlot™ RDU120 to address and mitigate cybersecurity risks. The default settings, along with designed features, security, and management functions of the Liebert® IntelliSlot™ RDU120, are intended to be part of a complete cybersecurity program.

Through our Vertiv SECURE product lifecycle, Vertiv is committed to minimizing cybersecurity risk in our products by deploying cybersecurity best practices across our engineering design of products and solutions, by making them more secure, reliable, and competitive for our customers.

Below are some lifecycle cybersecurity recommendations. The cybersecurity recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement a customers', existing cybersecurity program. The following sites are available for more information on general cybersecurity best practices and guidelines:

<https://www.cisa.gov/topics/cybersecurity-best-practices>

<https://www.vertiv.com/en-us/support/security-support-center/>

The factory defaults of the Vertiv™ Liebert® IntelliSlot™ RDU120 are set to the most secure deployment. As part of these settings, a user must create administrator account credentials on first login. This is intentional and part of the Vertiv SECURE program to support a fast, but secure installation. 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 Liebert® IntelliSlot™ RDU120 card. If the administrator elects to enable any port or protocol that does not have secure end-to-end encryption by the RDU120, it is up to the administrator to provide a secure communication path (such as an encrypted VPN connection) to securely transport all data and protocols.

Table 2.1 below, 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	Create the admin and user account names and passwords immediately on installation/power up.	There are no default credentials on factory units. All user credentials must be created on user first login. Change Usernames and Passwords Immediately. See Figure 2.3 on page 7.
IP Network Access	Enable/disable IPV4 and IPV6 network access to the Liebert® IntelliSlot™ RDU120 Card - disable unused network access.	Configure the Card on page 7
SSHv2 Access	Enable/disable and SSHv2 access for diagnostic and configuration support - disable when not in use.	Network Folder on page 31 on page 37
Web Server Protocol	Select HTTPS to use SSL/TLS v1.3 encryption when accessing data through the web user interface.	Web Server Folder on page 46 on page 39
SSL/TLS v1.3 Certificates	When using HTTPS, install your own SSL Certificates from a trusted certificate authority or generate alternative self-signed certificates.	Certificate Folder on page 46
Communication Protocols	Enable/disable BACnet, Modbus, SNMP, and YDN23 protocols - disable any that are unused.	Enable Communication Protocols on page 13
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 14
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 13
SNMP Version Settings	Enable/disable the desired SNMP versions; Consider using SNMPv3 with user authentication and encryption.	Configure SNMP Settings on page 16
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 CommRDU120 Strings	Change the SNMP v1/v2c Trap and Access CommRDU120 Strings from their default values.	Configure SNMPv1 Trap Settings on page 17 and Configure SNMPv1/v2c Access Settings on

Table 2.1 Settings to Review and Verify to Reduce the Risk of Unauthorized Access (continued)

Item	Description	Reference
		page 17
SNMPv3 Settings	Use the SNMPv3 Authentication and Privacy settings to make SNMPv3 communications more secure.	Configure SNMPv3 User Settings on page 17
Velocity Protocol Settings	Enable/disable the Velocity Protocol which is used by Vertiv™ management applications to access device data.	Ethernet Interface on page 55

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 Vertiv™ Liebert® IntelliSlot™ RDU120 card are listed in **Table 2.2** below. Some port settings may be changed by the administrator.

Table 2.2 Ports Used by the Liebert® IntelliSlot™ RDU120 Card

Network Service	Port Used	Default Enabled?	Can be Modified?	
Web	HTTP	TCP 80	No	Yes
	HTTPS	TCP 443	Yes	Yes
DNS	TCP & UDP 53	Yes	No	
NTP	TCP & UDP 123	Yes	No	
SMTP	TCP 25	No	Yes	
SSHv2	TCP & UDP 22	No	No	
Telnet	TCP 23	No	No	
SNMP	UDP 161, 162	No	Only trap port 162 may be changed	
Secure SMTP	TCP 587	No	Yes	
Modbus TCP	TCP 502	No	Yes	
BACnet IP	UDP 47808	No	Yes	
Velocity Protocol	UDP 47808	No	No	
Remote Services	TCP 5672	No	No	
Remote Syslog	TCP 514	No	Yes	
LDAP	TCP 636	No	Yes	
RADIUS	UDP 1812/1813 /1645/1646	No	No	
TACACS+	TCP 49	No	No	

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

2.6 Risk Assessment

Vertiv recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the security, availability and integrity of the system and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically.

2.6.1 Physical Security

The Vertiv™ Liebert® IntelliSlot™ RDU120 is designed and intended to be deployed and operated in a physically secure and network firewall protected location. Vertiv recommends a review of the physical security and operating environment of the unit. Since an attacker or disgruntled user can cause serious disruption, below are some recommended best practices that include, but are not limited to:

- Restrict access to areas, racks, and units with encrypted card RFID/badges, unique multi-factor passcode authentication for access, man traps, and biometric scanners for physical access to the equipment.
- Trusted and background checked security guards with 24x7x365 physical presence and written logs to help document and note physical access to a data center, building, rack, etc.
- Restricted physical access to telecommunications equipment and network cabling. Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. Best practices include uses of metal conduits for the network cabling running between equipment cabinets.
- All USB, RJ45, and/or any other physical ports should be restricted on the units.
- Do not connect removable media (e.g., USB devices, SD cards, etc.) for any operation (e.g., firmware upgrade, configuration change, or boot application change) unless the origin of the media is known and trusted. Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.

2.6.2 Account Access

The RDU120 account access privileges should be administered to provide the least account functions that still enables the end-user to perform their job functions. Login to the RDU120 should be restricted to legitimate users. Some of the following best practices should be adopted by an organization's written procedures for network and equipment access:

- First login to the RDU120 requires credentials to be created.
- No account/logon sharing. Each user should have their own specific account and password. Logging functions of the RDU120 expect each account to be a unique non-shared user.
- Admins should restrict access and privileges to only the required functions of the user's job function.
- Restrict all admin-level privileges (such as firmware updates, protocol enablement/disablement, etc.) to only approved administrators.
- Ensure password strength, complexity, and length requirements are enforced at the highest level per company IT policy.
- Ensure terminated employees instantly are removed from accessing the unit. Some examples include the user of a AAA, TACACS+ user authentication process.
- Enforce session time-out after a period of inactivity.

This page intentionally left blank

3 Enable Communication Protocols

The Vertiv™ Liebert® IntelliSlot™ RDU120 card communicates with equipment and third-party systems over the following protocols:

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

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 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 > Configuration > Protocols*).

NOTE: The enabled protocols can be viewed in Configuration/Protocols.

3.1.1 Enable Modbus Protocol

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

1. On the Communications tab, select *Configuration > Protocols > Modbus*.
2. Click *Edit* and enter a username and password if necessary.
3. Select the Modbus interface, (Modbus TCP or Modbus RTU).
4. Select the access level (Read Only or Read/Write).
5. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

6. Configure the Modbus interface chosen. See [Configure Modbus TCP](#) below or [Configure Modbus RTU](#) on the next page. For descriptions of the settings, see [Modbus Folder](#) on page 40.

Configure Modbus TCP

1. On the Communications tab, select *Configuration > Protocols > Modbus > Modbus TCP*.
2. Click *Edit* and enter a username and password if necessary.

See [Modbus TCP Folder](#) on page 41 for additional details.

3. The default Modbus server port is 502. The port can be changed if desired. The Modbus server will use to listen for and respond to Modbus protocol requests based on the selected Trusted IP Access table.
4. Enter the maximum client connection count if desired. The default maximum client connection is 4.
5. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

Configure Modbus RTU

1. On the Communications tab, select *Configuration > Protocols > Modbus > Modbus RTU*.
2. Click *Edit* and enter a username 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 41.

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

4. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

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 *Configuration > Protocols > BACnet*.
2. Click *Edit* and enter a username 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 Vertiv™ Liebert® IntelliSlot™ RDU120 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-

Click *Cancel* to discard them.

10. Configure the BACnet interface chosen, see [Configure BACnet IP Protocol](#) on the facing page or [Configure BACnet MSTP Protocol](#) on the facing page.

For description of the settings, see [BACnet Folder](#) on page 39.

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 *Configuration > Protocols > BACnet > BACnet IP*.
2. Click *Edit* and enter a username 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 BACnet broadcast management device (BBMD).
 - c. Enter a time, in seconds, for Foreign Device Time-to-Live. For descriptions of the settings, see [BACnet IP Folder](#) on page 40.
4. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

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 *Configuration > Protocols > BACnet > BACnet MSTP*.
2. Click *Edit* and enter a username 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 40.

7. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

3.1.3 Enable SNMP

SNMPv1/v2c and SNMPv3 are disabled by default. 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 *Configuration > Protocols > SNMP*.
2. Click *Edit* and enter a username and password if necessary.
3. To enable v1/v2 and or v3, click the corresponding checkboxes.

4. To enable Authentication Traps, click to checkbox.
5. To change the Heartbeat Trap Interval, choose a time from the dropdown 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.
6. For each trap type, choose whether to disable or leave enabled.
For descriptions of the settings, refer to [SNMP Folder](#) on page 42.
7. The SNMPv3 Engine ID Text options are discussed in the [Configure SNMPv3 User Settings](#) on the facing page.
8. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

Global Products MIB for SNMP Integration

The Vertiv™ Liebert® IntelliSlot™ RDU120 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 MIBs are available at <https://www.vertiv.com/en-us/support/software-download/monitoring/management-information-bases-mibs-for-liebert-products/>. It supports both Windows® and Unix 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 Liebert® IntelliSlot™ RDU120 card permits up to 8 SNMPv3 Users, up to 8 SNMPv1 Trap targets, and up to 8 SNMPv1/v2c Access addresses.

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

- SNMPv1 must have trap settings including - target IP addresses or hostnames, trap community strings and port number.
- SNMPv2c must have Access settings including – Name, Community, Mode, Trusted Network Address and Trusted Access prefix.
- SNMPv3 users must have settings including – Username, User Enable, Access type Authentication, Authentication Secret, Privacy, Privacy Secret, Trusted Access Address and Trusted Access Prefix configured.

NOTE: 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 text. The text used to generate the Engine ID can be changed as desired and customizable.

1. On the Communications tab, select *Configuration > Protocols > SNMP*.
2. Click *Edit* and enter a username and password if necessary.
3. Edit the Engine ID text as desired.
4. Click *Save*.

Refer to [SNMP Folder](#) on page 42, for descriptions of the settings and options.

Configure SNMPv3 User Settings

1. On the Communications tab, select *Configuration > Protocols > SNMP > SNMPv3User: Table*.

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

2. Click *Edit* and enter a username 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 43.

4. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

5. Repeat steps 1 through 4 for additional users.

Configure SNMPv1 Trap Settings

1. On the Communications tab, select *Configuration > Protocols > SNMP > SNMPv1/v2 Traps: Table*.

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

2. Click *Edit* and enter a username and password if necessary.
3. Enter the information and set the permissions appropriate to the user. For descriptions of the settings, see [SNMPv1/v2 Trap Folder](#) on page 44.

4. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

5. Repeat 1 through 4 for any additional users.

Configure SNMPv1/v2c Access Settings

1. On the Communications tab, select *Configuration > Protocols > SNMP > SNMPv1/v2c Access Table 8*

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

2. Click *Edit* and enter a username 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 45.

4. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

The card must be restarted before another user's settings may be changed.

3.2 Download Protocol Mappings

The Vertiv™ Liebert® IntelliSlot™ RDU120 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

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

4 Vertiv™ Liebert® IntelliSlot™ RDU120 Card Web Page Layout

Default settings of the Liebert® IntelliSlot™ RDU120 card let you to 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.

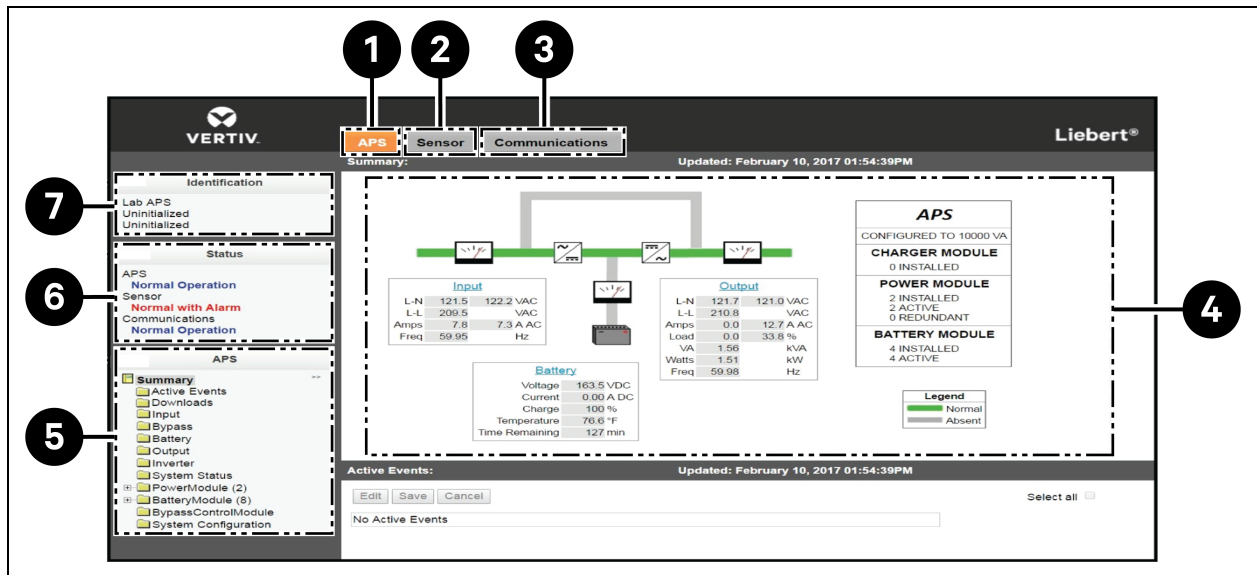
NOTE: The **Edit** button is grayed-out if the settings on a menu cannot be changed.

4.1 Web Page Sections

Each Unit card has a web 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 information 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 23 for details.
3	Communications tab displays information about the Vertiv™ Liebert® IntelliSlot™ RDU120 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 RDU120 card, and any Liebert SN sensors connected to the card.
7	Identification panel displays the System Name, System Location, and System Description.

4.2 Help Text

Each Web page shown by the Vertiv™ Liebert® IntelliSlot™ RDU120 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 six icons described in [Table 4.1](#) below.

Table 4.1 Help Text and Icons







Icon	Description
	Event Normal
	Event Information
	Event Alarm

Table 4.1 Help Text and Icons (continued)

Icon	Description
	Event Warning
	Event Critical
	Tool Tip

4.3 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 Vertiv™ Liebert® IntelliSlot™ RDU120 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.

4.4 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 **Table 4.2** below.

Table 4.2 Communications Tab Menus

Menu	Description	See Details
Active Events	Displays the current event activity.	Active Events Folder on page 27
Downloads <ul style="list-style-type: none"> Audit Log SNMP Trap Log System Events Log Ethernet.pcap 	Downloading files to text-accessible, comma-delimited or tab-delimited files ease troubleshooting. The protocol mapping files are available when the associated protocol is enabled/configured.	Downloads Folder on page 27
Configuration <ul style="list-style-type: none"> System Network Local Authentication Remote Authentication Protocols Web Server Email Cloud Service 	Displays information about the system setup, access, network connections, Managed Device settings and whether email messaging is enabled.	Configuration Folder on page 28

Table 4.2 Communications Tab Menus (continued)

Menu	Description	See Details
<ul style="list-style-type: none"> • Managed Device 		
Protocols <ul style="list-style-type: none"> • SNMP • Modbus • BACnetSNMP 	Lists information and settings related to available third-party protocols employed to monitor equipment.	Protocols Folder on page 39
Status <ul style="list-style-type: none"> • System Status • System Restart Required • LIFE™ device identity changed™ needs to be reconfigured. • Multiple protocols are configured to use the same RS-485 port. Please change configuration so that only one protocol is enabled (see Modbus RTU, BACnet MSTP, YDN23, and other). • Duplicate Velocity Protocol MSTP Node ID • Duplicate BACnet MSTP Node ID • Unconfigured System Name • Unsupported Managed Device 	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 63
Support <ul style="list-style-type: none"> • RDU120 time and Date • Model • Application Firmware Version • Application Firmware Label • Boot Firmware Version • Boot Firmware Label • Serial Number • Manufacture Date • Hardware Version • GDD Version • FDM Version • Product Sequence ID • Device label • Restart Card • Reset Card to Factory Defaults (see NOTE below) • Execute Partial Reset • Host Access Reset • Generate and download diagnostic file • Firmware Update • Active Networking 	Shows information needed for maintenance or troubleshooting and shortcuts to reboot the card, reset the RDU120 card to its factory defaults and to update the card's firmware.	Support Folder on page 57 (Firmware Update also on)

NOTE: The card may be reset to factory defaults manually using the reset button, see [Manually Restarting the Card on page 63](#).

4.5 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 Vertiv™ Liebert® IntelliSlot™ RDU120 card, the Sensor tab appears.

Figure 4.2 Sensor Tab Summary page

The screenshot shows the Vertiv Liebert interface with the 'Sensor' tab selected. The top navigation bar includes 'APS', 'Sensor', and 'Communications'. The 'Sensor' tab is active, showing a 'Summary' section with a table of sensors. The table has columns for ID, Type, Serial Number, Label, Value, and Status. Below the table, there is a detailed view for a 'Leak Detect Sensor' with sections for Status, Events, and Settings. Numbered callouts 1 through 6 are placed over the interface to highlight specific features: 1 points to the 'Label' column in the summary table; 2 points to the status graphs in the 'Status' column; 3 points to the status icons in the 'Status' column; 4 points to the 'Value' column; 5 points to the 'Leak Detect Sensor' details section; and 6 points to the 'Settings' section.

Item	Description
1	User-assigned labels for sensor identification/location.
2	Graphs indicate sensor readings in relationship to thresholds.
3	Icons indicate sensor status readings for example: cable fault or door open/closed depending on sensor function.
4	Actual sensor-reading values.
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 **Table 4.3** below.

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.

Table 4.3 Sensor Tab Menu Folders (continued)

Folder	Description
Sensor Subsystem <ul style="list-style-type: none"> • System Model Number • System Status • Too Many Sensors • Slots Not Available • Acknowledge Sensor Changes 	Displays overall information about the sensors.
Sensor Change	Lists events showing sensors that have been added or removed. If the list has any entries, an Acknowledge button appears. Clicking the Acknowledge button clears the list. The Acknowledge button on this page has the same behavior as the Acknowledge button on the Sensor Server page.
Sensor Order	Displays a list of sensors and allows setting the order in which the sensors are displayed on the Summary page.

4.5.1 Sensor Tab Summary Page

The Sensor tab Summary Page shows the status of all installed sensors, details about 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.

4.5.2 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:	
Geist	RT temperature-only sensor
Geist	RTAFHD3 temperature/airflow/humidity/dewpoint sensor
Geist	THD temperature/humidity/dewpoint sensor
Geist	T3HD 3xTemperature+humidity/dewpoint sensor
Vertiv	*SN-Z011 Temp Sensor
Vertiv	*SN-Z02 3 Temp Sensors
Vertiv	*SN-Z03 3 Temp, 1 Humidity Sensors
Vertiv	*SN-TH Temp/Humidity Sensor
Vertiv	*SN-2D 2 Door Sensors
Vertiv	*SN-3C 3 Contact Closure Sensor
NOTE: *Geist 6-pin to Vertiv 8-pin sensor adapter required.	

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 28.

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.

4.5.3 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 username and password if necessary.
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*.

This page intentionally left blank

5 Editing the Vertiv™ Liebert® IntelliSlot™ RDU120 Card Configuration

The Web UI can be used to configure the settings for the Liebert® IntelliSlot™ RDU120 card and for the managed 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 username and password if necessary.
5. Change the settings.
6. Click *Save* to confirm the changes.

-Or-

Click *Cancel* to discard them.

5.0.1 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
- [Support Folder](#) on page 57
- [Status Folder](#) on page 63

5.1 Active Events Folder

The Active Events folder contains no configurable settings. The folder displays events that affect the Liebert® IntelliSlot™ RDU120 card.

5.2 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 Liebert® IntelliSlot™ RDU120 card. The logs help in configuring and troubleshooting communication between the Network Management or Building Management Systems being used to monitor the managed device.

5.3 Configuration Folder

The top-level Configuration folder displays the System Model Number of the Vertiv™ Liebert® IntelliSlot™ RDU120 card. This name is factory-set and cannot be changed. The Configuration folder contains the following subfolders:

- [System Folder](#) below
- [Network Folder](#) on page 31
- [Local Authentication Folder](#) on page 34
- [Remote Authentication Folder](#) on page 35
- [Protocols Folder](#) on page 39
- [Web Server Folder](#) on page 46
- [Cloud Service](#) on page 52
- [Managed Device Folder](#) on page 55
- [Email Folder](#) on page 50

5.3.1 System Folder

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

To edit the information displayed:

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

SSH Setting Options

The System subfolder contains the SSH settings offers choices to enable/disable and port configuration.

- **SSH Enable**
The control used to enable/disable SSH.
- **Port number**
SSH port number. Default port is 22.
- **Time Status and Settings**
The System subfolder contains the Time Service folder. Each setting offers a menu of choices or an enable/disable checkbox.

Time Status

Time Source

The source of the last time update. Possible time sources are: NTP, Modbus, BACnet, SNMP or Manual mode. Manual mode means that time is updated using the System Date and Time Setting.

Time Setting Options

- **Time Mode**

Time Mode specifies the possible time sources. Automatic - the time can be updated using NTP, Modbus, BACnet or SNMP. Manual - time is updated using the **System Date and Time**.
- **Time Zone**

Time zone used to compute local time.
- **Enable Auto-Sync To Managed Device**

Enable automatic writing time to the managed device.
- **External Time Source**

The external source to use for time synchronization. Default = NTP Server.
- **NTP Time Server 1**

URL, Hostname, or IP address of the primary NTP time source. 64-character maximum.
- **NTP Time Server 2**

URL, Hostname, or IP address of the back-up NTP time source. 64-character maximum.
- **System Date and Time**

Manually set the system date and time. The date entry form is YYYY-MM-DD (Year, Month, Day). The time entry form is HH:MM:SS (Hour, Minute, Second).

Remote Syslog Service Setting Options

- **Enable Remote Syslog**

Remote syslog enable control.
- **Remote Syslog Server**

IP address of remote syslog server.
- **Remote Syslog Server Port**

Remote syslog server port. The default is 514.

USB Status and Settings

USB Status:

- **USB Vendor ID**
USB Device ID associated with the mounted device.
- **USB Device Vendor ID**
USB Device Vendor ID associated with the mounted device.
- **USB Device Product ID**
USB Device Product ID associated with the mounted device.
- **USB Device Product ID**
USB Device Product ID associated with the mounted device.
- **USB Device bcdDevice**
USB Device bcdDevice flag associated with the mounted device.
- **USB Device Product**
USB Device Product associated with the mounted device.
- **USB Device Serial**
USB Device Serial associated with the mounted device.
- **USB Device max Power**
USB Device Max Power attribute describes the maximum amount of power used by the mounted device.
- **USB Device Self Powered**
USB Device Self Powered attribute associated with the mounted device.
- **USB Device Remote Wakeup**
USB Device remote Wakeup attribute associated with the mounted device.

USB Commands and Setting Options

- **Eject USB Device**
Eject to USB to allow safe removal of the device.
- **USB Enable**
Enable or Disable control. Disabling the USB will disable the user USB port.

5.3.2 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 = RDU120-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](#) below
- [Domain Name Server \(DNS\) Test Folder](#) on page 33

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

5.3.3 Local Authentication Folder

The Local Users subfolder offers up to 8 users and three user access levels described in **Table 5.1** below.

Table 5.1 Privilege Levels

Level Name	Access /Permission Type	Description
View	Read-only	General User - Able to view all tabs, folders and sub-folders of the user-interface.
Control	Read/Write	Control User - Able to edit settings using the assigned password, which is always required to edit the managed equipment settings/configuration.
Administrator	Read/Write	Administrator User - Able to edit settings using the assigned password, which is always required to edit settings/configuration of the card and the managed equipment. 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. If an administrator user is not configured, the card will need to be reset to factory defaults and an administrator account created to restore access to configuration settings.

IMPORTANT! Record usernames and passwords and save them in a secure place where they can be found if forgotten. A lost password cannot be retrieved from the Vertiv™ Liebert® IntelliSlot™ RDU120 card. If the administrator password is lost, the card must be reset to factory defaults and reconfigured.

To change the usernames 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 username and password, then click *OK*.
3. Enter a new username 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-

Click *Cancel* to discard them.

5.3.4 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 authentication types:

- [RADIUS Authentication](#) below
- [LDAP Authentication](#) on the next page
- [TACACS+ Authentication](#) on page 37

RADIUS Authentication

NOTE: Knowledge of RADIUS server settings is required for this remote authentication protocol. If you are not familiar with these settings, consult your RADIUS server administrator.

Authentication and authorization are 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 configuration file, or a graphical user interface (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.

NOTE: Your RADIUS server may require additional attributes depending on the server manufacturer.

LDAP Authentication

Authentication and authorization are provided by the remote LDAP server.

NOTE: Knowledge of your LDAP server settings is required to set up this remote authentication protocol. If you are not familiar with these settings, consult your LDAP server administrator.

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 [LDAP Settings](#) below.

LDAP Settings

- **LDAP Server Address**
Specify the host address for LDAP server. The HOST can be an IPv4 address, an IPv6 address in brackets (Such as [2001:0DB8:AC10:FE01::]) or a hostname.
- **LDAP Server Port**
Used to set the LDAP port number. The default port for LDAP is 389 - use for Security Type None or StartTLS. Use 636 for Security Type SSL
- **LDAP Bind DN**
Distinguished Name used to bind to the directory server. Blank string for Bind DN and Password implies anonymous bind.
- **LDAP Password**
Password used to bind to the directory server.
- **LDAP Base DN**
Distinguished Name to use for the search base.

NOTE: The remaining fields come from the NIS schema, defined in RFC2307. They are used to authenticate users in LDAP. Leaving them blank will use the default value.

- **LDAP User Filter**
LDAP filter for selecting users.
- **LDAP User UID**
Name of the server attribute that corresponds to the uid attribute in the schema.
- **LDAP User UID Number**
Name of the server attribute that corresponds to the uidNumber attribute in the schema.
- **LDAP Group Filter**

LDAP filter for selecting groups. Open class equivalent to POSIX group.

- **LDAP Group ID**

Name of the server attribute that corresponds to the gid attribute in the schema.

- **LDAP Group Member ID**

Name of the server attribute that corresponds to the memberId attribute in the schema.

- **LDAP Mode**

LDAP mode that determines default compatibility among the different LDAP types.

- **LDAP Security**

The encryption type used when connecting to the LDAP server – SSL or StartTLS.

- **Enabled Group**

Users in this group have view-only privileges. This aligns with View user described in the Local Authentication section of this user guide.

- **Control Group**

Users in this group have Control privileges. This aligns with Control user described in the Local Authentication section of this user guide.

- **Admin Group**

Users in this group have admin privileges. This aligns with Administrator user described in the Local Authentication section of this user guide.

TACACS+ Authentication

NOTE: Knowledge of your TACACS+ server settings is required to set up this remote authentication protocol. If you are not familiar with these settings, consult TACACS+ server administrator.

Authentication and authorization are 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 configuration file contains the **unity_group=unityadmin;** string in the **raccess** field.

```
user = tacacsAdmin {  
  service = raccess {  
    unity_group=unityadmin;  
  }  
}
```

– Or –

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

```
user = tacacsAdmin {  
  service = raccess {  
    unity_group=unityuser;  
  }  
}
```

The attributes in a configuration 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.

NOTE: Your TACACS+ server may require additional attributes.

Example: A Cisco TACACS+ server may require the **priv-level** attribute. Example: **priv-level=15**

5.4 Protocols Folder

The Protocols folder displays the types of protocols that may be enabled for a Vertiv™ Liebert® IntelliSlot™ RDU120 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 Velocity protocol, see [Ethernet Interface](#) on page 55.

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 41
- [Modbus RTU Folder](#) on page 41

SNMP, see:

- [SNMPv3 User Folder](#) on page 43
- [SNMPv1/v2 Trap Folder](#) on page 44
- [SNMPv1/v2c Access Folder](#) on page 45

5.4.1 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.

5.4.2 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 Vertiv™ Liebert® IntelliSlot™ RDU120 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

5.4.3 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 CommRDU120 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 Vertiv™ Liebert® IntelliSlot™ RDU120 card's MAC address.
- Text = Engine ID built from text entered in SNMPv3 Engine ID Text. See [Select SNMPv3 Engine ID Format](#) on page 16.

- **SNMPv3 Engine ID Text**

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

SNMPv3 User Folder

The Liebert® IntelliSlot™ RDU120 card supports up to 8 SNMPv3 users and offers advance security including authentication and encryption. The top-level page is a table with settings for all 8. 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 Username 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 except for colon, tab, double quote, and question mark. Note: The entry must be 8 or more characters but not more than 64.

- **SNMPv3 User Trap Targets**

Network hosts that will receive SNMPv3 traps, identified with either a network name or IP address. Up to 2 addresses can be configured.

- **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 in the table on the [Configure SNMPv3 User Settings](#) on page 17.

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/v2 Trap Folder

This page contains settings for network hosts that receive SNMPv1/v2 traps. Up to 8 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 that is 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 CommRDU120 String**

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

5.4.4 Web Server Folder

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

Web Server Settings

- **HTTP**
Enable or Disable HTTP operation.
- **HTTPS**
Enable or Disable HTTPS operation.
- **HTTPS Redirect**
Enable or Disable HTTPS Redirect operation.
- **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.
- **Session Idle Timeout**
The interval the software will wait before logging off a user unless there is user activity (default is 5 min).
- **Trusted Access**
Trusted Access sources can be identified by IP address or Network Name. A maximum of 5 sources can be configured.

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 facing 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 the next page.

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 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.

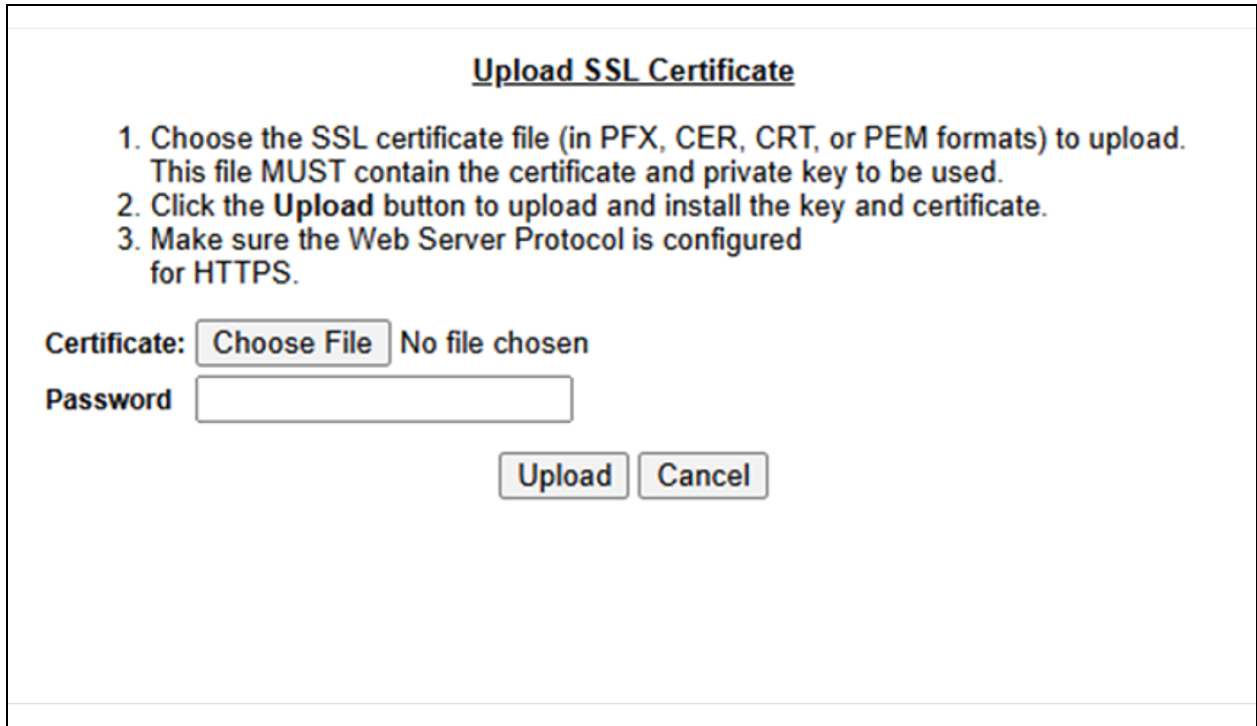
- **Email Address**

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 [Figure 5.1](#) on the next page.
3. Follow the instructions in the dialog to select and upload the appropriate files.

Figure 5.1 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 **Figure 5.2** on the facing page.
4. Follow the instructions in the dialog to generate and install the certificate.

Figure 5.2 Generate Self-Signed SSL Certificate Dialog



5.4.5 Email 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.

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 Vertiv™ Liebert® IntelliSlot™ RDU120 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**.

Messaging Test

Tests the set up for email and SMS messages. If the test fails, incorrect settings should be changed to ensure that the Vertiv™ Liebert® IntelliSlot™ RDU120 card sends proper notifications if an event should occur.

5.4.6 Cloud Service

Remote Service 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

The folder contains subfolders for connectivity and diagnostics:

- [Remote Services Connectivity Subfolder](#) on the facing page.
- [Remote Services Diagnostics Subfolder](#) on page 54.

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-service 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**
Manufacturer's device identification number.
- **Service Center Country**
Country in which the device is serviced.

Remote Services Connectivity Subfolder

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 Username**
Username 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 Subfolder

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.

5.4.7 Managed Device Folder

Managed Device contains two sub-folders: Serial Interface and Ethernet Interface. Velocity is the input protocol from a managed/monitored system.

- Connection Status
- FDM Version
- Product Sequence ID
- Interface Type

Serial Interface

Node ID Assignment

- Node ID
- Network number
- Max Address
- Baud rate

Ethernet Interface

When disabled, prevents access from a remote, IP-based system using the Velocity Protocol. Default = Disabled. See **Figure 5.3** on the next page.

- Ethernet interface
- Port Number
- Network Number
- IP Address

Figure 5.3 Managed Device Folder—Ethernet Interface

The screenshot displays the Vertiv web interface for configuring the Ethernet Interface of a GXT5-2000LVRT2UXXL device. The interface is divided into several sections:

- Identification:** Shows the device name "RDU120".
- Status:** Displays the device status as "Normal Operation" for the Sensor and "Normal with Alarm" for Communications.
- Communications:** A tree view on the left shows the navigation structure, with "Ethernet Interface" selected under "Managed Device".
- Ethernet Interface Settings:** A table with columns "Settings", "Edit", "Save", "Cancel", and "Units".

Settings	Edit	Save	Cancel	Units
Ethernet Interface	<input checked="" type="checkbox"/>			
Port Number		47808		
Network Number		1000		
IP Address (IP Only)				

5.5 Support Folder

The Support folder permits restarting the Vertiv™ Liebert® IntelliSlot™ RDU120 card, resetting the card to its factory defaults and updating the card's firmware. Agent refers to the Liebert® IntelliSlot™ RDU120 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 (Liebert® IntelliSlot™RDU120 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.

This includes the partial and Host Reset parameters.

- **Execute Partial Reset**

Reset the card's configuration to its factory defaults. Partial reset shall reset the following configuration items to its factory defaults:

- System
- Time
- Remote syslog service
- USB
- SNMP (Including Trusted Access, Traps, Users, and other.)
- Modbus (RTU + TCP, Trusted Access, and other.)
- BACnet (MSTP + IP, Trusted Access, and other.)
- Email (Including Email Addresses)
- Locale
- Sensor configuration

- **Host Access Reset**

Reset the card's configuration to its factory defaults

Host Access reset shall reset the following configurations:

- Console Access (that is serial)
- SSH
- Network
- IPv4
- IPv6
- 802.1x
- LLDP
- Local Authentication (Including all local users)
- Remote Authentication (Including LDAP, Radius, and TACACS configurations)
- Web Server (Including Trusted Access and Certificates)

Generate and download diagnostic file

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

5.5.1 Active Networking Folder

Status of the currently active IP network settings for the Vertiv™ Liebert® IntelliSlot™ RDU120 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.

5.5.2 Firmware Update Folder

The Vertiv™ Liebert® IntelliSlot™ RDU120 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 an alternate image.

The folder supports updating the firmware of the Liebert® IntelliSlot™ RDU120 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 Vertiv™ Liebert® IntelliSlot™ RDU120 card:

1. <https://www.vertiv.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 username 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.

NOTE: To update the firmware on the Liebert® IntelliSlot™ RDU120 card via the USB C interface: The USB-C can currently be used to firmware update the Liebert® IntelliSlot™ RDU120. The firmware image must reside in a \firmware folder on the USB drive.

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 username 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.

5.5.3 Configuration Export/Import Folder

Liebert® IntelliSlot™ RDU120 configuration settings may be backed up to a local disk or USB drive, and the backed-up files may be restored to the same card or other cards as needed.

5.5.4 Manually Restarting the Card

Steps for 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 the Card](#) below.

5.5.5 Manually Resetting the Card

Steps for manually resetting the card:

1. Locate the small rectangular hole on the front of the card between the status LED's that contains the reset button, see **Figure 1.1** on page 1.
2. Insert a small, non-conductive tool (example—tooth pick) into the small hole and press and hold for approximately 30 seconds.
3. Hold the reset button until the Green and Red LEDs start toggling. This indicates that the card reset to factory defaults has been accepted. Allow the card to reboot. For LED behavior, see **Table 1.1** on page 2.

The **Please Create an Administrator Level Account** window will appear, see **Figure 2.3** on page 7.

NOTE: HTTPS is the default web server access mode.

4. The card is reset to factory-default configuration. This manual action is typically taken if the card is not accessible via the Web interface.

NOTE: A short press will simply restart/reboot the card.

5.6 Status Folder

The Status folder contains no configurable items. It displays the System Status of the Vertiv™ Liebert® IntelliSlot™ RDU120 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 20 for a description of the icons.

5.6.1 Status

Status Events:

- System Restart Required
- Multiple protocols are configured to use the same RS-485 port. Please change configuration so that only one protocol is enabled (see Modbus RTU, BACnet MSTP, YDN23, and other).
- Duplicate Velocity Serial Node ID
- Duplicate BACnet MSTP Node ID
- Unconfigured System Name
- Unsupported Managed Device

This page intentionally left blank

Appendices

Appendix A: Technical Support and Contacts

A.1 Technical Support/Service in the United States

Vertiv Group Corporation

24x7 dispatch of technicians for all products.

1-800-543-2378

Liebert® Thermal Management Products

1-800-543-2778

Liebert® Channel Products

1-800-222-5877

Liebert® AC and DC Power Products

1-800-543-2378

A.2 Locations

United States

Vertiv Headquarters

505 N Cleveland Ave

Westerville, OH, 43082, USA

Europe

Via Leonardo Da Vinci 8 Zona Industriale Tognana

35028 Piove Di Sacco (PD) Italy

Asia

7/F, Dah Sing Financial Centre

3108 Gloucester Road, Wanchai

Hong Kong

This page intentionally left blank

Connect with Vertiv on Social Media



<https://www.facebook.com/vertiv/>



<https://www.instagram.com/vertiv/>



<https://www.linkedin.com/company/vertiv/>



<https://www.x.com/Vertiv/>



Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082 USA

©2025 Vertiv Group Corp. All rights reserved. Vertiv™ and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions.

AV-50006_REVB_04-25