



**Liebert®**

SiteScan Web™

Installer/User Guide

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

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

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

### **Technical Support Site**

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

# TABLE OF CONTENTS

<b>1 What Is Liebert SiteScan Web?</b> .....	<b>1</b>
1.1 How Does Liebert SiteScan Web Work? .....	2
1.2 Client Requirements .....	3
1.3 Server Requirements .....	4
<b>2 SiteScan Web User-Interface Overview</b> .....	<b>9</b>
2.1 Logging-on to SiteScan Web .....	10
2.2 Saving Changes .....	11
2.3 Navigation Tree .....	11
2.4 Zooming and Resizing in the Viewing Area .....	11
2.5 Hover-over Text .....	11
<b>3 Using the Geographic View</b> .....	<b>13</b>
3.1 Using the Geographic-view Navigation Tree .....	13
3.1.1 Icons in the Geographic-view Tree .....	13
3.2 Viewing Unit Data .....	14
3.3 Viewing the Graphic for an Area .....	14
3.4 Viewing Statuses on the Graphic Floor Plan .....	15
3.5 Viewing a Summary Page .....	15
3.6 Viewing and Managing Alarms on Equipment .....	16
3.6.1 Acknowledging Alarms .....	17
3.6.2 Acknowledging All Alarms at Once .....	17
3.6.3 Force an Alarm to Return-To-Normal .....	17
3.6.4 Deleting Alarms .....	18
3.6.5 Deleting All Alarms at Once .....	18
3.7 Viewing Trend Graphs .....	18
3.7.1 Tools for Viewing Trends .....	18
3.8 Viewing Reports .....	20
3.9 Using Shortcuts in the Geographic View .....	21
3.9.1 Using the Notes Shortcut .....	22
3.9.2 Using Maintenance Mode .....	22
3.9.3 Using the Edit Page Shortcut .....	23
3.9.4 Editing an Area .....	23
<b>4 Alarms</b> .....	<b>25</b>
4.1 Alarm Messages .....	25
4.1.1 Message Field-Code Definitions .....	27
4.2 Alarm Actions .....	30
4.2.1 Alarm Popup Action .....	32
4.2.2 Print on Alarm Action .....	32
4.2.3 Run External Program on Alarm Action .....	33
4.2.4 Send Alphanumeric Page on Alarm Action .....	34
4.2.5 Send E-Mail on Alarm Action .....	35
4.2.6 Send SNMP Trap on Alarm Action .....	36
4.2.7 Write Property on Alarm Action .....	37
4.2.8 Write to Database on Alarm Action .....	37
4.2.9 Write to File on Alarm Action .....	39
4.3 Enable/Disable Alarms .....	40
4.3.1 Viewing Selected Sources .....	42
4.4 Alarm Categories .....	43

4.5 Alarm Templates .....	44
4.6 Alarm Reports .....	46
<b>5 Trends .....</b>	<b>47</b>
5.1 Create a New Trend Graph .....	47
5.2 Configuring Trend Graphs .....	47
<b>6 Reports .....</b>	<b>49</b>
6.1 Finding Reports .....	49
6.2 Setting-Up New Reports .....	50
6.3 Setting Report Options .....	51
6.4 Adjusting Report Layout .....	52
6.5 Built-In Reports .....	52
6.5.1 Adjusting the Layout of Built-in Reports .....	53
<b>7 Using the Configuration View .....</b>	<b>55</b>
7.1 My Settings Configuration .....	55
7.1.1 Configuring User Settings .....	55
7.1.2 Configuring User Contact Info .....	56
7.2 System Settings Configuration .....	57
7.2.1 Configuring General System Settings .....	57
7.2.2 Configuring Daylight Saving Settings .....	57
7.3 Configuring Operators .....	58
7.3.1 Configuring Operator Groups .....	59
7.3.2 Configuring Privilege Sets .....	59
7.4 Services Status .....	62
7.5 Configuring Client Installs .....	62
7.6 Configuring the Trends Display Setup .....	62
7.7 Configuring Trends Print Setup .....	63
7.8 Changing Unit Bezel Colors .....	63
7.9 Event Color Scheme .....	63
<b>Appendices .....</b>	<b>65</b>
Appendix A: Technical Support .....	65

# 1 WHAT IS LIEBERT SITESCAN WEB?

The SiteScan Web 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 SiteScan Web system can be accessed from anywhere in the world through a web browser. On a workstation or mobile device, you can perform building management functions such as:

- adjust setpoints and other control parameters
- set and change schedules
- graphically trend important building conditions
- view and acknowledge alarms
- run pre-configured and custom reports on energy usage, occupant overrides, and much more

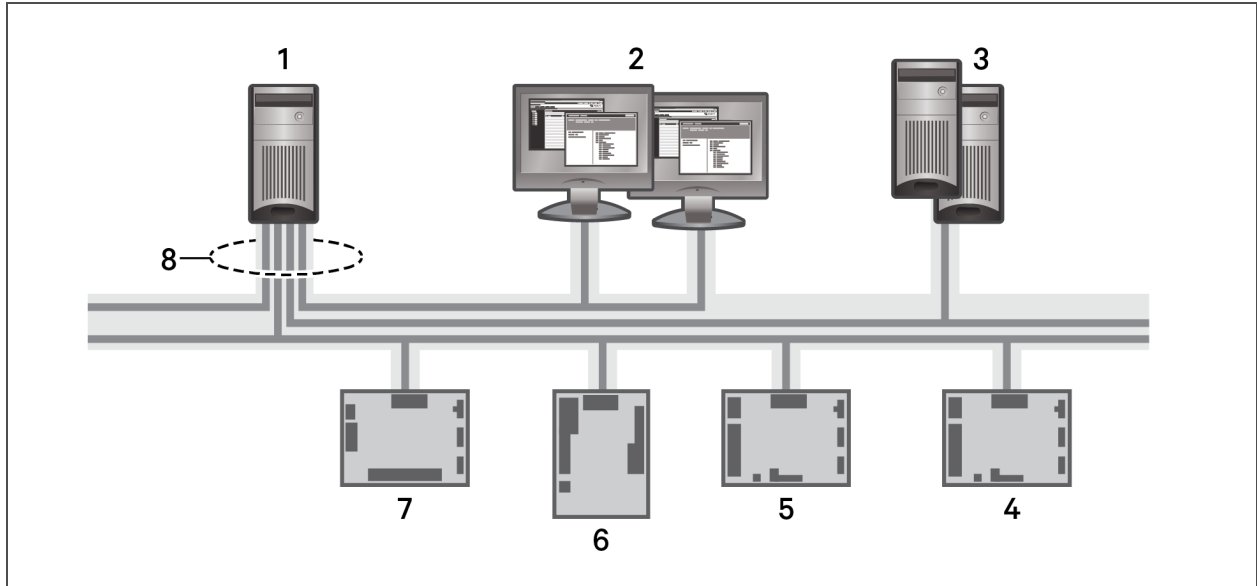
A SiteScan Web system supports:

- Unlimited simultaneous users
- Multiple operating systems and databases
- Mobile devices
- Built-in and custom alarms, trends, and reports
- 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

## 1.1 How Does Liebert SiteScan Web Work?

A SiteScanWeb system uses a network of microprocessor-based controllers to control heating, air conditioning, and other facility systems. A web-based server communicates with these controllers and generates the SiteScanWeb 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.

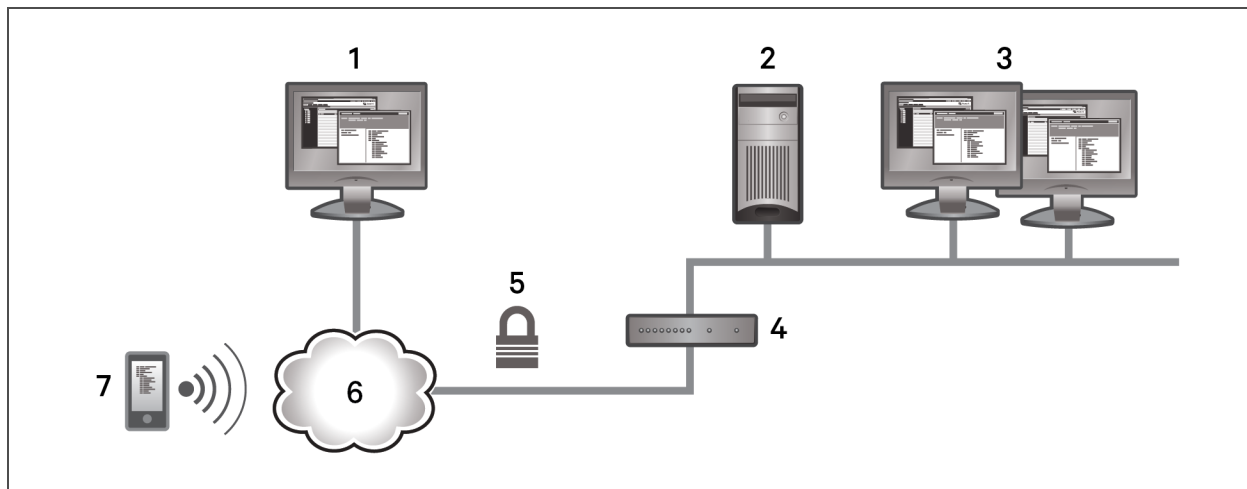
**Figure 1.1 Typical SiteScan Web System**



ITEM	DESCRIPTION
1	SiteScan Web server. Runs the SiteScan Web server application.
2	SiteScan Web clients. Access the SiteScan Web server as a web site using a standard web browser. Simultaneous users allowed based-on licensing.
3	Enterprise integration. With add-ons and web services, SiteScan Web integrates with other enterprise applications to share data across a facility's network.
4	SiteTPI-E integrates third-party protocols such as Modbus, LonWorks, and N2.
5	SiteIP-E integrates SNMP devices.
6	SiteIO-E is a multi-equipment controller.
7	SiteLink-E communications with Liebert® environmental/power equipment and with the Liebert® gateway.
8	Ethernet TCP/IP. Protocols include: BACnet, HTTP/HTTPS, XML/SOAP, and Liebert® legacy.

The SiteScanWeb client uses a web browser to access the SiteScanWeb Server application as a website.

**Figure 1.2 SiteScan Web Access and Security Options**



ITEM	DESCRIPTION
1	SiteScan Web client with outside, internet connection
2	SiteScan Web server (Java platform)
3	SiteScan Web clients on internal network
4	I/P router/Firewall
5	Network security: Transport layer security (TLS/HTTPS), Virtual private network (VPN)
6	Internet
7	SiteScan Web clients with outside, wireless browsers

## 1.2 Client Requirements

### Computers

The client computer should have at least the following:

- Dual-core processor
- 1.5 GB RAM
- Communication link of 10 Mbps or higher

**NOTE: SiteScan Web will work with slower computers, but the results may not be satisfactory.**

### Operating Systems and Web Browsers

A computer with Windows® operating system supports:

- Google™ Chrome™ v66.0 or later
- Internet Explorer® v11 Desktop
- Microsoft® Edge v40 or later
- Mozilla® Firefox® v60.0 or later

A computer with Mac® OS X® (Apple® Mac only) operating system supports:

- Safari® v11 or later
- Google™ Chrome™ v66.0 or later

- Mozilla® Firefox® v60.0 or later

A computer with Linux® operating system supports:

- Google™ Chrome™ v66.0 or later
- Mozilla® Firefox® v60.0 or later

## Mobile Devices

For smart-phone devices, the Android™ and iOS platforms are supported. For tablet devices, the Android™, iOS, and Surface™ platforms are supported.

**NOTE: Some functionality may be limited by the capability of the mobile device and operating system.**

## 1.3 Server Requirements

The SiteScan Web server must be 64-bit, and memory requirements will vary based on the following:

- number of pieces of equipment and device instances
- size of the control programs
- number of simultaneous users logged in to the SiteScan Web application

**Table 1.1 Server Requirements by System Size**

SIZE	WITH THE FOLLOWING NUMBER OF:		THE SERVER SHOULD HAVE AT LEAST A DUAL-CORE PROCESSOR AND THE FOLLOWING:			
	EQUIPMENT AND DEVICE INSTANCES <sup>1</sup>	PHYSICAL POINTS AND DISPLAY OBJECTS	PASSMARK TOTAL SCORE <sup>2</sup>	PASSMARK SINGLE-THREADED SCORE	GB RAM (MINIMUM /RECOMMENDED)	GB JVM MEMORY (MINIMUM /RECOMMENDED)
Small	0 – 250	0 – 1000	2000	800	4/4	1/1
Medium	250 – 1000	1000 – 5000	3000	1000	4/8	2/4
Large	1000 – 10,000	5000 – 50,000	5000	1400	6/12	4/8
Huge	more than 10,000	more than 50,000	6500	1600	16/16 <sup>3</sup>	12/12

<sup>1</sup> Total number of control programs and controllers.  
<sup>2</sup> For more information, see [www.CPUBenchmark.net](http://www.CPUBenchmark.net).  
<sup>3</sup> For a huge system with minimal user activity, the average piece of equipment or instance device requires approximately 300 KB of server RAM. Contact Vertiv™ Technical Support for server sizing recommendations.

## Operating-System and Database Requirements

To determine which operating system and database management system (DBMS) to use, consider:

- Operating systems and DBMS's already in use in your customer's organization
- Project size and trending requirements. See [Trend Archival Requirements](#) on page 7.
- Project budget
- Your skill with the operating system and DBMS

The SiteScan Web system use of database resources may require:

- a moderate increase in the number of allowed connections if your database management system is set to the default value for the maximum allowed connections.
- an increase in the maximum number of database cursors allowed may also be required for Oracle databases.



## Supported operating systems and database management systems

A WebCTRL® for OEMs v7.0 or later system is supported on the following 64-bit operating systems. The following table shows which operating systems can be used with each DBMS.

- Windows® 10 Professional
- Windows® 8.1 Professional and Enterprise
- Windows® 7 Professional and Ultimate
- Windows® Server 2016
- Windows® Server 2012 R2
- Red Hat Enterprise Linux® 7.4
- Ubuntu® Desktop 16.04 LTS

**Table 1.2 DBMS and Supported OS Matrix**

DATABASE	SUPPORTED OS	SPEED	MULTIPLE SERVERS SUPPORTED	DYNAMIC DEFRAGMENTATION	DATABASE REPLICATION	NOTES
SQL Server® Express 2017, 2016, 2014	Windows®	Fast	No	Yes	Yes	Database cannot exceed 10 GB.
SQL Server® 2017, 2016, 2014	Windows®	Fast	Yes	Yes	Yes	SQL Server® 2016 Enterprise, Business Intelligence, and Standard editions can be used. SQL Server® 2014 Enterprise, Business Intelligence, and Standard editions can be used.
Oracle 12c	Windows® Linux®	Moderate	Yes	Yes	Yes	Oracle® 12c Standard Edition is sufficient. Oracle 12c requires a Named-User License for each WebCTRL® for OEMs user or a Processor License. (Dual processor machines count as two users.) See Oracle® License Policies for more details.

**Table 1.2 DBMS and Supported OS Matrix (continued)**

DATABASE	SUPPORTED OS	SPEED	MULTIPLE SERVERS SUPPORTED	DYNAMIC DEFRAGMENTATION	DATABASE REPLICATION	NOTES
MySQL 5.7.2	Windows® Linux®	Fast	Yes	No	Yes	This open source database is free under the GNU Public License.
PostgreSQL 9.4 and 10	Windows® Linux®	Fast	Yes	Yes	Yes	This open source database is free under the BSD Public License.
Apache Derby	Windows® Linux®	Slow	No	No	Yes	<ul style="list-style-type: none"> <li>• The WebCTRL® for OEMs Installs for Windows and Linux include all the files needed to use an Apache Derby database.</li> <li>• Only one application can access the database at one time. Example: VewBuilder cannot access the database if SiteBuilder is already running.</li> <li>• Do not use Derby if total historical trend capacity will exceed 2 GB.</li> <li>• Audit database cannot contain an entry of more than 32,700 characters; compact the database before migrating to Derby.</li> </ul>

## Trend Archival Requirements

Trend archival (historical trending) requirements are the most significant factors in database selection. Alarms are not usually an issue unless large quantities (10,000+) will be kept for online access. For each archived trend sample, the WebCTRL® for OEMs application stores approximately 30 bytes of data. Disk space requirements per trended point are:

SAMPLE INTERVAL	FOR 1 WEEK	FOR 1 MONTH	FOR 3 MONTHS	FOR 1 YEAR
1 minute	300 kB	1.5 MB	5 MB	18 MB
5 minutes	60 kB	250 kB	1 MB	4 MB
15 minutes	21 kB	85 kB	250 kB	1 MB
1 hour	5 kB	20 kB	60 kB	240 kB

For example, a system with 2000 points archiving at 15-minute intervals for one year will require as much as 5.6 GB (2000 x 2.8 MB) disk space.

Notes on trend requirements:

- To limit disk space required for trend storage, archive trend data only for important system points.
- If your archival requirements are 5 GB or greater, you should consider using a separate server for the trend database.
- If you use a separate trend database server, you can run the SiteScan Web application on a Microsoft operating system with any or all of its databases on non-Microsoft operating systems. But, you cannot run the SiteScan Web application on a non-Microsoft operating system and connect to Microsoft® database products. So, if you have Apache Derby or SQL Server® databases, the SiteScan Web application must be running on Windows 8.1 Professional, 8.1 Enterprise, or 10.

Example: The SiteScan Web application on Linux® can connect to MySQL on Linux®. But, it cannot connect to Apache Derby, SQL Server® on Windows.

This page intentionally left blank

## 2 SITESCAN WEB USER-INTERFACE OVERVIEW

Figure 2.1 on the next page, describes the main sections and features of the SiteScan Web window.

Views logically divide the functions of SiteScan Web. Table 2.1 below, describes the icons located above the navigation tree that select the items and functions displayed in the navigation tree, menu tabs, and view pane.

**Table 2.1 View-selection icons**





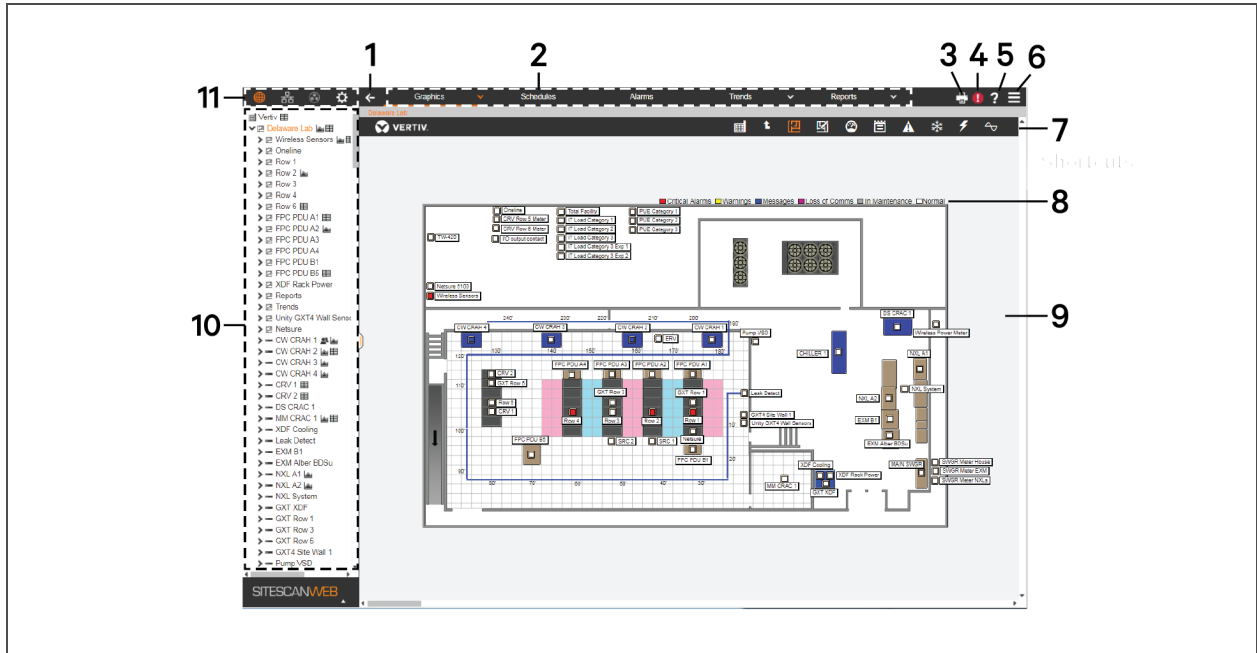
ICON	DESCRIPTION
	Geographic view. See <a href="#">Using the Geographic View</a> on page 13.
	Network view.
	Schedule Groups view.
	System Configuration view. See <a href="#">Using the Configuration View</a> on page 55.

Figure 2.1 Workspace features and options



ITEM	DESCRIPTION
1	Back button
2	Menu tab options. See
3	Print
4	System-wide alarms. See <a href="#">Viewing and Managing Alarms on Equipment</a> on page 16.
5	Help
6	SiteScan Web Menu
7	Shortcuts bar. See <a href="#">Using Shortcuts in the Geographic View</a> on page 21.
8	Color-coded shortcuts legend. See <a href="#">Viewing Statuses on the Graphic Floor Plan</a> on page 15.
9	View pane
10	Navigation tree pane. See <a href="#">Navigation Tree</a> on the facing page.
11	Navigation tree options. See <a href="#">Navigation Tree</a> on the facing page

## 2.1 Logging-on to SiteScan Web

To access SiteScan Web:

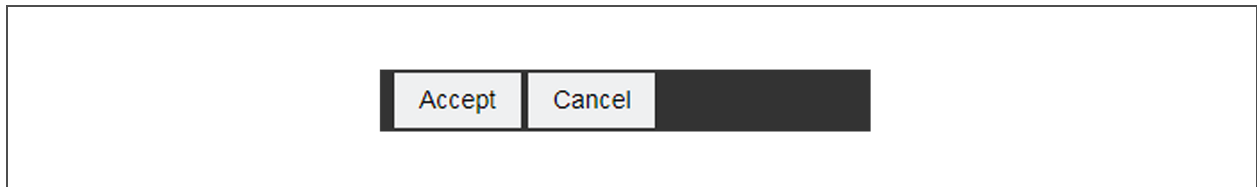
1. Open a web browser, and enter the URL for the SiteScan Web server in the address bar.
2. Enter your user name and password (provided by Vertiv™ Technical Support), and click *Log in*.

## 2.2 Saving Changes

You must save certain changes to SiteScan Web. Whenever you make a change that must be saved, the Accept and Cancel buttons appear in the tool bar.

- Click *Accept* to save the changes.
- Click *Cancel* to discard the changes.

**Figure 2.2** Save-changes buttons in toolbar



## 2.3 Navigation Tree

The Navigation tree provides quick access to options depending on the selected view.

To show the navigation tree:

- Click the down arrow next to the application name in the upper-left of the window, see **Figure 2.3** below.

To hide the navigation tree:

- Click the up arrow next to the application name at the bottom of the navigation tree, see **Figure 2.3** below.

**Figure 2.3** Opening and Closing the navigation tree



ITEM	DESCRIPTION
1	Down arrow to expand the navigation tree
2	Up arrow to hide the navigation tree.

## 2.4 Zooming and Resizing in the Viewing Area

- Hold the CTRL key while rolling the mouse wheel to zoom in or out on the contents of the Viewing Area.
- Right-click the Viewing Area and select *Scale to 100%* to restore the contents to their original size.
- If a graphic does not fit in the viewing area, right-click it and select *Scale to Fit* to make it fit the viewing area.

## 2.5 Hover-over Text

Hover text reveals information about an item when you hold the cursor over a system, area or equipment icon. Depending on the options enabled, you can display a list of associated schedules, trends, reports, and alarm actions.

1. Right-click anywhere in the navigation tree and select *Tree Display Options*.
2. Click to check the information to display, click *Apply* and then *Close*.



## 3 USING THE GEOGRAPHIC VIEW

The Geographic view lets you navigate SiteScan Web based on the geographic layout of the monitored site.

When you select the geographic view, the menus described in **Table 3.1** below, are offered.

**Table 3.1 Geographic View menus and options**

MENU TAB	DESCRIPTION
Graphics	Offers a quick look of the status of your entire system or any portion of it as a graphic-overlay. See <a href="#">Viewing the Graphic for an Area</a> on the next page.
Alarms	Lets you view and acknowledge system alarms. See <a href="#">Viewing and Managing Alarms on Equipment</a> on page 16. This menu-tab also offers several other alarm-management options, see <a href="#">Alarms</a> on page 25, for more details.
Trends	Lets you review equipment status values over time to monitor the equipment's operation. See <a href="#">Viewing Trend Graphs</a> on page 18. You can also use this tab to customize and manage trends, see <a href="#">Trends</a> on page 47, for more details.
Reports	Lets you compile alarm and other information to help manage and troubleshoot your system. See <a href="#">Viewing Reports</a> on page 20. You can also use this tab to configure existing reports and create and customize reports, see <a href="#">Reports</a> on page 49, for more details.




### 3.1 Using the Geographic-view Navigation Tree

When you are in the geographic view, the navigation tree provides information about and access to your site and equipment.

#### 3.1.1 Icons in the Geographic-view Tree

The navigation tree displays an icon to the left of each item to denote the type of item. **Table 3.2** below, describes the icons.

**Table 3.2 Geographic-view tree icons**





ICON	DESCRIPTION
	System
	Area
	Equipment

In addition to the identification icons that display to the left of the equipment in the tree, you can display additional icons to the right of the items to indicate where equipment was created or is assigned. **Table 3.3** on the next page, describes the optional icons.

To display the optional icons:

1. Right-click anywhere in the navigation tree and select *Tree Display Options*.
2. Click to check the icons to display, click *Apply* and then *Close*.

**Table 3.3 Optional Geographic-view tree icons**

ICON	DESCRIPTION
	Indicates schedules assigned to the item.
	Indicates trends assigned to the item.
	Indicates reports assigned to the item.
	Indicates alarm actions assigned to the item.

### 3.2 Viewing Unit Data


The unit-data view shows the status and other information about the unit in the view pane. Select a unit in the navigation tree to display the unit data.

The unit-data view includes an alarms section at the bottom of the window that displays descriptive text for detected alarms.

### 3.3 Viewing the Graphic for an Area

The Graphics menu-tab in the geographic view opens a drawing or floor plan that shows device placement

To view an area graphic:

Select a unit in the geographic-view tree, then click *Graphics* in the menu bar or  in the shortcuts bar.

### 3.4 Viewing Statuses on the Graphic Floor Plan

In the geographic view, when you view an area graphic, status information is available for the units and equipment.

Each item in the floor plan has an icon with two parts:

- A text label with the assigned name of the item.
- A color-coded button that indicates whether or not notifications or alarms are present. **Table 3.4** below, describes the color coding, which are also defined in a legend above the floor plan in the view pane. For more details on alarms, see [Viewing and Managing Alarms on Equipment](#) on the next page.

**Table 3.4 Graphic-status color codes**

COLOR	INDICATES:
Red	Critical alarm present
White	No alarms present
Yellow	Warning present
Blue	Message present
Purple	Loss of communication
Gray	In maintenance mode

To view status and other information for any item:

- Hover over the color-coded button to display key information pop-up—the current status and the number of alarms, warnings and other information.
- Click the color-coded button to open the view of that item.

### 3.5 Viewing a Summary Page

Summary pages list the status of all the components of a selected item. **Table 3.5** on the next page describes the available summaries.

To view a summary page:

- Select a unit in the geographic-view tree, and click the appropriate icon in the shortcuts bar. See **Table 3.9** on page 21.
- or –
- Select a unit in the geographic-view tree, click the drop-down arrow next to the Graphics tab to display the available summaries, and select a summary.

**NOTE:** The summaries available depend on the item you select in the navigation tree.


**Table 3.5 Summary Pages**

SUMMARY	DESCRIPTION
Unit_summary	The unit summary differs depending on the level of the item selected in the tree. <ul style="list-style-type: none"> <li>At the top level, all areas are listed along with the alarm information for each.</li> <li>The unit summary for an area lists all the monitored equipment in that area, including cooling units, power equipment, UPS's and static switches.</li> <li>At lower levels, the summary lists data for the monitored equipment at that level.</li> </ul>
Air_summary	Summary list of all thermal-management units at the site.
Power_summary	Summary list of all power units at the site.
UPS_summary	Summary list of all UPS units at the site.
Staticswitch_summary	Summary list of all static switches at the site.

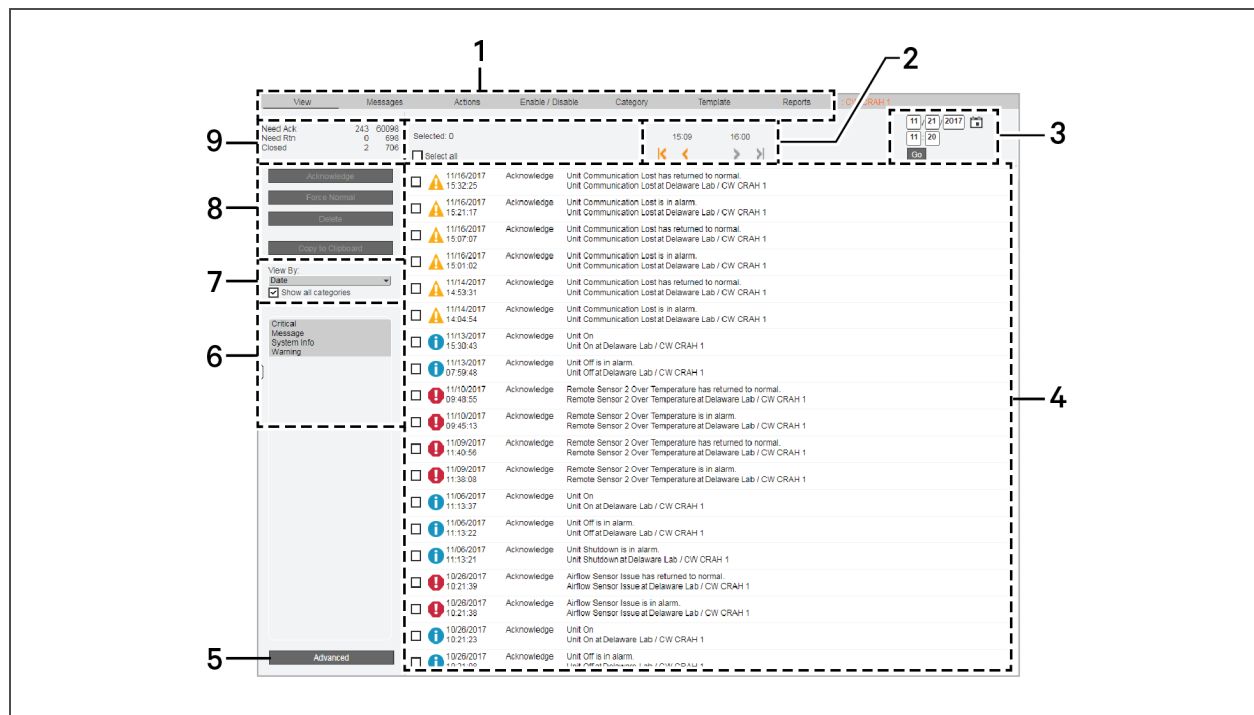
### 3.6 Viewing and Managing Alarms on Equipment

The View tab under the Alarms menu-tab allows you to view alarms and perform functions such as acknowledging alarms.

To view alarms:

1. Click , then click an item in the navigation tree.
2. Click the *Alarms* menu tab, then *View*.  
The alarm list displays, see **Figure 3.1** below.
3. Double-click an alarm in the list to show/hide details.

**Figure 3.1 Alarms view tab**



**Table 3.6 Alarm View fields and options**

ITEM	DESCRIPTION
1	Alarm menu tabs. See <a href="#">Alarms</a> on page 25, for more details on each.
2	Navigation buttons. Scroll through the list one alarm at a time, a page at a time or to the beginning or end of the list.
3	Search for an Alarm by Time of Occurrence. Select the date and time, and click <i>Go</i> . A list of alarms matching the selection displays.
4	Alarms list. Three columns display the following: <ul style="list-style-type: none"> <li>The first column indicates the date and time the alarm was generated.</li> <li>The second column indicates the status of the alarm: <ul style="list-style-type: none"> <li>Acknowledge = needs acknowledged.</li> <li>Waiting for Normal = requires a return-to-normal.</li> <li>Closed = the alarm is closed.</li> </ul> </li> <li>The third column is the alarm message including a description of what occurred and where.</li> </ul>
5	Advanced management. Acknowledge and management all alarms at once, see: <ul style="list-style-type: none"> <li><a href="#">Acknowledging All Alarms at Once</a> below</li> <li><a href="#">Deleting All Alarms at Once</a> on the next page</li> </ul>
6	Alarm Categories. To display only alarms, click an item in the Categories list. Use <b>CTRL+click</b> to select multiple categories.
7	View by. To sort or group the listed alarms. Options are: <ul style="list-style-type: none"> <li>Date = all alarms sorted by the time each alarm was generated, from newest to oldest.</li> <li>To Do = alarms requiring one or more actions to be done before they can be closed.</li> <li>Incident Group = all alarms related to a particular incident with a bracket to the left of the icons—for example, an alarm and its subsequent return-to-normal event form an incident group.</li> </ul>
8	Options to manage single and multiple-selected alarms, see: <ul style="list-style-type: none"> <li><a href="#">Acknowledging Alarms</a> below</li> <li><a href="#">Force an Alarm to Return-To-Normal</a> below</li> <li><a href="#">Deleting Alarms</a> on the next page</li> </ul>
9	Status summary counts. a quick glance at the current state of alarms at the location selected in the tree ( <i>Here</i> ) and in the entire system ( <i>Total</i> ): <ul style="list-style-type: none"> <li>Need Rtn = Number of alarms that need a return-to-normal.</li> <li>Need Ack = Number of alarms that need to be acknowledged.</li> <li>Closed = Number of alarms that are closed.</li> </ul>

### 3.6.1 Acknowledging Alarms

In the alarms list, click to check the alarm(s) to acknowledge, then click *Acknowledge*.

### 3.6.2 Acknowledging All Alarms at Once

The *Advanced* button allows you to acknowledge all alarms in selected categories at once.

1. Select the categories in the list.
2. Click *Advanced* below the category list, then click *Acknowledge All*.

### 3.6.3 Force an Alarm to Return-To-Normal

If an alarm is not followed by a return-to-normal event, you can force a Return-To-Normal state.

1. Select an alarm that shows *Waiting for normal* in the list.
2. Click the *Force Normal* button.

### 3.6.4 Deleting Alarms

In the alarms list, click to check the alarm(s) to delete, then click *Delete*.


### 3.6.5 Deleting All Alarms at Once

The *Advanced* button allows you to acknowledge all alarms in selected categories at once.

1. Select the categories in the list.
2. Click *Advanced* below the category list, then click one of the following options:
  - Delete Closed Incidents - Removes all closed alarms.
  - All - Removes all alarms at the selected location in the tree.

## 3.7 Viewing Trend Graphs

To view a trend graph:

1. Click , then click an item in the navigation tree.
2. Click the *Trends* menu-tab at the top of the window.
  - If more than one graph is available for the view, click the drop-down arrow next the Trends tab, and choose a graph.
3. Click *View* to display the graph.
  - For tips on navigating the graph—zoom/pan, choose start dates, view point data—see **Table 3.7** below.
  - Use the print icon in the top right corner of the Trends window to print the graph.
  - For details on setting-up and configuring trend graphs, see [Trends](#) on page 47.

### 3.7.1 Tools for Viewing Trends

- A vertical dashed line indicates missing data.
- A large marker indicates a point that is in alarm, in fault, out-of-service, or is overridden. CTRL+click the marker to view details.
- Right-click anywhere on a trend graph to display a pop-up menu with tools described in **Table 3.7** below. Click an item in the menu—or use keyboard shortcuts shown in parentheses ( ) on the menu.

**Table 3.7** Trend-view tools


TOOL	KEYBOARD SHORTCUT	NOTES
Pan left/right/up/down	Arrow keys	If you display more than one graph, panning up and down affects only one graph at a time. Panning left to right affects all graphs. You can also Alt+click and drag inside the graph.
Zoom in	Page Down	You can also use the plus (+) key on the numeric keypad, the <b>X</b> key, or drag a rectangle around area.
Zoom out	Page Up	You can also use the minus (-) key on the numeric keypad or the <b>Z</b> key.
Zoom to extents	Home	Shows all the data you have viewed in the current session of a particular trend graph.
Reset view	End	Resets the display to its default setting. You can also use the Enter or <b>R</b> key.
Undo	Esc	Undo up to 10 changes to your view.
Set start date	J	Enter the date you want the trend to jump to. The trend displays the same time range for the new date. Press the <b>J</b> key again to hide the date fields.
History Only	H	Displays only the historical data on the graph.
Auto Update	U	The trend graph polls for data every 10 seconds. Press <b>U</b> again to stop updating.

**Table 3.7 Trend-view tools (continued)**

TOOL	KEYBOARD SHORTCUT	NOTES
Point Markers	M	Shows a marker for each data point in the graph.
Copy	Ctrl+C	Copies only the data from the time range that is currently displayed.
Refresh the display (gather trend data) <i>(not available on the popup menu)</i>	—	Click the <i>Trends</i> menu-tab.
Display data for a specific sample <i>(not available on the pop-up menu)</i>	—	<b>Ctrl</b> +click a sample to view the point name, time, and date the sample was read, the exact point value, and if the point is in alarm, is in fault, out of service, or has been overridden. Click anywhere to clear the details.

### 3.8 Viewing Reports

To view reports:

1. Click , then click an item in the navigation tree.
2. Click the *Reports* menu-tab, then click the *View* tab.
3. To view an existing report, click the *Reports* drop-down arrow, then on a category. Choose a report from the sub menu.  
– or –  
Click *Run* button generate a report.

**Table 3.8** below, describes the SiteScan Web built-in reports available. For more details on managing and running reports, see [Reports](#) on page 4-9.

**Table 3.8 Available reports**

REPORT	DESCRIPTION
<b>Alarms</b>	
Alarm Actions	Create a summary of the information configured in the Alarms > <i>Actions</i> tab.
Alarm Prefixes & Details	Create a summary of the information configured in the Alarms > <i>Messages</i> tab.
Alarm Sources	Create a summary of potential alarm sources configured in the Alarms > <b>Enable/Disable</b> tab.
Alarms	View, sort and filter the information displayed in the Alarms <i>View</i> tab.
<b>Commissioning</b>	
Equipment Checkout	View the information on the <i>Equipment Checkout</i> tab of the Point Checkout tool during commissioning. Also, find equipment that has not been fully commissioned.
<b>Equipment</b>	
Locked Values	Find all locked points and locked values. <b>NOTE: Locks in the Airlfow microblock are not reported.</b>
Network IO	Verify the programming and status of all network points—especially useful for commissioning control modules used for third-party integration.
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	Create a summary of the information configured in the Trends <i>Enable/Disable</i> tab.
<b>Schedules</b>	
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 entered at and below a selected tree item. This report shows the location of each item and can help you find newly added and conflicting schedules.
<b>Security</b>	
<b>NOTE: You must have the Advanced Security package to run these reports.</b>	
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.



**Table 3.8 Available reports (continued)**












REPORT	DESCRIPTION
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.

### 3.9 Using Shortcuts in the Geographic View










A toolbar with shortcuts appears directly below the menu tabs in the view pane. The icons vary according to the item you are viewing. If power equipment is selected, the icons relate to power equipment. If cooling equipment is selected, icons related to cooling equipment display. **Table 3.9** below describes the icons.

**NOTE: The toolbar icons disappear in some views. They will reappear when the cursor hovers over the toolbar area.**



**Table 3.9 Shortcut Icons**

ICON	DESCRIPTION
	System Overview. Navigates to the highest level of the geographic-view tree.
	Summary. Displays summary data for the equipment selected in the tree/displayed in the area graphic (in the view pane). See <a href="#">Viewing a Summary Page</a> on page 15.
	Show/Hide Notes. View or add notes about the item. See <a href="#">Using the Notes Shortcut</a> on the next page.
	Area Graphic. Displays the floor plan of the selected item. See <a href="#">Viewing the Graphic for an Area</a> on page 14
	Up One Level. Moves the view up one level in the tree.
	Maintenance mode. Enables/Disables maintenance mode and lets you schedule maintenance for the selected equipment. See <a href="#">Using Maintenance Mode</a> on the next page.
	Trend Graphs. Opens the trend graph for the selected item. See <a href="#">Viewing Trend Graphs</a> on page 18.
	Edit Page. Opens a page to view and edit the characteristics of the selected item. See <a href="#">Using the Edit Page Shortcut</a> on page 23.
	Area Edit. Displays an editable floor plan to moving and rename units and customize the area floor plan. See <a href="#">Editing an Area</a> on page 23.
	Air Summary. Displays a summary of thermal-management units, temperature, heating, cooling, humidification, and dehumidification. See <a href="#">Viewing a Summary Page</a> on page 15.
	Power Summary. Displays a summary of power status, input voltage, output (voltage and amps), load percentage, and power factor. See <a href="#">Viewing a Summary Page</a> on page 15.

**Table 3.9 Shortcut Icons (continued)**

ICON	DESCRIPTION
	Static Switch Summary. Displays a summary of static-switch status (voltage, current, and power in kVA, kW, and Hz). See <a href="#">Viewing a Summary Page</a> on page 15.
	UPS Summary. Displays a summary of UPS status, bypass voltage, input voltage, battery conditions, inverter status, output (voltage, current, and power in kVa, kW, and Hz). See <a href="#">Viewing a Summary Page</a> on page 15.
	Disable Notifications. Displays a list of notifications for the unit with option to disable notifications.
	Pencil (only in area-edit mode). Edit item names and setpoints for selected units. See <a href="#">Editing an Area</a> on the facing page.
	Save Changes (only in area-edit mode). Saves changes to the floor plan. See <a href="#">Editing an Area</a> on the facing page.
	Unlock Units (only in area-edit mode). Unlocks the floor plan to move units and their labels. See <a href="#">Editing an Area</a> on the facing page.
	Lock Units (only in area-edit mode). Locks the floor plan to prevent moving units and labels. See <a href="#">Editing an Area</a> on the facing page.
	Add Object (only in area-edit mode). Opens a drop-down list of items to add to the floor plan. See <a href="#">Editing an Area</a> on the facing page.
	Delete Object (only in area-edit mode). Deletes an object for the floor plan. See <a href="#">Editing an Area</a> on the facing page.


### 3.9.1 Using the Notes Shortcut

1. With an item selected, click .  
The notes page opens.
2. Enter the note text.
3. Click  again to return to the previous view.

**NOTE: Notes remain until deleted.**

### 3.9.2 Using Maintenance Mode


To view or edit a maintenance schedule:

1. With an item selected, click .  
The maintenance page opens listing the Description (name of the device) and the Maintenance Status (On or Off).
2. Select the Type of maintenance:
  - Now = enables the option to *Run Maintenance Now*.
  - Future = enables the option to *Schedule Maintenance*, and displays time and date options to schedule the maintenance.
3. Set the Duration of maintenance for the device in hours and minutes.
4. If scheduling future maintenance, select the date and time for maintenance to begin.

5. Depending on the type of maintenance selected:
  - Click *Run Maintenance Now* to perform maintenance immediately.
  - Click *Schedule Maintenance* to save and activate the maintenance schedule.
6. In the menu bar, click *Accept* to confirm the maintenance-mode settings or *Cancel* to discard the changes.

### 3.9.3 Using the Edit Page Shortcut

To view or change the characteristics of the selected unit or point:




1. With an item selected, click . The edit page opens.
2. Make changes as needed.
3. When finished, click *Submit*. To cancel changes, navigate to another page without clicking *Submit*.

### 3.9.4 Editing an Area




In area-edit mode, you can add, move, rename, and delete items on a floor plan.

**NOTE: If any units are outside the view: CTRL+Right-click > Clear Unit Positions and reposition units as needed.**





To add an object:

1. View an area graphic, and click  in the shortcuts bar.
2. Click , select an object from the list, adjust the parameters, and click *Apply*.
3. Click  to save the changes.




To rename an object:

1. View an area graphic, and click  in the shortcuts bar.
2. Click , and edit the name.
3. Click  to save the changes.

To move an object:

1. View an area graphic, and click  in the shortcuts bar.
2. Click  to unlock the floor plan.
3. Drag the unit and/or label to the new location.
4. Click  to save the changes.
5. Click  to lock the floor plan and prevent unauthorized changes.

To delete an object:

1. View an area graphic, and click  in the shortcuts bar.
2. Select an object to delete, then click .
3. Click  to save the changes.

## 4 ALARMS

The Alarms menu-tab in the geographic view offers quick access to alarm-related features, described in [Table 4.1](#) below.

**Table 4.1 Alarms menu-tab options**

TAB	DESCRIPTION
View	Lets you view and acknowledge system alarms. See <a href="#">Viewing and Managing Alarms on Equipment</a> on page 16.
Messages	Lets you format the content of alarm messages. See <a href="#">Alarm Messages</a> below.
Actions	<p>Lets you configure the actions performed by SiteScan Web when an alarm occurs including:</p> <ul style="list-style-type: none"> <li>• Sending an alert to designated recipients' computers when specified alarms occur. See <a href="#">Alarm Popup Action</a> on page 32.</li> <li>• Sending an alert to a designated printer when a specified alarm occurs. See <a href="#">Print on Alarm Action</a> on page 32.</li> <li>• Launching a script that starts a program or batch file on the server when an alarm is received. See <a href="#">Run External Program on Alarm Action</a> on page 33.</li> <li>• Sending a page to one or more alphanumeric pagers or sends text messages to cell phones. See <a href="#">Send Alphanumeric Page on Alarm Action</a> on page 34.</li> <li>• Sending customized e-mail messages to selected recipients when an alarm occurs. See <a href="#">Send E-Mail on Alarm Action</a> on page 35.</li> <li>• Sending an SNMP trap in response to receiving an alarm. See <a href="#">Send SNMP Trap on Alarm Action</a> on page 36.</li> <li>• Updating a microblock property value. See <a href="#">Write Property on Alarm Action</a> on page 37.</li> <li>• Storing alarm information in a database. See <a href="#">Write to Database on Alarm Action</a> on page 37.</li> <li>• Recording alarm information in a file. See <a href="#">Write to File on Alarm Action</a> on page 39.</li> </ul>
Enable/Disable	Lets you customize the treatment of alarms and return-to-normal events for selected alarm sources. See <a href="#">Enable/Disable Alarms</a> on page 40.
Reports	Lets you access all alarm-related reports. See <a href="#">Alarm Reports</a> on page 46

### 4.1 Alarm Messages

An alarm message is the text displayed in the Alarms View and in alarm reports. An alarm message may consist of three parts:

- Prefix (optional) - Text at beginning of message
- Text - The alarm or return-to-normal
- Details (optional) - Text at end of message

Changes to messages apply to the location in the navigation tree where they are added and to all the area or device's subordinate members in the tree. For example, if you add Details at the system level to show the Acknowledge Time for alarms in a certain category, the details will appear in all alarm message for every item in the system.

To view the message options:


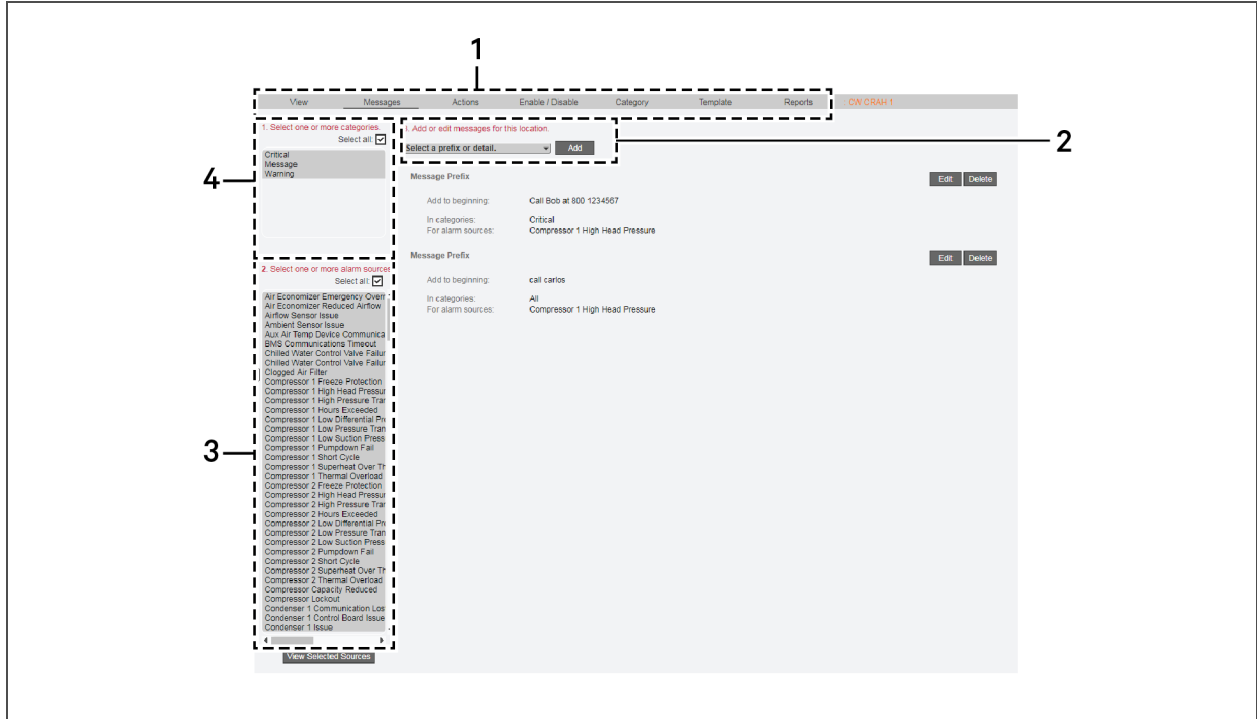
1. Click  then click an item in the navigation tree.
2. Click the *Alarms* menu tab, then *Messages*.

Figure 4.1 Alarm messages tab



ITEM	DESCRIPTION
1	Alarm menu tabs.
2	Edit options
3	Alarm sources
4	Message categories

To add message prefixes and details:

1. Select the categories that contain the alarm sources with messages you want to edit.
2. Select the alarm sources for the selected categories.

**NOTE:** In steps 1 and 2, control-click to select multiple items, or check the *Select All* box.

3. Select an option to add or edit from the drop-down list:
  - Add new prefix to beginning of message  
– or –  
Add new details to end of message.
4. Click *Add*.  
The Message Details window opens with options for entries for alarms and return-to-normal events.
5. Enter the text to add in the text boxes.
6. To add a field code, click *Append Field Code* and select from the drop-down list (see **Table 4.2** on the facing page for definitions).
7. Click *Accept* to save the changes or *Cancel* to close without saving.  
The new Prefix or Details display in the Messages view area.

### To edit message prefixes and details:

1. Select the categories that contain the alarm sources with messages you want to edit.
2. Select the alarm sources for the selected categories.
3. Click *Edit*.  
The Message Details window opens.
4. Make the changes, then click *Accept* to save the changes or *Cancel* to close without saving.  
The updated Prefix or Details display in the Messages view area.

### To delete message prefixes and details:

1. Select the categories that contain the alarm sources with prefix or details you want to delete.
2. Select the alarm sources for the selected categories.
3. Click *Delete*, then click *Accept* to save the changes or *Cancel* to close without saving.  
The Prefix or Details are removed.

## 4.1.1 Message Field-Code Definitions

**Table 4.2** below, shows the field codes displayed in Action and Messages windows.

**Table 4.2 Field code definitions**

FIELD CODE NAME	FIELD CODE	DEFINITION
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 that the alarm is assigned to. Example: HVAC Critical
Alarm Priority	\$alarm_priority\$	The priority number associated with the alarm's priority (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.
Alarm Type	\$event_type\$	The alarm type of the alarm source Example: CHANGE OF STATE.
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
Device	\$device\$	The display name of the device where the alarm came from.

**Table 4.2 Field code definitions (continued)**

FIELD CODE NAME	FIELD CODE	DEFINITION
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	\$exceed_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. Examples: 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 alarm's entire incident group closed. Example: Nov 12, 2012 6:35:18 PM
Latched Data Value (Analog)	\$latched_data_analog:x\$	"x" ranges from 1 to 10. Returns a numerical value.
Latched Data Value (Digital)	\$latched_data_digital:x\$	"x" ranges from 1 to 10. Returns On or Off.
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.
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.



**Table 4.2 Field code definitions (continued)**

FIELD CODE NAME	FIELD CODE	DEFINITION
		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 Web 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
Receive Time	\$receive_time\$	The time at the workstation when the alarm was received. Example: Nov 12, 2012 6:35:18 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, 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 FLOATINGLIMIT. 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 6:35:18 PM
Setpoint Value	\$setpoint_value\$	The 'setpoint value' from the alarm source. Valid only for alarm type FLOATINGLIMIT. 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

**Table 4.2 Field code definitions (continued)**

FIELD CODE NAME	FIELD CODE	DEFINITION
Source Path	\$source:<path>\$	Substitute <path> with the path to the value you want to display. 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\$ <b>NOTE: You can use Global Modify to get the path.</b>
System Directory	\$system_dir\$	The system folder name. Example: c:\SiteScanWeb6.0\webroot\ world_corporation
To State	\$to_state\$	The current state of the alarm source. Example: NORMAL, FAULT, OFF NORMAL, HIGH LIMIT, LOW LIMIT

## 4.2 Alarm Actions

Alarm actions protect valuable equipment, data and other assets by responding automatically to alarms in devices affected by events such as power failures, overheating and mechanical failures.

For example, if a cooling unit's performance becomes impaired, SiteScan Web can send e-mail alerts to various personnel, record data pertaining to the event, append it to a file, and launch a command or batch file to execute user-customized scripts.

To access the action functions:


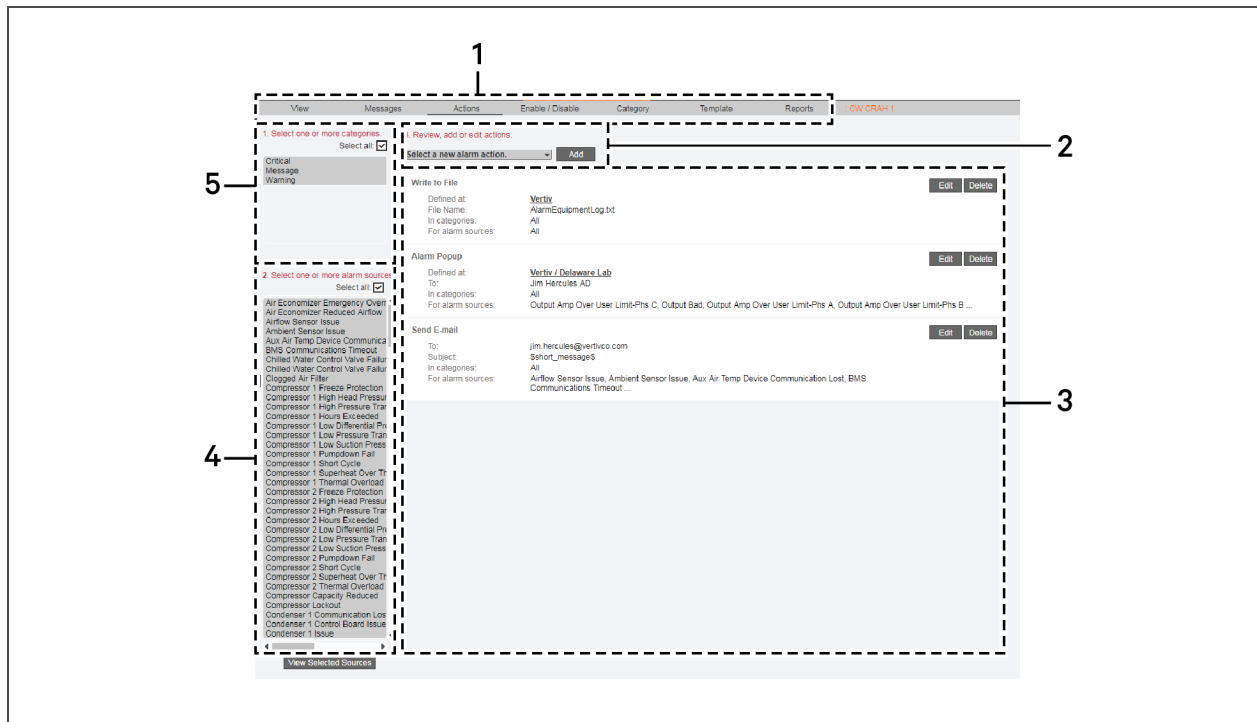
1. Click , then click an item in the navigation tree.
2. Click the *Alarms* menu tab, then *Actions*.

Figure 4.2 Alarm Actions tab



ITEM	DESCRIPTION
1	Alarm menu tabs.
2	Action options
3	Configured actions
4	Alarm sources
5	Alarm categories

1. Select the categories that contain the alarm sources to set up.
2. Select the alarm sources for the selected categories.

**NOTE:** In steps **Select the categories that contain the alarm sources to set up.** above and **Select the alarm sources for the selected categories.** above, control-click to select multiple items, or check the **Select All** box.

3. To choose an action, click the down arrow and select an option from the drop-down menu.
4. Click the **Add** button.
5. Proceed to the appropriate section to continue setting up the action.
  - [Alarm Popup Action](#) on the next page
  - [Print on Alarm Action](#) on the next page
  - [Run External Program on Alarm Action](#) on page 33
  - [Send Alphanumeric Page on Alarm Action](#) on page 34
  - [Send E-Mail on Alarm Action](#) on page 35
  - [Send SNMP Trap on Alarm Action](#) on page 36
  - [Write Property on Alarm Action](#) on page 37
  - [Write to Database on Alarm Action](#) on page 37
  - [Write to File on Alarm Action](#) on page 39

## 4.2.1 Alarm Popup Action

The Alarm Popup action sends an alert to designated recipients' when the specified alarms occur, which pops up in a dialog box on each recipient's computer

A recipient may be any networked computer running the SiteScan Web Alarm Popup application. Individuals and groups may be selected from a list set up in configuration. For details on editing these lists, see [Configuring Operators](#) on page 58 and [Configuring Operator Groups](#) on page 59.

To set an alarm pop-up action:

1. Click , then click an item in the navigation tree, click the *Alarms* menu tab, then *Actions* .

**NOTE: When configured, the action applies to the designated item in the tree as well as its subordinate items.**

2. Select the categories that contain the alarm sources to set up from the drop-down list., then select the alarm sources for the selected categories to link to the action.
3. Select *Alarm Popup* from the drop-down, then click *Add*.
4. Select the recipients from the drop-down list:
  - Select individuals from *To Operator* , and click *Add* .
  - Select groups of operators from *To Group*, and click *Add* .
  - In the Recipients list, click to check the *Generate Alarm if Delivery Fails* box to send a system-info alarm to the SiteScan Web server if the recipient is not running the Alarm Popup application when an alert is sent.
5. In the *Message Text* box, enter the message to appear in the pop-up window, using the appropriate punctuation, including spaces, and returns to separate lines of text.
6. To add dynamic alarm data to the message, place the cursor in the message text, and select a code from the Append Field Code drop-down (see [Field code definitions](#) on page 27 for definitions).
7. By default, the action occurs when an alarm is detected and after the device returns to normal. To specify when to run the action:
  - Only when the device is *In Alarm* or after *Return to Normal*.
  - After a specified time if not *Returned to Normal* or not *Acknowledged*.\*
  - If a group with a specified schedule is *Occupied* (e.g., during work hours) or *Unoccupied*.\*

\*Available only with Advanced Alarming.
8. Click *Accept* to save the action or *Cancel* to close without saving. The action appears in the Actions view.

## 4.2.2 Print on Alarm Action

The Print action sends an alert to a designated printer when a specified alarm occurs. The printed message may be sent to any printer connected to the server or a workstation on the network.

To set an alarm print action:

1. Click , then click an item in the navigation tree, click the *Alarms* menu tab, then *Actions* .

**NOTE: When configured, the action applies to the designated item in the tree as well as its subordinate items.**

2. Select the categories that contain the alarm sources to set up from the drop-down list., then select the alarm sources for the selected categories to link to the action.
3. Select *Print* from the drop-down, then click *Add*.

- Click to check the box next to the printing method by printer type, and select the related print options described in [Print methods](#) below.

**Table 4.3 Print methods**

PRINTER TYPE	DESCRIPTION AND SETTINGS
Text Printing	For dot-matrix printer. Prints multiple alarms per page. <ul style="list-style-type: none"> <li>Enter the designated <i>Printer Name</i>.</li> <li>Enter the maximum line width in <i>Line Width</i>.</li> </ul>
Graphics Printing	For laser printer. Prints one alarm per page. <ul style="list-style-type: none"> <li>Select the <i>Font Name</i>.</li> <li>Select the <i>Font Style</i>.</li> <li>Enter the <i>Font Size</i> (in points).</li> </ul>

- In the *Text to print box*, enter the message to print, using the appropriate punctuation, including spaces, and returns to separate lines of text.
- To add dynamic alarm data to the message, place the cursor in the message text, and select a code from the Append Field Code drop-down (see [Field code definitions](#) on page 27 for definitions).
- By default, the action occurs when an alarm is detected and after the device returns to normal. To specify when to run the action:
  - Only when the device is *In Alarm* or after *Return to Normal*.
  - After a specified time if not *Returned to Normal* or not *Acknowledged*.\*
  - If a group with a specified schedule is *Occupied* (e.g., during work hours) or *Unoccupied*.\*

\*Available only with Advanced Alarming.
- Click *Accept* to save the action or *Cancel* to close without saving. The action appears in the Actions view.

### 4.2.3 Run External Program on Alarm Action

The Run External Program alarm action launches a script that starts a program or batch file on the server when an alarm is received.

To set a run external program action:

- Click , then click an item in the navigation tree, click the *Alarms* menu tab, then *Actions*.

**NOTE: When configured, the action applies to the designated item in the tree as well as its subordinate items.**

- Select the categories that contain the alarm sources to set up from the drop-down list, then select the alarm sources for the selected categories to link to the action.
- Select *Run External Program* from the drop-down, then click *Add*.
- Enter the path of the executable file to be run followed by the path of the output file. For example:

c:\windows\notepad.exe

c:\SiteScan Web\output1.txt

In the example, Notepad opens and a text file named *output1.txt* is created in the *SiteScan Web* program folder on the server's C: drive.

- Append Field Codes to the command line by choosing from the drop down list (see [Field code definitions](#) on page 27 for definitions). More than one field code may be chosen. For example:

```
c:\reports\run_report.bat $Generation_time$$To_State$
```

The example starts a batch file on the server and uses the alarm's generation time and state as values.

- Check the *Synchronize* box to force a delay until the external program has finished running before initiating the next Run External Program alarm action.
- By default, the action occurs when an alarm is detected and after the device returns to normal. To specify when to run the action:
  - Only when the device is *In Alarm* or after *Return to Normal*.
  - After a specified time if not *Returned to Normal* or not *Acknowledged*.\*
  - If a group with a specified schedule is *Occupied* (e.g., during work hours) or *Unoccupied*.\*

\*Available only with Advanced Alarming.
- Click *Accept* to save the action or *Cancel* to close without saving. The action appears in the Actions view.

#### 4.2.4 Send Alphanumeric Page on Alarm Action

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

**NOTE: Do not assign the Alphanumeric Page action to frequently-occurring alarms if you are using a stand-alone workstation. Sending pages for a frequently-occurring alarm may dramatically slow down your system and cause problems with your mail server.**

If the page will be sent over the Internet from a workstation that is not directly connected to the Internet, the workstation must first be configured to connect to the Internet automatically (see [Setting Up a Dial-Up Networking Connection](#) on the facing page).

To set a send page action:

- Click , then click an item in the navigation tree, click the *Alarms* menu tab, then *Actions*.

**NOTE: When configured, the action applies to the designated item in the tree as well as its subordinate items.**

- Select the categories that contain the alarm sources to set up from the drop-down list., then select the alarm sources for the selected categories to link to the action.
- Select *Send Alphanumeric Page* from the drop-down, then click *Add*.
- In *To*, enter the service provider's phone number in this format: 1 800-555-1212. Do not use parentheses around the area code. More than one recipient may be specified.
- In *From*, enter a valid address, if required by your mail server.
- In Subject, enter the subject of the notification.
- In Mail Host enter your Simple Main Transfer Protocol. This can be an IP address or a system name, such as *mail.mycompany.com*.
- If your mail server requires a user name and password, check *Specify Mail User*, and enter the *Mail User* and *Password*.
- If your mail server allows only MIME attachments., check *Send mail as MIME attachment*
- In the *Message Text* box, enter the message to appear in the page, using the appropriate punctuation, including spaces, and returns to separate lines of text.
- To add dynamic alarm data to the message, place the cursor in the message text, and select a code from the Append Field Code drop-down (see [Field code definitions](#) on page 27 for definitions).

12. By default, the action occurs when an alarm is detected and after the device returns to normal. To specify when to run the action:
  - Only when the device is *In Alarm* or after *Return to Normal*.
  - After a specified time if not *Returned to Normal* or not *Acknowledged*.\*
  - If a group with a specified schedule is *Occupied* (e.g., during work hours) or *Unoccupied*.\*

\*Available only with Advanced Alarming.
13. Click *Accept* to save the action or *Cancel* to close without saving. The action appears in the Actions view.

## Setting Up a Dial-Up Networking Connection

A dial-up networking connection is required if the page will be sent over the Internet from a workstation that is not directly-connected to the Internet. This enables SiteScan Web to dial out to send an e-mail or alphanumeric page. After creating and executing an alarm action, the modem should dial automatically, then hang up after 1 minute of inactivity.

1. Set-up your server and modem to dial the default connection to your Internet Service Provider. See your server and modem documentation.
2. Connect to the Internet and enter your Internet Service Provider's name and phone number, then your user name and password. Your modem must be detected before you can configure your Internet account connection.
3. Type the following line at the end of the **system.properties** file in your system directory:

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

### 4.2.5 Send E-Mail on Alarm Action

Use the Send E-Mail action to send customized e-mail messages to selected recipients when an alarm occurs.

Do not assign the Send E-Mail alarm action to frequently-occurring alarms if you are using a stand-alone workstation. Sending e-mails for a frequently-occurring alarm may dramatically slow down your system and cause problems with your mail server.

If the e-mail will be sent from a workstation that is not directly connected to the Internet, the workstation must first be configured to connect to the Internet automatically (see [Setting Up a Dial-Up Networking Connection](#) above).

To set an e-mail action:

1. Click , then click an item in the navigation tree, click the *Alarms* menu tab, then *Actions*.

**NOTE: When configured, the action applies to the designated item in the tree as well as its subordinate items.**

2. Select the categories that contain the alarm sources to set up from the drop-down list., then select the alarm sources for the selected categories to link to the action.
3. Select *Send E-mail* from the drop-down, then click *Add*.
4. In *To*, enter the recipient's e-mail address. More than one recipient may be specified.
5. In *From*, enter a valid address, if required by your mail server.
6. In Subject, enter the subject of the notification.
7. In Mail Host enter your Simple Main Transfer Protocol. This can be an IP address or a system name, such as *mail.mycompany.com*.
8. If your mail server requires a user name and password, check *Specify Mail User*, and enter the *Mail User* and *Password*.
9. If your mail server allows only MIME attachments., check *Send mail as MIME attachment*

10. In the *Message Text* box, enter the message to appear in the e-mail, using the appropriate punctuation, including spaces, and returns to separate lines of text.
11. To add dynamic alarm data to the message, place the cursor in the message text, and select a code from the Append Field Code drop-down (see [Field code definitions](#) on page 27 for definitions).
12. By default, the action occurs when an alarm is detected and after the device returns to normal. To specify when to run the action:
  - Only when the device is *In Alarm* or after *Return to Normal*.
  - After a specified time if not *Returned to Normal* or not *Acknowledged*.\*
  - If a group with a specified schedule is *Occupied* (e.g., during work hours) or *Unoccupied*.\*

\*Available only with Advanced Alarming.
13. Click *Accept* to save the action or *Cancel* to close without saving. The action appears in the Actions view.

#### 4.2.6 Send SNMP Trap on Alarm Action

The Send SNMP Trap alarm action sends an SNMP trap in response to receiving 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.

SiteScan Web supports SNMP v1.

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

To set a send SNMP trap action:

1. Click , then click an item in the navigation tree, click the *Alarms* menu tab, then *Actions*.

**NOTE: When configured, the action applies to the designated item in the tree as well as its subordinate items.**

2. Select the categories that contain the alarm sources to set up from the drop-down list., then select the alarm sources for the selected categories to link to the action.
3. Select *Send SNMP Trap* from the drop-down, then click *Add*.
4. Check *Enable*, and enter the SNMP server's network address community name in the appropriate boxes. Obtain this information from your network administrator.

**NOTE: Deleting the check mark from *Enable* removes the attendant address from the SNMP trap notification.**

- You can use *Comment (optional)* to note the location of the SNMP server.
5. In *Trap number*, enter a numeral from 1 to 127 to identify a message from this alarm action. Use this feature if trap numbers have been configured. Obtain this information from your network administrator. The same trap number is used for all messages from this alarm action.
  6. In the *Text to send as the SNMP Trap* box, enter the message using the appropriate punctuation, including spaces, and returns to separate lines of text.
  7. To add dynamic alarm data to the message, place the cursor in the message text, and select a code from the Append Field Code drop-down (see [Field code definitions](#) on page 27 for definitions).
  8. By default, the action occurs when an alarm is detected and after the device returns to normal. To specify when to run the action:
    - Only when the device is *In Alarm* or after *Return to Normal*.
    - After a specified time if not *Returned to Normal* or not *Acknowledged*.\*
    - If a group with a specified schedule is *Occupied* (e.g., during work hours) or *Unoccupied*.\*

\*Available only with Advanced Alarming.



9. Click *Accept* to save the action or *Cancel* to close without saving. The action appears in the Actions view.

#### 4.2.7 Write Property on Alarm Action

The **Write Property** alarm action updates a microblock property value.

To set a write property action:

1. Click , then click an item in the navigation tree, click the *Alarms* menu tab, then *Actions* .

**NOTE: When configured, the action applies to the designated item in the tree as well as its subordinate items.**

2. Select the categories that contain the alarm sources to set up from the drop-down list., then select the alarm sources for the selected categories to link to the action.
3. Select *Write Property* from the drop-down, then click *Add*.
4. In *Expression*, enter the microblock value to update.
5. In *Value to Write*, type the value to write to the microblock property. For a binary property, type *0* or *1*.
6. Select field codes from the drop-down list to add to the Value to Write field.
7. By default, the action occurs when an alarm is detected and after the device returns to normal. To specify when to run the action:
  - Only when the device is *In Alarm* or after *Return to Normal*.
  - After a specified time if not *Returned to Normal* or not *Acknowledged*.\*
  - If a group with a specified schedule is *Occupied* (e.g., during work hours) or *Unoccupied*.\*

\*Available only with Advanced Alarming.
8. Click *Accept* to save the action or *Cancel* to close without saving. The action appears in the Actions view.

#### 4.2.8 Write to Database on Alarm Action

The **Write to Database** alarm action stores alarm information in a table in the SiteScan Web 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 such actions as triggering a stored procedure or running a report.

To set a write to database action:

1. Click , then click an item in the navigation tree, click the *Alarms* menu tab, then *Actions* .

**NOTE: When configured, the action applies to the designated item in the tree as well as its subordinate items.**

2. Select the categories that contain the alarm sources to set up from the drop-down list., then select the alarm sources for the selected categories to link to the action.
3. Select *Write to Database* from the drop-down, then click *Add*.
4. Depending on the type of database, see [Writing to the Liebert SiteScan Web Alarm Database](#) on the next page, or [Writing to a Custom Database](#) on the next page

## Writing to the Liebert SiteScan Web Alarm Database

When you add the Write to Database alarm action, by default SiteScan Web writes alarm information to the *write\_db\_ra* table in the alarm database. The following table describes the information that SiteScan Web writes to the database and gives the column name and data type you need to access the alarm information from a third-party application.

DESCRIPTION	COLUMN NAME	DATA TYPE
Alarm generation time	EVENT_TIME_	Datestamp
Reference name 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 from the <i>Append Field Code</i> list (see <a href="#">Field code definitions</a> on page 27 for definitions).	RA_TEXT_	String

To keep the database table from growing too large, you must delete old entries using a third-party database application. You cannot view, edit or delete entries from SiteScan Web.

**NOTE: If your system uses an Access or MSDE database, you cannot open the database in a third-party application while Liebert SiteScan Web or SiteBuilder is running.**

## Writing to a Custom Database

SiteScan Web can write alarm information to the following types of custom databases. The custom database does not have to be the same type as the SiteScan Web 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 write to a custom database instead of to the SiteScan Web alarm database, check *Specify Custom Database*, and complete the fields required to write to the custom database described in [Custom Database fields](#) on the facing page.

**Table 4.4 Custom Database fields**

FIELD	NOTES
Text to write to the database	The text is made up of field codes that add live data to the text. You can select additional field codes from the Append Field Code list (see <a href="#">Field code definitions</a> on page 27 for definitions). <b>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.</b>
Database Connect String	<p>The connect string format is...</p> <p>jdbc:odbc:&lt;odbc_alias&gt;            jdbc:mysql://&lt;host&gt;:&lt;port&gt;/&lt;instance&gt;            jdbc:postgresql://&lt;host&gt;:&lt;port&gt;/&lt;instance&gt;            jdbc:oracle:thin@&lt;host&gt;:&lt;port&gt;/&lt;instance&gt;</p> <p>where:            &lt;host&gt; is the database server name/IP address            &lt;port&gt; is the port number for the database            &lt;instance&gt; is the database name in the database server            &lt;odbc_alias&gt; is the name of the ODBC data source</p>
Database Login and Password	The log in and password to connect to the database.
Database Insert String	<p>Use the following format:            Insert into &lt;TABLE_NAME&gt; (&lt;column1_name&gt;, &lt;column2_name&gt; ...) values (&lt;\$field_code1\$&gt;, &lt;\$field_code2\$&gt;, ...)</p> <p>Example:            Insert into SiteScan Web_ALARMS (TIME_, LOCATION_, TO_STATE_, TEXT_) values (\$generation_time\$, \$location_path\$, \$to_state\$, \$report_text\$)</p> <p><b>NOTE: You can add field codes to the Insert String using the Append Field Code list. See <a href="#">Field code definitions</a> on page 27.</b></p> <p>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 codes to format the time.</p>

### 4.2.9 Write to File on Alarm Action

The Write to File action allows you to record alarm information in a file.

To set a write to file action:

1. Click , then click an item in the navigation tree, click the *Alarms* menu tab, then *Actions*.

**NOTE: When configured, the action applies to the designated item in the tree as well as its subordinate items.**

2. Select the categories that contain the alarm sources to set up from the drop-down list, then select the alarm sources for the selected categories to link to the action.
3. Select *Write to File* from the drop-down, then click *Add*.
4. Enter a File Name, and select *Write to File* or *Write as Report*.
5. Click to check *Append* to add new entries at the end of the file.

**NOTE: If you do not check the Append box, the file contents will be overwritten with each new alarm message.**

6. In the *Text to write to the file* box, enter the message to appear in the pop-up window, using the appropriate punctuation, including spaces, and returns to separate lines of text.
7. To add dynamic alarm data to the message, place the cursor in the message text, and select a code from the Append Field Code drop-down (see [Field code definitions](#) on page 27 for definitions).

8. By default, the action occurs when an alarm is detected and after the device returns to normal. To specify when to run the action:
  - Only when the device is *In Alarm* or after *Return to Normal*.
  - After a specified time if not *Returned to Normal* or not *Acknowledged*.\*
  - If a group with a specified schedule is *Occupied* (e.g., during work hours) or *Unoccupied*.\*

\*Available only with Advanced Alarming.
9. Click *Accept* to save the action or *Cancel* to close without saving. The action appears in the Actions view.

### 4.3 Enable/Disable Alarms

The Enable/Disable tab allows you to customize the treatment of alarms and return-to-normal events for selected alarm sources. Through this function, you may:

- Activate or deactivate alarms and return-to-normal events
- Classify alarms as critical or non-critical
- Specify whether an operator must acknowledge alarms and return-to-normal events

To enable/disable alarm functions:


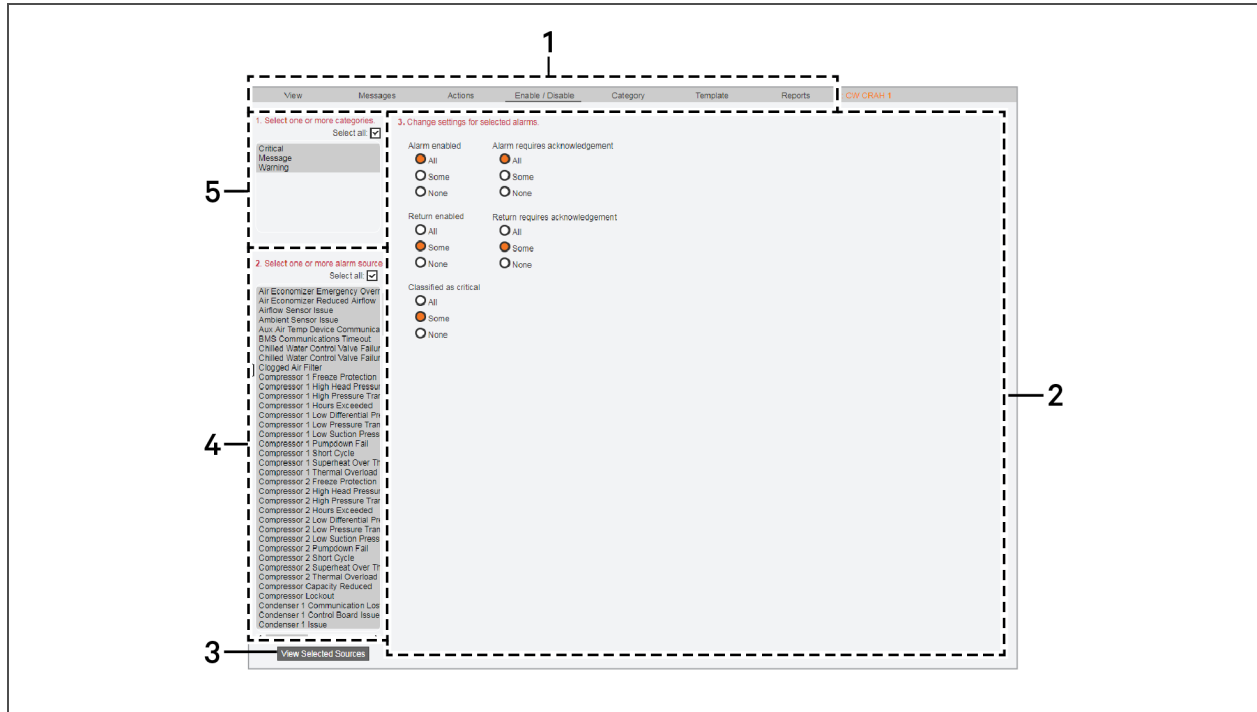
1. Click , then click an item in the navigation tree.
2. Click the *Alarms* menu tab, then *Enable/Disable*.

Figure 4.3 Alarm Enable/Disable tab



ITEM	DESCRIPTION
1	Alarm menu tabs.
2	Feature settings
3	View selected sources for access to advanced options. See <a href="#">Viewing Selected Sources</a> on the next page.
4	Alarm sources
5	Alarm categories.

3. Select the categories that contain the alarm sources with messages you want to edit.
4. Select the alarm sources for the selected categories.

**NOTE:** In steps [Select the categories that contain the alarm sources with messages you want to edit.](#) above and [Select the alarm sources for the selected categories.](#) above, control-click to select multiple items, or check the **Select All** box.

5. To change settings for the selected alarm sources, select *All*, *Some*, or *None* for each of the following:
  - Alarm enabled = generates an alarm when specified conditions occur in the alarm source.
  - Return enabled = generates a return-to-normal when the alarm source returns to a normal state.
  - Classified as critical = changes the system-wide alarm button to red when an alarm occurs. Critical alarms that pass through a modem are delivered to the SiteScan Web server immediately.


**NOTE: If the Classified as critical feature is disabled (None button selected), SiteScan Web changes the system-wide alarm button to yellow when an alarm occurs. Non-critical alarms that pass through a modem are stored in the gateway until a critical alarm occurs, the gateway is contacted by SiteScan Web, or the gateway buffer is full, at which time all alarms are sent to Liebert SiteScan Web.**

- Alarm requires acknowledgment = requires that an operator acknowledge the alarm.
  - Return requires acknowledgment = requires that an operator acknowledge the return-to-normal event.
6. Click *Accept* to save the changes or *Cancel* to close without saving.

### 4.3.1 Viewing Selected Sources

In the Enable/Disable tab, you may use the View Selected Sources button to view a listing of all selected alarm sources where you may enable or disable features for any source.

To access the selected sources:

1. Click , then click an item in the navigation tree.
2. Click the *Alarms* menu tab, then *Enable/Disable*.
3. Select the categories that contain the alarm sources you want to view.
4. Select the alarm sources for the selected categories.

**NOTE: In steps [Select the categories that contain the alarm sources you want to view.](#) above and [Select the alarm sources for the selected categories.](#) above, control-click to select multiple items, or check the **Select All** box.**

5. Click *View Selected Sources*.  
A dialog opens, listing all selected alarm sources with check boxes for enabled features. Use the scroll bar as needed to view additional sources.
  - You may click an alarm source to open a details window. The name of the alarm source appears to the right of the tabs.
6. To enable a feature, click to check the box. To disable a feature, click to remove the check mark.
7. Click *Accept* to save the changes or *Cancel* to close without saving.

## 4.4 Alarm Categories

The Category lets you customize alarm categories, which are groups of related alarm sources and their alarms.

Alarm categories let you perform tasks on groups of alarms, for example:

- View, acknowledge, or delete selected categories of alarms
- Assign alarm actions to selected categories of alarm sources
- Set up alarm sources in selected categories

Each alarm source is assigned to an alarm category, but you can change the category assignment in this window.

Liebert SiteScan Web has default alarm categories, but you can also create custom categories, if needed, using the Configuration view.

To access the category functions:


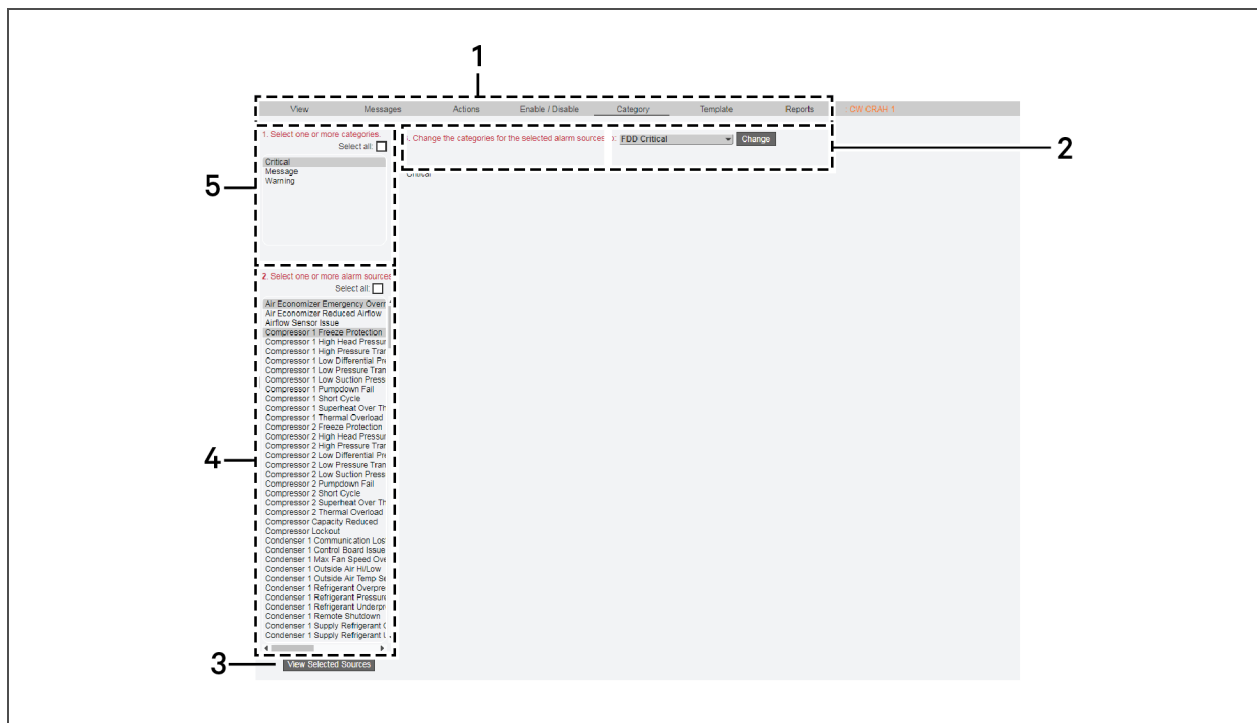
1. Click  then click an item in the navigation tree.
2. Click the *Alarms* menu tab, then *Category*.

Figure 4.4 Alarm Category tab



ITEM	DESCRIPTION
1	Alarm menu tabs.
2	Category options
3	View selected sources for further detail.
4	Alarm sources
5	Alarm categories

To change category assignments:

1. Select the categories that contain the alarm sources you want to customize.
2. Select the alarm sources for the selected categories.

**NOTE: In steps and , control-click to select multiple items, or check the **Select All** box.**

3. Select a category to assign the drop-down and click *Change*.
  - Use the *View Selected Sources* button to show the selected items, a link to a details about the source, and currently-assigned category.
4. Click *Accept* to save the changes or *Cancel* to close without saving.

## 4.5 Alarm Templates

All alarms in SiteScan Web v2.5 and later use one template called Universal. The template lets you define alarm message text, the critical setting, and the required acknowledgments at the alarm source.

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, we recommend 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 access the template functions:


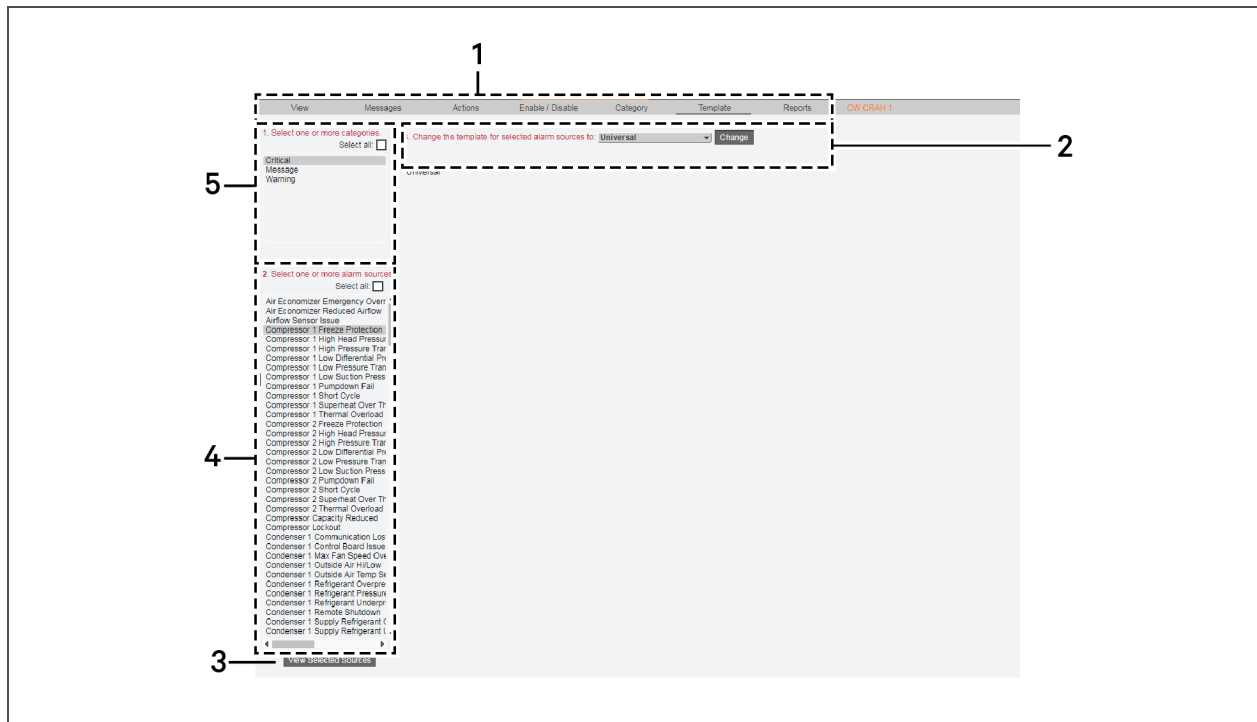
1. Click , then click an item in the navigation tree.
2. Click the *Alarms* menu tab, then *Template*.



Figure 4.5 Alarms Template tab



ITEM	DESCRIPTION
1	Alarm menu tabs.
2	Template options
3	View alarm sources for further detail.
4	Alarm sources
5	Alarm categories.

To change template assignments:

1. Select the categories that contain the alarm sources for which you want to change the template.
2. Select the alarm sources for the selected categories.

**NOTE:** In steps and , control-click to select multiple items, or check the **Select All** box.

3. Select a template to assign the drop-down and click *Change*.
  - Use the *View Selected Sources* button to show details about the source, and currently-assigned template.
4. Click *Accept* to save the changes or *Cancel* to close without saving.

## 4.6 Alarm Reports

The **Reports** tab in the Alarms window offers quick access to all alarm-related reports. These reports are also accessible from the **Reports** menu action button (see [Reports](#) on page 49).

To access the reports:


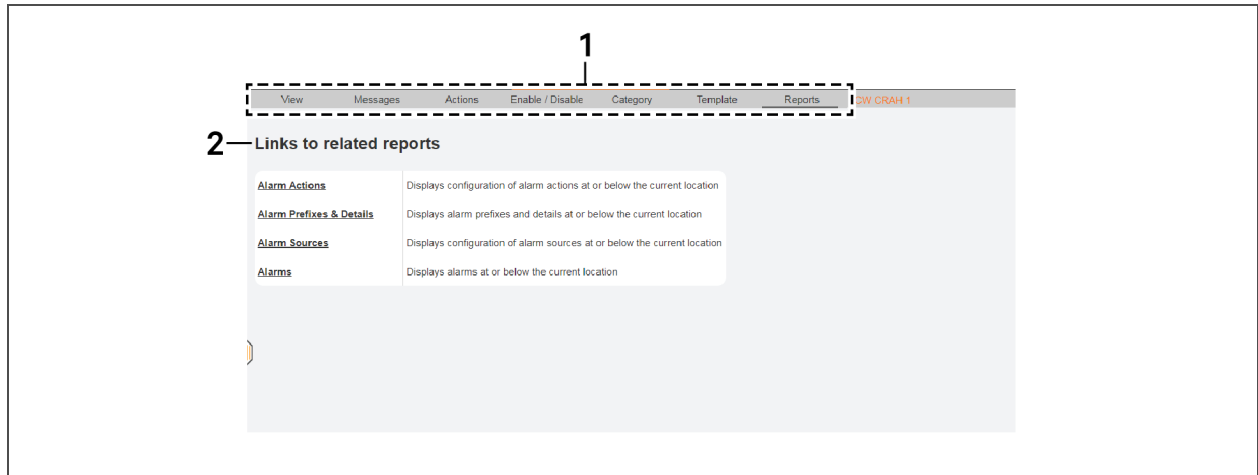
1. Click , then click an item in the navigation tree.
2. Click the *Alarms* menu tab, then *Reports*.
3. Click a link to the alarm-related report to view.  
The Reports menu-tab opens.
4. If needed, select the *View* tab, and click *Run* to generate the report.
  - To copy the report contents to a file, select a file type. See [Viewing Reports](#) on page 20, for more details.
  - To change the report settings, select the Options tab. See [Setting Report Options](#) on page 51, for more details.

Figure 4.6 Alarms Reports tab



ITEM	DESCRIPTION
1	Alarm menu tabs.
2	Links list

## 5 TRENDS

The Trends menu-tab in the geographic view offers quick access to alarm-related features, described in [Trends menu-tab options](#) below.

The Trends button allows you to create trend graphs that may be viewed, printed or copied to a spreadsheet program. SiteScan Web can read and store equipment status values over time and then display this information in a graph to help you monitor the equipment's operation.

Trend data can be collected for any BACnet input or output point. The control module reads values for a point at intervals that you define and then stores that data in the module.


Because a control module has limited memory for storing trend data, you can set up historical trending to archive the trend data from the module to the SiteScan Web database. A trend graph can display data from both the control module and the database.

**Table 5.1 Trends menu-tab options**

TAB	DESCRIPTION
View	Lets you review equipment status values over time to monitor the equipment's operation. See <a href="#">Viewing Trend Graphs</a> on page 18.
Configure	Lets you customize the graph including change the name and appearance, add and delete points, and change the data source. See <a href="#">Configuring Trend Graphs</a> below.

### 5.1 Create a New Trend Graph

To create a graph:

1. Click , then click an item in the navigation tree.
2. Click the drop-down arrow next to the *Trends* menu tab, and select *New Trend Graph*.
3. Select up to 16 items for the trend graph. Use **SHIFT**+click and **CTRL**+click to select multiple items.
4. Click *Save*, and enter a name (a reference name is created automatically), then click *OK*. The new graph is created.

### 5.2 Configuring Trend Graphs

Once a trend graph is saved, the **Configure** tab appears in the Trends window, allowing you to specify options for the graph, such as changing the name, changing the appearance, adding or deleting points or selecting a different data source.

To configure a trend graph:


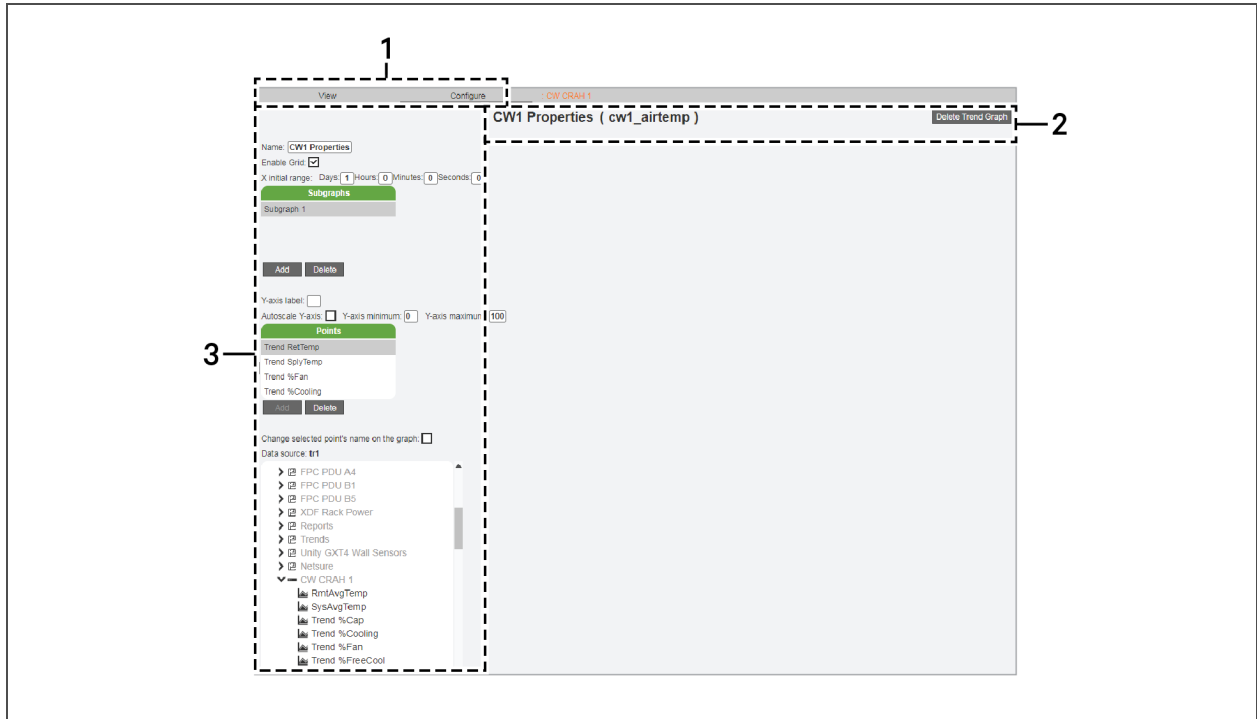
1. Click , then click an item in the navigation tree.
2. Click the *Trends* menu tab, then *Configure*.
3. Select and enter the graph options, then click *Accept* to save changes or *Cancel* discard.

Figure 5.1 Trends Configure tab



ITEM	DESCRIPTION
1	Trend menu tabs
2	Selected graph
3	Configuration options

## 6 REPORTS

The Reports menu-tab compiles alarm and other information to help manage and troubleshoot your system described in **Table 6.1** below.

**Table 6.1 Reports menu-tab options**

TAB	DESCRIPTION
View	Lets you compile alarm and other information to help manage and troubleshoot your system. See <a href="#">Viewing Reports</a> on page 20.
Configure	Lets you specify page size, orientation, maximum length, and other options depending on the type of report. See <a href="#">Setting Report Options</a> on page 51.
Design	Lets you create, customize, and manage reports including: <ul style="list-style-type: none"> <li>• Creating custom reports. See <a href="#">Setting-Up New Reports</a> on the next page.</li> <li>• Managing the standard, built-in reports. See <a href="#">Built-In Reports</a> on page 52.</li> <li>• Viewing the equipment check-out/commissioning status. See .</li> <li>• Viewing, sorting, and filtering alarms by equipment. See .</li> <li>• Viewing specific reports on equipment including locked points/values, network status, whether or not trends are tracked, and parameter configuration. See .</li> <li>• Viewing when and were changes were made to system and equipment. See .</li> <li>• Viewing equipment's network status and network communication.</li> </ul>

### PDF Report

To create a PDF that may be opened with Adobe Reader or Acrobat:

1. Click *PDF*.  
A program window displays the PDF.
2. Click *Save a Copy*, browse to the save location, enter a file name, and click *Save*.

### Excel Reports

To create a spreadsheet that may be opened with Microsoft Excel:

1. Click *XLS*, a browser opens with the Excel file to download.
2. Click the file and select *Save*, then browse to the save location, enter a file name, and click *Save*.


### CSV Reports

Make sure the CSV feature is enabled (see [Setting Report Options](#) on page 51).

To create a CSV file that may be opened with a spreadsheet program or text editor:

1. Click *CSV*.
2. Select *Save*, browse to the save location, enter a file name, and click *Save*.

### 6.1 Finding Reports

To find a custom report, look for the reports symbol,  on the geographic navigation tree. To edit the report, see [Setting Report Options](#) on page 51.

## 6.2 Setting-Up New Reports

In addition to the standard reports available from the Reports drop-down arrow, SiteScan Web provides three basic templates for report design:

- Equipment Summary
- Equipment Values\*
- Trend Samples\*

\*Available with the optional Advanced Reporting package

Once set up, reports appear on the drop-down list.

After creating a new report, the *Options* tab changes to the *Design* tab to make additional changes if needed.

To create a new report:


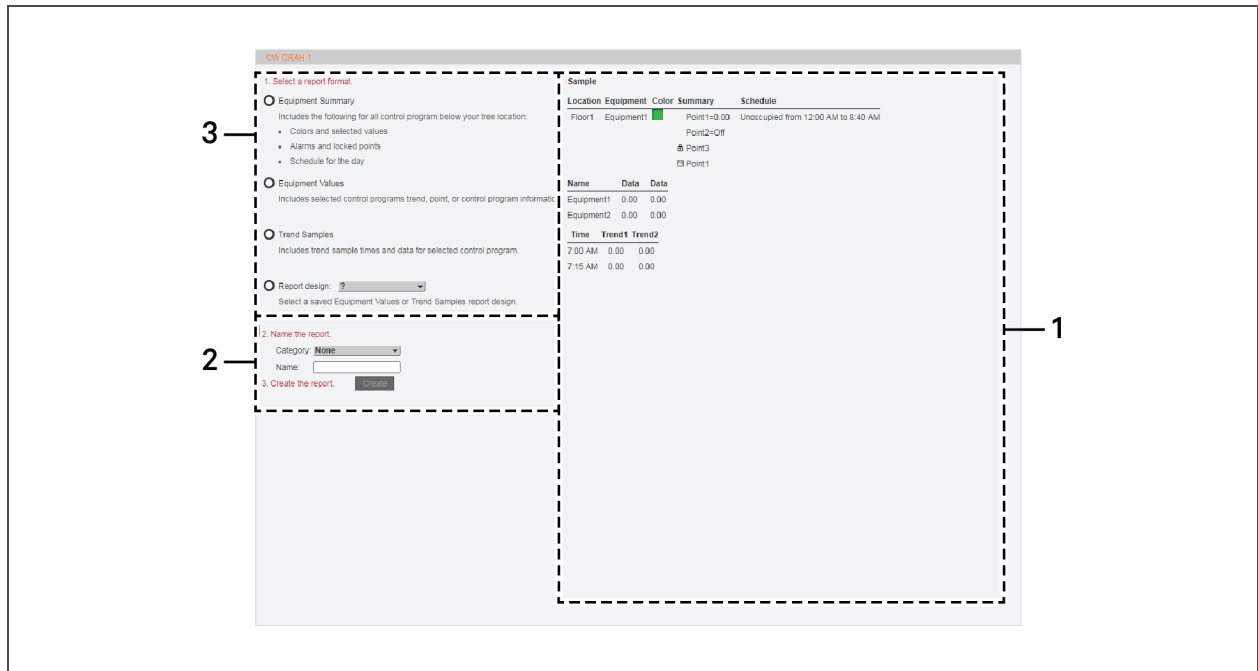
1. Click , then click an item in the navigation tree.
2. Click the *Reports* menu tab, then *New Report*.
3. Select a format, category, and name, then click *Create*.
4. Use the Options tab to customize the configuration and output. See [Setting Report Options](#) on the facing page.

Figure 6.1 New Report page




ITEM	DESCRIPTION
1	Layout example
2	Category and name
3	Format options

### 6.3 Setting Report Options

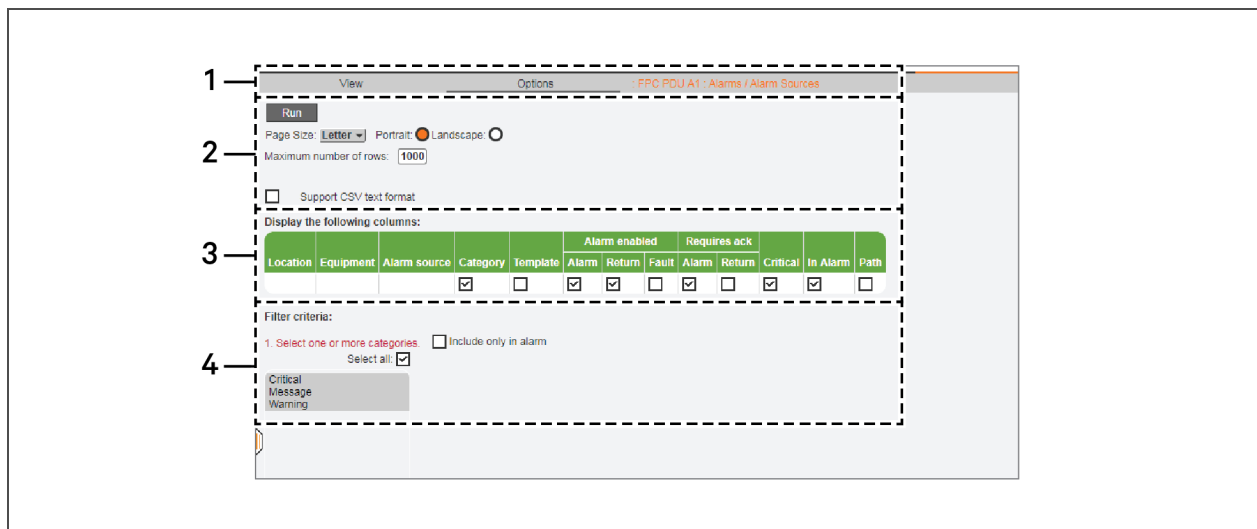
The Reports **Options** tab permits customizing reports. For all report types, you may specify page size, orientation and maximum length. Other options vary by type of report.

To configure a report:

1. Click , then click an item in the navigation tree.
2. Click the drop-down arrow next to the *Reports* menu tab, select a report, and then select *Options*.
3. Select the options, and click *Accept* to save the changes or *Cancel* to discard.

**NOTE:** You can *Run* a report at any time.

**Figure 6.2** Report Options page





ITEM	DESCRIPTION
1	Reports menu tabs
2	<p>Printing details.</p> <ul style="list-style-type: none"> <li>Specify the size of the page.</li> <li>Choose the page orientation, Portrait or Landscape.</li> <li>Specify the maximum number of rows to appear in the report—the default is 1000. This may help reduce the size of reports you expect to be excessively long. If the length is exceeded, a note at the end of the report saying “maximum number of rows exceeded. This may be resolved by either filtering the report results or increasing the maximum number of rows permitted.</li> <li>When checked, <i>Support CSV text format</i> permits using the report in many database programs. When enabled, the CSV Text button is activated in the View tab (see <a href="#">Viewing Reports</a> on page 20).</li> </ul>
3	<p>Content options (not available for all report types).</p> <ul style="list-style-type: none"> <li>Sort the report data by available criteria.</li> <li>Select the columns to include in the report. When an item is grayed-out the selection cannot be changed.</li> </ul>
4	Filtering options. (vary by report type).

## 6.4 Adjusting Report Layout


Clicking on the Design tab permits filtering the information displayed in a report. This can be used to limit the size of the report and its layout.

To adjust the page, rows, and columns for a report:

1. Click , then click  next to an item in the navigation tree.
2. On the *Reports* menu tab, click *Design*.
3. Use the Page, Rows, and Columns sections to customize the layout of the generated report.

## 6.5 Built-In Reports

Standard reports appear throughout the system, though their function changes depending on where in the geographic-view tree or network-view tree the report is run. If a report is run on a single unit in the geographic-view tree, the report will contain results from only that unit. Moving up to an area and running a report that will yield results from all the units in that area. A report run at the root of the system will contain results from the entire system.


**NOTE:** These built-in reports are not marked with the  symbol.

To view built-in reports:

Click the drop-down arrow next to the Reports menu tab, and select the report. [Built-in Reports](#) below, describes the groups of built-in reports and the specific reports for those groups.

You can adjust the report layout before you run them, see [Adjusting the Layout of Built-in Reports](#) on the facing page, for more details.

**Table 6.2 Built-in Reports**

REPORTS GROUP	REPORT	DESCRIPTION
Security	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 in the configuration-view navigation tree, login/logout, and scheduled processes like deleting expired trends <b>NOTE: the Reason field will be empty unless system is configured to require operator notes when making changes. Contact Vertiv™ technical support to enable this feature.</b>
Alarms	Alarm Actions	Create a summary of the information configured on the Alarms > Actions tab. Also useful to find where these are configured in the system, just run this report in the root of the geographic-view navigation tree. Additionally, if you are looking for where an alarm action is defined, look for  in the geographic-view navigation tree.
	Alarm Prefixes and Details	Create a summary of the information configured on the Alarms > Messages tab. To determine where these are configured in the system, run this report in the root of the geographic-view navigation tree.
	Alarm Sources	Create a summary of potential alarms. The list will help familiarize operators with the equipment by listing all the alarms a piece of equipment might generate.
	Alarms	Create a summary of all alarms.
Schedules	Effective Schedules	Create a summary of control programs using a schedule.
	Schedule Instances	Create a summary of all schedules.




**Table 6.2 Built-in Reports (continued)**

REPORTS GROUP	REPORT	DESCRIPTION
Equipment	Locked Values	Find all locked points and locked values. A common way to test alarms is to lock a point to an alarm condition, you can verify if they are cleared and will respond normally with this report. It is very rare to have a normal situation where a point is locked all the time.
	Network IO	Verify the programming and status of all network points. Especially useful for verifying if third-party integration points are reading with no errors. If you get a loss-of-communication alarm from a third party device, this report can help you determine what the trouble is. Detailed information on point-read errors is generally located in the control module under driver, protocols, error definitions. When you are looking at equipment on the geographic-view navigation tree, and you need to quickly get to the control module it is in, run manual command go -net and the system takes you to that equipment on the network-view navigation tree.
	Parameter Mismatch	Discover where your system has parameter mismatch between the database and the field controllers that need to be resolved. Contact Vertiv™ technical support if you have persistent problems with parameter mismatches.
	Point List	Find all points for selected equipment.
	Trend Usage	Creates a summary of the information configured on the Trends > Enable/Disable tab.
Commissioning	Equipment Checkout	View the information on the Equipment Checkout tab of the equipment's Properties page. Also, find equipment that has not been fully commissioned. Not all installing technicians use these reports, if they are blank, ask the technician for their commissioning notes.
Network (Only when network navigation tree is selected)	Controller Status	Discover network communication problems (shown as purple squares on the report) that need troubleshooting. The report also shows the boot and driver version, download information, and whether the controller has 4.x or later driver. The report shows the serial number and Local Access port status. The Controller Status is helpful when dead module alarms are generated and SiteScan Web SiteScan control module communication on the network must be verified.
	Equipment Status	Display the unit alarm color, status, and prime variable of each control program. It is normal for SiteScan Web to not utilize the prime variable.

### 6.5.1 Adjusting the Layout of Built-in Reports

The Options tab for a built-in report lets you filter the information displayed in the report. Use these options to limit the size of the report and its layout.

To adjust the layout of a built-in report:

1. Click , then click the drop-down arrow next to the *Reports* menu tab, and select a built-in report.
2. Click *Options*, and use the options to customize the layout of the generated report.

This page intentionally left blank

## 7 USING THE CONFIGURATION VIEW

Most of the configuration for SiteScan Web is performed by Vertiv™. This section provides instructions on how to change the most-commonly-used configuration settings.

When you select the configuration view, the menus described in [Configuration View menus and options](#) below, are offered.

**Table 7.1 Configuration View menus and options**

NAVIGATION TREE OPTION	VIEW TAB OPTIONS
My Settings	Lets the logged-in user configure personal options and information. See <a href="#">My Settings Configuration</a> below.
System Settings	Lets you view and in some cases, configure general SiteScan Web options and daylight saving options. See <a href="#">System Settings Configuration</a> on page 57
Operators	Lets you set up SiteScan Web users. See <a href="#">Configuring Operators</a> on page 58.
Privilege Sets	Lets you set up and assign access and use SiteScan Web options to individual operators or groups. See <a href="#">Configuring Privilege Sets</a> on page 59.
Operator Groups	Lets you group operators to simplify assigning access privileges and setting up message-notification recipients. See <a href="#">Configuring Operator Groups</a> on page 59.
Services	Lets you view a list of services used by SiteScan Web and the status of each. See <a href="#">Services Status</a> on page 62.
Trends Display Setup	Lets you customize the color and other display options of the trend graphs. See <a href="#">Configuring the Trends Display Setup</a> on page 62.
Trends Print Setup	Lets you specify the appearance of printed trend graphs. See <a href="#">Configuring Trends Print Setup</a> on page 63.

### 7.1 My Settings Configuration


My Settings configures passwords, start-up views, and other preferences that apply to the currently logged-in user, described in [My Settings tab options](#) below.

**Table 7.2 My Settings tab options**

TAB	DESCRIPTION
Settings	Lets the logged-in user configure a password and other preferences. See <a href="#">Configuring User Settings</a> below.
Contact Info	Lets the logged-in user add contact information for notifications. See <a href="#">Configuring User Contact Info</a> on the next page.

#### 7.1.1 Configuring User Settings

To access the user settings:

1. Click , then click *My Settings* in the navigation tree.
2. Click the *Settings* tab, then refer to the following to adjust your personal settings:
  - [Changing Your Password](#) on the next page
  - [Changing Your Starting Location](#) on the next page
  - [Changing Your Preferences](#) on the next page

## Changing Your Password

To change the log-in password:

1. In the *Login* section, click to check *Change Password*.
2. Enter the existing password in *Current Password*.
3. Enter the new password in *New Password* (case-sensitive).
4. Confirm the new password by re-entering in *Retype New Password*.
5. Click *Accept* to save the change, or *Cancel* to close without saving.

## Changing Your Starting Location

To specify the opening view for SiteScan Web after you log in:

1. Select the following in the Login section:
  - In *Starting Location*, select the view button for the view you want at start-up.
  - After selecting the view, you can select to open a specific item in that view's navigation tree, click the arrow to expand an item.
  - In *Starting Page*, select the menu tab to be active at start-up.
2. Click *Accept* to save the change, or *Cancel* to close without saving.


## Changing Your Preferences

To specify you personal preferences:

1. In *Preferences*:
  - Select a language for the user interface. To set up your system for a language other than English, see the Help file for detailed procedures.
  - Select whether or not to automatically collapse the navigation trees, to expand one branch at a time.
  - Select whether or not to automatically download schedules after each change.
  - Specify whether or not to play a sound with alarm notifications, and select the sound file to play (with the extension .au or .wav).
  - In *Starting Page*, select the menu tab to be active at start-up.
2. Click *Accept* to save the change, or *Cancel* to close without saving.

### 7.1.2 Configuring User Contact Info

To configure you contact information:

1. Click , then click *My Settings* in the navigation tree.
2. Click the *Contact Info* tab, and enter your contact information in the appropriate fields.
3. Click *Accept* to save the change, or *Cancel* to close without saving.

## 7.2 System Settings Configuration


System Settings configures general SiteScan Web options and daylight saving options, described in [System Settings tab options](#) below.

**Table 7.3 System Settings tab options**

TAB	DESCRIPTION
General	Lets you view system settings and, in some cases, adjust the settings such as time/data and frequency of log reports. See <a href="#">Configuring General System Settings</a> below.
Daylight Saving	Lets you configure daylight-saving time settings for the system. See <a href="#">Configuring Daylight Saving Settings</a> below.

### 7.2.1 Configuring General System Settings

To access the system settings:

1. Click , then click *System Settings* in the navigation tree.
2. Click the *General* tab, then refer to the following to adjust the settings:

**NOTE: The General tab displays several items that are not editable: System Directory Name, Current System Time, Path to the Web Root Directory, Database Type, System Language**

- Choose the Time Format.
- Choose the Date Format.
- Select the number of levels displayed in paths.

For example, if this value is set at 2, a typical path might be `.\First Floor\AHU`.


If set at 3, a typical path might be `..\Atlanta R&D\First Floor\AHU`

**NOTE: This change does not take effect until you restart the SiteScan Web server.**

- Select whether or not to use a single alarm template for CMnet alarms (applies to upgraded legacy systems). Check to use the *alert\_auto alarm* template only, or leave unchecked to allow multiple alarm templates.
  - Use *Logs* to download a zip file containing logs of system activity for a specified week. Choose a beginning date, then click *Download*.
3. Click *Accept* to save the change, or *Cancel* to close without saving.

### 7.2.2 Configuring Daylight Saving Settings

To configure daylight-saving settings:

1. Click , then click *System Settings* in the navigation tree.
2. Click the *Daylight saving* tab, then refer to the following to adjust the settings:
  - *Offset for Daylight Saving* time should be *1 hour* (HH:MM).
  - *Daylight Saving Start Time* is typically 2:00 a.m. (HH:MM:SS).
  - *Daylight Saving Dates* should have Begin and End dates for each year.
3. Click *Accept* to save the change, or *Cancel* to close without saving.

## 7.3 Configuring Operators


The Administrator may set up users, defined as Operators in SiteScan Web, with customized access privileges. These operators may also be designated as recipients of alarm messages, as described in [Alarm Actions](#) on page 30.

**NOTE: SiteScan Web has a default Administrator operator. For security, either assign a password to this operator or delete it after assigning Admin privileges to another operator.**

**IMPORTANT! With hierarchical servers, you must create identical operators on each server.**

You can assign users to Operator Groups to simplify the process of assigning access privileges and setting up recipients for alarm messages, as described in [Configuring Operator Groups](#) on the facing page.

To add, edit or delete operators and assign access privileges:

1. Click , then click *Operators* in the navigation tree.
2. Click *Add* to create a new user or click an existing user in the *Operators* list. The operator's data appears to the right of the list.
3. To remove an existing operator, click *Delete*.
4. When adding an operator, complete *Login* section:
  - Enter a *Name* that will appear in lists in SiteScan Web.
  - Enter a *Login Name* for the operator to enter when logging in. This name must be unique within the system.
  - To assign a new password, check *Change password*, then refer to [Configuring User Settings](#) on page 55.
  - To prompt an operator to create a password, check *Force user to change password at log in*. Be sure to assign a temporary password.
  - Specify whether or not to use automatic log-off for the operator: after 15 minutes of inactivity, a different time (up to 500 hours maximum) or not at all.
5. Complete the Personal Information for this user (see [Configuring User Contact Info](#) on page 56 for details).
6. Specify the *Starting Location* when the operator logs in (see [Configuring User Settings](#) on page 55, for details).
7. In the *Privilege* section:
  - Check the appropriate boxes under *System-Wide Privilege Sets* assign access privileges to the operator (see [Configuring Privilege Sets](#) on the facing page to add or edit privileges).
  - Check the appropriate boxes under *Groups* assign the operator to groups (see [Configuring Operator Groups](#) on the facing page). The operator will have the same privileges as the group.

**NOTE: To hide items not assigned to this user, check *Show current privileges only*. A grayed-out privilege set indicates that it was assigned to the operator through a group listed next to the privilege—for example, *Admin From Reps*.**


8. Click *Accept* to save the change, or *Cancel* to close without saving.

### 7.3.1 Configuring Operator Groups

Operators may be assigned to Groups to simplify the process of assigning access privileges and setting up recipients for alarm messages. This step requires that individual operators have been created, as described in [Configuring Operators](#) on the previous page.


**NOTE: SiteScan Web has a permanent default group called *Everybody* that automatically includes all operators as members. You may assign privilege sets to this default group.**

To create or edit a group:

1. Click , then click *Operator Groups* in the navigation tree.
2. Click *Add* to create a group or click an existing group in the *Name* list. The group's data appears to the right of the list.
3. To remove an existing group, click *Delete*.
4. When adding a group:
  - In *Display Name*, enter a name that will appear in lists in SiteScan Web.
  - Enter a *Reference Name*. The reference name must consist of alphanumeric and underscore characters only and may not begin with a numeral.
  - In *Members*, check the *Operators* to add to the group. You may also add other groups by checking boxes under *Groups*.
5. Check the appropriate boxes under *Privilege Sets* assign access privileges to the group (see [Configuring Privilege Sets](#) below to add or edit privileges).
6. Click *Accept* to save the change, or *Cancel* to close without saving.

### 7.3.2 Configuring Privilege Sets

To create or edit privilege set:

1. Click , then click *Privilege Set* in the navigation tree.
2. Click *Add* to create a set or click an existing set in the list. The set's data appears to the right of the list.
3. To remove an existing privilege set, click *Delete*.
4. Choose the type of privilege set.
  - System-wide = Privileges include access and functional privileges. System-wide sets may be assigned to other operators (see [Configuring Operators](#) on the previous page) and operator groups (see [Configuring Operator Groups](#) above).
  - Local = Privileges include access, parameter, and functional privileges.

**NOTE: Once a privilege set is created, the only way to change the type is to delete the set and create a new one.**

5. Enter a *Name* that will appear in lists in SiteScan Web.
6. Enter a *Reference Name*. The reference name must consist of alphanumeric and underscore characters only and may not begin with a numeral.
7. Check each privilege to include in this privilege set. See [Privilege descriptions](#) on the next page, for a description of available privileges.
8. Click *Accept* to save the change, or *Cancel* to close without saving.

**Table 7.4 Privilege descriptions**

PRIVILEGE	DESCRIPTION
Access Privileges	Operators may access (but not edit):
Access Geographic Locations	Pages from the geographic-view tree.
Access Network Items	Pages from the network-view tree.
Access Groups	Pages from the schedule-groups view tree.
Access Config Items	Pages from the configuration view 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. <b>Note:</b> These categories may be used to create 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 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.
<b>Parameter Privileges. Operators may edit properties such as:</b>	
Edit Setpoint Parameters	Occupied and unoccupied heating and cooling setpoints.
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 Device Parameters	Module driver properties.
Edit Critical Configuration	Critical properties the installer protected with this privilege.
Edit Area Name	Area display names.
Edit Equipment Name	Equipment 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 SiteScan 2000.
<b>Functional Privileges. Operators may:</b>	
Manage Alarm Messages and Actions	Add, edit and delete alarm messages and actions.
Maintain System Parameters	Edit all properties on the System Settings page.



**Table 7.4 Privilege descriptions (continued)**

PRIVILEGE	DESCRIPTION
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 Trends Display and Print Setup	Edit Trends Display Setup and Trends Print Setup on the configuration-view tree.
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 Audit Log Report.
Download Devices	Mark equipment for download and initiate a download.
System Shutdown	Issue the Shutdown manual command that shuts down Liebert SiteScan Web Server.
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 Liebert SiteScan Web. Add text in the Notes field on an equipment's Properties page.
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 data through an Enterprise Data Exchange (SOAP) application.
Do not audit changes made using SOAP (Web services)	Not have SOAP (Web services) changes recorded in the Audit Log.
Manual Commands/Console Operations	Access the manual command dialog box and issue basic manual commands.

**Table 7.4 Privilege descriptions (continued)**

PRIVILEGE	DESCRIPTION
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.

## 7.4 Services Status

The Services window displays all current services for SiteScan Web and the status of each.

To view services:

Click , then click *services* in the navigation tree.


## 7.5 Configuring Client Installs

Client Install is used to install the Java Virtual Machine on the current connected workstation. Install only if required.

Wafer Font is used to display specific text in the SiteScan Web session. Install only if required.

Alarm Pop Application is a thin application that can be used by a client to receive alarm notifications to a workstation outside of the SiteScan Web browser.


To download a client install:

1. Click , then click *Client Install* in the navigation tree.
2. Click a link to download:
  - *Sun's Java VM*: Java Virtual Machine plug-in for Internet Explorer applets.
  - *Wafer font*: Wafer font for use with logic pages. (Place in your Windows install directory/fonts folder.)
  - *Alarm Popup Application*: Stand-alone client application that receives Alarm Popup action messages.
  - *HTTP proxy tool*: Engineering tool to tunnel web pages across BACnet (through RNet or access port).

## 7.6 Configuring the Trends Display Setup

The Trends Display Setup options allow you to specify the appearance of graphs on the screen.


To configure trend display:

1. Click , then click *Trend Display Setup* in the navigation tree.
2. In the *Trend Colors* section, choose options to specify colors for all graphs for the background, grid and axis, as well as text portions: labels for x-axis and y-axis labels, the main title and the y-axis title.
3. You may set up display options for up to four types of graphs, including line style and color and marker color and type.

## 7.7 Configuring Trends Print Setup

The Trends Print Setup options allow you to specify the appearance of printed graphs.

To configure printed trend graphs:

1. Click , then click *Trend Print Setup* in the navigation tree.
2. In the *Trend Colors* section, choose options to specify colors for all graphs for the background, grid and axis, as well as text portions: labels for x-axis and y-axis labels, the main title and the y-axis title.
3. You may set up display options for up to four types of graphs, including line style and color and marker color and type.

## 7.8 Changing Unit Bezel Colors

1. On the top-level floor plan in the geographic-view navigation tree, click the drop-down arrow next to the *Graphics* menu-tab, and select *Bezel Color Scheme*.
2. The *Unit/System* drop-down offers several color schemes and *Custom*. To change colors, select either an option from the list.
  - Selecting a color from *Unit/System*, applies a color scheme based on that color to the table header, bezel background, and table background.
  - Selecting **Custom** lets you set different colors for each of the bezel elements. If the color you want is not available, select *New* in the element drop-down to open a color wheel and set the color.

## 7.9 Event Color Scheme

**NOTE: Alarm colors are a System setting. Changing a System setting, such as alarm colors, will affect all users. If any user changes the event color scheme it will overwrite the previous setting.**

**NOTE: Alarm colors can only be changed by an operator with administrative privileges. Changing the event color scheme may also require downloading a module.**

To change the alarm colors:

1. On the top level floor plan in the geographic-view navigation tree, click the drop-down arrow next to the *Graphics* menu-tab, and select *Event Color Scheme*.
2. In *Event Selection*, select *Custom* and select a color under each of the event types to change:
  - Critical Color
  - Warning Color
  - Message Color
  - Maintenance Color
  - Normal Color
3. Click *Save Event Color*, and click *OK* each time a confirmation pops up to make the changes. Making the color change may take more than two minutes, depending on the size of the system.

**NOTE: If the event color scheme does not take effect, a module download may be required. Contact your IT department to download the module.**

This page intentionally left blank

## APPENDICES

### Appendix A: Technical Support

For help on setting up Liebert® SiteScan Web or any other monitoring product, contact Vertiv™ Technical Support at:

UNITED STATES	1 800 222 5877
FRANCE	+33 (0) 1 46 87 51 52
GERMANY	+49 (0) 89 99 19 220
ITALY	+39 (0) 2 98250 324
NETHERLANDS	+31 (0) 475 503333
UNITED KINGDOM	+44 1628403200
EUROPE	+800 11554499
ASIA	+800 11554499
AUSTRALIA	1 800 147704
NEW ZEALAND	0 800 447415 1 614 841 6755
WORLDWIDE	FAX: 1 740 833 8631 <a href="http://www.VertivCo.com/en-us/support/">http://www.VertivCo.com/en-us/support/</a>

This page intentionally left blank





---

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

© 2018 Vertiv Co. All rights reserved. Vertiv and the Vertiv logo are trademarks or registered trademarks of Vertiv Co. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness herein, Vertiv Co. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications are subject to change without notice.

SL-27050\_REV6\_10-18/590-1626-501B