VERTIV™

Liebert® SiteScan™ Web v8.0

User Manual

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

This page intentionally left blank

1 Vertiv™ Liebert® SiteScan™ Web v8.0

1.1 Introduction

The Liebert® SiteScan™ building automation system offers an intuitive user interface and powerful tools to help facility managers keep occupants comfortable, manage energy conservation measures, identify key operational problems, and analyze the results. The web based Liebert® SiteScan™ system can be accessed from anywhere in the world through a web browser (Internet Explorer, Chrome, Firefox, etc.). Building management functions can be performed on a workstation or mobile device, such as:

- Adjust setpoints and other control parameters
- Set and change schedules
- Graphically trend important building conditions
- View and acknowledge alarms
- Run preconfigured and custom reports on energy usage, occupant overrides, and much more.

A Liebert® SiteScan™ system supports:

- Unlimited simultaneous users
- Multiple operating systems and databases
- Mobile devices
- Built in and custom alarms, trends, and reports
- Time lapse
- International languages (International English, Brazilian Portuguese, French, German, Italian, Japanese, Korean, Russian, Traditional and Simplified Chinese, Spanish, Swedish, Thai, Vietnamese)
- Third party integration
- Secure server access using TLS.

1.2 A Typical Liebert® SiteScan™ System

A Liebert® SiteScan™ system uses a network of microprocessor based controllers to control heating, air conditioning, lighting, and other facility systems. A web based server communicates with these controllers and generates the Liebert® SiteScan™ interface that the user can access through a web browser. Through the interface, you can gather information, change operating properties, run reports, and perform other building management functions on a single building, an entire campus, or a network of facilities that stretch around the globe.

The Liebert® SiteScan™ client uses a web browser to access the Liebert® SiteScan™ Server application as a website.

1.3 Liebert® SiteScan™ Tools

A Liebert® SiteScan™ system includes the following tools.

Table 1.1 Design Tools

Tool	Description
EIKON	Create control programs and Properties pages.
SiteBuilder	Create and modify the system database and associate control programs and graphics with equipment.
EquipmentBuilder	Generate the following files from a library of predefined applications. • Control program (.equipment) • Graphic (.view) • BACview file (.bacview), if applicable to the equipment • Sequence of operation (.odt) • Visio schematic (.vdx)
Permissions Key Builder	Create a key that will permit recipients to override restricted access to .equipment files and .view files.

2 New Features in Vertiv™ Liebert® SiteScan™ v8.0

2.1 New Features

Table 2.1 Feature Improvements in Liebert® SiteScan™ v8.0

Feature	Improvement
Security enhancements	• Apache Tomcat web server has been upgraded to v9.0.x and TLS 1.3 • The Liebert® SiteScan™ application has been upgraded to OpenJDK Java 11 LTS.
BACnet Rev. 19	The Display microblocks that are used to model the options of a third-party BACnet device include new fields on the Properties > Details page of microblock popup to implement BACnet Rev. 19.
BACnet/SC (See Signing a BACnet/SC Certificate Signing Request with Keystore Explorer on page 179)	Added support for BACnet/SC.
New manual command to view security settings	The new manual command **sreview** displays the security best practices compliance data for the application installation. This includes web server security settings, SSL certificate details, email security settings, password policy, and the latest software updates. See Manual Commands on page 128 for details.
Connections	This feature allows to select a network connection in a new table on the System Configuration ⚙ tree > Connections > Configure tab, without accessing the View tab.
Alarm Notification improvement	• When using location-dependent security, users only receive alarms for locations they are allowed to access. • You can use an IPv6 Server address in the Server field. Access to the IPv6 address can be restricted in the System Settings > General tab > Alarms of Liebert® SiteScan™ interface.
Semantic tagging (See Using Semantic Tags in a Path on page 139)	Semantics tags and rules are included in the Liebert® SiteScan™ v8.0 application to apply semantic meaning to locations in the system. You can use the tags that are included or create custom tags and custom rules. **NOTE: Tags can be used to define a path. See Using Semantic Tags in a Path on page 139).**
Legacy autopilot	The legacy autopilot feature has been removed from the Liebert® SiteScan™ application.

2.2 SiteBuilder Application - New Features

Table 2.2 Feature Improvements in Sitebuilder Application

Feature	Improvement
Improved security settings	Vertiv™ Liebert® SiteScan™ application defaults to the following settings to provide improvised security: • If your system is set to use TLS, the Liebert® SiteScan™ application automatically uses TLS 1.3. • The Liebert® SiteScan™ application requires SOAP applications to run over HTTPS. • The Liebert® SiteScan™ application allows only addons that have been approved by Vertiv. **NOTE: These defaults can be override in Sitebuilder if necessary, but this will compromise the security of the system.**

This page intentionally left blank

3 Using the Vertiv™ Liebert® SiteScan™ Application

3.1 Running Liebert® SiteScan™ Server

The Liebert® SiteScan™ Server application communicates with the controllers and accesses of the system and maintains the system database. You can view and edit the system in client web browsers. SiteScan Server must be running for the user to log in from a web browser.

The Current Users, Connections, and Output tabs of the application allows you to monitor the status of the system. Output information is continually archived to SiteScan_Web_x.x\logs\< date >\core.txt.

NOTE: The instructions below are for a system that has been designed and set up. The Liebert® SiteScan™ application can run without communicating with the controllers of the system while the user is designing a system. See Options for Running the Liebert® SiteScan™ System on page 210 .

3.1.1 Starting the Liebert® SiteScan™ System

1. Click *Start* > *All Programs* > *SiteScan_Web_ x.x* > *SiteScan Server*.

NOTE: The computer starts the application every time it boots up, if the user runs the Sitescan application as a Windows service. See Running SiteScan Server as a Windows Service on page 210 .

2. Open a *web browser* on one or more client computers.
3. Verify that your web browser is set up to display the Liebert® SiteScan™ interface. See Setting Up Vertiv™ Liebert® SiteScan™ Client Devices and Web Browsers on page 194 .
4. Type the address of Liebert® SiteScan™ server in the address bar of web browser.

NOTE: Type http://localhost if SiteScan Server and the web browser are running on the same computer.

5. Enter a *Name* and *Password*.

3.1.2 Sending a Message to Logged In Users

Messages are delivered immediately to Liebert® SiteScan™ client web browsers. To send multiple messages the user must click *OK* for the first message before moving on to the next message. If the web browser window is minimized, the message is not visible.

1. On the Current Users tab of the Sitescan server application, click 🔈 alongside the user to whom you want to send the message. Alternatively, click *Notify All Users*.
2. Type a *message*.
3. Click *OK*.

3.1.3 Logging Off the User

From the Liebert® SiteScan™ Server Application

NOTE: The user will be logged off without any warning.

1. On the Current Users tab of the Liebert® SiteScan™ server, right click the user, then select *Log Off User*.
2. Click *Yes*.

From the Vertiv™ Liebert® SiteScan™ Interface

NOTE: The user will be logged off without any warning.

1. On the Liebert® SiteScan™ interface, press *Ctrl+M*.
2. Type *whoson* in the manual command field.
3. Obtain the ID number of the user you want to log off.
4. Press *Ctrl+M.*
5. Type *logoffuser x* (where x will be the ID number).
6. Click *OK*.

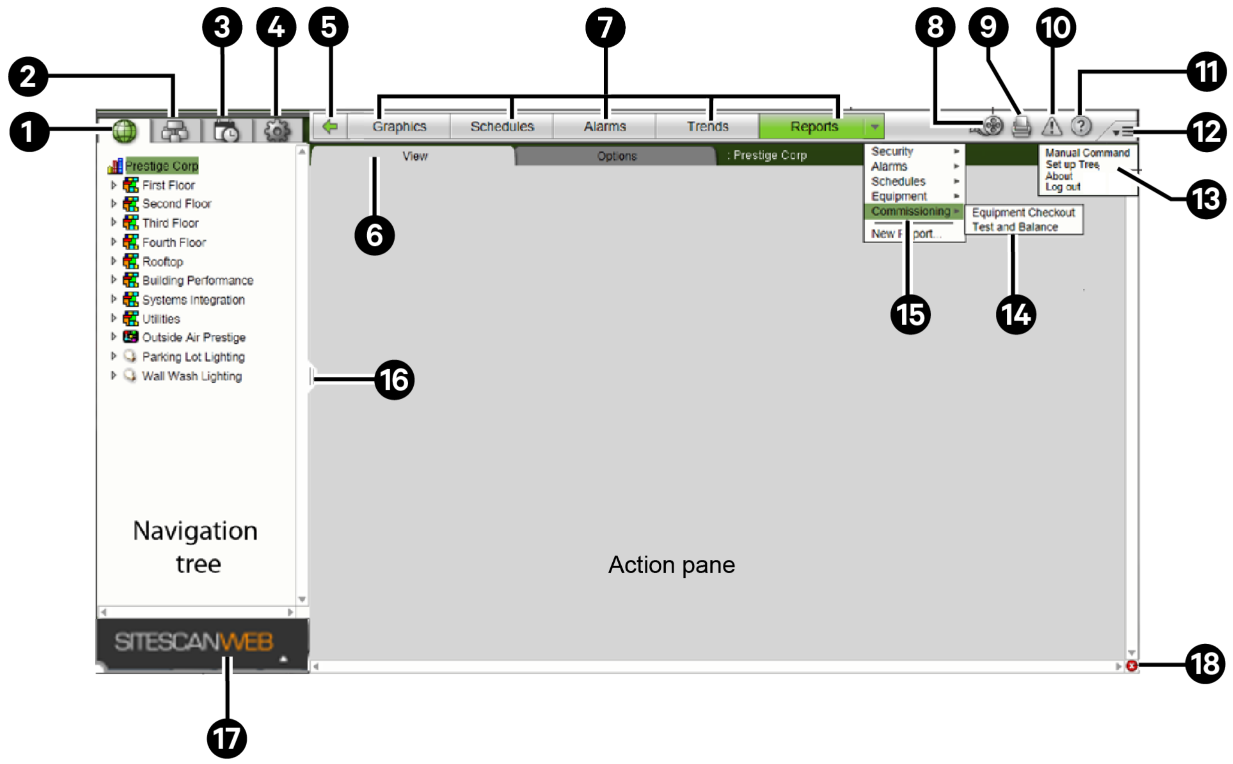
3.1.4 Shutting Down a System

1. In the Liebert® SiteScan™ Server application, select *Server > Shut Down.*
2. Optional: Select a *delay option*, then edit the *Notification message*.
3. Click *Shut Down.*

3.2 Getting to Know the Liebert® SiteScan™ Interface

3.2.1 Desktop and Large Screen Mobile Interface

Figure 3.1 Desktop and Large Screen Mobile Interface



Item	Description
1	Geographic Tree
2	Network Tree
3	Schedule Groups Tree
4	System Configuration Tree
5	Back Buttons
6	Tabs
7	Action Buttons
8	Time Lapse Button
9	Print Button
10	System wide Alarms Buttons
11	Help Button
12	Click to Display
13	Menu
14	Item
15	Category
16	Click and drag to adjust width of tree
17	Click to show/hide navigtion tree
18	Indicates error on page

3.2.2 Small Screen Mobile Interface

On small-screen mobile devices, the Vertiv™ Liebert® SiteScan™ interface looks the same.

- When you click SITESCANWEB to hide the tree, the button changes to
- Help and Print are in the menu.

NOTE: After logging in, you will see the page defined as your starting location on the My Settings page. To change your opening page, see Changing My Settings on page 122 .

Privileges control what the user can see or do in the Liebert® SiteScan™ system. If you cannot see or do something that you read about it in Help, ask your System Administrator to check your privileges.

3.2.3 Navigation Trees

The Liebert® SiteScan™ interface has 4 navigation trees.

1. Geographic Tree - Allows the user to navigate through the Liebert® SiteScan™ interface using the geographic layout of the system.
2. Network Tree - Allows the user to navigate through the Liebert® SiteScan™ interface using the network layout of the system.

3. **Schedule Groups Tree -** Allows the user to create groups that can consist of areas, equipment, or other groups and then assign a schedule to the entire group instead of the individual items. See To apply a schedule to a group of items (page 46).
4. **System Configuration Tree -** The majority of the items on this tree are used for system setup and maintenance.

Table 3.1 Navigation Options

Item	Description
My Settings	Allows the user to change settings that are user specific such as your password, viewing preferences and contact information. See Changing My Settings on page 122 .
System Settings	Contains the system wide settings that control the way the Vertiv™ Liebert® SiteScan™ system runs. See System Settings on page 199 .
Operators Privilege Sets Operator Groups	Allows the system administrator define operators and what they can see and do in the Liebert® SiteScan™ interface. See Operator Access on page 116 .
Categories	Lets you define categories for the following. See schedules, alarms (Alarms on page 30), graphics , properties, trends (Trends on page 22), and reports (Reports on page 68). Categories allow the user to view or control groups of similar items.
Scheduled Reports	Shows any report that was scheduled on the report's page. See Managing Scheduled Reports on page 106 for details.
Alarm Templates	See If you upgraded alarms from v2.0 or earlier (Alarms on page 30).
Connections	Allows the user to set up, start/stop, and troubleshoot the network connections. See Setting up Networks on page 143 .
Services	Shows internal processes of the Liebert® SiteScan™ application for troubleshooting.
License Administration	Allows the user to update your Liebert® SiteScan™ license. See Registering Your Liebert® SiteScan™ Software on page 206 .
Update	Click Update to select and apply patch, service packs, drivers, language packs, graphics libraries, and Help updates.
Hierarchical Servers	This page displays the servers to which your server is connected if your system has hierarchical servers.
Client Installs	Allows the user to install applications that are to run on client computers.

3.2.4 Navigating the System

NOTE: Use only the Liebert® SiteScan™ interface to navigate; do not use the web browser's navigation buttons.

Navigating to an Item in the System

1. Select an item on the Geographic or Network tree.

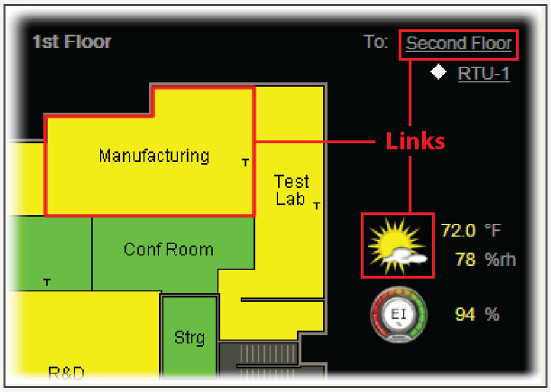
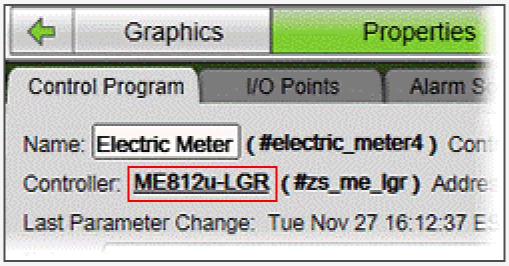
NOTE: The Schedule Groups and System Configuration trees are used to set up your system.

2. Use the action buttons and their drop down menus to navigate to specific types of information about the selected tree item.
3. Use the tabs to filter the information further.

Navigating using Links

Click *links* to jump to related pages.

Table 3.2 Links for Graphics Page and Properties Page

On a Graphics Page	On a Properties Page
	

Name: Electric Meter (#electric_meter4) Con

Controller: ME812u-LGR (#zs_me_lgr) Addre

Last Parameter Change: Tue Nov 27 16:12:37 E

3.2.5 Tree Icons and Hover Text

The navigation tree displays an icon to the left of each item to denote the type of item. For example:

Table 3.3 Display of Navigation Tree Icons

Icon	Name
🏙	System
▦	Area
▣	Equipment

To select custom equipment icons in the Vertiv™ Liebert® SiteScan™ interface, right click the *equipment* on the Geographc 🌐 or Network 🖧 tree, select *Configure,* then select the *Icon*. Custom icons can also be selected in the EIKON application.

Optional Icons

To denote locations on the Geographic 🌐 tree where items were created or assigned, the user can display the following icons:

Table 3.4 Optional Icons

Icon	Name
🕒	Schedules
📈	Trend Graphs
⚠	Alarm Actions
👥	Schedule Groups
▦	Reports
🔑	Privileges

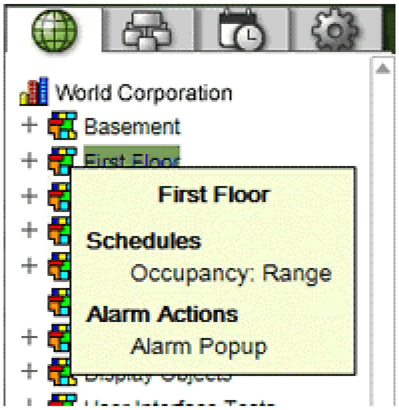
To Turn On Optional Icons:

1. Right click on the *Geographic* 🌐 *tree.*
2. Select *Tree Display Options.*
3. Select the desired *Tree Icons.*
4. Click *Accept.*

Optional Hover Text

If the hover text option is turned on, the user can hold the cursor over a system, area, or equipment icon to display information about its item. The information displayed depends on which hover text options are selected.

Figure 3.2 Hover Text



To Turn On Hover Text:

1. Right click on the tree.
2. Select *Tree Display Options.*
3. Select the desired *Tree Hover Text.*

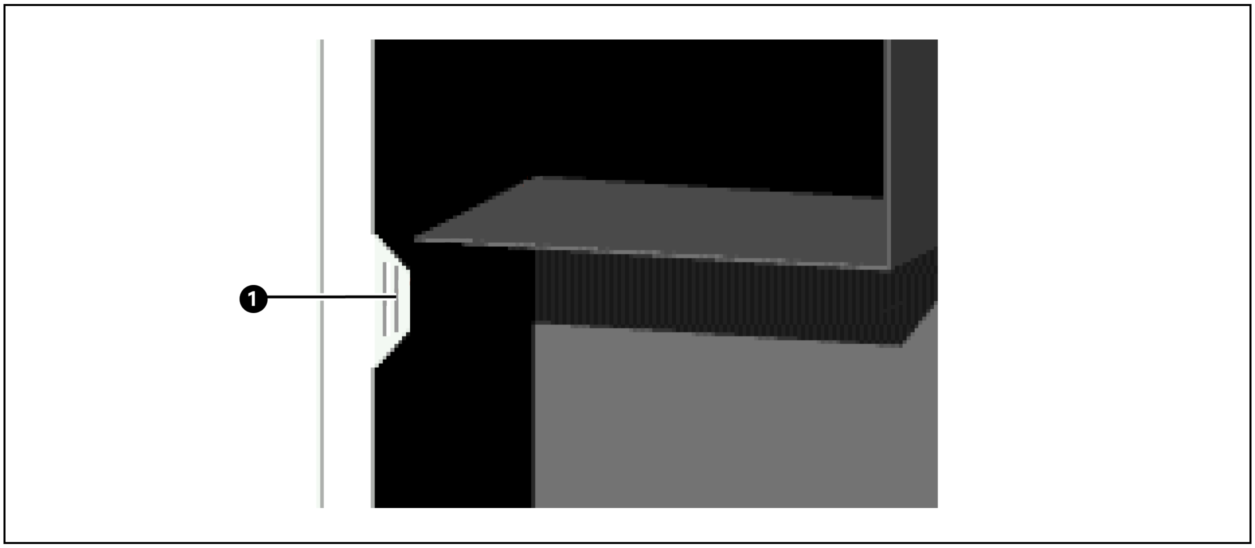
4. Click *Accept*.

3.2.6 Show, Hide, or Resize the Navigation Tree

On a Computer or Large Screen Mobile Device

1. Click SITESCANWEB to hide or show the tree.
2. Click and drag the *tab* on the right side of the tree to adjust its width.

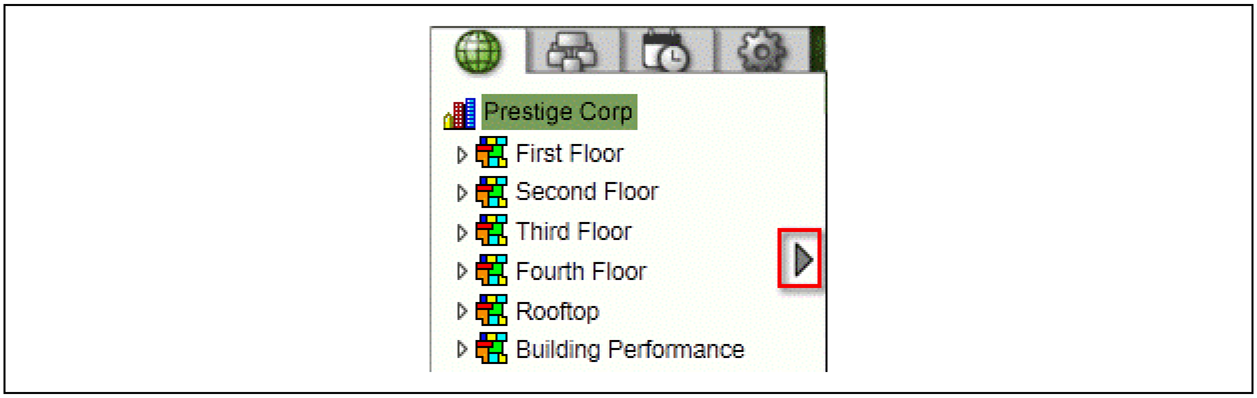
Figure 3.3 Adjusting Tab Width



Item	Description
1	Click and drag the tab

On a Small Screen Mobile Device

1. Touch SITESCANWEB at the bottom of the navigation tree to hide the tree. Touch to show it again.
2. Double tap the arrow on the right side of the tree to widen the tree. Double tap again to return to the original size.



3.2.7 Zooming In and Out

On a Computer

1. Refer the steps below to zoom in/out the Vertiv™ Liebert® SiteScan™ interface:
    - Hold down *Ctrl* and press + or -. Press *Ctrl+0* to return to 100%.
    - Hold down *Ctrl* while rolling the mouse wheel.
    - Use the zoom functions of web browser.
2. If a graphic does not fit in the action pane, right click on the graphic and select *Scale to Fit* to make it fit the action pane. Select *Scale to Fit* again to return the graphic to its original size.

On a Mobile Device

1. Apple iPad and iPhone
    - Double tap to zoom in/out.
2. Microsoft Surface
    - Pinch zoom works on individual frames, instead of the whole screen. So, you can zoom and scroll the navigation pane and action pane separately.
    - If browser text is too small, use *Ctrl +* to increase your browser's zoom level, then reload the page.
3. Google Nexus and Nexus Lumia
    - Pinch zoom to zoom in/out.

3.2.8 Right Click Menus

On a Computer

Right click on the following items to select options:

Table 3.5

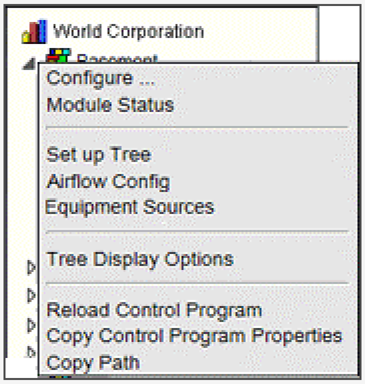
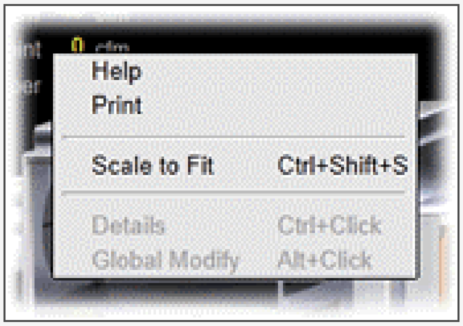
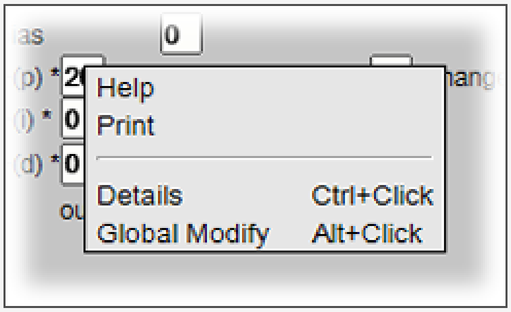
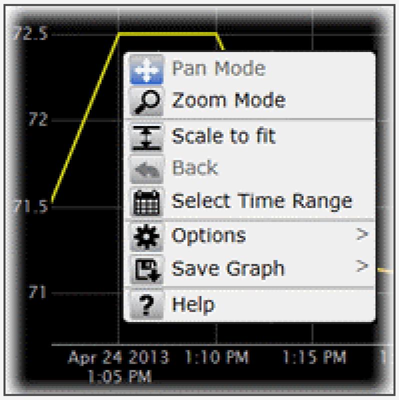
A Tree Item	The Action Pane
 World Corporation Basement Configure ... Module Status Set up Tree Airflow Config Equipment Sources Tree Display Options Reload Control Program Copy Control Program Properties Copy Path	 Help Print Scale to Fit Ctrl+Shift+S Details Ctrl+Click Global Modify Alt+Click

Table 3.6

A Property	A Trend
	

On a Mobile Device

To access the right click menu for:

- A Tree Item –Select the item first, then touch and hold the item for sa few seconds.
- The Action Pane –Touch and hold the item for a few seconds.

NOTE: For iPhones and iPads, touch and hold your finger on the item to bring up the right click menu, then drag your finger to the menu option that you want without lifting your finger.

3.2.9 Printing the Action Pane

On a Computer

Click 🖨 at the top of the page to print the contents of the action pane. Set the *print orientation* to Landscape in the Print dialog box.

NOTE: To print a Graphics page that exceeds the size of the action pane, right-click the graphic and select *Scale to Fit*.

On a Mobile Device

Touch ▾☰ and then select *Print*.

3.2.10 Downloading to Controllers

The user must download the new data from the Liebert® SiteScan™ application to the affected controllers, if any of the following changes are made:

Table 3.7 Changes to Controller

Controller	Changes Made
In the Liebert® SiteScan™ interface	• Change or reload a *control program* • Change or reload a *driver* • Change a *schedule* **NOTE: A schedule change automatically downloads unless you uncheck *Automatically download schedules on each change* on the My Settings page.** • Change a *touchscreen* or *BACview file* • Check or uncheck a *.view file* Included in download option
In SiteBuilder	• Add a *device* • Add *equipment* • Change or reload a *control program* • Set an *object instance* • Change or reload a *driver* • Assign or unassign *equipment* • Check or uncheck a *.view file* Included in download option

The Liebert® SiteScan™ application automatically marks the affected controllers as requiring a download. These controllers can be downloaded from the Downloads page (See Downloading from the Downloads Page on the facing page) or Properties page (See Downloading from a Properties Page on page 16) for the controller, the equipment, or a microblock.

The Liebert® SiteScan™ application determines what information needs to be downloaded when it marks a controller for download depending on the type of information that changed. See Download Options (See Download Options below).

NOTE: A property change in the Liebert® SiteScan™ interface automatically gets downloaded to the controller. If the download fails, the controller is added to the Downloads page with the reason for the failure.

To see who downloaded a controller last, go to the Network tree, select the controller, then do one of the following:

- Go to *Reports* > *Network* > *Controller Status*, then click *Run*.
- View *Downloaded* by on the Properties page.
- Click *Module Status* on the Properties page.

Download Options

The Liebert® SiteScan™ application determines what information needs to be downloaded when it marks a controller for download and it depends on the type of information changed. Below are the options that can be downloaded.

Table 3.8 Download Options

Options	Downloads
All Content	• The names and executable portion of the driver and control programs. • The names and full content of Equipment Touch and BACview files. • The names of any .view files that are marked to be included in a download. • Parameters. • Schedules **NOTE: An All Content download also:** **Synchronizes the time of the controller to the Liebert® SiteScan™ server.** **Overwrites trends in the controller.** **Restarts the controller.**
Only Schedules	All schedules that are not set for automatic download
Only Parameters	All editable properties
Only BBMDs	BBMD tables (.bdt file) that you have updated but have not yet written to the controller

NOTE: An All Content download clears trend, history, and alarm data from the affected controllers. Trends with the Trend Historian enabled are saved to the system database at the start of the download process.

The user can choose to download the full source files by selecting the All Content option. On the Liebert® SiteScan™ Network tree, select a *controller*, then enable *Download Source Files* on the Properties page.

Downloading from the Downloads Page

The Downloads page shows any controllers that the Liebert® SiteScan™ application marked for download. But if needed, you can add other controllers to the list.

Below are the steps to download:

1. On the Network tree, select an item to download controllers at and below that item.
2. Click *Downloads*.
3. Click ▶ to the left of a Location to see controllers that require a download.
4. Optional: To add controllers to the list:
   a. Click *Add*.
   b. Select the *controllers*.

NOTE: Use *Ctrl+click* or *Shift+click* to select multiple controllers.

   c. Select a *Download Option* (See Download Options on the previous page).
   d. Click *Add*, then click *Close*.
5. Select the *controllers* that you want to download.

NOTE: Use *Ctrl+click*, *Shift+click*, or the *Select All* checkbox to select multiple controllers.

The controllers of a network download in the order shown. To change the order, select a controllers, then drag and drop or click *Move to Top* or *Move to Bottom*.

NOTE: If the router of a controller requires a download, it will download first regardless of its position on the Download page.

6. Click *Start*.

NOTE: Click *Hold* to stop 🕒 pending downloads. Active downloads ⬇ cannot be stopped.

Up to 5 routers can download simultaneously.

A controller is removed from the list when its download is complete.

Icons in the Tasks column indicate the following:

Table 3.9 Task Column Icons

Icon	Description
⬇	Active — The Vertiv™ Liebert® SiteScan™ application is downloading to the controller.
🕒	Pending — You initiated the download, and the controller is waiting for its turn to download.
❌	Failed — The download failed. See If a controller fails to download (See If a Controller Fails to Download below).
✋	On Hold — Indicates either of the following: • The controller requires a download. • You clicked Hold to stop a pending download.

NOTE: Click ℹ in the upper left hand corner to view a log of download activity in the current session. Copy to Clipboard allows the user to copy the text to paste it into another application.

To remove an item from the download list, right click the *item*, then select *Remove selected tasks*.

Downloading from a Properties Page

A red download message and a Download button appears at the top of the Properties page for the controller, equipment, or microblock if the controller requires a download. Click the *Download button* to start the download.

Downloading from the Properties page downloads All Content to the controller.

If a Controller Fails to Download

A controller that fails to download appears on the Downloads page with this icon ❌.

1. Review the reason for the failure:
   - Hold your cursor over the failed task to see hover text giving the reason.
   - Click ❌ in the upper left hand corner of the page to see information on all failed downloads. Copy to Clipboard allows the user to copy the text to paste it into another application.
2. Correct the problem that caused the failure.
3. Select the *controller* on the Downloads page, then click *Start*.

3.2.11 Checking Controller Status

On the Vertiv™ Liebert® SiteScan™ Network 🖧 tree, select a network, router, site, or the system, and then click the *Devices button* to:

- View the status of controllers (See Status Messages below).
- View controller information such as address, model, driver, and .view files included in download.
- Download or upload to resolve a mismatch (See Handling Parameter Mismatches on page 19).
- Troubleshoot network communication (See Troubleshooting Networks on page 159).
- Download or upload files for Field Assistant (See Downloading Source Files from the Vertiv™ Liebert® SiteScan™ Application on page 189).

NOTE: Use *Ctrl+click*, *Shift+click*, or the *Select All* checkbox to select multiple controllers.

Click Hold to stop pending 🕒 downloads or uploads. Active downloads ⇩ or uploads ⇧ cannot be stopped.

Icons in the Tasks column indicate the following:

Table 3.10 Task Column Icons

Icon	Description
⇩	Active — The Liebert® SiteScan™ application is downloading to the controller.
⇧	Active — The Liebert® SiteScan™ application is uploading from the controller.
🕒	Pending — The user initiated the download, and the controller is waiting for its turn to download.
❌	Failed — The download failed. See If a Controller Fails to Download on the previous page .
✋	On Hold — Indicates the user clicked Hold to stop a pending download.

NOTE: Click ℹ in the upper left hand corner to view a log of activity on the Devices page in the current session. Copy to Clipboard allows the user to copy the text to paste it into another application.

Status Messages

To view the status of controllers, select a router, network, site or the system on the Liebert® SiteScan™ Network 🖧 tree. On the Devices page, the Status column shows a description of the controller's current state. Hold your cursor over that description to see hover text with a more detailed description.

If multiple conditions exist, Liebert® SiteScan™ displays the message with the highest priority.

The Table 3.11 on the next page shows all possible messages. The message color indicates the following:

Black — In process

Red — An error occurred

Blue — Requires action from the user

Table 3.11 Status Messages

Status Column Message	Hover Text Message	Notes
Black Messages:		
Downloading	The controller is downloading, communications may be disabled	
Pending	This controller is waiting to be processed.	
Processing clipping	Clipping operation is in progress. Do not make changes as they may corrupt your system.	
Uploading	The controller is uploading, communications may be disabled	
Red Messages:		
Communications Error	Cannot communicate with this controller.	
Connection Disabled	The connection for this controller has been disabled.	This message occurs if the connection is broken. This includes stopping a connection, using the *No Connect* connection, or running SiteScan Design Server.
Connection Error	The connection for this controller failed to start.	This message occurs if the connection is misconfigured or failed to start.
Download Failed	(Message depends on the cause of the failure.)	
Download Not Permitted	This controller is not permitted to download.	One or more source files have their *Permit Download* file permission disabled.
Error	An unknown error has occurred.	
Missing Files	Upload failed. Server is missing source files.	
Not Uploadable	This controller is not configured for content upload.	This message occurs if you attempt to upload a controller with a pre-4.x driver.
Out of Service	This controller is out of service.	*Out of Service* is checked on the controller's Properties page.
Unsupported controller	Controller does not support content upload.	
Upload Not Permitted	This controller is not permitted to upload.	One or more source files have their *Permit Upload* file permission disabled.
Blue Messages:		
Controller Replaced	This controller has been replaced by another controller of the same type in the field.	4.x driver only
Download All Content	Please download all content to the controller.	
Download Parameters	To download parameters, highlight row and select *Parameters* from the Download Action menu and click *Download*	
Download Schedule	To download schedules, highlight row and select *Schedules* from the Download Action menu and click *Download*	

Table 3.11 Status Messages (continued)

Status Column Message	Hover Text Message	Notes
Driver Parameter Mismatch	Driver parameter differences detected. Upload parameters from the controller or download parameters to the controller.	
Parameter Mismatch	Control Program parameter differences detected. Upload parameters from the controller or download parameters to the controller.	
Program Mismatch	Content differences detected. Upload all content from the controller or download all content to the controller.	4.x driver only
Unprogrammed controller	This is a programmable controller. To add control programs, click on the *Add Control Program* button at the top of the screen.	
Upload All Content	Please upload all content from the controller.	
General Messages:		
☑	This controller is ok.	
Cancelled	The last operation on this controller was cancelled.	

Handling Parameter Mismatches

A parameter mismatch occurs when a value in a controller does not match the value in the SiteScan Server application. This can be a driver or control program value.

Use either of the following methods to handle mismatches in your system:

1. **Method 1:** To have the Liebert® SiteScan™ application automatically upload if a value was changed in the controller or automatically download if a value was changed in the Liebert® SiteScan™ interface, check *Always resolve parameters on mismatch* on the System Settings > Communications tab.
2. **Method 2:** To evaluate a mismatch and determine the correct value, uncheck *Always resolve parameters on mismatch*.

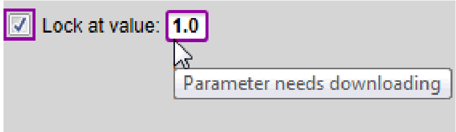
Finding Mismatches in your System

If the system uses Method 2, the user can find mismatches in the following places:

- The *Devices page* > *Manage tab* > *Status* column will show Parameter Mismatch.
- The Properties page for a controller, driver, control program, or point will show one of the following red messages at the top of the page stating:
  - Control Program parameter differences detected.
  - Driver parameter differences detected.
  - Parameter download required.

The value that has a discrepancy will appear with a purple box around it. Hover your cursor over the field to see:

Figure 3.4

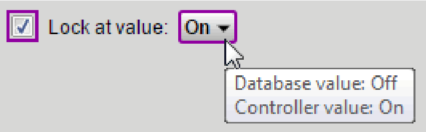


☑ Lock at value: 1.0

Parameter needs downloading

OR

Figure 3.5



☑ Lock at value: On

Database value: Off
Controller value: On

- Go to *Reports* > *Equipment* > *Parameter Mismatch*, and then click *Run* to get a report of any existing mismatches in your system.

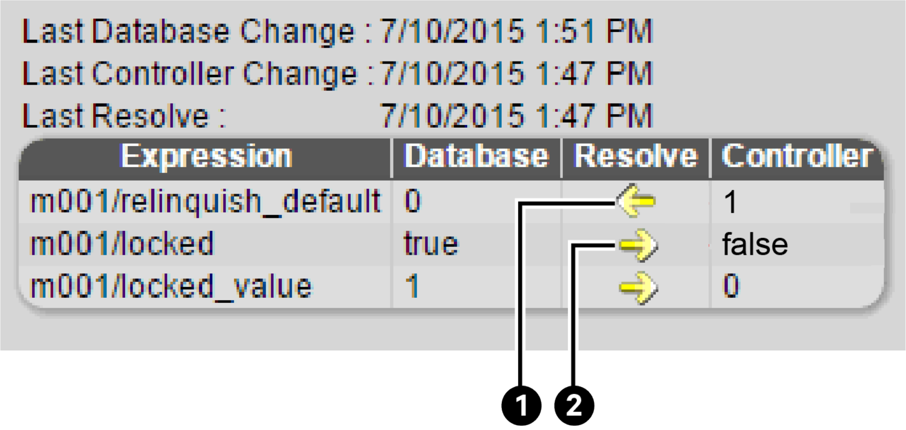
NOTE: The *Downloads page* > *Tasks* column will show *Resolve Parameters* for any mismatches that your system discovered in the 3 places listed above.

Resolving a Mismatch

To resolve a mismatch, follow the below steps:

1. Go to any one of the following pages:
   - Devices page - Click the *Parameter Mismatch* link.
   - Properties page - That shows one of the red messages above.
2. Click one of the following:
   - Resolve to allow the Vertiv™ Liebert® SiteScan™ application download changes made in the Liebert® SiteScan™ interface or upload changes made in the controller. Click the *Details* button to learn more about the discrepancy and whether Resolve will download or upload parameters.

Figure 3.6



Last Database Change : 7/10/2015 1:51 PM
Last Controller Change : 7/10/2015 1:47 PM
Last Resolve : 7/10/2015 1:47 PM

Expression	Database	Resolve	Controller
m001/relinquish_default	0	←	1
m001/locked	true	→	false
m001/locked_value	1	→	0

Item	Description
1	Upload
2	Download

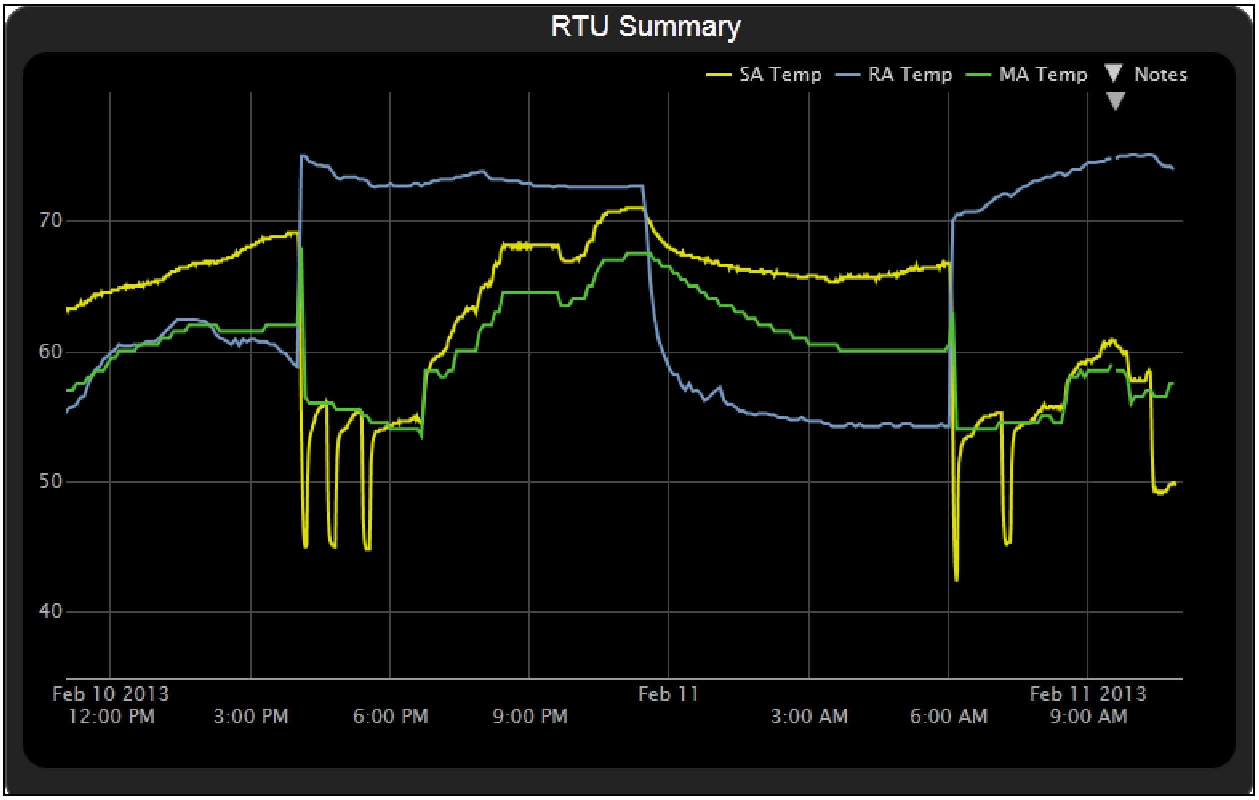
- Upload - To upload the parameters from the controller to the Liebert® SiteScan™ application.
- Download - To download the parameters from the Liebert® SiteScan™ application to the controller.

NOTE: If a controller has simultaneous mismatches in the driver and control program and Show Control Programs is unchecked on the Devices page, clicking *Details* will show that a control program mismatch exists but will only show details for the driver mismatch. To view the details of that mismatch, navigate to the control program in the tree. However, clicking *Resolve* will resolve both mismatches.

3.3 Trends

The Vertiv™ Liebert® SiteScan™ system can read and store equipment status values over time and then display this information in a trend graph to help the user to monitor the operation of the equipment..

Figure 3.7 Trend Graph

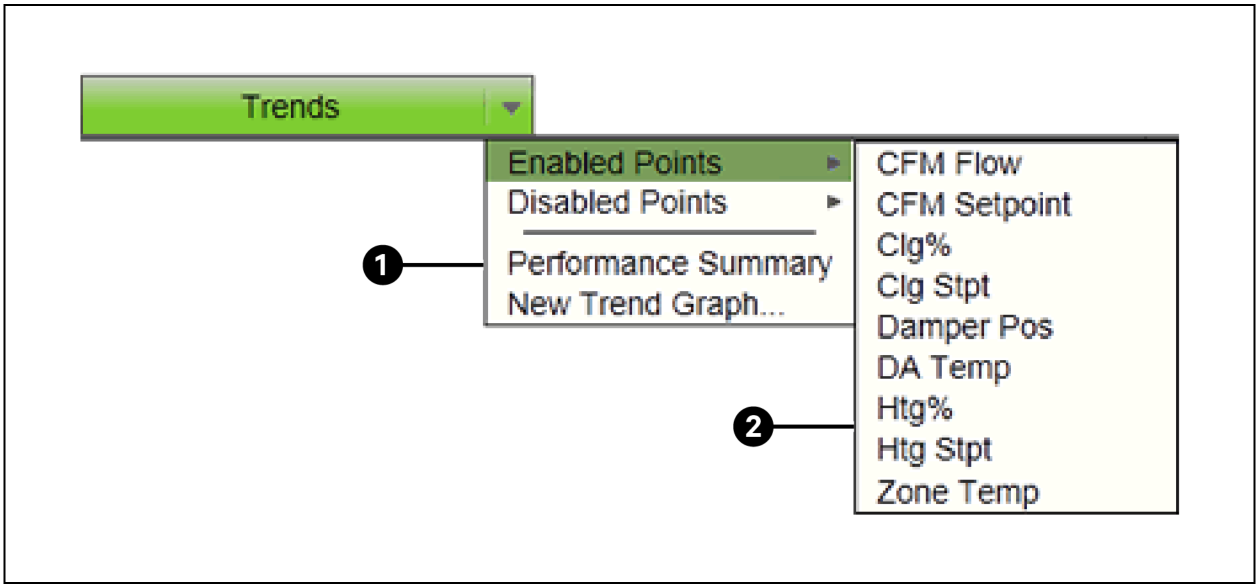


The user can collect trend data for any point value in the Liebert® SiteScan™ system. The controller reads point values at intervals that the user defines and then stores that data in the controller. A controller has limited memory for storing trend data, so the user can set up historical trending to archive the trend data from the controller to the Liebert® SiteScan™ database. A trend graph can display data from the controller and the database, or it can display only data stored in the database.

Once the desired points for trend data collection are set (See Collecting Trend Data for a Point on the facing page), you can:

- View built in trend graphs that show a single point (See Viewing a Builtin, Single Point Trend Graph on page 25).
- Create custom trend graphs with multiple points (See Creating a Custom Trend Graph on page 25).

Figure 3.8



Item	Description
1	Custom Trend Graph
2	Single-point graphs

3.3.1 Collecting Trend Data for a Point

To see a trend graph for a point, the user must first enable trending for that point and then define how the user wants the controller to collect the data for that point. This can be done in the EIKON application or in the Vertiv™ Liebert® SiteScan™ interface using the instructions below.

NOTE: I/O microblocks have trending capability built in, and you enable trend logging in the I/O microblock. Any other microblock value must have a trend microblock attached in the control program, and you enable trend logging of the value in the trend microblock.

To set up trending for a point in the Liebert® SiteScan™ Interface, follow the below steps:

1. On the Geographic 🌐 tree, select the equipment that has the point you want to trend.
2. Click the *Trends* button drop down arrow, select *Disabled Points*, then select the point.
3. On the Enable/Disable tab, check *Enable Trend Log*.
4. Enter information in the appropriate fields. See table below.
5. Click *Accept*.

NOTE: On the Trend Sources tab of the Properties page of .the equipment, the user can set up all trends for a piece of equipment at once.

Table 3.12

Field	Notes
Sample every _:_:_ (hh:mm:ss)	Records the value of the point at this interval. **NOTE: Set trend intervals for U line controllers to one minute or greater. U line controllers are designed to meet low end, high volume terminal control applications and are not suited to very short trend intervals.**
Sample on COV (change of value)	Records the value of the point only when the value changes by at least the amount of the COV Increment. **NOTE: Use this method for a binary point or for an analog point that has infrequent changes in value.**
Max samples	The maximum number of samples that you want the controller to store. ⚠ **CAUTION: Changing the value in Max samples will delete all the trend samples of the point currently stored in the controller. Click the Store Trends Now button before changing the value to transfer the trend data from the controller to the system database.** **NOTE: Trending consumes memory in the controller. The amount of memory available depends on the type of controller. Each trended point consumes 48 bytes of memory plus 10 bytes for each trend sample. Each trend microblock consumes 416 bytes of memory plus 10 bytes for each trend sample.** **NOTE: Click *Reset* to delete all samples currently stored in the controller.**
NOTE: The above sample and memory allocation fields together define trend data storage in the controller in terms of hours. **Example: If you set these fields so that samples are collected every 5 minutes for a maximum of 120 samples, the controller will store 600 minutes (5 x 120) or 10 hours of trend data.**	
Stop When Full	Check this field to stop trend sampling when the maximum number of samples is reached.
Enable trend log at specific times only	Collects trend data for the specific period of time that the user defines in the time and date fields.
Enable Trend Historian	Archives trend data to the system database.
Store Trends Now	Writes all trend data in the controller to the system database without having to enable trend historian.
Write to historian every __ trend samples	Writes all trend data in the controller to the system database each time the controller collects the number of samples that the user enters in this field. This number must be greater than zero and less than the number entered in the field *Max samples*. The number of trends specified must be accumulated at least once before the historical trends can be viewed.
Trend samples accumulated since last notification	Shows the number of samples stored in the controller since data was last written to the database.
Last Record Written to Historian	Shows the number of trend samples that were last written to the database.
Keep historical trends for __ days	This is based on the date that the sample was read. Select the first option to use the system default that is defined on the *System Settings > General* tab. Select the second option to set a value for this trend only.
Delete	Deletes all trend samples stored in the database for the item selected on the Geographic 🌐 tree.
BACnet Configuration	The Object Name is a unique alphanumeric string that defines the BACnet object. Although the Object Name field can be edited, it is not recommended. The Notification Class is set to 1 to receive alarms generated by Vertiv controllers.

NOTE: Use Global Copy to copy trend properties to other pieces of equipment that use the same control program.

Run a Trend Usage report (See Preconfigured Reports on page 68) to view trend configurations.

3.3.2 Viewing a Builtin, Single Point Trend Graph

1. On the Geographic tree, select the equipment whose trend you want to view.
2. Click the *Trends* button drop down arrow, select *Enabled Points*, and then select the graph you want to view.
3. Select the *View* tab. See Using Trend Graphs on page 28 .

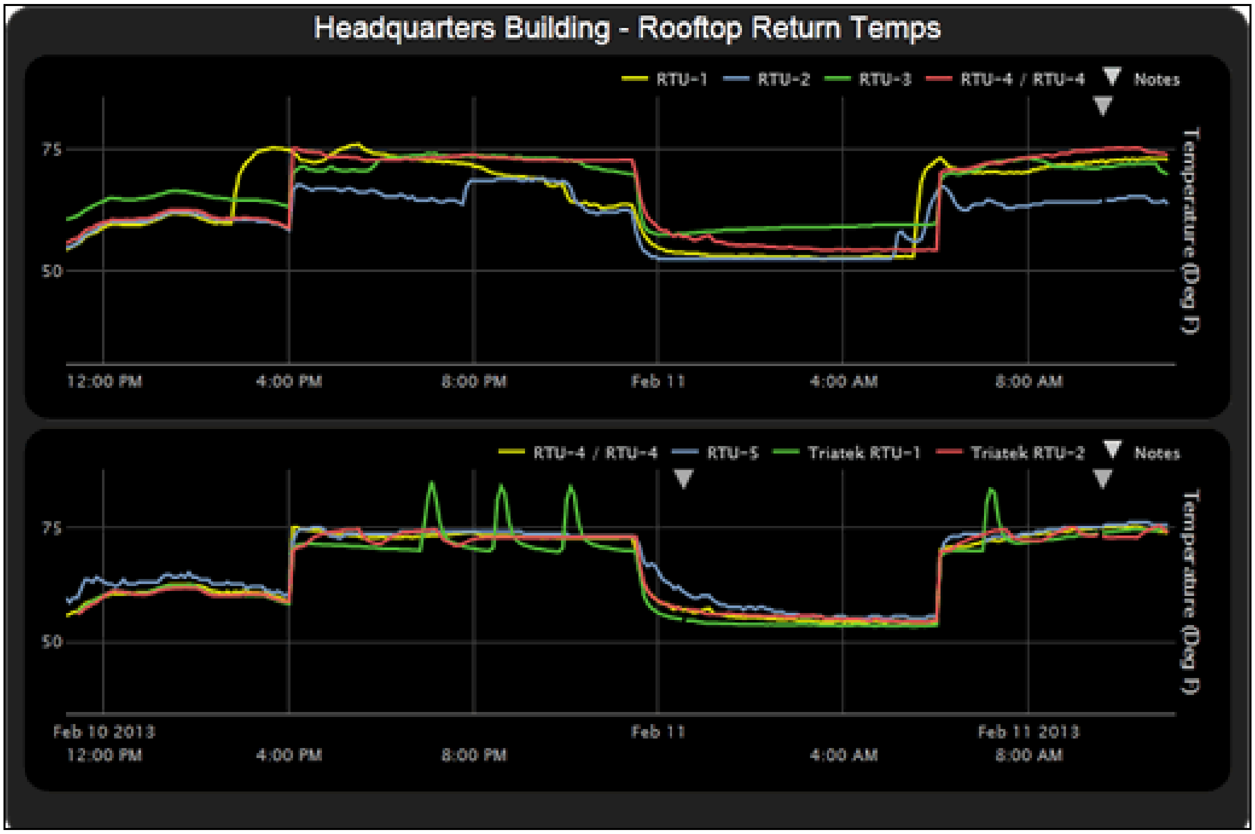
NOTE: On the Configure tab, you can:

- Enable/disable the grid.
- Set the time range for the X axis. For example, enter 7 days to see the data for the last week.
- Turn off autoscaling so that the user can define a range for the Y-axis.
- Type a Y axis label that will appear on the right side of the graph.

3.3.3 Creating a Custom Trend Graph

The user can select up to 16 points when creating a custom trend graph. The Liebert® SiteScan™ application divides the data into subgraphs if more than 4 points or points with different units are selected. A maximum of 4 points with comparable units can be displayed in each subgraph.

Figure 3.9 Custom Trend Graph



NOTE: To include points in the custom trend graph, enable trending for that points. See Collecting Trend Data for a Point on page 23 .

The user can display icons and hover text on the Geographic 🌐 tree that show where custom trend graphs were created. See Tree Icons and Hover Text on page 9 .

Creating a Custom Trend Graph

Follow the below steps to create a custom trend graph:

1. On the Geographic 🌐 tree, select the area or equipment where you want to see the graph.
2. Click the *Trends* button drop down arrow, then select *New Trend Graph*.

NOTE: If the Trends button does not have a drop down arrow, the New Trend Graph page is already displayed.

3. In the tree on the New Trend Graph page, use *Ctrl+click* or *Shift+click* to select the points (16 maximum) that you want to see on a graph.

NOTE: The tree shows only points that have trending enabled. See Collecting Trend Data for a Point on page 23 .

4. Click *Save*.
5. Optional: If your system has trend categories defined, you can select a *Category* for this trend. For more information on trend categories, see Adding Trend Categories on the facing page .
6. Type a *Name* for the graph that will appear at the top of the graph and in the Trends button drop down list.
7. Click *OK*.
8. Select:
   - The *View* tab to see the custom trend graph. See Using Trend Graphs on page 28 .
   - The *Configure* tab to edit the trend graph. See Editing a Custom Trend Graph below .

Editing a Custom Trend Graph

Follow the below steps to edit a custom trend graph:

1. On the Geographic 🌐 tree, select the area or equipment where you created the graph.
2. Select the *Trends* > *Configure* tab. On this page, you can:
   - Change the name of the custom trend graph.
   - Enable/disable the grid.
   - Set the time range for the X axis.
   - Edit a Y axis label of subgraph that will appear on the right side of the graph.
   - Turn off autoscaling so that you can define a range for the Y-axis.
   - Add/delete subgraphs (see Adding a Subgraph to a Custom Trend Graph below).
   - Add/delete points (see Adding a Point to a Subgraph on the facing page).
   - Change the name of a point on the graph.
   - Change the active/inactive text of a binary point on the graph.
   - Click *Delete Trend Graph* to delete the entire custom trend graph.

Adding a Subgraph to a Custom Trend Graph

1. Click *Add* below the *Subgraphs* list.
2. Type a Y axis label.

3. Click *Add* below the *Points* list.
4. Select a point in the *Data source* tree.

NOTE: The tree shows only points that have trending enabled. See Collecting Trend Data for a Point on page 23 .

5. Repeat steps 3 and 4 to add up to 4 points to the subgraph.
6. Click *Accept*.

NOTE: To delete a subgraph, select it in the Subgraphs list, click *Delete* below the list, and then click *Accept*.

Adding a Point to a Subgraph

1. Select the subgraph in the *Subgraphs* list.
2. Click *Add* below the *Points* list.
3. Select a point from the *Data source* tree.

NOTE: The tree shows only points that have trending enabled. See Collecting Trend Data for a Point on page 23

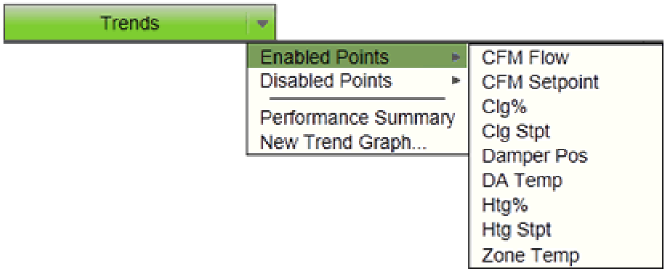
4. Click *Accept*.

NOTE: To delete a point, select the appropriate subgraph, select the point, click *Delete* below the Points list, and then click *Accept*.

3.3.4 Adding Trend Categories

A point trend graph is in the *Enabled* or *Disabled* category in the *Trends* button drop down menu.

Figure 3.10 Enabling/Disabling Point Trend Graph



Follow the below steps to create additional categories for your custom trend graphs:

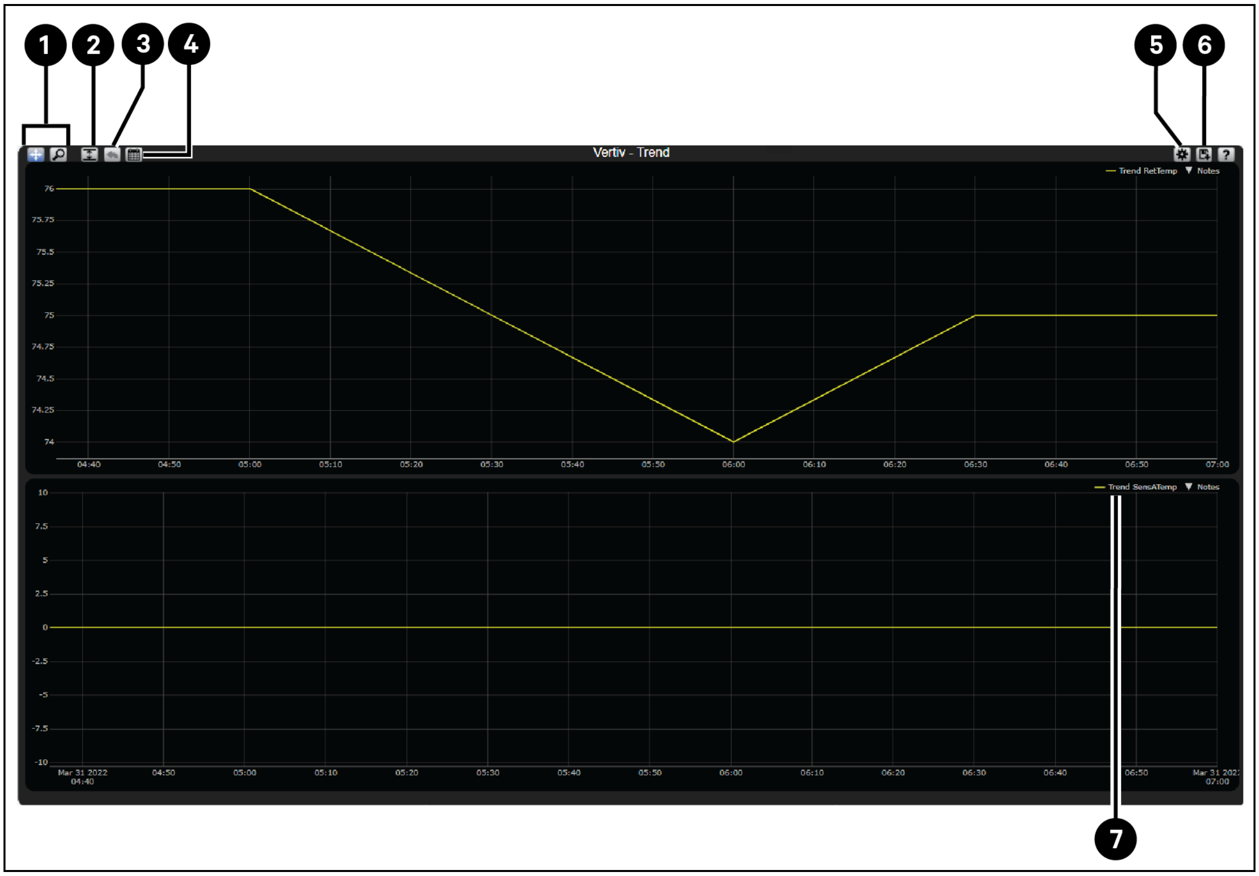
1. On the System Configuration ⚙ tree, click ▶ to the left of *Categories*, then select *Trend*.
2. Click *Add*.
3. Type the *Category Name* and *Reference Name*.
4. Optional: Select a privilege so that only operators with that privilege can access trends in the category.
5. Click *Accept*.

NOTE: To edit a category, select the category, make your changes, then click *Accept*.

To delete a category, select the category, click *Delete*, then click *Accept*.

3.3.5 Using Trend Graphs

Figure 3.11



Item	Description
1	Mouse Mode: • Pan • Zoom NOTE: Click and drag will Pan or Zoom. Hold Shift to swap
2	Scale NOTE: Scale the Y-axis to fit the data
3	Back
4	Graph Center

Item	Description
5	Toolbar options: • Auto update from field • Show database values only • Black and White • Display gap in graph line for missing data
6	Save as: • PNG • JPEG • SVG • PDF • CSV
7	Legend **NOTE: Click *Legend* to toggle visibility**

NOTE: A gray triangle at the top of a graph indicates a note from the system. Hover the cursor on the triangle to see which of the following occurred:

- Equipment received a time synchronization from its network router or from the Vertiv™ Liebert® SiteScan™ application.
- Trend Historian has been enabled or disabled.
- Trend Log has been enabled or disabled.

The trend object ID of a third party trend source has been changed. This is for information only, and the user do not need to do anything.

- Click 🖨 at the top of the Liebert® SiteScan™ page to print the graph. You may need to set your printer's orientation to Landscape.
- Toolbar options are also accessible by right clicking a trend graph.
- You can check *Display gap in graph line for missing data* on an individual trend graph page, or you can go to the System *Settings* > *General* tab (See General Tab on page 199) to set this for all future trend graphs.

Viewing Trend Data in a Spreadsheet Program

The user can save trend data as csv data that can be opened in a spreadsheet program such as Microsoft Excel.

1. On the *Trends* > *View* tab, select 💾 > *Save as CSV data*.
2. Save the data (.zip file) wherever you want. The .zip file contains the following:
   - A .csv file for each trend source (point). The filenames match the point names.
   - A combined folder containing a file with the combined data for all the trend sources of the graph.
3. Open the .csv file in a spreadsheet program.

NOTE: The data in the Time column of the spreadsheet must be converted to a readable date/time format

If you are using Microsoft Excel on a Mac and the converted date shows the wrong year, follow the below steps:

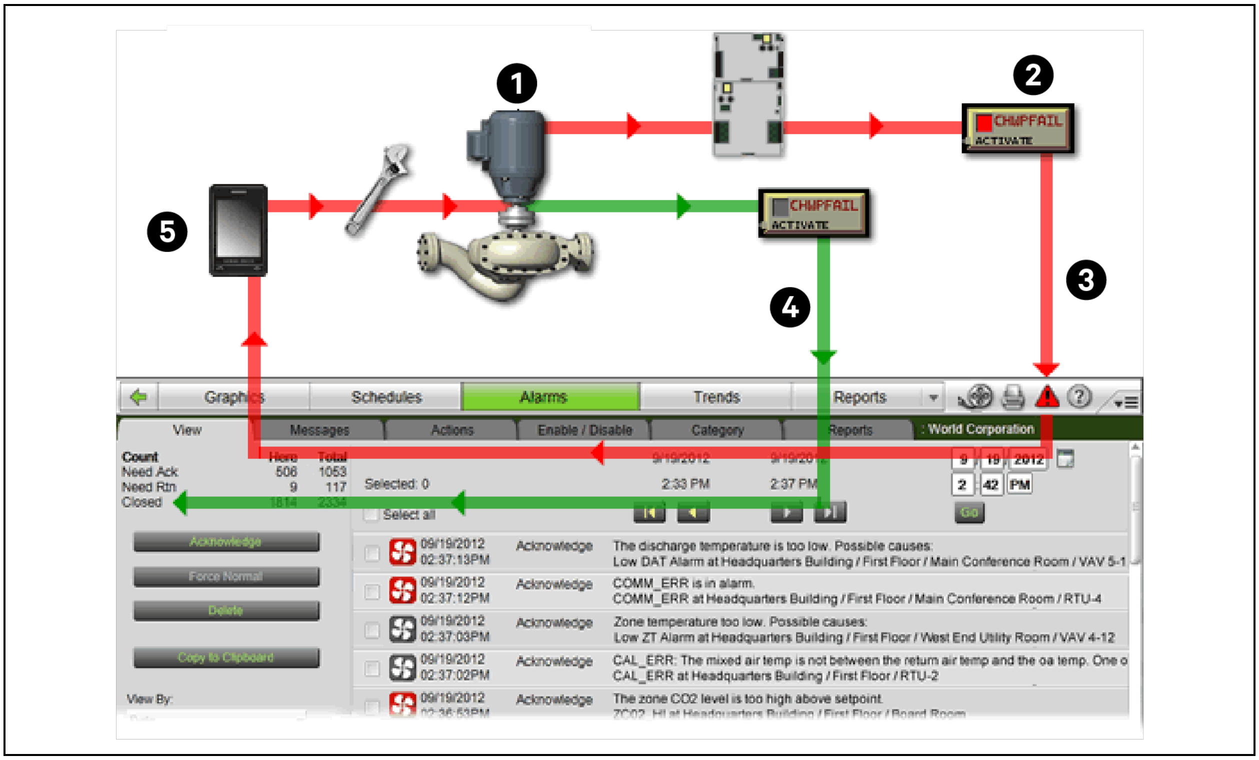
1. In Excel, go to *File* > *Options* > *Advanced*.

2. Scroll down to the section when calculating this workbook, and then uncheck Use 1904 date system.

3.4 Alarms

An alarm is a message sent from an alarm source (usually a microblock in a control program) to the Vertiv™ Liebert® SiteScan™ application to notify the user that certain conditions exist, such as a piece of equipment has stopped running or a temperature is too high. When the Liebert® SiteScan™ application receives an alarm, it displays information about the alarm on the Alarms page. It can also perform alarm actions to inform personnel of the condition and to record information about the alarm. An alarm source can also send a return to normal message when the alarm condition returns to its normal state.

Figure 3.12



09/19/2012 02:37:13PM Acknowledge The discharge temperature is too low. Possible causes: Low DAT Alarm at Headquarters Building / First Floor / Main Conference Room / VAV 5-1

09/19/2012 02:37:12PM Acknowledge COMM_ERR is in alarm. COMM_ERR at Headquarters Building / First Floor / Main Conference Room / RTU-4

09/19/2012 02:37:03PM Acknowledge Zone temperature too low. Possible causes: Low ZT Alarm at Headquarters Building / First Floor / West End Utility Room / VAV 4-12

09/19/2012 02:37:02PM Acknowledge CAL_ERR: The mixed air temp is not between the return air temp and the oa temp. One o CAL_ERR at Headquarters Building / First Floor / RTU-2

09/19/2012 02:36:53PM Acknowledge The zone CO2 level is too high above setpoint. ZCO2_HI at Headquarters Building / First Floor / Board Room

Item	Description
1	Start point of Alarm Process
2	Alarm Source
3	Alarm
4	Return to Normal
5	Alarm Action

Alarm sources and the alarms they generate are assigned to categories, such as HVAC Critical or HVAC Maintenance, to help you work with related alarms.

The application engineer usually sets up alarm sources in the EIKON application. In the Vertiv™ Liebert® SiteScan™ interface, you can:

- View, troubleshoot, acknowledge, and delete alarms (See Viewing, Troubleshooting, Acknowledging, and Deleting Alarms on the facing page).

- Set up the alarm actions that the Liebert® SiteScan™ application performs (See Setting up Alarm Actions on page 38).
- Edit alarm sources that were set up in the EIKON application or set up new alarm sources to generate alarms (See Setting Up an Alarm Source in the Liebert® SiteScan™ Interface on page 54).
- Customize alarms by changing the category or message (See Customizing Alarms on page 57).

NOTE: The Liebert® SiteScan™ application features built-in system and equipment alarms in addition to the alarms that you set up.

3.4.1 Viewing, Troubleshooting, Acknowledging, and Deleting Alarms

The Liebert® SiteScan™ Alarms page displays alarms as they are received. When an alarm is received, the user can set options on the My Settings page to have the Liebert® SiteScan™ application play an audio file.

The setup of an alarm may require that it be acknowledged and/or the alarm condition returned to normal. An alarm incident group includes the alarm, its return to normal, and any other alarms associated with the incident. The Liebert® SiteScan™ application closes an alarm incident group when all of the following have occurred:

- You acknowledge the alarm (if required).
- The Liebert® SiteScan™ application receives a return to normal (if required).
- The Liebert® SiteScan™ application performs all alarm actions defined for the group.

NOTE: The user should delete alarms from your system as they are closed because large quantities of stored alarms can reduce the efficiency of your system.

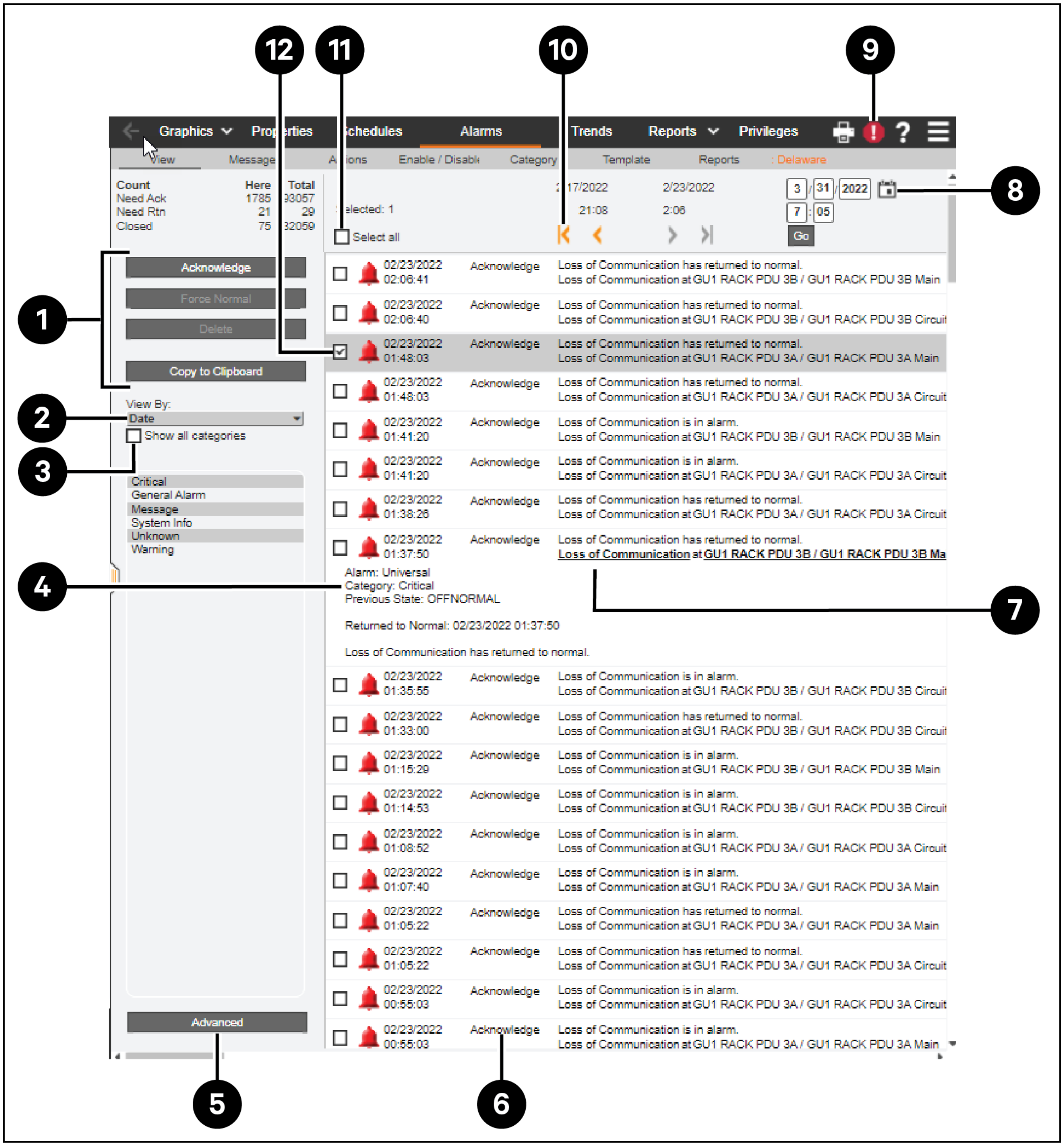
Viewing Alarms in the Liebert® SiteScan™ Interface

- Click ⚠ at the top of the page to see all alarms in the system.

  or

- Click the *Alarms* button and then select an item on the navigation tree to see all alarms at and below that level.

Figure 3.13



Count	Here	Total
Need Ack	1785	93057
Need Rtn	21	29
Closed	75	32059

2/17/2022 21:08 2/23/2022 2:06 3 / 31 / 2022 7 : 05

Selected: 1

☐	02/23/2022 02:06:41	Acknowledge	Loss of Communication has returned to normal. Loss of Communication at GU1 RACK PDU 3B / GU1 RACK PDU 3B Main
☐	02/23/2022 02:06:40	Acknowledge	Loss of Communication has returned to normal. Loss of Communication at GU1 RACK PDU 3B / GU1 RACK PDU 3B Circuit
☑	02/23/2022 01:48:03	Acknowledge	Loss of Communication has returned to normal. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Main
☐	02/23/2022 01:48:03	Acknowledge	Loss of Communication has returned to normal. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Circuit
☐	02/23/2022 01:41:20	Acknowledge	Loss of Communication is in alarm. Loss of Communication at GU1 RACK PDU 3B / GU1 RACK PDU 3B Main
☐	02/23/2022 01:41:20	Acknowledge	Loss of Communication is in alarm. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Circuit
☐	02/23/2022 01:38:26	Acknowledge	Loss of Communication has returned to normal. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Circuit
☐	02/23/2022 01:37:50	Acknowledge	Loss of Communication has returned to normal. Loss of Communication at GU1 RACK PDU 3B / GU1 RACK PDU 3B Ma

Alarm: Universal
Category: Critical
Previous State: OFFNORMAL

Returned to Normal: 02/23/2022 01:37:50

Loss of Communication has returned to normal.

☐	02/23/2022 01:35:55	Acknowledge	Loss of Communication is in alarm. Loss of Communication at GU1 RACK PDU 3B / GU1 RACK PDU 3B Circuit
☐	02/23/2022 01:33:00	Acknowledge	Loss of Communication has returned to normal. Loss of Communication at GU1 RACK PDU 3B / GU1 RACK PDU 3B Circuit
☐	02/23/2022 01:15:29	Acknowledge	Loss of Communication is in alarm. Loss of Communication at GU1 RACK PDU 3B / GU1 RACK PDU 3B Main
☐	02/23/2022 01:14:53	Acknowledge	Loss of Communication is in alarm. Loss of Communication at GU1 RACK PDU 3B / GU1 RACK PDU 3B Circuit
☐	02/23/2022 01:08:52	Acknowledge	Loss of Communication is in alarm. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Circuit
☐	02/23/2022 01:07:40	Acknowledge	Loss of Communication is in alarm. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Main
☐	02/23/2022 01:05:22	Acknowledge	Loss of Communication has returned to normal. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Main
☐	02/23/2022 01:05:22	Acknowledge	Loss of Communication has returned to normal. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Circuit
☐	02/23/2022 00:55:03	Acknowledge	Loss of Communication is in alarm. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Circuit
☐	02/23/2022 00:55:03	Acknowledge	Loss of Communication is in alarm. Loss of Communication at GU1 RACK PDU 3A / GU1 RACK PDU 3A Main

Item	Description
1	Acknowledge, Force Normal or Delete Alarms
2	View By: • **Date -** Most recent at top • **To do -** Only alarms that requore action • **Incident Group -** All aralrms for one incident
3	Show all Categories
4	Alarm Category
5	Advanced **NOTE: Click on Advanced to acknowledge or delete all alarms in selected categories, or to delete closed incident groups.**
6	Alarm Status: • **Acknowledge -** Needs to be acknowledged. Red text indicates a return to normal is also required • **Waiting for Normal -** Require return to normal • **Closed -** All required actionshave been performed
7	Show/Hide details **NOTE: Click on the alarm to show or hide details.**
8	Date and Time **NOTE: Type or select a date. Click *Go* to see alarms since that date/time.**
9	Click to see all alarms in system. Color indicates alarm needs to be acknowledged. • Red - Critical • Yellow - Non-Critical • Gray - None
10	Alarms > Views shows 50 alarms at a time. Click arrows to see more
11	Select all Alarms
12	Select one or more alarms

NOTE: The Vertiv™ Liebert® SiteScan™ tree can show 10 levels. If an alarm source is deeper than 10 levels, the alarm is reassigned to the system level.

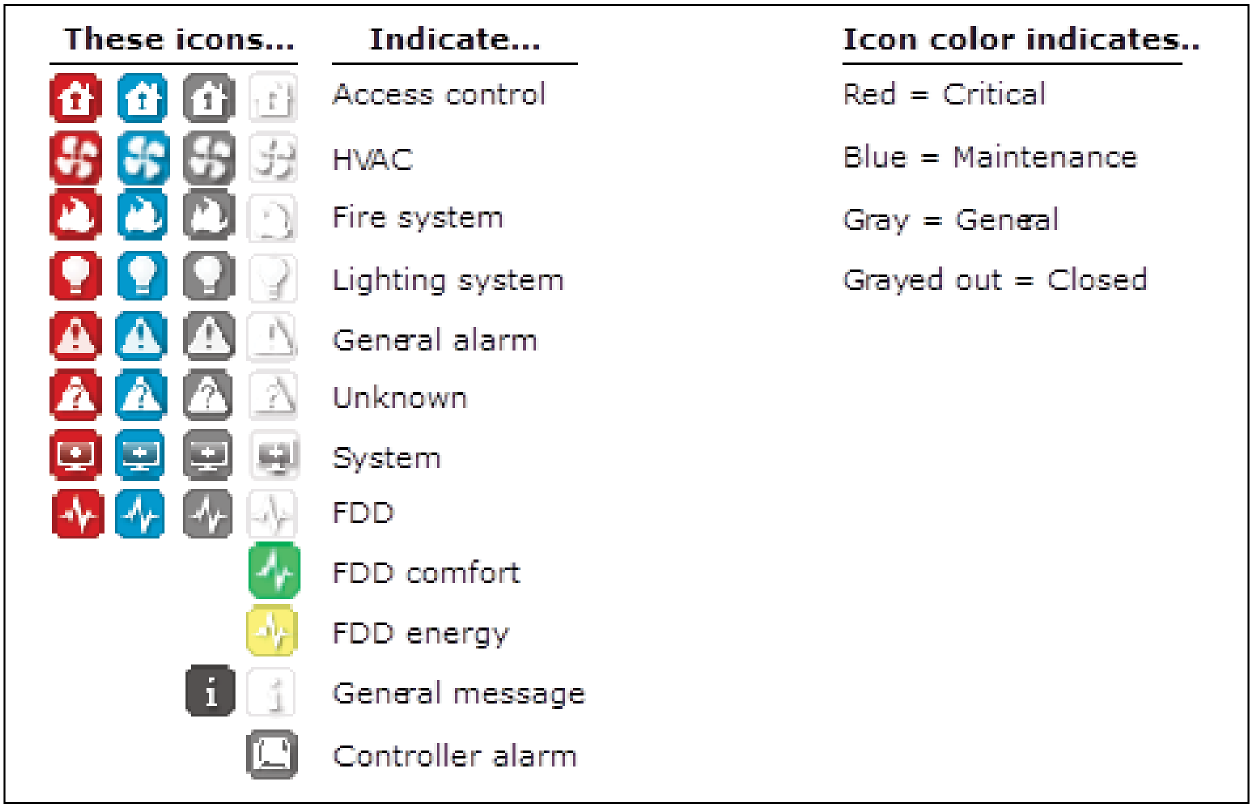
Alarms generated by the Liebert® SiteScan™ application appear at the system level.

Alarms generated by controllers appear at the system level on the Geographic tree, but in the network hierarchy on the Network tree.

The details of an alarm include a path to the alarm source. Each section of the path is a link to that location. For example, in the path East Wing/RTU-4/SSP_LO, East Wing links to the East Wing graphic, RTU-4 links to the equipment graphic, and SSP_LO links to the Properties page of the microblock.

The Liebert® SiteScan™ interface may display any of the following alarms icons:

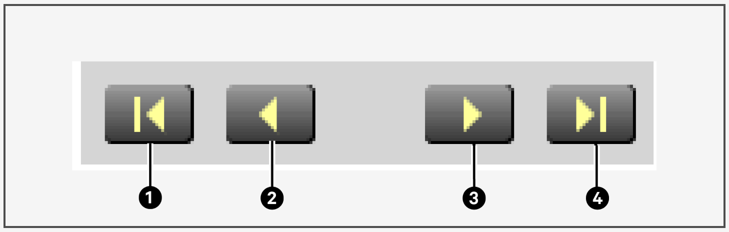
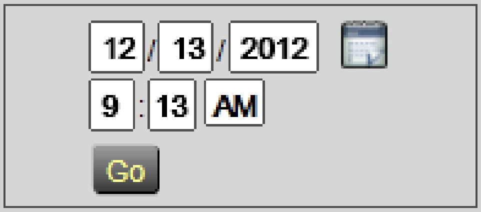
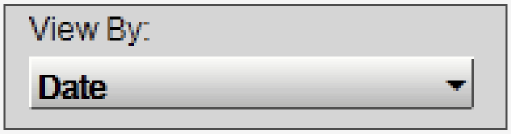
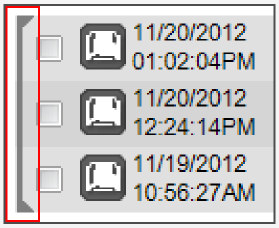
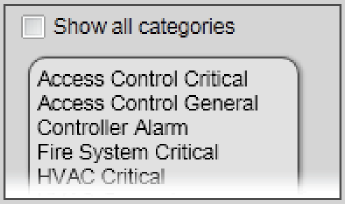
Figure 3.14 Alarm Icons



These icons...	Indicate...	Icon color indicates..
	Access control	Red = Critical
	HVAC	Blue = Maintenance
	Fire system	Gray = General
	Lighting system	Grayed out = Closed
	General alarm	
	Unknown	
	System	
	FDD	
	FDD comfort	
	FDD energy	
	General message	
	Controller alarm	

Controling the Alarms

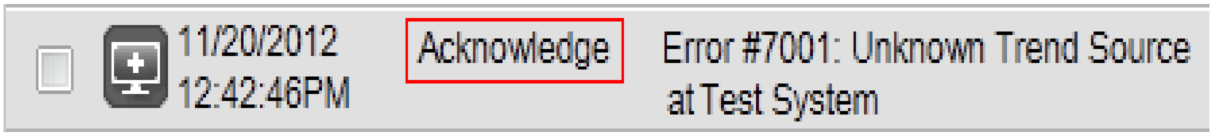
Table 3.13 Controling the Alarms

Tools	Actions to Control the Alarms List
 1. Oldest Alarms 2. Previous 50 Alarms 3. Next 50 Alarms 4. Newest Alarms	Click the arrow buttons to display other alarms.
 12 / 13 / 2012 9 : 13 AM 	Type a date and time or click 📅 to select a date. Then click *Go* to show up to 50 alarms since that date/time. When finished, click ⏭ to display the 50 newest alarms or ⏮ to display the oldest 50 alarms.
 View By: Date	Date–Sorts list by date/time the alarms were generated with the most recent at the top. To Do–Shows only alarms that require one or more actions before they are closed. Incident Group–Sorts alarms by incident. For example, an alarm and its return to normal form an incident group. Brackets indicate a group.  □ 11/20/2012 01:02:04PM □ 11/20/2012 12:24:14PM □ 11/19/2012 10:56:27AM
 □ Show all categories Access Control Critical Access Control General Controller Alarm Fire System Critical HVAC Critical	Select the alarm categories that you want to see in the alarms list. Use *Ctrl+click*, *Shift+click*, or both to select multiple categories, or check *Show all categories.*

Acknowledging Alarms

Alarms that have been set up to require acknowledgement must be acknowledged. An alarm shows if it needs to be acknowledged.

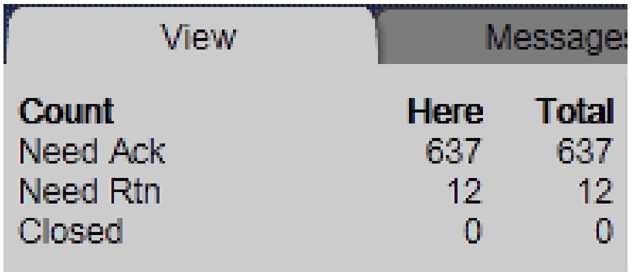
Figure 3.15 Acknowledging Alarms



□ 11/20/2012 12:42:46PM Acknowledge Error #7001: Unknown Trend Source at Test System

The table in the upper left corner of the page displays the number of alarms that need to be acknowledged at the current location (Here) and in the entire system (Total). This table also displays the number of alarms that need a return to normal and the number of alarms that are closed. See Figure 3.16 below .

Figure 3.16 Alarm Count



Count	Here	Total
Need Ack	637	637
Need Rtn	12	12
Closed	0	0

Acknowledging an Alarm:

1. On the *Alarms* page > *View* tab, select the checkbox of an alarm that shows *Acknowledge*.
2. Click the *Acknowledge* button.

Acknowledging all Alarms in the Alarms Database for Selected Categories

1. On the *Alarms* page > *View* tab in the left hand column, select the categories whose alarms you want to acknowledge.

NOTE: Use *Ctrl+click, Shift+click*, or both to select multiple categories, or select the *Select All* checkbox.

2. Click *Advanced*.
3. Click *Acknowledge All*.

NOTE: It takes a long time to acknowledge multiple alarms simultaneously. To avoid long waits, acknowledge alarms as they occur.

Deleting Alarms

Alarms should be deleted from your system as soon as they are closed because having a large number of stored alarms can reduce the efficiency of your system. To save alarm information before deleting, select *Alarms* > *Reports* tab > *Alarms*, then click the *Run* button.

To delete an alarm, follow the below steps:

1. On the *Alarms* page > *View* tab, select an alarm's checkbox.
2. Click *Delete*.

To delete all alarms in the alarms database for selected categories, follow the below steps:

1. On the *Alarms* page > *View* tab in the left hand column, select the categories whose alarms you want to delete.

NOTE: Use *Ctrl+click*, *Shift+click*, or both to select multiple categories, or select the *Select All* checkbox.

2. Click *Advanced*.
3. Click *Delete All Acknowledged*.

To delete all closed alarm incident groups in the alarms database, follow the below steps:

An incident group contains all alarms related to a particular incident.. For example, an alarm and its return-to-normal form an alarm incident group. An incident group is considered closed when all the alarms in the group are closed.

1. On the *Alarms* page > *View* tab in the left-hand column, select the categories whose alarms you want to delete.

NOTE: Use *Ctrl+click*, *Shift+click*, or both to select multiple categories, or select the *Select All* checkbox.

2. Click *Advanced*.
3. Click *Delete Closed Incidents*.

NOTE: An alarm that requires acknowledgment cannot be deleted until it has been acknowledged.

To have the Vertiv™ Liebert® SiteScan™ application automatically delete alarm incident groups a specified number of days after the groups close, select this option on the *System Settings > Scheduled Tasks* (See Scheduled Tasks Tab on page 203) tab.

Also on the *System Settings > Scheduled Tasks* tab, you can set the Liebert® SiteScan™ application to archive alarm information to a text file as alarms are deleted.

An alarm source may be set up to generate an alarm and a return to normal. If an alarm occurs but the Liebert® SiteScan™ application never receives the return to normal, you can select the alarm and then click *Force Normal* so that the alarm can be closed. Force Normal has no effect on the alarm condition that generated the alarm.

Receiving Audible Notification of Alarms

The Liebert® SiteScan™ application can be configured to play an audio file on your workstation when it receives a critical or non critical alarm.

1. On the System Configuration tree, select *My Settings*. See Changing My Settings on page 122 .
2. On the Settings tab, select *Non critical alarms* or *Critical alarms* to be notified of each type of alarm.
3. In the *Sound File* field, type the path to the sound file.

When an alarm triggers the audio file to play, you can click and then select:

- Snooze to temporarily stop the sound for 5 minutes.
- Silence to stop the sound.

The alarm sound is silenced until another alarm that triggers a sound is received.

3.4.2 Setting up Alarm Actions

The Vertiv™ Liebert® SiteScan™ application can perform alarm actions listed below to notify personnel of an alarm or to record information about the alarm. You can assign alarm actions to an alarm source, a category of alarm sources, alarm sources from a certain location, or a combination of these criteria.

The alarm actions that the Liebert® SiteScan™ application can perform are:

- Alarm Popup
- Print
- Propagate To Server
- Run External Program
- Send Alphanumeric Page
- Send E-Mail
- Send SNMP Trap
- Send Web Service Request
- Write Property
- Write to Database
- Write to File

See the following topics for a description of each alarm action:

Assigning Alarm Actions to Alarm Sources

Assigning Alarm Actions to Multiple Alarm Sources

Although the user can assign an alarm action to a single alarm source, at the area or equipment level, the user typically assigns an action to multiple alarm sources.The alarm action applies to all instances of the alarm sources at the selected location and below. Click the *Edit* button of Action tab to make any changes.

To assign an alarm action to alarm sources, follow the below steps:

1. On the Geographic or Network tree, select the area, equipment, or controller containing the alarm sources.
2. On the *Alarms* page > *Actions* tab, follow the 3 steps on the screen.

NOTE: Use *Ctrl+click*, *Shift+click*, or both to select multiple items.

3. Click *Add*.
4. Set up the alarm action by editing the fields on the alarm action page. See the appropriate alarm action below for field descriptions.
5. Click *Accept*.

Once the alarm actions are assigned to an alarm source,, simulate the alarm (See Simulating an Alarm on page 57) to check your work. If an alarm action fails, the Liebert® SiteScan™ application receives an alarm for the failed action.

NOTE: Click *View Selected Sources* to view or change settings for each alarm.

You can display icons and hover text on the Geographic tree that show where alarm actions have been created. See Tree icons and hover text (Tree Icons and Hover Text on page 9).

To assign an alarm action to a single alarm source, follow the below steps:

1. On the Geographic or Network tree, select the alarm source (microblock).
2. On the *Alarms* page > *Actions* tab, click the drop-down arrow, then select an alarm action.
3. Click *Add*.
4. Set up the alarm action by editing the fields on the alarm action page. See the appropriate alarm action below for field descriptions.
5. Click *Accept*.

Alarm Popup

The Alarm Popup alarm action pops up a message on any computer with a Windows operating system that is running the Vertiv™ Liebert® SiteScan™ Alarm Notification Client application.

Table 3.14

Field	Notes
To Operator To Group	Select individual operators or operator groups who should receive alarm notification. **NOTE: When using location dependent security, users only receive alarms for locations they are allowed to access.**
Generate alarm if delivery fails	Select this checkbox to generate a System Info alarm if the popup recipient is not currently running the Alarm Notification Client application.
Message text	Use punctuation, spaces, or returns to format the text. To add live data to the text, select field codes (See Using Field Codes on page 62) from the Append Field Code list.
Append Field Code	Add field codes (See Using Field Codes on page 62) to the message text if needed.
Perform Action	By default, the Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under *Perform Action*, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied*. • Create the alarm action that is to be performed after work hours. Under Perform Action, select *If schedule group <your new group> is Unoccupied*.

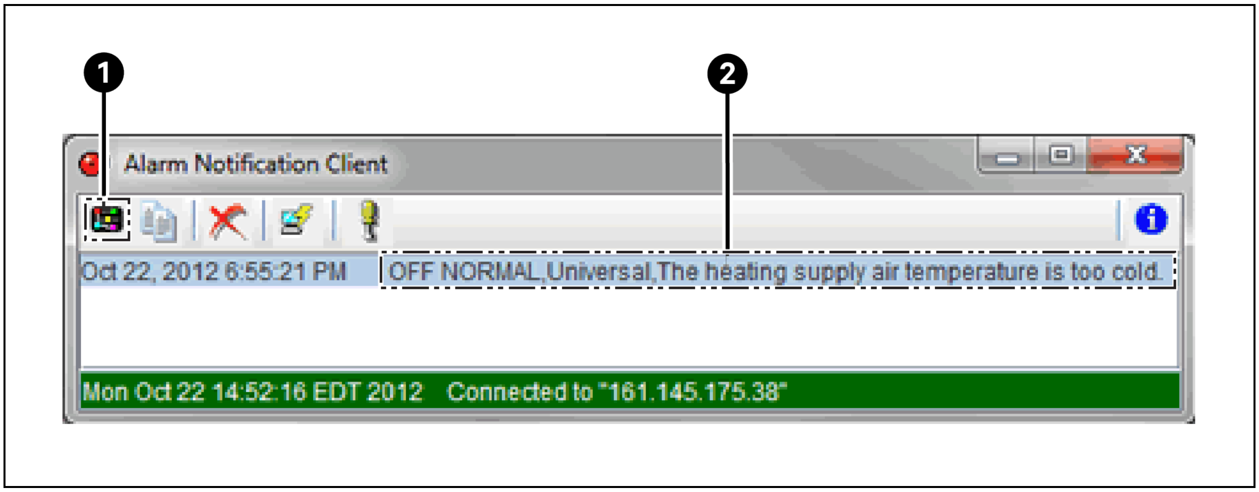
Alarm Notification Client Application

The Alarm Notification Client application must be running on each client computer (Windows only) that should receive popup notifications. Keep the application minimized to the right side of the Windows task bar. The window will pop up with a message when an alarm occurs.

Select an alarm message, then click to open a web browser window displaying the piece of equipment that generated the alarm. A grayed out alarm indicates that it was acknowledged in the Liebert® SiteScan™ interface.

If the Alarm Notification Client is set up to play a continuous alarm sound, you can silence an alarm by clicking *Silence!*, by pressing *Ctrl+S*, or by acknowledging the alarm in the Liebert® SiteScan™ interface.

Figure 3.17 Alarm Notification Client Window



Oct 22, 2012 6:55:21 PM

OFF NORMAL,Universal,The heating supply air temperature is too cold.

Mon Oct 22 14:52:16 EDT 2012 Connected to "161.145.175.38"

Item	Description
1	Browse to source equipment
2	Alarm message

Table 3.15 Alarm Notification Client Buttons

Button	Notes
	Opens a web browser window that displays the equipment that generated the alarm. **NOTE: If SiteScan Server is to use https (SSL), you must do the following to enable communication between the server and Alarm Notification Client. In SiteBuilder, go to *Configure > Preferences > Web Server*. For Enabled Web Server Ports, select *Both HTTP and SSL* or *SSL only*. In the Server Connection field described below, enter the number of the SSL port.** **If SiteScan Server is v6.0 and an Alarm Notification Client is an earlier version, you will have to log in when you click .**
📋	Copies the selected alarm information to the clipboard.
✗	Removes the alarm information from the alarm popup list. Removing items from this list has no effect on the alarms list in the Vertiv™ Liebert® SiteScan™ interface.
	View information about the server connection.

Table 3.15 Alarm Notification Client Buttons (continued)

Button	Notes	
	On this Tab	You Define
	Server Connection	The Vertiv™ Liebert® SiteScan™ server and port, and the Liebert® SiteScan™ operator name and password **NOTE: The default port is TCP 47806. If you change this, you must also change the Port field in the Liebert® SiteScan™ System Settings. See "To set up the SiteScan Server application to support Alarm Popup clients" below.** **You can use an IPv6 Server address in the Server field. In the Liebert® SiteScan™ interface, in *System Settings > General tab > Alarms*, you can restrict access to the IPv6 address.**
	Browse To	The Liebert® SiteScan™ page that you want to see first when browsing to the equipment
	Notification Sounds	• If you want to hear a sound when an alarm occurs. • Which sound you want to hear for each type of alarm. **NOTE: A Connection Failure occurs when the Alarm Notification Client loses communication with the SiteScan Server application.** • Whether you want the sound to continue until silenced. **NOTE: If multiple types of alarms occur simultaneously, the application plays the sound of the most critical alarm (Connection Failure first, then Critical, then Normal).**

To set up the SiteScan Server application to support Alarm Popup clients, follow the below steps:

1. On the System Configuration tree, select *System Settings*.
2. On the General tab, select *Enable support for Alarm Notification Clients to connect to this server*.
3. If the server has more than one network interface adapter, enter the IP address to which the Alarm Notification Client application will connect in the *Restrict to IP Address* field. You must specify the same IP address in the *Server* field in the Alarm Notification Client.
4. Use the default port or specify a different port. You must specify the same port in the *Port* field in the Alarm Notification Client.
5. Click *Accept*.

NOTE: If the Alarm Notification Client application is not on the local network and will access Liebert® SiteScan™ alarms through a NAT router, you must port forward the TCP port you defined in step 4 above.

To install the Alarm Notification Client application, follow the below steps:

Follow the steps below on each client computer that should receive alarm popups.

Prerequisite - Enable support for Alarm Popup client in System Settings. See Alarm Popup on page 39 .

1. On the System Configuration tree, click *Client Installs*.
2. Select *Alarm Notification Client*.
3. Click *Run*, then follow the on screen instructions to install the Alarm Notification Client application. After you click *Done*, the application starts automatically.
4. In the Settings dialog box, enter appropriate values. You can also click to open this box. See the table above for a description of each setting.

NOTE: You can lock the Settings so that a user cannot edit them. See Locking the Settings Feature of a Client: below .

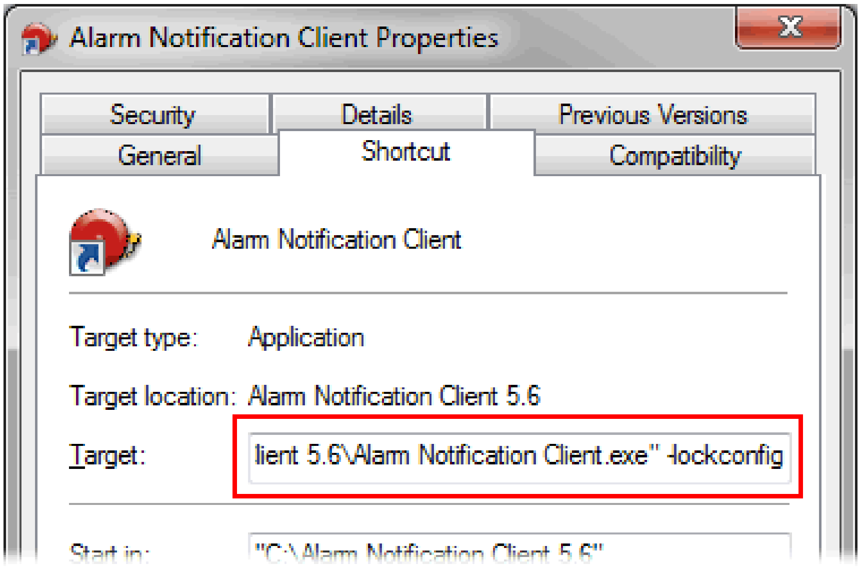
5. Click *OK*.
6. Minimize the Alarm Notification Client window.

Locking the Settings Feature of a Client:

To lock the settings feature of a client to prevent the user from editing the settings , follow the below steps:

1. Right click *Alarm Notification Client* in the Windows Start menu.
2. Select *Properties*.
3. On the *Shortcut* tab, type *-lockconfig* at the end of the Target path.

Figure 3.18 Locking the Settings Feature of a Client



Alarm Notification Client Properties

Alarm Notification Client

Target type: Application

Target location: Alarm Notification Client 5.6

Target: lient 5.6\Alarm Notification Client.exe" -lockconfig

Start in: "C:\Alarm Notification Client 5.6"

3.4.3 Print

The Print alarm action prints alarm information.

Table 3.16 Print Alarm Action Options

Field	Notes
Text Printing	Select to use the local dot-matrix printer of the Vertiv™ Liebert® SiteScan™ server. Text Printing will not print to a network printer. In the Port Name field, type the computer port to which the printer is connected. In the Line Width field, type the number of characters to be printed per line. Prints multiple alarms per page.
Graphics Printing	Select to use the default printer (local or network printer) of the Liebert® SiteScan™ server. Prints one alarm per page to the default printer of the Liebert® SiteScan™ server.
Text to Print	Use punctuation, spaces, or returns to format the text. To add live data to the text, select field codes (See Using Field Codes on page 62) from the *Append Field Code* list.
Perform Action	By default, the Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under *Perform Action*, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under PerformAction, select *If schedule group <your new group> is Unoccupied.*

Propagate to Server

The Propagate To Server alarm action sends the selected alarm to the parent server in a system with hierarchical servers.

Table 3.17 Propagate To Server Alarm Action Options

Field	Notes
Message text	The alarm message that is sent to the parent server.
Append Field Code	Add field codes (See Using Field Codes on page 62) to include live data in the Message text field.
Perform Action	By default, the Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under *Perform Action*, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under PerformAction, select *If schedule group <your new group> is Unoccupied.*

Run External Program

The Run External Program alarm action starts a program or batch file on the server.

NOTE: To set up this alarm action, the user must be running SiteScan Design Server.

Table 3.18 Run External Program Alarm Action Options

Field	Notes
Command Line	The path of the executable file on the Vertiv™ Liebert® SiteScan™ server followed by the path of the output file. Example: c:\windows\notepad.exe c:\SiteScan\webroot\alarms.txt
Append Field Code	Add field code (See Using Field Codes on page 62) to the Command Line field. Example: c:\reports\run_report.bat $Generation_time$$To_State$ This starts a batch file on the server and uses the generation time of the alarm and state as values.
Synchronize	Tells the Liebert® SiteScan™ application to wait for the external program to finish running before initiating the next *Run External Program* alarm action.
Perform Action	By default, the Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under Perform Action, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under PerformAction, select *If schedule group <your new group> is Unoccupied.*

Send Alphanumeric Page

The Send Alphanumeric Page alarm action sends a page to one or more alphanumeric pagers or sends text messages to cell phones. The pager or phone must be able to accept e-mail.

Table 3.19 Send Alphanumeric Page Alarm Action Options

Field	Notes
To	Enter the email address to which the alarm should be sent. To enter multiple addresses, type a space or press *Enter* after each address.
From	Enter a valid address if required by your mailserver.
Mail Host	Address of the mailserver. This can be an IP address or a system name, such as mail.mycompany.com.
Mail Host Port	Change this field if using a port other than the default port 25.
Mail Host Security Options	Select the type of security the mailserver uses. • Cleartext – Uses the SMTP protocol to send as clear text over TCP/IP. • Secure SSL – Uses SSL, a communication protocol that provides data encryption. • Secure TLS – Uses TLS, but does not begin encryption until the Liebert® SiteScan™ application issues STARTTLS command.

Table 3.19 Send Alphanumeric Page Alarm Action Options (continued)

Field	Notes
Specify Mail User For Mail Host Authentication	Select if your mailserver requires a username and password.
Send mail as MIME attachment	Select if your mailserver allows only MIME attachments.
Message Text	Use punctuation, spaces, or returns to format the text. To add live data to the text, select field codes (See Using Field Codes on page 62) from the Append Field Code list.
Perform Action	By default, the Vertiv™ Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under Perform Action, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under Perform Action, select *If schedule group <your new group> is Unoccupied.*

NOTE: This alarm action should not be assigned to frequently occurring alarms since it may cause problems on your network or the Internet.

Securing Mailserver Communication using SSL or TLS

Liebert® SiteScan™ application requests an SSL certificate from the mailserver, before the it sends an email using SSL or TLS. If the certificate that the Liebert® SiteScan™ application receives is in its list of trusted certificates, it sends the email. If the certificate is not in the list, the Liebert® SiteScan™ application generates a system alarm indicating that the email alarm action failed. If this occurs, you will need to add the certificate of mailserver to the Liebert® SiteScan™ list of trusted certificates of.the Liebert® SiteScan™ application..

1. Get a copy of the certificate file from the mailserver. Ask your Network Administrator for help.
2. Put the file on the Liebert® SiteScan™ server.
3. On the Liebert® SiteScan™ server, click the Windows Start button.
4. In the Search programs and files field, type the following command:

   ```
   C:\SiteScan_Web_<x.x>\bin\java\jre\bin\keytool.exe -import -trustcacerts -alias smtpserver -keystore webserver\keystores\certkeys -file <file_path>
   ```

   replacing:

   <x.x> with the version number of the system
   <file_path> with the full path and file name of the certificate file

5. The information for the smtpserver key is displayed and you are prompted to trust this certificate. Type *yes*.

NOTE: If your mailserver is using SSL or TLS, the Vertiv™ Liebert® SiteScan™ server is running antivirus software, and the email alarm action fails because an SSL certificate cannot be found, try one of the following solutions:

Disable scanning of outgoing SMTP traffic in the antivirus software. For more information, consult the Help section of your antivirus software.

Obtain the SSL certificate for the antivirus software and install it on the Liebert® SiteScan™ server using the above procedure.

Setting up a Dial up Networking Connection

The Liebert® SiteScan™ application can use a dial up internet connection through a modem to deliver e-mail for the Send *E-mail* or *Send Alphanumeric Page alarm action*.

To set up the dial up connection follow the below steps:

1. Set up your modem to dial out to your Internet Service Provider. See your modem documentation.
2. On the *Liebert® SiteScan™* server, open Internet Explorer.
3. Select *Tools* or ⚙ > *Internet Options*.
4. On the Connections tab, click *Setup*.
5. Follow the instructions in the wizard. See Windows Help for assistance.
6. In a text editor such as Windows Notepad, open *SiteScan_Web_x.x\webroot\<system>\ system.properties*.
7. At the end of the file, type the following line:

   ```
   repactions.connection.name=<name of connection>
   ```

   where <name of connection> is the ISP name you entered in the wizard in step 2.
8. Open Internet Explorer, then select *Tools* > *Internet Options* > *Connections* tab.
9. If the box under *Dial up and Virtual Private Network settings* shows more than one connection, select the connection that you just created, then click *Set Default*.
10. Select *Always dial my default connection*.

Send E-mail

The Send E-mail alarm action sends a message to one or more e-mail accounts. The alarm action can also run a report and attach it to the e-mail as a PDF, HTML, or XLS file.

Table 3.20 Send E-mail Alarm Action Options

Field	Notes
To and CC	Type the mail addresses to which you want to send the alarm. To enter multiple addresses, type a space or press *Enter* after each address.
Subject	*Enter* the text that you want to appear on the Subject line of the email. The subject can include field codes (See Using Field Codes on page 62).
Use default email server configuration	Check this field to have this alarm action use the email server configuration settings defined on the *System Settings > General* tab. Uncheck to enter settings specific to this alarm action.
From	Enter a valid address if required by your mailserver.
Mail Host	Address of the mailserver. This can be an IP address or a system name, such as mail.mycompany.com.
Mail Host Port	Change this field if using a port other than the default port 25.
Mail Host Security Options	Select the type of security the mailserver uses. • Cleartext (SMTP) – Uses the SMTP protocol to send as clear text over TCP/IP.

Table 3.20 Send E-mail Alarm Action Options (continued)

Field	Notes
	• **Secure SSL (SMTP with SSL)** – Uses SSL, a communication protocol that provides data encryption. • **Secure TLS (STARTTLS)** – Uses TLS, but does not begin encryption until the Liebert® SiteScan™ application issues STARTTLS command.
Specify Mail User For Mail Host Authentication	Select if your mailserver requires a username and password.
Send mail as MIME attachment	Select if your mailserver allows only MIME attachments.
Message Text	Use punctuation, spaces, or returns to format the text. To add live data to the text, select field codes (See Using Field Codes on page 62) from the Append Field Code list.
Attach Report	Select to attach a report to the e-mail, then select the *Report* and the *Format*. The attached report will include the date and time. For example, Alarm Sources 2017 Jan 01 1230. **NOTE: The Report Name field shows a custom report only if it is accessible at the current level.** *Run as* shows the name and login name of the operator creating the alarm action. The report will be run using the privileges and report options of this operator. **NOTE: For this purpose, you might want to create a new operator with limited privileges.**
Perform Action	By default, the Vertiv™ Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under Perform Action, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under Perform Action, select *If schedule group <your new group> is Unoccupied.*

NOTE: This alarm action should not be assigned to frequently occurring alarms since it may cause network or Internet problems.

Securing Mailserver Communication using SSL or TLS

Before the Vertiv™ Liebert® SiteScan™ application sends an email using SSL or TLS, it requests an SSL certificate from the mailserver. If the certificate that the Liebert® SiteScan™ application receives is in its list of trusted certificates, it sends the email. If the certificate is not in the list, the Liebert® SiteScan™ application generates a system alarm indicating that the email alarm action failed. If this occurs, you will need to add the certificate of the mailserver to the list of trusted certificates of the Liebert® SiteScan™ application..

1. Get a copy of the certificate file from the mailserver. Ask your Network Administrator for help.
2. Put the file on the Liebert® SiteScan™ server.
3. On the Liebert® SiteScan™ server, click the Windows *Start* button.
4. In the Search programs and files field, type the following command:

```
C:\SiteScan_Web_<x.x>\bin\java\jre\bin\keytool.exe -import -trustcacerts -alias smtpserver -keystore
webserver\keystores\certkeys -file <file_path>
```

replacing:

<x.x> with the system's version number
<file_path> with the full path and file name of the certificate file

5. The information for the smtpserver key is displayed and you are prompted to trust this certificate. Type *yes*.

NOTE: If your mailserver is using SSL or TLS, the Liebert® SiteScan™ server is running antivirus software, and the email alarm action fails because an SSL certificate cannot be found, try one of the following solutions:

Disable scanning of outgoing SMTP traffic in the antivirus software. For more information, consult the Help section of your antivirus software.

Obtain the SSL certificate for the antivirus software and install it on the Liebert® SiteScan™ server using the above procedure.

Setting up a Dial up Networking Connection

The Liebert® SiteScan™ application can use a dial up internet connection through a modem to deliver e-mail for the Send E-mail or Send Alphanumeric Page alarm action.

To set up a dial up networking connection, follow the below steps:

1. Set up your modem to dial out to your Internet Service Provider. See your modem documentation.
2. On the Liebert® SiteScan™ server, open *Internet Explorer*.
3. Select *Tools* or ⚙ > *Internet Options*.
4. On the *Connections* tab, click *Setup*.
5. Follow the instructions in the wizard. See Windows Help for assistance.
6. In a text editor such as Windows Notepad, open *SiteScan_Web_x.x\webroot\<system>\ system.properties*.
7. At the end of the file, type the following line:

   ```
   repactions.connection.name=<name of connection>
   ```

   where <name of connection> is the ISP name you entered in the wizard in step 2.

8. Open Internet Explorer, then select *Tools* > *Internet Options* > *Connections* tab.
9. If the box under *Dial up and Virtual Private Network settings* shows more than one connection, select the connection that you just created, then click *Set Default*.
10. Select *Always dial my default connection*.

Send SNMP Trap

The Send SNMP Trap alarm action sends an SNMP trap in response to receive an alarm. Traps contain the text created in the Text to send as the SNMP Trap field in the alarm action dialog box. You can configure up to five SNMP servers to receive traps.

NOTE: Liebert® SiteScan™ supports SNMP v1.

Each SNMP server you want to receive these traps must have SNMP monitoring equipment installed. If problems arise with your SNMP connection or receiving traps, contact your IS department.

This alarm action uses Port 162 to send SNMP traps. To use a different port, open *SiteScanx.x\webroot\<system_name>\system.properties* in a text editor such as Notepad. In the line *#snmp.trap.port = 162*, delete # at the beginning of the line and change 162 to the port you want to use. If you make this change while the Liebert® SiteScan™ Server application is running, you must restart it to have the change take effect.

Table 3.21 Send SNMP Trap Alarm Action Options

Field	Notes
Network Address*	The network address of the SNMP server receiving the SNMP trap.
Community Name*	The community name to which the SNMP server belongs.
Comment	The physical location of the SNMP server. This field is optional.
Trap number*	If the network administrator has configured trap numbers, type a unique number from 1 to 127. **NOTE: The same trap number is used for all messages from this alarm action.**
Text to send as the SNMP Trap	255 character limit. Type punctuation, spaces, or returns after the entries to format the message. You can customize this text by selecting field codes (See Using Field Codes on page 62) from the Append Field Code list.
Perform Action	By default, the Vertiv™ Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under Perform Action, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under PerformAction, select *If schedule group <your new group> is Unoccupied.*
* Ask your network administrator for this information.	

Send Web Service Request

The Web Service Request alarm action sends a web service request to a third-party server when an alarm event occurs. For example, the Vertiv™ Liebert® SiteScan™ application could send a request to a work order system so it could create a work order for someone to respond to the alarm condition.

Table 3.22 Web Service Request Alarm Action Options

Field	Notes
Destination Address	The URL of the server that will receive the request. Example: https://192.168.168.102/workorder/bas
Web Service Action	Select the type of web service request required by the target server: GET or POST
Content Type	If you selected POST in the previous field, select the format required by the target server: Application/json or /x-www-form-urlencoded

Table 3.22 Web Service Request Alarm Action Options (continued)

Field	Notes
Web Service Request Parameters	Optional– Create a parameter for each piece of information that the target server requires. You should be able to find information about required parameters in the documentation for target server..
Parameter Name	Enter a *name* for the parameter. For example, Parm1 or Date. Click *Add Parameter*.
Value	Text required for the parameter. To add live data to the request, select a field code (See Using Field Codes on page 62) from the *Append Field* list.
Perform Action	By default, the Vertiv™ Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under Perform Action, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: - Create a schedule group, but do not assign members to it. - Create a schedule for the group. Set the occupied hours to be the same as the work hours. - Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied*. - Create the alarm action that is to be performed after work hours. Under Perform Action, select *If schedule group <your new group> is Unoccupied*.

Write Property

The Write Property alarm action writes a specified value to a BACnet property. You typically set up 2 alarm actions, the first writes a value when the alarm occurs and the other writes a value when the return to normal occurs.

Table 3.23 Write Property Alarm Action Options

Field	Notes
Expression	Enter the path to the target property. To get the path, right click the property on a Properties page, then select Global Modify. The Geographic Location field in the Advanced section shows the path. Click to copy it. **NOTE: The present value of a BACnet parameter microblock cannot be written to directly. However, you can change the present value by writing to the relinquish_default property, or to the priority_array/priority16 property.** **For example, change *#rtu-1/vfd_ovrde/present_value* to *#rtu-1/vfd_ovrde/relinquish_default*, or *#rtu-1/vfd_ovrde/priority_array/priority16*.** **Do not use a BACnet address in this field.**
Value to Write	Type the value you want to write to the microblock property. Type 0 or 1 for a binary property.
Append field code to value	Select field codes (See Using Field Codes on page 62) to add this information to the Value to Write field.
Perform Action	By default, the Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under Perform Action, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation.

Table 3.23 Write Property Alarm Action Options (continued)

Field	Notes
	3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under Perform Action, select *If schedule group <your new group> is Unoccupied.*

Write to Database

The Write to Database alarm action stores alarm information in the tabular form in the Vertiv™ Liebert® SiteScan™ alarm database or in a custom database. Third party applications can access the alarm information for building maintenance management or alarm analysis. For example, an application can perform actions such as triggering a stored procedure or running a report.

Writing to the Liebert® SiteScan™ Alarm Database

By default the Liebert® SiteScan™ application writes alarm information to the write_db_ra table in the Liebert® SiteScan™ alarm database when you add the *Write to Database* alarm action. The information written to the database is described in the Table 3.24 below , along with the column name and data type you will need to access the alarm data from a third-party application.

Table 3.24 Database Information

Description	Column Name	Data type
Alarm generation time	EVENT_TIME_	Datestamp
Path to the alarm source Example: #slm/m073	SOURCE_PATH_	String
Display name path to the alarm source Example: Atlanta Office/R&D Facility/Second Floor/VAV 2-1/Zone Temp	DISPLAY_NAME_	String
Alarm state Example: OFF NORMAL, LOW LIMIT, HIGH LIMIT	EVENT_STATE_	String
Alarm text as defined in the Text to write to the database field on the alarm action page. You can add live data to the text by selecting field codes (See Using Field Codes on page 62) from the Append Field Code list.	RA_TEXT_	String

Table 3.25 Write to Database Alarm Action Options

Field	Notes
Perform Action	By default, the Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under Perform Action, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under PerformAction, select *If schedule group <your new group> is Unoccupied.*

NOTE: Use a third party database application to delete old entries to keep the database table from becoming too large. The Vertiv™ Liebert® SiteScan™ interface does not allow you to view, edit, or delete entries.

If your system uses an Access or Derby database, you cannot open the database in a third party application while the Liebert® SiteScan™ or SiteBuilder application is running.

Writing to a Custom Database

The Vertiv™ Liebert® SiteScan™ application can write alarm information to the following types of custom databases. The custom database does not have to be the same type as the Liebert® SiteScan™ database.

- SQL Server
- MySQL
- PostgreSQL
- Oracle

You may create a table in an existing third party database or create a new database.

Using your database management tool, create a table in your custom database that includes fields for each alarm field code to be written to the table. Each field length in the table should be as long as the longest value to be written to that field.

To set up writing to a custom database instead of the Liebert® SiteScan™ alarm database, select the *Specify Custom Database* checkbox on the Alarms page Actions tab, then enter information in the remaining fields. See Table 3.26 on the facing page .

Table 3.26 Write to Custom Database Alarm Action Options

Field	Notes	
Text to write to the database	The text is made up of field codes (See Using Field Codes on page 62) that add live data to the text. You can select additional field codes from the *Append Field Code* list. **NOTE: To write the text in this field to the custom database, you must include the Report Text field code ($report_text$) in the *Database Insert String* field described below.**	
Database Connect String	Database Type • SQL Server • MySQL • PostgreSQL • Oracle	Connect String Format • jdbc:odbc:<odbc_alias> • jdbc:mysql://<host>:<port>/<instance> • jdbc:postgresql://<host>:<port>/<instance> • jdbc:oracle:thin@<host>:<port>/<instance> where: • <host> is the database server name/IP address • <port> is the port number for the database • <instance> is the database name in the database server • <odbc_ alias> is the name of the ODBC data source
Database Login and Password	The login and password to connect to the database.	
Database Insert String	Use the following format: Insert into <TABLE_NAME> (<column1_name>, <column2_name> ...) values (<$field_code1$>, <$field_code2$>, ...) Example: Insert into SiteScan_ALARMS (TIME_, LOCATION_, TO_STATE_, TEXT_) values ($generation_time$, $location_path$, to_state, $report_text$) **NOTE: You can add field codes (See Using Field Codes on page 62) to the Insert String using the Append Field Code list.** **If you add a timestamp type field code (for example, $generation_time$), you should have the data go into a timestamp data type field in the custom database. Otherwise, you must use field code formatting (See Using Field Codes on page 62) to format the time.**	
Perform Action	By default, the Vertiv™ Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under Perform Action, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under Perform Action, select *If schedule group <your new group> is Unoccupied.*	

Write to File

The Write to File alarm action can do either of the following:

- Record alarm information in a standard ASCII text file that you can view and edit using a text editor such as Windows Notepad.
- Write a report to a file.

Table 3.27 Write to File Alarm Action Options

Field	Notes
File Name	Path name for the file you want to write to such as: c:\SiteScanx.x\webroot\alarms.txt. • If you do not specify a path, the file is written to the system folder. • If you type a path that does not exist, the Vertiv™ Liebert® SiteScan™ application will create the necessary folders. • You can write to one of the following: • a file on the server • a networked computer if you map the network drive. Use the drive mapping in the path from the server to the computer. • The path name may contain field codes (See Using Field Codes on page 62).
Write alarm data	Select to record alarm information in a text file. Select *Append* to add new alarm information to the end of the file instead of writing over existing data. **NOTE: Because you can append new alarm information to the end of the file, this file can become very large. The file size can become very large as you can append new alarm information to the end of the file.** In the field *Text to write to the file*, enter the information you want to record for an alarm. Use punctuation, spaces, or returns to format the text. To add live data to the text, select field codes (See Using Field Codes on page 62) from the Append Field Code list.
Write a Report	Select to write a report to a file, then select the *Report* and the *Format*. **NOTE: The Report Name field shows a custom report only if it is accessible at the current level.** Run as shows the name and login name of the operator creating the alarm action. The report will be run using the privileges and report options of this operator. **NOTE: For this purpose, you might want to create a new operator with limited privileges.**
Perform Action	By default, the Liebert® SiteScan™ application performs an alarm action when the alarm source generates an alarm and when it returns to normal. Under Perform Action, you can choose to run the alarm action: 1. Only when the alarm source generates an alarm or when it returns to normal. 2. After a specified amount of time if the alarm has not been acknowledged or has not returned to normal. Use this option for alarm escalation. 3. If the alarm occurs during the occupied hours defined for a schedule group or run if the alarm occurs during the unoccupied hours defined for a schedule group. Example: To have one alarm action performed during work hours and a different alarm action performed after work hours: • Create a schedule group, but do not assign members to it. • Create a schedule for the group. Set the occupied hours to be the same as the work hours. • Create the alarm action that is to be performed during work hours. Under Perform Action, select *If schedule group <your new group> is Occupied.* • Create the alarm action that is to be performed after work hours. Under Perform Action, select *If schedule group <your new group> is Unoccupied.*

3.4.4 Setting Up an Alarm Source in the Liebert® SiteScan™ Interface

The application engineer usually sets up alarm sources in the EIKON application. In the Liebert® SiteScan™ application, you can:

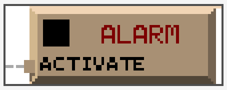
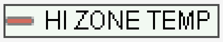
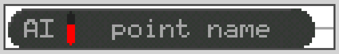
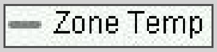
- Edit settings of an existing alarm source or set up a new alarm source to generate alarms.
- On the *Alarm Sources* tab in the *Properties* page of the equipment, set up all alarms for a piece of equipment at once.
- Simulate an alarm to test its setup.

Two types of microblocks generate alarms in control programs.

- Alarm microblocks include logic that considers conditions such as space occupancy.
- I/O point microblocks can generate an alarm when the present value exceeds defined limits (analog) or when the present value changes to an off normal state (binary). This type of microblock is typically set up for analog points to generate alarms for sensor failure.

Alarm microblocks and I/O microblocks can have similar names. So, when you are going to enable an alarm source, first look for an alarm microblock on the Geographic or Network tree.

Table 3.28 Microblock Appearance on Geographic and Network Tree

Microblock Type	Appearance on the Geographic or Network Tree
 ALARM ACTIVATE	 HI ZONE TEMP
 AI point name	 Zone Temp

Setting Up, Editting, or Disabling Alarm Sources

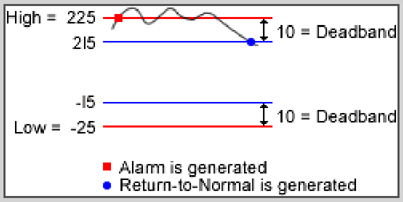
To set up, edit, or disable a single alarm source, follow the below steps:

NOTE: On the Geographic or Network tree, select the alarm source (microblock).

1. Click *Alarms*, then select the *Enable/Disable* tab.
2. Make changes to the fields as needed. The fields can vary for different types of alarm sources. See table below.
3. Click *Accept*.

NOTE: To set up all the alarms for a piece of equipment at once, click *Properties*, then select *Alarm Sources*.

Table 3.29 [caption]

Field	Notes
Potential alarm source	Check to enable the alarm source to generate alarms. Uncheck to disable the alarm source.
Alarm	Check to have the alarm source generate an alarm when the specified conditions occur. - For a binary input, enter the conditions for generating an alarm. - For an analog input, type the low and high limits that, when exceeded, will generate an alarm. **Deadband -** The amount inside the normal range by which an alarm condition must return before a return to normal notification is generated. Example:  High = 225 215 10 = Deadband -15 Low = -25 10 = Deadband Alarm is generated Return-to-Normal is generated **NOTE: If Status is checked, the alarm condition currently exists.**
Return to Normal	Check to have the alarm source generate a return to normal when the alarm condition returns to a normal state.
Alarm requires acknowledgment	Check to have the Vertiv™ Liebert® SiteScan™ application require that an operator acknowledge the alarm.
Return requires acknowledgment	Check to have the Liebert® SiteScan™ application require that an operator acknowledge the return to normal.
Classified as critical	This property determines the color of the system wide alarm button when the alarm comes in. ⚠ - Critical ⚠ - Non critical
Event State	The current state of the alarm source can be: - **Normal**—The value is normal. - **Off Normal**—The value is not normal (binary only). - **Fault**—The alarm source microblock may be misconfigured. - **High Limit**—The value exceeds the normal range (analog only). - **Low Limit**—The value is below the normal range (analog only).
BACnet Configuration:	
Dial on alarm	Check to have this alarm immediately delivered through a modem connection. **NOTE: When monitoring your system through a modem connection, non-critical alarms are stored in the gateway until one of the following happens:** - A critical alarm occurs. - The gateway is contacted by the Liebert® SiteScan™ application. - The gateway buffer is full, at which time all alarms are sent to the Liebert® SiteScan™ application.
Notification Class	Do not change this field.

To set up, edit, or disable multiple alarm sources simultaneously, follow the below steps:

1. On the Geographic or Network tree, select the area, equipment, or controller containing the alarm sources.
2. Click *Alarms*, then select the *Enable/Disable* tab.
3. In Step 1 , select the categories that contain the alarm sources.

NOTE: In Step 1 and Step 2 , *Ctrl+click*, *Shift+click*, or both to select multiple items, or check *Select All*.

4. In Step 2 , select the alarm sources.
5. Make appropriate changes in Step 3 .
6. Click *Accept*.

NOTE: Click *View Selected Sources* to view or change settings for each alarm.

Simulating an Alarm

To test the setup of an alarm source and its alarm actions (Setting up Alarm Actions on page 38), you can simulate an alarm or its return to normal.

1. On the Geographic tree, select the alarm source (▭, but not ▭) whose alarm you want to simulate.
2. On the *Alarms* > *Enable/Disable* tab, check *Enable* next to Alarm or Return to Normal.
3. Click *Simulate* next to Alarm or Return to Normal.
4. Select the equipment on the tree, then select the *View* tab to see the alarm.

Viewing all Instances of an Alarm Source

To find all instances of an alarm source at and below a selected area:

1. On the Geographic or Network tree, select an *area*.
2. Select the *Message*, *Actions*, *Enable/Disable*, or *Category* tab.
3. Select an *alarm source* from the list in step 2.
4. Click *View Selected Sources*.

Each path in the dialog box links to the alarm source microblock.

NOTE: It is possible to change the settings that relate to the tab you selected.

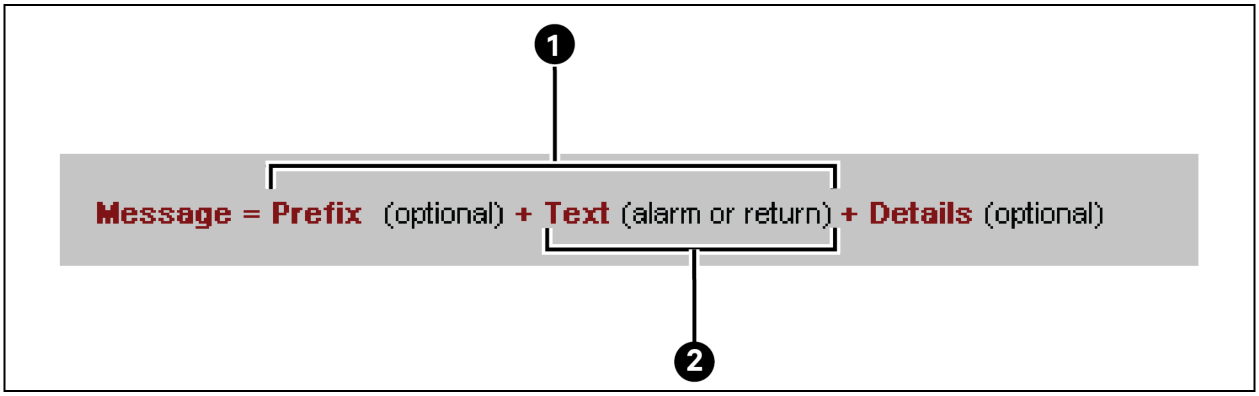
3.4.5 Customizing Alarms

Each alarm source has an alarm message, category, and template defined in the EIKON application. You can change messages and categories in the Vertiv™ Liebert® SiteScan™ application.

Alarm Messages

An alarm message is the information that appears on the Alarms page *View* tab for an alarm. An alarm message can consist of 3 parts.

Figure 3.19 Alarm Message


1
Message = Prefix (optional) + Text (alarm or return) + Details (optional)
2

Item	Description
1	Prefix and Text make up the alarm message you see without double clicking the alarm
2	Text defined in the control program

You can edit Text only at the alarm source in the EIKON application.

Prefix and Details are hierarchical. They apply at the location where they are added and to all its children. For example, you could enter Details at the system level to show the acknowledge time for alarms in the HVAC Critical category. The acknowledge time would then be in any HVAC critical alarm message in the system.

NOTE: An alarm action can have a different message from the alarm message seen on the View tab. To edit the message for a particular alarm action, see Setting up alarm actions (See Setting up Alarm Actions on page 38).

To edit the message for an alarm source, follow the below steps:

1. On the Geographic tree, select the alarm source (microblock).
2. Click *Alarms*, then select the *Messages* tab.

NOTE: Sample Alarm Message and Sample Return Message show the messages as they are currently defined.

3. Do the following as needed:
   - Edit the *Text* for *Alarm* or *Return*. You can add live data to the text by selecting field codes (Using Field Codes on page 62) from the *Append Field Code* list.
   - Click the *Edit* button to edit *Message Prefix* or *Message Details*.
   - In the drop down list to the right of Message formation, select *Add new prefix to beginning of message* or *Add new details to end of message*, then click *Add*.
4. Click *Accept*.

To add a Prefix or Details for multiple alarm sources, follow the below steps:

1. On the Geographic or Network tree, select the area, equipment, or controller containing the alarm sources.
2. Click *Alarms*, then select the *Messages* tab.
3. In Step 1 , select the categories that contain the alarm sources whose messages you want to edit.

NOTE: In Step 1 and Step 2 , *Ctrl+click*, *Shift+click*, or both to select multiple items, or check *Select All*.

4. In Step 2 , select the alarm sources.
5. In Step 3 , select *Add new prefix to beginning of message* or *Add new details to end of message*.
6. Click *Add*.
7. Type text and add field codes as needed.
8. Click *Accept*.

Alarm Categories

Alarm categories sort related alarm sources and their alarms into groups such as HVAC Critical and Access Control General. Alarm categories allows you to do the following:

- View, acknowledge, or delete selected categories of alarms (See Viewing, Troubleshooting, Acknowledging, and Deleting Alarms on page 31) received by the Vertiv™ Liebert® SiteScan™ application.
- Assign alarm actions (See Setting up Alarm Actions on page 38) to selected categories of alarm sources.
- Set up alarm sources (See Setting Up an Alarm Source in the Liebert® SiteScan™ Interface on page 54) in selected categories.

Each alarm source is assigned to an alarm category in either the EIKON application or in the Liebert® SiteScan™ interface. See "To use custom alarm and schedule categories" in EIKON Help.

In addition to the default alarm categories in your system, you can create custom categories if needed. If you create a custom category in the EIKON application, you must create the same category in the Liebert® SiteScan™ interface. The Reference Name must be identical in both applications.

To assign alarm sources to a category in the Liebert® SiteScan™ interface, follow the below steps:

1. On the Geographic 🌐 or Network 🖧 tree, select the area, equipment, or controller containing the alarm sources.
2. Click *Alarms*, then select the *Category* tab.
3. In step 1, select the category that currently contains the alarm sources.

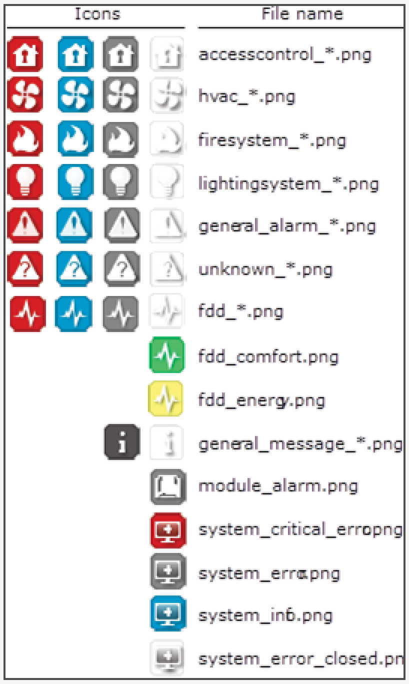
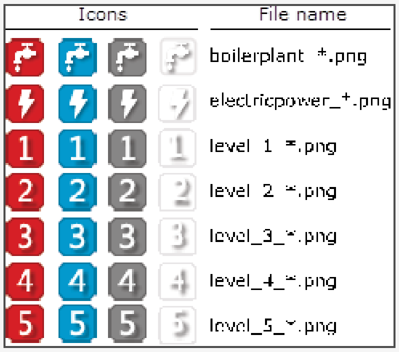
NOTE: In step 1 and step 2, *Ctrl+click*, *Shift+click*, or both to select multiple items, or check *Select All*.

4. In step 2, select the alarm sources whose category you want to change.
5. In step 3, select a category from the drop-down list, then click *Change*.
6. Click *Accept*.

To add a custom alarm category , follow the below steps:

1. On the System Configuration ⚙ tree, click ▷ to the left of *Categories*.
2. Click *Alarm*.
3. Click *Add*. See table below.
4. Click *Accept*.

Table 3.30

Field	Notes
Reference Name	It must be unique in the database, lowercase, and not contain any spaces. This name must be identical to the name of the custom alarm category that you added in the EIKON application.
Icon	Type */_common/lvl5/graphics/event_categories/<file_name>.gif*, replacing *<file_name>* with the name of the icon file you want to use. The event_categories folder contains the following alarm icons:
	Icons used in the SiteScan interface:  Icons available for custom categories: 
* Represents critical, maintenance, general, or closed You can create your own 24 x 24 pixel icon (.gif or .png) and store it in the event_categories folder. However, your custom file will not be transferred during a Vertiv™ Liebert® SiteScan™ upgrade, so you will need to copy the file to the new install directory after the upgrade.	

Icons used in the SiteScan interface:

Icons	File name
	accesscontrol_*.png
	hvac_*.png
	firesystem_*.png
	lightingsystem_*.png
	general_alarm_*.png
	unknown_*.png
	fdd_*.png
	fdd_comfort.png
	fdd_energy.png
	general_message_*.png
	module_alarm.png
	system_critical_erropng
	system_erro.png
	system_inb.png
	system_error_closed.pn

Icons available for custom categories:

Icons	File name
	boilerplant *.png
	electricpower_*.png
	level 1 *.png
	level 2 *.png
	level_3_*.png
	level_4_*.png
	level_5_*.png

If You Upgraded Alarms from v2.0 or Earlier

All v2.5 and later alarms use one template called Universal. This template lets you define your alarm message text, the critical setting, and the required acknowledgments at the alarm source in the EIKON or Vertiv™ Liebert® SiteScan™ application.

Templates in Upgraded Systems

If you upgraded your system from v2.0 or earlier, the alarm sources retained their existing templates and existing alarm settings. If the existing alarm sources contain little or no customization to the alarm settings, Vertiv recommends that you change all of the alarms to use the Universal template. If the alarm sources had customized alarm settings, continue using the existing templates.

To assign a different template to alarm sources, follow the below steps:

Prerequisite: The Alarms Template tab must be visible. If it is not, on the System Configuration ⚙ tree, select *Privilege Sets*, then check *Maintain Alarm Templates*.

1. On the Geographic 🌐 tree, select the piece of equipment containing the alarm sources to be changed.
2. Click *Alarms*, then select the *Template* tab.
3. Follow the 3 steps on the screen.

NOTE: Use *Ctrl+click*, *Shift+click*, or both to select multiple items.

4. Click *Change*.
5. Click *Accept*.

NOTE: To change all alarms in the system simultaneously, go to the system level and then select all categories and all alarm sources on the Templates tab.

Adding an Alarm Template

1. On the System Configuration ⚙ tree, select *Alarm Templates*.
2. Click *Add*.
3. Select *Source based* (a v2.5 template) or *Stand alone* (a pre-v2.5 template), then click *OK*.
4. Edit the template fields as needed. See table below.
5. Click *Accept*.

Table 3.31 Adding an Alarm Template

Field	Template Type	Notes
Reference Name	All	It must be unique in the database, be lowercase, and not contain any spaces. This name must be identical to the name of the template in the EIKON application.
Display Name	All	The name that will appear in the Vertiv™ Liebert® SiteScan™ interface for this template.
Alarm Message	Source based	The message text displayed on the *View* tab or in the alarm action when an Alarm requires acknowledgment.
Return Message	Source based	The message text displayed on the *View* tab or in the alarm action when a return to normal requires acknowledgment.
Fault Message	Source based	The message text displayed on the *View* tab or in the alarm action when a Fault requires acknowledgment.
Critical	Stand alone	Select if this is a template you will use with a critical alarm.
Acknowledgement Required	Stand alone	Select which alarm states require an acknowledgment.

Table 3.31 Adding an Alarm Template (continued)

Field	Template Type	Notes
Out of Range	Stand alone	Analog inputs and outputs that have low and high limit alarm properties. Click ▷ to the left of *Out of Range* to make changes to the alarm messages displayed on the *Alarms page > View* tab. Short text is the message displayed when the alarm is not expanded. Long text is the message displayed when the alarm is double clicked and expanded.
Change of State	Stand alone	Binary inputs and alarm microblocks. See *Out of Range* above to change the alarm messages.
Copy Field Code to Clipboard	Stand alone	To add a field code to any of the message text fields: 1. Select a field code to copy it. 2. Click in the appropriate text field where you want the field code. 3. Press *Ctrl+V* to paste the field code.

3.4.6 Using Field Codes

Use field codes to insert live data into:

- The message on an alarm action
- Text displayed on the *Alarms page > View* tab
- Alarm information archived to a text file when an alarm is deleted

By appending field codes to each of these items, you can customize their setup. For example, to have the device that generated the alarm included in the message of an alarm action, append the Device field code to the message of the action.

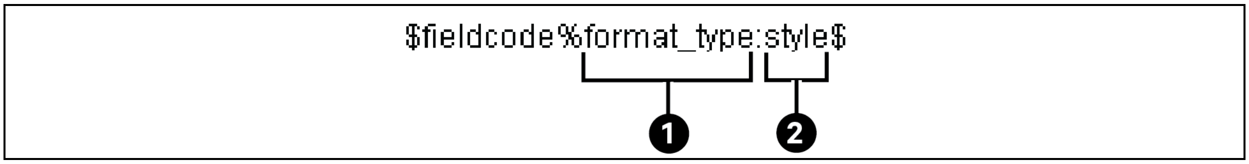
Formatting Field Codes

You can type a formatting command after a field code to format the field code in one of the following 3 ways:

- Format a number field code (Example: ##.##).
- Format a date/time field code (Example: MM/dd/yyyy hh:mm:ss).
- Left, right, or center align a field code and set the field width.

A formatting command must have the following syntax:

Figure 3.20 Syntax for Formatting Command



Item	Description
1	Format type
2	Style

See the **Table 3.32** on the facing page to determine the format_type and style for a formatting command.

Table 3.32 Format Type and Style for a Formatting Command

Formatting Command	Format Type	Style	Example
To format a number	N	The actual formatting, such as ##.##. The basic format uses the pound sign (#) to represent a number. For more information, search the Internet for "customizing number formats with java".	To always round a setpoint value to two digits to the right of the decimal, the field code is: *$setpoint_value%N:##.##$* For example, 78.9935 becomes 78.99.
To format date/time	D	The actual formatting, such as MM/dd/yyyy hh:mm:ss. For more information, search the Internet for "customizing date time formats with java".	To show the date and time when an alarm is generated in a format like 03/15/2004 10:50:43, the field code is: *$generation_time%D:MM/dd/yyyy hh:mm:ss$*
To set alignment and field width	L for left align R for right align C for center align	Indicate the field width by number of characters.	To left align the name of the device that generated the alarm and set the field width to 15 characters, the field code is: *$device%L:15$*

Using Multiple Formatting Commands

You can type multiple formatting commands for a field code. For example, you can format a number and then set the alignment and field width. The syntax for multiple formatting commands is: *$fieldcode%format_type1:style%format_type2:style$*

Example: To format the alarm date and time, center it and set the field at 20 characters, the field code is: *$generation_time%D:MM/dd/yyyy hh:mm:ss%C:20$*

NOTE: The date/time or number formatting command must be entered before the alignment/field width command.

Field Codes

Table 3.33 Field Codes Description

Field Code Name	Field Code	Description
Acknowledge Operator	$acknowledge_operator$	The operator who acknowledged the alarm. Example: John Doe
Acknowledge Time	$acknowledge_time$	The time when the operator acknowledged the alarm. Example: Nov 12, 2012 6:46:31 PM
Alarm Category	$alarm_category$	The alarm category to which the alarm is assigned.. Example: HVAC Critical
Alarm Priority	$alarm_priority$	The priority number associated with the priority of the alarm (Off-Normal, Fault, or Normal) on the controller's *Driver > Notification Class* page.
Alarm Template	$alarm_template$	The alarm template that the alarm is assigned to.Example: Universal
Alarm Type	$alarm_type$	The alarm type of the alarm source. Example: CHANGE OF STATE
Alert Text	$alerttext$	For a converted SuperVision system if the option Create a single alarm template... was selected during upgrade. Retrieves alarm message text from cmnet_alert_text.properties. To use this field code: 1. Select the Alert Text field code. 2. After $alerttext, type one of the following: • :normalshort • :normallong • :alarmshort

Table 3.33 Field Codes Description (continued)

Field Code Name	Field Code	Description
		- :alarmlong For example, $alerttext:alarmlong$
Character	c	A single ASCII character. Often used for form feeds and other printer escape sequences. Example: $C:65$ displays A
Command Value	$command_value$	The commanded value from the alarm source. Valid only for alarm type COMMAND FAILURE. Example: 3
Control Program	$equipment$	The display name of the equipment where the alarm came from. Example: Chiller
Controller	$device$	The display name of the device where the alarm came from. Example: SE6104
Dead Band	$deadband$	The deadband value from the alarm source. Valid only for alarm type OUT-OF-RANGE. EXAMPLE 5
Deletion Operator	$deletion_operator$	The operator who deleted the alarm.Example: John Doe
Deletion Time	$deletion_time$	The time the alarm was deleted.Example: Nov 12, 2012 6:46:31 PM
Error Limit	$error_limit$	The error limit, from the alarm source. Valid only for alarm type FLOATING LIMIT. Example: 90
Event Values	$event_values$	Returns a string of alarm values associated with the alarm.
Exceeded Limit	$exceeded_limit$	The exceeded limit value from the alarm source. Valid only for alarm type OUT-OF-RANGE. Example: 90
Exceeding Value	$exceeding_value$	The exceeding value from the alarm source. Valid only for alarm type OUT-OF-RANGE. Example: 91
Fault	$fault$	The status of the fault condition from the alarm source. Example: True or false
Field Message	$field_message$	Text generated in the alarm by the controller.
Feedback Value	$feedback_value$	The feedback value from the alarm source. Valid only for alarm type COMMAND FAILURE. EXAMPLE 10
From State	$from_state$	The previous state of the alarm source. Example: NORMAL, FAULT, OFF NORMAL, HIGH LIMIT, LOW LIMIT
Generation Operator	$generation_operator$	The operator who forced the alarm to return to normal. Example: John Doe
Generation Time	$generation_time$	The time in the controller when the alarm was generated. Example: Nov 12, 2012 6:35:18 PM
In Alarm	in_alarm	The In Alarm status from the alarm source. Example: True or false
Incident Closed Time	$incident_closed_time$	The time the entire incident group closed of the alarm. Example: Nov 12, 2012 6:46:31 PM
Latched Data Value (Analog)	$latched_data_analog:x$	"x" ranges from 1 to 10. Returns a numerical value. Use for legacy systems.
Latched Data Value (Digital)	$latched_data_digital:x$	"x" ranges from 1 to 10. Returns On or Off. Use for legacy systems.
Location Path	$location_path$	Displays the path display names from root to source. Example: Building B / Basement / VAV AHU B / SSP_STOP The number of levels in the path is based on the System Settings field *Levels displayed in paths.* To override this setting, enter the field code as $location_path:#$, substituting # with the number of path levels you want to show. For example, $location_path:5$ will show 5 levels.

Table 3.33 Field Codes Description (continued)

Field Code Name	Field Code	Description
Long Message	$long_message$	The formatted alarm long text displayed by double clicking the alarm on the Alarms page.
Message Details	$message_details$	The message details displayed on the Alarms page *View* tab.
Message Prefix	$message_prefix$	The message prefix displayed on the Alarms page *View* tab.
Message Text	$message_text$	The message text displayed on the Alarms page *View* tab.
New State	new_state	The status of new state from the alarm source. Valid only for alarm type CHANGE OF STATE. Example: Alarm, Fault
New Value	new_value	The new value from the alarm source. Valid only for alarm type CHANGE OF VALUE. Example: 70
Notification Class	$notification_class$	The notification class assigned denotes how the received alarm was generated. For example, if set to 1, the alarm would typically be sent to SiteScan by Vertiv controllers.
Object ID	$object_ID$	Object ID of the alarm source. Example: 5:26
Out of Service	$out_of_service$	The status of 'out of service' from the alarm source. Example: True or false
Overridden	$overridden$	The status of 'overridden' from the alarm source. Example: True or false
Program ID	$program_id$	The address of the control program that generated the alarm. BACnet program address format: device ID, program number Example: 2423101,1 SuperVision program address format: site, gateway, controller, fbExample: 1, 2, 13, 5
Receive Time	$receive_time$	The time at the workstation when the alarm was received. Example: Nov 12, 2012 6:46:31 PM
Recipient Device ID	$device_id$	The device ID of the device where the alarm came from.Example: 8:2423101
Record Type	$record_type$	The type of alarm. Example: BACnet, Supervision, System
Reference Path	$reference_path$	Path to alarm source. Available in all alarm actions. Example: #e_b_vav_ahu_b/ssp_stop
Reference Value	$reference_value$	The 'reference value' from the alarm source. Valid only for alarm type FLOATING LIMIT. EXAMPLE 83
Referenced Bitstring	$referenced_bitstring$	The value of the 'referenced bitstring' value from the alarm source. Valid only for alarm type CHANGE OF BITSTRING. Example: 1011011101101
RTN Time	RTN_time	The time when the alarm returned to normal. Example: Nov 12, 2012 6:46:31 PM
Setpoint Value	$setpoint_value$	The 'setpoint value' from the alarm source. Valid only for alarm type FLOATING LIMIT. EXAMPLE 72
Short Message	$short_message$	The formatted alarm short text.
Site	$site$	The display name of the site the alarm came from. Example: Kennesaw
Source	$source$	The display name of the alarm source microblock that generated the alarm. Example: SAT_HI
Source description	$source:description$	The Description field of the alarm source microblock that generated the alarm. Example: High Cooling Supply Air Temp
Source Path	$source:<path>$	Substitute <path> with the path to the value you want to display. See Defining Vertiv™ Liebert® SiteScan™ Paths on page 135 . Example to add text value: $source:~equipment.display-name$ Example to add a numeric value: $source:/trees/geographic/rd_facility/ zone_1/lstat/present_value$ **NOTE: You can use Global Modify to get the path.**

Table 3.33 Field Codes Description (continued)

Field Code Name	Field Code	Description
		For legacy systems, use the latched data field codes.
System Directory	$system_dir$	The system folder name. Example: c:\SiteScanx.x\webroot\ world_corporation
To State	$to_state$	The current state of the alarm source. Example: NORMAL, FAULT, OFF NORMAL, HIGH LIMIT, LOW LIMIT

3.5 Time Lapse

Time lapse can be a helpful troubleshooting tool. You can replay Graphics, Alarms, or Trends pages for up to 24 hours starting on a specific date and time.

The Graphics page can replay only trended values. Values that are not trended are grayed out. Floorplan areas without trend data are dark gray.

NOTE: If a graphic is linked to a microblock value without an embedded trend but a Digital Trend or Analog Trend microblock is attached to the linked microblock by a wire, Time lapse will use the wire trend's value.

NOTE: When the graphic is viewed in Time Lapse:

The data in a data table or chart will not change.

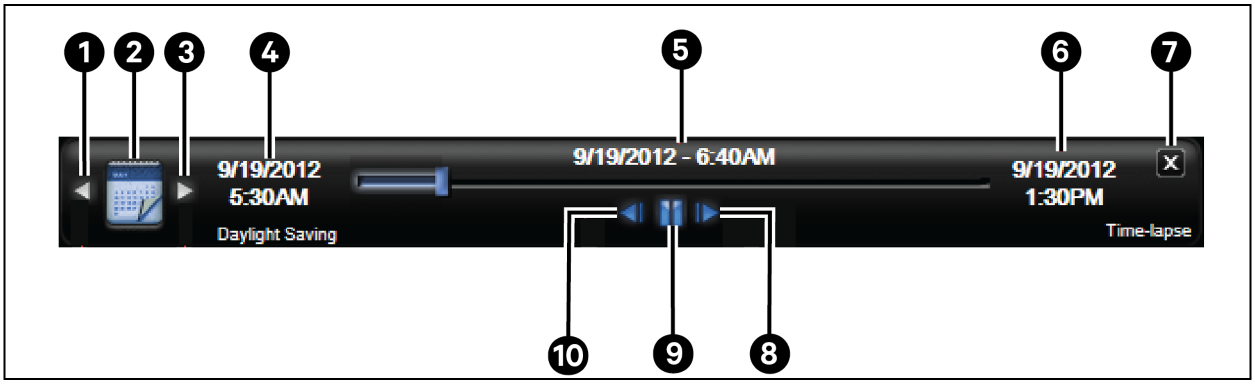
A color map will ignore report data and show thermographic colors.

For Time lapse to show thermographic colors, the Vertiv™ Liebert® SiteScan™ application polls each router in the system at specified intervals and collects color. Color is collected for the router and its downstream controllers only if their control program contains a Setpoint, Set Color, or Set Color If True microblock. The Server then uses the collected colors to create a trend called Color Trend.

3.5.1 Playing Time Lapse

1. Select the location on the tree where you want to see the time lapse.
2. Click 🎞 at the top of the page.
3. In the Replay field, select the length of time that you want to replay. The replay will step through the data at the interval shown.
4. In the Start field, select the date and time that you want the replay to begin. You can click:
    - The buttons ▲▼ to change the day or time.
    - The 📅 to select the date.
    - A date/time field, and then type the new number.
5. Click *Accept*. The time lapse immediately begins to play.
6. Use the following items in Figure 3.21 on the facing page to work with the time lapse.

Figure 3.21 Time Lapse Options



Item	Description
1	Shows an earlier time period
2	Change number of hours to reply or start date/ time
3	Shows a later time period
4	Start date/ time
5	Date/ time of current time-lapse display
6	End Date/ time
7	Exit Time lapse
8	Steps through the time lapse
9	Pause the Time lapse
10	Steps through the time lapse

NOTE: You can enable historical trending for trended values to have more trend data available in Time lapse and to have the data retrieved faster.

NOTE: While in time lapse, you can navigate to other locations in the tree.

You can select an alarm on the Alarms page and then click the *Activate Time lapse* button. This changes the time lapse to the 1-hour period in which the alarm occurred. You can step backward or forward through the time lapse at 1-minute intervals to see what other alarms occurred during that hour. You can also go to *Graphics* or *Trends* to see what else happened when the alarm occurred.

The white horizontal line on a Trends time lapse indicates where the replay currently is in the time lapse range.

3.5.2 Changing Polling Interval or Duration or to Turn Off Color Collection

1. On the System Configuration tree, select *System Settings*.
2. On the General tab under Trends, do one of the following:
    - In the Poll Interval field, change the frequency that the server collects color trend data from the routers.

NOTE: Last Poll Duration shows how long the last polling of the routers took.

- If directed by Vertiv Technical Support, uncheck *Enable Server Trending of Color* to stop color collection.

3. Click *Accept.*

3.6 Reports

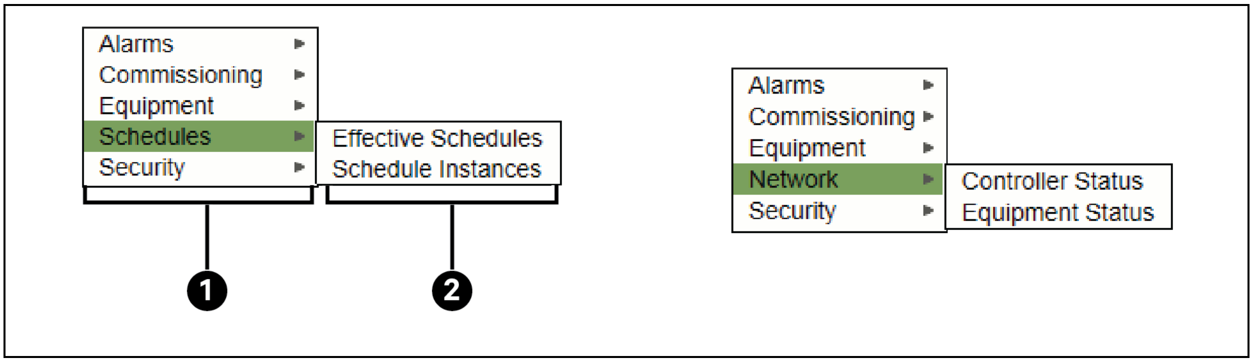
Monitor and troubleshoot your system with Vertiv™ Liebert® SiteScan™ reports. The Liebert® SiteScan™ license and/or edition determines which of the following things you can accomplish in the Liebert® SiteScan™ interface:.

- Run preconfigured reports
- Run custom reports
- Schedule reports
- Create custom reports

3.6.1 Preconfigured Reports

The preconfigured reports shown in the Reports button drop down list vary depending on which tree you selected.

Figure 3.22 Preconfigured Reports in the Geographic Tree and Network Tree



Item	Description
1	Report Category
2	Report Nae

A preconfigured report shows data for the selected tree item and all its children.

Table 3.34 Preconfigured Report for Selected Tree Item

Preconfigured Report	Allows
Alarms	
Alarm Actions	Create a summary of the information configured on the Alarms > Actions (Setting up Alarm Actions on page 38) tab.
Alarm Prefixes & Details	Create a summary of the information configured on the Alarms > Messages (See Alarm Messages on page 57) tab.
Alarm Sources	Create a summary of potential alarm sources as configured on the Alarms > Enable/Disable (See Setting Up an Alarm Source in the Liebert® SiteScan™ Interface on page 54) tab.
Alarms	View, sort, and filter the information on the Alarms View (Viewing, Troubleshooting, Acknowledging, and Deleting Alarms on page 31) tab.
Commissioning	

Table 3.34 Preconfigured Report for Selected Tree Item (continued)

Preconfigured Report	Allows
Equipment Checkout	View the information on the Equipment Checkout tab on the Properties page of the equipment during commissioning. Also, find equipment that has not been fully commissioned.
Test & Balance	View the results of VAV box commissioning. Running this report automatically uploads calibration parameters to the Vertiv™ Liebert® SiteScan™ application.
Equipment	
Locked Values	Find all locked points and locked values. **NOTE: Locks in the Airflow microblock are not reported.**
Network IO	Verify the programming and status of all network points—especially useful for commissioning controllers used for third-party integration.
Parameter Mismatch	Discover where your system has parameter mismatches that need to be resolved.
Point List	View the details of all points. Verify that all points have been checked out during commissioning. Also, create custom lists for other contractors. For example, create a list of BACnet IDs.
Trend Usage	Creates a summary of the information configured on the Trends > Enable/Disable (See Collecting Trend Data for a Point on page 23) tab.
Schedules	
Effective Schedules	View all equipment that may be scheduled and the net result of all schedules in effect for a selected date and time.
Schedule Instances	Find every schedule with its location that is entered at and below a selected tree item. This report can help you discover newly added and conflicting schedules.
Security	**NOTE: You must have the Advanced Security package to run these reports.**
Location Audit Log	View chronological lists of location-based changes, the operators that made them, and the reasons for the changes. This report includes changes such as property edits, downloads, driver changes, and view changes.
System Audit Log	View chronological lists of system-wide changes, the operators that made them, and the reasons for the changes. This report includes changes such as any change made on the System Configuration tree, login/logout, and scheduled processes like deleting expired trends
Network	
Controller Status	Discover network communication problems (shown as purple squares on the report) that need troubleshooting. The report also shows boot and driver version, download information, and if controller has 4.x or later driver, the report shows the serial number and Local Access port status.
Equipment Status	Display the thermographic color, status, and prime variable of each control program.

Running a Preconfigured Report

1. Select an *item on the Geographic or Network tree*.
2. Click the *Reports button drop down arrow*, then select a *report*.
3. On the Options tab, define the *layout and content of the report*.

NOTE: Changing the size and orientation of the printed page also changes the report layout on the View tab.

To create a CSV (Comma Separated Values) file after you run the report, select Support CSV text format. See Creating a PDF, XLS, or CSV File on page 104 .

The report options of the current operator are saved so that when that operator logs in again, the same options are used.

4. Click *Run*.

NOTE: Click Schedule to schedule the report to run on a recurring basis. See Scheduling Reports on page 105 .

Running an Ad Hoc Alarms or Security Report

Follow these steps to run a single ad hoc version of an Alarms, or Security report.

1. Click the *Reports drop-down arrow*, and then select the report that you want to schedule.
   - Alarms > Alarms
   - Security Reports > Location Audit Log
   - Security Reports > System Audit Log
2. Go to the *Options tab*.
3. In the Ad Hoc Report section, select the time span of the report.

Table 3.35

Date Range Option	Description
Unrestricted	The report contains all data for the entire duration of available dates.
Continuous Data (Date)	The report contains all data occurring between the specified Start and End dates.
Continuous Data (Date and Time)	The report contains only the data occurring between the specified Start Date and Time and End Date and Time.
Shift Report*	The report contains only the data occurring between the specified Shift Start and End Times within the specified date range.
* Requires Advanced Reporting Package	

4. Click *Accept*, and then click *Run*.

NOTE: Changes made here affect ad hoc report settings for the selected Alarms or Security report in all locations.

Configuring Scheduled Alarms and Security Reports

The following reports have additional scheduling options available. Scheduling these reports without configuring schedule options results in an error; see Managing Scheduled Reports on page 106 .

- Alarms > Alarms
- Security Reports > Location Audit Log
- Security Reports > System Audit Log

1. Go to the *Options tab*, open Scheduled Report, and check Enable schedule options for this location.
2. Select the *time span of the report*.

Table 3.36

Date Range Option	Description
Continuous Data (Date)	The report contains all data occurring between the specified Start and End dates.
Continuous Data (Date and Time)	The report contains only the data occurring between the specified Start Date and Time and End Date and Time.
Shift Report*	The report contains only the data occurring between the specified Shift Start and End Times within the specified date range.
* Requires Advanced Reporting Package	

3. Select the *number of Days, Weeks, Months, Quarters, or Years* the report will contain.

NOTE: The use of "previous": Selecting "previous week" returns data for the previous full calendar week, Sunday through Saturday. Select "previous 7 days" to see the most recent week of data. For example, selecting "previous 7 days" on a Wednesday returns data from last Wednesday through the current Tuesday.

Checking include current causes the report to contain data for the most recent iteration of the report. For example, a report for the previous week with the include current option checked contains only the data for the current week, even if it is not a complete week. In order to get the last week and the current week, it would be necessary to specify the previous 2 weeks.

4. Click *Accept*.

NOTE: Changes made here affect the selected Alarm or Security scheduled report in the current location only.

3.6.2 Custom Reports

Custom reports are managed through the Vertiv™ Liebert® SiteScan™ Report Manager that shows a list of all custom reports in your system. In the Report Manager, you can:

- Create a new custom report (Creating a Custom Report below)
- Copy an existing report as a starting point for a new report (See Creating a Custom Report below)
- Edit or delete an existing report (See Editing or Deleting a Custom Report on page 89)
- Export reports to a file so that it can be imported into another system (See Exporting or Importing a Custom Report on page 89)

A custom report can provide data for a data table (To Produce a Data Table on page 91), chart (Producing a Chart on page 96), or color map (Producing a Color Map on page 100) on a Graphics page.

NOTE: A custom report may appear in the Report Manager but not appear in the Reports button menu because its only purpose is to provide data to an item on a Graphics page.

To support upgraded systems, you can still create and access legacy (v6.5 and earlier) custom reports (See Working with Legacy (v6.5 and Earlier) Custom Reports on page 107). These reports appear only in the Reports button drop-down menu, but not in the Reports Manager.

Creating a Custom Report

1. Click the *Reports drop down arrow*, and then select *Report Manager*.
2. Click *Add*.

NOTE: To save time when making a report that is similar to an existing report, select the existing report in the Report Manager, and then click Copy. The Report Editor opens the new report so that you can make changes.

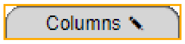
Click on the *Display Name* or ID heading in the Report Manager to sort the column.

3. Enter information on the following Report Editor tabs until you have created the report.
    - Type tab (Type Tab on the next page)
    - Columns tab (Columns Tab on page 74)
    - Variables tab (Variables Tab on page 84)
    - Where tab (Where Tab on page 85)
    - Options tab (Options Tab on page 1)
    - Output tab (Output Tab on page 86)

NOTE: As you create your report, you can use the Preview section on each tab to check your work. See Previewing a Report on page 88 .

After you create the report, you can go to any item in the tree where the report is accessible, and run it. See Running a Custom Report on page 89 .

A report can have a maximum of 50 columns and 1000 rows.

CAUTION: As you move from tab to tab in the Report Editor, click Apply to save your changes on a tab. If you click Cancel on a tab, all unsaved changes on any tab will be lost. Tabs that have unsaved changes have a pencil icon beside the tab name. For example, 

Columns

Type Tab

1. Enter the *necessary information* about the report you are creating. See table below.
2. Click *Accept or Apply*.

Table 3.37 Type Tab Fields

Field	Notes	
Display name	The name that will appear in the Reports button drop-down list.	
ID	A unique ID for the report (letters, numbers, underscores, and hyphens only; no spaces or special characters).	
Show in Reports menu	By default, the report name will appear directly in the Reports button drop-down list, not in a category. You can: • Check this box and then select a category for the report. SeeOrganizing Custom Reports by Category on page 90 . • Uncheck this box so that this report does not appear in the Reports button drop-down list. For example, you could uncheck this box if the report will provide data to a Graphics page but does not provide valuable information as a stand-alone report.	
Primary column	Select the type of information on which you want the report to be based. Click Change if you want to change your initial selection and have your new selection to take effect.	
	Select	Then
	Control Programs	To create the list of control programs., do one or both of the following. The primary column will list the equipment that use those control programs. • Enter a control program name, and then click Add. You can use wildcards. See the help text to the right of this field. • Select from the list of existing control programs.
	Locations	To create the list of locations that will appear on each row in the primary column, do one or both of the following.: • Select locations in the Geographic or Network tree. • Enter a location name, and then click Add.
	Reference Names	Enter a reference name and then click Add. You can use wildcards. See the help text to the right of this field. If needed, add more reference names, to build a list of reference names. The primary column will list the locations that have the reference names. Select the types of reference names that you added.
	Tag Names	To create the list based on tagged locations for each row in the primary column of the report:

Table 3.37 Type Tab Fields (continued)

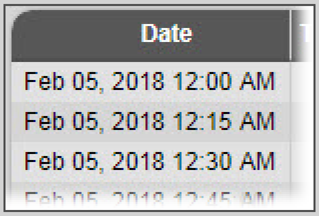
Field	Notes	
		1. Click to the left in the list of system tags to add that tag to the Tag Names table. **NOTE: To combine several tags for a single location, keep clicking next to each tag you want.** 2. Click Add to assign the selected tags to the list of tag names to use for a location. 3. Check the types of locations (Area, Equipment, Microblock) that you want in the column. 4. Click *Apply*. The locations selected for the report will be those that match any row of tag names. For example, to get a report of locations tagged Chilled Water and Hot Water: 1. Click *next to Chilled*. 2. Click *next to Water*. 3. Click *Add*. 4. Click *next to Hot*. 5. Click *next to Water*. 6. Click *Add*.
	Date Range	Choose any one of the following: • Previous: A specified number of previous days, weeks, months, quarters, or years. You can choose to include the current time period. • From date: A specified number of days, weeks, months, quarters, or years starting at a specific date (yyyy/mm/dd). **NOTE: In the fields for the above 2 options, , you can enter a value or variable name. If you enter a variable, it must be defined on the Variables Tab on page 84 .** Frequency: If you choose Months or Days in the Previous or From date fields, you can choose how often the data is to be reported. For example, if you choose a frequency of Every 15 minutes, the primary column could look similar to the following:  Date Feb 05, 2018 12:00 AM Feb 05, 2018 12:15 AM Feb 05, 2018 12:30 AM Feb 05, 2018 12:45 AM Date Range Format in Report: Type the date format that you want to see in the report. See Date formats (Date Formats on the next page) for a list of supported formats.
	Existing Report	Select an existing report from the drop-down list or enter a report name in the text field. The existing report will be embedded in the new report so that you can add columns to it. Any changes to the existing report will also be reflected in the new report.

Table 3.37 Type Tab Fields (continued)

Field	Notes	
	Color Map	Select this option to show colors on a Graphics page. For example, you could have a campus map where each building would show green for good energy usage or red for high energy usage. See Producing a Color Map on page 100 .
Hide Primary column in report	Check if you don't want this column to appear in the report.	
Primary column header	If you do not hide the Primary column, type the header that you want to appear at the top of this column.	

Date Formats

If your Primary column is a Date Range, use the following information to enter a format in the Date Range format in report field.

Table 3.38 Date Range Format

For	Type	Example
Year	yyyy yy	2017 17
Month	MMMM MMM MM	September Sep 9
Week in year	w	27
Week in month	W	2
Day in year	D	189
Day in month	d	12
Day of week in month	F	2 (2nd Thursday in June)
Day name	EEEE E	Tuesday Tue
Day number in week	u	1 (Monday), 2 (Tuesday), etc.

Table 3.39 Examples of Combinations

Type	Example
yyyy-MM-dd	2017-06-02
MMMM yy	June 17
MMM/yyyy	Jun/2017
MM/dd/yy D	06/02/17 153

NOTE: To include a single quote, type two single quotes. Example: MMM "yy = Jun '17

To include static text, enclose it in single quotes. Example: 'Year' yyyy = Year 2017

For more information on date formats, search the Internet for "java simple date format".

Columns Tab

The Primary column for a table is defined on the Type tab. The remaining columns can be defined on the *Columns* tab.To define the columns in your report, you can:

- Add each individual column (Adding a Column on the facing page)
- Copy an existing column (Copying a Column on page 76)

- Replicate a column (Trend Data only) (Replicating a Trend Data Column on the next page)

Adding a Column

1. Click *Add*.
2. Enter or select *options* in the first four fields that appear. See table below.
3. Select an option in the *Column data is from* field. See the bold highlighted rows in the **Table 3.40** below for a description of the options.

NOTE: Click *Change* if you want to change your initial selection and have your new selection to take effect.

4. Select or enter *information* for the option you chose in Step 1 . See **Table 3.40** below .
5. Click *Accept or Apply*.

Table 3.40

Field	Notes	
The following four fields are common to all the options from Step 1 .		
Display name	The name that will be shown in the report as the header of the column..	
ID	A unique ID for the column (letters, numbers, underscores, and hyphens only; no spaces or special characters).	
Render data as	Value	Shows a value in the report.
	Hidden	Hides the column in the report. The column data can be used to produce a value for another cell.
	Color	Uses the column's value to determine a color on a color map (Producing a Color Map on page 100). Set the Column data is from field to Expression or Function, and then enter the appropriate information that returns a color value.
	Icon	Shows an icon to indicate a certain condition. Set the Column data is from field to Expression, and then enter an expression that says what icon filename to show for a particular condition. You can use the icons included with your system or you can create custom icons. See Icons on page 83 for more information.
Column format	Allows you to define the alignment, width, and format of digits of the column. **NOTE: Column format does not apply if you select Hidden or Color in the Render data as field.**	
The following fields are based on your selection in the Column data is from field.		
Path	**The column output will be based on a path to a value in the Vertiv™ Liebert® SiteScan™ system.**	
Path	Enter the path to the value you want. See Defining Vertiv™ Liebert® SiteScan™ Paths on page 135 .	
Show value as text	Check to have the value reported as text instead of its numerical value. For example, show the word On instead of 1.	
Expression	**The column output will be based on the result of an expression (Expressions on page 77).**	
Trend Data	**The column's output will be based on a value calculated from a range of trend data.**	
Trend path	Do one of the following: • Click the Select Trend Path button to select the trended point. Typically, you want the full (absolute) path, but if needed, you can select the relative path. • Type the path to the trend that you want the report to pull data from. See Defining Vertiv™ Liebert® SiteScan™ Paths on page 135 .	
Operation	Select the type of value or calculation that you want the column to show. See Operations on page 83 for a description of each option.	
Interval sample	If the selected operation allows, you can choose how to handle the first and last sample of the time period. For example, Include start time / exclude end time.	

Table 3.40 (continued)

Field	Notes	
Database trends only	Check to include only trends saved in the database, not those in the controller.	
Show time of sample	Check to include the time of the sample in the column.	
Time range	From primary column	You can use this option if the primary column of the report is a date range.
	From column	You use this option if your report began with an embedded external report that has a column containing date ranges.
	Value	A time period specified by entering a Start date and End date.
	Past	Enter the number of days, weeks, months, quarters, and years in the past. You can select whether to include the current time period or not.
	NOTE: You can use a variable (Variables Tab on page 84) for a Time range count or date field. The variable must be defined on the Variables tab.	
Function	The column output will be based on the value or manipulation of the value from another column.	
Input column	The column on which you want to perform a function.	
Function	Select an option in the drop-down list. See Functions on page 82 .	
Arguments	A statement that contains the criteria of the function. See Functions on page 82 for argument formats and examples. **NOTE: You can use a variable (Variables Tab on page 84) name in the argument. The variable must be defined on the Variables tab.**	
+/- Date Range	The column output will be based on the date range you choose.	
Adjust by	Adjusts the data by these many days, weeks, months, quarters, or years. Enter a value or variable name.	
From column	Enter the Column ID of the date range you want to adjust. To adjust the primary date range, leave this field blank.	

NOTE: To delete a column, select the column in the table at the top of the page, then click *Delete.*

To change the order of the columns, select a column and then click or to move the column.

Copying a Column

1. Select the column you want to copy in the table at the top of the Columns tab.
2. Click the *Copy button.*
3. Change the fields of the column as needed. See field descriptions in To add a column (Adding a Column on the previous page).

NOTE: The column's ID is incremented by 1.

Replicating a Trend Data Column

When you have defined all the criteria for a trend column, you can quickly reproduce that column for other trend sources.

1. Select the *column in the table at the top of the Columns tab.*
2. Click the *Replicate Column button.*

3. Select whether you want the Trend Path for the new columns to be the full (absolute) path or the relative path. This is usually set to Full path. See Defining Vertiv™ Liebert® SiteScan™ Paths on page 135 .
4. In the left column, select a *location*.
5. The right column displays all trend sources at or below the selected location. Select the trend sources that you want. A column will be added for each instance of the selected trend sources at or below the selected location.
6. Repeat steps 4 and 5 for any additional locations and points that you want in you report.
7. Click *Apply*.
8. Click *Close*.
9. Change the fields in each column as needed. See field descriptions Adding a Column on page 75 .

Expressions

On the Columns tab of the Report Editor, you can specify that a column's data is from an expression. Vertiv™ Liebert® SiteScan™ expressions are similar to expressions used in spreadsheet programs. The most basic expression is a math calculation, but an expression can also manipulate text.

An expression generally consists of at least one item in dollar signs and an operator. See table below. The item in dollar signs can be:

- Another column's ID
- A path to an item in your system or a semantic tag
- A variable defined on the Variables tab of the Report Editor.

Static text in an expression must be enclosed with quotes (either single or double quotes can be used). Any item that results in text should also be enclosed with quotes. This example shows both situations: 'Filter is ' + '$filter_status$'

Example of a simple expression: to compute the average value of min_temp and max_temp columns

Expression: ($min_temp$ + $max_temp$) / 2

To verify that the expression you entered is formatted correctly, click *Check Syntax*. The result appears to the right of the button. The numerical position of the first error in the expression appears and the error is highlighted.

NOTE: The result of checking an expression with a variable may not be accurate since variables can be used in such a wide variety of ways.

Operators

An operator defines how each piece of an expression is to be handled. The following table lists operators that can be used in expressions.

Table 3.41 List of Operators to be Used in Expressions

Symbol	Name	Description
Operators that return true/false (1/0)		
<	Less than	Compares numeric data. Returns true if the value to the left of the operator is smaller than the value to the right.
>	Greater than	Compares numeric data. Returns true if the value to the left of the operator is larger than the value to the right.
<=	Less than or equal to	Compares numeric data. Returns true if the value to the left of the operator is smaller than or equal to the value to the right.

Table 3.41 List of Operators to be Used in Expressions (continued)

Symbol	Name	Description
>=	Greater than or equal to	Compares numeric data. Returns true if the value to the left of the operator is larger than or equal to the value to the right.
!	Not	Evaluates the expression and returns the opposite. Example: !$zone_temp$ > 72 If zone_temp is greater than 72, the expression is false. If zone_temp is not greater than 72, the expression is true.
==	Equal to	Compares data. Returns true if the values on both sides of the operator are equal.
!=	Not equal to	Compares data. Returns true if the value to the left of the operator does not match the value to the right.
&&	And	Combines expressions. Returns true if the expressions on both sides of && result in true.
||	Or	Combines expressions. Returns true if the expression on either side or both sides of the operator results in true.
Operators that return a numeric value		
+	Add	Adds numeric data, expressions, or values. **NOTE: You can use this operator to concatenate mixed numbers and strings. Example: 1 + 'alpha' returns "1alpha".**
-	Subtract	Subtracts numeric data, expressions, or values.
*	Multiply	Multiplies numeric data, expressions, or values.
^	Power	To the power of. Example: 2^3 (returns 8)
/	Divide	Divides numeric data, expressions, or values.
%	Modulus	Finds the remainder in the division of numeric data, expressions, or values.
Other operators		
( )	Parentheses	Use to nest expressions. Operations in parentheses are evaluated before those outside parentheses.
if		Syntax: if (expression, true value, false value) Expression is evaluated and if 1/true, the true value is returned, otherwise the false value is returned
?	Ternary	Syntax: <condition> ? <expression to execute if the condition is true> : <expression to execute if the condition is false> This operator can be used as an alternative to an if statement. Example: 1 == 2 ? 'true' : 'false'
#	Comment	Use to make the characters in the line after this operator a comment

NOTE: If no operator is present in an expression, "+" is assumed. Example: "1 2 3" returns "6", and "a b c" returns "abc".

Combining Expressions

Example 1:

Expression: $zone_temp$ < 60 || $zone_temp$ > 75

Translation: True if the current zone temperature is less than 60 or greater than 75

Example 2:

Expression: ! ($ai1/locked$ || $ai1/present_value$ > 100)

Translation: True if ai1 is not locked and al's present value is not greater than 100

Example 3:

Expression: if ($zone_temp$ < 60 || $zone_temp$ > 75, 'out of range', 'good')

Translation: If zone temperature is less than 60 or greater than 75, show out of range. Otherwise, show good.

Math Functions

Table 3.42 Math Functions

Function	Description
abs (a)	Returns the absolute value of a value.
acos (a)	Returns the arc cosine of a value; the returned angle is in the range 0.0 through pi.
asin (a)	Returns the arc sine of a value; the returned angle is in the range -pi/2 through pi/2.
atan (a)	Returns the arc tangent of a value; the returned angle is in the range -pi/2 through pi/2.
atan2 (y, x)	Returns the angle theta from the conversion of rectangular coordinates (x, y) to polar coordinates (r, theta).
cbrt (a)	Returns the cube root of a value.
ceil (a)	Returns the smallest (closest to negative infinity) value that is greater than or equal to the argument and is equal to a mathematical integer.
cos (a)	Returns the trigonometric cosine of an angle.
exp (a)	Returns Euler's number e raised to the power of a value.
floor (a)	Returns the largest (closest to positive infinity) value that is less than or equal to the argument and is equal to a mathematical integer.
hypot (x, y)	Returns sqrt(x2 +y2) without intermediate overflow or underflow.
IEEEremainder (f1, f2)	Computes the remainder operation on two arguments as prescribed by the IEEE 754 standard.
log (a)	Returns the natural logarithm (base e) of a value.
log10 (a)	Returns the base 10 logarithm of a value.
max (a, b)	Returns the greater of two values.
min (a, b)	Returns the smaller of two values.
pow (a, b)	Returns the value of the first argument raised to the power of the second argument.
random ()	Returns a value with a positive sign, greater than or equal to 0.0 and less than 1.0.
rint (a)	Returns the value that is closest in value to the argument and is equal to a mathematical integer.
round (a)	Returns the closest long to the argument, with ties rounding to positive infinity.
sin (a)	Returns the trigonometric sine of an angle.
signum (float f)	Returns the signum function of the argument; zero if the argument is zero, 1.0f if the argument is greater than zero, -1.0f if the argument is less than zero.
sqrt (a)	Returns the correctly rounded positive square root of a value.
tan (a)	Returns the trigonometric tangent of an angle.
toDegrees (angrad)	Converts an angle measured in radians to an approximately equivalent angle measured in degrees.
toRadians (angdeg)	Converts an angle measured in degrees to an approximately equivalent angle measured in radians.

Text Functions

Table 3.43 Text Functions

Function	Description
char (code)	Returns a single character string for the given Unicode character code. For example, char(36) will create the string "$".
charAT (s, pos)	Returns the character and the position.
compareTo (s1, s2)	Compares two strings. <0 if s1 <s2, 0 if s1 == s2, >0 if s1 > s2
compartToIgnoreCase (s1, s2)	Compares two strings ignoring case. <0 if s1 <s2, 0 if s1 == s2, >0 if s1 > s2
concat (s1, s2, ...)	Concatenates the two or more strings together. Same as "s1 + s2 + "
dateDiff (s1, s2)	Returns the difference between two dates, in days. Parameters may be date variables or strings of format 'yyyy/mm/dd'
endsWith (s1, s2)	Returns "1" if s1 ends with the string s2, else "0".
equals (s1, s2)	Returns "1" if strings are equal, else "0".
equalsIgnoreCase (s1, s2)	Returns "1" if strings are equal ignoring case, else "0".
indexOf (s1, s2, start)	Returns the index (position) of the first occurrence of the second string in the first string after "start" position. Use 0 to start from beginning of string. It returns -1 if S2 is not found.
lastIndexOf (s1, s2)	Returns the index (position) of the last occurrence of the seconds string in the first string. It returns -1 if S2 is not found.
length (s1)	Returns the length of the strings.
newline() or \n	Inserts a return.
now (s1)	Returns the current time and accepts one time-format string based on "Java SimpleDateFormat". If the string is empty, the default system date and time format is used. Examples: • "" → 08/28/2020 8:56:59 AM • "EEEE" → "Friday" • "MM/dd/yyyy" → 08/28/2020 • "h:mm a" → 8:56 AM • "hh:mm a" → 08:56 AM
replace (s1, s2, s3)	Replaces all occurrences in "s1" of "s2" with "s3".
startsWith (s1, s2)	Returns 1" if s1 starts with s2.
substring (s1, i2, i2)	Returns subset from string s1 starting at index i1 to index i2. (i2 must be >= i1)
toLowerCase (s)	Converts string to lower case.
toUpperCase (s)	Converts string to upper case.
trim (s)	Removes white space from the beginning and end of the string.
\	Used to escape operator characters by placing it before the operator. Example: 'Cost is \$' +$cost$' returns "Cost is $10.99".

Functions

On the Columns tab of Report Editor, you can specify that the data of a column comes from one of the following functions that returns another column's value or manipulation of that value.

Table 3.44 Functions on Column Tab

Function	Description
Valid Column	Returns true/false if input column is valid
Default Value	Returns the column's value if it is a valid value, otherwise returns the argument.
Format	Formats a value using Java String format function. For more information, search the Internet for "string format with java 8".
Format Duration	Formats a trend duration value. Argument formats: %d%, %h%, %m%, %s% (clock based) %D%, %H%, %M%, %S% (total count rounded down) Example 1: %ddd% days %hh%:%mm% = 003 days 13:50 Example 2: %M% min = 283 min
Convert Values to Text	Converts a number to a text value. Argument format: Define a set of comma separated statements. Format of each statement: lower limit=value Example 1: 0=F,60=D,70=C,80=B,90=A,100=A+ Example 2: F,60=D,70=C,80=B,90=A,100=A+ (first bucket is default for anything below second bucket's value) Example 3: Cold,68=Perfect,75=Warm Example 4: 65=Cold,68=Perfect,74=Perfect,75=Warm,76=Warm
Convert Integer to Text	Converts an integer value to text. If no match, value is empty. Argument format: Comma separated list of statements. Format of each statement: #=text Example: 0=Zero,1=One,2=Two,3=Oops
Convert Text to Integer	Converts text to an integer value. Matching is case insensitive. Argument format: Comma separated list of statements. Format of each statement: text=# Use * to match any letters. Example 1: Off=0,On=1 -or- off=0 -or- OFF=0 Example 2: a*=1,b*=2 a=1 -or- APPLE=1 B=2 -or- Book=2
Convert to Color	Attempts to convert an ALC color value (0 to 15) to a color for a color map.
Color Gradient	Converts a defined minimum and maximum number each to a color. It then maps numbers between minimum and maximum to colors to form a gradient. Format: min,max,color1,color2 Example 1: 1, 10, red, blue Example 2: 1, 10, #FF0000, #0000FF
Date Range Start	Formats the START date/time of a Date Range. Examples: yyyy/MM/dd hh:mm = 2017/07/04 11:30 hh:mm:ss = 08:35:16 For more information, search the Internet for "customizing date time formats with java".
Date Range End	Formats the END date /time of a Date Range. Examples: yyyy/MM/dd hh:mm = 2017/07/04 11:30 hh:mm:ss = 08:35:16 For more information, search the Internet for "customizing date time formats with java".
Ordinal Value	Converts a text enumeration to its integer value when possible.
Location Tags	Lists all of the semantic tags assigned to the location in each row. Enter location for the input column ID to create a simple report that shows all of the tags for the locations.
Regular Expression	Finds a piece of text from a larger text body. Example: Finds a piece of text in a modstat. For more information, search the Internet for "regular expression patterns with java 8".

Operations

On the Columns tab of Report Editor, you can specify that the data of a column comes from trend data. You can then specify one of the following operations be performed on the trend data.

Table 3.45 Operations to be Performed on Trend Data

Operation	Shows the following for the specified time range
Average Value	The average value.
Count All Trend Records	Number of trend records collected (includes items such as time changes and enabling/disabling the trend log).
Count Trend Samples Only	Number of times the trend value was read.
First Value w/Time	The first trend sample and the time it was read.
Last Value w/Time	The last trend sample and the time it was read.
Maximum Value w/Time	The largest value and the time it was read.
Minimum Value w/Time	The smallest value and the time it was read.
Aggregate Consumption	Total consumption for meter trend data. This operation makes appropriate calculations for meters that reset to 0.
Sum of Values	The total of all trend values.
% Time in Range	You can enter 3 types of arguments to determine the percentage of time that the trend value was: • One or more single values. Format: A comma separated list of values Example: Enter 1,2,3,4 to get the percentage of time that the trend value was 1, 2, 3, or 4. • Between two values Format: A single statement or a comma separate list of statements Example 1: Enter the statement 65:75 to get the percentage of time that the trend value was 65 to 75. Example 2: Enter the statement 28:30,38:40,48:50 to get the percentage of time that the trend value was 28 to 30, 38 to 40, or 48 to 50. • Not a specified value or between two values Format: !(value) Example 1: Enter !10 to get the percentage of time that the trend value was not 10. Example 2: Enter !28:30,38:40 to get the percentage of time that the trend value was not 28 to 30 or 38 to 40.

Icons

You can design a report that displays icons to indicate different conditions. You can use the icons included with your system or create custom icons. On the Columns tab of the Report Editor:

1. Set *Column data* is from field to Expression.
2. Set Render data as field to Icon.
3. Enter an Expression that contains the file name opf the icon. See the **Table 3.46** on the next page for the file names of icons included with your system, or see Custom Icons on the next page .

Table 3.46 Included Icons

Color	On	Off	Animated .gif that flashes on and off
Red	🟥 light_on_red.png	⬛ light_off_red.png	🟥 light_alarm_red.gif
Blue	🟦 light_on_blue.png	⬛ light_off_blue.png	🟦 light_alarm_blue.gif
Light blue	⬜ light_on_ltblue.png	⬛ light_off_ltblue.png	⬜ light_alarm_ltblue.gif
Green	🟩 light_on_green.png	⬛ light_off_green.png	🟩 light_alarm_green.gif
Yellow	🟨 light_on_yellow.png	⬛ light_off_yellow.png	🟨 light_alarm_yellow.gif
Magenta	🟪 light_on_magenta.png	⬛ light_off_magenta.png	🟪 light_alarm_magenta.gif
Orange	🟧 light_on_orange.png	⬛ light_off_orange.png	🟧 light_alarm_orange.gif
White	⬜ light_on_white.png	⬛ light_off_white.png	⬜ light_alarm_white.gif

Custom Icons

If you choose to use a custom icon, put the icon in one of the following places:

- In Vertiv™ Liebert® SiteScan™ X.X\webroot\<system name>\tables. Put only the icon's file name in the expression.
- Anywhere under the webroot folder. Put the full path from the webroot folder in the expression. Example: /_common/lvl5/skin/graphics/type/area.gif.

Variables Tab

You can enter a variable in a Report Editor field so that you can edit that field when you run the report. For example, if you create a Date Range report for the previous 4 months, you can put a variable named number_of_months in the field instead of a 4. When you run the report, you can change the variable value to 12 to show the previous 12 months.

1. Click *Add* to create a new variable.
2. Enter the criteria of variable. See **Table 3.47** on the facing page .
3. Click *Accept or Apply*.

Table 3.47 Variables Tab Fields

Field	Notes	
ID	This ID is what you will insert in a report field that you want to be able to change when you run the report. (Use letters, numbers, underscores, and hyphens only; no spaces or special characters).	
Type	Select an option from the drop-down list, and then enter a Value.	
	Type	Value
	String	A text phrase. Can contain letters, numbers, and special characters.
	Number	Can contain any number in any format.
	Date	Format is yyyy/mm/dd.
	Time	Format is hh:mm:ss.
User editable Display name	Check to let a user edit the value of variable when they run the report. Enter a Display name for the variable that will appear on the page where you run the report.	

NOTE: The table at the top of the Variables tab shows the variables that you defined. Their order in this table is how they will appear in on the page where you run the report. To change the order on the Variables tab, select a variable in the table and then click ▲ or ▼ .

Where Tab

1. Click the *drop down list* for This report can be accessed from, and then select an option.
2. Click *Define Where*.
3. Select or enter *information* for the option you chose. See table below.
4. Click *Accept or Apply*.

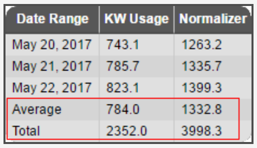
Table 3.48 Where Tab Fields

Field	Notes
Anywhere	The report can be run from anywhere in the system.
Control Programs	Do one or both of the following: • Type a control program name, and then click Add. **NOTE: You can use wildcards. See the examples in the Liebert® SiteScan™ interface.** • Select existing control programs from the list.
Location Types	Select the types of locations where you want the report to be available.
Locations	Select locations on the trees, or type a location name in the text box.

Options Tab

1. Click the *drop down list* to the left of the Add button, and select an option.
2. Click *Add*.
3. Select or enter *information* for the option you chose. See **Table 3.49** on the next page .
4. Click *Accept or Apply*.

Table 3.49 Options Tab Fields

Field	Notes	
Show Max/Min/Avg/Total	Check the appropriate boxes to show the maximum value, minimum value, average, standard deviation, or total at the bottom of the columns. Enter the Column ID of the column that you want labels to be in.	
Show first ___rows	Enter the maximum number of rows to be displayed when the report is previewed or run. This does not include the Max/Min/Avg/Total rows. NOTE: You can enter a value or variable name in this field. If you enter a variable, it must be defined on the Variables tab.	
Sort column	Sorts the specified column(s) from A to Z or 1 to ... Example of comma separated list of column IDs: date_range, kw_usage, normalizer Check Reverse Sort to sort Z to A, ... to 1.	
Filter rows	Select Include row when or Exclude row when a specified column (ID) equals a specified value.	

Date Range	KW Usage	Normalizer
May 20, 2017	743.1	1263.2
May 21, 2017	785.7	1335.7
May 22, 2017	823.1	1399.3
Average	784.0	1332.8
Total	2352.0	3998.3

NOTE: You can create a report with multiple options, but take into account that they will be processed in the order they appear in the table at the top of the Options page. For example, if your first option is to Show the first 10 rows and your second option is Filter rows, only the 10 rows will be filtered. To change the order of processing, select an option in the table and then click ▲ or ▼ .

Output Tab

On this tab, you can define the criteria for a report PDF or a chart on a graphic.

1. Select or enter *information* as needed. See Table 3.50 below .
2. Click *Accept or Apply*.

Table 3.50 Output Tab Fields

Field	Notes	
PDF Output		
Page orientation	Select Portrait or Landscape .	
Page size	Select the page size that you want for a pdf.	
Ignore page width	If the report exceeds the width of the selected Page size, select to ignore that width and show all columns in the online PDF.	
Font size	You can adjust the font size for the body of the report.	
Title font size	You can adjust the font size for the title of the report.	
Chart	These fields apply if you add a Chart control to a graphic in ViewBuilder. See Producing a Chart on page 96 .	
Axis label	For a Horizontal Bar Chart, this label will appear below the X axis. For a Vertical Bar Chart or Line Chart, this label will appear to the left of the Y axis.	
Data series	A column or row of numbers that are plotted in the chart.	
	Example:	For this report,

Table 3.50 Output Tab Fields (continued)

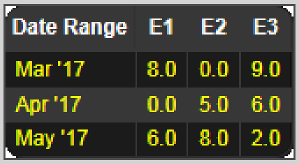
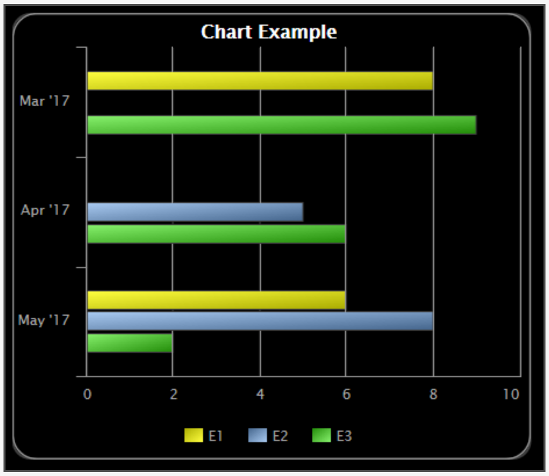
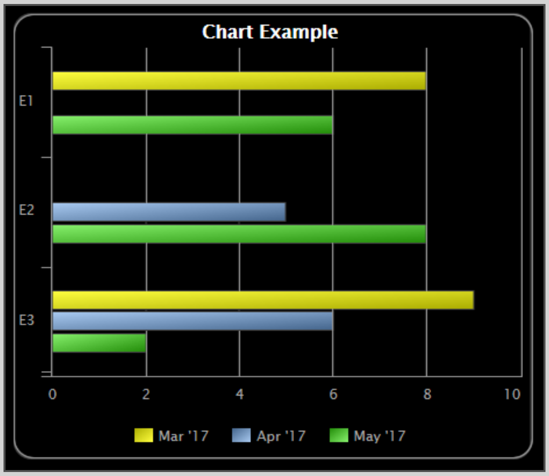
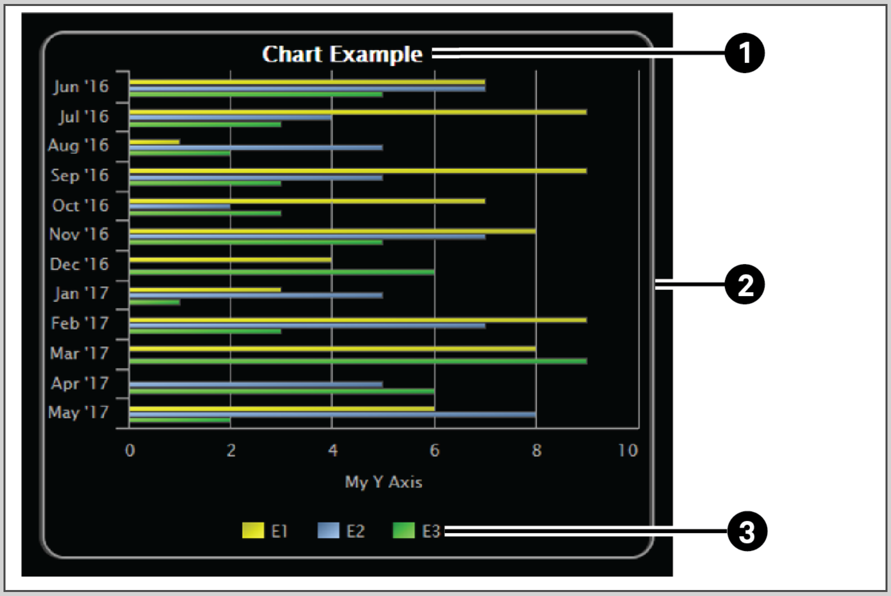
<table>
<tr><th>Field</th><th colspan="2">Notes</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Date Range</th><th>E1</th><th>E2</th><th>E3</th></tr>
<tr><td>Mar '17</td><td>8.0</td><td>0.0</td><td>9.0</td></tr>
<tr><td>Apr '17</td><td>0.0</td><td>5.0</td><td>6.0</td></tr>
<tr><td>May '17</td><td>6.0</td><td>8.0</td><td>2.0</td></tr>
</table></td></tr>
<tr><td></td><td>By column</td><td>A horizontal bar chart will look like this,

</td></tr>
<tr><td></td><td>By row</td><td>
</td></tr>
<tr><td></td><td colspan="2"><b>NOTE: Pie charts show only one data series.</b></td></tr>
</table>

Table 3.50 Output Tab Fields (continued)

<table>
<tr><th>Field</th><th colspan="2">Notes</th></tr>
<tr><td>Show title
Show legend
Show chart border</td><td colspan="2">

1. Title
2. Chart Border
3. Legend</td></tr>
<tr><td rowspan="5">Graphics Refresh</td><td colspan="2">A chart or data table control will refresh its report data every time you visit the Graphics page or at the following refresh rates while the Graphics page is displayed.</td></tr>
<tr><td>Primary column of report</td><td>Default refresh rate</td></tr>
<tr><td>A Date Range with a Frequency of Hourly or Every 15 minutes</td><td>Every 5 minutes</td></tr>
<tr><td>Any other Date Range</td><td>0 (never refreshes)</td></tr>
<tr><td>Anything else</td><td>Every 30 seconds</td></tr>
<tr><td>Use custom refresh rate</td><td colspan="2">Check this field to change the refresh rate. If your chart or data table shows a lot of data, refreshing frequently could slow down your system. If most of the data is historical data that does not change, you may want to set a longer refresh time.</td></tr>
<tr><td>Reset to defaults</td><td colspan="2">Click <i>Reset</i> to return all fields on the Output tab to their original settings.</td></tr>
</table>

Previewing a Report

At the bottom of every tab in the Report Editor is a Preview section so that you can check your work. Click *Show* to see the report. If you make changes to the report, click *Refresh* to update the preview.

You have the following options when previewing the report: See **Table 3.51** below .

Table 3.51 Options in Previewing Report

Option	Description
Show all columns	Includes columns defined as hidden and a column with additional information about the Primary column.
Show Column ID	Each column header shows the display name and column ID.
Show Debug Information	Gives information for troubleshooting a report.

NOTE: If the preview shows "Error", hover your cursor over the word to see a description of the error.

If the preview shows "?", this indicates there is no data.

Running a Custom Report

1. Select an *item* on the Geographic or Network tree where the report you want to run is accessible.
2. Click the *Reports button drop-down arrow*, and then select the *report*.
3. Optional: If the report was designed with variables (Variables Tab on page 84), you can change the values of the variable at the top of the page.

NOTE: Click Reset if you want to change the variables back to the value that was assigned when the report was created.

4. Click *Run*.

NOTE: A "?" in the report indicates there is no data.

Click *Edit* to change the design of the report. See Creating a Custom Report on page 71 for field descriptions.

Click *Schedule* to schedule the report to run on a recurring basis. See Scheduling Reports on page 105 .

Editing or Deleting a Custom Report

1. Click the *Reports button drop-down arrow*, and then select Report Manager.

NOTE: *Click* on the Display Name or ID heading to sort the column.

2. Select the *report*, and then do one of the following:
    - Click *Edit* to open the Report Editor, make changes as needed, then click Accept. See Creating a custom report (Creating a Custom Report on page 71) for field descriptions.

NOTE: To open a report in the Report Editor, double click on it.

- Click *Delete*, then click *OK*.

Exporting or Importing a Custom Report

You can export one or more reports from one system, copy them to another system, and then import the reports into the Vertiv™ Liebert® SiteScan™ interface.

To export reports, follow the below steps:

1. Click the *Reports drop down arrow*, and then select *Report Manager*.
2. Click *Export*.
3. Select the *checkboxes for the reports* that you want to export, or check *Select All*.
4. Click *Export*.

NOTE: A single report is exported as a .table file. Multiple reports are exported as a .zip file.

NOTE: In the Report Manager or Export Report window, you can click on the Display Name or ID heading to sort the column.

To import reports, follow the below steps:

1. Copy the *.table or .zip file* to the computer where you are importing them.

2. In the Liebert® SiteScan™ interface, click the *Reports drop-down arrow*, and then select *Report Manager*.
3. Click *Import*.
4. Browse to the *file* that you are importing.
5. If a report ID that you are importing matches an existing report ID, select *how you want to handle the situation:*

Table 3.52

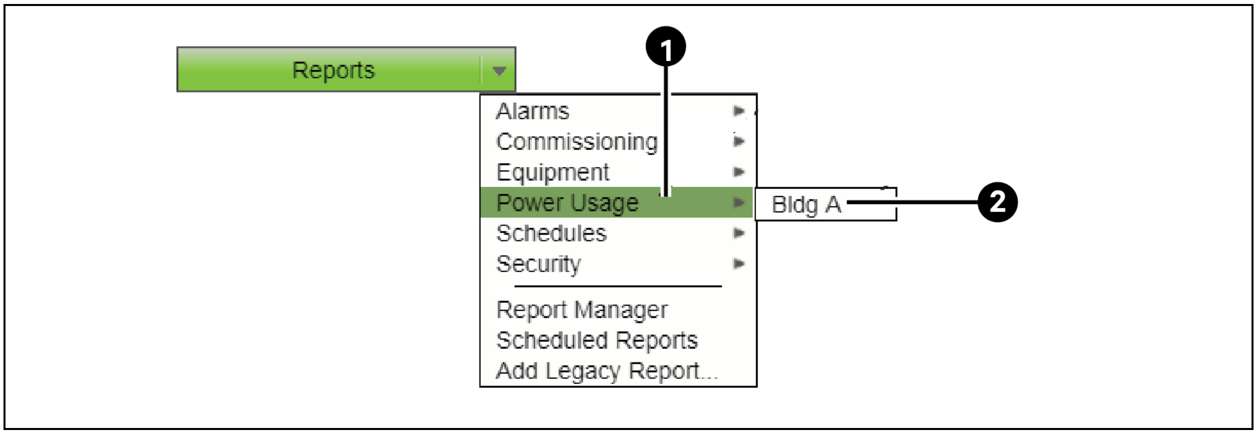
Option	Description
Rename	Rename the report that you are importing.
Replace	Replace the existing report with the report you are importing.
Skip	Do not import the report with the duplicate name.

6. Click *Import*.

Organizing Custom Reports by Category

When you create a custom report, you can assign it to a category so that the report appears in the category in the Reports button drop-down list.

Figure 3.23 Reports Button Drop-down List



Item	Description
1	Report Category
2	Report Name

To create a report category,follow the below steps:

1. On the System Configuration tree, click ▷ to the *left of the Categories folder*, then click *Report*.
2. Click *Add*.
3. Type the Category Name and Reference Name.
4. Select a *privilege* so that only operators with that privilege can access reports in the category.
5. Click *Accept*.

NOTE: To edit a category, select the category, make your changes, then click *Accept*. To delete a category, select the category, click *Delete*, then click *Accept*.

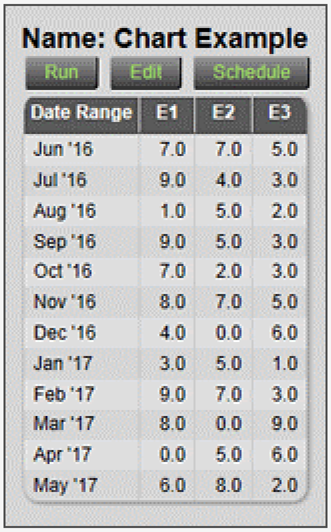
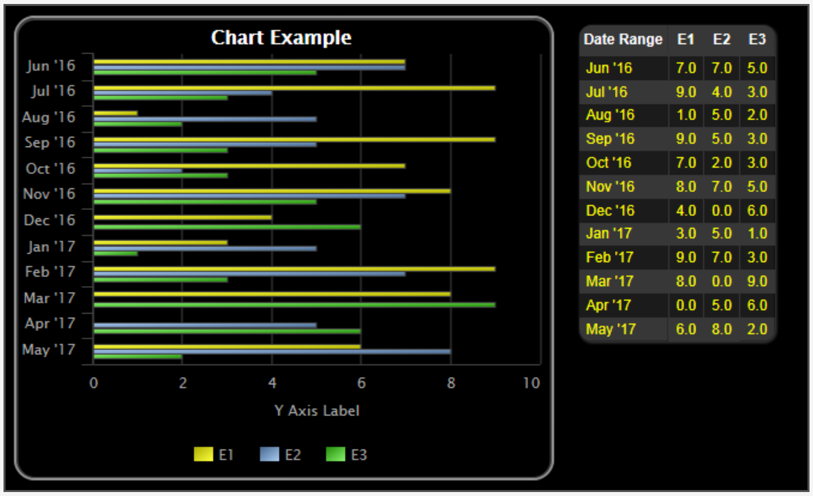
Using a Custom Report as the Source for a Graphics Page

A Vertiv™ Liebert® SiteScan™ custom report can be the data source for the following items on a Graphics page:

- A data table
- A value
- A chart
- A color map

Please see the Table 3.53 below that shows the report that supplies data to the chart and data table.

Table 3.53 Data Chart and Data Table for a Report

Report	Data Chart and Data Table
	

Name: Chart Example

Run Edit Schedule

Date Range	E1	E2	E3
Jun '16	7.0	7.0	5.0
Jul '16	9.0	4.0	3.0
Aug '16	1.0	5.0	2.0
Sep '16	9.0	5.0	3.0
Oct '16	7.0	2.0	3.0
Nov '16	8.0	7.0	5.0
Dec '16	4.0	0.0	6.0
Jan '17	3.0	5.0	1.0
Feb '17	9.0	7.0	3.0
Mar '17	8.0	0.0	9.0
Apr '17	0.0	5.0	6.0
May '17	6.0	8.0	2.0

Date Range	E1	E2	E3
Jun '16	7.0	7.0	5.0
Jul '16	9.0	4.0	3.0
Aug '16	1.0	5.0	2.0
Sep '16	9.0	5.0	3.0
Oct '16	7.0	2.0	3.0
Nov '16	8.0	7.0	5.0
Dec '16	4.0	0.0	6.0
Jan '17	3.0	5.0	1.0
Feb '17	9.0	7.0	3.0
Mar '17	8.0	0.0	9.0
Apr '17	0.0	5.0	6.0
May '17	6.0	8.0	2.0

NOTE: When the graphic is viewed in Time Lapse:

The data in a data table or chart will not change.

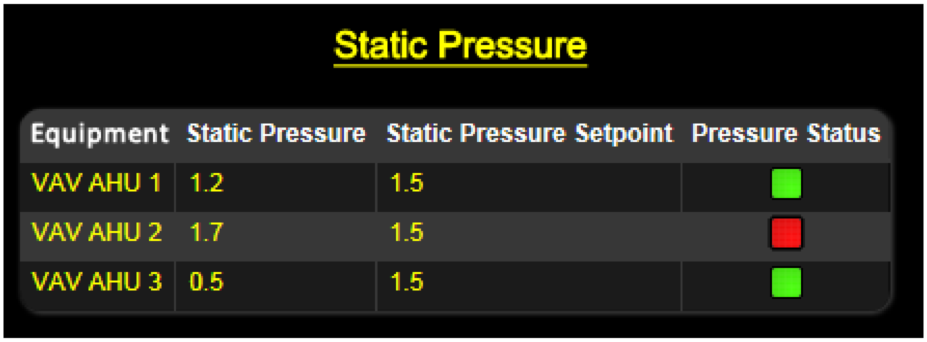
A color map will ignore report data and show thermographic colors.

You can modify custom report variables (Variables Tab on page 84) directly from a graphic in Liebert® SiteScan™ by clicking ✎ the button.

To Produce a Data Table

To produce a data table like the example in Figure 3.24 on the next page , first create the report in theVertiv™ Liebert® SiteScan™ interface and then create the corresponding graphic in ViewBuilder.

Figure 3.24 Data Table



Static Pressure

Equipment	Static Pressure	Static Pressure Setpoint	Pressure Status
VAV AHU 1	1.2	1.5	🟩
VAV AHU 2	1.7	1.5	🟥
VAV AHU 3	0.5	1.5	🟩

Creating the Report in the Vertiv™ Liebert® SiteScan™ Interface

Table 3.54 Instructions to Create a Report in Vertiv™ Liebert® SiteScan™ Interface

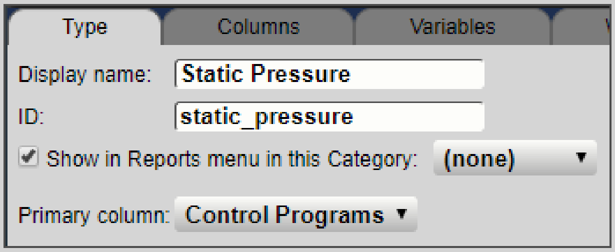
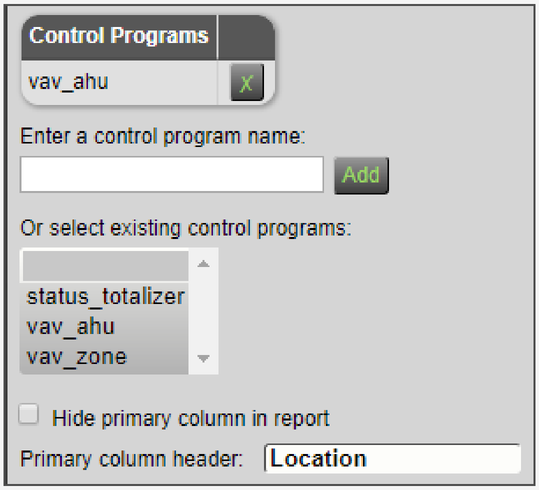
Instructions	Example
1. Click the Reports drop down arrow, and then select *Report Manager*.	
2. Click *Add*. 3. On the Type tab of the Report Editor, type a Display name and ID for the report. 4. In the Primary column field, select the type of information that you want the report to be based on (Control Programs in this example).	 Type | Columns | Variables Display name: Static Pressure ID: static_pressure ☑ Show in Reports menu in this Category: (none) ▼ Primary column: Control Programs ▼
5. On the Type tab (Type Tab on page 72), enter the criteria for the option that yout selected in Step 4 . 6. In the Primary column header field, enter the heading that you want for that column (Equipment in this example).	 Control Programs vav_ahu X Enter a control program name: Add Or select existing control programs: status_totalizer vav_ahu vav_zone □ Hide primary column in report Primary column header: Location

Table 3.54 Instructions to Create a Report in Vertiv™ Liebert® SiteScan™ Interface (continued)

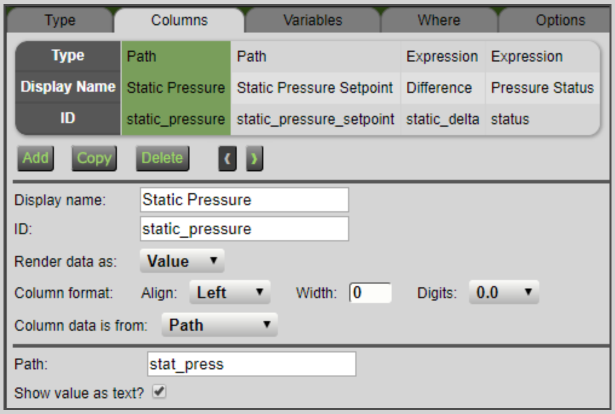
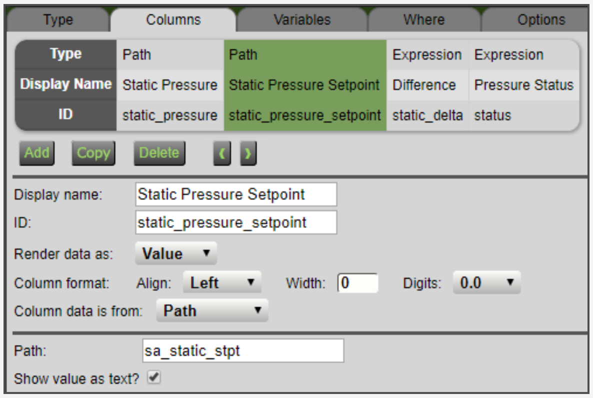
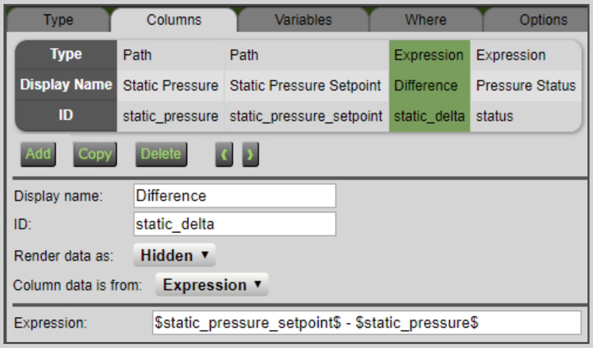
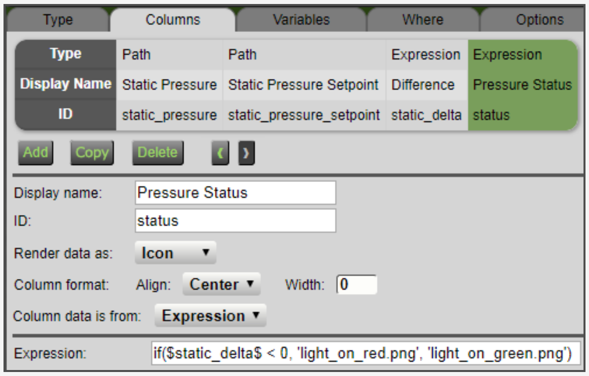
Instructions	Example
7. Define each column in the report on the Columns tab (Columns Tab on page 74). See the examples on the right. 8. Define any other information you may want, and then click *Accept*.	 Type | Path | Path | Expression | Expression Display Name | Static Pressure | Static Pressure Setpoint | Difference | Pressure Status ID | static_pressure | static_pressure_setpoint | static_delta | status Display name: Static Pressure ID: static_pressure Render data as: Value Column format: Align: Left Width: 0 Digits: 0.0 Column data is from: Path Path: stat_press Show value as text? ☑ Type Columns Variables Where Options Add Copy Delete

Table 3.54 Instructions to Create a Report in Vertiv™ Liebert® SiteScan™ Interface (continued)

Instructions	Example
	
	
	

Type	Path	Path	Expression	Expression
Display Name	Static Pressure	Static Pressure Setpoint	Difference	Pressure Status
ID	static_pressure	static_pressure_setpoint	static_delta	status

Display name: Static Pressure Setpoint

ID: static_pressure_setpoint

Render data as: Value

Column format: Align: Left Width: 0 Digits: 0.0

Column data is from: Path

Path: sa_static_stpt

Show value as text? ☑

Type	Path	Path	Expression	Expression
Display Name	Static Pressure	Static Pressure Setpoint	Difference	Pressure Status
ID	static_pressure	static_pressure_setpoint	static_delta	status

Display name: Difference

ID: static_delta

Render data as: Hidden

Column data is from: Expression

Expression: $static_pressure_setpoint$ - $static_pressure$

Type	Path	Path	Expression	Expression
Display Name	Static Pressure	Static Pressure Setpoint	Difference	Pressure Status
ID	static_pressure	static_pressure_setpoint	static_delta	status

Display name: Pressure Status

ID: status

Render data as: Icon

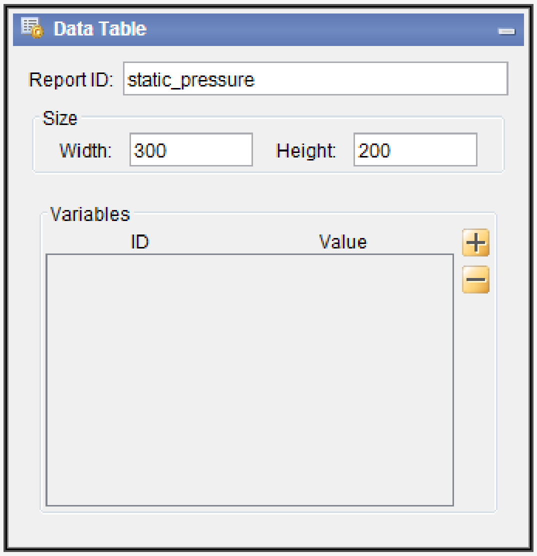
Column format: Align: Center Width: 0

Column data is from: Expression

Expression: if($static_delta$ < 0, 'light_on_red.png', 'light_on_green.png')

Creating the Graphic in ViewBuilder

Table 3.55 Instructions to Create a Graphic in ViewBuilder

Instructions	Example
1. Select *File* > *New* > *Graphic*, and then click *OK*.	
2. Click the *Add Control tab* ⚙+ in the Tools window. 3. Click the *Data Table control* and then click in the *workspace*.	
4. In the Properties window, enter the Report ID exactly as it appears in the Vertiv™ Liebert® SiteScan™ Report Editor. 5. Resize the control to at least the same size as the table in the Liebert® SiteScan™ interface. Enter a specific size in the Properties window or drag the handles on the control to resize it. **NOTE: Increase the size of the data table control in ViewBuilder if the table is cut off when viewing the graphic in the Liebert® SiteScan™ interface.** 6. If you defined variables in the Report Editor and you want to use a different default value for the Data Table, click ⊞ in the Properties window, type the variable's ID (from the Report Editor), and then type the new default value. **NOTE: To have the data table show data for a location other than the graphic's location, add a variable and type location in the ID column. Type the path to the location in the Value column.**	 Data Table Report ID: static_pressure Size Width: 300 Height: 200 Variables
7. Save the graphic.	

Referencing a Value in a Data Table

To reference the value of a cell in a data table, use one of these expressions:

- CELL::table ID,column ID,column ID=value
- CELL::table ID,column ID,numerical position in the column

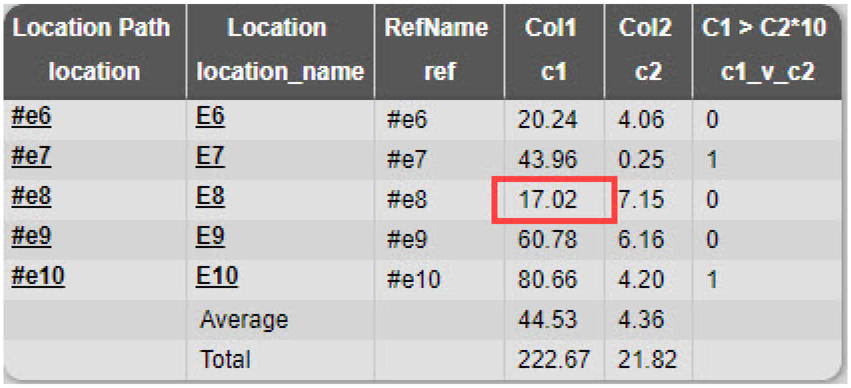
NOTE: The numerical position in the column can be positive if counting for the top or negative if coming from the bottom.

Examples

There are several methods to refer to the value of 17.02 in the table called "sample table" as shown in **Figure 3.25** on the next page :

- CELL::sample_table,c1,location=#e8
- CELL::sample_table,c1,ref=#e8
- CELL::sample_table,c1,3
- CELL::sample_table,c1,-5

Figure 3.25 Sample Table

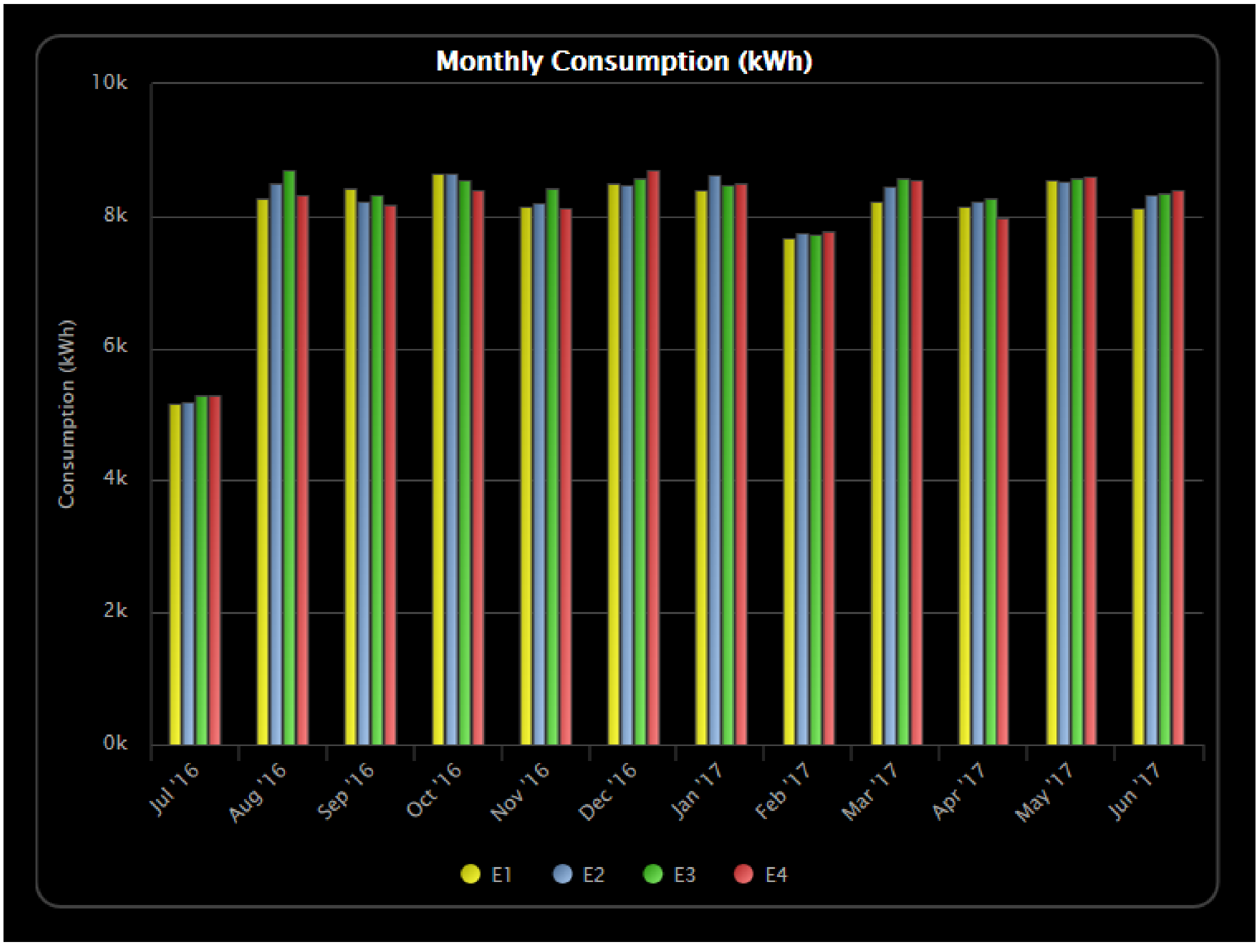


Location Path	Location	RefName	Col1	Col2	C1 > C2*10
location	location_name	ref	c1	c2	c1_v_c2
#e6	E6	#e6	20.24	4.06	0
#e7	E7	#e7	43.96	0.25	1
#e8	E8	#e8	17.02	7.15	0
#e9	E9	#e9	60.78	6.16	0
#e10	E10	#e10	80.66	4.20	1
	Average		44.53	4.36	
	Total		222.67	21.82	

Producing a Chart

To produce a bar chart as shown in Figure 3.26 below , first create the report in the Vertiv™ Liebert® SiteScan™ interface and then create the corresponding graphic in ViewBuilder.

Figure 3.26 Bar Chart for Mionthly Consumption



NOTE: When a chart that is based on a report is displayed on a Graphics page, you can hover over various points on the chart to see values. You can also click on each item in the legend to turn that information on and off. See "Using a custom report as the source for a Graphics page" in Vertiv™ Liebert® SiteScan™ Help for more information on a chart.

Creating the Report in the Liebert® SiteScan™ Interface

Table 3.56 Instructions to Create Report in the Vertiv™ Liebert® SiteScan™ Interface

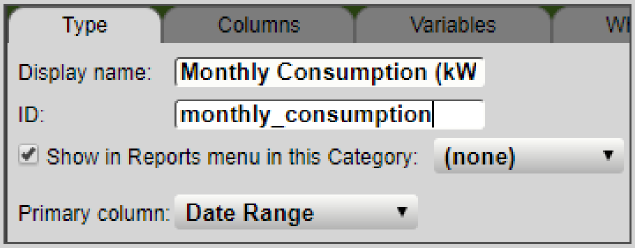
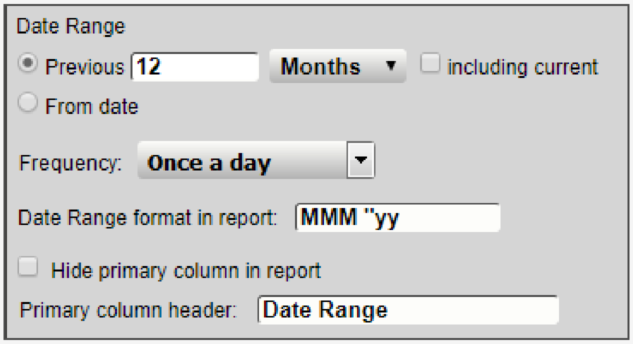
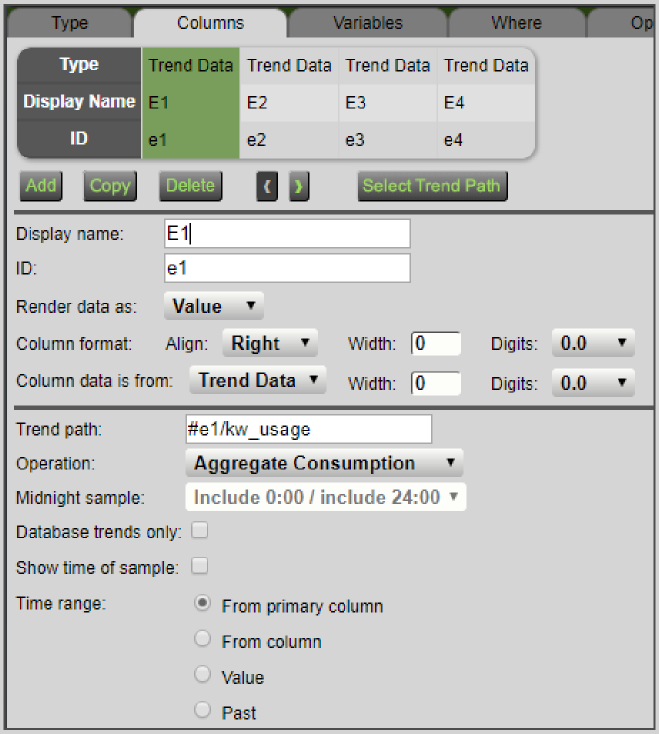
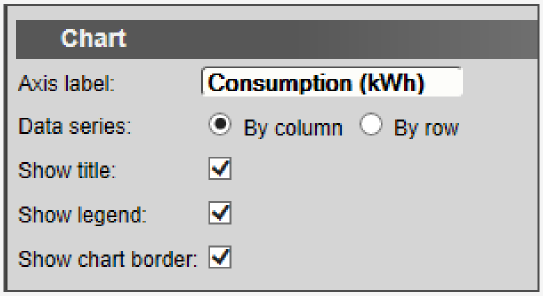
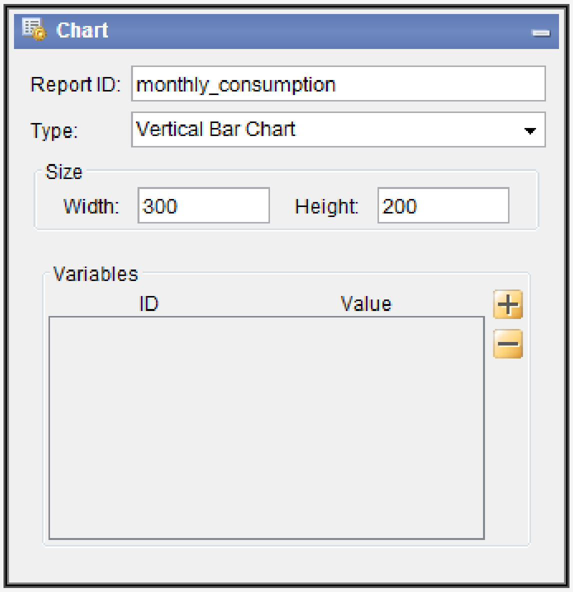
Instructions	Example
1. Click the *Reports drop down arrow*, and then select Report Manager.	
2. Click *Add*. 3. On the Type tab of Report Editor, type a Display name and ID for the report. 4. In the Primary column field, select the type of information that you want to report based on (Date Range in this example).	 Display name: Monthly Consumption (kW ID: monthly_consumption ☑ Show in Reports menu in this Category: (none) ▼ Primary column: Date Range ▼
5. On the Type tab (Type Tab on page 72), enter the criteria for the option that you selected in step 4 . 6. In the Primary column header field, enter the heading that you want for that column (Date Range in this example).	 Date Range ● Previous 12 Months ▼ □ including current ○ From date Frequency: Once a day ▼ Date Range format in report: MMM ''yy □ Hide primary column in report Primary column header: Date Range

Table 3.56 Instructions to Create Report in the Vertiv™ Liebert® SiteScan™ Interface (continued)

Instructions	Example
7. Define each column in the report on the Columns tab (Columns Tab on page 74). **NOTE: In the example to the right, all four columns have the same criteria.**	 Type | Columns | Variables | Where | Op Type: Trend Data | Trend Data | Trend Data | Trend Data Display Name: E1 | E2 | E3 | E4 ID: e1 | e2 | e3 | e4 Add | Copy | Delete | (|) | Select Trend Path Display name: E1 ID: e1 Render data as: Value Column format: Align: Right Width: 0 Digits: 0.0 Column data is from: Trend Data Width: 0 Digits: 0.0 Trend path: #e1/kw_usage Operation: Aggregate Consumption Midnight sample: Include 0:00 / include 24:00 Database trends only: □ Show time of sample: □ Time range: ● From primary column ○ From column ○ Value ○ Past
8. Define the Chart options on the Output tab (Output Tab on page 86). 9. Define any other information you may want, and then click Accept.	 Chart Axis label: Consumption (kWh) Data series: ● By column ○ By row Show title: ☑ Show legend: ☑ Show chart border: ☑

Creating the Graphic in ViewBuilder

Table 3.57 Instructions to Create a Graphic in ViewBuilder

Instructions	Example
1. Select *File > New > Graphic*, and then click *OK*.	
2. Click the *Add Control tab* in the Tools window. 3. Click the *Chart control* and then click in the *workspace*.	
4. In the Properties window, enter the Report ID exactly as it appears in the Vertiv™ Liebert® SiteScan™ Report Editor. 5. Select the Type of chart you want. 6. esize the control so that it is at least the size that the chart will be in the Liebert® SiteScan™ interface. To resize, enter a specific size in the Properties window or drag the handles on the control. **NOTE: Increase the size of the chart control in ViewBuilder if the chart is cut off when you view the graphic in the Liebert® SiteScan™ interface.** 7. If you defined variables in the Report Editor and you want to use a different default value for the chart, click in the Properties window, type the variable's ID (from the Report Editor), and then type the new default value. **NOTE: To have the chart show data for a location other than the location of the graphics, add a variable and type location in the ID column. Type the path to the location in the Value column.**	 Chart Report ID: monthly_consumption Type: Vertical Bar Chart Size Width: 300 Height: 200 Variables ID Value
8. Save the *graphic*.	

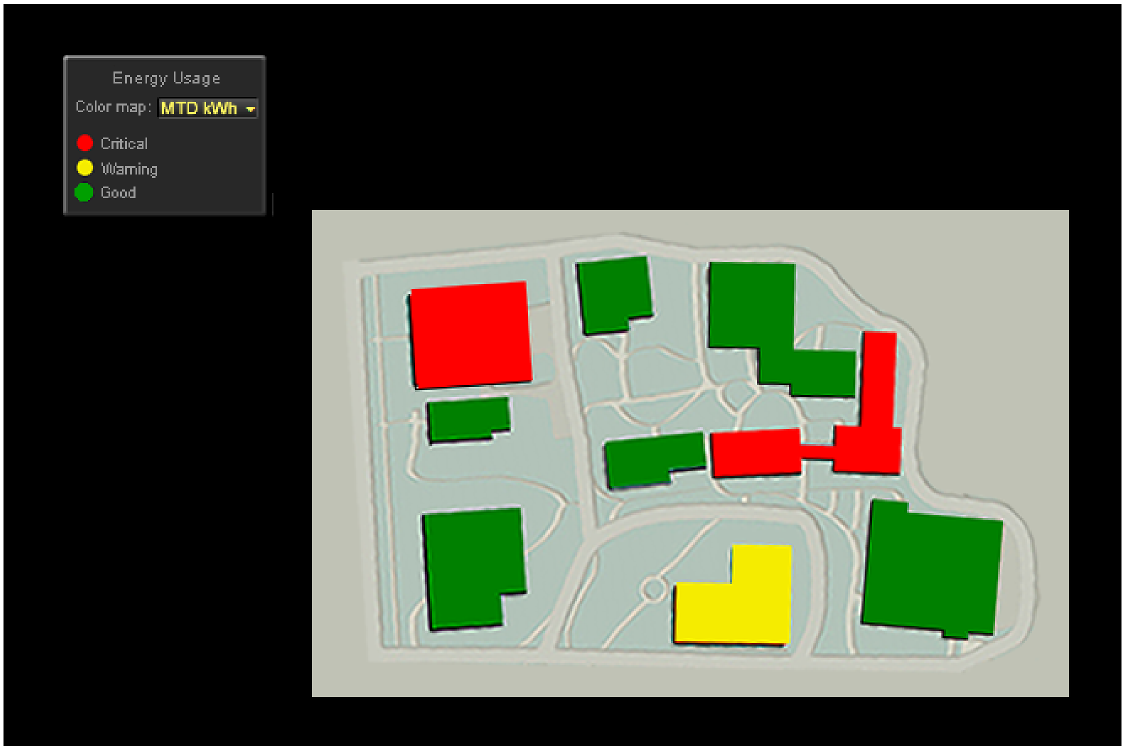
Producing a Color Map

A Graphics page color map shows specified colors for various conditions that are defined in a Vertiv™ Liebert® SiteScan™ report. For example, each building on a campus map could show a color that indicates its energy usage. See **Figure 3.27** below

.

A color map can also have an option that lets a user switch between different kinds of information. For example, in the image below, a user could click on the MTD kWh drop down list and select YTD kWh.

Figure 3.27 Graphics Page Color Map

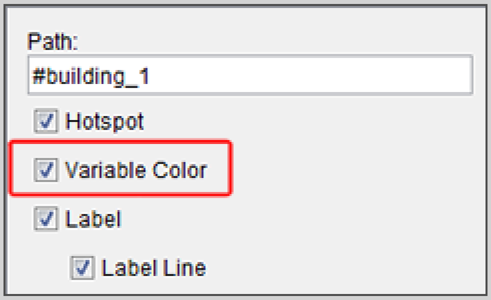


To produce a color map, follow the below steps::

1. Create the graphic in ViewBuilder.
2. Create the corresponding report in the Liebert® SiteScan™ interface.
3. Edit the graphic to add information specific to the Liebert® SiteScan™ report.

Create the Graphic in ViewBuilder

Table 3.58 Instructions to Create the Graphic in ViewBuilder

Instructions	Example
1. Add an image (floorplan, campus map, etc.) to the graphic, and then double click the image to open the Associations window.	
2. Associate each item on your image (zone, building, etc.) just as you would associate zones on a thermographic floorplan. See "Associating zones on a floorplan to equipment" in ViewBuilder Help. **NOTE: The Variable Color checkbox in the Associations window must be checked.** 3. Click *Save and Close.*	 Path: #building_1 ☑ Hotspot ☑ Variable Color ☑ Label ☑ Label Line

Create the Report in the Vertiv™ Liebert® SiteScan™ Interface

Table 3.59 Instructions to Create the Report in the Vertiv™ Liebert® SiteScan™ Interface

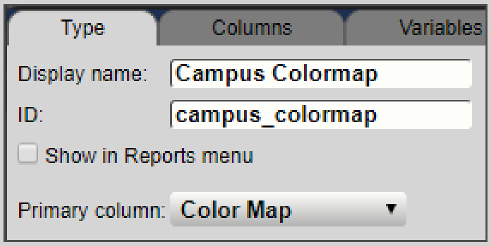
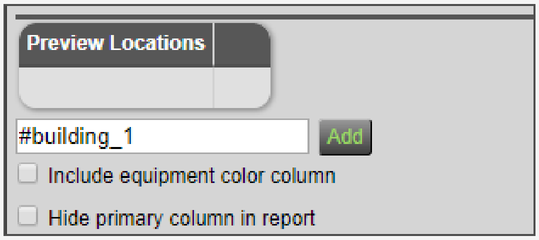
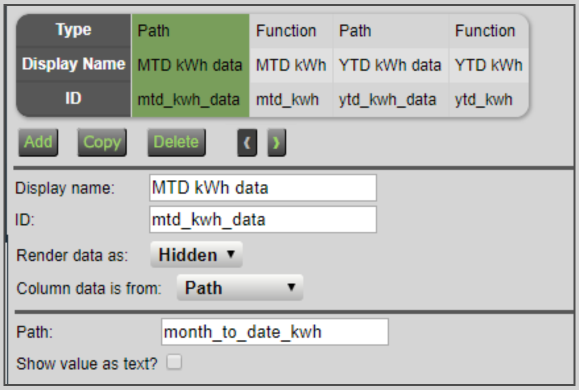
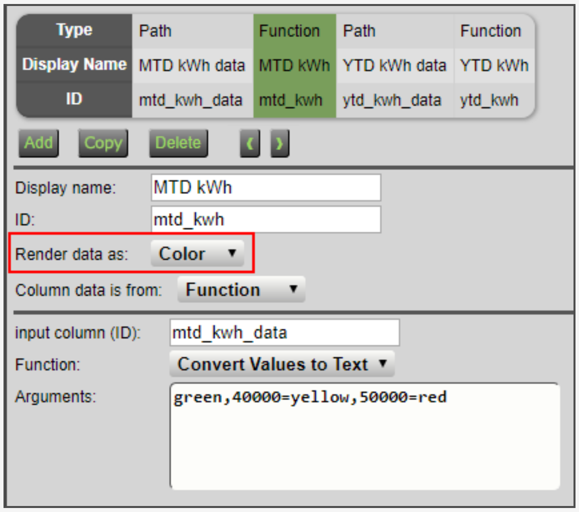
Instructions	Example
1. Click the *Reports drop down arrow*, and then select *Report Manager*.	
2. Click *Add*. 3. On the Type tab of Report Editor, type a *Display name* and *ID* for the report. 4. In the Primary column field, select *Color Map*.	 Display name: Campus Colormap ID: campus_colormap □ Show in Reports menu Primary column: Color Map ▾
5. Type a location in your system so that you can preview the report (#building_1 in the example). This location is only for testing your entries in the Report Editor. Associations to actual locations in the system will be made in ViewBuilder. **NOTE: You can add more than one location if you want to see more in the preview.** 6. Click Add. 7. Optional: Select Include equipment color column if you want to automatically include a column for Vertiv™ Liebert® SiteScan™ thermographic colors. **NOTE: You can see this column in the Preview section if you check Show all columns.**	 #building_1 □ Include equipment color column □ Hide primary column in report

Table 3.59 Instructions to Create the Report in the Vertiv™ Liebert® SiteScan™ Interface (continued)

Instructions	Example
8. Define each column in the report on the Columns tab (Columns Tab on page 74). See examples of the first two columns on the right.	 Type: Path, Function, Path, Function Display Name: MTD kWh data, MTD kWh, YTD kWh data, YTD kWh ID: mtd_kwh_data, mtd_kwh, ytd_kwh_data, ytd_kwh Display name: MTD kWh data ID: mtd_kwh_data Render data as: Hidden Column data is from: Path Path: month_to_date_kwh Show value as text? □
A color map can retrieve color information only from a column that has the Render data as field set to Color. 9. Define any other information needed on the Report Editor tabs, and then click Accept.	 Type: Path, Function, Path, Function Display Name: MTD kWh data, MTD kWh, YTD kWh data, YTD kWh ID: mtd_kwh_data, mtd_kwh, ytd_kwh_data, ytd_kwh Display name: MTD kWh ID: mtd_kwh Render data as: Color Column data is from: Function input column (ID): mtd_kwh_data Function: Convert Values to Text Arguments: green,40000=yellow,50000=red

Edit the Graphic in ViewBuilder to Add Report Information

Table 3.60 Instructions to Edit the Graphic in ViewBuilder to Add Report Information

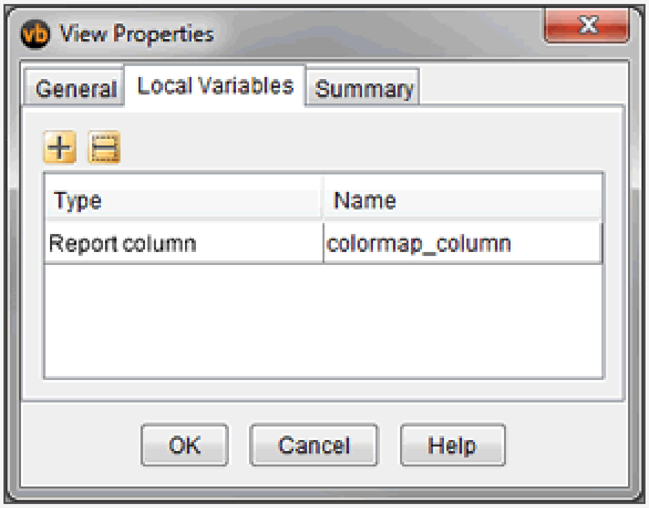
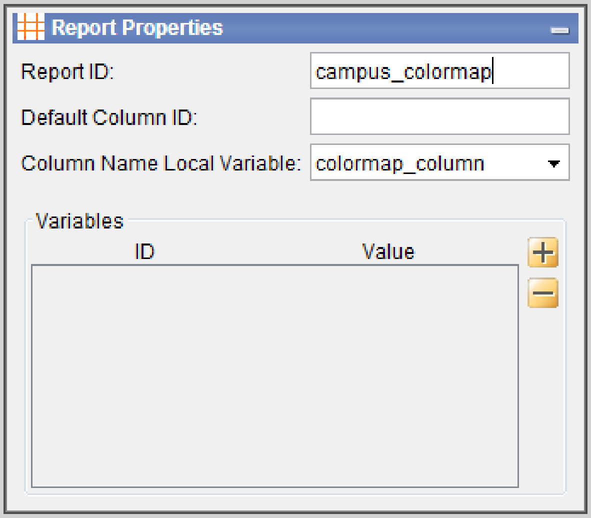
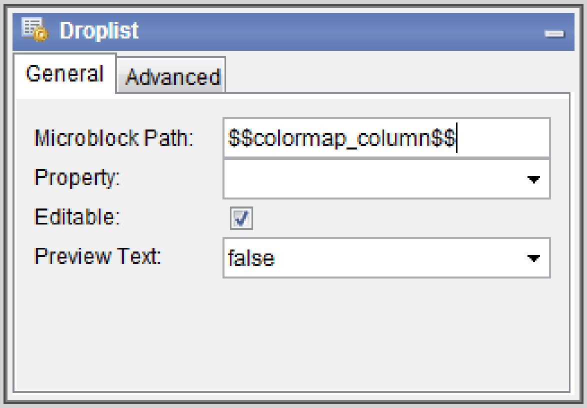
Instructions	Example
Follow Step 1 through Step 5 if the colormap will show information from more than one report column. If not, skip to step 6 . 1. Select *Configure > View Properties.* 2. On the Local Variables tab, click ⊞ . 3. Double-click Boolean in the Type column, and then select Report column in the drop-down list. 4. Double click variable in the Name column, and then replace variable with colormap_column. **NOTE: If the Graphic has multiple images that will pull data from different reports, add one variable called colormap_column1, another called colormap_column2, etc.** 5. Click *OK*.	 View Properties General Local Variables Summary OK Cancel Help Type: Report column Name: colormap_column
6. Double-click the image to open the Associations window. 7. Click ▦ , and then enter the following information: - Report ID: Get the report ID from the Vertiv™ Liebert® SiteScan™ Report Editor. - Default Column ID: This is the column whose color is displayed when the graphic first appears. Get the Column ID from the Liebert® SiteScan™ Report Editor. Leave blank if the graphic will pull data from only one report column. - Column Name Local Variable: Type the name of the variable that you created in Step 5 . Leave blank if the graphic will pull data from only one report column.	 Report ID: campus_colormap Default Column ID: Column Name Local Variable: colormap_column
8. If a report uses a variable and you want the colormap to use a different default value than what is defined in the Liebert® SiteScan™ Report Editor, click in the Report Properties window, type the variable's ID (defined in the Report Editor), and then type the new default value.	

Table 3.60 Instructions to Edit the Graphic in ViewBuilder to Add Report Information (continued)

Instructions	Example
9. If the colormap will show information from more than one report column, add a control (droplist or radio buttons) that will allow the user to select the information they want to see. 10. In the Microblock Path field, enter the local variable that you defined in Step 4 enclosing it in $$. 11. Finish the graphic and then test it in the Liebert® SiteScan™ interface.	 Droplist General / Advanced Microblock Path: $$colormap_column$$ Property: Editable: ☑ Preview Text: false

Troubleshooting Custom Reports

If a Graphics page contains a chart, data table, or color map that is retrieving information from a very large report, the graphic may be slow to load or refresh. You can do the following to improve this condition:

- Verify that your system follows the recommendations inVertiv™ Liebert® SiteScan™ v8.0 client, server, operating system, and database requirements.
- Reduce the size of the report by redefining the primary column criteria on the Type tab of Report Editor.
- Filter the report to show only a portion of the information. You can filter the report on the Options tab of Report Editor.
- Increase the refresh time (default is 30 seconds). If the chart, data table, or color map is based on information that changes infrequently, increase the refresh rate or set it to 0 to turn off refreshing. You can adjust the refresh rate on the Report Editor's Options tab.
- Reduce the number of controls on the graphic that are pulling data from different reports.

If an Invalid Report Definitions section appears at the bottom of the Report Manager page, one of the following has occurred:

- The file or file name of the report has been manually manipulated, invalidating the report's digital signature. Contact Technical Support to resolve this problem.
- The report is set up to have an addon supply content for the report, but the addon has not been installed in the Liebert® SiteScan™ interface. Install the addon to resolve this problem.

3.6.3 Creating a PDF, XLS, or CSV File

To create a PDF, XLS, or CSV file of the reports, see Table 3.61 below

Table 3.61 Create Output for Reports

Reports	Output	Notes
v7.0 custom reports	A PDF file A CSV file	
Preconfigured reports and v6.5 and earlier custom reports	A PDF file An XLS file A CSV file	For a v6.5 and earlier CVS file, you must enable *Support CSV text format* on the *Reports > Options* tab before you run the report.

To create a output a file, follow the below steps:

1. Run a *report*.
2. Click *PDF, XLS,* or *CSV* to download the file.

To Create a CSV File when Using Safari, follow the below steps:

1. Run a *report*.
2. Click *CSV*. A pop up displays the results.
3. Select *File* > *Save As*.
4. In the Format field, select *Page Source*.
5. Add the *.csv extension* to the file name.
6. Select the *save location* in the *Where* field.
7. Click *Save*.
8. Close the *popup*.

NOTE: If you need a digitally signed PDF to comply with 21 CFR Part 11, open it in a program that supports digital signatures, such as Adobe Acrobat, and sign it. The Vertiv™ Liebert® SiteScan™ application does not support digital signing because 21 CFR Part 11 requires that the signature be added manually, not through an automated process.

3.6.4 Scheduling Reports

You can schedule a report so that it runs on a recurring basis. The report is saved as a file (PDF, CSV, or XLS), and you can choose to have it automatically emailed to someone.

NOTE: To run a report, use the following alarm actions:

The Send E-mail alarm action (Send E-mail on page 46) can run any Liebert® SiteScan™ report and attach it to the email.

The Write to File alarm action (Write to File on page 53) can run any Liebert® SiteScan™ report and save it as a file. For both alarm actions, the report can be a PDF, HTML, XLS, or CSV file.

Scheduling a Report

1. Click the *Reports drop down arrow*, and then select the report that you want to schedule.
2. Click the *Schedule button*.
3. Enter the *information* in each field.

Table 3.62 Scheduling a Report Fields

Fields	Notes
Description	Enter a brief description of the report or how this schedule will be used.
Operator	The report will be run based on the selected operator's privileges.
Run report	Define when the report will run by selecting options in the drop down lists.
At __:__ __	Enter the time of day that you want the report to run.

Table 3.62 Scheduling a Report Fields (continued)

Fields	Notes
Save report as	v7.0 reports can be output as a PDF or CSV file. Preconfigured reports and v6.5 reports can also be output as an XLS file. Select the type of report file that you want. **NOTE: See Output Tab on page 86 for a description of the PDF options that are available in the Report Editor.**
Keep latest	Enter the number of files and Schedule History entries that you want to keep for this report. As a new file or entry is saved, the oldest one is deleted.
Email report	Enter the information needed to email the report each time it runs. **NOTE: For the Vertiv™ Liebert® SiteScan™ application to email a report, you must define the Email Server configuration on the System Settings > General tab (General Tab on page 199).**

4. Click *Accept*.

NOTE: The following reports have additional scheduling options available. Scheduling these reports without configuring schedule options results in an error; see View History in Managing Scheduled Reports below .

- Alarms > Alarms
- Security Reports > Location Audit Log
- Security Reports > System Audit Log

See Configuring Scheduled Alarms and Security Reports on page 70 .

Managing Scheduled Reports

Click the *Reports drop down arrow*, and then select *Scheduled Reports*. The Table 3.63 below shows any report that was scheduled to run.*

Table 3.63 Reports Scheduled to Run

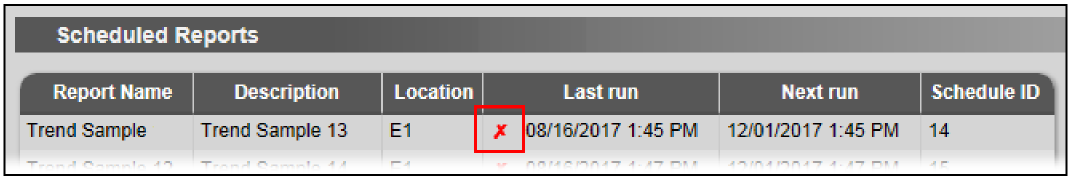
Select a Schedule and then Click	To
Edit	Change the schedule of the report in the Schedule Editor. You can also double click a schedule in the table to open the Schedule Editor.
View History	See when the report ran. Click *PDF*, *CSV*, or *XLS* in the Results column to download the report that was produced. **NOTE: The XLS option is not available for v7.0 custom reports.**
Delete	Remove the schedule. This removes its history and all associated files.

NOTE: You can also access this table by going to the System Configuration tree and selecting Scheduled Reports (*).

If a Report Fails

The table shown in Figure 3.28 below will show a red X and a system alarm will be generated.

Figure 3.28 Displaying Failed Report



Scheduled Reports

Report Name	Description	Location	Last run	Next run	Schedule ID
Trend Sample	Trend Sample 13	E1	✗ 08/16/2017 1:45 PM	12/01/2017 1:45 PM	14
Trend Sample 13	Trend Sample 14	E1	✗ 08/16/2017 1:47 PM	12/01/2017 1:47 PM	15

Select the schedule in the table above, and then click *View History*. Hold the cursor over the word *Failure* to see hover text describing what failed.

3.6.5 Working with Legacy (v6.5 and Earlier) Custom Reports

Although the Vertiv™ Liebert® SiteScan™ v7.0 interface has a new method of creating and managing reports, you can still create or edit the following reports that were available in Liebert® SiteScan™ v6.5 and earlier systems. These reports will be accessible from the *Reports* button drop down list, but not the Report Manager.

Table 3.64

Report	Allows to
Equipment Summary	View the following information for equipment at or below the location where the report was created: • Color • Active alarm • Locked values • Current value of selected points • Combined schedule See Creating an Equipment Summary Report below).
Equipment Values	Compare point information. See Creating an Equipment Values Report on the next page .
Trend Samples	View trend values for a particular time frame. See Creating a Trend Samples Report on page 110 .

NOTE: You can display icons and hover text on the Geographic 🌐 tree that show where custom reports have been created. See Tree Icons and Hover Text on page 9 .

You can schedule a report to run on a recurring basis. See Scheduling Reports on page 105 .

Creating an Equipment Summary Report

An Equipment Summary report can provide the following information for equipment at or below the location where the report is created.

- Color
- Active alarm
- Locked values
- Current value of selected points
- Effective schedule

To Create an Equipment Summary Report:

1. On the Geographic 🌐 tree, select the *location* where you want to view the report.
2. Click the *Reports button drop down arrow*, then select *Add Legacy Report.*
3. Select *Equipment Summary*.
4. Optional: Select a *Category*.

NOTE: The Category field is visible only if you have defined report categories. See Organizing Custom Reports by Category on page 90 .

5. Type a *name* for the report.

6. Click *Create*.
7. Define the *Title, Page Size and orientation*, and the Maximum number of rows.
8. Check or uncheck the *Optional Sections* checkboxes as needed.
9. Optional: Check *Include only specific control programs* at or below this location, then type the names of the control programs.
10. Select Available Points that you want to include in the report. Use *Ctrl+click, Shift+click, or both* to select multiple items.
11. Click *Add*.
12. Click *Accept*.
13. Click *Run*.

NOTE: To run this report later, go to the location where the report was created. Click the *Reports button drop down arrow*, select the report, then click *Run*.

Creating an Equipment Values Report

NOTE: To see if your system has this optional package, click ▾≡, then select *About*. You have this package if Enabled Features shows *Adv. Reporting*.

An Equipment Values report allows you to compare point information.

To Create an Equipment Values Report:

1. On the Geographic 🌐 tree, select the location where you want to view the report.
2. Click the *Reports button drop down arrow*, then select *Add Legacy Report*.
3. Select *Equipment Values*.
4. Optional: Select a *Category*.

NOTE: The Category drop down list is only visible if you have defined report categories. See Organizing Custom Reports by Category on page 90 .

5. Type a name for the report.
6. Click *Create*.
7. Do one of the following:
    - Select *Include only specific control programs at or below this location*, then type the control program names.
    - On the selection tree, select the pieces of equipment you want to view in the report. (Use *Ctrl+click, Shift+click,* or both to select multiple items.) Then click *Add*.
8. Optional: Check *Highlight alternate rows* to make the report easier to analyze.
9. Click *Next or* ▷ *next to Columns*.
10. Verify or change the report Title, Page units of measure for defining column widths, and Outer border characteristics.
11. Select a *column* in the report preview.

NOTE: The selected column is light blue.

12. Under Column Header, define how you want the column header to look.

13. Under Column Data, define the data you want in the column and how you want it to look. See table below.

NOTE: Select General from the Format drop-down list unless you want to define the number of places to the right of the decimal point for the displayed value.

14. Optional: Use the *Add, Delete, and arrow buttons* below the report preview to manipulate the columns.

15. Optional: Click ▶ *next to Page* to change the page size and orientation.

NOTE: Changing the size and orientation of the printed page also changes the report layout on the View tab.

16. Click *Accept*.
17. Click *Run*.

NOTE: To run this report later, go to the location where the report was created. Click the *Reports button drop down arrow*, select the report, then click *Run*.

Table 3.65

Type of Column Data	Description	
Point	Displays point data in the column.	
	Display	Select the property to show in this column.
	Data is named differently in some control programs	Select this checkbox if similar points have different names in different control programs. Then add each of the names to the Name to use list. For example, if a point is named Zone Temp in one control program and Zone Temperature in different control program, add both names to the list.
	Point to use	Select the name of the point to show in the column.
Trend Sample	Display	Select First, Minimum, Maximum, or Last recorded trend value.
	Data is named differently in some control programs	Select this checkbox if similar points have different names in different control programs. Then add each of the names to the Name to use list. For example, if a point is named Zone Temp in one control program and Zone Temperature in different control program, add both names to the list.
	Trend to use	Select the name of the point to show in the column.
	Set	Click to have all columns in the report use the same time range.
	Time Range	Select the time range to run the report for.
Trend Calculation	Display	Select the type of calculation to show in the column, Average or Total.
	Data is named differently in some control programs	Select this checkbox if similar points have different names in different control programs. Then add each of the names to the Name to use list. For example, if a point is named Zone Temp in one control program and Zone Temperature in different control program, add both names to the list.
	Trend to use	Select the name of the point to show in the column.
	Set	Click to have all columns in the report use the same time range.
	Time Range	Select the time range to run the report for.

Table 3.65 (continued)

Type of Column Data	Description	
Control Program	Display	Select Color, Display Name, Display Path, Notes, Prime Variable, or Reference Name to show in the column.
Expression	Data is named differently in some control programs	Select this checkbox if similar points have different names in different control programs. Then add each of the names to the Name to use list. For example, if a point is named Zone Temp in one control program and Zone Temperature in different control program, add both names to the list.
	Expression	Type the path relative to the current control program. The path must return a string value. Defining Vertiv™ Liebert® SiteScan™ Paths on page 135 for more information on paths. To display the Notes on an equipment's Properties page, type .notations in this field.

Creating a Trend Samples Report

NOTE: To see if your system has this optional package, click ▾☰, then select *About*. You have this package if Enabled Features shows *Adv. Reporting*.

A Trend Samples report provides trend values for a particular time frame.

To Create a Trend Samples Report:

1. On the Geographic 🌐 tree, select the location where you want to view the report.
2. Select the *Reports button drop down arrow*, then select Add Legacy Report.
3. Select *Trend Samples*.
4. Optional: Select a *Category*.

NOTE: The Category drop down list is only visible if you have defined report categories. See Organizing Custom Reports by Category on page 90 .

5. Type a *name* for the report.
6. Click *Create*.
7. Select a Time Range from the drop down list, then refine that option by selecting an option from the drop down lists to the right.
8. Define the *trend data*.

NOTE: Calculate values for missing samples calculates a value based on the 2 closest values to the time interval.

Find the closest sample displays the value closest to the time interval selected.

9. Optional: Check Highlight alternate rows to make the report easier to analyze.
10. Click *Next or* ▷ *next to Columns*.
11. Verify or change the report Title, Page units of measure for defining column widths, and Outer border characteristics.
12. Select a column in the report preview.

NOTE: The selected column is light purple.

13. Under Column Header, define how you want the column header to look.

14. Under Column Data, select the source of the trend data and how you want the data to look.

NOTE: Select General from the Format drop-down list unless you want to define the number of places to the right of the decimal point for the displayed value.

15. Optional: Use the *Add, Delete, and arrow buttons* below the report preview to manipulate the columns.
16. Optional: Click ▷ next to Page to change the page size and orientation.

NOTE: Changing the size and orientation of the printed page also changes the report layout on the View tab.

17. Click *Accept*.
18. Click *Run*.

NOTE: To run this report later, go to the location where the report was created. Click the *Reports button drop down arrow*, select the report, then click *Run*.

Saving the Design of v6.5 or Earlier Custom Report for Use in Another Location or System

You can save the design of an Equipment Values report or a Trend Samples report for reuse in another location or in another system. Or, you can create a library of different report designs to pull from as needed.

To save the design of report, follow the below steps:

1. Create the *Equipment Values* (Creating an Equipment Values Report on page 108) or Trend Samples (Creating a Trend Samples Report on the previous page) report.
2. On the Reports > Design tab, click the Save Report Design button. The design is saved to SiteScanx.x/webroot/<system>/Reports/<report name>.reportdesign.

NOTE: The .reportdesign file includes the report name. If you save multiple report designs in your system, each of those reports must have a unique name.

To use the report design at a different location in the system, follow the below steps:

1. Select the *location* in the Geographic 🌐 tree.
2. Select *Reports > Add Legacy Report*.
3. In Step 1 , select Report design, then select the report name in the drop-down list.
4. In Step 2 , type a *report Name*.
5. In Step 3 , click *Create*.

To copy individual report design files to another system, follow the below steps:

1. In Windows Explorer, go to the *SiteScanx.x/webroot/<system>/Reports/ folder*.
2. Copy the **.reportdesign files* that you want.
3. In the new system, paste the *copied files* in the SiteScanx.x/webroot/<system>/Reports/ folder.
4. Follow the steps above in "To use the report design at a different location in the system".

To create a .zip file to import into another system, follow the below steps:

NOTE: The import process will not import a file if it has the same name as a file in the other system. Make sure your file names are unique.

1. Do one of the following:

- Create *a .zip file* that contains the *.reportdesign files that you want. These files may be in the SiteScanx.x/webroot/<system>/Reports/ folder, or in a library that you created.
- On the System Settings > General tab, under Source Files, click *Export*.

NOTE: Export creates a .zip file that contains all of the system's source files (control programs, drivers, view files, touchscreen or BACview files, report design files).

2. In the new system, go to the System *Settings > General tab*.
3. Under Source Files, click *Import*.
4. Browse to the .zip file.
5. Click *Continue*.
6. Click *Close*. The Vertiv™ Liebert® SiteScan™ application will put the imported files in the correct folder.

Editing or Deleting a v6.5 or Earlier Custom Report

1. Select the *item* on the Geographic 🌐 tree where the report was created.
2. Click the *Reports button drop-down arrow*, then select the *report* you want to edit or delete.
3. Do one of the following on the Design tab:
   - Edit the *report*, then click *Accept*.
   - Click the *Delete Report button*, then click *OK*.

3.6.6 Semantic Tagging

Semantics tags and rules are included in the Vertiv™ Liebert® SiteScan™ v8.0 application to apply semantic meaning to locations in the system. You can use the tags that are included or create custom tags. You can assign tags to locations manually or by rules that are included or your custom rules. Once assigned, the locations can be selected by their semantic tags to use in reports, graphics, and ACxelerate Automated Commissioning Tool.

The Built in and Haystack tags are included in the Liebert® SiteScan™ v8.0 application and you cannot alter or delete them. The Built in rules cannot be modified but you can disable them. You can create custom tags and rules as needed.

The two kinds of tags are Marker and Value. The key difference is that Value tags also have a string value associated with them. You assign a Value tag to a location and specify the value. Value tags assigned by a rule have the same value assigned to each location.

On the Geographic 🌐 tree > Properties > Tags tab, you can:

- Assign *tags* manually to a selected location
- View *tags* that are assigned by a rule or manually for a location
- View *any microblocks* underneath an equipment location that have been tagged by a rule

On the System Configuration ⚙ tree > Semantics, you can:

- Search, add, delete, import, and export *custom tags*
- Search, enable, and disable the *Built in Rules*
- Search, add, delete, edit, import, and export *Custom Rules*

You can also use semantic tagging:

- In Reports > Report Manager, to create custom reports.
- In ViewBuilder, in place of microblock reference names for a path on a graphic.
- In the ACxelerate Automated Commissioning Tool

Manually Assigning Tags to a Location or Equipment

Tags are typically assigned using rules. The only way to assign a tag to a microblock is through a rule.

You can manually assign tags to an individual location area or equipment location from the Geographic 🌐 tree.

When selecting an equipment (control program) in the Geographic 🌐 tree > Properties > Tags tab, all tags currently assigned to that equipment are displayed. There may also be a Microblock Tags table to display the tags that are assigned from the Built-in or Custom rules.

Use the Search Tag/ID: field to find one or more specific tags. Type a word or phrase that is included in the Tag or the ID column of the tags you want to isolate in the table. For example, "cool". Click the Show All button to return to viewing the entire list.

1. On the Geographic 🌐 tree, select a location and go to Properties, or select an equipment and go to the Properties > Tags tab.
2. Click to expand the Assign Tags table. See column descriptions below.

NOTE: Click in any column heading to arrange the order of the tags alphabetically by that column. Click again to reverse the order.

3. Click + to the left of a tag in the Assign Tags table to assign it to your selection in the tree.

NOTE: You can assign an unlimited number of tags to a selection

You can assign a tag to more than one selection

To remove an assigned tag, click ✗ in the Assigned Tags table.

4. Click *Accept* when finished assigning tags.
5. Select *another location or equipment* in the Geographic tree 🌐and repeat the above steps until finished.

Table 3.66 Assign Tag Table

Column	
+	Click to add the tag to a location or equipment that you selected in the Geographic 🌐 tree.
Tag	Semantic tag name **NOTE: Tags beginning with ACx are available for the ACxelerate Automated Commissioning Tool to use.**
ID	Reference name

Table 3.66 Assign Tag Table (continued)

Column	
Value Tag	Displays a check mark for an item with a value. For example, the square feet in an area.
Namespace	• Built in - created specifically for the Vertiv™ Liebert® SiteScan™ v8.0 application • Haystack - an industry standard • Custom - created by the user
Description	An understandable explanation of the tag

Adding, Deleting, Importing, or Exporting Custom Tags

The System Configuration ⚙ tree > Semantics > Tags tab is for viewing and managing custom tags. Every tag in your system is included in the table.

Use the Search Tag/ID: field to find one or more specific tags. Type a word or phrase that is included in the Tag or the ID column of the tag(s) you want to isolate in the table. For example, "cool". Click the Show All button to return to viewing the entire list.

To add a custom tag, follow the below steps:

1. On the System Configuration ⚙ tree, click Semantics > Tags tab.
2. Click *Add* and enter the information shown in**Table 3.67** below

Table 3.67 Fields for Adding Custom Tags

Field	Enter the Information
Display Name	Semantic tag name - no limits or special rules for characters
ID	Reference name - (letters, numbers, underscores, and underscores only; no spaces or special characters)
Description	An understandable explanation of the tag
Value	Click the checkbox if the tag has a value

3. Click *Accept.*

To delete a custom tag, follow the below steps:

1. Select a *custom tag* in the Tags table by clicking anywhere in the tag's row.

NOTE: Use the Search Tag/ID: to easily locate a tag

You cannot delete Built in and Haystack tags

2. Click *Delete to remove* the tag.
3. Click *Accept*.

To import or export custom tags, follow the below steps:

- Click *Import Custom*, click in the Choose File field to browse to and select a .csv file you have saved from another Vertiv™ Liebert® SiteScan™ system. Click *Import*.
- Click *Export Custom* to create a .csv file that you can import into another Liebert® SiteScan™ system.

Adding, Deleting, Importing or Exporting Rules

Rules govern the semantic tags that are assigned to a location-based Reference Name or Equipment Name. To view and manage the Custom Rules and the Built-in Rules, go to the System Configuration ⚙ tree and select Semantics.

To search for specific tags in rules, built-in or custom, enter a word or words from the Tag Name in the Search Tags: field.

Built in Rules

All of the Built in Rules are included in the Vertiv™ Liebert® SiteScan™ application and all of them assign tags based on Reference Name of a microblock. On the System Configuration ⚙ tree, select Semantics > Built-in Rules tab. All Built-in Rules are enabled by default. Uncheck the Enabled checkbox to disable. They cannot be deleted or modified.

Custom Rules

The Liebert® SiteScan™ v8.0 application does not come equipped with custom rules. You can create your own or import them from anotherLiebert® SiteScan™ system. You can also enable, disable, delete, or export them.

To import or export, follow the below steps:

- Click *Import*, click in the Choose File field to browse to and select a .csv file you have saved from another Liebert® SiteScan™ system. Click Import.
- Click *Export* to create a .csv file that you can import into another Liebert® SiteScan™ system.

To add a new custom rule, follow the below steps:

1. On the System Configuration ⚙ tree > select Semantics > Custom Rules tab.
2. Click the *Add button* and follow the **Table 3.68** below :

Table 3.68 Fields for Adding a Custom Rule

Rule	Enter a Description
Enabled	Enabled by default. Uncheck to disable.
Type	Select: Control Program Name Matches for control programs. **NOTE: Using the control program names can save time by finding groups of equipment. or Reference Name Matches for matching the reference name of any location in the Geographic ⚙ tree: Areas, equipment, or microblocks.**
Names	Enter the *Control Program Names or Reference Names.* **NOTE: To locate a name, go to the Geographic tree, select the area or control program, right-click, and select Configure.** Control Program Name Matches Use ? (to match one letter) and * (to match any letters) for matching names. Separate additional names with a comma and no spaces. Reference Name Matches Use ? (to match one letter) and * (to match any letters) for matching names. You can match a partial path using /. For example, "vav*/zone_temp". Separate additional names with a comma and no spaces.

3. To assign a tag from the Available Tags table, click once anywhere in a row and it is immediately added to the Assigned Tags table.

NOTE: To narrow the list of tags, in the Search field, type a word or phrase that is included in the Tag name or the ID field (visible on the Tags tab).

4. Continue to add as many tags as necessary for that rule.
5. Click *Accept*.

To delete or modify tags in an existing custom rule, follow the below steps:

1. Select a *Rule* in the Rules table by clicking anywhere in the row.
2. Click the *Delete button* to remove the rule.
3. To assign a tag, see Step 3 .
4. To remove an assigned tag, click X in the Assigned Tags table.

3.7 Operator Access

Privileges control which parts of the Vertiv™ Liebert® SiteScan™ system an operator can access. Privileges also control what an operator can do and what he can change.

To set up operator access to your system, follow the below steps:

1. Log in to the Liebert® SiteScan™ application as the Administrator. See Operators and Operator Groups on page 120 .
2. Define privilege sets by job function. See Privilege Sets below .
3. Enter each operator in the system by assigning him privilege sets and entering settings that apply only to him. If you need to assign the same privilege set to multiple operators, you can create an operator group and assign the privilege set to the group. See Operators and Operator Groups on page 120

See Changing My Settings on page 122 change the settings of an operator.

To access the Liebert® SiteScan™ interface, an operator must enter his user name and password. See Advanced Password Policy on page 123 to change the rules for passwords.

Restricting Operator Access

To restrict access to your system, follow the below steps:

- Restrict the privileges of an operator.
- Use location dependent operator access (Location Dependent Operator Access on page 123)
- Change *Editing Privilege* of a microblock from *Preset* to a specific privilege. The properties of a microblock will be editable only by an operator that has that privilege.

CAUTION: Each microblock property has a default Editing Privilege (represented by the *Preset* option) that is appropriate for that property. Changing *Preset* to a specific privilege changes every property in the microblock to the same privilege which may produce undesirable results.

3.7.1 Privilege Sets

A privilege set is a group of one or more privileges (Privileges on the facing page). The Administrator creates privilege sets and assigns them to operators and operator groups.

Privileges

Table 3.69 Privilege

This Privilege	Allows an Operator
System Administration Privilege	• Add, edit, and delete operators, operator groups, and privilege sets. • Update the Liebert® SiteScan™ system with service packs and patches. • Register the Liebert® SiteScan™ software. See Registering Your Liebert® SiteScan™ Software on page 206 . • Enable and set up advanced security features such as location dependent operator access (Location Dependent Operator Access on page 123) and the advanced password policy (Advanced Password Policy on page 123). • ·Add and remove Liebert® SiteScan™ addons such as EnergyReports.

Table 3.70 Access Privilege

This Access Privilege	Allows an Operator to Access (But Not Edit)
Access Geographic Locations	Pages from the Geographic tree.
Access Network Items	Pages from the Network tree.
Access Groups	Pages from the Schedule Groups tree.
Access Config Items	Pages from the System Configuration tree.
Access Alarms	Alarms.
Access Logic Pages	Logic pages.
Access User Category 1-5	Anything in a category that has the same privilege assigned to it. See "To create a custom privilege" below.

Table 3.71 Parameter Privilege

This Parameter Privilege	Allows an Operator to Edit Properties such as
Edit Setpoint Parameters	Occupied and unoccupied heating and cooling setpoints.
Edit Setpoint Tuning Parameters	Demand level setpoint offsets, thermographic color band offsets, heating and cooling capacities and design temperatures, color hysteresis, and learning adaptive optimal start capacity adjustment values.
Edit Tuning and Logic Parameters	Gains, limits, trip points, hysteresis, color bandwidths, design temperatures, and optimal start/stop.
Edit Manual Override Parameters	Locks on input, output, and network points.
Edit Point Setup Parameters	Point number, type, range, and network source and destination.
Edit Restricted Parameters	Properties the installer restricted with this privilege.
Edit Category Assignments	Alarm, Graphic, Trend, and Report category assignments.
Edit History Value Reset	Elapsed active time and history resets, and runtime hours.
Edit Trend Parameters	Enable trend logging, log intervals, and log start/stop times.
Edit Calibration Parameters	Point calibration offsets.
Edit Hardware Controller Parameters	Driver properties.
Edit Critical Configuration	Critical properties the installer protected with this privilege.

Table 3.71 Parameter Privilege (continued)

This Parameter Privilege	Allows an Operator to Edit Properties such as
Edit Area Name	Area display names.
Edit Control Program Name	Control program display names.
Edit Alarm Configuration	Enabling/disabling alarms and editing alarm messages, actions, categories, and templates.
InterOp Privilege 1 - 10	Those protected by password levels 1-10 in SuperVision.

Table 3.72 Functional Privilege

This Functional Privilege	Allows an Operator to
Manage Alarm Messages and Actions	Add, edit, and delete alarm messages and actions.
Maintain System Parameters	Edit all properties on the *System Settings* page.
Maintain Schedules	Add, edit, delete, and download schedules.
Maintain Schedule Group Members	Add, edit, and delete schedule groups.
Maintain Categories	Add, edit, and delete categories.
Maintain Alarm Templates	Edit Alarm Template and Reporting Action Templates.
Acknowledge Non-Critical Alarms	Acknowledge all non-critical alarms.
Acknowledge Critical Alarms	Acknowledge all critical alarms.
Force Normal Non-Critical Alarms	Force non-critical alarms to return to normal.
Force Normal Critical Alarms	Force critical alarms to return to normal.
Delete Non-Critical Alarms	Delete non-critical alarms.
Delete Critical Alarms	Delete critical alarms.
Execute Audit Log Report	Run the *Location Audit Log* and *System Audit Log* reports.
Download Controllers	Mark equipment for download and initiate a download.
System Shutdown	Issue the Shutdown manual command that shuts down the Vertiv™ Liebert® SiteScan™ Server application.
Engineer System	• Log in and make database changes in SiteBuilder. • Use the copy, notify, reload, and revert manual commands. • Access the *Configure* and *Set up Tree* right-click menus in the Liebert® SiteScan™ interface. • Add text in the *Notes* field on an equipment's Properties page of an equipment.
Access Commissioning Tools	Access: • Equipment Checkout • Airflow Configuration • Trend, Report, and Graphic categories that require this privilege • Discovery tool
Maintain Graphs and Reports	Add, edit, and delete trend graphs and reports.
Maintain Connections	Edit *Connections* page properties.
Remote File Management	Access files using a WebDAV utility.
Remote Data Access-SOAP	Retrieve Liebert® SiteScan™ data through an Enterprise Data Exchange (SOAP) application.

Table 3.72 Functional Privilege (continued)

This Functional Privilege	Allows an Operator to
Do not audit changes made using SOAP (Web services)	Not have his SOAP (web services) changes recorded in the Audit Log.
Manual Commands/Console Operations	Access the manual command dialog box and issue basic manual commands.
Manual Commands/File IO	Execute manual commands that access the server's file system.
Manual Commands/Adv Network	Execute manual commands that directly access network communications.
Manual Commands/Unrestricted	Execute manual commands that bypass all safeguards and may cause unpredictable results if used incorrectly.
Change My Settings	Edit his preferences on the *My Settings* page.

Creating a Custom Privilege

You can assign a privilege to a Graphic, Property, Trend, or Report category so that only operators with that privilege can access the category. You can assign a category privilege on the page where you create or edit categories.

If all the other privileges are too widely used to accomplish the results you want, you can assign one of the five Access User Category privileges to the operators and category.

For example, your system has 2 graphics categories, HVAC and Lighting/Security. You want HVAC technicians to see only the HVAC graphics and security personnel to see only the Lighting/Security graphics. To do this, see **Table 3.73** below :

Table 3.73

Assign	To	Results
Access User Category 1	HVAC graphics category and HVAC technicians only	The security personnel cannot see the HVAC graphics because they do not have Access User Category 1.
Access User Category 2	Lighting/Security Graphics category and Security personnel only	The HVAC technicians cannot see the Lighting/Security graphics because they do not have Access User Category 2.

Adding or Editing a Privilege Set

1. On the System Configuration tree, select Privilege Sets.
2. Click *Add* to create a new privilege set, or select a privilege set to edit.
3. Type the *Name* and *Reference Name* for the privilege set.
4. Check each privilege (Privileges on page 117) that you want to include in the privilege set.
5. Click *Accept*.

CAUTION: Include all required access privileges in a privilege set. For example, if you add Acknowledge Non-Critical Alarms to a privilege set, also add Access Alarms to that privilege set.

NOTE: To create a privilege set that is similar to an existing set, select the existing set, then click *Add*. The privileges that are initially selected are identical to those of the existing set (Location independent security only).

Deleting a Privilege Set

1. On the System Configuration tree, select Privilege Sets.

2. Select the privilege set to be deleted.
3. Click *Delete*.
4. Click *OK*.
5. Click *Accept*.

3.7.2 Operators and Operator Groups

When you create a new system in SiteBuilder, you assign a login name and password to the administrator operator. This administrator operator sets up each operator in the Vertiv™ Liebert® SiteScan™ interface by entering the necessary settings and assigning one or more privilege sets (Privilege Sets on page 116) to the operator.

Operator groups give you the ability to assign privilege sets to a group of operators instead of the individual operators. Operator groups are useful if you have multiple operators who need the same privilege set or you have positions with high turnover rates. You can assign an operator to a group when you enter the operator or when you create the operator group.

NOTE: When using hierarchical servers, you must create identical operators on each server in order to navigate across servers.

⚠ **CAUTION: Passwords can be forgotten. To ensure access to the Liebert® SiteScan™ administrative functions, assign the Admin privilege set to at least 2 operators.**

Adding or Editing an Operator

1. On the System Configuration tree, select *Operators*.
2. Click *Add* to enter a new operator, or select an *operator* to edit his settings.
3. Enter information on this page as needed. See Table 3.74 below .
4. Click *Accept*.

Table 3.74

Field	Notes
Login Name	The name the operator must type to log in to the system. This name must be unique within the system.
Change password	Enable this field, then type the current and new passwords. **NOTE: An operator can change his password on the My Settings page (Changing My Settings on page 122).**
Force User to Change Password at login?	Forces the operator to change his password immediately after his next login. **NOTE: Use this field with the Change Password field to create a temporary password that the operator must change after his next login.**
Exempt From Password Policy	If *Use advanced password policy* is enabled on the *System Settings > Security* tab (Security Tab on page 201), select this option if you do not want the policy to apply to this operator.
Logoff options	If *Log off operators after __ of inactivity* is enabled on the *System Settings > Security* tab (Security Tab on page 201), select one of the 3 logoff options.

Table 3.74 (continued)

Field	Notes
Personal Information	You can enter contact information for this operator. **NOTE: An operator can enter contact information on the My Settings page (Changing My Settings on the next page).**
Starting Location and Starting Page	The Liebert® SiteScan™ location and page that will be displayed after the operator logs in.
System-wide Privilege Sets	Select the privilege sets that you want to assign to the operator. The *Effective System-wide Privileges* list show which privileges the operator will have. **NOTE: Click Show current privileges only to see only the selected privilege sets and privileges.** **NOTE: A grayed out privilege set with a group name beside it indicates the operator is inheriting that privilege set from the group.**

NOTE: To test the settings and privileges that you gave to an operator, you can open a second browser session on your computer and log in as the operator. For instructions on opening a second session in the browser you are using, see Setting up and using a web browser to view the Vertiv™ Liebert® SiteScan™ interface (Setting Up and Using a Web Browser to View the Vertiv™ Liebert® SiteScan™ Interface on page 195).

Deleting an Operator

1. On the System Configuration tree, select Operators.
2. Select the operator.
3. Click *Delete*.
4. Click *Accept*.

Adding or Editing an Operator Group

1. On the System Configuration tree, select Operator Groups.
2. Click *Add* to create a new operator group, or select an operator group to edit it.
3. Type the *Display Name* and *Reference Name* for the operator group.
4. Under *Members*, select the operators and/or groups that you want to add to the new group.
5. Under *Privilege Sets*, select the privilege sets (Privilege Sets on page 116) that you want to assign to the new group.

NOTE: To see what privileges are included in a privilege set, go to the *Privilege Sets* page and then select the privilege set in the table.

6. Click *Accept*.

NOTE: Every operator is automatically a member of a permanent default group called *Everybody*. You can assign privilege sets to this group.

Deleting an Operator Group

1. On the System Configuration tree, select Operator Groups.
2. Select the operator group.
3. Click *Delete*.

4. Click *Accept*.

CAUTION: When you delete an operator group, its individual members lose the privilege sets that were assigned to the group.

3.7.3 Changing My Settings

On the *My Settings* page, you can change settings, such as your:

- Password
- Viewing preferences
- Contact information

NOTE: The System Administrator can also change these settings on the Operators page.

To change your settings, follow the below steps:

1. On the System Configuration ⚙ tree, select *My Settings*.
2. Make changes on the *Settings* or *Contact Info* tab. See Table 3.75 below .
3. Click *Accept*.

Table 3.75 Fields for Changing Settings

Field	Notes
Change password	Enable this field, then type your current and new passwords.
Starting Location and Starting Page	The Vertiv™ Liebert® SiteScan™ location and page that will be displayed after you log in.
Language	The language and formatting conventions you want to see in the Liebert® SiteScan™ interface. **NOTE: If you will be using a language other than English, see Setting up a System for Non English Languages on page 213 for additional requirements.** **NOTE: If support for your selected language is removed in SiteBuilder, the Liebert® SiteScan™ application will automatically assign the System language to you.**
Automatically collapse trees	Expands only one tree branch at a time.
Automatically download schedules on each change	Select to automatically download all new schedules that you create and schedules that you change.
Play sound at browser when server receives	Check *Non critical alarms* or *Critical alarms* if you want the system to audibly notify you when that type of alarm is received. You can specify a different sound file. • Internet Explorer, Firefox, and Safari support .wav, .mp3, or .au files. • Google Chrome supports .wav or .mp3 files. 1. Put your file in the webroot_common\lvl5\sounds folder. 2. In the Sound File field, replace normal_alarm.wav or critical_alarm.wav with the name of your sound file. **NOTE: You can put your sound file anywhere under the SiteScanx.x folder, but you must change the path in the Sound File field.**

3.7.4 Advanced Password Policy

You can set up a Liebert® SiteScan™ password policy to meet your security needs.

1. On the System Configuration ⚙ tree, select *System Settings*.
2. On the *Security* tab under *Operators*, enter information in the fields described Table 3.76 below .

NOTE: See System Settings on page 199 for information on all the other fields.

Table 3.76 Fields for Advanced Password Policy

Field	Notes
Use advanced password policy	Enable this field to put restrictions on passwords. Login name and password of an operator must be different when this policy is enabled. After you change the password policy, any operator whose password doesn't meet the new requirements will not be locked out of the system, but will be prompted to create a new password.
Passwords must contain	You can specify how many characters and which of the following types of characters a password must contain: • Numbers • Special characters—any keyboard character that is not a number or letter. • Letters—uppercase, lowercase, or both.
Cannot be changed more than once every __ days.	Enter a number to limit how often users can change their passwords. When set to 0, users can change them as often as they want.
May not be reused until __ different passwords are used.	Enter a number between 1 and 20. Enter 0 to reuse passwords without a delay.
Expire after __ days	Enable to set the number of days an operator can use his password before the system requires him to change it. Enter a number between 1 and 999.
Force expiration	Click this button to force every user's password to expire. Each user will be prompted to change their password when they next attempt to log in to the Vertiv™ Liebert® SiteScan™ interface.

NOTE: The Advanced password policy settings do not synchronize across hierarchical servers. You should set up each system with the same advanced password settings to avoid problems when navigating between the systems.

3.7.5 Location Dependent Operator Access

You can set up operator access to your system to be location-dependent. This type of operator access lets you assign privileges to an operator only at locations in the system where he needs them. For example, you could assign an operator mechanic privileges in one building in a system, view-only privileges in another building, and no privileges in a third building.

New and converted Liebert® SiteScan™ systems default to location-independent operator access in which an operator's privileges apply throughout the system. You should understand this type of operator access before switching to location dependent. See Operator Access on page 116 for more information on location-independent operator access.

NOTE: When using hierarchical servers, the security policy and privilege sets are local to each server, so you can have location independent security on one server but not on another.

Switching to Location Dependent Access

CAUTION: Create a backup of your system before you begin. Switching to location-dependent operator access changes the configuration of operators and privilege sets. If you need to revert to location-independent operator access, your previous configuration cannot be automatically restored.

CAUTION: If you change the policy after you create and assign privilege sets to operators, you may need to reconfigure your operators' privileges.

To switch to location dependent operator access, follow the below steps:

1. On the System Configuration ⚙ tree, select *System Settings*.
2. On the *Security* tab under *Security Policy*, click *Change Policy*.
3. Follow the on screen instructions.

Privileges and Privilege Sets

When using location dependent operator access, privileges are either system wide or local.

System wide privileges allow an operator to perform functions throughout the entire system, such as accessing the Configuration tree or performing a system shutdown.

Local privileges allow an operator to perform functions in a specific area of the system, such as editing setpoints or viewing alarms. Assigning any local privilege to an operator also allows him to change his password and set preferences on his My Settings (Changing My Settings on page 122) page.

You assign system-wide privileges to system-wide privilege sets and local privileges to local privilege sets. See **Table 3.77** on the facing page for planning which privileges to assign to a privilege set. For a description of each privilege, see Privileges on page 117).

Table 3.77 System Wide and Local Privileges

System Wide Privileges	Local Privileges
Access Groups	Access Geographic Locations
Access Config Items	Access Network Items
Maintain System Parameters	Access Alarms
Maintain Schedule Group Members	Access Logic Pages
Maintain Categories	Access User Category 1 - 5
Maintain Trends Display and Print Setup	Edit Setpoint Parameters
Maintain Alarm Templates	Edit Setpoint Tuning Parameters
Acknowledge Non-Critical Alarms	Edit Tuning and Logic Parameters
Acknowledge Critical Alarms	Edit Manual Override Parameters
Force Normal Non-Critical Alarms	Edit Point Setup Parameters
Force Normal Critical Alarms	Edit Restricted Parameters
Delete Non-Critical Alarms	Edit Category Assignments
Delete Critical Alarms	Edit History Value Reset
Execute Audit Log Report	Edit Trend Parameters
Download Controllers	Edit Calibration Parameters
System Shutdown	Edit Hardware Controller Parameters
Engineer System	Edit Critical Configuration
Access Commissioning Tools	Edit Area Name
Maintain Graphs and Reports	Edit Control Program Name
Maintain Connections	Edit Alarm Configuration
Remote File Management	InterOp Privilege 1 - 10
Remote Data Access-SOAP	Manage Alarm Messages and Actions
Do not audit changes made using SOAP (Web services)	Maintain Schedules
Manual Commands/Console Operations	
Manual Commands/File IO	
Manual Commands/Adv Network	
Manual Commands/Unrestricted	
Change My Settings	

NOTE: For an operator to add, edit, or delete schedule groups, he must have the system wide privilege Maintain Schedule Group Members. He must also have the local privileges Access Geographic Locations and Maintain Schedules at each location that is a member of the schedule group.

NOTE: If you switch to location-dependent operator access in a system that has operators and privileges set up, the Vertiv™ Liebert® SiteScan™ application splits any existing privilege set containing local and system wide privileges into 2 separate privilege sets - one local and one system wide. Operators' system wide privilege sets still apply throughout the system. The operators' local privilege sets are automatically assigned at the system level. You can then reassign the local privilege sets to the operators at the locations where they need them.

Adding a Privilege Set

Adding a privilege set using location dependent operator access is the same as using location independent operator access except that you must select whether you are adding a system wide or local privilege set. See Privilege Sets on page 116 .

Assigning Privilege Sets to an Operator

Assign a system wide privilege set to an operator on the Operators page in the same way you would assign privilege sets in a system using location independent operator access. See Operators and Operator Groups on page 120 .

Assign a local privilege set to an operator at locations on the Geographic or Network tree where he needs the privileges.

1. Select a location on the Geographic or Network tree.
2. Click *Privileges*.
3. On the *Configure* tab, click *Add*.
4. Select the operator or operator group.
5. Click *OK*.
6. Select the privilege sets that you want the operator to have.
7. Click *Accept*.

NOTE: You can display icons and hover text on the Geographic tree that show where privileges have been assigned. See Tree Icons and Hover Text on page 9 .

Deleting a Local Privilege Set Assignment

1. On the Geographic or Network tree, select the location where the assignment was made.
2. Click *Privileges*.
3. Select the assignment under *Privilege Set Assignments at this Level*.
4. Click *Delete*.
5. Click *Accept*.

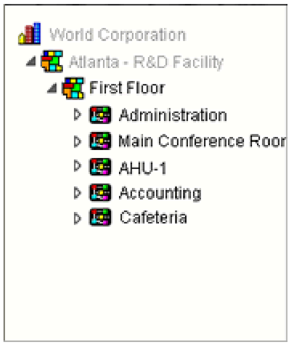
Restricting Access in the System

Restricting Access of an Operator to Areas of the System

You can give an operator access to only a specific area of the system. All other areas will be either grayed out or not visible when the operator logs in to the Vertiv™ Liebert® SiteScan™ interface.

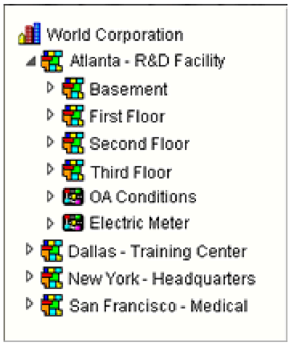
Example: If you give an operator the Access Geographic Locations privilege only at the first floor of the system shown below, he will see a navigation tree like the one on the left. The areas above the first floor are visible because he needs them to navigate to the first floor, but grayed out because he cannot access them. The operator does not see Dallas, New York, or San Francisco because he can't access them and does not need them to navigate.

Figure 3.29 Restricted Access



World Corporation
Atlanta - R&D Facility
First Floor
Administration
Main Conference Roor
AHU-1
Accounting
Cafeteria

Figure 3.30 Full System Access



World Corporation
Atlanta - R&D Facility
Basement
First Floor
Second Floor
Third Floor
OA Conditions
Electric Meter
Dallas - Training Center
New York - Headquarters
San Francisco - Medical

Restricting All Operator Access to a Location

To remove all local privileges of all operators from a location so that you can assign access only to a specific operators, navigate to the location, select *Privileges*, then uncheck *Inherit security privileges from above this level.*

Security Assignments Report

A Security Assignments Report shows local and system-wide privileges and privilege setsof an operator at a specific location.

1. Select the location on the Geographic or Network tree.
2. Click the *Reports* button drop down arrow, then select *Security > Security Assignments*.
3. On the *Options* tab, select an operator.
4. Click *Run*.

Recording Reasons for Edits (21 CFR Part 11)

Vertiv™ Liebert® SiteScan™ provides support for 21 CFR Part 11. The Liebert® SiteScan™ application can require an operator to record a reason for changing an equipment property, or acknowledging an alarm, before it accepts the change. The Liebert® SiteScan™ Audit Log report then displays the operator's name and the recorded reason for making the change.

To set up equipment to require reasons for changes, follow the below steps:

1. On the Liebert® SiteScan™ Geographic or Network tree, right click the equipment, then select Configure.

2. Check *Require operator to record any changes to control program and when acknowledging alarms.*

NOTE: In order to enable this feature to record changes, you must also enable *Alarm requires acknowledgment* and/or *Return requires acknowledgment*. See Setting Up, Editting, or Disabling Alarm Sources on page 55).

3. Click *Accept.*

NOTE: You can also turn this setting on in SiteBuilder in the equipment's properties dialog box.

To view reasons for changing equipment properties, follow the below steps:

1. On the Liebert® SiteScan™ tree, select a piece of equipment that requires reasons for change.
2. Click the *Reports button drop-down arrow*, select *Security > Location Audit Log* or *System Audit Log*.
3. On the *Options* tab under *Display the following columns*, select the *Reason* checkbox.
4. Click *Run.*

3.8 Advanced Topics

3.8.1 Manual Commands

To run a manual command, follow the below steps:

1. Click , then select *Manual Command*.
2. Type the manual command in the dialog box, then click *OK*.

NOTE: *Ctrl+Shift+M* also opens the dialog box.

You must have the Manual Commands/Console Operations privilege to access the manual commands dialog box. The descriptions shown in Table 3.78 below notify you if you need an additional privilege to run the corresponding command.

Table 3.78 Description for Manual Commands

Command	Description
addon	Opens a dialog box where you can upload, start, stop, or remove an addon program.
arcnet	Run this command each time you plug a device, such as a laptop, into a controller using an ARCNET card. The arcnet command configures the Vertiv™ Liebert® SiteScan™ application to recognize your device as Liebert® SiteScan™ server. Run this command from the equipment, controller, or network level on the Network tree.
autopilot location	Displays the full path for the current location. You can copy and paste the path into Enter custom autopilot location of the Autopilot addon user interface. See the Autopilot User Guide for details.
bacnet bind show	Shows the selected device's current BACnet bindings.
bacnet bind clear	Clears the selected device's BACnet bindings so that they can be rediscovered.
bacnet showindex	Displays all files (file name, size, date) downloaded to the selected controller.
bbmd commands:	You must have the Manual Commands/Adv Network privilege to run bbmd commands.
bbmd read <IP address>	Reads the BBMD table of the controller at the given IP address. For example, to display the BBMD table in the BACnet device router at IP address 154.16.12.101, type: bbmd read 154.16.12.101
bbmd update <network number>	Selects BBMDs on the specified network and marks them for download. If no network is entered at the end of the command, all networks in the system are scanned. For example, if the network number is 888, type: bbmd update 888

Table 3.78 Description for Manual Commands (continued)

Command	Description
bbmd view <network number>	Views the list of BBMDs that have been selected for the network number at the end of the command. Assumes the update has been run. For example: bbmd view 888
bbmd viewall <network>	Displays all devices with auto-managed bbmd for network
bbmd write <table file> <IP address>	Writes the BBMD table into the controller at the given IP address. See Setting up BACnet Broadcast Management Devices (BBMDs) on page 154 and Setting up BBMDs through the Vertiv™ Liebert® SiteScan™ Interface on page 155). For example, to write the BBMD table in dallasbbmd.bdt into the BACnet device router at IP address 154.16.12.101, type: bbmd write dallasbbmd.bdt 154.16.12.101
bbmd clear <IP address>	Clears the BBMD for the specified controller. For example: bbmd clear 154.16.12.101
bbmd dump <network> <file>	Writes to a file the BBMD from the specified controller. For example: bbmd dump 888 dallasbbmd.bdt
bbmdFdr [active] [<connection>]	Returns information on which BBMD is active for FDR (no connection parameter gives information on all active connections)
checkurls	1. Finds all network point exp: expressions for the selected item on the Geographic or Network tree. 2. Converts the exp: expressions to bacnet:// equivalent expressions that the controllers use. 3. Compares the equivalent bacnet:// expressions to the bacnet:// expressions currently downloaded in the controllers. 4. Displays any mismatches.
checkurls -p	Does the same as checkurls, then adds any mismatches to the download queue as parameter downloads.
checkurls -v	Does the same as checkurls, but displays the exp: and bacnet:// expressions for all network points that were checked.
commstat	Gives a complete set of diagnostic information for all defined connections as well as information regarding all modems in the system.
copy	Displays a global copy utility that allows you to selectively copy trend graphs, custom reports and all editable properties from the selected equipment to other equipment in the system with the same control program.
download commands:	Each of these commands performs an immediate download to a controller for the selected control program, device, or driver.
download m	Downloads all content, including parameters, schedules, and BBMDs (if applicable).
download p	Downloads parameters only.
download s	Downloads schedules only.
go commands:	
go <refname or path>	Goes to the point in the system that is referenced. For example: go #oa_conditions or go vav_1/m28 See Defining Vertiv™ Liebert® SiteScan™ Paths on page 135 .
go ~net	Takes you from a piece of equipment on the Geographic tree to the same equipment on the Network tree.
go ~geo	Takes you from a piece of equipment on the Network tree to the same equipment on the Geographic tree.
go ~device	Takes you to the controller for a point or piece of equipment on the Network tree.

Table 3.78 Description for Manual Commands (continued)

Command	Description
go ~network	Takes you to the network the selected object's controller is associated to.
go -logicpopup <refname>	Goes to the microblock popup for the microblock that is referenced. You must run this command from the microblock's equipment of microblock in the navigation tree. For example: go -logicpopup lstat
go <device ID>	Goes to a device on the Network tree. For example, to go to device 301205 referenced in a dead module alarm, type: go 301205
go <device ID>/<object ID>	Goes to a device and object on the Geographic or Network tree. For example: go 300550/AI:3
go <object ID>	Goes to an object for the current device on the Geographic or Network tree. For example, if a module alarm reports a control program Locked I/O Alarm and references an error in program 11, click the link to go to the device, then go to the object by typing: go PRG:11
go <s.g.m.p>	(site, gateway, controller, program) Goes to the item that the s.g.m.p address references. Use this command for legacy equipment only. For example: go 2,1,4,1
localhost	Shows the IP address of the Vertiv™ Liebert® SiteScan™ server
logoffuser	Logs off a user (without warning the user). Type a whoson manual command to view the IDs of logged in operators, then type logoffuser x, where x is the user's ID.
markdownload commands:	These commands place the controller for the selected tree item on the list to download at a later time. The download list can be viewed at Network tree > Downloads.
markdownload	Marks for an All Content download, that includes parameters, schedules, and BBMDs (if applicable).
markdownload p	Marks for a Parameters download.
markdownload s	Marks for a Schedules download.
memory	Shows the amount of server memory allocated for the Liebert® SiteScan™ application and the amount being used.
memory -free	Releases unused server memory, then shows the Liebert® SiteScan™ memory usage before and after the release.
modstat commands:	These commands display a Modstat Obtaining a Modstat on page 161) report. **NOTE: It is not necessary to download a controller before running a Modstat on it. Binding takes place when you run the modstat.**
modstat	Displays status of the controller at the current location, including: • Hardware components of the device • Software components of the device • Error conditions that may exist in the device • Date and time the device is using
modstat 8:<device instance number>	Displays status for a specific controller in the IP network using the controller's ID. Your location in the system does not have to be the controller you are querying. For example: modstat 8:489202

Table 3.78 Description for Manual Commands (continued)

Command	Description
modstat mac:<network number>,<media type>:<mac address>	Displays a Modstat for a specific controller in the system using the controller's MAC address. Network number is the number of the network this controller is on as specified in SiteBuilder; media type is the type of network the controller is on; MAC address can be either the controller address or the IP address and depends on the controller's media type. For example: modstat mac:48161,ms/tp:2 or modstat mac:888,bacnet/ip: 172.16.101.119
notify	Sends a message to all operators currently logged in to the system. For example, "The server is going to shut down in 5 minutes. Please log off." To run this command, type: notify <your message>. The message must use only alphanumeric characters. You must have the Admin privilege set or the Engineer System privilege to run this command.
paramupload	Uploads parameters (editable properties) to the Liebert® SiteScan™ application from the equipment or driver at the current location and below. If you want to upload editable properties for all equipment on a floor, navigate to the floor level on the Geographic tree. If you want to do this for everything under a particular router, navigate to the router or the network on the Network tree. You must have the Manual Commands/Adv Network privilege to run this command.
ping	Ping to verify communication between to IP devices. You cannot ping devices on non-IP networks. To run this command type: ping <hostname> where <hostname> is the IP address or device name. For example: ping 192.168.168.1 (will ping the IP address 4 times)
rebootserver	Restarts the Vertiv™ Liebert® SiteScan™ Server application. You must log back in to the Liebert® SiteScan™ interface if you want to continue. You must have the System Shutdown privilege to run this command.
rebuild	Rebuilds a Properties page. If you make changes to control program property text in the EIKON application, navigate to a control program in the Liebert® SiteScan™ tree, and then run this command to see your changes.
reload	Reloads a control program. Use if you make changes to control program in the EIKON application. Reloading updates all instances of the control program throughout the system and marks the controller(s) for download. The Liebert® SiteScan™ application determines the type of download based on what changed in the control program. You must have the Engineer System privilege to run this command.
restartmodule	Restarts the current controller. You must have the Manual Commands/Adv Network privilege to run this command.
rnet here	Overrides the address configuration of the Rnet host controller to allow a subsequent All Content or Parameters download. Run this command if you experience communication problems with the controller because the controller's network number does not agree with SiteBuilder's network number. Run this command from a control program, device or driver.
revert	Resets the selected driver or control program to its default values.
setdefault	Sets the current page as the default view for the selected action button and the selected tree location. You must have the Engineer System privilege to run this command.
setgcm	Initializes any LANgate (gateway) from a converted SuperVision system. After downloading to the LANgate, run setgcm if you: • Added a controller to a CMnet where the address is set higher than any other address on the CMnet • Changed the 3-letter system name • Changed the Generate controller alarm after no communication for ___ minutes (dead module timeout value) on the System Settings page • Changed the site number in SiteBuilder (previously referred to as the line number) setgcm sends the following information from the Liebert® SiteScan™ database to the LANgate: • Maxnet (the highest addressed controller plus one) • 3-letter system name • Site number • Dead module timeout value

Table 3.78 Description for Manual Commands (continued)

Command	Description
	NOTE: You can send this command over network, direct or modem connections, but not over a direct network (access port). **In Supervision, the command set the workstation phone number in the LANgate. You must now type the LANgate's phone numbers on the LANgate's parameter pages.** **You must have the Manual Commands/Adv Network privilege to run this command.**
showhistory	Gives historical information on the system, such as when it was created and updated. You must have the Manual Commands/Unrestricted privilege to run this command.
shutdown	Shuts down the SiteScan Server application. This stops communication between the server and the client, but does not close any open Liebert® SiteScan™ pages. You must have the System Shutdown privilege to run this command.
sreview	Provides a Security Report that displays critical security compliance in your Liebert® SiteScan™ system. This includes: Web Server • SSL Mode: on or off or both • TLS in use: true or false (only displayed if SSL Mode is on) • TLS protocols: version number (only displayed if SSL Mode is on) • Allow unsigned addons: true or false • Allow SOAP over HTTP: true or false • Reads X-Forwarded-For Header: true or false Certificate · Self-signed certificate in use: true or false · Certificate issued by: Distinguished Name of the certificate signer · Certificate expired: true or false · Certificate not yet valid: true or false · Certificate expires: date and time the certificate becomes invalid Email • Secure SMTP enabled on email server: true or false Passwords • Password policy enforced: true or false Software Updates • Latest cumulative update applied: none or date You must have the Admin privilege to run this command.
storetrends	Uploads trend data from the controller(s) to the database for all equipment at and below the selected item on the Geographic 🌐 tree. This command stores trend data for points that have Trend Historian enabled.
timesync	Synchronizes the time on all controllers at the current location and below to the time on the server. Run this command only from a location on the Network 🖧 tree. **NOTE: For CMnet networks, executing a timesync on a controller sends the timesync to its gateway, and all the controllers under that gateway.** You must have the Manual Commands/Adv Network privilege to run this command.
updatedriver commands:	You must have the Engineer System privilege to run updatedriver commands.

Table 3.78 Description for Manual Commands (continued)

Command	Description
updatedriver	Updates the selected controller to the latest version of its driver.
updatedriver net	Updates the selected controller to the latest version of its driver and any other controllers on the same network that use that driver.
updatedriver all	Updates the selected controller to the latest version of its driver and all other controllers in the system that use that driver.
upgradejsp commands:	Upgrading to a v6.0 or later system automatically upgrades any .jsp graphics created inVertiv™ Liebert® SiteScan™ Extensions for FrontPage. If you edit one of the .jsp files after upgrade, you must run one of the following commands. These commands could take several minutes to complete. A message is displayed when finished.
upgradejsp <absolute path>	Use to update a single graphic. For example: c:\SiteScanx.x\webroot\<system>\graphics\lvl5\sitea\building1.jsp
upgradejsp <folder path>	Use to update all graphics in a folder. For example: c:\SiteScanx.x\webroot\<system>\graphics\lvl5\sitea
upgradejsp all	Use to update all graphics in c:\SiteScanx.x\webroot\<system>\graphics\lvl5
whereami	Displays the full path for the current location and gives the display and reference names of the action button, category, instance and tab. If the selected tree location differs from the location shown in the action pane (for example, a point trend page), whereami returns information on both locations. Use this command when you create links in ViewBuilder.
whoson	Shows the list of users currently logged in to the Vertiv™ Liebert® SiteScan™ system, the IP addresses from where they are logged on, what kind of interface they are using (for example, lvl5 for a web browser on a computer), and how long it has been since they have actively interfaced with the Liebert® SiteScan™ system.
zap	Restarts the current controller. You must have the Manual Commands/Adv Network privilege to run this command.

3.8.2 System Database Maintenance

You should perform the following system maintenance on a regular basis. See Safely Shutting Down the Liebert® SiteScan™ Application for Database Server Maintenance on page 135 before doing any maintenance on your database server.

Backing Up a System

The type of database your system uses determines the method you use to back up the system. In Liebert® SiteScan™, you can find the database type on the System Settings (System Settings on page 199) > General tab.

CAUTION: Do Not use SiteBuilder's Replicate feature to back up your database.

For Apache Derby or SQL Server Express

1. Shut down the SiteBuilder and SiteScan Server applications.
2. In the SiteScanx.x\webroot folder, copy your system folder.
3. Paste the copy to a new location.

NOTE: Zip the copy before transporting it over a network or to a CD.

For MySQL, MS SQL Server, Oracle, or PostGreSQL

1. Follow the instructions above to copy your system folder in SiteScanx.x\webroot.

2. Use the database management system's backup method. See Safely Shutting Down the Liebert® SiteScan™ Application for Database Server Maintenance on the facing page before doing any maintenance on your database server.

Compacting and Defragmenting

In a new Liebert® SiteScan™ system, the records in a database are contiguous. As records are added, deleted, and modified, the records become scattered in the database. This condition, called fragmentation, can slow down system performance and increase the database size. Compact the database to correct this situation.

The files on the server's hard drive can also become fragmented. Defragment the hard drive to correct this situation.

You should compact and defragment on a regular schedule such as once a month. But, you may need to do these more often, depending on how often the data or files change.

NOTE: Compacting a database may take several minutes to several hours, depending on its size.

To minimize the effects of fragmentation, you should maintain at least 20% free disk space on the server.

Compacting the Database

The following databases are compacted dynamically compacting occurs in the background when a database is open.

- MySQL
- MS SQL Server
- MS SQL Server Express
- Oracle
- PostGreSQL

Compacting a Derby Database:

1. Shut down the SiteBuilder and Vertiv™ Liebert® SiteScan™ Server applications.
2. Open the computer's Command Prompt application and type cd c:\SiteScanx.x, replacing x.x with your system version number.
3. Click *Enter*.
4. Type "Derby Compression Tool.exe" <system name>.
5. Click *Enter*.
6. When compacting finishes, close the command window.

Defragmenting the Hard Drive of Server

For all database types, use a defragmentation utility such as Windows® Disk Defragmenter.

NOTE: If you are using a single computer as both the Liebert® SiteScan™ server and the client, you must defragment the disk more often than the disk of a dedicated server especially if people access the Internet from this computer.

Minimizing the Database Size

The larger a database is, the less responsive it may become. Deleting closed alarm incident groups, expired schedules, and expired historical trends on a regular basis will reduce the database size. You can set up your Liebert® SiteScan™ application to automatically delete these. See "System Settings > Scheduled Tasks tab (Scheduled Tasks Tab on page 203)" in Liebert® SiteScan™ Help.

Safely Shutting Down the Liebert® SiteScan™ Application for Database Server Maintenance

Occasionally, the database server is shut down for maintenance or backups. If this is done without shutting down the Liebert® SiteScan™ Server first, the database may get locked and the Liebert® SiteScan™ application may not be able to reconnect.

1. Shut down the Liebert® SiteScan™ application.
2. Shut down the database server.
3. Perform the maintenance or repair needed on the server.
4. Restart the database server.
5. Restart the Liebert® SiteScan™ application.

To unlock a database, follow the below steps:

1. In SiteBuilder, click *File* > *Open* and *Select Database* to open your site. The following message appears The database appears to be in use by another application. Do you want to override the lock?
2. Click *Yes* to override the lock.
3. Log in to the site.
4. Exit *SiteBuilder*.
5. Start the Liebert® SiteScan™ Service.

3.8.3 Defining Vertiv™ Liebert® SiteScan™ Paths

A path tells the Liebert® SiteScan™ application the route through the system hierarchy to an item in the system. For example, a path tells the Liebert® SiteScan™ application where to find a microblock property value to display on a graphic or where to jump to when the operator clicks a link on a graphic.

You can use semantic tags as part of the path. See Using Semantic Tags in a Path on page 139 .

In ViewBuilder, you use paths in:

- Controls
- Links
- Conditional expressions

In Vertiv™ Liebert® SiteScan™, you use paths in:

- The source field code (Using Field Codes on page 62) in alarm actions and messages
- An Equipment Values report (Creating an Equipment Values Report on page 108)
- The go manual command (Manual Commands on page 128)
- Custom reports (Custom Reports on page 71)

You can do one of the following to get the path:

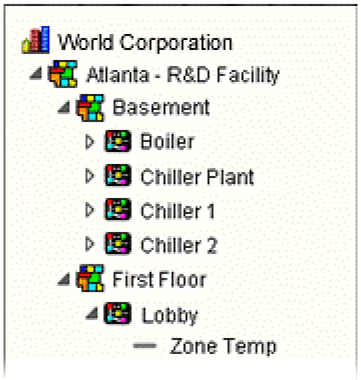
- In ViewBuilder, let ViewBuilder write the path or use Logic Graphics Properties that were defined in the EIKON application.
- In the Liebert® SiteScan™ interface, determine the path yourself (Determining a Path or Microblock Property on page 138).

A path consists of the reference name of each tree item included in the path, separated by a forward slash (/). For example, first_floor/zone_1/lstat.

A path can be absolute (Absolute Path on the next page) or relative (Relative Path on the next page).

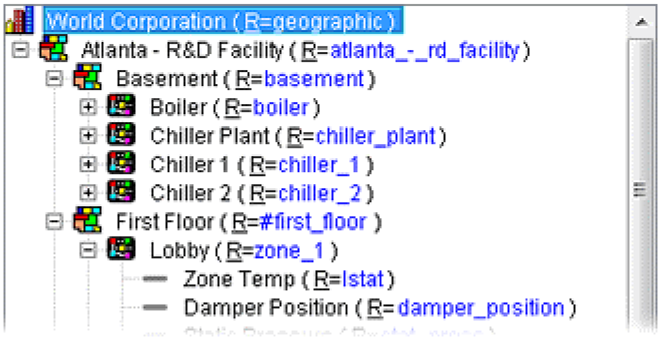
Liebert® SiteScan™ paths are based on parent-child hierarchy. In the tree below, the Lobby is a child of First Floor, and First Floor is a child of Atlanta R&D Facility. Conversely, Atlanta R&D Facility is the parent of First Floor, which is the parent of Lobby.

Figure 3.31 A System in the Liebert® SiteScan™ Interface



World Corporation
- Atlanta - R&D Facility
  - Basement
    - Boiler
    - Chiller Plant
    - Chiller 1
    - Chiller 2
  - First Floor
    - Lobby
      - Zone Temp

Figure 3.32 Same System in SiteBuilder Showing Reference Names in Blue



World Corporation (R=geographic)
- Atlanta - R&D Facility (R=atlanta_-_rd_facility)
  - Basement (R=basement)
    - Boiler (R=boiler)
    - Chiller Plant (R=chiller_plant)
    - Chiller 1 (R=chiller_1)
    - Chiller 2 (R=chiller_2)
  - First Floor (R=#first_floor)
    - Lobby (R=zone_1)
      - Zone Temp (R=lstat)
      - Damper Position (R=damper_position)

Absolute Path

An absolute path begins at a specific point in the system hierarchy and is followed by the children below it down to the object or property of interest. An absolute path can begin with either of the following:

- A global reference name a reference name that is unique within the entire system and begins with a # sign.

  Example: If OA Conditions has a global reference name of #oa_conditions, the absolute path to OA Conditions is simply #oa_conditions. The absolute path to any child of OA Conditions, such as OA Temperature, begins with #oa_conditions. For example, #oa_conditions/oa_temp.

- The top of the Vertiv™ Liebert® SiteScan™ tree

  Example: (using the system in the figure above) To display the Lobby's zone temperature on any graphic, the absolute path is /trees/geographic/atlanta_-_rd_facility/first_floor/zone_1/lstat.

Relative Path

A relative path is useful for items such as graphics or alarm messages that you will reuse in multiple Liebert® SiteScan™ locations because the path is relative to the item that contains the path.

A Relative Path Going Down the Tree

A relative path going down the tree begins with the reference name of the item below the location where the path is used. Examples using the system shown above:

- To display zone temperature of the Lobby on the Lobby graphic, the path is rs.
- To display zone temperature of the Lobby on the Atlanta-R&D Facility graphic, the path is first_floor/zone_1/rs.

A Relative Path Going Up the Tree

A relative path going up the tree begins with a ~ followed by one of the options shown in **Table 3.79** below :

Table 3.79

Use	To Go	Examples Using the System Shown Above
~parent	Up one level	1. To put a link on the Lobby graphic that goes to the First Floor graphic, the path is ~parent. 2. To put a link on the Lobby graphic that goes to the Atlanta R&D Facility (up 2 levels), the path is ~parent/~parent. 3. To display the Lobby's zone temperature on the Boiler graphic, the path is ~parent/~parent/ first_floor/zone_1/lstat/present_ value.
~equipment	To the control program of microblock	To display the Lobby zone temperature in a High Temp alarm message, the path is ~equipment/lstat/present_value.
~device	From a control program in the Geographic tree to its device in the Network tree.	To show the device name on an equipment graphic, use ~device.display-name.
~network	From a location in the Network tree up to its network (IP, ARCNET, etc.)	1. To show the network name on an equipment graphic, ~device/~network.display-name. 2. To show the network number on a dead module alarm, use the following field code and path: $source:~network.network-number$.
~geo	From a control program in the Network tree to the same item in the Geographic tree.	Use the manual command go ~geo.
~net	From a control program in the Geographic tree to the same item in the Network tree.	Use the manual command go ~net.

Relative Path to Heat, Cool, Demand, or Custom Source Values

To get a heat, cool, demand, or custom source value, use one of the following relative paths, replacing xxx with the reference name of the point you want to display and yyy with the reference name of a custom tree.

~heat/~parent/~geo/xxx

~cool/~parent/~geo/xxx

~dem/~parent/~geo/xxx

~changetree(yyy)/~parent/~geo/xxx

NOTE: You must do the following before you can display a source value using the above paths. In the EIKON application, configure Analog Status microblocks in the child control program for outgoing heat, cool, and run requests. Also configure Total, Minimum, and Maximum microblocks for the incoming requests in the parent control program. In SiteBuilder, assign your child equipment to its parent on the Heat Source or Cool Source tab.

Relative Path to Prime Variables and Thermographic Colors

- To get a prime variable, use the relative path ~prime. The control program must contain a Prime Variable microblock.
- To get a thermographic color, use the relative path ~color. The control program must contain a Setpoint or Set Color If True microblock

Determining a Path or Microblock Property

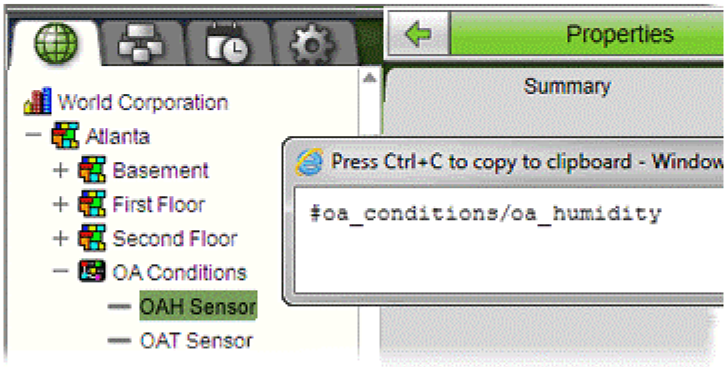
A path tells the Vertiv™ Liebert® SiteScan™ application the route through the system hierarchy to an item in the system. Paths are used in graphics, links, alarm messages, alarm actions, network microblock address, autopilot, and other items.

Getting the Path to an Area, Equipment, or Microblock

In the Liebert® SiteScan™ interface, right click the item on the tree, then select *Copy Path*. Paste the path where you need it.

Getting the Path to a Microblock Property Value

1. In the Liebert® SiteScan™ interface, right click the value, then select *Global Modify*.

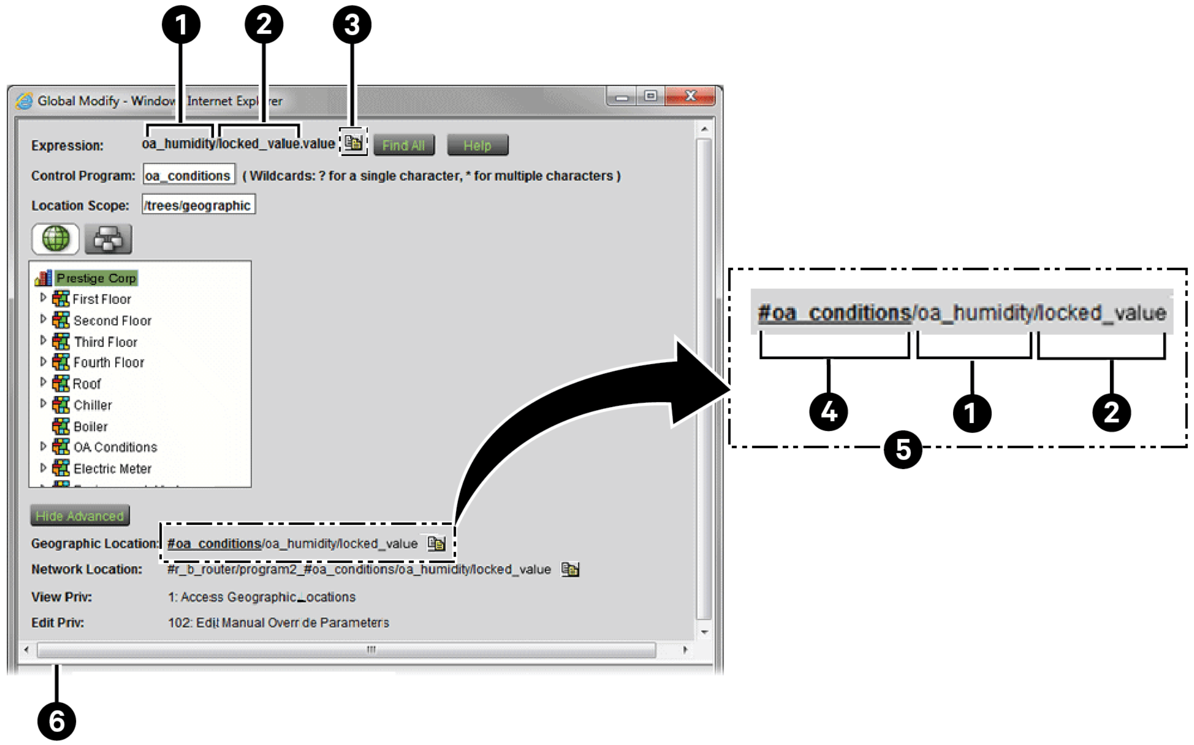


Press Ctrl+C to copy to clipboard - Window

```
#oa_conditions/oa_humidity
```

2. Click *Show Advanced* to see the full path to the property value and the Edit Privilege associated with the property.

Figure 3.33 Global Modify Window



Expression: oa_humidity/locked_value.value

Control Program: oa_conditions (Wildcards: ? for a single character, * for multiple characters)

Location Scope: /trees/geographic

Geographic Location: #oa_conditions/oa_humidity/locked_value

Network Location: #r_b_router/program2_#oa_conditions/oa_humidity/locked_value

View Priv: 1: Access Geographic Locations

Edit Priv: 102: Edit Manual Override Parameters

Item	Description
1	Microblock
2	Property
3	Copies expression to Windows Clipboard
4	Location
5	Full absolute Path
6	Click and drag this divider down to see the view and edit privileges

Using Semantic Tags in a Path

You can use a semantic tag in place of a reference name in paths. Follow the conventions in the table below to use them in the Vertiv™ Liebert® SiteScan™ v8.0 interface to set up custom reports and, in ViewBuilder, to use on graphics. See Semantic Tagging on page 112 in Liebert® SiteScan™ Help for details on assigning tags and the rules governing them.

Table 3.80

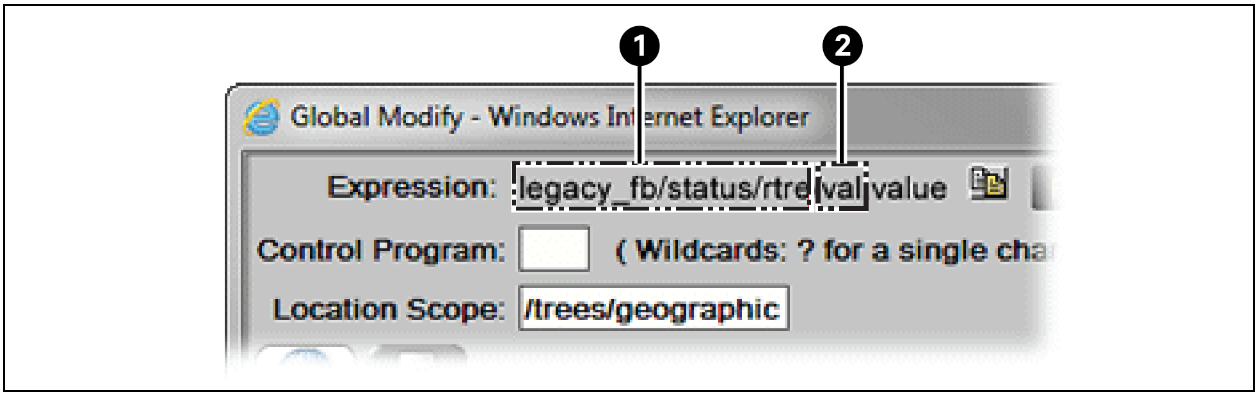
Function	Description
Specify a semantic tag	A tag is always preceded by "@" to differentiate it from a reference name.
Use multiple tags	"|" for ANY "&" for ALL Examples • @tag1|tag2|tag3 - find the first child tagged "tag1" OR "tag2" OR "tag3" (ANY tag) • @tag1&tag2&tag3 - find the first child tagged "tag1" AND "tag2" AND "tag3" (must have ALL tags) **NOTE: You cannot mix "|" and "&" in the same tag list.**
Search up	Search from the current location and up by prefixing the tag with "@up:". Example @up:tag1&tag2 - search up the tree, including the current location for a location with "tag1" AND tag2"
Search down	Search from the current location and down by prefixing the tag with with "@down:". This returns the first matching location. Example @down:tag1&tag2 - search down the tree, INCLUDING the current location for tags with "tag1" AND tag2"
Get a value	Value tags can be used like an attribute. Use the "@" tag name where an attribute would be specified. **NOTE: Like all attributes, you must precede the name with a period to obtain a value.** Examples • #floor1.@area • To search up for a location with an Area tag and get the Area tag value: @up:area.@area

Determining a Path or Microblock Property in a Converted SuperVision System

1. Follow the procedure in Determining a path or microblock property (Determining a Path or Microblock Property on page 138) to get the equipment path. For example, #o_a_conditions_1801.
2. Select the equipment on the Geographic tree.
3. Click *Properties*.
4. Alt+click the value that you want the path to.

In Global Modify, the Expression field shows the path to the microblock property.

Figure 3.34 Global Modify Window



Expression: legacy_fb/status/rtre/val/value

Control Program: (Wildcards: ? for a single cha

Location Scope: /trees/geographic

Item	Description
1	Microblock Path
2	Property

The full path of the microblock property is #o_a_conditions_1801/legacy_fb/status/rtre/val

NOTE: A status microblock does not have a property.

For a graphic to display a trend graph for a microblock property in a converted SuperVision system, type the microblock property path followed by /~trend in the trend graph control's Trend location field. To add a comparison trend graph, type the path followed by /~reports/<name of trend>.

This page intentionally left blank

4 Setting up and Configuring a Vertiv™ Liebert® SiteScan™ system

4.1 Setting up Networks

4.1.1 Setting up IP Network Communication

To set up an IP network:

1. Set the *IP addresses* of the controller. See Setting ExecB Device IP Addresses below and Setting a Custom IP Address of the Controller in SiteBuilder on page 145
2. Set up a BACnet/IP connection in the Liebert® SiteScan™ interface (See Setting up a BACnet/IP connection in the Vertiv™ Liebert® SiteScan™ interface on page 149)
3. Test the *server to client connections* (See Testing the Server to Client Connections on page 152)
4. Test the *server to controller connections* (See Testing the Server to Controller Connections on page 153)
5. Set up *BACnet Broadcast Management Devices* if an IP router is used. (See Setting up BACnet Broadcast Management Devices (BBMDs) on page 154)

NOTE: The Liebert® SiteScan™ server name must be less than 15 characters and must not contain hyphens or underscores.
For Linux systems, you must change the Liebert® SiteScan™ default name of the server. (localhost.localdomain).

Setting ExecB Device IP Addresses

For the Liebert® SiteScan™ server to communicate with Vertiv controllers on the IP network, the Liebert® SiteScan™ server and each controller must have the following:

- IP address (unique and static)
- Subnet mask
- Default gateway address, if your system has a default gateway (IP router)

You can use one of the following methods to set IP address for the Liebert® SiteScan™ system.

Use	If
DHCP addressing (See Setting the DHCP IP address of ExecB device on the next page) (requires v6.0 or later controller drivers)	The IP network uses a DHCP server for IP addressing
Custom addressing (See Setting the custom IP address of the ExecB device on page 145)	The answer to any of the following questions is yes and you do not have a DHCP server. • Will the system share an existing IP data network of the facility? • Will it have 199 or more Vertiv IP devices, or 254 or more devices with static IP addresses? • Will it be connected to the Internet? • Will it have at least one device located on the other side of an IP router? • Will it have any third party controllers?
Default addressing (See Setting the default IP address of the ExecB device. on page 149)	The answer to all the above questions is no.

Setting the DHCP IP address of ExecB device

Prerequisites

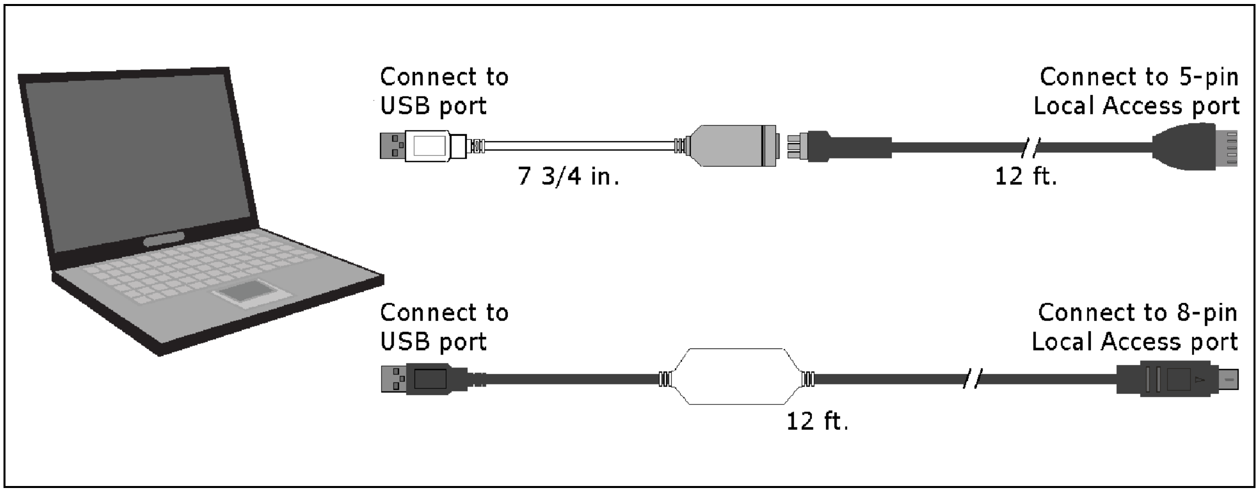
- A computer with a USB port
- A USB Link Kit.

NOTE: The USB Link Kit driver is installed with a Vertiv™ Liebert® SiteScan™ v5 or later system. Refer to the Silicon Labs website and search "CP210x USB to UART Bridge VCP Drivers" for the most current device drivers. Install the driver before you connect the USB Link Kit to your computer.

- v6.0 or later driver

CAUTION: If multiple controllers share power but polarity was not maintained when they were wired, the difference between the ground of the controller and the AC power ground of the computer could damage the USB Link Kit and the controller. If you are not sure of the wiring polarity, use a USB isolator between the computer and the USB Link Kit. Purchase a USB isolator online from a third party manufacturer.

1. Connect the *laptop to the controller* using the appropriate USB Link Kit cable(s).


Connect to USB port
7 3/4 in.
12 ft.
Connect to 5-pin Local Access port
Connect to USB port
12 ft.
Connect to 8-pin Local Access port

NOTE: If using a USB isolator, plug the isolator into the USB port of your computer, and then plug the USB Link Kit cable into the isolator.

2. Turn off the *power* of the controller, set its Enhanced Access Port DIP switch to ON, then turn the power of the controller on again.
3. In SiteBuilder, set your *Configure* > *Preferences* > *Connections tab settings.*

Field	Value
Port	The Com port number of the laptop to which the USB Link Kit is connected to.
Baud Rate	115200
Data Bits	8
Parity	None
Stop Bits	1

4. On the Network tree, double click the *controller*.

5. On the Address tab, click *Module Status*.
6. Note the *Ethernet MAC address* of the controller.
7. When finished, turn off the *power* of the controller, set its Enhanced Access Port DIP switch to OFF to restore normal functionality to the Local Access port, then turn the power on again.
8. Give the *Ethernet MAC address* to your DHCP network administrator and request that he reserve a static IP address for that MAC address.
9. Get the *reserved IP address, subnet mask, and default gateway address* for your router from DHCP network administrator.
10. Repeat steps 1 and 2 .
11. Set the *Default/Assigned DIP switch* of the controller to Default.
12. Repeat steps 3 and 4 .
13. On the Address tab, select *Specify a custom or DHCP IP Address*.
14. Type the *IP Address, Subnet Mask, and Default Gateway Address* that the DHCP network administrator gave you.
15. Click *Download Address*.
16. Turn off the *power* of the controller, set its Enhanced Access Port DIP switch to OFF, then turn its power on again.

Setting the custom IP address of the ExecB device

If IP addresses of the system are assigned by the network administrator, you can connect a laptop to a Local Access Port of the controller and then use either of the following methods to set the custom IP address of the controller so that the Vertiv™ Liebert® SiteScan™ server can communicate with it.

- Set the *custom IP address* in SiteBuilder (See Setting a Custom IP Address of the Controller in SiteBuilder below)
- Set the *custom IP address* using PuTTY (See Setting a custom IP address of the Controller with PuTTY on the next page)

Setting a Custom IP Address of the Controller in SiteBuilder

Prerequisites

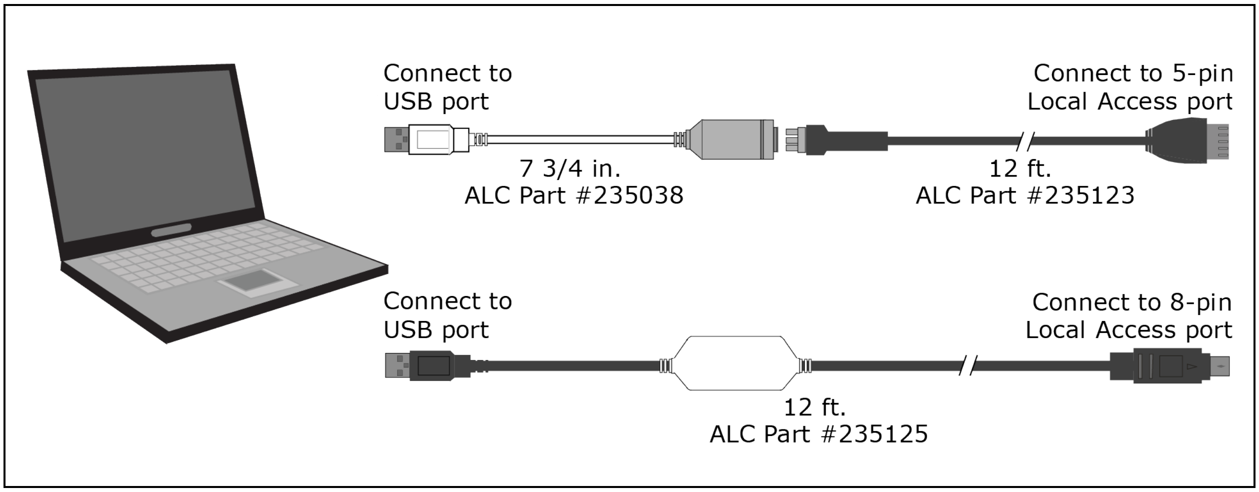
- A computer with a USB port
- A USB Link Kit. See the USB Link Kit Technical Instructions.

NOTE: The USB Link Kit driver is installed with a Liebert® SiteScan™ v5 or later system. Refer to the Silicon Labs website and search "CP210x USB to UART Bridge VCP Drivers" for the most current device drivers. Install the driver before you connect the USB Link Kit to your computer.

- The appropriate controller driver

CAUTION: If multiple controllers share power but polarity was not maintained when they were wired, the difference between the ground of the controller and the AC power ground of the computer could damage the USB Link Kit and the controller. If you are not sure of the wiring polarity, use a USB isolator between the computer and the USB Link Kit. Purchase a USB isolator online from a third party manufacturer.

1. Connect the *computer* to the controller with the appropriate USB Link Kit cable(s).



NOTE: If using a USB isolator, plug the isolator into your USB port of the controller, and then plug the USB Link Kit cable into the isolator.

2. Turn off the *power* of the controller, set its Enhanced Access Port DIP switch to ON, then turn the power of the controller on again.
3. Set the *IP Address DIP switch to Assigned* of the controller.
4. In SiteBuilder, set your *Configure > Preferences > Connections tab settings*.
5. Click *OK*.
6. Double-click the *controller*.
7. On the Address tab, select *Specify a custom or DHCP IP Address*.
8. Type the *IP Address, Subnet Mask, and Default Gateway Address*.
9. Click *Download Address*.
10. After the download is complete, click *Module Status* to verify the router's address.
11. When finished, turn off the controller's power, set its Enhanced Access Port DIP switch to Off, then turn the *power* on again.

Setting a custom IP address of the Controller with PuTTY

Prerequisites

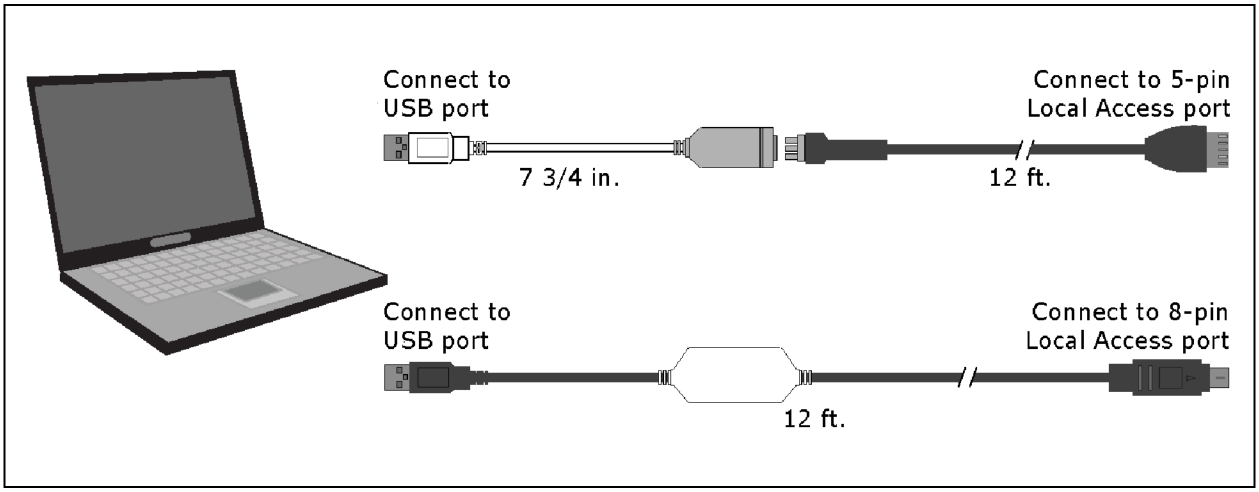
- A computer with a USB port
- A USB Link Kit.

NOTE: The USB Link Kit driver is installed with a Vertiv™ Liebert® SiteScan™ v5 or later system. Refer to the Silicon Labs website and search "CP210x USB to UART Bridge VCP Drivers" for the most current device drivers. Install the driver before you connect the USB Link Kit to your computer.

CAUTION: If multiple controllers share power but polarity was not maintained when they were wired, the difference between the ground of the controller and the AC power ground of the computer could damage the USB Link Kit and the controller. If you are not sure of the wiring polarity, use a USB isolator between the computer and the USB Link Kit. Purchase a USB isolator online from a third party manufacturer.

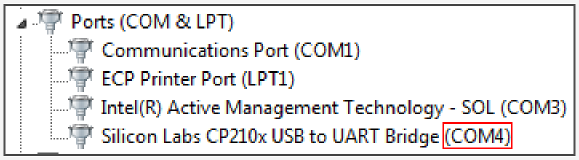
1. Download and install *PuTTY from* the PuTTY website (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).

2. Connect the *laptop* to the controller with the appropriate USB Link Kit cable(s).

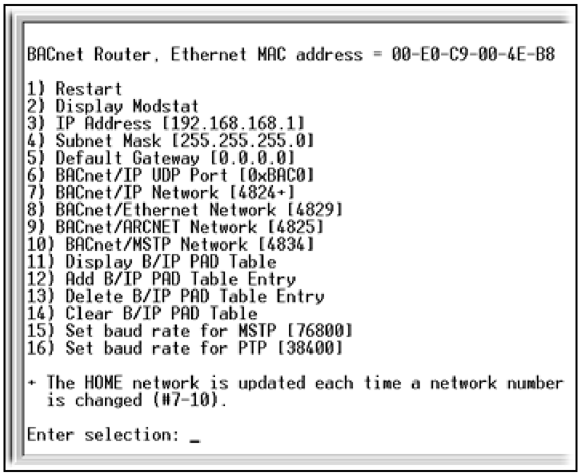


NOTE: If using a USB isolator, plug the isolator into your USB port of the computer, and then plug the USB Link Kit cable into the isolator.

3. If the controller has a DIP switch labeled Enhanced Access, turn off the power of the controller, set the *Enhanced Access DIP switch to ON*, then turn the power of the controller on again.
4. Set the *IP Address DIP switch to Assigned* of the controller.
5. Set the *IP Address* DIP switch of the controller to *Assigned*.
6. Start *PuTTY*.
7. Under Category > Connection, select *Serial*.
8. Under Options controlling local serial lines, enter the following settings:

Field	Value
Serial line to connect to	Replace X with the port number of the controller to which the USB Link Kit cable is connected to. **NOTE: To find the port number, select Start > Control Panel > System > Device Manager > Ports (Com & LPT). The COM port number is beside Silicon Labs CP210x USB to UART Bridge.**  Ports (COM & LPT) Communications Port (COM1) ECP Printer Port (LPT1) Intel(R) Active Management Technology - SOL (COM3) Silicon Labs CP210x USB to UART Bridge (COM4)
Speed (Baud)	Type the appropriate baud rate.
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

9. Click *Open*. A window appears as shown below.



```
BACnet Router, Ethernet MAC address = 00-E0-C9-00-4E-B8

1) Restart
2) Display Modstat
3) IP Address [192.168.168.1]
4) Subnet Mask [255.255.255.0]
5) Default Gateway [0.0.0.0]
6) BACnet/IP UDP Port [0xBAC0]
7) BACnet/IP Network [4824+]
8) BACnet/Ethernet Network [4829]
9) BACnet/ARCNET Network [4825]
10) BACnet/MSTP Network [4834]
11) Display B/IP PAD Table
12) Add B/IP PAD Table Entry
13) Delete B/IP PAD Table Entry
14) Clear B/IP PAD Table
15) Set baud rate for MSTP [76800]
16) Set baud rate for PTP [38400]

+ The HOME network is updated each time a network number
  is changed (#7-10).

Enter selection: _
```

10. Type the *number of the address field*, then press *Enter*.
11. Type the *new address*, then press *Enter*.
12. Type *1*, then press *Enter* to restart the controller.
13. Close *PuTTY*.
14. If you set the Enhanced Access DIP switch of the controller, turn off the power of the controller, set the *DIP switch to Off*, then turn the power of the controller on again.

Changing Remotely the Custom IP Address of the Controller

Steps 1 through 5 below change the IP address in the controller. Steps 6 to 10 change it in the system database. Communication with the controller will be disrupted until all steps are performed.

1. On the Vertiv™ Liebert® SiteScan™ Network tree, go to the *controller's Driver > BACnet Router Properties page*.
2. Under IP Configuration, select *Enable IP configuration changeover*.

NOTE: The field Allow remote management of IP configuration is for future use.

3. In the Next column, type the *new IP Address, Subnet Mask, and Default Gateway Address*. Type the UDP Port that your server is using to communicate to all controllers.

NOTE: You must enter values in all 4 fields, even if the values will not change.

4. Do one of the following.

Set the Changeover timeout field to...	To have the controller use the Next settings...
0:00	As soon as the controller can communicate with the Next Default Gateway Address.
A specific length of time	As soon as the controller can communicate with the Next Default Gateway Address, or when the timeout expires, whichever occurs first.

5. Click *Accept*.
6. On the System Configuration tree, select *Connections*.
7. On the Configure tab, select the *BACnet/IP Connection*, then click *Stop*.
8. On the Network tree, go to the Properties page of the controller.

9. Make the necessary changes in the Address, Subnet mask, and Default Gateway fields.
10. Click *Accept*.
11. On the System Configuration tree, select *Connections*.
12. On the Configure tab, select the *BACnet/IP Connection*, then click *Start*.
13. On the Network tree, go to the *Properties page* of the controller, then click *Module Status* to verify communication with the controller.

Setting the default IP address of the ExecB device.

NOTE:

If you want to use the default IP addressing but a DHCP server exists, follow the instructions in Setting a Custom IP Address of the Controller in SiteBuilder on page 145 , and enter the default addresses listed in NOTE: below below.

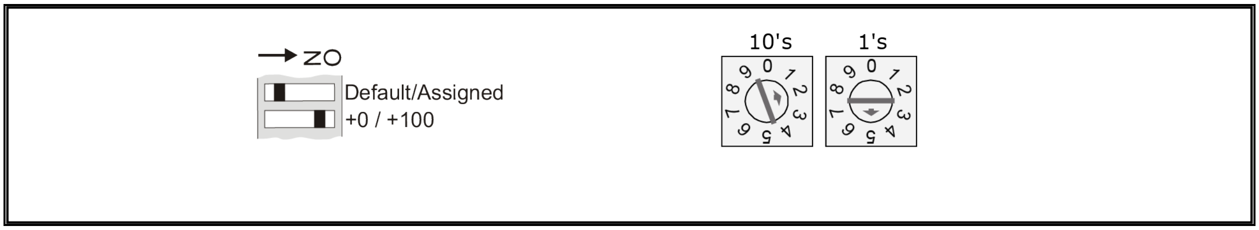
A network using default addressing does not have a default gateway (IP router).

1. If wired for power, turn off the power of the controller.

NOTE: The controller only reads the rotary switch positions during power up or upon reset.

2. Set the Default/Assigned DIP switch to the Default position to use the following IP networking parameters.
   IP address = 192.168.168.x
   where x is the controller address you will set in steps 3 and 4 .
   Subnet mask = 255.255.255.0
   Default gateway address = 192.168.168.254
3. Using the rotary switches, set the controller's address to match the Address in the controller's properties dialog box in SiteBuilder. Set the Tens (10's) switch to the tens digit of the address, and set the Ones (1's) switch to the ones digit.
4. Set the +0/+100 DIP switch to off for a controller address from 0 to 99, or to on for a controller address from 100 to 199. (On your controller, this DIP switch may be labeled 100's or +100 and 0.)

Example: Setting the switches as shown in the figures below produces an IP address of 192.168.168.125.



5. On SiteBuilder's Network tree, double-click the *controller*.
6. On the Address tab, select *Use Default IP Address*.
7. In the Address (Dial Setting on Device) field, type *the value of x*.
8. Click *OK*.

NOTE: The default address is an intranet address. Data packets from this address are not routable to the Internet.

Setting up a BACnet/IP connection in the Vertiv™ Liebert® SiteScan™ interface

Using a BACnet/IP connection and an Ethernet Network Interface Card, the Liebert® SiteScan™ server can speak BACnet/IP over an Ethernet network.

1. On the System Configuration tree, select *Connections*.
2. On the Configure tab, select *BACnet/IP Connection*.
3. If the Status column shows:
   - Connected, click *Disconnect*.
   - Stopped or Design Mode, go to step 4 .
4. Set up the fields as needed for that connection. See tables below.
5. Click *Accept*.
6. If running the Liebert® SiteScan™ Server (not SiteScan Design Server) application, select the BACnet/IP Connection, then click *Start*.

Table 4.1

Field or Button	Notes
Server IP Address	Type the server's IP address. The IP address and subnet mask must also be set on the server's network connections page. **NOTE: If the server has more than 1 NIC, use the IP address of the interface connected to the controllers.**
Server IP Subnet Mask	• For default IP addressing, type 255.255.255.0. • For custom IP addressing, type the subnet mask provided by the facility network administrator.
BACnet Port	Type 47808 unless you need to communicate with a third-party device using a different port for BACnet communication or your IT administrator specified a different port.
Disable Field Alarms	Select if you do not want to retain incoming alarms on this connection. Typically this box might be checked during start-up then cleared for normal operation.
Poll Interval	How often the Liebert® SiteScan™ application checks the communication status of the peer caching router. If it cannot communicate with the router, the Liebert® SiteScan™ application generates a Dead Module Timeout alarm.
Foreign Device	If the Vertiv™ Liebert® SiteScan™ server is on an IP network segment that does not have an Vertiv controller serving as a BBMD, select Force Registration. See Setting up BACnet Broadcast Management Devices (BBMDs) on page 154 .
Register with Device	If you selected Force Registration in the previous field, select the BBMD on a remote IP network from which the Liebert® SiteScan™ server will receive BACnet/IP broadcasts.
Network Node	Specify which network the Liebert® SiteScan™ server is physically connected to. This is primarily used to specify which ARCNET network the ARCNET card is connected to. This is also used to specify which BACnet/IP network the Liebert® SiteScan™ server is on if there are multiple BACnet/IP network nodes with different network numbers in your system.

Tuning Parameters	Notes
Comm Timeout	Amount of time, in milliseconds, that is allowed before retrying a transmission on the network if a required acknowledgment is not received.
Comm Attempts	The number of times to try a transmission on the network.
Do Sync	Amount of time, in milliseconds, allowed for the Liebert® SiteScan™ application to complete a communication task such as downloading to a controller or reading trends from a controller.
Register FD Interval	Amount of time, in seconds, that is allowed before the Liebert® SiteScan™ application notifies a BBMD that the Liebert® SiteScan™ server is a foreign device to that BBMD. If the re-registration does not occur within this time, the BBMD will delete the Liebert® SiteScan™ server from its list.

Setting up a BACnet/IP Service Port connection in the Liebert® SiteScan™ interface

You can connect to the Service Port to access your network through the:

- Liebert® SiteScan™ application
- Vertiv touchscreen device

The Service Port on OptiCORE controllers could be either an Ethernet or USB port. Also, the information shown on the controller setup pages is specific to the controller. See the controller's Installation Guide for details on connecting the controller's Service Port to a laptop and on using the controller setup pages.

1. Connect the controller's Service Port to your laptop as specified in the Installation Guide.
2. Turn off the *computer's Wi-Fi* if it is on.
3. If your computer uses a static IP address, use the following settings:
    - Address: 169.254.1.x, where x is 2 to 7
    - Subnet Mask: 255.255.255.248
    - Default Gateway: 169.254.1.1
4. If it uses a DHCP address, leave the *address as it is*.
5. Open a web browser on the computer and open your *Liebert® SiteScan™ application*.
6. In the Liebert® SiteScan™ interface, on the System Configuration ⚙ tree, select Connections.
7. On the Properties page > Configure tab, select *BACnet/IP Service Port Connection* from the drop-down list and click Add.
8. If needed, enter the *Service Port Network Number* as follows:
    - 0 - the will communicate only with the computer or
    - 1 to 65534 - The number for network communication
    - 65535 - searches for an available network number from 65531 to 65534. If any of these numbers are not available, you will have to assign a network number and enter it.
9. Click *Accept*.
10. On the right of the page, in the Networks using selected *connection table*, click the *checkbox* next to the network you want to connect to.
11. Click the *Start button*. The status changes to *Connected*.

NOTE: If an error message appears, make sure the COM port you selected is not in use. For example, PuTTY may be open and is holding the port open.

Setting up a BACnet/IPv6 Connection in the Vertiv™ Liebert® SiteScan™ Interface

Using a BACnet/IPv6 connection and an Ethernet Network Interface Card, the Liebert® SiteScan™ server can speak BACnet/IPv6 over an Ethernet network.

1. On the System Configuration tree, select *Connections*.
2. On the Configure tab, select *BACnet/IPv6 Connection*.
3. If the Status column shows:
    - Connected, click *Disconnect*.
    - Stopped or Design Mode, go to step 4 .
4. Set up the fields as needed for that connection. See tables below.
5. Click *Accept*.
6. If running the SiteScan™ Web v8.0 Server (not SiteScan Design Server) application, select the *BACnet/IPv6 Connection*, then click *Start*.

Field or Button	Notes
Server IPv6 Address	Type the IPv6 address of the server. The IPv6 address and subnet mask must also be set on the network connections page of the server. **NOTE: If the server has more than 1 NIC, use the IP address of the interface connected to the controllers.**
Prefix Length	Value set between 10 and 127 to define the number of leftmost bits identifying the network portion of the address.
BACnet Port	Type 47809 unless you need to communicate with a third party device using a different port for BACnet communication or your IT administrator specified a different port. Ensure that you IPv6 ports are different than your IPv4 ports and that you assign the connection to the same IPv6 multicast group.
IPv6 Multicast Address	Used for broadcasts on an IPv6 network using SLAAC. Defined by the building network administrator.
IPv6 Multicast Port	The port that the controller will use for BACnet communication broadcasts and must be the same as the BACnet Port.
Disable Field Alarms	Select to not to retain incoming alarms on this connection. Typically this box might be checked during startup then cleared for normal operation.
Poll Interval	How often the Liebert® SiteScan™ application checks the communication status of the peer caching router. If it cannot communicate with the router, the Liebert® SiteScan™ application generates a Dead Module Timeout alarm.
Foreign Device	If the Liebert® server is on an IPv6 network segment that does not have an Vertiv controller serving as a BBMD, select Force Registration. See Setting up BACnet Broadcast Management Devices (BBMDs) on page 154 .
Register with Device	If you selected Force Registration in the previous field, select the BBMD on a remote IPv6 network from which the Liebert® SiteScan™ server will receive BACnet/IPv6 broadcasts.
Primary BBMD	If you selected Force Registration in the previous field, select the primary BBMD.
Backup BBMD if primary fails	To have a backup in case the first BBMD fails, select another BBMD.
Network Node	Specify which network the Vertiv™ Liebert® SiteScan™ server is physically connected to. This is used to specify which BACnet/IPv6 network the Liebert® SiteScan™ server is on if there are multiple BACnet/IPv6 network nodes with different network numbers in your system.

Tuning Parameters	Notes
Comm Timeout	Amount of time, in milliseconds, that is allowed before retrying a transmission on the network if a required acknowledgment is not received.
Comm Attempts	The number of times to try a transmission on the network.
Do Sync	Amount of time, in milliseconds, allowed for the Liebert® SiteScan™ application to complete a communication task such as downloading to a controller or reading trends from a controller.

Testing the Server to Client Connections

After making sure that the Ethernet cabling has been set up properly, make sure you can ping the server from each client computer. Then test the HTTP connection by running SiteScan Design Server.

To Ping the Server from Each Client

Use the Ping utility from each client computer to test its low-level IP communication with the Liebert® SiteScan™ server.

Prerequisites

- An IP network connection between your server and client computers
- A solid Link light and a flickering LAN light on the Liebert® SiteScan™ client computers and the Network Interface Card (NIC) of the Liebert® SiteScan™ server. If either device indicates it is not on the network, see Troubleshooting an IP/Ethernet Connection on page 159

After the link and the LAN lights on the server’s NIC and on the client are lighting properly, ping the Liebert® SiteScan™ server from each client machine.

1. At the Command Prompt, type the following command: ping xxx.xxx.xxx.xxx [Enter], where xxx.xxx.xxx.xxx is the IP address of the device you are pinging.
   The reply should indicate that a device with address xxx.xxx.xxx.xxx is present and passing IP packets on the network.
   Example For a device with an IP address of 192.168.168.100, type the following:
   - ping 192.168.168.100

   Tip To continuously ping a device, type the following command: ping xxx.xxx.xxx.xxx -t.
   Press Ctrl+C to stop the ping command.
2. If you receive the reply Request timed out or you do not receive a reply, contact the facility’s network administrator to check the NIC, the hub's settings, and the IP configuration settings. You do not have a valid IP connection between the 2 devices.

To Test the HTTP Connection

SiteScan Design Server does not attempt communication with field hardware, so you can isolate client-to-server issues from server-to-field issues.

1. Click *Start > All Programs > SiteScan_Web_ x.x > SiteScan Design Server*.
2. From each client computer, start the web browser, then type the IP address of the server in the Address field.

If the Vertiv™ Liebert® SiteScan™ login screen does not appear, contact the facility's network administrator.

Testing the Server to Controller Connections

If the system is running, go to the Liebert® SiteScan™ Devices page from different levels of the Network tree to view the status of your communication networks and controllers. If you detect a networking problem with an Ethernet connection, see Troubleshooting an IP/Ethernet Connection on page 159 .

After making sure that the Ethernet cabling has been set up properly, use the Ping utility from the Liebert® SiteScan™ server to test its low level IP communication with each controller on the IP network, then obtain a Modstat (page 210) from each controller to ensure its BACnet communication with the Liebert® SiteScan™ server.

Pinging a Controller on the IP Network from the Liebert® SiteScan™ Server

Use the Ping utility to test low level IP connections between the server and each controller on the IP network.

Prerequisites

- An IP network connection between the server and the Vertiv controller.
- A solid link light and a flickering LAN light on the Vertiv controller and the Liebert® SiteScan™ Network Interface Card (NIC) of the server. See Troubleshooting an IP/Ethernet Connection on page 159 .

After the link and LAN lights on the server's NIC and on the controller are lighting properly, ping each controller from the Liebert® SiteScan™ server.

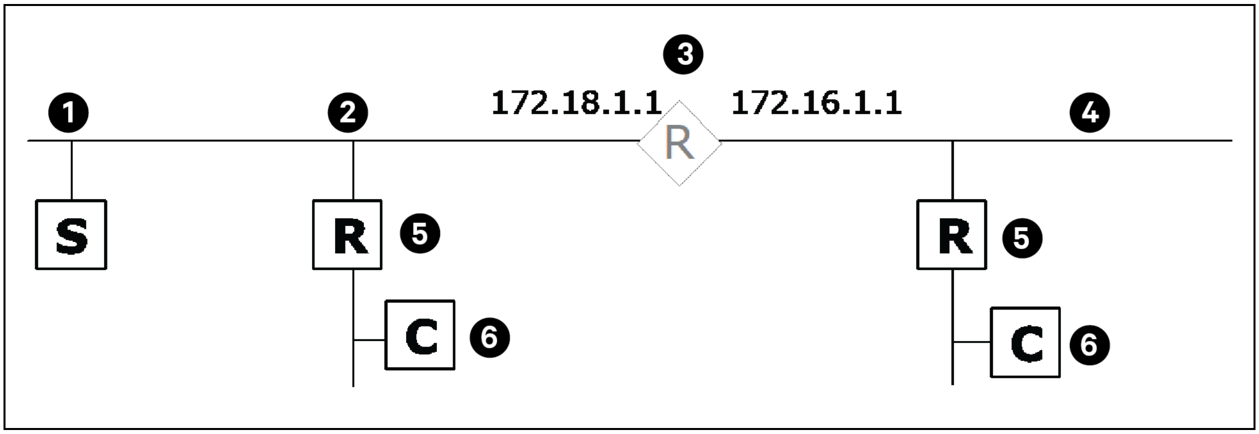
1. At the Command Prompt, type the following command: ping xxx.xxx.xxx.xxx [Enter], where xxx.xxx.xxx.xxx is the IP address of the device you are pinging.
   The reply should indicate that a device with address xxx.xxx.xxx.xxx is present and passing IP packets on the network.
   Example For a device with an IP address of 192.168.168.100, type the following:

   ping 192.168.168.100
   TIP To continuously ping a device, type the following command: ping xxx.xxx.xxx.xxx -t.
   Press Ctrl+C to stop the ping command.

2. If you receive the reply Request timed out or you do not receive a reply, contact the facility's network administrator to check the NIC, the hub's settings, and the IP configuration settings. You do not have a valid IP connection between the 2 devices.

Setting up BACnet Broadcast Management Devices (BBMDs)

To minimize network communications, IP routers do not pass on broadcasts that they receive. If your system has controllers on different IP subnets separated by an IP router, you must set up a BACnet router on each IP subnet as a BACnet Broadcast Management Device (BBMD). A BBMD passes BACnet/IP broadcasts across the IP router to other BBMDs.



Iteam	Description
1	System Server
2	IP Subnet
3	IP Router
4	IP Subnet
5	BBMP
6	Controller

To set up BBMDs, use the appropriate method in the **Table 4.2** on the facing page .

Table 4.2

If your Liebert® SiteScan™ system has...	Use this method
100 or less IP subnets with:* • No third party BACnet routers • Authority from your customer to manage all Vertiv and third party BBMDs on the network • Third party BACnet routers that support BBMD writes from the network	Let SiteBuilder automatically configure your BBMDs.
Any of the following: • More than 100 IP subnets * • Third party BBMDs that you do not have authority to manage • Third party BBMDs that use a non standard port for BACnet communications	Set up custom BBMDs through the Vertiv™ Liebert® SiteScan™ interface or using the BBMD Configuration Tool.

NOTE: If the Liebert® SiteScan™ server is on an IP subnet without an Vertiv BACnet router, register the server as a foreign device. See Setting up the Vertiv™ Liebert® SiteScan™ Server as a Foreign Device on page 158 .

Setting up BBMDs in SiteBuilder

As you add each Vertiv BACnet router to an IP network on the Network tree, check Automatically Configure My BBMDs on the Address tab. SiteBuilder automatically selects a router in each IP subnet as the BBMD and sets up BBMD tables appropriately.

To see which BACnet routers SiteBuilder assigned as BBMDs, select View > Display > BBMD. BBMDs show B=assigned on the Network tree.

To override BBMD selection of the SiteBuilder, right click a different BACnet router on the same IP subnet, then select Force to BBMD.

NOTE: If you are managing third party BBMDs, you must add every third party device that could be a BBMD as a third party device router in SiteBuilder.

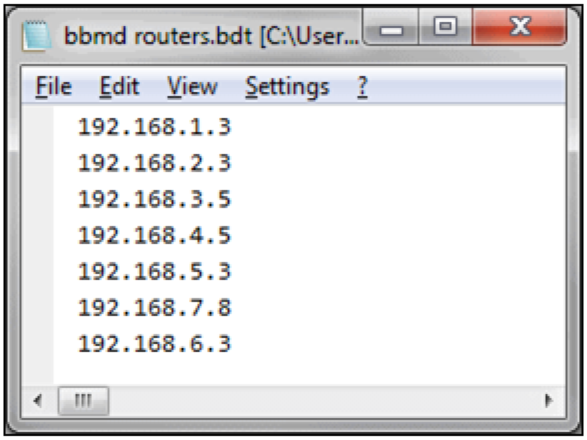
Setting up BBMDs through the Vertiv™ Liebert® SiteScan™ Interface

1. Make a list of the IP addresses for every controller that will function as a BBMD in your system.

CAUTION: Multiple BBMDs on an IP subnet disrupt BACnet communications. Define only one BBMD on either side of each IP router in your system.

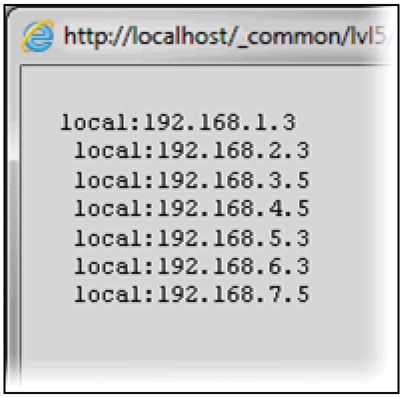
2. In Notepad, type each IP address on a separate line to prepare a list. (ExecB routers support up to 100 IP addresses per .bdt file.)

NOTE: To communicate with a third party router that does not use the BACnet/IP port 47808 (0xbac0), you must include the hexadecimal port number in the IP address. For example, 172.168.23.67:0xe78a.



```
192.168.1.3
192.168.2.3
192.168.3.5
192.168.4.5
192.168.5.3
192.168.7.8
192.168.6.3
```

3. Save the file in the webroot\<system_name> folder with a .bdt extension instead of .txt.
4. On the Liebert® SiteScan™ Network tree, select one of the Vertiv controllers that will function as a BBMD.
5. To check if the controller has an existing BBMD table, click , then select Manual Command.
6. In the manual command field, type: bbmd read x.x.x.x
   where x.x.x.x is the IP address of the controller you are on.
7. Click *OK*.
8. If the Broadcast Distribution Table contains IP addresses that are not in your .bdt file, add them to your .bdt file.
9. Click , then select *Manual Command*.
10. In the manual command field, type: bbmd write filename.bdt x.x.x.x
    where filename.bdt is the .bdt file in the webroot\<system_name> folder and x.x.x.x is the IP address of the controller you are on.
11. Click *OK*.
12. Issue another bbmd read command to verify that the .bdt file was written correctly.



```
local:192.168.1.3
 local:192.168.2.3
 local:192.168.3.5
 local:192.168.4.5
 local:192.168.5.3
 local:192.168.6.3
 local:192.168.7.5
```

Setting up BBMDs using the BBMD Configuration Tool

Before you begin, do the following:

- Set up the IP address, subnet mask, default gateway, and network numbers for the Vertiv™ Liebert® SiteScan™ server and each Vertiv controller on the IP network. See Setting up IP Network Communication on page 143 .

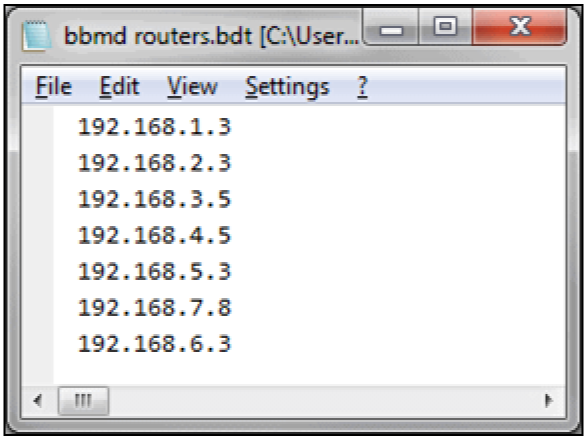
- Go to the Automated Logic Partner Community website. Under Engineering and Startup Tools, select Utilities > BBMD Configuration Tool. Follow the instructions.

1. Make a list of the IP addresses for every controller that will function as a BBMD in your system.

CAUTION: Multiple BBMDs on an IP subnet disrupt BACnet communications. Define only one BBMD on either side of each IP router in your system.

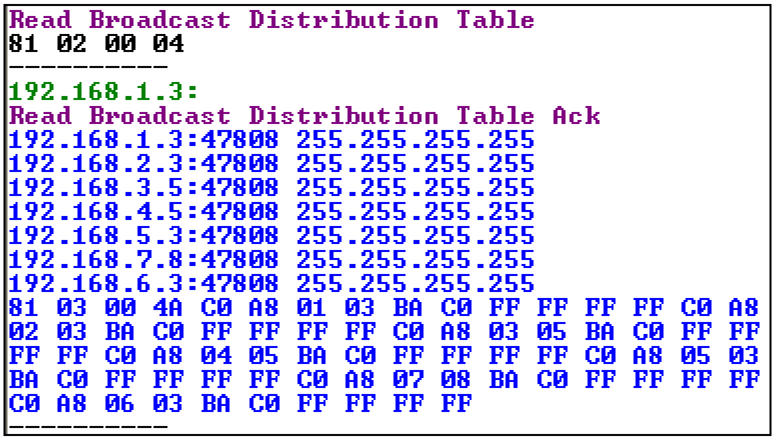
2. In Notepad, type the list putting each IP address on a separate line. (ExecB routers support up to 100 IP addresses per .bdt file.)

NOTE: To communicate with a third party router that does not use the BACnet/IP port 47808 (0xbac0), include the hexadecimal port number in the IP address. For example, 172.168.23.67:0xe78a.



```
192.168.1.3
192.168.2.3
192.168.3.5
192.168.4.5
192.168.5.3
192.168.7.8
192.168.6.3
```

3. Save the file in the webroot\<system_name> folder with a .bdt extension instead of .txt.
4. Open the *BBMD Configuration Tool*.
5. In the IP Address or Host Name field, type the IP address of an Vertiv controller that functions as the BBMD (BACnet Broadcast Management Device) for its subnet.
6. Click the *Broadcast Distribution* Table Read button to see if the controller has an existing BBMD table. The information found is displayed in the bottom half of the window.
7. If the Broadcast Distribution Table contains IP addresses that are not in the .bdt file you created in steps 2 and 3 , add them to your .bdt file.
8. Verify that the same controller IP address is still in the IP Address or Host Name field.
9. Click the *Broadcast Distribution Table Browse button*, then select the *.bdt file* that you created in steps 2 and 3 .
10. Click the *Broadcast Distribution Table Write button* to send the information to the controller.
11. Click *Read again* to verify that the new .bdt file was written to the Vertiv controller.
12. Repeat steps 5 to 11 for each Vertiv controller that will function as a BBMD in your system.



```
Read Broadcast Distribution Table
81 02 00 04
----------
192.168.1.3:
Read Broadcast Distribution Table Ack
192.168.1.3:47808 255.255.255.255
192.168.2.3:47808 255.255.255.255
192.168.3.5:47808 255.255.255.255
192.168.4.5:47808 255.255.255.255
192.168.5.3:47808 255.255.255.255
192.168.7.8:47808 255.255.255.255
192.168.6.3:47808 255.255.255.255
81 03 00 4A C0 A8 01 03 BA C0 FF FF FF FF C0 A8
02 03 BA C0 FF FF FF FF C0 A8 03 05 BA C0 FF FF
FF FF C0 A8 04 05 BA C0 FF FF FF FF C0 A8 05 03
BA C0 FF FF FF FF C0 A8 07 08 BA C0 FF FF FF FF
C0 A8 06 03 BA C0 FF FF FF FF
----------
```

Setting up the Vertiv™ Liebert® SiteScan™ Server as a Foreign Device

If the Liebert® SiteScan™ server is on an IP subnet without an Vertiv BACnet router, register the server as a foreign device to a BBMD in the system. That BBMD will then forward BACnet broadcasts to the server. Register the server with the BBMD that will have the fastest response time. Distance and network complexity affect the response time.

1. On the Liebert® SiteScan™ System Configuration ⚙ tree, select Connections.
2. On the Configure tab, select BACnet/IP Connection.
3. If the Status column shows:
   - Connected, click *Disconnect*.
   - Stopped or Design Mode, go to step 4 .
4. Type the Liebert® SiteScan™ IP address of the server in the IP Address field. (172.18.64.37, in the example above.)

NOTE: If you have more than one network interface card, type the address that connects to the controller network.

5. Type the Liebert® SiteScan™ subnet mask of the IP address in the IP Subnet Mask field. (255.255.0.0, in the example above.)
6. Select Force Registration from the Foreign Device drop down list.
7. Select the BBMD in the Primary BBMD field.
8. To have a backup in case the first BBMD fails, select another BBMD in the Backup BBMD if primary fails field.
9. Click ▷ next to Tuning Parameters.
10. Keep the 600 seconds default value in the Register FD Interval field.

NOTE: If the re-registration does not occur within time, the BBMD will delete the Vertiv™ Liebert® SiteScan™ server from its list.

11. Click *OK*.
12. If running Liebert® SiteScan™ Server (not Liebert® SiteScan™ Design Server), select the BACnet/IP Connection, then click Start.

If your system does not have any BBMDs

Follow the below steps to create pseudo BBMDs to register the server.

1. In the SiteBuilder application, double click each BACnet router and check Automatically Configure My BBMDs on the Address tab.

2. In the Liebert® SiteScan™ application, select any location on the Network tree.
3. Run the manual command bbmd update to create a blank .bdt table in every router and mark them for download.
4. Download parameters to the routers.
5. Follow the steps above to register the Liebert® SiteScan™ server as a foreign device to one of the routers.

4.1.2 Troubleshooting Networks

If a controller is not communicating, select the network of the controller on the Liebert® SiteScan™ Network tree, then click the Devices button. This page shows the communication status of all controllers on the network. If all controllers on the network are not communicating, you have a network problem. Begin moving up the Network tree, checking communication status at each level to determine the starting point of the communications problems.

Troubleshooting an IP/Ethernet Connection

Normal Condition

Most Ethernet devices have link lights that indicate connectivity. If the Ethernet cable is terminated correctly, the link lights at each port (server, Vertiv controller, and hub or switch) will be lit. A controller LAN lights will flicker, indicating Ethernet data packet activity.

Problem

If the Ethernet connection is not wired correctly, you may experience the below symptoms:

- Link light is off
- LAN light remains off

Possible cause	Solution
The physical integrity of the cable or connectors is compromised.	If a known good cable results in a normal condition, replace the cable.
An improper connection type is used.	• Use a crossover cable to connect two IP devices without a hub. • Use a straight cable to connect an IP device to a hub.
A cable is plugged into a uplink port of the hub.	Use a different port. **NOTE: Many hubs and switches share the first or last port with the uplink port. Other hubs have an uplink switch or button. If you need to use the first port, make sure that the hub or switch is set up correctly (usually a small switch on the back or bottom of the device) and that the first port is not shared with the uplink connection.**
The devices are not on the same IP network.	Change one of the IP addresses or install an IP router. **NOTE: To determine whether the devices are on the same network, use the Subnet calculator below.**
A NIC is installed incorrectly.	If you are unable to ping the IP address of the host from the host computer, reinstall the NIC, checking for correct drivers.
Faulty hardware: NIC, hub, switch, or Vertiv controller	The diagnosis may be the same as the solution: replace the faulty hardware.

NOTE: After checking these possible causes, if you are unable to get a link or LAN light on an Vertiv controller, contact Automated Logic Technical Support.

When troubleshooting an Ethernet connection, Automated Logic Technical Support may request to provide network diagnostics information from the System Configuration tree > Connections > Statistics tab.

Troubleshooting an ARCNET Connection

Problem

Intermittent communication over an ARCNET network may cause the below symptoms:

- Vertiv™ Liebert® SiteScan™ graphics or properties pages intermittently display actual values then question marks.
- You can obtain a Modstat (page 210) from a controller, but a download fails.

Possible Cause

The Liebert® SiteScan™ communication timeout settings are not sufficient for your network configuration.

Solution

Increase your communication timeout settings.

1. On the Liebert® SiteScan™ System Configuration ⚙ tree, select Connections.
2. On the Configure tab, select your BACnet/ARCNET Connection.
3. Click ▶ next to Tuning Parameters.
4. Double the values in the Comm Timeout and Comm Attempts fields.
5. Click Accept.

NOTE: If changing these values does not fix your intermittent communication, contact Automated Logic Technical Support.

Troubleshooting BACnet Bindings

Every controller has a Device Binding Table that contains all Device IDs that the controller communicates with and the network address of each device. This typically includes the Device ID of the BACnet Alarm Recipient. If Network Address Translation (NAT) is enabled in SiteBuilder, the alarm recipient is omitted.

If the Liebert® SiteScan™ application is not receiving alarms/trends or if the point value is incorrect, you can view this table to see where the controller is looking for its data.

1. On the Liebert® SiteScan™ Network tree, select the controller that has incorrect or missing data.
2. On the Properties page, click Show Bindings.

Example: If a controller has been sending alarm/trend data to Device 249999, but someone changed the BACnet Alarm Recipient field in SiteBuilder to 249996 and did not download parameters, the following information will be displayed at the bottom of the Device Binding Table:

```
*** No binding for event recipient DEV:249999
```

```
*** Will not be able to deliver alarms/trend notifications
```

```
*** Alarms should be delivered to DEV:249996
```

4.1.3 Using a Modstat to Troubleshoot your System

A Modstat (Module Status) provides information about a controller and verifies proper network communication with the controller.

Obtaining a Modstat

You can get a ModStat of the controller in the following places:

- ExecB device—In the Vertiv™ Liebert® SiteScan™ or SiteBuilder application

In the Liebert® SiteScan™ Application

Use one of the following methods:

- Right click a *controller* on the Network tree, then select Module Status.
- Select a controller on the Network tree. On the Properties page, click Module Status.

NOTE: You cannot get a Modstat if running SiteScan Design Server because it cannot communicate with controllers.

In the SiteBuilder Application (ExecB Device only)

1. Use a USB Link Kit to connect your computer to the Local Access port of the controller. See Connecting to a Local Access Port of the Device on page 163 .
2. In SiteBuilder, select Configure > Preferences.
3. On the Connections tab, select the computer Port that the USB Link Kit cable is connected to, and Baud Rate to one of the following:

Local Access port	Baud Rate
5-pin Rnet	115200
8-pin round	38400

4. Right click the controller in SiteBuilder Network tree, then select Module Status.

Modstat Field Descriptions

NOTE: Modstats vary for different types of controllers. The list below describes all information that could appear on any Modstat. If a description differs between different generations of controllers, the generation is noted.

Field	Description
Date/Time	Date and time the Modstat was run
CM	The rotary switch address of the controller (MAC address)
Model Name	Identifies the Product Type
Device Instance	A unique ID assigned to the controller
Driver built	When the driver was built
Downloaded by	When and where the last download was performed
Application Software Version	The name of the first control program that is downloaded

Field	Description
Flash Archive Status	Shows the validity, date, and time of the most recent archive of parameters and status to the permanent flash memory of the controller. The archive takes place once a day.
# PRGs initialized # PRGs running	If applicable, the number of control programs that were downloaded vs. the number that are running. If these numbers are not the same, the controller has a problem such as lack of memory.
Firmware sections in flash memory	The name, version, and date of the driver
Reset Counters:	ExecB device: The number of times each of the following events have occurred since the last time the controller was formatted.
Power failures	Interruption of incoming power
Brownouts	Low level of incoming power
Commanded boots	Includes commands issued from the Vertiv™ Liebert® SiteScan™ interface such as the zap manual command, plus commands issued during a memory download.
System errors	Error in the firmware or hardware of the controller
Watchdog timeouts	Watchdog is firmware that monitors the firmware for normal operation. If watchdog detects a problem, it restarts the firmware.
S/W Watchdog timeouts	Watchdog is firmware that monitors the application firmware for normal operation. If the watchdog firmware detects a problem, it restarts the application firmware.
H/W Watchdog timeouts	H/W Watchdog will restart the controller if it detects a severe problem with the operating system of the controller
System status	Gives the current status of the operation of the controller.
Network status	Gives the current status of the networks of the controller.
System error message history	ExecB device: High severity errors since the last memory download or format. Shows the first 5 and last 5 messages.
Warning message history	ExecB device: Low severity errors and warning messages since the last memory download or format. Shows the first 5 and last 5 messages.
Information message history	ExecB device: Information only messages since the last memory download or format. Shows the first 5 and last 5 messages.
Manifest revision	Firmware revision
Installed bundles	Components of the firmware
ARC156 reconfigurations during the last hour	An ARCNET network normally reconfigures itself when a controller is added to or taken off the network. The Total field indicates the number of reconfigurations in the last hour. Initiated by this node indicates the number of reconfigurations initiated by this controller. Typical sources of the problem could be this controller, the controller with the next lower rotary switch address, any controller located on the network between these two controllers, or the wiring between these controllers. An excessive number in these fields indicates a problem with the network.
BACnet comm errors in the last 7 days	BACnet communication errors usually indicates dropped packets caused by high traffic on network.
Core (or Main) and Base board hardware	Gives the following information about the controller's boards: • Type and board numbers that are used internally by Vertiv. • The manufacture date and serial number. • ExecB device only: The core board's RAM and Flash memory. RAM is used for driver and control program executables. Flash memory is used for firmware and file storage. See Flash storage size below.

Field	Description
Number of BACnet objects	The number of BACnet objects that were created in the device and the number of those objects that are network visible.
Largest free heap space	Size of the largest piece of unused dynamic memory
Database size	ExecB device: Size of the controller's memory designated for running programs. Database memory is used for control program parameters, status and history; trends, schedules, and alarms; and driver parameters, status and history.
Flash storage size	The size of the flash memory that is not used by the firmware. This memory is used for file storage and archiving.
Archive storage size	The amount of flash memory remaining for archival after files are downloaded.
File storage size	The size of all files (control programs, graphics, driver, etc.) downloaded to the controller. How much information is in these files depends on whether the Download source files option of the controller is selected in SiteBuilder or Vertiv™ Liebert® SiteScan™.
Raw physical switches	The readings used to test the DIP or rotary switches
Network Information	ExecB device: The various network addresses for a controller installed on an Ethernet. The Current and Assigned addresses will be the same unless: • The Assigned addresses were changed in PuTTY. • The Default/Assigned DIP switch of the controller was moved to the Default position after the Assigned addresses were defined in SiteBuilder. • The Enable IP configuration changeover on the on the BACnet Router Properties page is being implemented.
Route Information	BACnet networks that a router is currently routing traffic to. The list changes as BACnet routers are added or removed from the system.
Ethernet statistics	Diagnostic counters directly related to the ethernet communications hardware.

4.1.4 Communicating Locally with ExecB Devices

You can connect locally to controllers and some sensors to commission, start up, or troubleshoot equipment, or download to controllers. Use a local connection in any of the following situations:

- The entire network is not yet functional.
- The permanent Liebert® SiteScan™ server is not operating.
- The server is operating, but you don't have a convenient IP connection.

To make a local connection, use a USB Link Kit to connect a laptop running either the:

- Liebert® SiteScan™ application - Requires a copy of the system database and that you set up a Local Access connection in the Liebert® SiteScan™ interface.

NOTE: If required, you can disable a local access of the controller. (See Disabling Local Access of the Controller on page 169).

Connecting to a Local Access Port of the Device

Prerequisites

- A computer with a USB port
- A USB Link Kit. See the USB Link Kit Technical Instructions.

NOTE: The USB Link Kit driver is installed with a Vertiv™ Liebert® SiteScan™ v5 or later system. Please refer to the Silicon Labs website and search "CP210x USB to UART Bridge VCP Drivers" for the most current device drivers. Install the driver before you connect the USB Link Kit to your computer.

- The appropriate controller driver

For...	Use driver...
Devices with a 5-pin Local Access port	v1.70 or later
Devices with a round 8-pin Local Access port	v2.00 or later

⚠ **CAUTION: If multiple controllers share power but polarity was not maintained when they were wired, the difference between the ground of the controller and the AC power ground of the computer could damage the USB Link Kit and the controller. If you are not sure of the wiring polarity, use a USB isolator between the computer and the USB Link Kit. Purchase a USB isolator online from a third party manufacturer.**

1. Connect the laptop to the controller, ZS sensor, or RS sensor using the appropriate USB Link Kit cable(s).

NOTE: If using a USB isolator, plug the isolator into your USB port of the controller, and then plug the USB Link Kit cable into the isolator.

2. Turn off the power of the controller, set the Enhanced Access DIP switch of the controller as follows, then turn its power on again.

To communicate with...	Set switch to...
The Vertiv™ Liebert® SiteScan™ application	Off
PuTTY or HyperTerminal	On
SiteBuilder to set a custom IP address	On

3. When you are through communicating with the Local Access port, return the Enhanced Access DIP switch to its original setting.

NOTE: Using a Local Access port does not interrupt the delivery of alarm and trend notifications to the specified BACnet Alarm Recipient of the controller.

You cannot use a Local Access port to set up BBMDs because Local Access connections do not communicate using BACnet/IP.

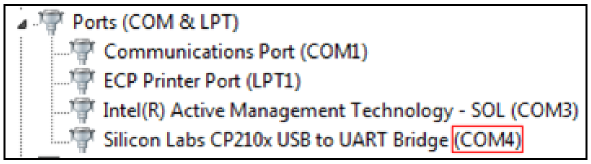
A router must be present to receive colors from the controller network.

Setting up a Local Access Connection

To set up communication between the Liebert® SiteScan™ application on your laptop and the controller:

1. On the Liebert® SiteScan™ System Configuration ⚙ tree, select *Connections*.
2. On the Configure tab, click *Add*.
3. On the Configure tab, from the Type drop down list, select BACnet/Rnet Local Access Connection.
4. Click *Add*.
5. Optional: Edit the Description.
6. Type the Port number of the computer to which the USB cable is connected to.

NOTE: To find the port number, plug the USB cable into the USB port of the computer, then select Start > Control Panel > System > Device Manager > Ports (Com & LPT). The COM port number is beside Silicon Labs CP210x USB to UART Bridge.



Ports (COM & LPT)
- Communications Port (COM1)
- ECP Printer Port (LPT1)
- Intel(R) Active Management Technology - SOL (COM3)
- Silicon Labs CP210x USB to UART Bridge (COM4)

7. Set the Baud rate.

Local Access Port	Baud Rate
5-pin	115200
8-pin round	38400

8. On the right side of the page, in the Networks using selected connection table, click the checkbox next to the network you want to connect to.
9. Click *Accept*.
10. Click the *Start button*.

NOTE: If an error message appears, make sure the COM port you selected is not in use. For example, PuTTY may be open and is holding the port open.

11. If using the 5-pin Local Access port, on the Network tree, select the controller that you are connected to.
12. Click , then *select Manual Command*.
13. Type rnet here in the dialog box, then click *OK*.
14. On the Properties page, click Module Status. If a Modstat (See Obtaining a Modstat on page 161) report appears, the Vertiv™ Liebert® SiteScan™ application is communicating with the controller.

Troubleshooting a Local Access Connection

Inability to communicate over a Local Access connection may cause the following symptoms:

- Question marks on Liebert® SiteScan™ Properties pages and Graphics pages
- Cannot obtain a Modstat from the connected controller
- Controller Status report displays purple for a connected BACnet/IP controller
- Cannot download to connected controller
- A message says Local Access is disabled or unable to connect.

Possible cause	Solution
Network number in SiteBuilder does not match the number found in the controller	Use the rnet here manual command to force the local device to accept the next download applied. 1. Click , then select Manual Command. 2. In the manual command field, type rnet here. 3. Download Parameters or All Content to the controller to which you are connected. 4. On the Vertiv™ Liebert® SiteScan™ Network tree, select the controller. 5. On the Properties page, click Module Status to verify communication with the controller.
Liebert® SiteScan™ communication timeout settings are not sufficient for your network configuration.	Increase your communication timeout settings. 1. On the System Configuration ⚙ tree, select Connections. 2. On the Configure tab, select BACnet/Rnet Connection. 3. Click ▶ next to Tuning Parameters. 4. Double the values in the Comm Timeout and Comm Attempts fields. **NOTE: If changing these values does not fix your intermittent communication, contact Automated Logic Technical Support.**
Selected COM port is in use	Shut down other applications such as PuTTY that may be running and holding the port open.
Baud rates are inconsistent	Verify that the Silicon Labs CP210x USB to UART Bridge and the Liebert® SiteScan™ application are using the baud rate used by the controller.
Local Access is disabled	See Disabling Local Access of the Controller on page 169 .

Communicating using PuTTY

You can connect a computer to a Local Access port of the controller and then use PuTTY, a free open source terminal emulation program, to:

- Set the baud rate for ports S1 or S2 on Vertiv™ Liebert® SiteLink controllers
- Set controller properties, such as IP address and network information
- Retrieve a Modstat (See Obtaining a Modstat on page 161)

Prerequisites

- A computer with a USB port
- A USB Link Kit. See the USB Link Kit Technical Instructions.

NOTE: The USB Link Kit driver is installed with a Liebert® SiteScan™ v5 or later system. Please refer to the Silicon Labs website and search "CP210x USB to UART Bridge VCP Drivers" for the most current device drivers. Install the driver before you connect the USB Link Kit to your computer.

- The appropriate controller driver

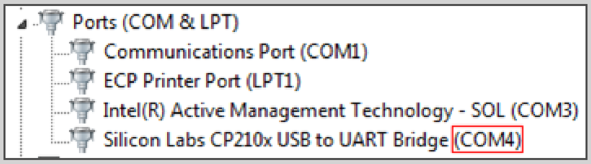
For devices with a...	Use driver...
5-pin Local Access port	v1.70 or later
Round 8-pin Local Access port	v2.00 or later

CAUTION: If multiple controllers share power but polarity was not maintained when they were wired, the difference between the ground of the controller and the AC power ground of the computer could damage the USB Link Kit and the controller. If you are not sure of the wiring polarity, use a USB isolator between the computer and the USB Link Kit. Purchase a USB isolator online from a third-party manufacturer.

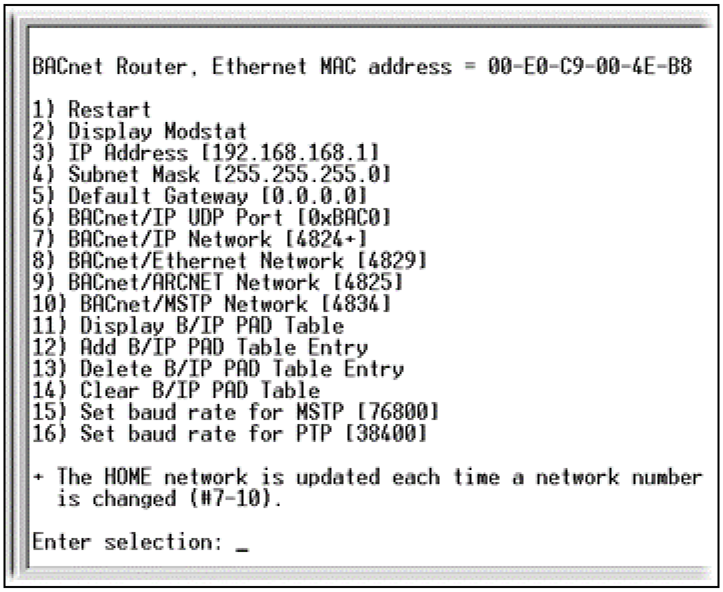
1. Download and install *PuTTY* from the PuTTY website (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).
2. Connect the *laptop* to the controller, ZS sensor, or RS sensor using the appropriate USB Link Kit cable(s).

NOTE: If using a USB isolator, plug the isolator into the USB port of your computer, and then plug the USB Link Kit cable into the isolator.

3. Turn off the power of the controller, set its Enhanced Access Port DIP switch to ON, then turn its power on again.
4. To change a router IP address, subnet mask, or default gateway, set its IP Address DIP switch to Assigned.
5. Start *PuTTY*.
6. Under Category > Connection, select Serial.
7. Under Options controlling local serial lines, enter the below settings:

<table>
<tr><td>Field</td><td colspan="2">Value</td></tr>
<tr><td>Serial line to connect to</td><td colspan="2">Replace X with the port number of the computer that the USB Link Kit cable is connected to.
NOTE: To find the port number, select Start > Control Panel > System > Device Manager > Ports (Com & LPT). The COM port number is beside Silicon Labs CP210x USB to UART Bridge.

Ports (COM & LPT)
Communications Port (COM1)
ECP Printer Port (LPT1)
Intel(R) Active Management Technology - SOL (COM3)
Silicon Labs CP210x USB to UART Bridge (COM4)</td></tr>
<tr><td>Speed (baud)</td><td colspan="2">Type the appropriate baud rate from the table below.</td></tr>
<tr><td></td><td>For</td><td>Speed</td></tr>
<tr><td></td><td>Vertiv™ Liebert® SiteLink-E</td><td>115200 for Rnet 38400 for S2</td></tr>
<tr><td></td><td>Vertiv™ Liebert® SiteGate-E</td><td>38400</td></tr>
<tr><td>Data Bits</td><td colspan="2">8</td></tr>
<tr><td>Stop Bits</td><td colspan="2">1</td></tr>
<tr><td>Parity</td><td colspan="2">None</td></tr>
<tr><td>Flow Control</td><td colspan="2">None</td></tr>
</table>

8. Click *Open*. A window appears as shown below.



```
BACnet Router, Ethernet MAC address = 00-E0-C9-00-4E-B8

1) Restart
2) Display Modstat
3) IP Address [192.168.168.1]
4) Subnet Mask [255.255.255.0]
5) Default Gateway [0.0.0.0]
6) BACnet/IP UDP Port [0xBAC0]
7) BACnet/IP Network [4824+]
8) BACnet/Ethernet Network [4829]
9) BACnet/ARCNET Network [4825]
10) BACnet/MSTP Network [4834]
11) Display B/IP PAD Table
12) Add B/IP PAD Table Entry
13) Delete B/IP PAD Table Entry
14) Clear B/IP PAD Table
15) Set baud rate for MSTP [76800]
16) Set baud rate for PTP [38400]

+ The HOME network is updated each time a network number
  is changed (#7-10).

Enter selection: _
```

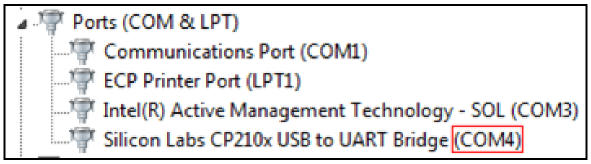
9. Do one of the following:
   - To change a property value:
     - Type the number of the property, then press Enter.
     - Type the new value, then press Enter.
   - To take an action, type number of the action, then press Enter.
10. If you changed a value, type 1, then press *Enter* to restart the controller.
11. Close *PuTTY*.
12. When finished, turn off the power of the controller, set its Enhanced Access Port DIP switch to Off, then turn the power on again.

Setting up a BACnet/Rnet Connection in the Vertiv™ Liebert® SiteScan™ Interface

For the Liebert® SiteScan™ application to communicate with the Rnet port, you must do the following:

1. On the System Configuration tree, select Connections.
2. On the Configure tab, from the Type drop down list, select *BACnet/Rnet Local Access Connection*.
3. Click *Add*.
4. Optional: Edit the *Description*.
5. Type the Port number of the computer that the USB cable is connected to.

NOTE: To find the port number, plug the USB cable into the USB port of the computer, then select Start > Control Panel > System > Device Manager > Ports (Com & LPT). The COM port number is beside Silicon Labs CP210x USB to UART Bridge.



- Ports (COM & LPT)
  - Communications Port (COM1)
  - ECP Printer Port (LPT1)
  - Intel(R) Active Management Technology - SOL (COM3)
  - Silicon Labs CP210x USB to UART Bridge (COM4)

6. Set the *Baud rate to 115200*.

7. On the right of the page, in the Networks using selected connection table, click the *checkbox* next to the network you want to connect to.
8. Click *Accept*.
9. Click the *Start button*.

NOTE: If an error message appears, make sure the COM port you selected is not in use. For example, PuTTY may be open and is holding the port open.

10. On the Network tree, select the *controller* that you are connected to.
11. Click , then *select Manual Command.*
12. Type rnet here in the dialog box, then click *OK*.
13. On the Properties page, click *Module Status*. If a Modstat report appears, the Vertiv™ Liebert® SiteScan™ application is communicating with the controller.

4.1.5 Disabling Local Access of the Controller

To limit access to your system, you can disable the Local Access port of the ExecB device from communicating with the Liebert® SiteScan™ application running on a laptop.

1. Select the *controller* on the Liebert® SiteScan™ Network tree.
2. On the Properties page, select Disable Local Access to Server and Tools.
3. Click *Accept*.

NOTE: Use Global Modify to change this setting for multiple controllers simultaneously.

The following can communicate with a disabled port:

- Touchscreen device
- PuTTY (ExecB only)
- Virtual BACview application (ExecB only)
- HyperTerminal (ExecB only)
- SiteBuilder—for IP devices (ExecB only)

4.1.6 Network Security

.The controller of the Liebert® SiteScan™ building automation system and server must be secure. However, achieving this security can be challenging because of the complexities of networks, firewalls, and virtual private networks (VPN's). Two means for increasing the security of your system are:

- While the Liebert® SiteScan™ server was designed to be secure, BACnet is an open protocol that can pose risks for the controllers. The most secure system is one that is completely isolated from the Internet, but that is not always possible. The v6-02 or later drivers for Vertiv controllers with Ethernet capability have a BACnet firewall feature that allows you to restrict communication with the controller to all private IP addresses and/or to a whitelist of IP addresses that you define. To set this up, go to the Network tree > the router > Driver > Bacnet Firewall. Follow the instructions in the interface.
- You should use TLS (HTTPS, not HTTP) to secure the client device that you are using to connect to the Liebert® SiteScan™ server. See What is TLS (HTTPS)? (See Network Security above) for instructions on setting up TLS.

For information on secure network configurations, options, and best practices, see the following documents on https://accounts.oemctrl.com/tsapl/ctrackweb.nsf/download under Documents > SiteScan Security.

- Security Best Practices for a Vertiv™ Liebert® SiteScan™ system
- Liebert® SiteScan™ Security

What is TLS (HTTPS)?

The Liebert® SiteScan™ application supports Transport Layer Security (TLS), a secure protocol used for transmitting private information over the Internet using HTTPS.

NOTE: TLS is a more recent version of Secure Sockets Layer (SSL).

TLS uses a method called public-key cryptography to provide:

- Client/server authentication before transmitting data.
- Strong encryption of all data before it is transmitted over the TLS connection and decryption of the data upon receipt.

Public key cryptography uses keys and certificates to authenticate users. The keys and certificates are protected with a keystore password.

There are 2 options as mentioned below for creating a certificate:

- A certificate from a trusted Certificate Authority (CA). This option provides the most security because the CA performs the authentication. See Setting up TLS Using a Certificate Authority (CA) Certificate below .
- A self signed certificate. This option is quicker and easier to set up, but is less secure. See Setting up TLS using a Self Signed Certificate on page 174 .

Keystore Explorer (See To set up Keystore Explorer on page 177) is an open source, third party tool that can be used to manage your certificates.

Setting up TLS Using a Certificate Authority (CA) Certificate

NOTE: TLS is a more recent version of Secure Sockets Layer (SSL).

NOTE: For a list of trusted Certificate Authorities see the web browser certificates documentation.

Step 1: Creating a key and Certificate

1. In SiteBuilder, select *Configure* > *Preferences* > *Web Server*.
2. Select *HTTPS* Only in the Enabled Web Server Ports field.

NOTE: For quicker navigation, select Both HTTP and HTTPS if operators will connect to the system from an internal network and the Internet. Change the setting in the HTTPS Port field only if the system will be using a non standard port.

3. Click *Delete Certificate*.

⚠ **CAUTION: Clicking *Delete Certificate* button will delete all certificates in your system.**

4. Click *Make Certificate*.
5. In the Make Certificate dialog box, type a Keystore password.
6. In the DNS name of your server field, type the address of the server using one of the following formats:

- The domain name if accessing through the Internet. Example: www.abi.com.
- The IP address if accessing through the Internet. Example: 216.227.49.36.
- The computer name if accessing internally. Example: mycomputerxp.

NOTE: The address format you use in this field is the format operators must use to access the system in a web browser.

The entered names will be used as the Subject Alt Names in the certificate.

You can enter more than one name. Separate the names by a comma and no spaces.

7. The next 5 fields are optional, but the more information you enter, the more secure your key is.
8. Click *Apply*.
9. In the Keystore Password field, type the password that you entered in step 5 above.

NOTE: This field is case sensitive.

10. Click *OK*.

Step 2: Obtaining a CA Certificate

1. Create a Certificate Signing Request (CSR).
   - In the start menu of Vertiv™ Liebert® SiteScan™ server, select All Programs > Accessories > Command Prompt.
   - Type the below command as a single line of text, replacing <x.x> with the version number of the system:
     C:\SiteScan_Web_<x.x>\bin\java\jre\bin\keytool.exe -certreq -alias SiteScan -keystore C:\SiteScan_Web_<x.x>\webserver\keystores\certkeys -file C:\SiteScan_Web <x.x>\webserver\keystores\request.csr
   - Press *Enter*. This creates a request.csr file located in C:\SiteScan_Web_x.x\webserver\keystores.
2. Get a certificate from a certificate authority (typically from their website). The CA will ask you to send a copy of the CSR file (request.csr). Or, the CA may ask you to paste the contents of the request.csr file into their website.
3. You will receive the following files from your CA. Copy these .cer files to the SiteScan_Web_x.x folder:
   - A chain or root certificate
   - One or more intermediate certificates (Not all CAs provide intermediate certificates.)
   - A received certificate
     See NOTE at the bottom of this topic.
4. Import the root certificate.
   - In the start menu of Liebert® SiteScan™ server, select All Programs > Accessories > Command Prompt.
   - Type the following command as a single line of text, replacing <x.x> with the versionof the system number and <root.cer> with the name of the root certificate file:
     C:\SiteScan_Web_<x.x>\bin\java\jre\bin\keytool.exe -import -trustcacerts -alias root -keystore C:\SiteScan_Web_<x.x>\webserver\keystores\certkeys -file \SiteScan_Web_<x.x>\<root.cer>
   - Press *Enter*.
   - The information for the root key is displayed and a window will appear to confirm the certificate. Type yes.
5. If the CA provided an intermediate certificate, import that certificate.
   - In Command Prompt, type the following command as a single line of text, replacing <x.x> with the version number of the system and <intermediate.cer> with the name of the intermediate certificate file:
     C:\SiteScan_Web_<x.x>\bin\java\jre\bin\keytool.exe -import -trustcacerts -alias intermed -keystore C:\SiteScan_Web_<x.x>\webserver\keystores\certkeys -file \SiteScan_Web_<x.x>\<intermediate.cer>
   - Press *Enter*.

NOTE: If the CA provided more than one intermediate certificate, repeat step 5 for each one. Replace -alias intermed with -alias intermed1, -alias intermed2, etc.

6. Import the received certificate.
   - In Command Prompt, type the following command as a single line of text, replacing <x.x> with the version number of the system and <received.cer> with the name of the received certificate file: C:\SiteScan_Web_<x.x>\bin\java\jre\bin\keytool.exe -import -trustcacerts -alias SiteScan_Web_ -keystore C:\SiteScan_Web_<x.x>\webserver\keystores\certkeys -file \SiteScan_Web_<x.x>\<received.cer>
   - Press *Enter*.

NOTE: If you are not sure which file is which certificate, double click each .cer file. Go to the Certificate Path tab. If you see:

- Only 1 entry, this is your root certificate.
- Multiple entries but the last one is your domain name, this is your received certificate.
- Multiple entries but the last one is not your domain name, this is an intermediate certificate.

Step 3: Installing the Certificate

Start the Vertiv™ Liebert® SiteScan™ Server application (this may take up to a minute), then do the appropriate steps below on each workstation to access SiteScan Server.

1. Start your *browser*.
2. In the address bar, type the URL of the server running the Liebert® SiteScan™ application using the server address that you entered in Step 1: Creating a key and Certificate on page 170 . Use the TLS indicator https instead of http. For example, https://216.227.49.36.
3. Do one of the following:
   - If the TLS certificate is valid and trusted by the browser, skip to Step 4: Enable TLS in your web browser (See Step 4: Verifying that TLS is Enabled in your Web Browser on the facing page).
   - If the certificate is not valid or not trusted by the browser, follow the steps below for your browser.

For **Edge** and **Google Chrome**

1. If the page displays Your connection is not private, do the below steps.
2. Export certificate to a known location:
   - Press *F12* to bring up the Developer Tools pane.
   - Navigate to the Security tab, and then click *View Certificate*.
   - On the Details tab, click *Copy to File*.
   - In the Certificate Export Wizard, click *Next*.
   - Choose an option, then click *Next*.
   - Click *Browse*.
   - In the File Name field, type a name for your export file.
   - Click *Save*.
   - Click *Next*.
   - Click *Finish*.
   - In the message box The export was successful, click *OK*.
   - Click *OK* again.
   - Press *F12* to close the Developer Tools pane.

3. Import saved certificate:
   - Click ⋮ on the *browser toolbar*, then select *Settings*.
   - Click *Privacy, search, and services*, then click *Manage certificates*.(for Step)
   - Click Advanced.(for Google Crome)
   - Scroll down to Privacy and security, then click Manage certificates.(for Google Crome)
   - On the Trusted Root Certification Authorities tab, click *Import*.
   - In the Certificate Import Wizard, click *Next*.
   - Click *Browse*, then select the *file* you exported in step 2.
   - Click *Open*.
   - Click *Next*.
   - Select *Place* all certificates in the following store.
   - Click *Browse*, then select *Trusted Root Certification Authorities*.
   - Click *OK*.
   - Click *Next*.
   - Click *Finish*.
4. Click *Yes* in the Security Warning dialog box to install the certificate.
5. In the message box Import was successful, click *OK*.
6. Click *Close*.
7. Close *Edge*, then open it again.
8. Log in to the *Vertiv™ Liebert® SiteScan™ interface*.

Mozilla Firefox

1. If the page displays This Connection is Untrusted, expand I understand the Risks, then click Add Exception.
2. Check *Permanently store* this exception.
3. Click *Confirm Security Exception*.
4. Close *Firefox*, then open it again.
5. Log in to the Liebert® SiteScan™ interface.

Safari

1. If the page displays the message, Safari can't verify the identity of the website, click *Show Certificate*.
2. Check Always trust <DNS name you entered in SiteBuilder> when connecting to <SiteScan Server address>.
3. Click *Continue*.
4. Enter the administrator password for your Apple device.
5. Click *Update Settings*.

Step 4: Verifying that TLS is Enabled in your Web Browser

The Liebert® SiteScan™ application attempts to use TLS when communicating with a web browser. The web browser must be set up for TLS.

- Google Chrome, Mozilla Firefox, and Safari use TLS by default.
- In the Internet Explorer security options:
- Verify that Use TLS 1.x is checked.

- Verify that SSL 2.0 and SSL 3.0 are not checked.

Setting up TLS using a Self Signed Certificate

NOTE: TLS is a more recent version of Secure Sockets Layer (SSL).

Step 1: Create a Key and Certificate

1. In SiteBuilder, select *Configure* > *Preferences* > *Web Server*.
2. Select *HTTPS Only* in the Enabled Web Server Ports field.

NOTE: For quicker navigation, select Both HTTP and HTTPS if operators will connect to the system from an internal network and the Internet. Change the setting in the HTTPS Port field only if the system will be using a non-standard port.

3. Click *Delete Certificate*.

CAUTION: Clicking this button will delete all certificates in your system.

4. Click *Make Certificate*.
5. In the Make Certificate dialog box, type a *Keystore password*.
6. In the DNS name of your server field, type the address of the server using one of the following formats:
    - The domain name if accessing through the Internet. Example: www.abi.com.
    - The IP address if accessing through the Internet. Example: 216.227.49.36.
    - The computer name if accessing internally. Example: mycomputerxp.

NOTE: The address format you use in this field is the format operators must use to access the system in a web browser.

The entered names will be used as the Subject Alt Names in the certificate.

You can enter more than one name. Separate the names by a comma and no spaces.

7. The next 5 fields are optional, but the more information you enter, the more secure your key is.
8. Click *Apply*.
9. In the Keystore Password field, type the password that you entered in step 5 above.

NOTE: This field is case sensitive.

10. Click *OK*.

Step 2: Install the Certificate

NOTE: If you change the server address after you create and install your certificate (for example, change from an IP address to a domain name), you must create a new key and certificate using the new address, then install the new certificate.

Start the Vertiv™ Liebert® SiteScan™ Server application (this may take up to a minute), then do the appropriate steps below on each workstation that will access SiteScan Server.

Edge

1. If the page displays Your connection is not private, follow the steps below.

2. Export certificate to a known location:
   - Press *F12* to bring up the Developer Tools pane.
   - Navigate to the Security tab, and then click *View Certificate*.
   - On the Details tab, click *Copy to File*.
   - In the Certificate Export Wizard, click *Next*.
   - Choose an option, then click *Next*.
   - Click *Browse*.
   - In the File Name field, type a name for your export file.
   - Click *Save*.
   - Click *Next*.
   - Click *Finish*.
   - In the message box The export was successful, click *OK*.
   - Click *OK* again.
   - Press *F12* to close the Developer Tools pane.
3. Import saved certificate:
   - Click ... on the *browser toolbar*, then select *Settings*.
   - Click *Privacy, search, and services*, then click *Manage certificates*.
   - On the Trusted Root Certification Authorities tab, click *Import*.
   - In the Certificate Import Wizard, click *Next*.
   - Click Browse, then select the file you exported in step 2 .
   - Click *Open*.
   - Click *Next*.
   - Select *Place all certificates* in the following store.
   - Click *Browse*, then select Trusted Root Certification Authorities.
   - Click *OK*.
   - Click *Next*.
   - Click *Finish*.
4. Click *Yes* in the Security Warning dialog box to install the certificate.
5. In the message box Import was successful, click **OK**.
6. Click *Close*.
7. Close *Edge*, then open it again.
8. Log in to the Vertiv™ Liebert® SiteScan™ interface.

Google Chrome

1. Start *Chrome*.
2. In the address bar, type the URL of the server running the Liebert® SiteScan™ application using the server address that you entered in Step 1: Create a key and certificate (See Step 1: Creating a key and Certificate on page 170). Use https instead of http. For example, https://216.227.49.36.
3. If the page displays Your connection is not private, follow the steps below.
4. Export certificate to a known location:
   - Press *F12* to bring up the Developer Tools pane.
   - Navigate to the Security tab, and then click View Certificate.

- On the Details tab, click *Copy to File*.
- In the Certificate Export Wizard, click *Next*.
- Choose an option, then click *Next*.
- Click *Browse*.
- In the File Name field, type a name for your export file.
- Click *Save*.
- Click *Next*.
- Click *Finish*.
- In the message box The export was successful, click *OK*.
- Click *OK* again.
- Press *F12* to close the Developer Tools pane.

5. Import saved certificate:
    - Click ⋮ on the *browser toolbar*, then select *Settings*.
    - Click *Advanced*.
    - Scroll down to Privacy and security, then click *Manage certificates*.
    - On the Trusted Root Certification Authorities tab, click *Import*.
    - In the Certificate Import Wizard, click *Next*.
    - Click Browse, then select the file you exported in step 2 .
    - Click *Open*.
    - Click *Next*.
    - Select Place all certificates in the following store.
    - Click *Browse*, then select Trusted Root Certification Authorities.
    - Click *OK*.
    - Click *Next*.
    - Click *Finish*.
    - Click Yes in the Security Warning dialog box to install the certificate.
    - In the message box Import was successful, click *OK*.
    - Click *Close*.
    - Close *Chrome, then open it again*.
    - Log in to the Vertiv™ Liebert® SiteScan™ interface.

Mozilla Firefox

1. Start *Firefox*.
2. In the address bar, type the URL of the server running the Liebert® SiteScan™ application using the server address that you entered in Step 1: Create a key and certificate (See Step 1: Creating a key and Certificate on page 170). Use https instead of http. For example, https://216.227.49.36.
3. If the page displays This Connection is Untrusted, expand I understand the Risks, then click Add Exception.
4. Check Permanently store this exception.
5. Click Confirm Security Exception.
6. Close Firefox, then open it again.
7. Log in to the Liebert® SiteScan™ interface.

Safari

1. If the page displays the message, Safari can't verify the identity of the website, click *Show Certificate*.
2. Check Always trust <DNS name you entered in SiteBuilder> when connecting to <SiteScan Server address>.
3. Click *Continue*.
4. Enter the administrator password for your Apple device.
5. Click *Update Settings*.

Step 3: Verifying that TLS is Enabled in your Web Browser

The Vertiv™ Liebert® SiteScan™ application attempts to use TLS when communicating with a web browser. The web browser must be set up for TLS.

- Google Chrome, Mozilla Firefox, and Safari use TLS by default.
- In the Internet Explorer security options:
- Verify that Use TLS 1.x is checked.
- Verify that SSL 2.0 and SSL 3.0 are not checked.

Step 4: Changing the Password Periodically

You may want to periodically change the keystore password as a precaution. To change the password, delete your existing certificate and create a new one. Follow the procedure in Step 1: Create a key and certificate (See Step 1: Creating a key and Certificate on page 170).

To set up Keystore Explorer

Keystore Explorer is an open source, third party tool that replaces working with the JAVA keytool on the command line. Follow the directions below to set up Keystore Explorer for WebServer and BACnet/SC Certificates. These instructions are for Keystore Explorer 5.4. Versions after 5.4 may have variations to the steps described in this document.

Downloading and Installing Keystore Explorer

NOTE: The following instructions apply to Keystore Explorer 5.5.0 or later.

1. Ensure you have the required version of Java. Java Runtime Environment (JRE) Version 8 or above is required. You may obtain Java from the following sources.
   - https://www.java.com/en/download/ *requires oracle technology network license agreement
   - https://adoptopenjdk.net/releases.html *open source option
2. Download Keystore Explorer from https://keystore-explorer.org.
3. Follow the directions in the Keystore Explorer user manual for installation and use. The user manual can be found on the same site as the download files.

Setting up a Web Server with Keystore Explorer

There are two methods available for setting up a web server using Keystore Explorer. You can use either of the following:

- Certificate Singing Request (See Setting up a Web Server using Certificate Signing Request below)
- Provided certificates (.pfx) (Setting up a Web Server with the Provided Certificates (.pfx file) on the next page)

Setting up a Web Server using Certificate Signing Request

For a web server to use HTTPS, it must have a TLS certificate signed with a standard trusted certificate authority (CA). This section describes how to take the generated self signed certificate, generate a CSR, and import the response from the CA.

Prerequisites

- An account with a Certificate Authority
- Webserver configured for HTTPS with self signed certificate. See Setting up TLS Using a Certificate Authority (CA) Certificate on page 170 .
- The keystore password that was used to setup the self signed certificate

1. Open the Webserver Keystore
   - In Keystore Explorer, click File > Open, and browse to <WebServer Install>\webserver\keystores.
   - Select *certkeys,* and then click *Open.*
   - Enter the *keystore password*.
   - Click *Entry Name*, and select Vertiv™ Liebert® SiteScan™.
2. Generate CSR (Certificate Signing Request)
   A CSR is a text file signed with your private key.
   - Right click SiteScan, and select *Generate CSR*.
   - Enter the *keystore password.*
   - Copy and save the path in CSR File. This is where the CSR file will be saved and you will need it later.
   - Check with your CA for any additional required fields, for example, Challenge, Optional Company Name, or Signature Algorithm. Defaults are set for most common options.
3. Import the *CSR File*
   - Send the CSR File to your Certificate Authority. Your CA Authority may accept requests by email attachment, or provide a portal where you can upload the file.
   - Save the CA reply file the CA provides to your computer.
   - Open the webserver keystore, click Entry Name, and select Liebert® SiteScan™.
   - Right click and select Import *CA Reply*" (From File).
   - Save the *keystore.*
   - Restart the webserver.

Setting up a Web Server with the Provided Certificates (.pfx file)

Prerequisites

- A Certificate Archive with private key, .pfx file, .jks file, .pcks12
- The password for the archive and private key.

Creating certkeys file from certificate archive.

1. Click *Open > File and select the .pfx file* containing certificates.
2. Enter the *keystore password.*
3. Click *Tools > Change Keystore Type* and select *PKCS12.*
4. Enter the *keystore password*.
5. Click *File > Save As* and save the files as *"certkeys"*. Type must be "All Files" with no file suffix.
6. Select the *private key entry*.
7. Right click and select *Rename*.
8. Enter alias SiteScan.
9. Save the *file.*
10. Move the new certkeys file into "<Install Directory>\webserver\keystores".

11. Replace the existing certkeys file with the new certkeys file.

Configuring the keystore password using Sitebuilder

1. Open Sitebuilder.
2. Click Configure and then select Web Server.
3. Set keystore password to the password used to create the certkeys file.
4. Restart the WebServer.

Creating a BACnet/SC Certificate Authority using Keystore Explorer

Use Keystore Explorer to create a Certificate Authority (CA) to sign BACnet/SC certificates for the devices on a BACnet/SC network.

NOTE: We recommend creating a separate keystore for each network, each with its own password.

1. Create a *new keystore* by clicking Create a Keystore from the Quick Start menu or by clicking the New icon in the tool bar.
2. Select *keystore type PKCS#12*.
3. Click *File > Save* to save the keystore as a ".pkcs12" file.
4. Click *Tools > Generate Key Pair*.
5. Select one of the following, set the associated fields as indicated below, then click OK.

Fields:

- EC (recommended):
  Set SEC, Named Curve secp256r1
- RSA:
  Key Size 2048

6. Set the *Validity Period*, and then click *Apply*. We recommend a minimum of 20 years. See replacing a BACnet/SC Certificate Authority of the network.
   TIP Set Validity Start to a previous date to avoid potential time zone issues.
7. Click the Edit icon beside the Name field to complete the Name fields with appropriate values for the site and customer.
8. Click *Add Extensions > Use Standard Template*, select *CA*, then click *OK*.
9. Click *OK* on the Add Certificate Extensions dialog.
10. Click *OK* on the Generate Key Pair Certificate dialog.
11. In Enter Alias, enter a meaningful alias that identifies the owner of the signing certificate , then click *OK*.
12. Set a *key pair password*. We recommend giving each CA its own unique password.
13. This new CA will be used to replace an existing CA on a BACnet/SC network. To export the new CA certificate:
    - Right click on the *CA* and select *Export > Export Certificate Chain*.
    - On the Export Certificate Chain dialog choose:

1. Export Length: Head Only
2. Export Format: X.509
3. PEM: select checkbox
4. Filename: Enter path and filename. File extension should remain .cer

Signing a BACnet/SC Certificate Signing Request with Keystore Explorer

A BACnet/SC network requires each device to have a unique operational certificate signed by a common Certificate Authority (CA). You can use Keystore Explorer to sign an operational certificate using an existing CA.

1. Open the *keystore* containing the CA you wish to use.
2. Right click *on the CA* and select Sign > Sign CSR.
3. Select the *CSR file* to sign. For example, "cert.csr".
4. On the *Sign CSR dialog*:
    - Select the desired Validity Period on the Sign CSR dialog, and then click *Apply*.

NOTE: When choosing a validity period, consider that this process will have to be repeated whenever certificates expire. See Creating or Replacing a BACnet/SC operational certificate of the deivce to replace this certificate when it expires.
Set Validity Start to a previous date to avoid potential time zone issues.

- Click *Add Extensions*.
- Click *Use Standard Template*.
- Select SSL Server, then click *OK*.
- Select the *Extended Key Usage extension* and click ✎ to select TLS Web Client Authentication. TLS Web Server Authentication should already be selected, do not deselect it. Click *OK*, then click OK on the Add Certificate Extensions dialog.
- On the Sign SCR dialog, click *OK*.
- On the Export Certificate Chain dialog, under Export File, set the path and filename where the signed certificate (.cer) file will be created. Click *Export*.

4.2 Setting Up Hardware

4.2.1 Commissioning Equipment

Follow the process below to commission system equipment.

Step 1 : Checking the Point Setup

1. On the Vertiv™ Liebert® SiteScan™ Geographic tree, select the piece of equipment you want to check out.
2. Click *Properties*.
3. View and change properties on the I/O Points, Alarm Sources, Trend Sources, Network Points, Display Points, BACnet Objects, and Rnet Points tabs. See "Property descriptions" below.
4. After completing the equipment checkout, click the *Equipment Checkout* tab.
5. Select *Checked Out*. This field is for your reference only.
6. Optional: Type notes.
    - Notes typed in this field appear in the Equipment Checkout report and can also be changed from the SiteBuilder Notes tab and the Properties page Notes field for this piece of equipment.
    - Notes remain in this field until an operator deletes them.
7. Optional: Click the *Reports* drop down arrow button, then select and run each of the following reports to verify your work:
    - Equipment > Point List
    - Alarms > Alarm Sources

- Equipment > Trend Usage
- Equipment > Network IO

NOTE: You can export the calibrated data so that you can import it into another control program. See Optional: Importing/Exporting the Calibration Data on page 188 .

Property Descriptions

Table 4.3 I/O Points

Item	Descripion				
Name	Click the name to display the microblock popup. **NOTE: A red name indicates a fault condition where the point may be misconfigured.** Example: No input/output number or a nonexistent input/output number.				
Type	Type of Input or Output point.				
Value	The present value of the point.				
Offset	Allows for fine calibration of the present value of an analog point.				
Polarity	Determines the binary normal of the point polarity in the control program. **NOTE: Polarity is not the hardware normally open/normally closed position.**				
Locked	Select the *checkbox* to lock the present value at the value you specify.				
Exp:Num	Expander numbers and input or output numbers associated with where the physical point wires, such as a sensor wire, are physically connected to a controller.				
I/O Type	Selects the bank of physical inputs or outputs on the controller.				
Sensor	Selects how the physical input is mapped to the engineering units. Min/Max is used with the sensor type of linear to scale the input to engineering units. **NOTE: This field is ignored for sensor types other than linear.**				
	Example: AI	Linear sensor type min	-10		
		max	50		
		When input reads	100%	The value is	50
			50%		20
			0%		-10
Actuator	Selects how the present value in engineering units is mapped to the physical output. Min/Max is used with the actuator type of linear to scale the output from engineering units. **NOTE: This field is ignored for actuator types other than linear.**				
	Example: AO	Linear sensor type min	*-10*		
		max	*50*		
		When input reads	*50*	The output is	*100%*
			20		*50%*
			-10		*0%*
Resolution	Amount by which the present value will change. Example: If a physical input changes by 1, but the resolution is set at 2, then the present value remains the same. If the input changes by 2, the present value will then change by 2.				
Checked Out Checkout Notes	These fields are for your reference only.				

Table 4.4 Alarm Sources

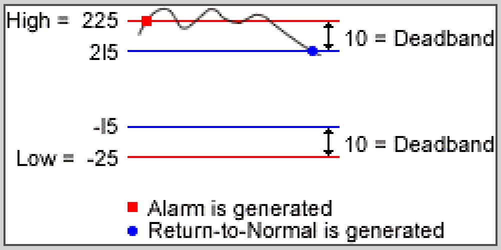
Name	Click the name to display the microblock popup.
Type	Type of point that is an alarm source.
Alarm	Shows *Alarm* in red if a current alarm exists.
Network Visible	Select to allow the microblock to be seen by the Vertiv™ Liebert® SiteScan™ application and third party BACnet controllers on the network.
Potential Alarm Source	Select to enable the microblock to generate alarms.
Alarm Enabled	**Alarm**—Select to generate an alarm when conditions exceed the limits set in the Condition column. **Return**—Select to generate a return to normal message when the alarm condition returns to a normal state. **Fault**—Select to have an alarm generated if the alarm source is not configured correctly. For example, a misconfigured channel number produces a no sensor fault.
Requires ack	**Alarm**—Select to require that the alarm be acknowledged. **Return**—Select to require that the return to normal message be acknowledged.
Critical	Select if the alarm is critical.
Template	You can change the alarm template assigned to the microblock.
Category	You can change the alarm category assigned to the microblock.
Dial on alarm	Select to have this alarm immediately delivered through a modem connection.
Condition	An alarm will be generated if conditions exceed the low or high limits set. Deadband: The amount inside the normal range by which an alarm condition must return before a return-to-normal notification is generated. Example:  High = 225 215 10 = Deadband -15 Low = -25 10 = Deadband Alarm is generated Return-to-Normal is generated
Delay	Delay time in seconds for notification after an alarm is generated.

Table 4.5 Trend Sources

Name	Click the name to display the microblock popup. **NOTE: A red name indicates a fault condition where the point may be misconfigured.** Example: No input/output number or a nonexistent input/output number.
Type	The type of point being trended.
Sample Interval	The interval or COV (Change of Value) increment that triggers the trend sample.

Table 4.5 Trend Sources (continued)

Max Samples	The maximum number of trend samples the controller will hold before replacing oldest samples with newest. **NOTE: Changing Max Num of Samples will delete all of the point trend samples currently stored in the controller. But, you can transfer the trend data from the controller to the system database before you change the value. Click on the point name. In the popup, go to *Trends > Enable/Disable*, and then click *Store Trends Now*.**
Stop When Full	Stops trend sampling when the maximum number of samples is reached.
Historian - Enable (Samples)	Triggers the trend historian to record trends when the controller has accumulated the defined number of samples. This must be less than the Max Samples allocated. **NOTE: A good value is a little less than 1/2 of the Max Samples.**
Keep for days	Defines how long trend data is stored in the system database. This is based on the date that the sample was read. Select *System Default* to use the value defined on the System Settings > General tab, or select *Custom* to set a value for this trend only.
Samples in Controller	The number of samples that are currently stored in the controller.

Table 4.6 Network Points

Name	Click the name to display the microblock popup. **NOTE: A red name indicates a condition where the point may be misconfigured.**
Type	Type of network point.
Value	The point's present value. Example: For a Maximum point type, Value is the maximum value of all the target BACnet object properties the point is communicating with.
Locked	Select the check box to lock the present value at the value you specify.
Default Value	The value that the control program will use as the value of the point when communication with the target defined in the Address column is lost or communication is disabled.
Com Enabled	Select to enable this network communications of the point. Disable this property for troubleshooting. **NOTE: Select *All* in the column header to quickly enable all points in the control program.**
COV Enable	Select to make: • A digital network output point write a value to the target defined in the Address column only when the value changes. • An analog network output point write a value only when the value changes by the specified increment.
Refresh Time (mm:ss)	The time interval at which the network point writes or retrieves the value to or from the target. For network output points, this time is used when COV is not enabled or when COV is enabled but fails. **NOTE: If COV fails and the Refresh Time is zero, the value is sent once per second.**
Test	Select to test the network connections. The Vertiv™ Liebert® SiteScan™ application immediately writes to or retrieves the value from the target.
Address	The address of the target BACnet object property or third-party value that the point communicates with. **NOTE: An address from a SiteBuilder source tree, such as a cool or heat source tree, can be edited only in SiteBuilder.** **NOTE: Click *Search/Replace* at the top of the Address column to have the Liebert® SiteScan™ application replace all instances of specific text in the addresses with different text. This is especially useful when copying a control program to use for multiple third party devices.**

Table 4.6 Network Points (continued)

Error	The error code and error if the point cannot communicate with the target.
Present Value	Current value of the target defined in the Address column.
Next Refresh/Next Subscription (mm:ss)	Shows one of the following: • The next time the network point will write to or retrieve a value from the target defined in the Address column. • The next time the network point will subscribe to the target.
Checked Out Checkout Notes	These fields are for your reference only.

BACnet Objects

This tab shows all BACnet objects in the control program. Display microblocks that have a Device Alias appear in separate tables, one table for each alias.

Name	The name used in the Vertiv™ Liebert® SiteScan™ interface for this object. **NOTE: A red name indicates a condition where the point may be misconfigured.**
Reference name	A unique identifier that allows the point to be referenced for use in graphics, source tree rules, or network links.
Type	The BACnet object type.
Present Value	The object's current value.
Locked	Check to lock the third-party object to a specific value.
Device	A device alias. See "To reuse a control program" in Device Alias.
Object Name	An alpha numeric string that is unique within the third party device.
Object ID	A combination of the object type and a unique instance number. The object ID must be unique within the device.
Address	The address of the third-party object that the microblock references.
Network Visible	Allows other BACnet equipment to read or change the present value of the microblock. Must be enabled for this microblock to generate alarms.

Rnet Points

This tab shows varying information for the different point types. Below are all possible properties that may appear on this tab and a list of the applicable points. The following list is arranged alphabetically.

Combination Algorithm	(Analog Sensed Values) The method used to combine the ZS sensors' values to determine the output value of the microblock.
Default Value	(Analog Parameters, Binary Parameters, Multi-State Parameters) The value the control program uses until a user changes the value in the system interface.
Display Name	(All points) The microblock label used in the EIKON application and the Liebert® SiteScan™ interface. You can use any characters except the " character.

Display Resolution	(Analog Sensed Values, Analog Statuses, Analog Parameters) Defines the resolution of the value to be displayed on the ZS sensor. For example, 1 displays only integers (example: 74) and 0.5 displays values to the nearest 0.5 (example: 74.5).
Edit Increment	(Analog Parameters) To set the amount that you want press the ▲ or ▼ button of the sensor to change the value of the microblock.
Editable	(Analog Parameters, Binary Parameters) When enabled, the value of the microblock is editable on the ZS sensor.
Lock Present Value to	(Binary Parameters) Check to output the locked value from the microblock instead of the calculated value of the microblock.
Maximum	(Analog Parameters) The highest amount that this value can be changed to on the ZS sensor or in the Vertiv™ Liebert® SiteScan™ interface.
Menu Configuration	(All points) Shows which sensor screens display the value.
Minimum	(Analog Parameters) The lowest amount that this value can be changed to on the ZS sensor or in the Liebert® SiteScan™ interface.
Minimum off time	(Binary Parameters) The minimum period (seconds) that the microblock sends an off signal to the controller, regardless of the input signal to the microblock.
Minimum on time	(Binary Parameters) The minimum period (seconds) that the microblock sends an on signal to the controller, regardless of the input signal to the microblock.
Object Id	(All points) A combination of the object type and a unique instance number.
Object Name	(All points) A unique alphanumeric string that defines the BACnet object. Although the Object Name field can be edited, it is not recommended.
Reference name	(All points) A unique identifier that allows the point to be referenced for used for graphics, source tree rules, or network links.
Rnet Tag	(All points) Defines what type of information this value represents and determines how the sensor will display the value. For example, for the Rnet Tag Fan Status, the sensor automatically displays ✢ on the Home screen when the microblock is active.
Show on sensors	(Analog Sensed Values) Defines whether the ZS sensors are to display their individual sensed values, or the value determined by the Combination Algorithm.
Type	(All points) Type of Input or Output point. See Adding a Point to a Subgraph on page 27 .
Value	(All points) The point's present value.

Step 2: Checking the Controller to Sensor Wiring

Prerequisite: On the Logic page, disable the run condition(s) in the control program to prevent control program execution from affecting output values while you check out the equipment.

Binary Inputs (BI)

1. Short the *binary inputs wires* at the end device, for example, at a pump proof or fan proof.
2. On the Properties page I/O Points tab, verify the *binary input* point is closed.
3. Open the *binary input* at the end device.
4. Verify the *binary input point* is open on the Properties page.
5. Repeat for *all binary inputs*.

NOTE: If the readings on the Properties page are reversed from actual conditions, the polarity (normally closed/normally open contact position) is set incorrectly.

Analog Inputs (AI)

1. Verify the *sensor type* and the min/max values are configured correctly.
2. On the Properties page I/O Points tab, read the *analog input value*.
3. Short the *point*. The sensor should go to full range when shorted.
4. Calibrate *analog input value* by adjusting the calibration offset if needed.

Binary Outputs (BO)

1. If the binary output of the controller is wired through an equipment starter, set the starter HOA switch to Automatic.
2. On the controller, set the *binary output's HOA switch to On*.
3. Verify that the *controlled equipment has turned on*.
4. On the controller, set the *binary output's HOA switch to Automatic*.
5. On the Properties page I/O Points tab, lock the *binary output point to On*.
6. Verify the *device has turned on*.
7. Unlock the *binary output point*.
8. On the controller, set the *binary output's HOA switch to Automatic*.

NOTE: If the locked conditions on the Properties page are reversed from actual conditions, the polarity (normally closed/normally open contact position) is set incorrectly.

Analog Outputs (AO)

1. Verify the output/actuator type and the min/max values are configured correctly.
2. Lock the analog output point to the device minimum output, such as 2 volts or 0%.
3. Verify movement of the end device to the desired position.
4. Lock the voltage output to the device maximum, such as 10 volts or 100%.
5. Verify movement of the end device to the desired position.
6. Unlock.

Step 3: Checking the Controller Communication

1. On the Network tree, select the network that the controller is on.
2. On the Devices page, view the status of all controllers on that network.

NOTE: Navigate to a network or router further down in the tree to show its controllers on the Devices page.

In the Reports button drop down list, select *Network > Equipment Status*, then click *Run* to see the status of all controllers below the selected tree item.

Step 4: Checking the Equipment Operation

Refer to the sequences of operation in the system specifications to verify that the equipment operates in each operational mode (for example, occupied and unoccupied) as specified.

NOTE: If needed, you can import calibration data that you exported from another control program. See Optional: Importing/Exporting the Calibration Data on the next page .

To verify heating and cooling source tree associations, right click an item the Vertiv™ Liebert® SiteScan™ tree, and then select *Equipment Sources*.

Step 5: Collating the Checkout Information

If field technicians use copies of a system database during the commissioning process, each technician can export their Equipment Checkout status and notes. Then, you can import their Equipment Checkout information into the final system database

1. In the copy of technician of SiteBuilder, select an area or piece of equipment.
2. Select *Edit* > *Export Checkout Information* to export the checkout information for that tree item and its children.
3. Name and save the .xml file to any folder.
4. In the final system database, select any area or piece of equipment.

NOTE: You can import the .xml files to any tree item regardless of their exported location.

5. Select *Edit* > *Import Checkout Information*.
6. Browse to the .xml file that you want to import, then click Select.

NOTE: SiteBuilder displays Checkout Conflicts if the imported information conflicts with the database information. Check *Replace* to overwrite the database information with the imported information.

7. Repeat steps 5 and 6 for each .xml file that needs to be imported.

Step 6: Checking the Commissioning Status of all Equipment

1. In the Vertiv™ Liebert® SiteScan™ interface, select the system.
2. Click the *Reports* drop-down arrow button, then select *Commissioning* > *Equipment Checkout*.
3. Run the *report*.

Optional: Importing/Exporting the Calibration Data

You can export I/O point calibration data from a control program and import it into the same control program or another control program with the same I/O point configuration.

Exporting Calibration Data

1. On the Liebert® SiteScan™ Geographic 🌐 tree, select the control program whose data you want to export.
2. Scroll to the bottom of the Properties page I/O Points tab, and then click *Export*. The file <control program name>_<ref name>.xml is saved in your Downloads folder of the browser.

Importing Calibration Data

NOTE: We recommend that to export existing data as a backup before you import new data.

1. On the Liebert® SiteScan™ Geographic 🌐 tree, select the *control program* that you want to import the data into.
2. Scroll to the bottom of the Properties page I/O Points tab, and then click *Import*.
3. Browse to the file you want to import.
4. Click *Continue*. A comparison of existing data and the new import data will appear. Red text indicates one of the following errors:
   - Duplicate Data—Existing data has duplicate I/O numbers so that import cannot determine its match.
   - I/O type Mismatch—I/O type in existing data does not match I/O Type in import data.
   - Missing Import Data—Existing data has a point that import data does not have.
   - Missing System Data—Import data has a point that existing data does not have.

5. Click *OK* to complete the import. Existing data that does not show an error will be overwritten by the imported data.

Downloading Source Files from the Vertiv™ Liebert® SiteScan™ Application

1. On the Liebert® SiteScan™ Network tree, select the controller.
2. On the Properties page, select the *Download Source Files* option.
3. Click *Accept*.
4. On the Network tree, select the network of the controller.
5. On the Devices page, select the controller that you want to download.

NOTE: Shift+click or Ctrl+click to select multiple controllers to download.

6. Select *All Content* in the Download drop down list, then click the *Download* button.

NOTE: If you check Download Source Files on the Properties page but the controller does not have enough memory for the files, the download will fail. Uncheck the option and export the source files.

Exporting Source Files from the Liebert® SiteScan™ Application

1. On the System Configuration tree, select *System Settings*.
2. On the General tab under Source files, click *Export*.

Uploading source files in the Liebert® SiteScan™ application

1. On the Liebert® SiteScan™ Network tree, select the controller network.
2. On the Devices page, select the controller whose files you want to upload.

NOTE: Shift+click or Ctrl+click to select multiple controllers to upload.

3. Select *All Content* in the Upload drop-down list, then click the *Upload* button.

NOTE: If an equipment has multiple views attached, the views will be uploaded with a display name of Default. To change the names, right click the equipment in the tree, select *Configure,* then select the view in the Views > Attached list. The Display Name field appears for you to edit.

Importing Source Files in the Liebert® SiteScan™ Application

1. On the System Configuration tree, select *System Settings*.
2. On the General tab under Source files, click *Import*.
3. Browse to the **sourcefiles.zip* file.
4. Click *Continue*.
5. Click *Close*.

NOTE: If the import detects a difference between a database file and an import file with the same name, import does not overwrite the database file. A message lists any file differences so that you can resolve them.

4.2.2 Working with Control Programs in the Vertiv™ Liebert® SiteScan™ Interface

A control program is typically defined in SiteBuilder when the system is engineered, but you can do the following in the Liebert® SiteScan™ interface. These changes require you to download (See Downloading to Controllers on page 13) the controller.

- Add a control program to a controller (See Adding a Control Program to a Controller below)
- Replace an existing control program (See Replacing an Existing Control Program on the facing page)
- Retrieve a control program from the Liebert® SiteScan™, edit it in EIKON, and then return the edited program to the server (See Editing a Control Program on the facing page)
- Reload a revised control program located in webroot\<system>\programs.

On the Liebert® SiteScan™ Geographic tree, right-click the equipment, then select *Reload Control Program*. Reloading updates all instances of a control program throughout the system and marks the controller(s) for download. Liebert® SiteScan™ determines the appropriate download option (See Downloading to Controllers on page 13) based on what changed in the control program.

NOTE: If you change a control program in the EIKON application and it does not display correctly in the Liebert® SiteScan™ interface, Ctrl+right-click the Liebert® SiteScan™ action pane, and then select *Refresh*.

Adding a Control Program to a Controller

1. Select the controller on the Liebert® SiteScan™ Network tree.
2. On the Devices page > Manage tab, click the *Add Control Program* button.
3. Type a *Display Name* for the control program.
4. Select the *Controller* that you are adding the program to.
5. Optional: You can change the control program's Reference Name if needed.
6. Optional: You can select a different Icon.
7. Do one of the following:

If the control program is...	
In the Control Program drop-down list	Select the control program.
Not in the Control Program drop-down list	1. Click *Add New*. 2. Browse to select the control program. 3. Click *Open*. 4. Click *Continue*. 5. Click *Close*.

6. Optional: Check *Require operator* to record any changes to control program. See Recording Reasons for Edits (21 CFR Part 11) on page 127 .
7. Click *Accept*.
8. Download All Content (SeeDownloading to Controllers on page 13) to the controller.

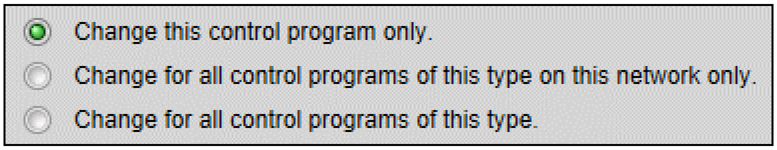
NOTE: You can click *Delete Unused* in the Control Programs section to delete all unattached control programs and any supporting files with the same name from the programs folder.

In the Add Control Program dialog box, you can also attach or remove a .view file that will be displayed in the Liebert® SiteScan™ interface for the control program.

If you need to change a control program's Object Instance number, right-click the control program in the navigation tree, and then select *Configure*. Click next to the field for additional information.

Replacing an Existing Control Program

1. Right click the control program on the Vertiv™ Liebert® SiteScan™ navigation tree, then select Configure.
2. The following steps are optional:
   - Change the *Display Name* for the control program.
   - Change the control program*Reference Name* if needed.
   - Select a different *Icon*.
3. If the system has other control programs of this type, select which control programs you want to change.



● Change this control program only.
○ Change for all control programs of this type on this network only.
○ Change for all control programs of this type.

NOTE: If you are changing the control program of the IP router, the second option will change all control programs of this type only on the IP network.

If you are changing a control program on the network below an IP router, the second option will not change control programs of this type in the router.

4. Do one of the following:

If the control program is...	
In the Control Program drop down list	Select the control program.
Not in the Control Program drop down list	1. Click *Add New*. 2. Browse to select the control program. 3. Click *Open*. 4. Click *Continue*. 5. Click *Close*.

6. Optional: Check *Require operator* to record any changes to control program. See Recording reasons for edits (21 CFR Part 11) (See Recording Reasons for Edits (21 CFR Part 11) on page 127).
7. Click *Accept*.
8. Download All Content (See Downloading to Controllers on page 13) to the controller.

NOTE: You can click *Delete Unused* in the Control Programs section to delete all unattached control programs and any supporting files with the same name from the programs folder.

In the Add Control Program dialog box, you can also attach or remove a .view file that will be displayed in the Liebert® SiteScan™ interface for the control program.

Editing a Control Program

On a Liebert® SiteScan™ client, you can get a copy of a control program from the server, edit it, then put it back on the server.

To Get the Control Program

1. Right click the equipment on the Vertiv™ Liebert® SiteScan™ Geographic or Network tree, then select Configure.
2. In the Control Programs section, click *Edit Existing*.
3. Click *Save as*.
4. Browse to the folder you want to put the file in.
5. Click *Save*.
6. Click *Close*.

To Put the Edited Control Program Back on the Server

1. Right click the equipment on the Liebert® SiteScan™ Geographic or Network tree, then select Configure.
2. In the Control Programs section, click *Add New*.
3. Browse to select the control program.
4. Click *Open*.
5. Click *Continue*.
6. Click *Close*.
7. Click *Close* again.

4.2.3 Working with Drivers in the Liebert® SiteScan™ Interface

A driver for the controller is defined in SiteBuilder when the system is engineered, but you can make the following changes in the Liebert® SiteScan™ interface.

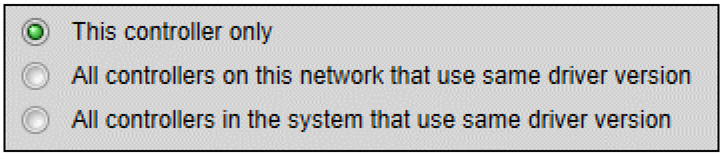
- Change the *driver settings*. See "Setting up the driver" in the Installation Guide of the controller.
- Change or upgrade a *driver*. See topic below.
- Reload a driver if it becomes corrupt (for example, a driver page is missing in the Liebert® SiteScan™ interface). On the Liebert® SiteScan™ Network tree, right click the controller or driver, then select Reload Driver. Reloading updates all instances of the driver throughout the system and marks the controller(s) for an All Content download. Changes you made on the driver pages in the Liebert® SiteScan™ interface remain in effect.

After you make these changes, you must download All Content (See Downloading to Controllers on page 13) to the affected controller(s).

NOTE: You can also make these changes in SiteBuilder. See Changing or Upgrading a Driver below in SiteBuilder Help.

Changing or Upgrading a Driver

1. On the Liebert® SiteScan™ Network tree, right click the controller, then select *Configure*.
2. If other controllers in the system use this driver, select which controllers you want to change.



● This controller only
○ All controllers on this network that use same driver version
○ All controllers in the system that use same driver version

3. Do one of the following:

If the driver is...	
In the Driver Version drop down list	1. Select the *driver*. 2. Click *Accept*.
Not in the Driver Version drop down list	1. Click *Add*. 2. Browse to select the driver. 3. Click *Open*. 4. Click *Continue*. 5. Click *Close*. 6. Click *Close* again.

7. Download All Content (Downloading to Controllers on page 13) to the controller.

NOTE: You can click *Delete Unused* in the Controller section to delete all unused drivers in SiteScanx.x\webroot\<system_name>\drivers.

4.2.4 BACnet Device Tools and Services

The tools and services described below let you control or troubleshoot BACnet devices. To access the tools and services, click on the BACnet device on the Liebert® SiteScan™ Network tree, then click *Properties*.

Tool	Description
Module Status	Generates a Modstat report. See Using a Modstat to Troubleshoot your System on page 161 .
Show Bindings	Displays all Device IDs that the BACnet device communicates with and the network address of each device. See Troubleshooting BACnet Bindings on page 160 .

BACnet Device Services

Although the following BACnet device services can be used for Vertiv controllers, you should not need to use them for this purpose. Their primary target is a third-party device that supports these services.

Service	Description
Time Sync UTC Time Sync	Sends the local time of the site to the BACnet device. Sends the Coordinated Universal Time (UTC) to the BACnet device. The device must be able to convert the time to its local time zone. **NOTE: Some devices support only one of the above time sync services.**
Backup, Restore, and Abort	Executes a BACnet Backup or BACnet Restore service as defined by the BACnet standards. A message appears when the backup or restore is complete. Click *Abort* to stop a Backup or Restore. **NOTE: These services are vendor specific and should be used with caution. A failed restore could make a device inoperable. Before using these on a device running in a live system, test them on the device during installation.**
BACnet Password	Applies to Backup, Restore, Warmstart, and Coldstart. Enter your BACnet password if required by the BACnet device. This password is typically defined in a third party tool.
Warmstart or Coldstart	Restarts the BACnet device. For a third party device, see the manufacturer documentation to determine the difference between these 2 services. For Vertiv controllers, these services are the same. These services will cycle the controller's outputs.

Service	Description	
DCC	Use to stop or start the BACnet device communication. Select one of the following options in the droplist, then click *DCC*.	
	Enable	Starts the device communication.
	Disable	Stops the device communication for the amount of time that you enter in the Timeout field. See NOTE: below .
	Disable Initiation	Stops the device from initiating communication for the amount of time that you enter in the Timeout field. See NOTE: below . The device will continue to respond to communications from other devices.
	NOTE: Type -1 in the Timeout field to disable communication indefinitely. Normal communication will resume only when the device receives an Enable command.	
Event Info	Displays detailed information about the objects that are currently in alarm.	
Event Summary	Displays summary information about the objects that are currently in alarm.	

4.3 Setting Up Vertiv™ Liebert® SiteScan™ Client Devices and Web Browsers

The Liebert® SiteScan™ system can be viewed on the following client devices and web browsers

Computers

The client computer should have at least:

- Quad core processor
- 4 GB RAM
- Communications link of 100 Mbps or higher

The Liebert® SiteScan™ application will work with slower computers and slower links, but the results may not be satisfactory.

A Computer with This Operating System	Supports These Web Browsers
Windows	Google Chrome v84.0 or later 1 Microsoft Edge v84 or later Mozilla Firefox v79.0 or later
Mac OS X (Apple Mac only)	Safari v11 or later 2 Google Chrome v84.0 or later Mozilla Firefox v79.0 or later
Linux	Google Chrome v84.0 or later Mozilla Firefox v79.0 or later

1. Best performance
2. Best performance unless browser is running on a Mac Mini or a MacBook:

WARNING! If machine is running Mountain Lion 10.8x with an integrated Intel HD 400 graphics card, it will experience display issues. Use one of these workarounds for better performance:

- If an additional NVIDIA graphics card is available, manually switch the graphic card setting in MAC OS X to use that card.

- If not, use GoogleTM ChromeTM v84.0 or later.

Mobile Devices

Device Type	Platform Support
Smart phone	AndroidTM, iOS
Tablet	AndroidTM, iOS, SurfaceTM

NOTE: Some functionality may be limited by the capability of the mobile device and operating system.

4.3.1 Setting Up and Using a Computer With the Vertiv™ Liebert® SiteScan™ System

- Set the monitor screen resolution to a minimum of 1920 x 1080 with 32-bit color quality
- You may want to disable the navigation sounds of the computer.

Mac Only

NOTE: The instructions below are for a Mac OS X 10.8. Other versions may vary slightly. See your computer Help menu, if necessary.

Computer Settings	To Change Setting
Enable right clicking to see right click menus:	
On a Mac	1. Select *System Preferences* > *Mouse*. 2. Click the drop down list that points to the mouse right click button, then select *Secondary Button*.
On a MacBook	1. Select *System Preferences* > *Trackpad*. 2. Enable *Secondary click*.

The instructions in Help are for a Windows computer. For instructions that include the *Ctrl* key, replace *Ctrl* with *Command*. For example, replace *Ctrl+click* with *Command+click*.

4.3.2 Setting Up and Using a Web Browser to View the Vertiv™ Liebert® SiteScan™ Interface

Setting up and Using the Microsoft Edge

The instructions below are for Microsoft Edge.

Web Browser Settings	To Set in Microsoft Edge
Do not block cookies	1. Click . . . to display the Actions droplist. 2. Select *Settings* > *Site Permissions* > *Cookies*.
Disable web browser popup blockers *	1. Click . . . to display the Actions droplist. 2. Then select *Settings* > *Site Permissions* > *Popups and redirects*.

To	Do the Following
Maximize the web browser window *	Use the minimize/maximize button in the top right corner of the browser window.
Have 2 different users logged in to the Liebert® SiteScan™ system on the same computer *	1. Click . . . to display the Actions droplist. 2. Select *New Window.*
Clear browser cache	1. Click . . . to display the Actions droplist. 2. Select *Settings > Privacy, Search, and Services > Clear browsing data.* 3. Click *Choose what to clear.* 4. Click *Clear now.*
* Does not apply to Microsoft Edge on a phone.	

Setting Up and Using Mozilla Firefox

NOTE: The instructions below are for Mozilla Firefox v60.0 on a Windows operating system. Other versions may vary slightly. See your web browser Help menu if necessary.

NOTE: If the menu bar is not visible, right click on the title bar of the window, and then select *Menu bar*.

NOTE: If a message appears in the Liebert® SiteScan™ interface that includes the checkbox *Prevent this page from creating additional dialogs*, Do not check this box.

Web Browser Settings	To Set in Firefox
Disable Popup blocker	1. Click *Tools > Options > Privacy & Security.* 2. Under *Permissions*, click *Exceptions* next to *Block popup windows.* 3. Type http:// (or https://) and then the server name or IP address of your system. 4. Click Allow and then Save Changes.
Enable JavaScript	1. In the address bar, type about:config, and then press *Enter.* 2. Click *I accept the risk.* 3. In the *Search* bar, type javascript.enabled. 4. If the value field shows *true*, JavaScript is enabled. If it shows *false*, right-click *javascript:enabled*, and then select *Toggle.*
Addons Manager	Select *Tools > Addons > Extensions.* On this page, you can enable/disable installed addons such as: • Adobe Acrobat Reader (to view PDF's) • QuickTime Plug-in (to play audible alarms) Only installed Firefox addons will show up in the list.

To	Do the Following
Maximize the web browser window	Press *F11* to turn full-screen mode on\off.
Clear browser cache	1. Click *Tools > Options > Privacy & Security.* 2. Under Cookies and Site Data, click Clear Data. 3. Click *Clear.*
Have 2 different users logged in to the Vertiv™Liebert® SiteScan™ system on the same computer	Start a new web browser session. Select File > *New Private Window.*

Setting Up and Using Google Chrome

NOTE: The instructions below are for Google Chrome v66.0. Other versions may vary slightly. See your web browser Help menu, if necessary.

NOTE: If a message appears in the Liebert® SiteScan™ interface that includes the checkbox Prevent this page from creating additional dialogs, Do not check this box.

On a Computer

Web browser settings	To Set in Chrome
Enable popups	1. Click on ⋮ the browser toolbar. 2. Select *Settings.* 3. Click *Advanced* at the bottom of the page. 4. Under *Privacy and security*, click *Content settings.* 5. Under *Pop-ups > Allow*, click *ADD*, and then type http:// (or https://) and then the server name or IP address of your system.

To	Do the Following
Clear browser cache	1. Click on ⋮ the browser toolbar. 2. Select *More tools > Clear browsing data.* 3. Select a time range in the drop-down list. 4. Check the types of information that you want to remove. 5. Click *Clear Data.*
Maximize the web browser window	Press *F11* on your keyboard to turn full-screen mode on/off.
Have 2 different users logged in to the Vertiv™ Liebert® SiteScan™system on the same computer	Start a new web browser session. Click ⋮, then select *New incognito window.*

On Chrome for Android

NOTE: The following settings are based on Android v11 - options may vary with versions.

Web Browser Settings	In the Chrome Menu
Turn off desktop mode	Uncheck *Request desktop site*
Disable popup blocker	*Settings > Advanced > Site Settings >* uncheck *Block popups*
Enable JavaScript	*Settings > Advanced > Site Settings >* check *Enable JavaScript*
Enable Cookies	*Settings > Advanced > Site Settings >* check *Accept Cookies*

To	In the Chrome Menu
Clear browser cache	*Settings > Basics > Privacy > CLEAR BROWSING DATA*

Setting Up and Using Safari

NOTE: The instructions below are for Safari v11. Other versions may vary slightly. See your web browser help if necessary.

NOTE: We recommend that you do not run Safari in full screen mode. If you do, Liebert® SiteScan™ popups will open full screen, covering the main application window.

On an Apple Computer (Mac)

Web Browser Settings	To Set in Safari
Disable popup blocker	*Preferences* > *Security* > uncheck *Block popup windows*
Enable JavaScript	*Preferences* > *Security* > check *Enable JavaScript*
Enable Plugins	*Preferences* > *Security* > check *Enable plug-ins*
Prevent popups from opening in a new browser tab	*Preferences* > *Tabs* > uncheck *Command-click opens a link in a new tab*
Prevent Safari from automatically opening zip files exported from the Liebert® SiteScan™ application	*Preferences* > *General* > uncheck *Open "safe" files after downloading*

To	Do the Following
Clear browser cache	*History* > *Clear History*
Have 2 different users logged in to the Liebert® SiteScan™ system on the same computer	Start a new web browser session. Select *Safari* > *Private Browsing* > *File* > *New window*

On an Apple iPad

Web Browser Settings	To Set on the iPad...
Disable popup blocker	*Settings*> *Safari* > set *Block popups* to *Off*
Enable JavaScript	*Settings* > *Safari* > set *JavaScript* to *On*

NOTE: Reenable popup blocking on your device when not using our software.

To	Do the Following
Clear browser cache	*Settings* > *Safari* > *Clear History*

NOTE: Enable popup blocking on your device again when not using our software.

On an Apple iOS 12.2

Web Browser Settings	To Set on the iPhone.
Enable JavaScript	*Settings* > *Safari* > *Advanced*

4.4 Setting Up a System In the Vertiv™ Liebert® SiteScan™ Interface

4.4.1 System Settings

The System Settings page contains information that you must enter before the Liebert® SiteScan™ application can run properly.

1. On the *System Configuration* tree, select *System Settings*.
2. Click each tab, then enter the necessary information. Tab details are described below

General Tab

The General tab presents the following system information:

- System Directory Name
- Path to the Webroot Directory
- Database Type
- System Language - The language to be used for:
  - The default language for new operators
  - Alarms logged to the database
  - State text and object names downloaded to the field
  - The login page

NOTE: Language also refers to formatting conventions. For example, English uses the date format mm/dd/yy, but English (International) uses the date format (dd/mm/yy).

You can edit or use the following fields and buttons.

Field	Notes
System Information	
System Statistics button	Click to see the following system information: • Number of controllers • Number of controllers that can run control programs • Number of points, regardless of vendor • Number of trend sources in database • Number of trend samples in database
Levels displayed in paths	The number of levels displayed inLiebert® SiteScan™ paths. For example, if Node Name Display Depth is set at: 2, a typical path might be ..\AHU-1\RA Temp 3, a typical path might be ..\Atlanta R&D\First Floor\AHU-1 **NOTE: Changing this field does not take effect until you restart the SiteScan Server application.**
Logs	
Select a week of logs to review	For troubleshooting, you can download a zip file that contains logs of system activity.
Time	
Time Sync	Click to immediately synchronize the time on all IP network controllers in the system database to the Vertiv™ Liebert® SiteScan™ server's time.

Field	Notes
	Time synchronization occurs daily if the Enable time synchronization of controllers daily at____ field on the Scheduled Tasks tab (See Scheduled Tasks Tab on page 203) is enabled. (Click this link for more information on time synchronization.)
Time Format	Select one of the following for the system time: • 12-hour clock (Example: 4:34 pm) • 24-hour clock (Example: 16:34)
Date Format	Select the format you want the system to use.
Alarms	
Use a single alarm template for CMnet alarms	If your system is an upgraded legacy system: • Check to have alarms for CMnet equipment use only the alert_auto alarm template. • Uncheck to allow multiple alarm templates.
Enable support for Alarm Notification Clients to connect to this server	Check to use the Alarm Notification Client application. See Alarm Popup (See Alarm Popup on page 39) alarm action. **NOTE: When using location-dependent security, users only receive alarms for locations they are allowed to access.**
Restrict to IP Address	If the server has more than one network interface adapter, type the IP address of the server network connection that the Alarm Notification Client application will connect to.
Port	Change this field if the Alarm Notification Client application will use a port other than 47806 on the server.
Current client connections	Shows any workstation whose Alarm Notification Client is actively connected to this server.
Schedules	
Disable Schedules	If your system has no need to run schedules, check this box so that the Schedules feature is no longer visible in Liebert® SiteScan™ interface.
Trends	
Keep historical trends for ___ days	Stores trend data in the Liebert® SiteScan™ database for the time you specify. This is a default setting that you can change when you set up trends for an individual point. Specify the time of day that the trends are deleted on the Scheduled Tasks tab.
Display gap in graph line for missing data	Check to show a gap if trend data is missing.
Enable Server Trending of Color	Leave this checked unless directed otherwise by Technical Support.
Poll Interval	The frequency that the server polls routers for color trend data. Increase this field only if Last Poll Duration exceeds the Poll Interval.
Source Files	
All Source Files	Use to export source files to a .zip file that can be imported into another Liebert® SiteScan™ system. Source files include: • Control programs (.equipment files only) • Drivers • BACview files • Report design files for Equipment Values or Trend Sample reports **NOTE: If import detects a difference between a database file and an import file with the same name, import does not overwrite the database file. A message lists any file differences so that you can resolve them.**
Email Server Configuration	The information in this section is used by the Send email alarm action (See Send E-mail on page 46) and used to email a Scheduled Report (See Scheduling Reports on page 105).

Field	Notes
From	Enter a valid address if required by your mailserver.
Mail Host	The mail server address. This can be an IP address or a system name, such as mail.mycompany.com.
Mail Host Port	Change this field if using a port other than the default port 25.
Mail Host Security Options	Select the type of security the mailserver uses. • Cleartext (SMTP) – Uses the SMTP protocol to send as clear text over TCP/IP • Secure SSL (SMTP with SSL) – Uses SSL, a communication protocol that provides data encryption • Secure TLS (STARTTLS) – Uses TLS, but does not begin encryption until the Vertiv™ Liebert® SiteScan™ application issues STARTTLS command
Specify Mail User for Mail Host Authentication	Select if your mail server requires a username and password.
Test connection	Click to have the Liebert® SiteScan™ application try to connect to the email server. A message will appear below this button stating if the connection was successful or if it failed.

Security Tab

Field	Notes
Logging	
Log audit data to file	Records operator activities and some system activities (such as opening and closing the database or automatic deletions) in a text file. The default file is auditlog.txt stored in *SiteScan\webroot\<system_name>*. You can change the file name and include a different path. To prevent the file from growing too large as new data is appended, you can archive the data to another text file by selecting an archive frequency in the Archive log file contents field. The archive file is auditlog_yyyy_mm_dd.txt, where yyyy_mm_dd is the creation date of the archive file. This file is created in the same location as auditlog.txt. **NOTE: If you do not archive the log file contents, you should manually delete the oldest entries.**
Log audit data to database	Records audit data in a database named audit.mdb that can be accessed by third party software. **NOTE: For Access, MSDE, and Derby, the database is automatically created. An Access database is named audit.mdb; a MSDE database is named audit.mdf. The Derby database consists of multiple files in a folder called audit. For MySQL, SQL Server, PostgreSQL, or Oracle, you must create the database manually.**
Delete database entries older than ____ days	Automatically deletes entries in the database that are older than the number of days you specify.
Log errors for invalid URLs	Enable this field to write to the core.txt log any time an external source sends a request to the Liebert® SiteScan™ Server application. **NOTE: Regular maintenance scans by external software can cause the log files to grow large.**
Security Policy	
Change Policy	See Location Dependent Operator Access on page 123) for information on Change Policy.
Remote Access	
Allow remote file management	Lets you access the system using WebDAV.
Operators	

Field	Notes
Return operators to previous locations when server reconnects	Returns operators to current tree locations when the server reconnects.
Log off operators after _:_ (HH:MM) of inactivity	The system automatically logs off an operator who has had no activity in the system for the time period specified. This is a default setting for the system. The System Administrator can change this setting for an individual operator on the Operators page.
Lock out operators for __ minutes after __ failed login attempts	Clear Lockouts removes lockouts for all users. **NOTE: Restarting the Vertiv™ Liebert® SiteScan™ Server application will remove lockouts.**
Use advanced password policy	You can place specific requirements on passwords to increase security. See Advanced Password Policy on page 123
Do not synchronize operator and privileges	If using hierarchical servers, the Liebert® SiteScan™ application automatically synchronizes the operator/privilege settings on the child servers with those on the parent server. You have the following options: • Enable this checkbox on all servers to stop the synchronization process. • Enable this checkbox on a child server to remove it from the synchronization process so that you can manage that server's settings locally.
Synchronize Now	Click this button on the parent server for immediate synchronization of operator/privilege settings.
Permissions	
Permissions	When control programs, views, and BACview files are created, the creator can remove any of the following permissions from them. • Permit Upload • Permit Download • Permit View Logic • Permit Edit A restriction applies to anyone who does not have the creator's Liebert® SiteScan™ license. However, the creator can produce a key for someone with a different license that will override the restrictions to let them perform any action that the key allows. The table in this Permissions section shows all keys in the SiteScan X.X\resources\keys folder. To activate a key, click *Add*, then browse to the key. To delete a key from your system, select the key in the table, then click *Delete*. Red text in the table indicates the key has a problem such as it does not apply or has expired. See the Notes column for an explanation.

Communications Tab

The fields on this tab let you define controller communication with the SiteScan Server application and BACnet network communication.

Field	Notes
SiteScan Server BACnet Controller Instance and BACnet Alarm Recipient Instance	The BACnet identifier for the system server and the alarm recipient. You enter these system properties in SiteBuilder.
Always upload properties from controllers to SiteScan database on mismatch	Automatic uploads are listed in the Audit Log. If you do not check this field, properties must be manually uploaded or downloaded by the operator when a mismatch occurs. **NOTE: If an automatic upload fails and the operator chooses to do nothing at that time, the upload will be attempted again when he returns to the page where he encountered the mismatch.**
Ignore incoming alarms from sources not in this database	The Vertiv™ Liebert® SiteScan™ application will ignore alarms from third party devices not in the database or devices from other Liebert® SiteScan™ systems on the same network.
BACnet Settings	Native Liebert® SiteScan™ system only
Log BACnet Binding Conflicts	The Liebert® SiteScan™ application uses BACnet (dynamic) binding for communication between devices unless your system uses NAT routing. If using NAT, the Liebert® SiteScan™ application uses information in its database to bind to BACnet devices. When checked, the Liebert® SiteScan™ application logs binding conflicts that result from duplicate network numbers or device IDs.

Scheduled Tasks Tab

Field	Notes
Automatically delete alarm incident groups which have been closed for more than ___ days	An incident group is all alarms related to a particular incident, such as Off Normal, Fault, and Return to Normal. **NOTE: Alarms in an incident group are not deleted until all alarms in the group have been closed.**
Archive alarm information upon alarm deletion	Writes alarm information to a text file.
Automatically delete expired schedules daily at ___	To ensure there are no time zone conflicts, the Liebert® SiteScan™ application waits 2 days after a schedule expires to delete it.

Field	Notes
Remove expired historical trends daily at ____	Deletes trend data that has been in the database longer than the time specified in the Keep historical trends for ___ days field on the General tab.
Enable time synchronization of controllers daily at____	Automatically synchronizes the time on all equipment to the time on the server, adjusting for different time zones and Daylight Saving Time. We recommend that you check this field. The Vertiv™ Liebert® SiteScan™ application will send a daily time sync message to each IP network device that is in the system database. IP devices not in the database will not be synchronized. For all ARC156 or MS/TP networks in the database, the Liebert® SiteScan™ application will send a broadcast time sync message. All devices on these networks will be synchronized, regardless of whether or not the devices are in the database. ⚠ **CAUTION: Make sure that your server time and time zone setting are correct. Make sure that each site's time zone setting in SiteBuilder is correct.** **To prevent time sync problems when the transition to and from Daylight Saving Time occurs, set the time sync to occur at least 1 hour after the last controller in the system is adjusted for DST. For example, your server and part of your system is in the Eastern Standard Time zone, but you also have controllers in the Pacific Time zone. Your server is adjusted for DST at 2:00 a.m. Eastern Standard Time, but the controllers in the Pacific Time zone are not adjusted until 3 hours later. So you would set the time sync to occur daily at 6:00 a.m. or later.** **NOTE: You can disable this function for an individual site on the site Properties page. See Setting Up Site Properties on page 206 .** **NOTE: You can perform system-wide time synchronizations using the Time Sync button on the General tab (See General Tab on page 199). Or, you can synchronize individual devices using the Time Sync button on the devices' Properties page (See BACnet Device Tools and Services on page 193).** **NOTE: Between time sync broadcasts, Vertiv routers include time sync information in each color request to the devices below the router. This ensures devices without a battery backed clock will get the time shortly after powering up.**
Check for expiring BACnet/SC certificates daily at ____	Triggers an alarm when a BACnet/SC Hub certificate will expire within the Warning or Critical thresholds. While in the Warning threshold, the alarm repeats once per week. In the Critical threshold, the alarm repeats daily and every operator will get a popup message when they log in.

Daylight Saving Tab

On this tab, you can adjust the Daylight Saving Time settings for SiteScan Server.

Click *Update* to automatically set the table's *Begin* and *End* dates for the next 10 years based on the system's timezone. This marks all controllers with ExecB drivers for a Parameters download.

If the Updated Dates are Incorrect

If you clicked *Update* but the dates are incorrect, your system's Java timezone data may be out of date. Do the following:

1. Go to the Oracle Java SE Download site (http://java.sun.com/javase/downloads).
2. Download the *JDK DST Timezone Update Tool* (*tzupdater-< version >.zip*) and unzip the file. The zip file contains 2 items:
    - tzdata.tar.gz
    - tzupdater.jar
3. In the Liebert® SiteScan™ interface, go to *System Settings > Daylight Saving*, then click *Import*
4. Browse to the tzupdater.jar file, select it, then click *Open*.
5. Click *Continue*. This restarts the SiteScan Server application.

6. After the restart, in the Liebert® SiteScan™ interface, go to *System Settings* > *Daylight Saving*, and then click *Import*.
7. Browse to the *tzdata.tar.gz* file, select it, and then click *Open*.
8. Click *Continue*. This restarts the SiteScan Server application.
9. On the *System Settings* > *Daylight Saving tab*, click *Update*.

NOTE: If you have sites in different time zones that use Daylight Saving Time, you can click *View DST Dates* on the site Properties page to see DST information and time change dates.

Addons Tab

A Vertiv™ Liebert® SiteScan™ system supports addons, such as EnergyReports, that retrieve and use the Liebert® SiteScan™ data.

By default, the Liebert® SiteScan™ application allows only signed addons that are supported by Vertiv. If needed, you can override this setting in SiteBuilder by going to *Configure* > *Preferences* > *Web Server*, and checking *Allow unsigned addons*.

To Install an Addon

1. Save the addons file (.addon or .war) to your computer.
2. On the *System Settings* > *Addons tab*, click *Browse*, and then open the file.
3. Click *Install*. After a few seconds, the addon will appear in the *Installed* table, and will be enabled. The table below gives a description of each column.

Column	Notes
Name	The addons name.
Path	To open the addon in a web browser, append this path to your Liebert® SiteScan™ system's address. For example, to open EnergyReports, type: http://<system_name>/EnergyReports, or http://<system_IP_address>/EnergyReports
Version	The version is shown if the author provided the information in the addon.
Status	If this column shows: • Running, you can open the addon in a web browser. • Disabled, click Enable to run the addon. • Startup error, select the table row to see an explanation of the error under Details.

4. Select an *addon* in the Installed table to disable or enable it, or to see the following Details.

Addon main page	Click the main page link to open the addon, if the author provided a main page.
Description	A description of the addon, if the author provided one
Vendor Name	The addon author
Public Data Directory	This public directory contains data generated by the addon. This data is visible in a web browser.
Private Data Directory	This private directory contains information such as configuration data.

To back up the Addons Private and Public Data Directories

NOTE: This procedure will not back up data stored in an external database. For example, EnergyReports uses an external database.

1. Select the *addon* in the table.
2. Click *Save Data*.

3. Click *OK*.
4. Click *Save*.
5. Select the location where you want to save the data, then click *Save*.

To Update an Addon

NOTE: Add-ons for Vertiv™ Liebert® SiteScan™ v6.0 or later systems have a different folder structure than previous versions.

1. Select the *addon* in the table
2. Click *Remove Addon and Data*.
3. Follow the procedure above to install the new version of the addon.

To Uninstall an addon

1. Select the *addon* in the table.
2. Click *Remove Addon* and Data

4.4.2 Setting Up Site Properties

1. On the *Network* tree, select the site.
2. Click *Properties*.
3. Configure site properties.

Field	Notes
Enable Timesync	Daily synchronizes the time in the site controllers with the server time, adjusting for different time zones and Daylight Saving Time. Synchronization occurs each day at the time specified in the field *Enable time synchronization of controllers daily at* on the System Settings > Scheduled Tasks (See Scheduled Tasks Tab on page 203) tab. ⚠ **CAUTION: Make sure that your server time and time zone setting are correct. Also, make sure that the site time zone setting is correct in SiteBuilder.**
View DST Dates	If the site time zone (set in SiteBuilder) uses Daylight Saving Time, you can click *View DST Dates* to see DST information and time change dates.
Group Cache Controller	The designated router where colors are cached when peer caching is enabled in SiteBuilder.

4.4.3 Registering Your Liebert® SiteScan™ Software

To register your software, you must obtain a registered license from Vertiv and then apply it in the Liebert® SiteScan™ interface. You can apply it when you install the software or at a later time.

1. Contact your local Vertiv Sales representative to obtain a new license.
2. Apply your license:
   - During the Vertiv™ Liebert® SiteScan™ installation—The installation requests the location of your license file. Browse to location where you saved it in step 4 above.
   - After the installation
     - On the Liebert® SiteScan™ System Configuration tree, select License Administration.

- Browse to the license file.
- Click *Apply*.
- Restart the *SiteScan Server application*.

NOTE: Do not edit any part of this registered license file. Editing a license file invalidates the license. Store the license in a safe location.

4.4.4 Adding Links or Text to the Liebert® SiteScan™ Login Page

You can add links or text, such as a disclaimer, to the login page.

Adding Links to the Login Page

1. In a text editor such as Notepad, type 2 lines for each link that you want on the login page.
   Line 1: link#.text=<the link text that is to appear on the login page
   Line 2: link#.url=<the link's address>

NOTE: link#.text and link#.url must be lowercase.

2. Save the *file* with the following name and location.
   File name: extra_login_links.properties
   Location: SiteScanx.x\webroot\<system_name>

Adding Text to the Login Page

1. In a text editor such as Notepad, type the text that you want on the login page.
2. Save the *file* with the following name and location.
   File name: legal_disclaimer.txt
   Location: SiteScanx.x\webroot\<system_name>

4.5 Editing a System Remotely

4.5.1 Editing Geographic or Network Tree

In the Liebert® SiteScan™ interface, you can edit the Geographic 🌐 or Network 🖧 tree that was originally set up in SiteBuilder. The system database is updated immediately.

Right click an item on the Geographic 🌐 tree, then select Set up Tree. Click Geographic 🌐 or Network 🖧 to display the tree you want to edit.

Click this button...	Or use this shortcut...	To...
+▦		Add an area as a child of the selected area. (Geographic tree only)
+📋		Import a clipping that was saved in SiteBuilder. See Steps to Import a Clipping on the next page .
✂	Ctrl+X	Cut a selected item so it can be pasted in another location in the tree. (Geographic tree only)

Click this button...	Or use this shortcut...	To...
📋	Ctrl+V	Paste an item that was previously cut from another location in the tree. The item will be pasted as a child to the selected item. (Geographic tree only)
⇧	Up arrow, or Drag and drop in new location	Move the selected item up the tree to a new location. (Geographic tree only)
⇩	Down arrow, or Drag and drop in new location	Move the selected item down the tree to a new location. (Geographic tree only)
▭		Rename the selected item.
✗	Delete	Delete the selected item. The item and all of its children will be deleted.
📝	Double-click the tree item	Edit the item's features such as: • names • view • control program—See Working with Control Programs in the Vertiv™ Liebert® SiteScan™ Interface on page 190

⚠ **CAUTION: Make a backup of your system before making changes. Make changes carefully as they cannot be undone.**

NOTE: You can also right-click items in the Set up Tree dialog box to perform the above tasks.

You can perform some of the above actions on multiple tree items simultaneously. Use Ctrl+click, Shift+click, or both to select multiple items.

Steps to Import a Clipping

You can export a clipping (a portion of a system) in SiteBuilder and then import it in the Vertiv™ Liebert® SiteScan™interface. The following items are imported:

- One or more selected Geographic and Network tree items including attached control programs, graphics, and drivers.
- Reports
- Trend data (if included in the clipping)
- Alarm templates and categories
- Location-dependent security information
- Schedules and schedule group membership (including the entire schedule group and schedules, if it does not exist in the target system)
- Alarm actions
- Alarm message prefixes and suffixes
- Source tree relationships (including source tree rules if the source tree does not exist in the target system)

To Import a Clipping:

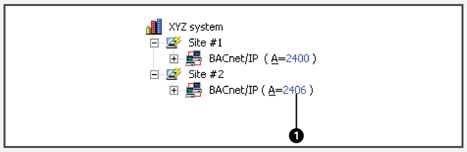
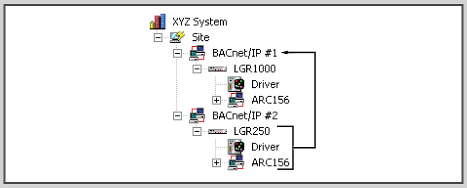
1. Right click *an item* on the Geographic 🌐 tree, then select Set up Tree.

2. Click the *Import clipping button* .
3. Browse to and select the *clipping* you want to import, then click *Next*.
4. Optional: If necessary, you can change the location path where the clipping will be imported. Select the *system fragment*, then select the *import location* in the tree below.
5. Click *Next*.
6. If asked if you want to replace event templates, follow the *on-screen instructions*.
7. If asked if you want to overwrite components, follow the *on-screen instructions*.
8. The interface shows any conflicts and problems that were found during the import. Make any needed corrections in SiteBuilder.

NOTE: Click Copy to Clipboard and then paste the list into another program such as Notepad for viewing or printing.

9. Click *Next*.
10. Click *Finish*.
11. Do any of the following that apply.

Table 4.7

If you imported...	Do the following in the SiteBuilder application...	Do the following in the Liebert® SiteScan™ application...
Another site into the system	Change the new site's BACnet/IP network number to be the same as the other BACnet/IP network(s).  XYZ system Site #1 BACnet/IP (A=2400) Site #2 BACnet/IP (A=2406) 1 1. Changing this address to 2400	Download All Content to all Vertiv IP routers in the system.
A second BACnet/IP network into a site	Move the items under the new network to the original BACnet/IP network, then delete the new network.  XYZ System Site BACnet/IP #1 LGR1000 Driver ARC156 BACnet/IP #2 LGR250 Driver ARC156	Download Parameters to any controllers that you moved.
Any controllers that use the SiteBuilder option Automatically Configure My BBMDs	N/A	Download BBMDs to the routers.
Any controllers that use manually configured BBMD tables	N/A	Update the routers' BBMD tables. See Setting up BACnet Broadcast Management Devices (BBMDs) on page 154 and Setting up BBMDs through the Vertiv™ Liebert® SiteScan™ Interface on page 155 orSetting up BBMDs using the BBMD Configuration Tool on page 156 .
A clipping without trends into a system using NAT	N/A	Restart IP connection(s) to new devices.

4.5.2 Managing Files on a Remote Vertiv™ Liebert® SiteScan™ server

The Liebert® SiteScan™ application supports WebDAV, a network protocol designed for managing remote server files through an Internet connection. Use a third-party WebDAV client application, such as WebDrive, to access the Internet from anywhere in the world and manage your system files residing on a distant Liebert® SiteScan™ server.

4.6 Options for Running the Liebert® SiteScan™ System

4.6.1 Running Liebert® SiteScan™ Server without Connecting to Controllers

To verify links between graphics and to set up properties, schedules, alarms, and trends before you connect to the network, run SiteScan Design Server instead of SiteScan Server. Then view the Liebert® SiteScan™ interface in a web browser.

NOTE: Question marks or purple thermographic color indicates correct microblock paths. Missing data or dark yellow thermographic color indicates errors.

4.6.2 Switching Liebert® SiteScan™ Server to a different system

Design engineers working on multiple projects can switch systems in the SiteScan Server application.

1. In the SiteScan Server application, select *Server*.
1. Change the *Active System*.
2. Select a *different system* (it must be in the webroot folder) and mode.
3. Click *Select*.

4.6.3 Running SiteScan Server as a Windows Service

For Windows 8.1, 10, 2012R2, 2016, 2019, and 2020

Run SiteScan Server as a Windows service if you want SiteScan Server to automatically start up when the server computer is restarted.

NOTE: If your Liebert® SiteScan™ system uses a database other than Derby and the database is located on the same computer as SiteScan Server, you must set up Windows to delay starting SiteScan Server until the database service has started. See "How to delay loading of specific services" (http://support.microsoft.com/kb/193888) on the Microsoft website.

Installing Liebert® SiteScan™ Server Service

NOTE: If you are not sure if the service was previously installed, see Determining the Installation Status of SiteScan Server Service on page 212 .

1. In the Windows Start menu, select *All Programs* and then *Accessories*.
2. Right click on the *Command Prompt*, then select *Run as administrator*.
3. Select *Yes* in the User Account Control message.
4. In the Command Prompt window, type: *cd* and the *path* to the SiteScan install directory.

   For example, type: cd c:\SiteScan_Web_x.x replacing x.x with your current version number.
5. Press *Enter*.
6. Type: *SiteScan Service.exe*.
7. Press *Enter*.

Installing Vertiv™ Liebert® SiteScan™ Server as a Windows service

To start Liebert® SiteScan™ Server as a Windows service.

1. In the Windows Start menu, select *Control Panel*.
2. Select *Administrative Tools*, then double click *Services*.
3. In the Services (Local) list, double click *SiteScan Service X.X*.
4. In the Startup type drop down list, select *Automatic*.
5. On the Log On tab, do one of the following:
    - Use the defaulted Local System account.
    - Select This account, then browse to select a user who is a member of the Administrator Group on that computer.
6. Optional: If you selected Local System account in step 5 and you want to be able to access SiteScan Server on the server computer's desktop, check Allow service to interact with desktop.

NOTE: If you do not check this field, the computer screen will give no indication that SiteScan Server is running; you must view the computer's Services page to see if it is running.

This check box applies only to a user logged in on the server. A Windows Remote Desktop user cannot access SiteScan Server running as a service.

If you check this field, you cannot use the instructions below to set up printing to a network printer. Ask your Network Administrator to set up Local System account to use a network printer.

If you check this field and the Liebert® SiteScan™ application is to run email alarm actions, ask your Network Administrator to set up Local System account to send emails.

7. On the General tab, click *Start*.
8. Click *OK*.

NOTE: If SiteScan Server does not start after you click Start, you may have a Windows permissions problem. Follow the procedure below in Setting up the Service for Network Printing below to set up the Windows user name and password.

Setting up the Service for Network Printing

If SiteScan Server runs as a service on a computer that is using a network printer, you must set up the Windows user name and password for the service. The Print alarm action requires this setup to be able to print.

1. In the Windows Start menu, select Control Panel.
2. Select *Administrative Tools > Services*.
3. Double click *SiteScan Service x.x*.
4. On the Log On tab, select *This account*.
5. Browse to the computer's domain, then select the *user* that the service will log in as.

NOTE: Contact your network administrator, if you need help determining the domain.

6. Type the user password in the Password and Confirm password fields.

Stopping or Uninstalling SiteScan Server Service

To stop or uninstall the SiteScan Server service

1. In the Windows Start menu, select *Control Panel*.
2. Select *Administrative* Tools, then double click *Services*.
3. In the Services (Local) list, double click *SiteScan Service X.X* (where X.X. is the SiteScan version number.
4. In the SiteScan Service X.X. properties dialog box, click *Stop* on the General tab.
5. Click *OK*.

To uninstall the SiteScan Server service

1. In the Windows Start menu, right click on the *Command Prompt*, then select *Run as administrator*.
2. Select *Yes* in the User Account Control message.
3. In the Command Prompt window, type: cd <path to the SiteScan install directory>

   For example, type: cd c:\SiteScan_Web_x.x
4. Press *Enter*.
5. Type: *SiteScan Service.exe* -remove
6. Press *Enter*.

Determining the Installation Status of SiteScan Server Service

If you do not know if the service was previously installed, follow the appropriate steps below.

1. In the Windows Start menu, right click *Command Prompt*, then select *Run as administrator.*
2. Select *Yes* in the User Account Control message.
3. In the Command Prompt window, type: cd <path to the SiteScan install directory>

   For example, type: *cd c:\SiteScanx.x*
4. Press *Enter*.
5. Type: *SiteScan Service.exe* -check
6. Press *Enter*.

4.6.4 Running SiteScan Server as a Linux Service

Setting up as a Service on Ubuntu or RedHat

To set up as a service on Ubuntu or RedHat:

1. On the terminal screen, type: *cd /opt/SiteScanx.x*
2. Click *Enter*.
3. On the terminal screen, type: *sudo ./SiteScan\ Service* add
4. Click *Enter*.
5. Reboot the computer for the application to run as a service.

Removing as a Service on Ubuntu or RedHat

To remove as a service on Ubuntu or RedHat:

1. On the terminal screen, type: *cd /opt/SiteScanx.x)*
2. Click *Enter*.
3. On the terminal screen, type: s*udo ./SiteScan\ Service remove*

4. Click *Enter*.
5. Reboot the computer.

4.7 Setting up a System for Non English Languages

English is the Vertiv™ Liebert® SiteScan™default language, but you can set up your system to display a different language. You can also set up multiple languages so different operators can view the system in different languages.

Follow the procedures below to display the Liebert® SiteScan™ interface in non-English languages.

1. Install a language pack (See Installing a Language Pack below).
2. Prepare your workstation for non-English text (See Preparing the Workstation for Non English Text below).
3. Create control programs and translation files (See Creating Control Programs and Translation Files for a Non English System on the next page).
4. Create graphics (See Creating Graphics for a Non English System on page 216).
5. Create your system in SiteBuilder (See Creating your System on page 218).
6. Set an operator’s language in the Liebert® SiteScan™ interface (See Setting an Operator’s Language in the Liebert® SiteScan™ Interface on page 219).

4.7.1 Installing a Language Pack

A language pack translates the text in the Liebert® SiteScan™ interface. A Liebert® SiteScan™ system is installed with an English language pack. To download other language packs:

1. Go to http://accounts.oemctrl.com/download.
2. Under Software Installs and Updates, select v# Language Packs, where # is your Liebert® SiteScan™ version.
3. Select the required language.
4. Follow the instructions given under To install this language pack.

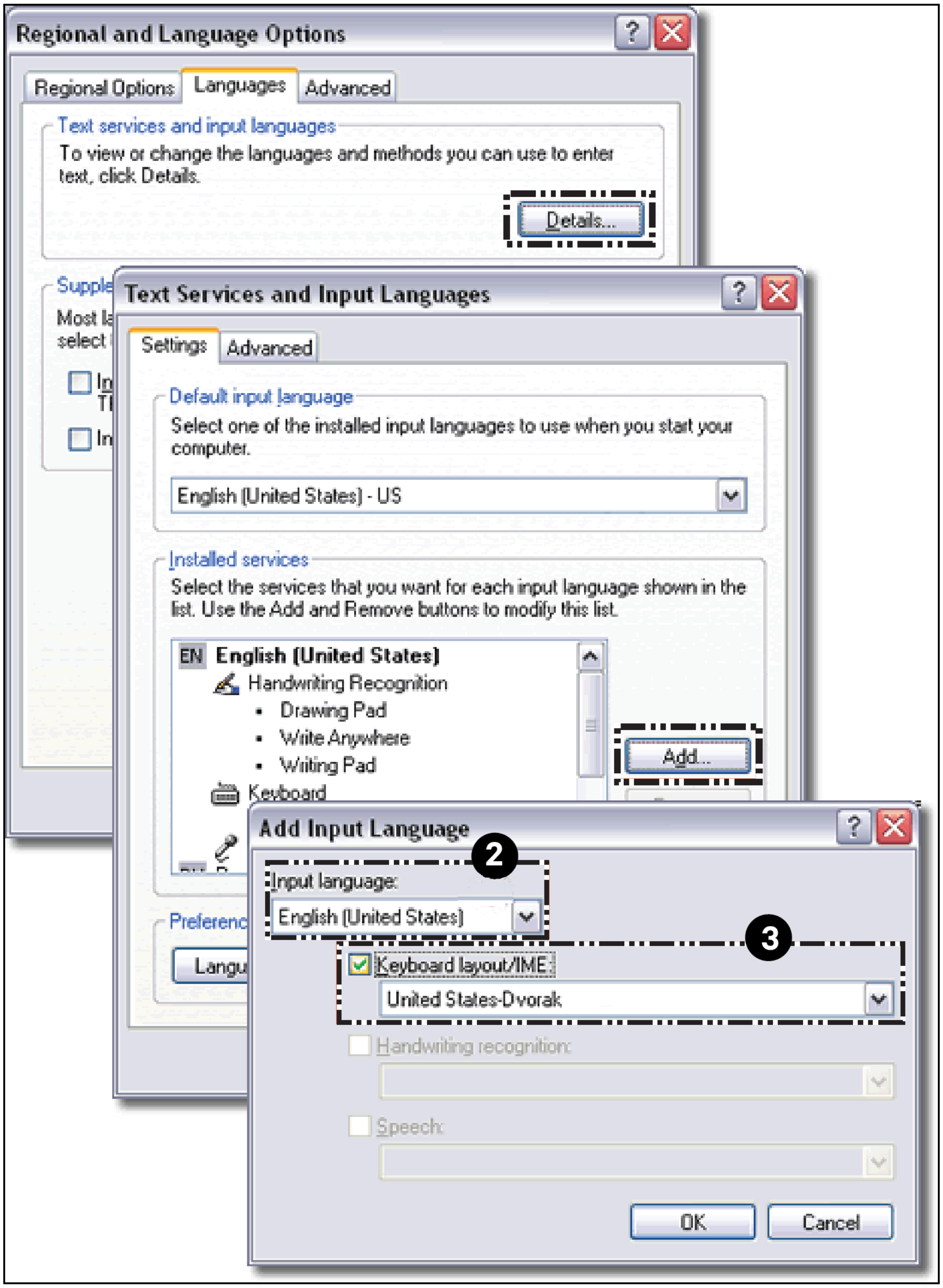
NOTE: If you create a system by copying an existing system that uses language packs, install the same language packs on the new system.

4.7.2 Preparing the Workstation for Non English Text

NOTE: The instructions below are for a Windows XP operating system. If you have a different operating system, see your system's Help for instructions.

Set up your workstation so you can type international characters in control programs, graphics, or SiteBuilder.

1. Install the appropriate fonts for the languages you will be using. In the Windows Control Panel, open Fonts, select *File* and then Install new fonts.
2. In the Control Panel, open *Regional and Language Options*, then select the *Input language*.
3. Install an Input Method Editor (IME) for non-alphanumeric characters.



To view or change the languages and methods you can use to enter text, click Details.

Select one of the installed input languages to use when you start your computer.

English (United States) - US

Select the services that you want for each input language shown in the list. Use the Add and Remove buttons to modify this list.

Input language: English (United States)

☑ Keyboard layout/IME: United States-Dvorak

See your operating system's Help for more information.

4.7.3 Creating Control Programs and Translation Files for a Non English System

To have the Vertiv™ Liebert® SiteScan™ interface display a control program's user defined text (such as microblock names and property text) in a non-English language, you must:

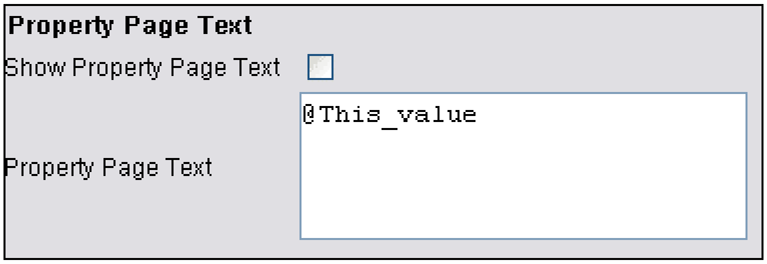
1. Create the control program using key terms instead of the text.
2. Create translation files of key terms and their language-specific equivalents.

In the Vertiv™ Liebert® SiteScan™interface, the key term is replaced with its equivalent in the translation file for the current operator language. If a Liebert® SiteScan™ Properties page or Logic page shows ??key term??, the key term is missing from the translation file.

NOTE: To edit existing control programs or translation files, see Editing Translation Files or Control Programs for a Non English System on page 219 .

Entering a Key Term in the EIKON Application

In the EIKON Property Editor, type @ before each key term.



Property Page Text

Show Property Page Text □

Property Page Text

```
@This_value
```

NOTE: Type only the key term in the EIKON application. Expressions such as $present_value$ are put in the translation file as part of the translated text. See EXAMPLES in "Translation files" below.

Key terms can contain only alphanumeric characters and underscores (no spaces) and cannot start with a number.

Translation Files

Translation files are used to translate key terms in control programs. A translation file contains key terms and their language-specific equivalents.

For a non-English system, you must create an English translation file and a non-English translation file* for each of the following:

- Each control program
- Key terms used in multiple control programs

Examples

Translation files	Key term=Language-specific equivalent
English	This_value=This value is $present_value$ Zone_temp=Zone temperature
Spanish	This_value=Este valor es $present_value$ Zone_temp=Temperatura de zona
*If the Liebert® SiteScan™ interface will display multiple non-English languages, create a translation file for each language.	

Creating and Implementing a Translation File

To create and implement a translation file

Create your translation file in a text editor, such as Microsoft Word, that supports the character encoding you need.

1. Type one key term and language equivalent per line, left justified, starting in column 1. Do not put spaces on either side of the equal sign.
2. Save the *file* using the appropriate file name and location in the Table 4.8 on the next page .

Table 4.8

If key terms are used in...	the file name is...	File location
A single control program	<any_name>_xx.native*	Any location
Multiple control programs	equipment_xx.native*	SiteScan_Web_\webroot\ <system_name>\resources
* xx = the language extension code. See "Extension codes and encoding" below.		

If you are using:

- The English character set, save the file as Text only.
- A non-English character set, save the file as Encoded text . (See your application’s help for information on saving files as encoded text.) When prompted for the language and encoding, seeExtension Codes and Encoding below .

3. Open the control program in the EIKON application, then select *Control Program > Bundled Resources*.
4. Click ⊞ , locate and select the *translation file(s)* for this control program, then click *Open*.

NOTE: Do not add equipment_xx.native files that you created for multiple control programs.

You can use Ctrl+click or Shift+click to select multiple files.

5. Save the control program. The translation files are embedded in the control program; the original files are no longer necessary.

Extension Codes and Encoding

Language	Extension Codes	Encoding*
Brazillian Portuguese	pt_BR	ISO-8859-1
English	en	ISO-8859-1
Canadian French	fr	ISO-8859-1
French	fr_FR	ISO-8859-1
German	de	ISO-8859-1
Italian	it	ISO-8859-1
Japanese	ja	EUC-JP
Korean	ko	EUC-KR
Russian	ru	KOI8_R
Spanish	es	ISO-8859-1
Swedish	sv	ISO-8859-1
Simplified Chinese	zh	GB2312
Traditional Chinese	zh_TW	Big5
Thai	th	TIS620
Vietnamese	vi	Cp1258
* Encoding is used when you create the translation file.		

4.7.4 Creating Graphics for a Non English System

To create a non-English graphic in ViewBuilder:

1. Set the *language font* (See Setting the Language Font below).
2. Create the *graphic*. (See Creating Graphics for a Non English System on the previous page)
3. Save the *.view file*.

NOTE: The names of your .view file and any inserted image files must contain only ASCII characters.

Setting the Language Font

If your system has language packs installed, you can select a font for each language. Your selection affects only how text in your graphic appears in ViewBuilder.

To set the font for each language

Select *Configure > Preferences > Graphic (.view)*.

On the Language tab, check the language that you want to be the default for all new graphics.

To select the Default language font for all new graphics

In the Preview Font column, click the font name to select a different font.

To select the Active Language when Creating a View

If you will use multiple language fonts in a single view, you can switch to a different language font as follows:

Select *Configure > View Properties*.

In the Language field, select the language you want to use.

Click *OK*.

Creating a Non English Graphic

The method you use to create a graphic that will be displayed in a non-English Vertiv™ Liebert® SiteScan™ system depends on the following:

- If the Liebert® SiteScan™ system will display only a single non-English language, create the graphic in that language.
- If the Liebert® SiteScan™ system will display multiple non-English languages, use either of the following methods:
  - Create the graphic in layers (one layer for each language), and then assign a show/hide conditional expression (see format below) to each layer so that it displays in Liebert® SiteScan™ based on the operator language. See "To show/hide a layer in the Liebert® SiteScan™ interface" in ViewBuilder Help.
  - Create each piece of the graphic in the different languages, and then assign a show/hide conditional expression (see format below) to each piece so that it displays in Liebert® SiteScan™ based on the operator language. See "Setting objects on a graphic to show/hide in the Liebert® SiteScan™ interface" in ViewBuilder Help.

Show/Hide Conditional Expression Format

$$operator_language$$='language'
where language is the language code from the list below.

For example, the conditional expression to display French would be:
$$operator_language$$=='fr_FR'

Language	Language code
Brazillian Portuguese English Canadian French French German Italian Japanese Korean Russian Spanish Swedish Simplified Chinese Traditional Chinese Thai Vietnamese	pt_BR en fr fr_FR de it ja ko ru es sv zh zh_TW th vi

4.7.5 Creating a Non English System in SiteBuilder

Choosing the Languages for your System

1. In SiteBuilder, select *Configure* > *Preferences*.
2. Select the *Language* tab.
3. Under Supported Languages, select each language that you want to be available in your system.

NOTE: This list shows all installed language packs. To install additional languages, see Installing a Language Pack on page 213 .

4. In the *System* field, select the system Language (See System Language on the facing page).
5. Click *OK*.
6. Save your database.

Creating your System

To create your system in each language that the system will display:

1. In SiteBuilder, select *Configure* > *Preferences*.
2. Optional: The *Font* tab shows the font that will be displayed in SiteBuilder for each language that you selected on the Language tab. To change a font, click on the name in the Preview Font column, then make a new selection.
3. On the Language tab, select a language in the Current Session field.
4. Click *OK*.
5. Create your *system*.
6. Save your *database*.
7. If your system will display multiple languages:

a. Select *Configure* > *Preferences*, select the *Language tab*, and select another language in the Current Session field.

b. Re-enter all node names and display names in the current language.

c. Save your database.

d. Repeat steps a. through c. for each additional language the system will display.

System Language

The system language is used for:

- The default language for new operators
- Alarms sent to the database
- State text and object names downloaded to the field
- The default login page *

All other information is displayed in the operator's language, which may be different than the system language. See Setting an Operator's Language in the Liebert® SiteScan™ Interface below .

NOTE: You can change the language shown on the Vertiv™ Liebert® SiteScan™ login page by selecting a different language from the list below the Password field (*).

4.7.6 Setting an Operator's Language in the Liebert® SiteScan™ Interface

An operator can change their language preference in the Liebert® SiteScan™ interface.

1. On the System Configuration tree⚙, select *My Settings*.
2. Under *Preferences*, select the *Language* in the drop down list.
3. Click *Accept*.

4.7.7 Editing Translation Files or Control Programs for a Non English System

If you add or edit a key term in a control program, be sure to make the same change in the translation file. SeeCreating Control Programs and Translation Files for a Non English System on page 214 .

If you make changes after attaching a control program in SiteBuilder, do one of the following:

- If you changed text only in a control program or its translation file, right click the control program on the Geographic tree, then select *Rebuild Equipment Pages*.
- If you changed logic in the control program, right click the control program on the Geographic tree, then select *Reload Control Program*.

Editing a Bundled Resource

The EIKON application bundles (embeds) the translation file(s) for a control program into the .equipment file. See steps 3 through 5 . To edit a bundled translation file:

1. Open the control program in the EIKON application.
2. Select *Control Program* > *Bundled Resources*.
3. Select the file, then click 💾 to save it to your hard drive.
4. Edit the translation file.

5. In the *Bundled Resources* dialog box in the EIKON application, click ⊞ and select the edited file.
6. Click *OK* to overwrite the existing file.

Editing an EIKON for SiteScan Control Program in the EIKON Application

To edit a non English control program that you created in the EIKON for SiteScan application:

1. Open the .eiw or .equipment file in the EIKON application, then make your edits.
2. Select *Control Program > Bundled Resources*.
3. Verify that the list shows all translation files specifically for the control program. Use the plus or minus button to add or delete translation files.

NOTE: This list shows the translation files in the *SiteScan\webroot\<system_name>\programs* folder. This list should not include translation files for multiple control programs.

4. Click *OK*.
5. Save the control program. The translation files are bundled with the control program; the original files are no longer necessary.

NOTE: If you need to change a translation file after you save the control program, see Editing a Bundled Resource on the previous page .

Copying Translation Files to Another System

To copy most translation files from one system to another, you copy the files in the source system and paste them into the same folders in the destination system.

However, if your source system and destination system have translation files with the same name, copying and pasting would overwrite the files in the destination system. In this case:

1. Open the source system's translation file in a text editor, then copy the key terms and translations.
2. Open the destination system's translation file in a text editor, then paste into it the key terms that you copied. Remove any duplicate key terms.

5 Integrating a Vertiv™ Liebert® SiteScan™ System with Other Systems

5.1 Integrating Liebert® SiteScan™ Data into Other Applications

The Liebert® SiteScan™ product has an application programming interface (API) that allows a programmer to write an application that can retrieve Liebert® SiteScan™ data, communicate with controllers, and in some case, contribute features to the Liebert® SiteScan™ application. In addition, Liebert® SiteScan™ supports data transfer using web services. If you need a new feature, report, or data from your system, you may be able to contract someone to develop an addon or custom report to meet your need. Contact your local field office for more information.

5.2 Integrating Third Party Data into a Liebert® SiteScan™ System

You can integrate third party devices into a Liebert® SiteScan™ system if the following are true:

- The third party devices are physically connected on the Liebert® SiteScan™ system’s network.
- You have an Vertiv controller that supports third party integration.
- You have the correct Vertiv driver for the third party protocol.
- You have enabled a port for a third party protocol on the Vertiv controller driver page.

To read from or write to a third party device, you need the following information from the third party vendor:

- Protocol
- Network address of the third party device
- Memory location of the object in the device you want to read from or write to

If you are integrating with BACnet devices, you can use the Liebert® SiteScan™ BACnet Discovery (See Discovering BACnet Networks, Devices, and Objects on the next page) feature to gather this information.

Before you begin a third party integration, study the Installation Guide of Vertiv controller and the third party protocol Integration Guide.

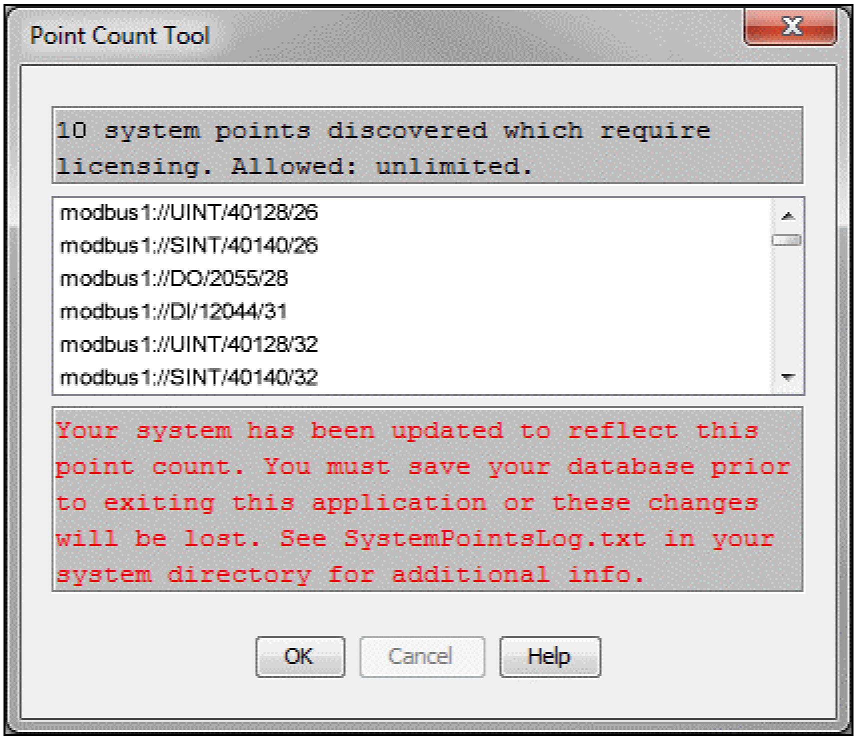
NOTE: While BACnet third party points are not restricted by hardware, we recommend that you do not exceed 2000 third party integration points in a router applications. You also should consider baud rate, number of nodes, number of network points, and trending frequency as these factors generally lower this recommendation.

The point allowance of a controller that provides third party points applies to only itself. You cannot apply a controller unused points to a different controller.

5.2.1 Determining the Number of Non BACnet Third Party Points Used in a System

In SiteBuilder, right-click the system level on the Geographic tree, then select Run *Global Point Count*.

NOTE: Select *Run Local Point Count* below the system level to count third-party points at and below the selected item. SiteBuilder displays the addresses that require licensing, but does not show the location of the point.



```
10 system points discovered which require
licensing. Allowed: unlimited.
```

```
modbus1://UINT/40128/26
modbus1://SINT/40140/26
modbus1://DO/2055/28
modbus1://DI/12044/31
modbus1://UINT/40128/32
modbus1://SINT/40140/32
```

```
Your system has been updated to reflect this
point count. You must save your database prior
to exiting this application or these changes
will be lost. See SystemPointsLog.txt in your
system directory for additional info.
```

5.2.2 Determining the Number of Third Party Points Used in a Controller

In the SiteBuilder Application

Right click the controller on the Network tree, then select Run Point Count.

In the Liebert® SiteScan™ application

1. On the Network tree, click to the left of the controller.
2. Click on *Driver*, then scroll to the bottom of the page.

Number of integration points requested and Number of integration points active show how many non BACnet third party Network I/O microblocks the controller is using. These two counts will differ if you exceed the integration point limits of the product. For example, if your controller provides 25 points and its control program includes 27 Modbus points, your Integration points requested will be 27 and your Integration points active will be 25.

5.2.3 Discovering BACnet Networks, Devices, and Objects

The Vertiv™ Liebert® SiteScan™ BACnet Discovery feature locates all accessible BACnet networks, BACnet devices, and BACnet objects (including devices in your Liebert® SiteScan™ system) on a BACnet network. The information gathered in this process is typically used to integrate third party BACnet devices and their BACnet objects into the Liebert® SiteScan™ system.

To use BACnet Discovery:

1. On the Liebert® SiteScan™ System Configuration tree, select *Connections*.
2. On the Configure ⚙ tab, disconnect the *BACnet/IP connection*.

3. While the connection is stopped, enter or verify the IP Address of the server and Subnet Mask for the BACnet/IP connection.
4. Restart the *connection*.
5. On the Network tree, select the system level.
6. Click *Devices*.
7. On the Advanced tab, click *Start* to discover BACnet sites for the system. An item called Discovered Networks appears in the tree.
8. To discover BACnet networks, select Discovered Networks, then click Go. A list of all BACnet networks appears on the Network tree. After all networks are found, close the status dialog box.

NOTE: Run a commstat manual command to determine which device routes to each network. The BACnet Bind Show Network section of the Commstat window shows the IP address of the router to each network.

9. To discover BACnet devices on a network, select a network on the Network tree, then click *Go*. After all devices are found, close the status dialog box. Click the plus sign beside an item to expand the list of devices.
10. To discover BACnet objects on a device, select the device on the Network tree, then click *Go*. After all objects are found, close the status dialog box. A list of all BACnet objects in this device appears on the Network tree.

NOTE: Make sure you are discovering objects in the correct device. It may take some time to discover objects in devices with more than 100 objects.

11. Optional: Do the following to export the BACnet information so that it can be used in the Third Party BACnet Utility or in the EIKON application:
    - On the Network tree, select a discovered network with devices or a single device.
    - Click *Export*.
    - Name and save the .discovery file in any folder.

NOTE: Some third party BACnet devices may not be discovered because they do not support the BACnet methods required for auto discovery.

If the discovery process returns ambiguous information, such as multiple points with similar names, contact the third party manufacturer's representative for clarification.

Device configuration or network load can prevent the Vertiv™ Liebert® SiteScan™ interface from showing all BACnet devices. If you do not see a BACnet device that you expect to see, check the system's BBMD configurations. If the configurations are correct, try the discovery process again.

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.twitter.com/Vertiv/

VERTIV™

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