Liqui-tect® LP3000™

Leak-detection System

Installer/User Guide

Technical Support Site

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

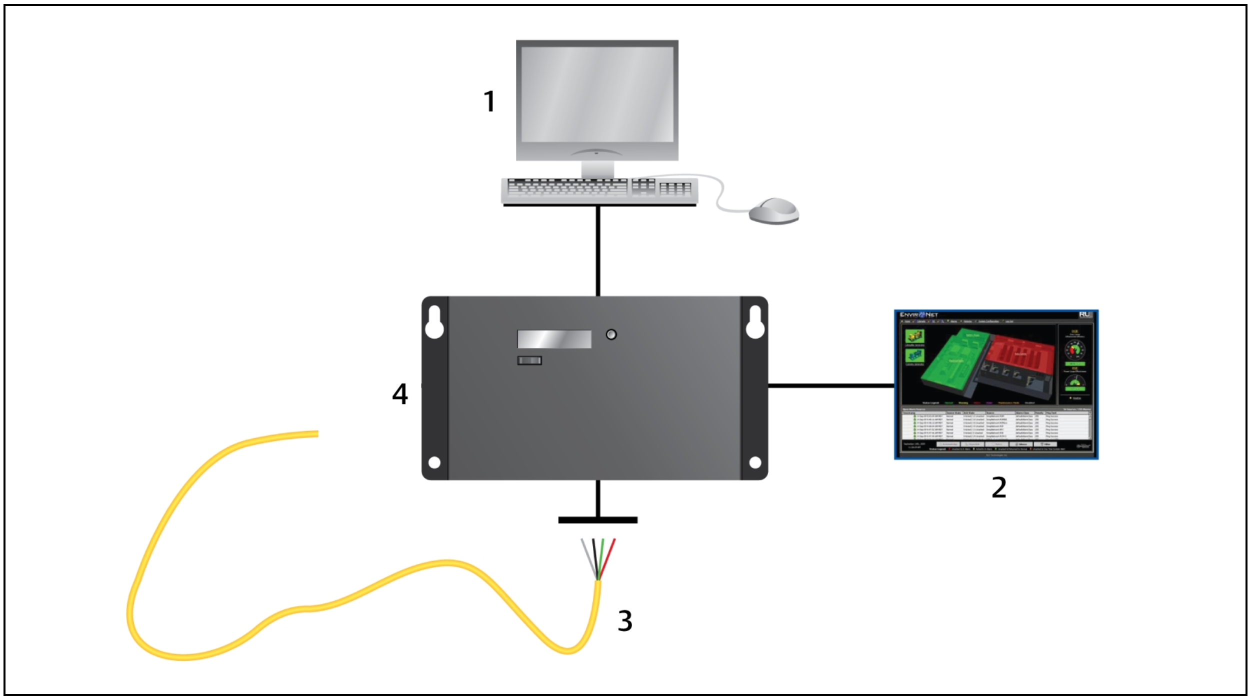
TABLE OF CONTENTS

1 PRODUCT DESCRIPTION

The Liqui-tect LP3000 is a complete monitoring system that reports the presence of water and other conductive liquids. Liqui-tect LP3000 is an advanced leak-detection controller that monitors up to 5,000 ft (15243048 m) of sensing cable. When a conductive liquid comes in contact with the sensing cable:

- An audible alarm sounds.
- The distance to the leak is shown on the front-paneldisplay and via the web user interface.
- Alarm notifications may be distributed via Modbus/BACnet/SNMP/SMTP.

Figure 3.1 LP3000 leak-detection system and communication overview



ITEM	DESCRIPTION
1	Web user interface.
2	BMS/NMS
3	Leak-detection cable
4	Liqui-tect panel

1.1 Supervised System

Liqui-tect LP3000 is a supervised system, which means that it continuously monitors for leaks and other fault conditions, including a cable break and cable contamination, that trigger an alarm. When a leak or fault is detected, a relay is activated, and LP3000 sends alarm notifications to predetermined recipients via the configured communication method.

Table 3.1 System Features

FEATURE	DESCRIPTIONS
Input Power	Includes an isolated power supply with interchangeable blades with input range 90 – 264 VAC, 47/63 Hz, 600 mA max.
Included Accessories	15' Connection cable and end terminator
Leak Detection Input (1)	
Maximum Cable Length	5,000 ft (1524 m) of LT500 Leak Detection Cable
Minimum Cable Length	35 ft (10.67 m)
Detection Accuracy	± 2 ft (0.6 m) ±0.5% of the cable length
Detection Repeatability	± 2 ft (0.6 m) ± 0.25% of the cable length
Detection Response Time	5 – 995 sec, software adjustable in 5-sec increments; ±2 sec
Outputs	
Form C dry-contact Relay	Summary alarm, 1 A @ 24 VDC; 0.5 A @ 120 VAC; Latched or non-latched
Communications Ports	
EIA-485	9600, 19200, or 38400 baud (selectable); No parity, 8 data bits, 1 stop bit
RJ-45	10/100 BaseT Ethernet port (TCP/IP)
Protocols	
TCP/IP, HTML	IPv4.0
SNMP	V1: V2C MIB-2 compliant: V3
SMTP	Supports Client Authentication (plain and login); compatible with ESMTP Servers
Modbus	Modbus RTU and Modbus TCP/UDP; Master & Slave
BACnet	BACnet MS/TCP and BACnet/IP
Alarm Notification	
Audible Alarm	70 dBA @ 2 ft (0.6 m); re-sound configurable (disabled, 0-24 hours)
Visible Alarm	Dot matrix LED display; bi-color status LED and through web interface
Email	4 Email recipients; email sent to all recipients on Alarm and Return to Normal
SNMP Traps	4 IP Addresses
Logging Capabilities	
Event Log	Last 500 events, downloadable to .txt file
Trend Log	Cable current level every day, for the last 288 days
Login Security	
Web Access	Two (2) passwords; One (1) Read-only; One (1) Read/Write
Operating Environment	
Temperature	32° to 122°F (0° to 50°C)
Humidity	5% to 95% RH, non-condensing
Altitude	15,000 ft (4,572 m) max.
Storage Environment	–4° to 158°F (–20° to 70°C)
Enclosure	Wall mountable; rack mount bracket LP3000-RMB (optional)
Dimensions	8 in. W x 4.25 in. H x 1.25 in. D (203 mm W x 108 mm H x 32 mm D)
Weight	1.5 lb (680 g)
Certifications	CE; ETL listed: conforms to UL 61010-1, EN 61010-1; certified to CSA C22.2 NO. 61010-1; RoHS compliance

1.2 Distance-read Leak Detection

When the Liqui-tect LP3000 measures a current in excess of the defined leak threshold, the microprocessor computes the distance to the leak, annunciates the leak, and logs the alarm in the event log. The leak is communicated via the front-panel display and other configured notification methods.

1.3 Communication with Liqui-tect LP3000

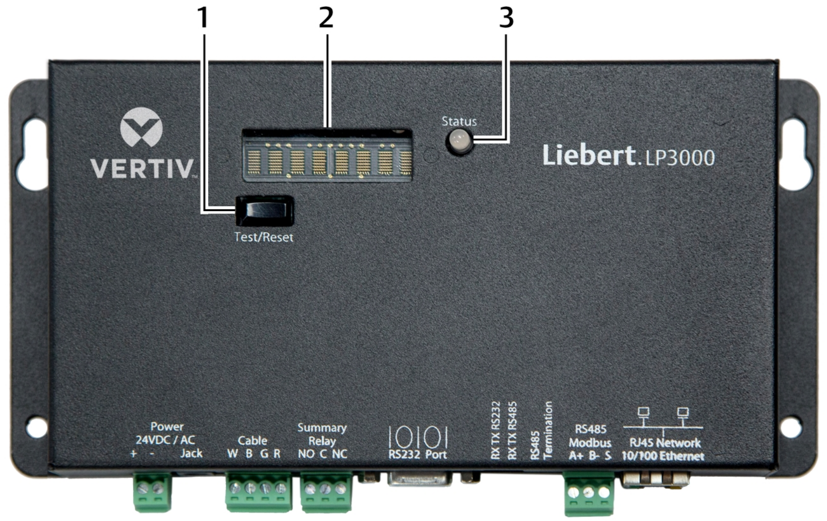
A Web-based user interface (UI) provides access to system conditions and settings on-site or via network communication.

In additon to the web-based UI, LP3000 communicates with external monitoring systems via the following outputs:

- Modbus via EIA-485, twisted-pair wire, or TCP/IP
- BACnet/IP or BACnet/MSTP
- SNMP

1.4 LP3000 Controls and Displays

Figure 3.2 LP3000 control and display options



ITEM	DESCRIPTION
1	Test/Reset button
2	Digital LED display
3	Status LED

1.4.1 Digital LED Display

During normal operation, the digital LED displays the product name with a spinning bar (|) to the right of the name.

When an alarm is present, information about the alarm condition displays. For example, if a leak is detected, a message about the location of the leak displays as follows:

```
Leak detected
250 uA
at 675 ft (or 205.74m)
```

1.4.2 Status LED

The color of the status LED indicates the operating state of the system.

- Green = powered-on and operating normally.
- Red = an alarm is present.

1.4.3 Test/Reset Button

The Test/Reset button runs a test cycle during normal operation and, during an alarm state, silences the audible alarm and clears alarms.

To silence the audible alarm:

When the alarm is sounding, briefly press Test/Reset.
The audible alarm turns off, the status LED remains red, and the digital LED continues to display the alarm condition.

To clear an alarm condition:

Press and hold Test/Reset whether the alarm is sounding or not.
The alarm clears.

To test the system

During normal operation, press Test/Reset.
The LED display cycles through the following 4 lines, then returns to the default display (un-less the Re-Alarm Interval is updated, an existing alarm may display. Refer to Leak Settings on page 23.)

```
LeakageC
nnnn uA
Length
nnn ft (or nnn m)
```

2 PREPARATION AND INSTALLING THE LIQUI-TECT SYSTEM

Installing the Liqui-tect system involves the following preparation before beginning:

- Choosing a readily-accessible location for the controller (wall mounted, rack mounted, under raised floor).
- Preparing the appropriate connections for power, leak detection, and communication.
- Consulting with your IT administrator to determine the following network settings for the LP3000 controller:
  - IP address
  - Subnet mask
  - Default gateway
- Creating a leak-detection cable layout diagram that considers the equipment in the area that may be damaged by water and the possible sources of leaks. Plan the cable layout to alert personnel when electronic equipment is threatened by a leak. An example of a layout diagram is included in Laying the Leak-detection Cable and Securing to the Floor on page 12.

Required Equipment and Supplies:

The following is included:

- Liqui-tect LP3000 controller
- CONNECT15 connection cable
- LT500-ET end terminator
- Isolated 24 VDC power supply with interchangeable blades
- Screws and anchors for wall mounting
- Crossover cable

The following equipment is sold separately:

- Leak-detection cable(s) of chosen length, 15-ft, 35-ft, or 50-ft
- LP3000-RMB rack-mount bracket

The following tools may be field-supplied, if needed:

- Electric drill (to drive screws or drill pilot holes)
- Screw driver
- Marker/Pencil to mark screw locations

2.1 Mounting the LP3000 Controller on a Wall

1. In the location determined during preparation, mark the wall for the mounting holes using the unit as a template.
2. If necessary, drill holes for the 4 screws that will secure the unit to the wall.
   - If the wall material is not strong enough, use the supplied wall anchors.
   - Clean up debris from drilling.
3. Install the 2 top screws, and hang the unit on the screws, allowing it to slip down so the screws are in the smaller part of the pear-shaped slot.

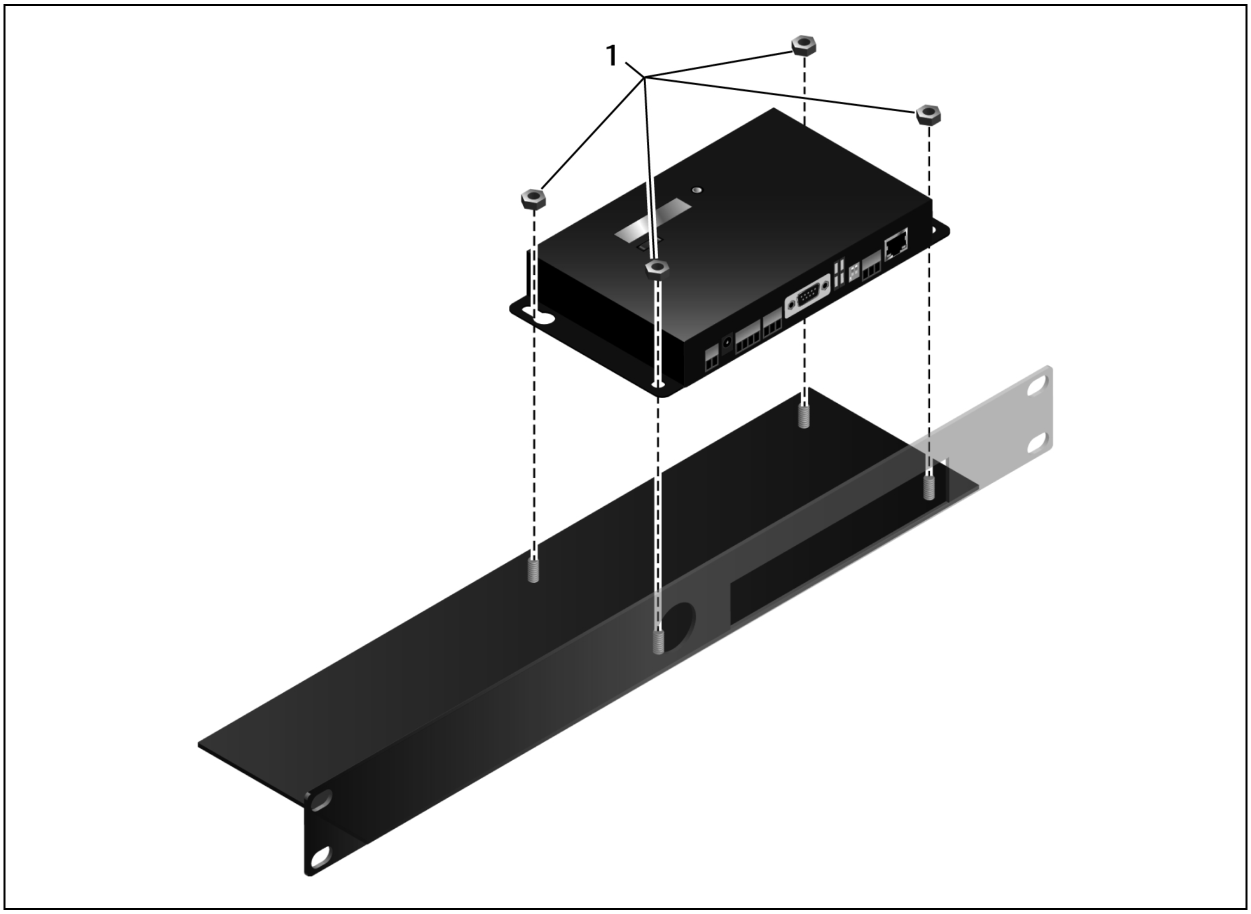
4. Tighten the screws until snug.
5. Insert the remaining 2 screws in the bottom holes and tighten.

2.2 Mounting the LP3000 Controller in a Rack

If using the optional rack-mount bracket, LP3000-RMB, install LP3000 in the bracket as follows.

1. Place the unit in the bracket with the connectors through the opening.
2. Using the 4 nuts, secure the unit to the bracket as shown in the figure below.

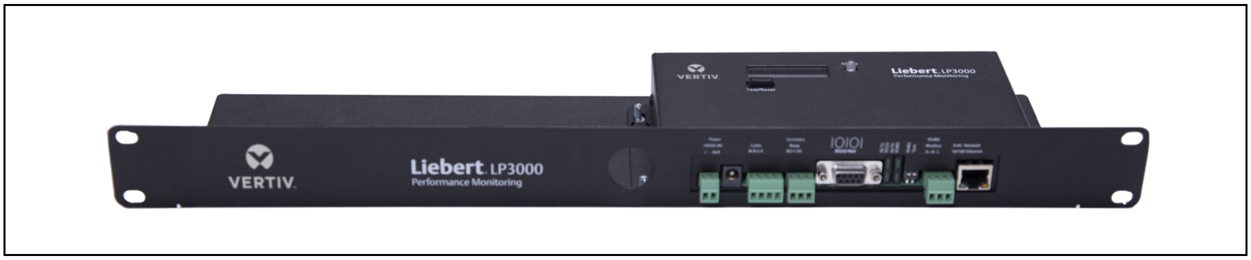
Figure 4.1 Tighten nuts in 4 places



ITEM	DESCRIPTION
1	Nut

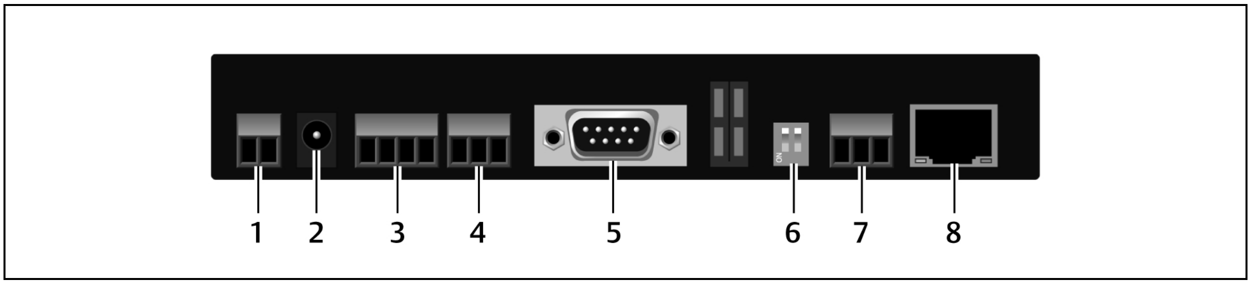
3. Install the bracket in the rack.

Figure 4.2 Liqui-tect installed in rack-mount bracket



2.3 Input and Output Connectors

Figure 4.3 Connections on Liqui-tect LP3000



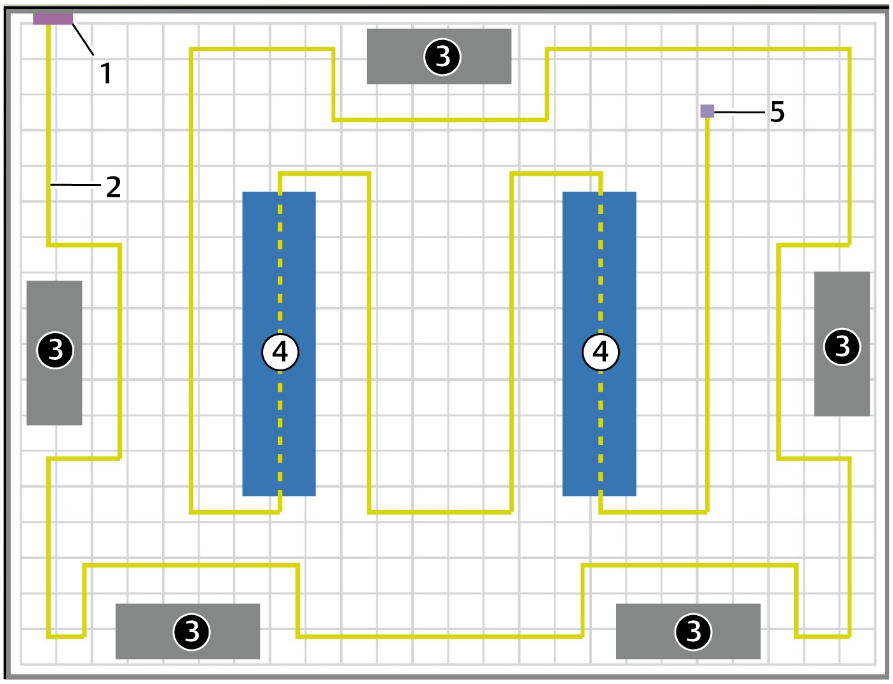
ITEM	DESCRIPTION
1	TB1 - input power
2	P1 - input power
3	TB2 - leak cable interface
4	TB3 - summary relay
5	P4 - EIA-232 connector
6	SW3 - EIA-485 termination
7	TB4 - EIA-485 Modbus port
8	P3 - RJ45 network port

2.4 Laying the Leak-detection Cable and Securing to the Floor

Refer to the site layout diagram for your installation, an example is shown in the following figure, and route the cable as indicated.

- The leak-detection cable may be placed in the ceiling if there is a liquid source to monitor.
- The cable may also be placed beneath a raised floor.

Figure 4.4 Example leak-detection cable layout diagram



ITEM	DESCRIPTION
1	Liqui-tect leak-detection monitoring system
2	Leak-detection cable (yellow)
3	Air-conditioning/Environmental units
4	Computer/Equipment rack
5	End terminator (at end of leak-detection cable run)

Observe the following guidelines and precautions when installing the leak-detection cable:

- Do not use conductive materials, such as Fire Block or caulk, on the leak-detection cable.
- Do not use any type of adhesive tape to secure the leak-detection cable.
- Do not use a leak-detection cable that is damaged or dirty for example, from plaster, spackle or debris.
- Do not drag the leak-detection cable through contaminants, such as dirt or grease.
- The floor must be clean for proper leak detection and for the hold-down clips to adhere. Use isopropyl alcohol to clean the spots on the floor for the hold-down clips.

- Use careful consideration to keep the leak-detection cable's route from the direct path of discharge air flow from air-conditioning or environmental equipment. If the cable is too close to the air stream, moisture from the discharge may cause false leak readings. Route the cable at least 6 ft (1.8 m) from discharge air flow to avoid nuisance alarms.
- Do not allow soldering or welding near the leak-detection cable without providing protection from heat and contamination. Also, avoid installing the cable near these types of areas.
- The clip’s adhesive backing does not work well on porous concrete floors. We recommend using a drop of silicone or another non-conductive adhesive to help secure the clip to the floor.

NOTE: If the leak-detection cable does become dirty or contaminated, refer to Troubleshooting on page 61 for steps to clean the cable.

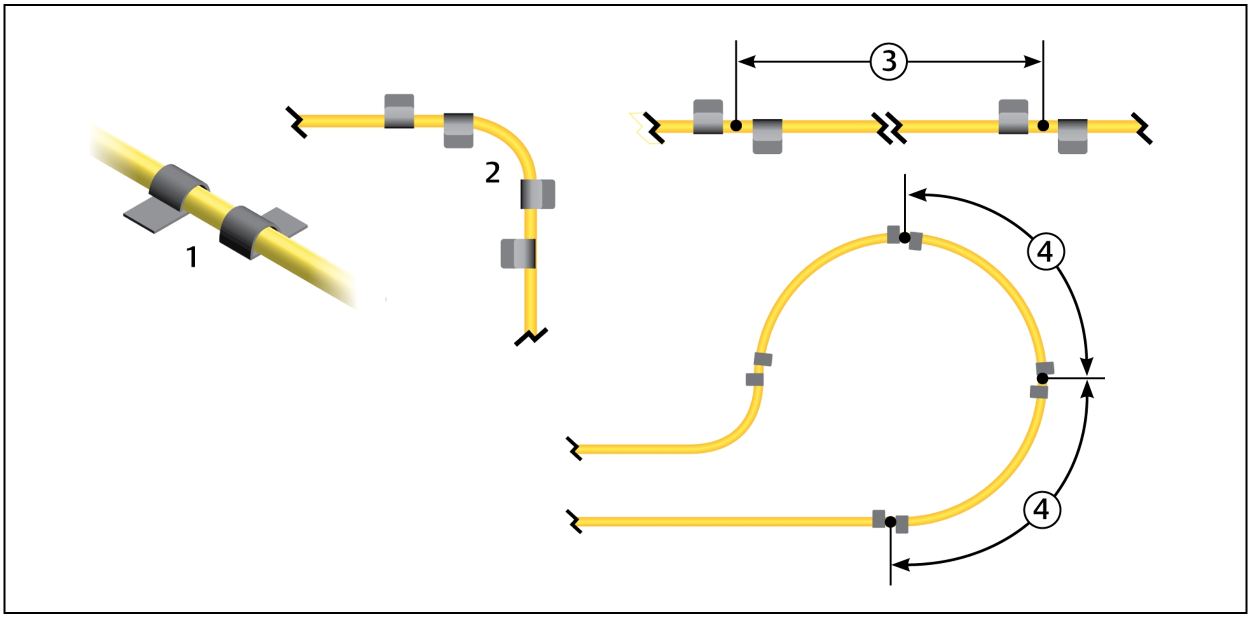
To install the cable:

1. Prepare the surface on which the leak-detection cable will be installed to avoid contaminating the cable. Clean the entire floor as much as possible.
2. Lay the cable in the pattern and route depicted in the layout diagram, maintaining consistent, uniform contact between the leak-detection cable and the floor.

3. Before inserting the cable in the clips, install the hold-down clips in pairs along the route as shown in the following figure.

CAUTION: Do not allow the adhesive used on the hold-down clips to come in contact with the leak-detection cable.

Figure 4.5 Hold-down clip installation



ITEM	DESCRIPTION
1	Install clips in pairs.
2	On a 90-degree turn, install 1 pair at the beginning of the arc and 1 pair at the end of the arc.
3	On straight sections, install 1 pair every 6 to 8 ft (1.8 to 2.4 m).
4	In a circular pattern, install 1 pair every 3 to 4 ft (0.9 to 1.2 m).

4. Allow the adhesive for the hold-down clips to dry completely, then snap the cable into each clip.
5. Make sure that there are no gaps between the floor and the cable, adding clips as needed.
6. If necessary, make adjustments to the cable-layout diagram to represent the cabling "as-installed." This diagram will be used to measure and map leak-detection landmarks when testing the installation.

You are ready to connect the leak-detection cable to the controller. See Connecting the Leak-detection Cable on page 15.

2.5 Connecting the Leak-detection Cable

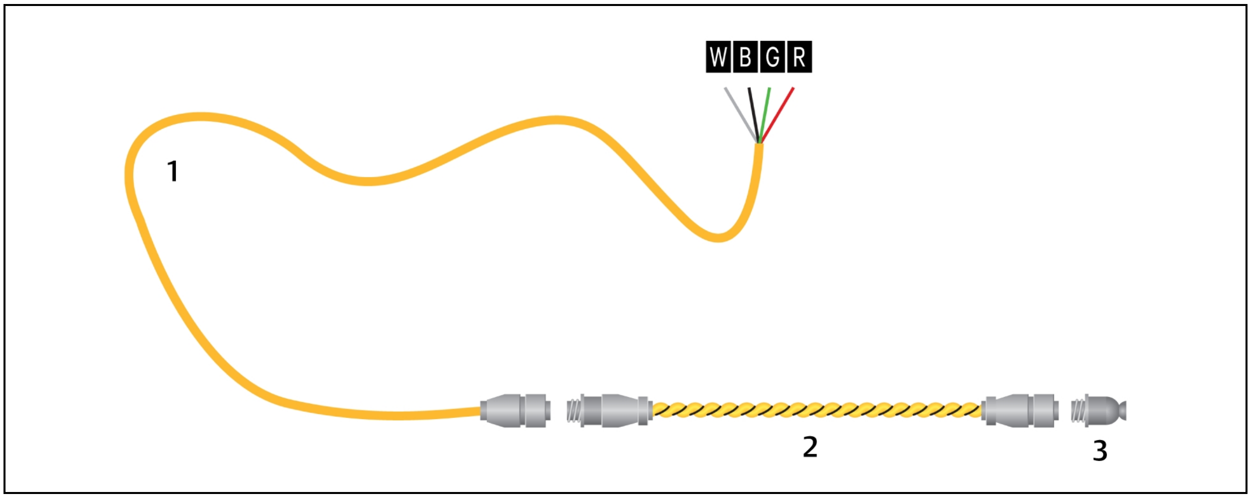
The leak-detection cable does not directly connect to the LP3000 controller. The 15-ft connection cable included with the system connects the controller to the leak-detection cable.

To connect the leak-detection cable to the controller:

1. With the screws of TB2 facing up on the controller, connect the 4, stripped, bare wires of the connector cable to the terminal block in the following order as shown in the following figure.
   - White
   - Black
   - Green
   - Red

NOTE: If the cable is removed from the terminal connector, make sure that the wires remain in the listed order when the connector is re-installed.

Figure 4.6 Connector cable and leak-detection cable connection to controller



ITEM	DESCRIPTION
1	Connector cable (CONNECT 15)
2	Leak-detection cable
3	End terminator (LT500-ET)

2. At the other end of the connector cable, unscrew the end terminator, and attach the male connector of the leak-detection cable to the connector cable as shown in the figure above.
3. Attach the end terminator to the end of the cable run and to the end of each branch-connector branch.

NOTE: A cable fault will register on the controller display if the end terminator is not attached.

You are now ready to connect power to the controller. See Connecting Power to Liqui-tect on page 16.

2.6 Connecting Power to Liqui-tect

⚠ **WARNING! Liqui-tect LP3000 requires an isolated power supply. Follow all state and local codes.**

1. Engage a certified electrician to run an isolated power supply to the location of the unit.
2. Connect power to the TB1 or P1 connector on unit, see Input and Output Connectors.
    - If using TB1, you may need to cut the barrel connector off the power supply and strip the ends of the wires to insert them into the terminal blocks.
3. Before applying power to the unit, make sure that all connections are correct and all screw terminals are secure.
4. Apply power and wait approximately 1 minute for the LP3000 to start up.
   There may be alarms because the leak-detection cable is not yet connected.
5. Verify that power is connected, and verify that the leak-detection cable is working by touching it with a clean, moist cloth or paper towel.
   If the cable is properly connected, an audible alarm sounds and an alarm notification displays on the digital display.

NOTE: Do not saturate the leak-detection cable for testing. A small amount of water triggers an alarm, and the cable must dry for the alarm to clear.

6. Dry the cable to remove the alarm condition. Use a hair dryer to speed up drying if needed.
7. Once you verify that the leak-detection cable is working, you are ready to calibrate the cable, map leak-detection points and test the installation. See Mapping and Testing the Installation on page 17.

2.7 Calibrating Resistance to Cable Length

The leak-detection cable has a base resistance of 4 ohms/ft. Because of manufacturing variances, the base resistance of each length of leak-detection cable may be slightly more or less than 4 ohms/ft, which means that the displayed length may be slightly more or less than the actual length of the cable.

While a configuration using base resistance values is very accurate, you can fine-tune the resistance to make it more precise to increase accuracy and bring the reported cable-length value in line with the actual cable length.

To calibrate cable resistance:

1. Make sure that the LP3000 controller is powered-on, has all sensing cables attached, and that there are no alarms.
2. Record the following data from the home page of the web UI:

DATA	RECORDED INFO
Cable length reported by LP3000.	
Cable current	
Leg 1 resistance	
Leg 2 resistance	

3. Select *Configuration* > *Leak Settings*, and record the following from the Leak Configuration page:

DATA	RECORDED INFO
Reported resistance per foot	

4. To calculate the actual length of the cable: Add the physical length of the cable (the sum of all of the lengths of installed cable) to the simulated length (the sum of all weighted lengths and branch connectors installed), refer to the following simulated lengths when determining the total simulated length.
   - LT500-WL simulates 35 ft
   - LT500-BC simulates 105 ft
   - Jumper cable adds 0 (zero) ft

   Calculate the actual length (physical length + simulated length) and record the result.

DATA	RECORDED INFO
Calculated actual length of cable	

5. Verify that the Cable Current recorded is less than 15 µA.
   - If the reading is higher than 15 µA, clean the cable using isopropyl alcohol to remove any contamination from installation.
6. Calculate the most-accurate resistance value by dividing the reported cable length by the actual cable length and multiplying the quotient by the reported resistance.

$$\left(\frac{\text{Reported Cable Length}}{\text{Actual Cable Length}}\right) \times \begin{array}{c}\text{Reported}\\ \text{Resistance}\end{array} = \begin{array}{c}\text{New}\\ \text{Resistance}\end{array}$$

7. On the Leak Settings page, enter the newly-calculated resistance-per-foot value and click *Submit Changes*.
   The reported cable length now more-closely matches the physical length of the cable and thereby improves leak-detected reporting accuracy.

2.8 Mapping and Testing the Installation

NOTE: If the LP3000 controller is already to connected to a BMS or NMS, notify monitoring personnel before beginning the test.

1. On the "as-installed" cable-layout diagram prepared after laying the leak-detection cable:
   - Mark the cable routing, connection points, equipment used in and monitored by the Liqui-tect system.
   - Mark the locations where leak detection is critical and the locations at which the leak-detection cable changes directions. These will be the locations measured and mapped during testing.
2. Before beginning, set the leak alarm delay to 5 seconds as follows:
   - On the web interface, click *Configuration* > *Leak Settings*.
     Leak Settings on page 23 opens.
   - In Leak Alarm Delay, enter 5, then click *Submit Changes*.
3. At each marked location on the diagram, use one of the following methods to simulate a leak, and record the reported distance on the diagram:

- Pour a small puddle of water on the cable while it rests on the floor.
- Dunk the cable in a cup of water.
- Soak a paper towel and wrap it loosely around the cable without putting pressure on the cable.

NOTE: To avoid inaccurate readings, do not grip the cable with your hand.

NOTE: Dry the cable to remove the leak alarm.

4. Verify that the simulated leaks are reported within a few feet of their actual, physical location based on the diagram.

NOTE: To fine tune the location of leak detections, see Calibrating Resistance to Cable Length on page 16.

5. When finished, remove the source of simulated leaks, reset the leak alarm delay, and return the system to normal operation.

You are ready to configure communication to the web user interface. See Initial System Communication Set Up on page 19.

3 INITIAL SYSTEM COMMUNICATION SET UP

Once the LP3000 controller and leak-detection cable are installed and tested, configure communication with the web UI.

3.1 Configuring Communication to the Web Interface

NOTE: Consult your IT administrator before configuring communication. If you intend to change the IP Address or Subnet Mask, obtain appropriate addresses from your IT department.

The default addresses for the LP3000 controller are:

- Default IP address: 169.254.24.7
- Default subnet mask: 255.255.0.0

If the address has been changed, use the following steps to get the IP address for the web interface.

Verify the IP address in use:

1. On the front of the LP3000 panel, press and hold the Test/Reset button.
   After 5 seconds, the versions and IP address scroll across the display.
2. Keep holding the display until you note the IP address of the LP3000 controller.
   When you release the button, the display resumes normal operation.

Connect the computer:

1. On the computer to use for configuration, make sure that WiFi is off and that DHCP is enabled.
2. Using the included cross-over cable, connect to the Ethernet port on the controller.
   It may take a minute or two for the computer to connect with the LP3000 controller.
3. Open a Web browser and enter the default IP address, 169.254.24.7, in the address bar.
   The Authentication Required dialog opens.
   - If the authentication dialog does not appear, temporarily change the computer's IP address to the following: IP address 169.254.24.10, subnet mask 255.255.0.0 then re-enter the default IP address in the web browser.
4. Enter the default read/write user name and password:
   - Default user name: Liebert (case sensitive)
   - Default password: Liebert (case sensitive)

   The Web UI opens to the home page.
5. On the home page, select *Configuration* > *Network Settings*.
   Network Settings opens.
6. Enter the values provided by the IT administrator in IP Address, Net Mask (subnet mask), and Def Route (default gateway), and click *Submit Changes*.
7. Connect LP3000 to the network with an Ethernet cable.

NOTE: The cross-over cable is not intended to be connected to a network hub, and will not work if it is connected to a hub.

8. Verify that the change is successful, open a web browser and enter the new IP address entered for the LP3000 controller, then enter the default user name and password (from Step Enter the default read/write user name and password: on page 19).
   The home page opens.

- If the authentication window does not display, make sure that all cables are firmly attached, that you entered the correct IP address, and that the Status LED on the controller is lit green.

4 USING THE WEB INTERFACE

Use the Liqui-tect web user interface (UI) to configure leak-detection and to monitor system status.

NOTE: The default IP address for the LP3000 controller is 169.254.24.7. This may have been changed. If the address has been changed, use the following steps to get the IP address for the web interface.

Verify the IP address in use:

1. On the front of the LP3000 panel, press and hold the Test/Reset button.
   After 5 seconds, the versions and IP address scroll across the display.
2. Keep holding the button until you note the IP address of the LP3000 controller.
   When you release the button, the display resumes normal operation.

To log-in to the web UI:

1. Open a web browser, and enter the LP3000 controller's IP address in the address bar.
   The authentication dialog opens.
2. Enter a User Name and Password, and click *Log In*.
   The default user name and password are as follows. This may have been changed. Contact your Liqui-tect system administrator for the assigned user name and password.
   - Default user name: Liebert (case sensitive)
   - Default password:

     Read-only access: There is no default password, leave the field blank.

     Read/Write access: Liebert (case sensitive)

   The web UI opens to the Liqui-tect Home Page on page 21.

4.1 Liqui-tect Home Page

The home page displays system information, including current alarm status, the reported length of the connected leak-detection cable, the last time an alarm activated, and the running system up-time. The image can be linked to interactive floor maps.

- To access the home page, click *Home* on the menu bar.

Table 6.1 Liqui-tect home page fields

FIELD	DESCRIPTION
Alarm Status	Details of alarm, if an alarm is present. The field changes color depending on type of alarm.
Cable Length	Calculated length of the connected leak-detection cable. See Calibrating Resistance to Cable Length on page 16 for a description of how Liqui-tect calculates the length.
Cable current	Amount of current running through the leak-detection cable.
Leg 1 Resistance	Resistance, in Ohms, of Leg 1.
Leg 2 Resistance	Resistance, in Ohms, of Leg 2
Leak Alarm Delay Count	Time delay, in seconds, that passes between leak detection and alarm notification.
Contamination Alarm Delay Count	Time delay, in seconds, that passes between contamination detection and alarm notification.
Re-alarm Countdown	Time remaining before an alarm is re-annunciated.
Last Alarm Time	Time the last alarm notification occurred.
sysUp Time	Time passed since system was reset or powered-on.

4.2 Identity Page

The Identity page displays the Liqui-tect model and system information. This page is a reference screen, and any adjustments are made using the Configuration Menu on page 22.

4.3 Configuration Menu

The Configuration Menu page lists options to adjust Liqui-tect system settings.

NOTE: When editing any configuration items, be sure to click *Submit Changes* to save the changes. If you navigate from the page without submitting, the changes are lost.

The configuration options are:

- Leak Settings on page 23
- Zone Settings on page 25
- Virtual Zone Settings on page 25
- Physical Zone Settings on page 26
- Zone Link/URL Settings on page 26
- Network Settings on page 27
- Web/Map Settings on page 27
- Clock Configuration on page 31
- NTP Configuration on page 31
- Email-SMTP/DNS Configuration on page 31
- SNMP/Syslog Configuration on page 32
- EIA-485 Port/Modbus Configuration on page 34
- BACnet Configuration on page 39
- Alarm Management on page 41
- System/Flash Management on page 42

4.3.1 Leak Settings

The Leak Settings page configures system variables including leak and contamination thresholds, latching and un-latching alarms, and leak-detection cable resistance.

Table 6.2 Leak Settings fields and options

FIELD	DESCRIPTION
Leak Trip Point	Threshold for amount of water to trigger a leak-detection alarm. Sets the sensitivity of the alarm. A lower number equals greater sensitivity, which triggers an alarm with less water. A higher number equals less sensitivity, requiring more water to trigger an alarm. Default: 150 µA.
Contamination Trip Point	Threshold for amount of contamination to trigger a contamination alarm. Sets the sensitivity of the alarm. A lower number equals greater sensitivity, which triggers an alarm with less contamination. A higher number equals less sensitivity, requiring more contamination to trigger an alarm. Default: 50 µA.
Leak Alarm Delay	Time delay between leak detection and alarm notification. The leak must be detected during the entire delay to trip the alarm. Default: 20 seconds.
Contamination Alarm Delay	Time delay between contamination detection and alarm notification. The contamination must be detected during the entire delay to trip the alarm. Default: 120 seconds.
Resistance Per Foot	Sets accuracy of distance-to-leak reporting. The resistance per foot (meter) determines the ability to detect cable length and distance to leaks. Must be a 4-digit number formatted: x.xxx. For further information on resistance and accuracy, see Calibrating Resistance to Cable Length on page 16. Default: 4.000 ohm.
Re-Alarm Interval	Defines interval at which notification for an un-resolved alarm condition is re-sent. Zero (0) disables re-send, sending a single notification. Default: 0 (disabled).
Measurement Display	Selects unit of measure for system/display. Default: feet.
Latching Alarm	Selects automatic alarm reset or manual alarm reset. • Yes = Latching—alarm must be reset manually even if alarm condition is resolved. • No = Non-latching—alarm resets automatically when leak or contamination is resolved. Default: No.
Audible Alarm	Enables/Disables audible alarm notification. Default: Enabled.
Length Calibration Factor	Display-only, factory-set calibration.
Set Cable Relay Button	Leak-detection cable simulation for troubleshooting the controller. See Troubleshooting Controller Using Set Cable Relay on page 24.

4.3.2 Troubleshooting Controller Using Set Cable Relay

Set Cable Relay simulates 8060 ohms of leak-detection cable for a period up to 5 minutes.

To test controller operation:

1. Click *Configuration > Leak Settings*.
   Leak Settings on page 23 opens.
2. Click *Set Cable Relay*, then click *Home*.
3. On the Liqui-tect Home Page, confirm proper function by verifying that the displayed values match those listed for the fields that follow:
   - Cable Length = approximately 2015 ft
   - Leg 1 Resistance = approximately 8060 ohms
   - Leg 2 Resistance = approximately 8060 ohms

4.3.3 Zone Settings

Zones are identified areas in which leak-detection cabling is installed. Using zones helps locate leaks quickly and simplifies troubleshooting by helping isolate cable sections and defined areas in other rooms.

You can configure up-to 32 zones for LP3000. The LP3000 controller is the "master" unit with up-to 31 virtual zones and physical (slaved hardware devices) zones connected.

LP3000 uses two types of zone:

- Virtual zone—a labeled reference point in the Liqui-tect system including entire rooms, a detection component in a drip pan, or any defined area to help locate detected leaks. Use the Zone Configuration page, described below, and Virtual Zone Settings on page 25 to set-up virtual zones.
- Physical zone—a "slaved" hardware device connected to a master LP3000 controller. See Physical Zone Settings on page 26 and Configuring the Controller as a Modbus Master on page 35 to set-up physical zones.

NOTE: The total number of virtual and physical zones is 32. Zone 1 is always the master unit. Virtual zones are "slaves" and assigned after the master, starting with zone 2. Physical zones are "slave" leak-detection devices and are assigned after virtual zones. The total number of "slave" zones available is 31 (zones 2 to 32), so plan accordingly.

NOTE: The serial address/slave ID assinged to a virtual zone or device must be identical to the zone number when using the LP3000 controller as a Modbus master. See Configuring the Controller as a Modbus Master on page 35.

To Set Up Virtual Zones:

1. Click *Configuration* > *Zone Settings*.
   Zone Configuration opens.
2. Enter the number of virtual zones to configure, and select the trap and alarm-relay settings, then click *Submit Changes*.
3. Refer to Virtual Zone Settings on page 25 to configure the zones.

Table 6.3 Zone Settings fields and options

FIELD	DESCRIPTION
Number of Virtual Zones	Sets the number of virtual zones to configure for the system/facility.
Modbus Zone Traps	Enables/Disables SNMP traps when the Liqui-tect controller is set as Modbus master. Default: Disable.
Enable Alarm Relay for Modbus Slaves	Enables/Disables the summary alarm when a slaved leak-detection device has an alarm condition. Default: Disable.

4.3.4 Virtual Zone Settings

Virtual Zone Configuration defines the virtual zones in your installation.

Table 6.4 Virtual Zone Configuration fields and options

FIELD	DESCRIPTION
Zone #	Number designating a zone. The number of virtual zones is set with Zone Settings on page 25.
Label	Descriptive label for the zone displayed in notifications and event logs. 30-character limit.
End Distance	Distance on the leak-detection cable at the end of the zone. Zone #1 always starts at 0 (zero), and the end of zone 1 is designated by distance from start. The each subsequent zone starts at the End Distance of the previous zone.

4.3.5 Physical Zone Settings

Physical zones represent actual hardware connected to the Liqui-tect system. Physical Zone Configuration defines the connected hardware in your installation.

NOTE: To display on this page, the devices must be connected in a master/slave configuration. See Configuring the Controller as a Modbus Master on page 35 The figure that follows shows no physical slave devices connected.

NOTE: The serial address/slave ID assigned to a physical slave device must be identical to the zone number when using LP3000 as a Modbus master.

Table 6.5 Modbus/Physical Zone Configuration fields and options

FIELD	DESCRIPTION
Zone #	Number designating a zone.
Label	Descriptive label for the zone (that is, the unit or device). Displayed in notifications and event logs.
Enable Comm Type	Type of communication used by unit. Depends on the type of connection used: • When using the EIA-485 port, select RS-485. • When using the Ethernet port, select Modbus/TCP or Modbus/UDP depending on the type of Modbus communication used by the device.
Serial Address/Slave ID	When using EIA-485 port, sets the serial address for slaved devices. When using Ethernet port/Modbus communication, sets the slave-ID address for slaved devices. In both cases, the number must match the address/ID assigned to the device for EIA-485 Port/Modbus communication, and it must match the zone number.
IP Address	For Ethernet port communication, sets the IP address for the slaved devices

4.3.6 Zone Link/URL Settings

You can add links to additional information about devices connected to the LP3000 controller. This is useful for accessing the web interface of slaved Liqui-tect units.

Up to 32 links may be configured. The links are displayed in the lower left side of the Liqui-tect Home page.

Table 6.6 Zone Link/URL Configuration fields and options

FIELD	DESCRIPTION
Zone	Designates the zone associated with the link.
Link Text	Displayed text for the link.
URL	URL to which the link connects.

4.3.7 Network Settings

The Network Settings/IP Configuration page displays the device's MAC address and configures the network communication settings for the web UI.

CAUTION: Incorrect network settings will make the web UI inaccessible. Consult with your IT/network administrator before making any changes.

Table 6.7 IP Configuration fields and options

FIELD	DESCRIPTION
MAC Address	Display-only, unique identifier set by device manufacturer.
IP Address	Sets the IP address of the LP3000 controller. Default: 169.254.24.7.
Net Mask	Sets the subnet address of the LP3000 controller. Default: 255.255.0.0.
Def route	Designates the default gateway of the device.
Tcp Max Seg Size	Selects packet size. • 1436 = packet size for web-page data. • 536 = packet size for limited bandwidth or VPN applications.
Disable Network Watchdog	Reboots device in the event of excess network traffic or detected errors.

4.3.8 Web/Map Settings

The Web Configuration page provides several configuration and customization options:

- Customize the user name and password for the web UI.
- Customize the home page graphics and links.
- Create an interactive leak-detection map.

Table 6.8 Web Configuration fields and options

FIELD	DESCRIPTION
Web Username	Sets user name to access web UI. Default: Liebert.
Web Password Read Only	Sets password for view-only access to web UI. Default: blank.
Web Password Read/Write	Sets password for view and edit access to web UI. Allows updates to Liqui-tect configuration. Default: Liebert.
Web Refresh Rate	Sets frequency to check for new data and reload web page. Zero (0) disables automatic refresh.
Main Page Image	Selects an image or interactive map to display on home page. See Uploading Images on page 44.
Main Page/Zone 1 Link Text	Displayed text for the link, see the figure that follows. Zone 1 may also be configured via Zone Link/URL Settings on page 26. Updates made using either option, are reflected on the other.
Main Page/Zone 1 Link URL	URL to which the link connects.
Floor Map #1 Link Text	Displayed text for the link, see the figure that follows.
Floor Map #2 Link Text	Displayed text for the link, see the figure that follows.
Floor Map #1 Interactive	Enables/Disables Interaction with Floor Map #1. See Facility Reference Maps on page 28 to set up an interactive map.

Facility Reference Maps

You can upload up to 2 facility maps and add interactive leak-detection data to map 1 for real-time leak-detection equipment location and status and for active-alarm location.

The mapping process creates an overlay for an uploaded map image based on coordinates designated using the Map Alarm links at the bottom of the Web/Map Settings on page 27.

NOTE: Do not attempt interactive mapping before the monitored area is completely installed and assembled and all leak-detection equipment is in place, tested and functional.

The file requirements for the uploaded map image are:

- File size: 500 kb or less
- Image dimension/size: 4000 x 4000 pixels or less
- File format: .png, .jpg or .gif

When the Liqui-tect system and facility map(s) are ready, see Uploading a Reference Map on page 29.

Uploading a Reference Map

1. Select *Configuration* > *System/Flash Management*.
   System/Flash Management on page 42 opens.
2. In *Image Index*, select the number of the image to upload.

NOTE: Uploading a file to an index that already contains a file overwrites the file.

3. Click *Choose File* and browse to select the image file , then click *Upload*.
   The map is uploaded.
4. Select *Configuration* > *Web/Map Settings*, enter a title for the image in the appropriate Floor Map # Link Text field, and click *Submit Changes*.
5. See Marking Interactive Reference Points on the Map on page 29 to add the interactive coordinates.

Marking Interactive Reference Points on the Map

After the map is uploaded, mark reference points to which you can refer when a leak is detected.

NOTE: The references are an overlay on the map image. If the map image needs minor adjustments, you do not need to reconfigure reference points if the replacement image is the same size (pixels x pixels) as the previous image and the layout does not change.

To mark reference points:

1. Select *Configuration* > *Web/Map Settings*, select Yes for Floor Map #1 Interactive, then click *Map Alarm Coordinates - Graphical*.
   An enlarged view of the map opens in the browser window.
2. Set the reference point for the beginning of the leak-detection cable:
   - In the Enter a distance field, enter 0 (zero).
   - On the map, click the beginning of the leak-detection cable.
     The distance and x-y coordinates are saved creating the reference point at the center of the cross hairs.
3. Continue entering distances and clicking points on the map for each reference point.

NOTE: We highly recommend that you enter a distance/point each time the leak-detection cable changes direction.

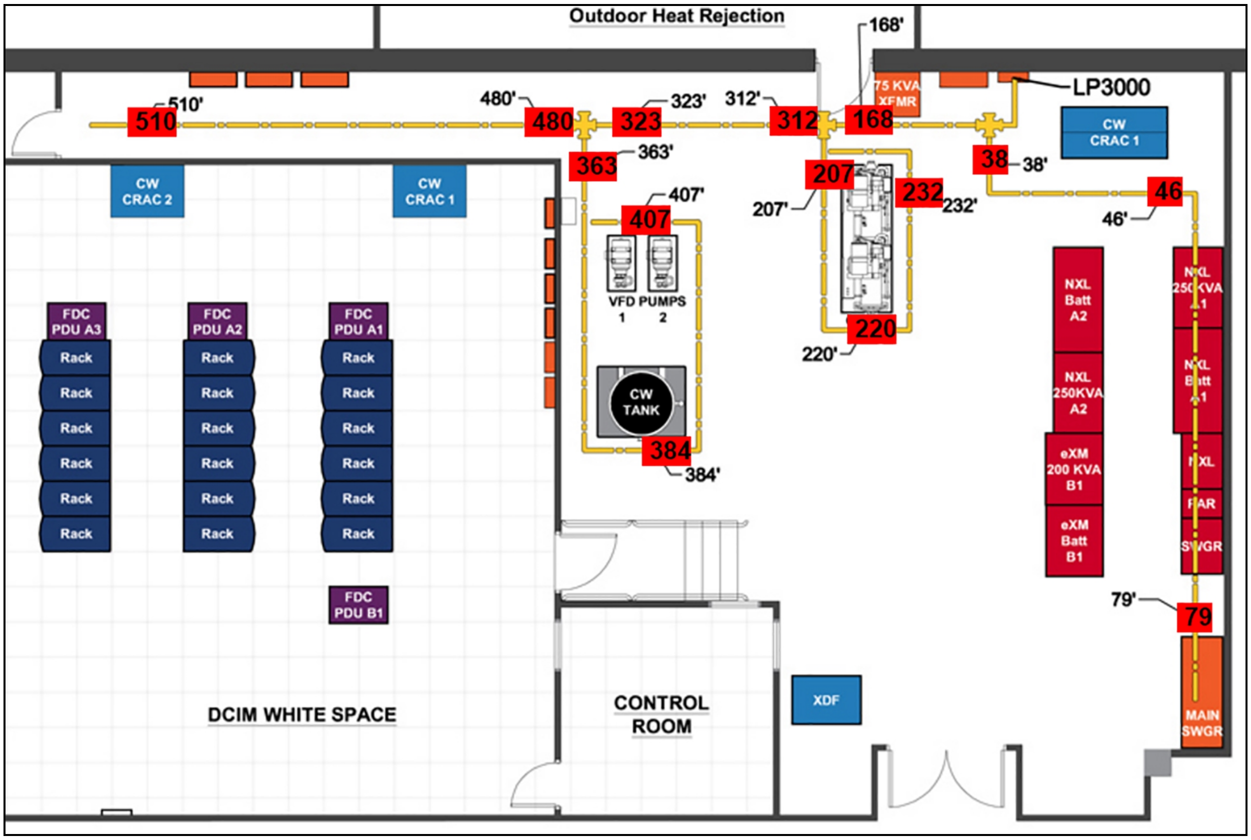
- To verify the reference points, see Testing Mapped Reference Points on page 30.
- To adjust reference points after marking, see Adjusting Map Reference-point Coordinates on page 30.

When a leak is detected, it's location is displayed as a red square on the map. See Viewing the Reference Map on page 30.

Testing Mapped Reference Points

1. Select *Configuration > Web/Map Settings*.
2. Click *Map Alarm Test*.
   The map opens with all of the reference points and their distances displayed in a red, "leak-detection" box as shown in the following figure.

Figure 6.1 Mapped reference points test



Adjusting Map Reference-point Coordinates

1. On the Web/Map Settings page, click *Map Alarm Coordinates - Text*.
   Map Alarm Coordinates opens.
2. Update distances and x-y coordinates as needed, then click *Submit Changes*.

Viewing the Reference Map

On the Liqui-tect Home Page, click the titled button below the map image for the map to view. An enlarged reference map opens in a web browser.

Saving a Map Image

We recommend saving a copy of map images along with the back-up configuration file because the map-image files are not saved in the configuration file.

To save a back-up map image:

1. On the Liqui-tect Home Page, click the titled button for the map below the image.
   The enlarged map opens in the web browser.
2. Right-click the image, and select *Save Image As* from the pop-up menu.
   The Save Image dialog opens.
3. Browse to the location of the back-up configuration file, enter a descriptive file name if needed, and save the image.

4.3.9 Clock Configuration

The Clock page adjusts the date and time settings for LP3000.

Table 6.9 Clock Configuration fields and options

FIELD	DESCRIPTION
Date	Sets the current date.
Time	Sets the current time.
Day	Display-only, day of week calculated from date setting.

4.3.10 NTP Configuration

The NTP (Network Time Protocol) synchronizes computer-system clocks on connected devices. This maintains accuracy and reliability for time-stamped events.

Table 6.10 NTP Configuration fields and options

FIELD	DESCRIPTION
NTP Server	IP address or host name of NTP server with which [[[Undefined variable Liquitect.ModelNo]]] synchronizes time. Public servers include us.pool.ntp.org or time.nist.gov.
Update Interval	Frequency at which synchronization occurs. Zero (0) disables synchronization.
Select Time Zone	Sets the time zone employed.
Daylight Savings Time	Enables/Disables use of Daylight Savings Time. When enabled, selects the time at which savings time goes into effect.
DST Begin Date	Selects the day/month daylight savings begins.
DST End Date	Selects the day/month daylight savings ends.

4.3.11 Email-SMTP/DNS Configuration

The Email-SMTP/DNS page configures email and SMTP settings.

Table 6.11 Email Configuration fields and options

FIELD	DESCRIPTION
Access Type	Enables/Disables e-mail alerts via local network connection. • LAN = enable e-mail alerts. • None = disables alerts.
Email Contamination Alarms	Enables/Disables e-mail alerts for contamination alarms. Disable in the case of frequent false alarms.
Primary DNS Server	IP address of primary DNS server (provided by internet service provider).
Secondary DNS Server	IP address of secondary DNS server (provided by internet service provider).
Mail (SMTP) Server	URL of mail server.
Mail Sender Address	Address for mail sent by Liqui-tect.
Mail Subject	Subject line of e-mail.
Mail Recipient (1)	Address of e-mail recipient.
Mail Recipient (2)	Address of e-mail recipient.
Mail Recipient (3)	Address of e-mail recipient.
Mail Recipient (4)	Address of e-mail recipient.
Smtp Authentication	For ESMTP, leave at default unless otherwise directed by your IT administrator.
Smtp Username	For ESMTP, leave at default unless otherwise directed by your IT administrator.
Smtp Password	For ESMTP, leave at default unless otherwise directed by your IT administrator.
View Smtp Log / Send Test Email	Opens log of e-mails sent by Liqui-tect and displays an e-mail test button. See Sending a Test E-mail on page 32.

4.3.12 Sending a Test E-mail

1. Click *Configuration > Email-SMTP/DNS*.
   Email-SMTP/DNS Configuration on page 31 opens.
2. At the bottom of the page, click *View Smtp Log*.
   The Email Log opens.
3. Click *Send Test E-mail*.
   An e-mail containing the SMTP log is sent.

4.3.13 SNMP/Syslog Configuration

The SNMP/Syslog page configures SNMP communication including SNMP traps. The page also allows testing the traps, refer to the following:

- Sending a Leak-detection Test Trap on page 33
- Sending a Cable-break Test Trap on page 34
- Sending a Contamination Test Trap on page 34

Table 6.12 MIB-2 System options

FIELD	DESCRIPTION
System Name	Name of the system. Displays below the menu bar and is included in e-mail notifications. 30-character limit.
System Contact	Indicates person responsible for the Liqui-tect system. Only available through SNMP Gets. Not included in e-mail or SNMP Trap notifications. 30-character limit.
System Location	Physical location of the Liqui-tect system. Not included in e-mail or SNMP Trap notifications.

Table 6.13 V1/V2C Community Names options

FIELD	DESCRIPTION
Get/Read	Community for get/read access.
Set/Write	Community for set/write access.
Trap	Community for trap access.

Table 6.14 Traps options

FIELD	DESCRIPTION
Select SNMP Trap Type	Selects the version of SNMP trap to use. • V1-Trap • V2C-Trap • V2C-Inform
Max Inform Retries	Number of re-send attempts for un-delivered traps. Zero (0) allows unlimited attempts.
Inform Interval	Length of time between re-send attempts.

Table 6.15 Trap Destinations options

FIELD	DESCRIPTION
IP Address	IP address of the receiving device. All zeros (0.0.0.0) enables any device to access LP3000 through an MIB broswer.
TrapEnable	Enables/Disables if device will receive traps.
Syslog Message	Enables/Disabes if device will receive system log messages.

Table 6.16 SnmpV3 options

FIELD	DESCRIPTION
Engine ID	Read-only display of engine ID.
Context Name	Alphanumeric name of the SNMP v3 interface.
User Name	Unique name for each user.
Access Mode	Selects mode of access for the user. • No-Auth - requires a user name, but not a password. • Auth-MD5 - requires a user name and password. • PrivAuth-MD5 - requires a user name and password.
Auth-Password	Sets the authentication password. 8 to 24 characters in length.
Priv-Password	Sets the privacy password. 8 to 24 characters in length.

Sending a Leak-detection Test Trap

1. Click *Configuration > SNMP/Syslog*.
   SNMP/Syslog Configuration on page 32 opens.
2. At the bottom of the page, click *Send Test Trap - Leak Detected*.
   The test message is sent.

Sending a Cable-break Test Trap

1. Click *Configuration > SNMP/Syslog*.
   SNMP/Syslog Configuration on page 32 opens.
2. At the bottom of the page, click *Send Test Trap - Cable Break*.
   The test message is sent.

Sending a Contamination Test Trap

1. Click *Configuration > SNMP/Syslog*.
   SNMP/Syslog Configuration on page 32 opens.
2. At the bottom of the page, click *Send Test Trap - Contamination*.
   The test message is sent.

4.3.14 EIA-485 Port/Modbus Configuration

Use this port-configuration page to set up the LP3000 controller as a Modbus "master" to communicate with the "slave" devices through the EIA-485 or Ethernet port. For slaved devices, use the web interface of each slave to configure communication with the master LP3000 controller. See Configuring the Controller as a Modbus Master on page 35 for the detailed set-up steps.

The page also sets-up access to BACnet-MS/TP slave devices and accesses the Modbus slave-register log, statistics and packet log. See Viewing the Modbus Slave-register Log on page 34, and Viewing the Modbus Packet Log on page 35.

NOTE: The options listed may differ from your screen depending on the port function selected.

Table 6.17 Modbus/EIA-485 Configuration fields and options

FIELD	DESCRIPTION
Modbus/TCP/UDP Slave Unit Identifier	If using the Ethernet port for a master/slave set-up, selects the slave-unit number designation for the device.
EIA-485 Port Function	Selects the function of the EIA-485 port for the LP3000 controller: • Modbus-Slave • Bacnet-MS/TP-Slave (only available on port 2) • Modbus-Master Note: Click *Submit Changes* after making the selection to display the options for selected function. See Configuring the Controller as a Modbus Master on page 35.
EIA-485 Baud Rate	Selects the baud rate for the port.
EIA-485 Parity	Selects the parity for the port.
EIA-485 Slave Address	Selects the slave address for the port.

Viewing the Modbus Slave-register Log

1. Click *Configuration > EIA-485 Port/Modbus*.
   EIA-485 Port/Modbus Configuration on page 34 opens.
2. At the bottom of the page, click *Modbus Slave Register Display Log / Statistics*.
   The log opens in the web browser.

Viewing the Modbus Packet Log

1. Click *Configuration > EIA-485 Port/Modbus*.
   EIA-485 Port/Modbus Configuration on page 34 opens.
2. At the bottom of the page, click *Modbus Packet Log*.
   The log opens in the web browser.

4.3.15 Configuring the Controller as a Modbus Master

The LP3000 controller can monitor and control other Liqui-tect units in a "master/slave" configuration using Modbus communication. Up to 31 other Liqui-tect panels can be connected and their status and alarms viewed through the "master" controller.

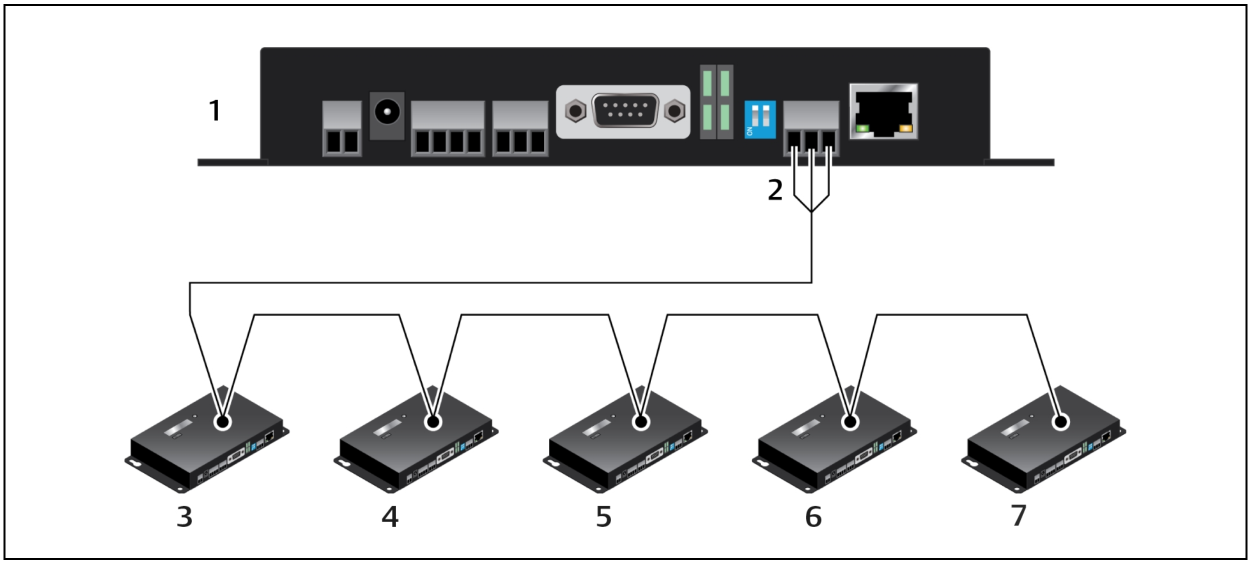
Setting up a Master/Slave system requires two steps. Connecting the slave units to the master unit, then configuring the Modbus communication settings for each device depending on type of connection:

- Connecting to the EIA-485 Port on page 35.
- Connecting to the Ethernet Ports on page 37.

4.3.16 Connecting to the EIA-485 Port

1. Referring to the EIA-485 connection diagram below, use a 2-wire configuration to connect the EIA-485 ports of the master and slave units in a daisy chain.

Figure 6.2 EIA-485 connection diagram



ITEM	DESCRIPTION
1	Master device - slave address 1 Note: The EIA-485 Slave Address must be 1 for the master device.
2	TB4 - EIA-485 port
3	Slave device - slave address 2. Note: If you have virtual zones configured, the serial addresses start after the virtual zones. For example, if this set up had 5 virtual zones, the slave addresses would start at 7.
4	Slave device - slave address 3 Note: Each slave address must be consecutive.
5	Slave device - slave address 4
6	Slave device - slave address 5
7	Slave device - slave address 6

2. Configure the master device:
   - Open the web UI for the LP3000 master controller and click *Configuration > EIA-485 Port/Modbus*.
     EIA-485 Port/Modbus Configuration on page 34 opens.
   - In Select EIA-485 Port Function, select *Modbus-Master*.
   - Select the EIA-485 Baud Rate and EIA-485 Parity.
   - In EIA-485 Slave Address, enter **1**.
   - Click *Submit Changes*.
     The controller is configured as the master device.

NOTE: The Slave Address for the Master device must be 1.

3. Configure the slave device:

NOTE: The slaved devices are "physical" zones. If you have virtual zones configured, the serial addresses start after the virtual zones.

NOTE: The serial address must be identical to the zone number.

   - Open the web UI for the slave device, and click *Configuration > EIA-485 Port/Modbus*.
     EIA-485 Port/Modbus Configuration on page 34 opens for the slaved unit.
   - In Select EIA-485 Port Function, select *Modbus-Slave*.
   - Select the EIA-485 Baud Rate and EIA-485 Parity to match that of the Modbus master.
   - In EIA-485 Slave Address, enter the slave address of the device. Start with the first available address and assign the next consecutive number to each unit in the chain.
   - Click *Submit Changes*.

4. Repeat Step Configure the slave device: on page 36 for each slaved device.

5. Configure the physical zones:

NOTE: If you have virtual zones configured, the serial addresses for the devices start after the virtual zones.

NOTE: The zone number and the slave address of the device must be identical.

- Open the web UI for the master controller, and click *Configuration > Physical Zone Settings*.
  Physical Zone Settings on page 26 opens.
- In Enable Comm Type, select *RS-485*.
- Click *Submit Changes*.

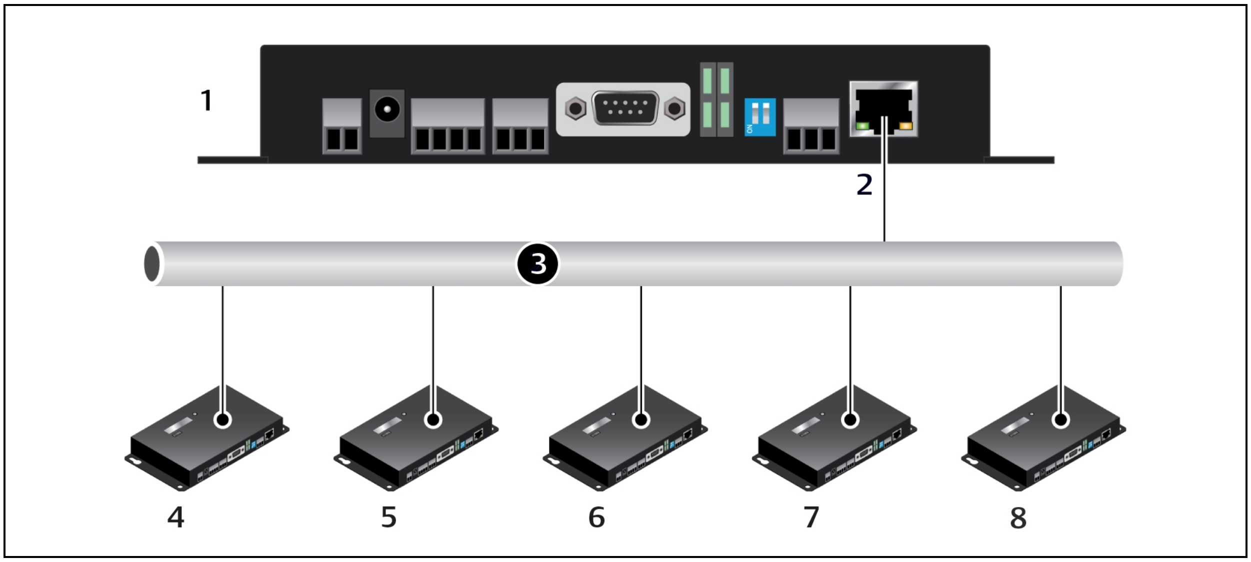
We recommend generating an alarm from each slave unit to confirm proper communication.

4.3.17 Connecting to the Ethernet Ports

When used as a Modbus master, LP3000 can be connected to the slave units via the local network connection, using TCP/IP or UDP/IP as follows:

1. Referring to the Ethernet-port connection diagram below, connect the Ethernet port of the master unit to the local area network.
2. Connect the Ethernet ports of the slave units to the local area network.

Figure 6.3 Ethernet-port connection diagram



ITEM	DESCRIPTION
1	Master device - Slave ID 1 Note: The Slave ID must be 1 for the master device.
2	P3 - Ethernet port
3	Local Area Network
4	Slave device - Slave ID 2. Note: If you have virtual zones configured, the slave IDs start after the virtual zones. For example, if this set up had 5 virtual zones, the slave IDs would start at 7.
5	Slave device - Slave ID 3 Note: Each slave ID must be consecutive.
6	Slave device - Slave ID 4
7	Slave device - Slave ID 5
8	Slave device - Slave ID 6

NOTE: Modbus communication uses port #502 for the IP address.

3. Configure the master device:
   - Open the web UI for the LP3000 master controller and click *Configuration > EIA-485 Port/Modbus*.
     EIA-485 Port/Modbus Configuration on page 34 opens.
   - In Modbus/TCP/UDP Slave Unit Identifier, enter **1**.
   - Click *Submit Changes*.
     The controller is configured as the master device.

NOTE: The Slave ID for the Master device must be 1.

4. Configure the slave devices:
   - Open the web UI for the slave device, and click *Configuration > EIA-485 Port/Modbus*.
     EIA-485 Port/Modbus Configuration on page 34 opens for the slaved device.
   - In Modbus/TCP/UDP Slave Unit Identifier, enter the slave ID of the device. Start with the first available ID and assign the next consecutive number to each unit in the chain.
   - Click *Submit Changes*.

NOTE: The slaved devices are "physical" zones. If you have virtual zones configured, the IDs start after the virtual zones.

NOTE: The slave ID must be identical to the zone number.

5. Repeat Step Configure the slave devices: on page 38 for each slaved device.

6. Configure the physical zones:

NOTE: If you have virtual zones configured, the serial addresses for the devices start after the virtual zones.

NOTE: The zone number and the slave ID of the device must be identical.

- Open the web UI for the master controller, and click *Configuration > Physical Zone Settings*.
  Physical Zone Settings on page 26 opens.
- In Enable Comm Type, select *Modbus TCP* or *Modbus UDP* depending on the device.
- In IP Address, enter the IP address for the device.
- Click *Submit Changes*

We recommend generating an alarm from each unit to confirm proper communication.

4.3.18 BACnet Configuration

Use the BACnet page to configure control and monitoring of the Liqui-tect system by a building-management system (BMS).

This page also sets up alarm notifications via BACnet. See BACnet Alarm Notifications on page 40 for a description of the options and set up.

The page also lists the BACnet objects and accesses the packet log. See Viewing the BACnet Packet Log on page 41.

Table 6.18 BACnet Configuration fields and options

FIELD	DESCRIPTION
BACnet Device Name	Unique name for the LP3000 controller. 30-character limit.
BACnet Device ID	Device ID number for the LP3000. 30-character limit. 0 (zero) = disabled.
BACnet Device Description	Description of the LP3000 device. 30-character limit.
BACnet UDP Port	Specifies UDP port used by the application. Enter 0 (zero) to specify port 47808 (0xBAC0) as the UPD port. If your application specifies a different port, enter that value here. Default: 0
BACnet MS/TP Max Master	Sets the slave address. Valid values: 1 to 127. 0 (zero) = slave-only. Default: 0
Register as Foreign Device at IP	IP address of master device with which to communicate. Requires a BBMD for foreign-device discovery.
Registration Time-to-Live	Time, in seconds, for foreign-device discovery.
Foreign Device Table #1	Display-only, content read from Register Foreign Device at IP and Registration Time-to-Live fields.
Foreign Device Table #2	Display-only, content read from Register Foreign Device at IP and Registration Time-to-Live fields.
BACnet BBMD-BDT	Used by some BACnet masters for discovery on different subnets.
LP3000 IP Address	Display-only, IP address configured via Network/IP link.
(Primary) #1 IP Address	IP address of primary device connected via BACnet communication.
#2 to #4 IP Address	IP addresses of devices connected via BACnet communication.

BACnet Alarm Notifications

This section of BACnet Configuration sets-up alarm-event notifications via BACnet communication.

To set-up and test notifications:

1. Enter the settings, and click *Submit Changes*.

NOTE: If you do not submit changes before sending the test e-mail, the updates will be lost.

2. At the bottom of the page, click *Send Test Alarms*.
   The test notifications are sent.
3. Verify that the test notifications are correctly sent and received.
   - To clear the test notifications once verified, click *Clear Test Alarms*.

Table 6.19 BACnet Alarm-event Settings

FIELD	DESCRIPTION
Recipient #1 IP Address	Address to which alarm notifications are sent.
PID	Process identifier.
Notification type	Selects whether or not the alarm notification requires acknowledgment. • Unconfirmed = no acknowledgment needed. • Confirmed = acknowledgment required. Default: Unconfirmed.
Notification Class	List of devices to receive notification.
Priority	Designates a priority in the event of conflicting control situations.
Leak Detected Alarms	Selects the format of the leak-detection alarm notification.
APDU_Timeout	Time between re-transmission, in milliseconds, of an un-acknowledged APDU (when acknowledgment is required).
Number_of_APDU_Retries	Maximum number of re-transmission attemps.

Viewing the BACnet Packet Log

1. Click *Configuration* > *Bacnet*.
   BACnet Configuration on page 39 opens.
2. At the bottom of the page, click *Bacnet Packet Log*.
   The log opens in the web browser.

4.3.19 Alarm Management

The Alarm Management page resets active alarms and manages alarm history with the following options:

- Resetting a Leak-detection Alarm on page 41
- Clearing the Alarm History on page 41
- Acknowledging Un-sent E-mail on page 42
- Acknowledging SNMP Informs on page 42
- Logging an Alarm for Power Cycle on page 42

Resetting a Leak-detection Alarm

1. Click *Configuration* > *Alarm Management*.
   Alarm Management on page 41 opens.
2. Click *Reset Leak Alarm*.
   The alarm is reset and audible notification silenced (if sounding).

Clearing the Alarm History

1. Click *Configuration* > *Alarm Management*.
   Alarm Management on page 41 opens.
2. Click *Clear Alarm History*.
   The history clears.

Acknowledging Un-sent E-mail

1. Click *Configuration > Alarm Management*.
   Alarm Management on page 41 opens.
2. Click *Acknowledge Unsent Emails*.
   The e-mails are acknowledged.

Acknowledging SNMP Informs

1. Click *Configuration > Alarm Management*.
   Alarm Management on page 41 opens.
2. Click *Acknowledge Snmp Informs*.
   The informs are acknowledged.

Logging an Alarm for Power Cycle

When enabled, an alarm event occurs each time LP3000 powers-on, which logs each time the LP3000 power-cycles in the alarm history for later review.

1. Click *Configuration > Alarm Management*.
   Alarm Management on page 41 opens.
2. Click to check Enable Power Up Alarm Logging, then click *Submit*.
   An alarm event is logged each time the system powers-on.

4.3.20 System/Flash Management

The System Management page offers firmware-managment functions, image upload, and configuration backup.

- Backing Up Configuration Settings on page 43
- Restoring Factory Default Settings on page 43
- Updating Firmware on page 44
- Uploading Images on page 44
- Deleting an Image on page 44

Backing Up Configuration Settings

Once you have adjusted the configuration of the LP3000, save a back-up configuration file to a safe place. The configuration file can be used to restore the system and to copy to other LP3000 units.

All parameters, including x-y coordinates for the interactive reference map are saved. Only the map image file is not saved in the configuration file. See Saving a Map Image on page 30 to back up the map image.

To back up configuration settings:

1. Select *Configuration > System/Flash Management*.
   System/Flash Management on page 42 opens.
2. Click *Download Configuration File (.cfg)*.
   The file is downloaded.
3. Save the downloaded file to a computer or USB drive.
   - If necessary, update the file name with a descriptive name for your configuration.
   - Do not change the file extension, .cfg. If the extension is changed, the file is not recognized when you attempt to upload.

Restoring Factory Default Settings

Use the Bootloader to restore the factory-default configuration.

1. Save a back-up copy of the current settings in case you must re-load them. See Backing Up Configuration Settings on page 43.
2. Select *Configuration > System/Flash Management*.
   System/Flash Management on page 42 opens.
3. Click *Exit to Bootloader*.
   The Bootloader opens in the web browser.
4. Click *Restore Factory Defaults*.
   The settings are restored to defaults.
5. Click *Start Application* to restart and return to the web interface.

Restoring Back-up Configuration Settings

1. Select *Configuration > System/Flash Management*.
   System/Flash Management on page 42 opens.
2. Click *Choose File* and browse to select the configuration (.cfg), then click *Upload*.
   The configuration uploaded, and the web interface opens when the update is complete.

Updating Firmware

LP3000 firmware updates are available from technical support: Telephone: 800-222-5877 option 2, Outside the US: 614-841-6755 E-mail: Liebert.monitoring@vertivco.com

1. Obtain the updated firmware (.bin file), and save it to local disk.

NOTE: Do not change the file name. If the file name is changed, it will not be recognized by LP3000 and the update will fail.

2. Select *Configuration > System/Flash Management*.
   System/Flash Management on page 42 opens.
3. Click *Choose File* and browse to select the firmware (.bin), then click *Upload*.
   The configuration uploaded. The currently-loaded firmware version is displayed in the Flash Application field on the Identity Page on page 22.

Uploading Images

You can upload up to 2 images.

NOTE: To load an interactive facility map, see Uploading a Reference Map on page 29.

The file requirements for an uploaded image are:

- File size: 500 kb or less
- Image dimension/size: 4000 x 4000 pixels or less
- File format: .png, .jpg or .gif

To upload:

1. Select *Configuration > System/Flash Management*.
   System/Flash Management on page 42 opens.
2. Select the *Image Index* of the image file to upload (**1** for image 1 or **2** for image 2).

NOTE: Uploading a file to an index that already contains a file overwrites the file.

3. Click *Choose File* and browse to select the image file , then click *Upload*.
   The map is uploaded.
4. Select *Configuration > Web/Map Settings* (see Web/Map Settings on page 27), enter a title for the image in the appropriate Floor Map # Link Text field, and click *Submit Changes*.

Deleting an Image

1. Select *Configuration > System/Flash Management*.
   System/Flash Management on page 42 opens.
2. Click *Delete Image N*, where "N" is the number of the image file to delete.
   The file is deleted.

4.4 Historical Data

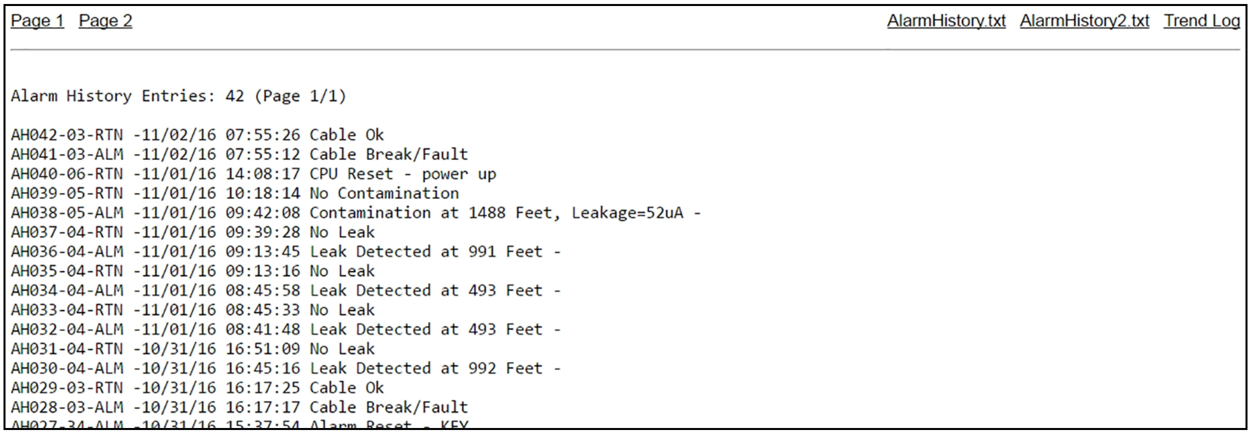
Historical data is a time-stamped list of events in the alarm-history log and current-leakage trend log.

The time-stamp format for each event, AHxxxyy MM/DD/YY HH:MM:SS, is described in the following table.

Table 6.20 History time-stamp format

ITEM	DESCRIPTION
AH	Alarm History
xxxx	Log-entry number for the event.
yy	Event code indicating type of event: 03 – Cable Fault 04 – Leak Detected 05 – Contamination Detected 06 – Reset/Power Up
MM/DD/YY	number of month/day of month/year
HH:MM:SS	Hour/Minute/Second (24-hour format)
text	Details about the event.

Figure 6.4 Historical Data page



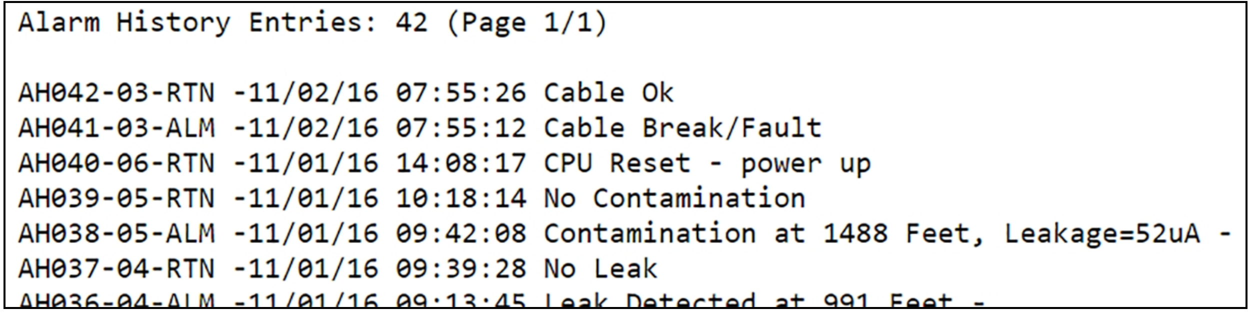
```
Alarm History Entries: 42 (Page 1/1)

AH042-03-RTN -11/02/16 07:55:26 Cable Ok
AH041-03-ALM -11/02/16 07:55:12 Cable Break/Fault
AH040-06-RTN -11/01/16 14:08:17 CPU Reset - power up
AH039-05-RTN -11/01/16 10:18:14 No Contamination
AH038-05-ALM -11/01/16 09:42:08 Contamination at 1488 Feet, Leakage=52uA -
AH037-04-RTN -11/01/16 09:39:28 No Leak
AH036-04-ALM -11/01/16 09:13:45 Leak Detected at 991 Feet -
AH035-04-RTN -11/01/16 09:13:16 No Leak
AH034-04-ALM -11/01/16 08:45:58 Leak Detected at 493 Feet -
AH033-04-RTN -11/01/16 08:45:33 No Leak
AH032-04-ALM -11/01/16 08:41:48 Leak Detected at 493 Feet -
AH031-04-RTN -10/31/16 16:51:09 No Leak
AH030-04-ALM -10/31/16 16:45:16 Leak Detected at 992 Feet -
AH029-03-RTN -10/31/16 16:17:25 Cable Ok
AH028-03-ALM -10/31/16 16:17:17 Cable Break/Fault
AH027-34-ALM -10/31/16 15:37:54 Alarm Reset - KEY
```

4.4.1 History Text Files for Download

1. On the Historical Data on page 45 page, click *AlarmHistory.txt* or *AlarmHistory2.text*.
   The .txt file opens in a web browser.
2. Download the file.

Figure 6.5 Alarm-history text file example

Figure 6.6



```
Alarm History Entries: 42 (Page 1/1)

AH042-03-RTN -11/02/16 07:55:26 Cable Ok
AH041-03-ALM -11/02/16 07:55:12 Cable Break/Fault
AH040-06-RTN -11/01/16 14:08:17 CPU Reset - power up
AH039-05-RTN -11/01/16 10:18:14 No Contamination
AH038-05-ALM -11/01/16 09:42:08 Contamination at 1488 Feet, Leakage=52uA -
AH037-04-RTN -11/01/16 09:39:28 No Leak
AH036-04-ALM -11/01/16 09:13:45 Leak Detected at 991 Feet -
```

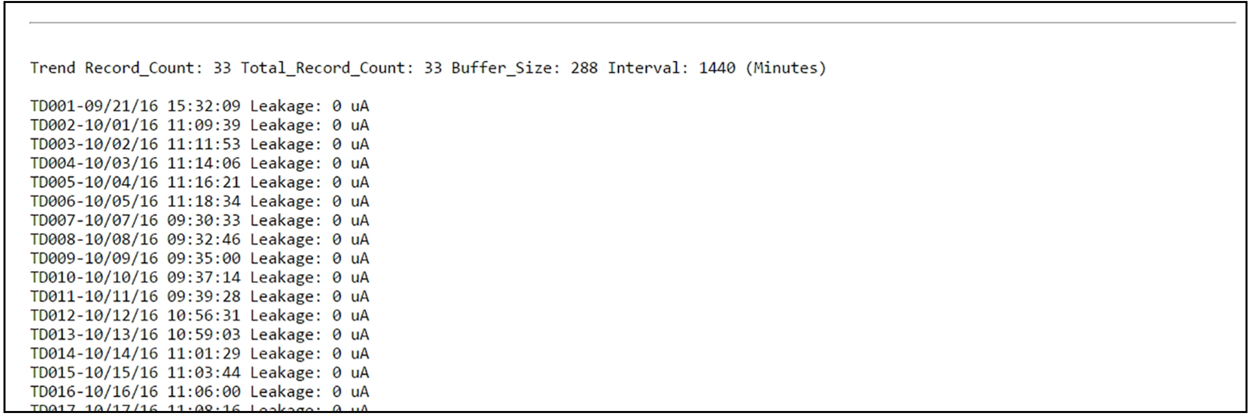
4.4.2 Viewing the Current-leakage Trends

The trend of current leakage assists in troubleshooting leaks and inaccurate readings.

- On the Historical Data on page 45 page, click *Trend Log*.
  The trend log opens.

Figure 6.7 Trend log of current leakage

Figure 6.8



```
Trend Record_Count: 33 Total_Record_Count: 33 Buffer_Size: 288 Interval: 1440 (Minutes)

TD001-09/21/16 15:32:09 Leakage: 0 uA
TD002-10/01/16 11:09:39 Leakage: 0 uA
TD003-10/02/16 11:11:53 Leakage: 0 uA
TD004-10/03/16 11:14:06 Leakage: 0 uA
TD005-10/04/16 11:16:21 Leakage: 0 uA
TD006-10/05/16 11:18:34 Leakage: 0 uA
TD007-10/07/16 09:30:33 Leakage: 0 uA
TD008-10/08/16 09:32:46 Leakage: 0 uA
TD009-10/09/16 09:35:00 Leakage: 0 uA
TD010-10/10/16 09:37:14 Leakage: 0 uA
TD011-10/11/16 09:39:28 Leakage: 0 uA
TD012-10/12/16 10:56:31 Leakage: 0 uA
TD013-10/13/16 10:59:03 Leakage: 0 uA
TD014-10/14/16 11:01:29 Leakage: 0 uA
TD015-10/15/16 11:03:44 Leakage: 0 uA
TD016-10/16/16 11:06:00 Leakage: 0 uA
TD017-10/17/16 11:08:16 Leakage: 0 uA
```

5 MODBUS COMMUNICATION PROTOCOL

This section describes the Modbus protocol supported by LP3000 for use when configuring communication via Modbus network.

LP3000 communicates via the half-duplex EIA-485 serial-communication standard. Liqui-tect LP3000 is a slave device and will not initiate a communication sequence.

5.1 Transmission Modes

LP3000 supports only RTU mode of transmission (does not support ASCII) with 8 data bits, no parity, and 1 stop bit.

Each packet consists of the following four fields:

- Slave Address Field: 1-byte length. Identifies the slave device in the transaction. Set on EIA-485 Port/Modbus Configuration on page 34.
- Function Field: 1-byte length. Indicates the function to perform. Supported functions are 03 (Read 4xxxx output registers), 04 (Read 3xxxx input registers), 06 (Preset single register) and 16 (Preset multiple registers).
- Data Field: variable length. 16-bit registers, transmitted high-order-byte first (big-endian).
- Error Check (Checksum) Field: Identifies transmission errors. Uses a 16-bit cyclic redundancy check (CRC-16).

5.1.1 Exception Responses

Exception responses are generated as a result of invalid commands from the Modbus master or an attempt to read and invalid register. The high-order bit of the function code is set to 1. The data field contains the exception error code, described in the following table.

Table 7.1 Exception Codes

CODE	NAME	DESCRIPTION
01	Illegal Function	Function code is not supported.
02	Illegal Data Address	Attempt to access an invalid address.
03	Illegal Data Value	Attempt to set a variable to an invalid value.

5.2 Modbus Packet Communication

A description of the packet registers.

5.2.1 Function 03: Read Output Registers

To read the parameter values, the master must send a Read Output Registers request packet.

The Read Output Registers request packet specifies a start register and the number of registers to read. The start register is numbered from zero (40001 = zero, 40002 = one, etc).

Table 7.2 Read-output Register Packet Structure

READ REGISTER REQUEST PACKET	READ REGISTERS RESPONSE PACKET
Slave Address (1 byte)	Slave Address (1 byte)
03 (Function code) (1 byte)	03 (Function code) (1 byte)
Start Register (2 bytes)	Byte count (1 byte)
# of registers to read (2 bytes)	First register (2 bytes)
CRC Checksum (2 bytes)	Second register (2 bytes)
	...
	Cry Checksum (2 bytes)

Table 7.3 Output Registers

REGISTER	NAME	DESCRIPTION	UNITS	RANGE
40001	Leak Threshold	Trip current for leak alarm	25-295 uAmps	0-65535
40002	Contamination Threshold	Trip current for contamination alarm	20-295 uAmps	0-65535
40003	Re-Alarm Delay	The time that elapses between when an alarm is detected and when it is annunciated	0-24 Hours	0-65535
40004	Latching Alarms	Designate the alarms as latching or non-latching	0=No, 1=Yes	0-65535
40005	Silence Audible Alarm	Silence the audible alarm	1=Silenced	0-65535
40006	Reset Alarms	Reset all the alarms	1=Reset	0-65535
40007	Spare			0-65535
40008	Spare			0-65535
40009	Spare			0-65535
40010	Spare			0-65535
40011	Spare			0-65535
40012	Spare			0-65535
40013	Spare			0-65535
40014	Spare			0-65535
40015	Spare			0-65535
40016	Leak Alarm Delay	Leak Alarm Delay	5-995 seconds	0-65535
40017	Contamination Alarm Delay	Contamination Alarm Delay	5-995 seconds	0-65535

5.2.2 Function 04: Read Input Registers

To read the input values, the master must send a Read Input Registers request packet.

The Read Input Registers request packet specifies a start register and the number of registers to read. The start register is numbered from zero (30001 = zero, 30002 = one, etc).

Table 7.4 Read-output Register Packet Structure

READ REGISTER REQUEST PACKET	READ REGISTERS RESPONSE PACKET
Slave Address (1 byte)	Slave Address (1 byte)
04 (Function code) (1 byte)	04 (Function code) (1 byte)
Start Register (2 bytes)	Byte count (1 byte)
# of registers to read (2 bytes)	First register (2 bytes)
CRC Checksum (2 bytes)	Second register (2 bytes)
	...
	Cry Checksum (2 bytes)

In the following table, Registers 30011 through 30041 are dedicated registers for Modbus Master. (See Configuring the Controller as a Modbus Master on page 35.)

Table 7.5 Input Registers

REGISTER	NAME	DESCRIPTION	UNITS	RANGE
30001	Status	Bit level status	None	0-65535
30002	Leak Distance	Location of leak	Ft/Meters	0-65535
30003	Units	Unit of measure	1=Ft 0=Meters	0-65535
30004	Leak Current	Leakage current on cable	uAmps	0-65535
30005	Cable Length	Installed cable length	Ft/Meters	0-65535
30006	Loop1 Res	Resistance of cable	Ohms	0-65535
30007	Loop2 Res	Resistance of cable	Ohms	0-65535
30008	Res/Ft	Resistance of cable	Ohms x 1000	0-65535
30009	Version	Firmware version	xx.xx X 100	0-65535
30010	Virtual Zone Alarm Status	Bit Level Status	None	0-65535
30011	Modbus Zone Enabled Flags	Bit Level Status	None	0-65535
30012	Modbus Zone2 Status	Bit Level Status	None	0-65535
30013	Modbus Zone2 Distance	Location of leak	Ft/Meters	0-65535
30014	Modbus Zone3 Status	Bit Level Status	None	0-65535
30015	Modbus Zone3 Distance	Location of leak	Ft/Meters	0-65535
30016	Modbus Zone4 Status	Bit Level Status	None	0-65535
30017	Modbus Zone4 Distance	Location of leak	Ft/Meters	0-65535
30018	Modbus Zone5 Status	Bit Level Status	None	0-65535
30019	Modbus Zone5 Distance	Location of leak	Ft/Meters	0-65535
30020	Modbus Zone6 Status	Bit Level Status	None	0-65535
30021	Modbus Zone6 Distance	Location of leak	Ft/Meters	0-65535
30022	Modbus Zone7 Status	Bit Level Status	None	0-65535
30023	Modbus Zone7 Distance	Location of leak	Ft/Meters	0-65535
30024	Modbus Zone8 Status	Bit Level Status	None	0-65535
30025	Modbus Zone8 Distance	Location of leak	Ft/Meters	0-65535
30026	Modbus Zone9 Status	Bit Level Status	None	0-65535
30027	Modbus Zone9 Distance	Location of leak	Ft/Meters	0-65535
30028	Modbus Zone10 Status	Bit Level Status	None	0-65535
30029	Modbus Zone10 Distance	Location of leak	Ft/Meters	0-65535
30030	Modbus Zone11 Status	Bit Level Status	None	0-65535
30031	Modbus Zone11 Distance	Location of leak	Ft/Meters	0-65535
30032	Modbus Zone12 Status	Bit Level Status	None	0-65535
30033	Modbus Zone12 Distance	Location of leak	Ft/Meters	0-65535
30034	Modbus Zone13 Status	Bit Level Status	None	0-65535

REGISTER	NAME	DESCRIPTION	UNITS	RANGE
30035	Modbus Zone13 Distance	Location of leak	Ft/Meters	0-65535
30036	Modbus Zone14 Status	Bit Level Status	None	0-65535
30037	Modbus Zone14 Distance	Location of leak	Ft/Meters	0-65535
30038	Modbus Zone15 Status	Bit Level Status	None	0-65535
30039	Modbus Zone15 Distance	Location of leak	Ft/Meters	0-65535
30040	Modbus Zone16 Status	Bit Level Status	None	0-65535
30041	Modbus Zone16 Distance	Location of leak	Ft/Meters	0-65535
30042	Modbus Zone Enabled Flags	Bit Level Status	None	0-65535
30043	Modbus Zone17 Status	Bit Level Status	None	0-65535
30044	Modbus Zone17 Distance	Location of leak	Ft/Meters	0-65535
30045	Modbus Zone18 Status	Bit Level Status	None	0-65535
30046	Modbus Zone18 Distance	Location of leak	Ft/Meters	0-65535
30047	Modbus Zone19 Status	Bit Level Status	None	0-65535
30048	Modbus Zone19 Distance	Location of leak	Ft/Meters	0-65535
30049	Modbus Zone20 Status	Bit Level Status	None	0-65535
30050	Modbus Zone20 Distance	Location of leak	Ft/Meters	0-65535
30051	Modbus Zone21 Status	Bit Level Status	None	0-65535
30052	Modbus Zone21 Distance	Location of leak	Ft/Meters	0-65535
30053	Modbus Zone22 Status	Bit Level Status	None	0-65535
30054	Modbus Zone22 Distance	Location of leak	Ft/Meters	0-65535
30055	Modbus Zone23 Status	Bit Level Status	None	0-65535
30056	Modbus Zone23 Distance	Location of leak	Ft/Meters	0-65535
30057	Modbus Zone24 Status	Bit Level Status	None	0-65535
30058	Modbus Zone24 Distance	Location of leak	Ft/Meters	0-65535
30059	Modbus Zone25 Status	Bit Level Status	None	0-65535
30060	Modbus Zone25 Distance	Location of leak	Ft/Meters	0-65535
30061	Modbus Zone26 Status	Bit Level Status	None	0-65535
30062	Modbus Zone26 Distance	Location of leak	Ft/Meters	0-65535
30063	Modbus Zone2 7 Status	Bit Level Status	None	0-65535
30064	Modbus Zone27 Distance	Location of leak	Ft/Meters	0-65535
30065	Modbus Zone28 Status	Bit Level Status	None	0-65535
30066	Modbus Zone28 Distance	Location of leak	Ft/Meters	0-65535
30067	Modbus Zone29 Status	Bit Level Status	None	0-65535

REGISTER	NAME	DESCRIPTION	UNITS	RANGE
30068	Modbus Zone29 Distance	Location of leak	Ft/Meters	0-65535
30069	Modbus Zone30 Status	Bit Level Status	None	0-65535
30070	Modbus Zone30 Distance	Location of leak	Ft/Meters	0-65535
30071	Modbus Zone31 Status	Bit Level Status	None	0-65535
30072	Modbus Zone31 Distance	Location of leak	Ft/Meters	0-65535
30073	Modbus Zone32 Status	Bit Level Status	None	0-65535
30074	Modbus Zone32 Distance	Location of leak	Ft/Meters	0-65535
30075	Virtual Zone Alarm Status	Bit Level Status	None	0-65535

Table 7.6 Status Flags (Register 30001)

BIT	DESCRIPTION
00	1 = Leak Detected
01	1 = Cable Break Alarm
02	1 = Contamination Detected
04 - 15	Spare

Table 7.7 Status Flags (Register 30010)

BIT	DESCRIPTION
00	1 = Zone1
01	1 = Zone2
02	1 = Zone3
03	1 = Zone4
04	1 = Zone5
05	1 = Zone6
06	1 = Zone7
07	1 = Zone8
08	1 = Zone9
09	1 = Zone10
10	1 = Zone11
11	1 = Zone12
12	1 = Zone13
13	1 = Zone14
14	1 = Zone15
15	1 = Zone16

Table 7.8 Status Flags (Register 30011)

BIT	DESCRIPTION
00	1 = Not enable
01	1 = Enabled, b1 = MBZ2
02	1 = MBZ3
03	1 = MBZ4
04	1 = MBZ5
05	1 = MBZ6
06	1 = MBZ7
07	1 = MBZ8
08	1 = MBZ9
09	1 = MBZ10
10	1 = MBZ11
11	1 = MBZ12
12	1 = MBZ13
13	1 = MBZ14
14	1 = MBZ15
15	1 = MBZ16

Table 7.9 Status Flags (Even Registers 30012 - 30040)

BIT	DESCRIPTION
00	1 = Leak Alarm
01	1 = Cable Break
02	1 = Contamination Alarm
03	1 = Communication Loss

Table 7.10 Status Flags (Register 30042)

BIT	DESCRIPTION
00	1 = MBZ17
01	1 = MBZ18
02	1 = MBZ19
03	1 = MBZ20
04	1 = MBZ21
05	1 = MBZ22
06	1 = MBZ23
07	1 = MBZ24
08	1 = MBZ25
09	1 = MBZ26
10	1 = MBZ27
11	1 = MBZ28
12	1 = MBZ29
13	1 = MBZ30
14	1 = MBZ31
15	1 = MBZ32

Table 7.11 Status Flags (Register 30075)

BIT	DESCRIPTION
00	1 = Zone17
01	1 = Zone18
02	1 = Zone19
03	1 = Zone20
04	1 = Zone21
05	1 = Zone22
06	1 = Zone23
07	1 = Zone24
08	1 = Zone25
09	1 = Zone26
10	1 = Zone27
11	1 = Zone28
12	1 = Zone29
13	1 = Zone30
14	1 = Zone31
15	1 = Zone32

5.3 Function 06: Preset Single Register

To set a parameter value, the master must send a Preset Single Register request packet. The Preset Single Register request packet specifies a register and the data to write to that register. The register is numbered from zero (40001 = zero, 40002 = one, etc).

Table 7.12 Preset Single Register Packet Structure

READ REGISTER REQUEST PACKET	READ REGISTERS RESPONSE PACKET
Slave Address (1 byte)	Slave Address (1 byte)
06 (Function code) (1 byte)	06 (Function code) (1 byte)
Register (2 bytes)	Register (2 bytes)
Data (2 bytes)	Data (2 bytes)
Cry Checksum (2 bytes)	Cry Checksum (2 bytes)

5.3.1 Function 16: Preset Multiple Registers

To set multiple parameter values, the master must send a Preset Multiple Registers request packet. The Preset Multiple Register request packet specifies a starting register, the number of registers, a byte count and the data to write to the registers. The register is numbered from zero (40001 = zero, 40002 = one, etc).

Table 7.13 Preset Multiple Registers Packet Structure

READ REGISTER REQUEST PACKET	READ REGISTERS RESPONSE PACKET
Slave Address (1 byte)	Slave Address (1 byte)
16 (Function code) (1 byte)	16 (Function code) (1 byte)
Start Register (2 bytes)	Start Register (2 bytes)
# of registers to write (2 bytes)	# of registers (2 bytes)
Byte count (1 byte)	CRC Checksum (2 bytes)
Data (2 bytes)	
...	
...	
Cry Checksum (2 bytes)	

5.4 RTU Framing

The following is a typical Query/Response from Liqui-tect.

Table 7.14 Response Sample

SLAVE ADDRESS	FUNCTION CODE	COUNT BYTES OF DATA	REGISTER DATA		REGISTER DATA		REGISTER DATA		CRC16 "LSB"	CRC 126 "MSB
			MSB	LSB	MSB	LSB	MSB	LSB		
02	04	06	00	00	00	00	00	01	B5	A3

Slave address 2 responds to Function Code 4 with six bytes of hexadecimal data and ends with CRC16 checksum.

Register Values:

40001 = 0000 (hex)

40002 = 0000 (hex)

40003 = 0001 (hex)

This page intentionally left blank.

6 PREVENTIVE MAINTENANCE

Monthly, perform the following system test to verify proper function of the Liqui-tect control panel.

1. Place a clean, damp cloth or paper towel on the cable, and verify that the leak is detected on the control panel.
2. Using a reference map (if available), verify that the correct leak location displays.
3. See Calibrating Resistance to Cable Length on page 16 if necessary.
4. Dry the cable and verify that operation returns to normal.
5. Remove the end terminator from the end of the cable run, and verify that a cable-break alarm displays on the control panel.
6. Reinstall the end terminator, and verify that operation returns to normal.
7. Monitor the cable current monthly to verify that the cable is not contaminated. The cable-contamination alarm displays if contamination is excessive.
8. Log-in to the web UI, and verify that the Cable Current is less than 24 µA.
   - If current is greater than 24 µA, troubleshoot the cables to determine which is contaminated. Remove the contaminated cable, clean and test it before re-installing.

This page intentionally left blank.

7 TROUBLESHOOTING

The following table lists problems that you may encounter with the Liqui-tect system, and action to take to resolve them. For all other troubleshooting questions or concerns, contact us at one of the following:

Telephone: 800-222-5877 option 2, Outside the US: 614-841-6755

E-mail: Liebert.monitoring@vertivco.com

Table 9.1 Troubleshooting the System

PROBLEM	ACTION
Control panel does not power-on	Using a DVOM (multi-meter), check for AC and DC input power on the lower, left-hand terminal block on the controller. If no voltage is present, check the circuit breaker or power supply that powers the controller. • If voltage is present at the circuit breaker/power supply, contact technical support for unit evaluation/replacement.
Cable-break alarm	• Verify that the leader from the leak-detection cable is plugged into the terminal block marked "Cable." • Verify that the end terminator is installed at the end of the leak-detection cable run. • If the end terminator is present, remove it from the end of the run and install it on the end of the leader cable from the control panel. • If the alarm clears, there is a damaged/faulty section in the leak-detection cable. • To find the damaged/faulty section, move the end terminator to the end of each section of leak-detection cable. • If the alarm does not clear, power-off the control panel, and remove the terminal block marked "cable" from the controller. • Remove the 4 conductors from the leader-cable wire connected to the 4-position terminal block. • Install a jumper wire between pins 1 and 2, and another between pins 3 and 4. • Re-install the terminal block. • If the alarm condition clears, the leader cable is the problem. Contact technical support.
Incorrect length-of-cable reported	• Verify proper wiring to the terminal block marked "Cable." See Connecting Power to Liqui-tect on page 16 for correct wiring. • Calibrate the cable. See Calibrating Resistance to Cable Length on page 16. • If the problem persists, contact technical support.
Incorrect distance to leak reported	• Check the distance on the cable run to verify that the control panel is monitoring. • Verify that there is no water along the cable run. If water is found: • Check for multiple leaks along the cable. The first leak should be read and latched. However, if the system is updated or if two or more simultaneous leaks occur within 30 seconds of the initial leak, the system may display the average distance to the leak (distance to first + distance to second/2), • If no water is found, check the cable as follows: • Power-off the control panel and remove the end terminator from the end of the leak-detection cable. • Locate the first section of leak-detection cable, disconnect it from the second leak-detection cable, and install the end terminator to the end of the first section. • Power-on the controller and let it run for 5 to 10 minutes, then place a damp cloth on the leak-detection cable. • If the test leak is correctly detected, remove the end terminator, re-connect the sections and move to the end of the next section to repeat the test until the faulty section is found. • If the fault reading is on the first cable section, the miscalculations may be in the controller. Contact technical support.
Cable-contamination alarm	Remove and clean the leak-detection cable using a clean damp rag. • If contaminated by oil, glycol, or chemicals, make a solution of 1 cap full of mild detergent mixed in 2 gallons of lukewarm water (<105°F). In a suitable container, gently agitate the cable in the solution, then rinse the cable with clear, lukewarm water. Wipe the cable dry with a clean towel. • You may also clean the cable by wiping it with isopropyl alcohol. Test the cable before re-installing it.

The following table lists questions that you may encounter with the Liqui-tect leak-detection cable, and answers to the questions. For all other troubleshooting questions or concerns, contact us at one of the following:

Telephone: 800-222-5877 option 2, Outside the US: 614-841-6755

E-mail: Liebert.monitoring@vertivco.com

Table 9.2 Troubleshooting the Leak-detection Cable

QUESTION	ANSWER
The leak-detection cable touches metal surfaces. Is this a problem or a potential problem?	In general, touching metal is not a problem. The sensing wires are covered with a non-conductive polymer weave that isolates the cable from metal surfaces. However, as with all cabling and electrical wires, avoid sharp objects that could pierce the insulation and polymer weave.
The leak-detection cable is routed so that it crosses over itself. Can this cause false alarms?	Crossing the leak-detection cable will not cause false alarms, but it may cause false distance readings if a leak occurs where the cable crosses over. If the leak-detection cable must cross, use a jumper cable to "jump over" the sensing cable.
If I suspect a bad section of leak-detection cable, how can I verify that it is bad without returning it to the factory for evaluation?	Because it can be very difficult to remove installed leak-detection cabling, confirm that there is a problem using the "Incorrect distance to leak reported on page 62" solution in the system-troubleshooting table.
How do I secure the sensing cable to the floor?	We recommend securing the cable with factory-provided hold-down clips. See Laying the Leak-detection Cable and Securing to the Floor on page 12 for the correct method of securing the cable.
How do I clean the cable?	If only a small section of the cable needs cleaned, wipe the contaminated section with isopropyl alcohol. To clean the entire cable, refer to the solution steps for Cable-contamination alarm on page 62 in the system-troubleshooting table.
My system shows a leak detected, but there is no leak found at the reported location. The alarm condition will not clear.	The most common causes for a constant alarm condition are: 1. Water is touching the cable in two places at the same time. • Check for multiple leaks along the cable. The first leak should be read and latched. However, if the system is updated or if two or more simultaneous leaks occur within 30 seconds of the initial leak, the system may display the average distance to the leak (distance to first + distance to second/2). • Displaying an average distance occurs if the operator resets the system without recording the first leak-location displayed. Check the alarm history for the first incidence of a leak. 2. The cable is exposed to high humidity, or the dew point has been reached in the facility. This is common when two or more air conditioners share the same under-floor space. • Although more easily said than done (especially if the air conditioners are working properly), one option is to correct the "over cooling" that causes moisture or condensation on the leak-detection cable. • At the controller, adjust the system to its least-sensitive setting to prevent the system from alarming. This does not correct the "over cooling" problem. • Move the cable at least 10 ft from the air-conditioner discharge air flow. • Cover the leak-detection cable that is in from of the air-conditioner discharge air flow with spiral wrap, a plastic covering that allows water to reach the cable but prevents condensation on the cable. 3. The cable is chemically contaminated (floor-sealing chemicals dissolve and damage the cable) or physically contaminated (metallic chips from filings or solder from piping or wiring installation). The cable must be replaced. 4. The cable is damaged, most often from dropping a floor tile on it. The damaged cable must be repaired or replaced.

7.1 Configuration Worksheet

The following information is used to set up Liqui-tect LP3000 at your site. Please complete as many fields as possible. If necessary, contact your IT department for the proper information.

NOTE: Pass code and security information is not required at this time.

IP Information	
Liqui-tect Static IP Address	
Subnet Mask	
Gateway/Default Router	
TCP Max Segment Size (1436 or 536)	
System Information	
System Name (The system name appears at the beginning of each web-UI page and each e-mail)	
System Contact	
System Location	
Log-in Information	
Web User Name	
Web password Read-only	
Web password Read/Write	
Web Refresh Rate	
E-mail Configuration	
NOTE: Liqui-tect can send e-mail over LAN using your company e-mail server *or* by connecting to an ISP, but it *cannot do both*.	
E-mail over LAN:	
Primary DNS Server IP address	
Secondary DNS Server IP address	
General E-mail Settings:	
Mail (SMTP) Server Domain Name or IP address	
SP Port	
Mail Sender Address (from field in e-mail) Must be a valid e-mail address for the mail server.	
Mail Subject The text that appears in the subject field.	
Email Recipient #1	
Email Recipient #2	
Email Recipient #3	
Email Recipient #4	
SMTP Authentication Some e-mail servers require a log-in to relay e-mail	
SMTP User name	
SMTP password	
NTP Settings	
Daylight Savings Time	
DST Begin Date	
DST End Date	
SNMP/Syslog	
System Name	
System Contact	
System Location	
SNMP Trap Type	

V1/V2C Community Names	
Trap Communities	
Modbus/EIA-485	
Modbus TCP/IP:	
Modbus TCP Slave Identifier (1 - 254)	
Modbus RTU:	
Baud Rate	
Parity	
Slave Address	
BACnet	
BACnet Device Name	
BACnet Device ID	
BACnet Description	
BACnet UDP Port	
BACnet MS/TP Max Master	
Register as Foreign Device at IP	
Registration Time to Live	
BACnet BBMD-BDT Settings:	
IP Address	
Port	
Mask	
BACnet Alarms Event Notification:	
IP Address	
PIS	
Notification Type	
Notification Class and Priority	
Leak Detected Alarms	
APDU Timeout (seconds)	
Number of APDU retries	
Virtual Zones	
Number of Zones	
Length of Each Zone	
Label for Each Zone	

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