M211975EN-A

User Guide

Vaisala viewLinc Enterprise Server

Version 5.0

VAISALA

PUBLISHED BY

Vaisala Oyj
Street address: Vanha Nurmijärventie 21, FI-01670 Vantaa, Finland
Mailing address: P.O. Box 26, FI-00421 Helsinki, Finland
Phone: +358 9 89491
Visit our Internet pages at www.vaisala.com.

© Vaisala 2018

No part of this manual may be reproduced, published or publicly displayed in any form or by any means, electronic or mechanical (including photocopying), nor may its contents be modified, translated, adapted, sold or disclosed to a third party without prior written permission of the copyright holder. Translated manuals and translated portions of multilingual documents are based on the original English versions. In ambiguous cases, the English versions are applicable, not the translations.
The contents of this manual are subject to change without prior notice.
Local rules and regulations may vary and they shall take precedence over the information contained in this manual. Vaisala makes no representations on this manual's compliance with the local rules and regulations applicable at any given time, and hereby disclaims any and all responsibilities related thereto.
This manual does not create any legally binding obligations for Vaisala towards customers or end users. All legally binding obligations and agreements are included exclusively in the applicable supply contract or the General Conditions of Sale and General Conditions of Service of Vaisala.
This product contains software developed by Vaisala. Use of the software is governed by license terms and conditions included in the applicable supply contract or, in the absence of separate license terms and conditions, by the General License Conditions of Vaisala Group.
This product may contain open source software (OSS) components. In the event this product contains OSS components, then such OSS is governed by the terms and conditions of the applicable OSS licenses, and you are bound by the terms and conditions of such licenses in connection with your use and distribution of the OSS in this product. Applicable OSS licenses are included in the product itself or provided to you included in the product itself or provided to you on any other applicable media, depending on each individual product and the product items delivered to you.

Table of Contents

1. Product Overview **1**
1.1 Vaisala viewLinc Enterprise Server 1
1.2 How Does viewLinc Work? 1
1.2.1 Hardware Requirements 1
1.2.2 Server Requirements 2
1.2.4 End User PC and Remote Display Requirements 3
1.2.5 Default Application File Locations 3
1.3 What's New 4
1.3.1 What's New for Upgrade Users 5
1.3.2 Watch a Tour 8
1.4 Device Connection Options 9
1.4.1 Ways to Connect Hardware 9
1.4.2 Using Wireless Devices 11
1.4.3 Using vNet Devices 12
1.4.4 Using Single or Multi-Port Ethernet Device Connectors 12
1.4.5 Using USB Ports 13
1.4.6 Using Serial Ports 13
1.5 About the viewLinc User Guide 13
1.5.1 How this Manual is Organized 14
1.5.2 Conventions Used in this Document 14
1.5.3 Related User Documentation 14
1.5.4 Contact Us 15
1.5.5 Need Training? 15
2. Setup and Installation **17**
2.1 Setup Checklist 17
2.2 viewLinc Enterprise Server Configuration 18
2.3 Plan your viewLinc Configuration 19
2.4 Install viewLinc 22
2.4.1 Installing viewLinc 22
2.4.2 Installing viewLinc on a Device Host Server 23
2.4.3 Installing viewLinc as an Upgrade 24
2.5 Log in to viewLinc 25
2.6 System Test 26
2.7 Validate your System 27
3. Device Management **29**
3.1 Device Hosts 29
3.1.1 Adding Server Hosts 29
3.1.2 Adding Access Point Hosts 30
3.2 Ways to Add Devices 31
3.2.1 Discovering Networked Devices 31
3.2.2 Accepting Wireless Devices 31

3.2.3 Adding Devices Manually 32
3.2.4 Adding Multiple Device Types 34
3.3 Configure Hosts and Devices 34
3.3.1 Viewing Host and Device Properties 35
3.3.2 Editing Host Properties 38
3.3.3 Editing Device Properties 39
3.3.4 Editing Channel Properties 42
4. Sites Management 45
4.1 Zones and Locations 45
4.2 Create Zones and Locations 46
4.2.1 Creating Zones 46
4.2.2 Creating Locations 47
4.3 Link Device Channels to Locations 47
4.3.1 Linking Channels to Locations 48
4.3.2 Creating Linked Locations Automatically 49
4.3.3 Viewing Channel Link History 49
4.3.4 Finding Linked Channels/Linked Locations 50
4.4 Build Dashboards 52
4.4.1 Building Dashboards 52
4.4.2 Changing Dashboard Display Settings 53
4.4.3 Deleting Dashboard Images or Data Points 55
5. Groups and Users 57
5.1 Rights 57
5.2 Groups 59
5.2.1 Adding Groups 59
5.3 Users 59
5.3.1 Adding Users 59
6. Alarm Templates 63
6.1 Types of Alarms 64
6.2 System Alarms 65
6.3 Threshold Alarms 65
6.3.1 Creating Threshold Alarm Templates 66
6.3.2 Applying Threshold Alarm Templates to Locations 68
6.3.3 Editing Threshold Alarm Templates 69
6.3.4 Editing Location Threshold Alarm Settings 70
6.3.5 Deactivating/Reactivating Threshold Alarms 70
6.4 Device Alarms 71
6.4.1 Types of Device Alarms 71
6.4.2 Host Communication Alarm Settings 73
6.4.3 Host Configuration Alarm Settings 74
6.4.4 Creating Device Alarm Templates 75
6.4.5 Applying Device Alarm Templates 76
6.4.6 Editing Device Alarm Templates 78

6.4.7 Editing Location Device Alarm Settings ... 78
6.5 Alarm Notifications ... 79
6.5.1 Creating Alarm Notification Templates ... 80
6.5.2 Applying Alarm Notification Templates ... 82
6.5.3 Editing Alarm Notification Templates ... 84
6.6 Email and SMS Content ... 85
6.6.1 Creating Custom Email or SMS Content ... 85
7. System Preferences ... 87
7.1 General Preferences ... 87
7.2 Remote Acknowledgement ... 88
7.3 Schedules Functionality ... 89
7.4 Audible Alarming ... 89
7.5 Temperature Measurement Units ... 90
7.6 MKT Activation Energy ... 90
7.7 Device or Channel Alias ... 91
7.8 Device Calibration Duration ... 91
7.9 Timebase Synchronization ... 92
7.10 viewLinc Aware ... 92
7.11 License Key ... 93
7.12 Authenticate System Changes ... 93
7.13 Technical Support Logs ... 93
7.14 Language Preferences ... 94
7.15 Unit Display Preferences ... 95
7.16 Email and SMS Settings ... 96
7.16.1 Setting Up Email Server Preferences ... 96
7.16.2 Setting Up SMS Modem Preferences ... 97
7.17 System Alarm Preferences ... 97
7.18 Comments ... 98
7.18.1 Adding Predefined Comments ... 99
8. Additional Setup Tasks ... 101
8.1 Permissions ... 101
8.1.1 Permission Levels ... 103
8.1.2 Applying Group Permission to Zones ... 103
8.1.3 Using Permissions Viewer ... 104
8.2 Schedules ... 105
8.2.1 Creating Schedules ... 105
8.2.2 Setting Threshold Alarm Schedules ... 107
8.2.3 Adding User Schedules ... 107
8.3 Views ... 108
8.3.1 Your Views ... 108
8.3.2 Creating Views ... 109
8.3.3 Sharing Views ... 110
8.3.4 Choosing a Default View ... 110
8.3.5 Creating Views for Remote Display ... 110

8.4 Access viewLinc via Remote Display or Mobile Device 111
8.4.1 Remote Display Requirements 111
8.4.2 Setting up a Remote Display 112
8.4.3 Using viewLinc Mobile 112
9. Daily Tasks 115
9.1 Desktop Orientation 115
9.1.2 Search for Zones and Locations 117
9.1.3 Working with Columns 118
9.2 Monitor Conditions 119
9.2.1 Identifying Active Alarms 120
9.2.2 Sites or Overview Window: Status Tab 120
9.2.3 How does viewLinc identify threshold alarms? 121
9.2.4 What Happens When an Alarm is Triggered? 122
9.2.5 Viewing Conditions on Dashboards 122
9.2.6 Viewing Dashboard Location Trends 123
9.2.7 Finding Linked Dashboard Location 123
9.2.8 Printing or Exporting Current Alarm Data 124
9.3 Receive Alarm Notifications 125
9.3.1 Ways to Acknowledge Alarms 125
9.3.2 Acknowledging Inactive Alarms 128
9.3.3 Responding to Audible Alarms 129
9.4 Pause Alarms 129
9.4.1 Pausing Threshold Alarming 129
9.4.2 Pausing Device or Host Alarming 130
9.4.3 Resuming Threshold, Device or Host Alarming 131
9.5 Track Events 132
9.5.1 Viewing Events 132
9.5.2 Adding Comments to Events 133
9.5.3 Adding Custom Events 134
9.5.4 Printing and Exporting Event Logs 134
9.6 Create Trends 136
9.6.1 Building Trends 137
9.6.2 Trend Functions 138
9.6.3 Trend Navigation 138
9.6.4 Modifying Trends 139
9.6.5 Saving Trends 140
9.7 Viewing Quick Trends 141
9.8 Reporting 142
9.8.1 Types of Reports 142
9.8.2 Generating Reports 142
9.8.3 Sharing Quick Reports 143
9.8.4 Generating Quick Reports 144
9.8.5 Viewing Report Downloads 144
9.8.6 Deactivating/Activating Reports 145

9.8.7 Alarm Period Reporting ... 145
9.9 Create Custom Reports ... 146
9.9.1 Creating Location History Reports ... 146
9.9.2 Creating Alarm Reports ... 150
9.9.3 Creating System Reports ... 152
9.10 Viewing Data with viewLinc Mobile ... 153
9.10.1 Pause or Resume Alarming with viewLinc Mobile ... 155
9.10.2 Acknowledging an Alarm with viewLinc Mobile ... 155
9.10.3 Viewing Data on a Remote Display ... 156
9.10.4 Changing a Display Terminal View ... 156
10. Administrator Tasks ... 159
10.1 Groups and Users ... 159
10.1.1 Editing User or Group Details ... 159
10.1.2 Deactivating/Reactivating Users ... 159
10.1.3 Deactivating/Reactivating Groups ... 160
10.2 Zones and Locations ... 161
10.2.1 Viewing Location Properties ... 161
10.2.2 Renaming a Location or Zone ... 163
10.2.3 Unlinking/Relinking Locations and Channels ... 163
10.2.4 Moving Locations ... 166
10.3 Removal of Zones and Locations ... 167
10.3.1 Deactivating Locations ... 167
10.3.2 Reactivating Locations ... 167
10.3.3 Hiding/Showing Deactivated Locations ... 168
10.3.4 Deleting Zones or Locations ... 168
10.4 Disable/Enable Alarming ... 169
10.4.1 Disabling/Enabling Threshold Alarm Settings ... 169
10.4.2 Disabling/Enabling Threshold Alarm Template Levels ... 170
10.4.3 Disabling/Enabling Device Alarming ... 170
10.4.4 Disabling/Enabling Host Alarming ... 171
10.5 Device Maintenance ... 171
10.6 Device Removal ... 171
10.6.1 Deactivating/Reactivating Hosts or Devices ... 172
10.6.2 Releasing RFL Data Loggers ... 172
10.7 Swap Devices ... 173
10.7.1 Swapping Devices ... 173
10.8 Device Calibration ... 174
10.8.1 Editing Channel Calibration Properties ... 175
10.8.2 Editing Device or Probe Calibration Properties ... 175
10.8.3 Off-site Calibration ... 176
10.8.4 On-site Calibration ... 176
10.9 Lock/Unlock DL Data Loggers ... 177
10.9.1 Locking/Unlocking DL Data Loggers ... 177
10.10 Clearing Historical Samples ... 178

10.10.1 Clearing Historical Samples in DL Data Loggers 178
10.11 Correct Security Status 179
10.12 Testing Network Communications 179
10.13 Restarting viewLinc 180
11. Frequently Asked Questions 181
11.1 Installing viewLinc 181
11.2 Managing Data 182
11.3 Managing Devices 183
11.4 Predefined Settings 185
11.5 Troubleshooting Tips 187
Glossary 191
Index 197

List of Tables

Table 1 Server Requirements Based on System Size 2
Table 2 Default Installation Folders 3
Table 3 New Features 4
Table 4 Key Features of viewLinc 5
Table 5 Important Changes for Upgrade Users 6
Table 6 Device Connection Options 10
Table 7 Reference Manuals 14
Table 8 Protocol Test References 27
Table 9 Device and Host Properties - Columns 35
Table 10 Rights Definitions 58
Table 11 Alarm Descriptions 64
Table 12 Permission Levels 103
Table 13 Icon Glossary 116
Table 14 Status Tab Columns 120
Table 15 Key Elements in a Trend Graph 136
Table 16 Location Properties Columns 162
Table 17 Definitions File Fields 183
Table 18 Email and SMS Content Macros 185
Table 19 Tips for Managing Alarms 188

1. Product Overview

1.1 Vaisala viewLinc Enterprise Server

Vaisala viewLinc Enterprise Server is the software used to support all combinations of the Vaisala viewLinc Monitoring System. It features triple-redundant data retention ensuring that data is immune to power outages, network interruptions, and human error.
Use viewLinc to monitor device readings locally on a PC, across a network using a supported Internet browser, or from mobile devices like the iPhone® or Google Android®.

Vaisala viewLinc Enterprise Server software provides continuous monitoring of real-time data, ensures data history is backed-up, recognizes alarm conditions, and can automatically send alarm notifications to individuals or groups wherever your business is located. This flexible and scalable system allows you to set up a server in Paris to monitor a sensor in Berlin, and schedule reports to be sent to your team members in their choice of eight languages.

viewLinc provides you with many configuration options. You can set up the system for users with different levels of responsibility, manage multiple alarm notification methods, display data for a wide range of display formats, and accommodate custom reporting requirements.

1.2 How Does viewLinc Work?

Every Vaisala viewLinc Monitoring System needs one installation of Vaisala viewLinc Enterprise Server software on a dedicated 24x7 Windows® server. Depending on your network requirements and data monitoring needs, you can install viewLinc Device Host software on additional Windows servers.

- viewLinc **Enterprise Server**: Gathers data from devices, recognizes fluctuating conditions, executes any associated alarm response actions, manages users and groups, and controls both system-wide and user-specific settings.
- viewLinc **Device Host**: Acts as a data distribution point for devices located in an off-site or remote location, forwarding device data to Vaisala viewLinc for processing and storage.

1.2.1 Hardware Requirements

Your Vaisala viewLinc monitoring system is made up of a combination of the following hardware components:

- A dedicated Windows® server continuously available 24 hours a day, 7 days a week, to run viewLinc Enterprise Server software.
- One or more Vaisala DL data loggers, RFL100-series or HMT140-series wireless data loggers, or 300-series transmitters.

- Optional hardware requirements:
  - VaiNet access points to manage RFL100-series data loggers.
  - Additional servers to manage devices at multiple locations (running viewLinc Device Host software).
  - Remote display terminals to provide additional monitoring opportunities in areas without PCs.
  - Vaisala cables, for connecting data loggers and setting up HMT140-series data loggers or 300-series transmitters.
  - vNet or multi-port Ethernet interface devices, for connecting Vaisala DL data loggers using an Ethernet connection.

1.2.2 Server Requirements

For optimum performance, the viewLinc Enterprise Server requires:

- 200 KB available per data point per day for storing linked channel data.
- 2 GB disk space for viewLinc Enterprise Server software installation.
- Microsoft® Windows® Server 2016 (64 bit), Windows Server 2012 R2 (64 bit) operating system, Windows 2008 R2 (64 bit), or Windows 10 (64 bit).
- (optional) A supported Internet browser is only required on the viewLinc Enterprise Server computer if you plan to use it to run viewLinc (Google Chrome™, Microsoft® Internet Explorer® 11, or Microsoft Edge™).

The viewLinc Device Host requires:

- Dedicated server available 24 hours a day, 7 days a week.
- 2 GB disk space.
- Microsoft® Windows Server 2016 (64 bit), Windows Server 2012 R2 (64 bit), Windows Server 2008 R2 (64 bit), Windows 10 (64 bit).
- A supported Internet browser installed (Google Chrome™, Microsoft® Internet Explorer® 11, or Microsoft Edge™).

1.2.3 Installed System Size

Depending on the number of device channels (data points) you plan to activate and monitor, the viewLinc Enterprise Server should also meet the following requirements:

Table 1 Server Requirements Based on System Size

System Size	viewLinc Enterprise Server Requirements
Large More than 100 devices (400+ channels)	A dedicated machine, 3.2 GHz, Quad Core, 16 GB RAM; Sufficient HD space to support 200 KB / data point / day. For example, if you have 400 linked device channels, you need approximately 30 GB (400 x 200 x 365) per year.

System Size	viewLinc Enterprise Server Requirements
Medium Up to 20 devices (up to 400 channels)	A dedicated or shared machine, 1.6 GHz, Dual Core, 12 GB RAM; Sufficient HD space to support 200 KB / data point / day. For example, if you have 40 linked device channels, you need approximately 3 GB (40 x 200 x 365) per year.
Small Less than 5 devices (<20 channels)	A dedicated or shared machine, 1.6 GHz, Dual Core, 8 GB RAM; Sufficient HD space to support 200 KB / data point / day. For example, if you have 4 linked device channels, you need approximately 300 MB (4 x 200 x 365) per year.

1.2.4 End User PC and Remote Display Requirements

Other machines connected to your network which have an Internet browser installed, can be used to monitor devices. The machine must meet these minimum requirements:

- 2.4 GHz
- 4 GB RAM
- Google Chrome™, Microsoft® Internet Explorer® 11, or Microsoft Edge™

1.2.5 Default Application File Locations

It is recommended that you use the default installation folders for data file storage, as other folders may have special security restrictions placed on them. For example, Windows Server 2008 does not allow files in the program files folders to be deleted by non-admin users.

Table 2 Default Installation Folders

Platform	Default File Storage Location
Windows Server 2012 R2 or Windows Server 2008 R2	Program files: C:\Program Files\Vaisala\Vaisala viewLinc Data files: C:\Users\Public\Documents\Vaisala\Vaisala viewLinc
Windows 10 and Windows Server 2016	Program files: C:\Program Files\Vaisala\Vaisala viewLinc Data files: C:\Documents and Settings\All Users\ Documents\Vaisala\Vaisala viewLinc

1.3 What's New

Vaisala viewLinc 5.0 is a feature-rich redesign of earlier versions of viewLinc software. It provides you and your team with a simplified User Interface (UI) and new ease-of-use functionality to help get you set up, configured, and using your viewLinc continuous monitoring system quickly and efficiently.

Table 3 New Features

Feature	Description
VaiNet support	Support for new devices using Vaisala's proprietary wireless technology, VaiNet.
Setup support	With interactive tours at your fingertips, a new system planning worksheet and checklist, setting up your viewLinc system has never been easier.
User guidance at your fingertips	The new user-focused design ensures more intuitive software interaction. Users can find tips on-screen, follow orientation and interactive tours, and access comprehensive online Help and eLearning videos (videos available with support plan).
Flexible alarm notifications	Send visual, audible, email, or SMS alarm notifications when conditions you are monitoring are out of compliance or if there is a network communication problem. Set up specific groups to receive different types of alarm notifications at different times.
Improved access control	Manage access to monitored areas, system configuration or alarm acknowledgement functions according to a user's group.
Multi-level thresholds	Easily enable one or more threshold levels on one template.
Integrated software functionality	Configure data logger calibration duration and other important device settings in viewLinc, without requiring additional software.
Improved graphical display	Easier access to important functions, greater visibility of alarm conditions, and embedded online Help when you need it most.
Audible alarms	New alarm commands support audible alarming.
Multi-language support	Send reports and notifications to your team members around the world in one of eight languages (EN, FR, DE, ES, PT, SV, JA, ZH).
Wireless device discovery	All new wireless devices connected to your network are automatically discovered by viewLinc.
Easier link management	Choose whether to include data history when linking a device channel to a Location.

Feature	Description
Improved system security	All users who log in to viewLinc require a secure connection. During installation you can upload existing security certificate and key files, or automatically generate self-signed certificate and key files.

Table 4 Key Features of viewLinc

Feature	Description
Audit trail security	Store complete audit trail records for reporting compliance with 21 CFR Part 11 and other regulatory and accreditation requirements.
Monitoring visibility	Add site maps to the dashboard to easily identify your devices and the areas where they operate.
Easy alarm response	Create predefined comments that can be used to provide a quick response to alarm notifications.
Data monitoring	View real-time data in a customizable, graphical format.
Global reporting	Generate reports on historical data and alarm reports according to user-specified language.
Efficient data logger maintenance	Swap a device for calibration or replacement purposes without breaking the data audit trail.

1.3.1 What's New for Upgrade Users

If you are already familiar with viewLinc, here is a review of important enhancements and changes.

Enhancements

- **Reusable notifications**: Separate alarm notification templates can be applied to device alarm and threshold alarm settings. These templates define the type of notification to initiate when an alarm is activated (email/SMS/command), who to notify, and whether to delay or repeat notifications.
- **Simplified access control**: To ensure greater control over user access to different functional areas of viewLinc, rights and permissions are now only assigned to groups.
- **Verified site security**: All new installations of viewLinc 5 require that you provide a security certificate and key file. During viewLinc Enterprise Server software installation, you can install existing certificate and key files, or automatically generate self-signed certificate and key files.
- **Expanded email support**: viewLinc 5 now includes support for both IMAP and POP3 email settings.
- **Improved graphing options**: Create data trends with up to 16 Locations and 4 measurement types.

- **Distributed system alarm notifications**: Never miss a notification—configure system alarm notifications to include distribution to members of the viewLinc Administrators group.
- **User-friendly terminology**: Zones and Locations are collectively referred to as Sites; On-demand reports are now Quick Reports. See all terminology changes (see "Glossary" on page 191).

Table 5 Important Changes for Upgrade Users

Feature	Description
Overview window, Getting Started	When an Administrators group member logs in for the first time, the **Getting Started** tab in the **Overview** window displays links to online Help in three categories, **Setup - Learn - Use**. When general users log in, the Getting Started tab displays links to online Help in two categories, **Learn - Use**.
Devices	When new wireless devices are recognized on your network, you are notified on the viewLinc desktop automatically. To learn more, see "Accepting Wireless Devices" on page 31.
Zones and Locations	Management of Zones and Locations is performed in Sites Manager. To avoid confusion between device and Location descriptions, you can now only use drag and drop functionality to link Locations within Zones. To learn more, see "Create Zones and Locations" on page 46.
Access Control	Permissions are only assigned to groups. For users who had permissions assigned in an earlier version, those permissions are still valid (legacy permissions); however, it is recommended that you remove user permissions and add the user to a group with the required permission level. Configure Custom Thresholds, is now Configure Alarms, and Hide permission is now managed by removal of View permission. New permissions are granted at the Zone level. To learn more, see "Applying Group Permission to Zones" on page 103.
Users and Groups	Assign a user-preferred language for receiving alarm notifications and reports. Rights are now assigned only to groups. For users who had rights assigned in an earlier version, those rights are still valid (legacy rights); however, it is recommended that you remove user rights and add the user to a group with the required rights. Manage Comments is now included in the **Manage System** right; Manage Threshold Templates is now included in **Manage Alarm Templates** right. Manage Locations is renamed **Manage Sites**. To learn more, see "Groups and Users" on page 57.
Alarm Templates	Alarm notification details have been removed from threshold and device

Feature	Description
	alarm templates, and are stored as independent alarm notification templates. Alarm notification templates can be added to a Location's device alarm settings, and to a Location's assigned threshold alarm settings. In Device and Threshold Alarm templates, the alarm color is identified as the alarm priority: High, Medium, Low, Information. To learn more, see "Alarm Templates" on page 63.
	Threshold Alarm Templates: • All threshold alarms support up to 5 thresholds. • All upgraded single-level thresholds can remain single or be set up to include additional threshold levels. • All threshold settings are captured in threshold alarm templates. If you had created private thresholds for specific Locations they are converted to threshold alarm templates on upgrade.
	Alarm Notification Templates: • Alarm notification templates identify who gets notified in the event of an alarm condition, when the notification is sent, and how it is delivered (email, SMS, command). - If you had notification settings assigned to specific Locations (private settings), notification details are saved as alarm notification templates. The new alarm notification templates are applied to the original Locations. - If you had notification settings assigned to any alarm or threshold templates, they are separated and stored as independent alarm notification templates. • Pop-up alarm notifications are no longer supported. • Email addresses to non-viewLinc users are no longer permitted, and are removed on upgrade.
	Device Alarm Templates are now applied and managed on Locations.
	Email and SMS Content: If you specify an alarm message or comment for auto-generated system alarm notifications or threshold alarm notifications, the content is included automatically in the associated default email templates and can be included in custom email or SMS templates. To learn more, see "Email and SMS Content" on page 85.
System Preferences	System alarm, email and SMS settings are configured in the System Preferences window. To learn more, see "System Preferences" on page 87.

Feature	Description
Views	Find all your views in the new Overview window. All users have access to and can create their own views in the Views Manager window. Manage Views right is required to share a view with others. Note that a pinned view is now a default view. To learn more, see "Your Views" on page 108.
Reports	To review changes in report output content and format, see samples in the Reports window. Email addresses to non-viewLinc users are no longer permitted, and are removed on upgrade. All users can create reports and assign ownership to other users. Ownership allows other users to modify or share a report. To learn more, see "Reporting" on page 142.
Trends	Trends can be built in Sites or Overview windows. Set threshold line color in a threshold alarm template. To learn more, see "Building Trends" on page 137.
Terminology	Terminology changes: • Sites = a collection of Locations and Zones • On-demand reports = Quick Reports • Deadband = Alarm off margin • Access Control List = Permissions • Permissions Inspector = Permissions Viewer To learn about all terminology changes, see "Glossary" on page 191.

For an overview of all new viewLinc 5.0 features, see "What's New" on page 4.

1.3.2 Watch a Tour

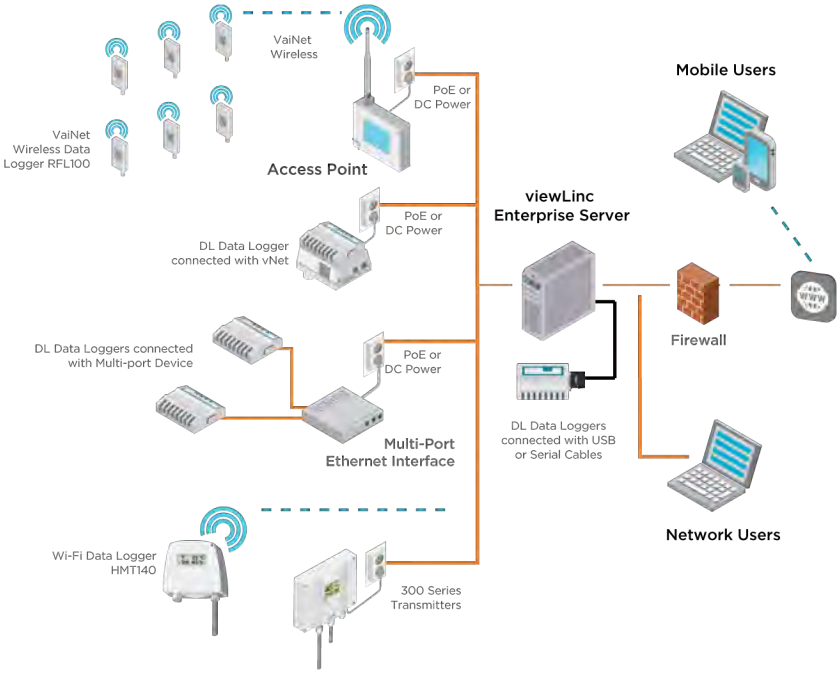
Learn about key changes with the redesigned viewLinc desktop or discover new viewLinc functionality. There are two types of tours available:

- **Orientation Tours**: Tour steps describe important functions.
- **Task Tours**: Tour steps allow you to complete specific viewLinc tasks—watch for the icon, .

Tours are always available from the viewLinc desktop, see **Help > Tours**.

1.4 Device Connection Options

Your viewLinc Enterprise Server can support a combination of device connections and setup configurations.



1.4.1 Ways to Connect Hardware

How you connect AP10 access points, RFL100-series, DL, HMT140-series data loggers, or 300 series transmitters to your network is a very important administrative decision. Each connection method requires specific hardware connections. It is also possible to use a mix of these methods depending on your system requirements.

Table 6 Device Connection Options

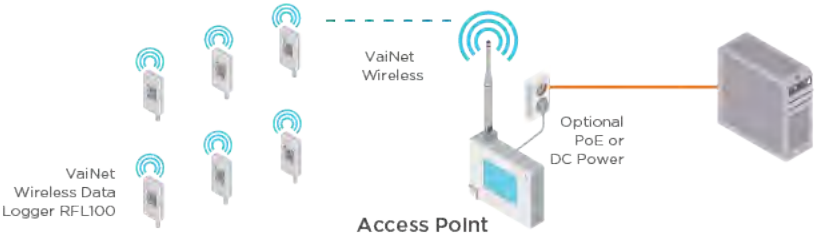
Data Logger	How Connected
RFL100-series	Connect devices using Vainet wireless: • Requires installation of a VaiNet AP10 access point (see related RFL and AP10 device user guides for installation information).
DL	Connect devices to an Ethernet interface device: • Installation using PoE requires a vNet device (using vNet drivers or viewLinc Aware), or a multi-port Ethernet device with supported drivers. • If you are installing vNet devices on the same subnet as viewLinc, device drivers are installed automatically when you enable viewLinc Aware functionality (see "viewLinc Aware" on page 92). • For installation instructions, refer to the vNet or other multi-port Ethernet device documentation. Connect devices to the viewLinc Enterprise Server or viewLinc Device Host server: • Requires Vaisala USB or a serial connector cables.
HMT140-series	Connect devices wirelessly using 802.11b/g Wi-Fi: • HMT140-series data loggers require configuration with an HMT140 Configuration Cable and HMT140 Utility software. For installation instructions, refer to the HMT140 user guides.
300 Series Transmitters	Connect devices to a LAN or WLAN: • For 300-series installation instructions, refer to the product documentation.

Refer to your device user guides for installation and configuration information.

1.4.2 Using Wireless Devices

VaiNet RFL100-Series

To set up VaiNet RFL100-series data loggers, you require an AP10 access point. Refer to the RFL100-series and AP10 device documentation for complete setup and configuration instructions. To learn how to connect RFL data loggers to viewLinc, see "Adding Access Point Hosts" on page 30 and "Accepting Wireless Devices" on page 31.



HMT140-Series

To set up HMT140-series data loggers, you require a configuration cable and HMT140 Utility software. Refer to the HMT140 device documentation for complete installation instructions. To add an HMT140 device to viewLinc, see "Accepting Wireless Devices" on page 31.

1.4.3 Using vNet Devices

For information about connecting Vaisala data loggers to your network using vNet devices, refer to the *vNet User's Guide*.

If you are installing vNet devices on the same subnet as viewLinc, device drivers are installed automatically when you enable viewLinc Aware functionality (see "viewLinc Aware" on page 92). Full details are available in the *vNet User's Guide*.
New devices are automatically detected in viewLinc. If it is taking too long, you can also force discovery. See "Discovering Networked Devices" on page 31.

1.4.4 Using Single or Multi-Port Ethernet Device Connectors

You can connect Vaisala data loggers to your viewLinc network using single- or multi-port Ethernet connection device (such as Digi or Moxa devices). Ethernet device drivers must be installed on each server used to connect Vaisala devices. For installation instructions, refer to Ethernet product documentation.

Obtain a reserved (recommended) or static IP address for your Ethernet device from your IT department, unless your networking policy requires you to reserve IP addresses using DHCP.

New devices are automatically discovered in viewLinc within a few minutes. If the auto-discovery process is taking too long, you can force discovery. See "Discovering Networked Devices" on page 31.

1.4.5 Using USB Ports

You can connect Vaisala data loggers directly to servers using a USB Port.

Drivers: Install USB Drivers

Install USB drivers on each server used to connect devices.

Connect a USB Port

1. Connect the Vaisala device to a Vaisala USB cable.
2. Connect the Vaisala USB cable to your viewLinc Enterprise Server or Device Host (ensure the computer is attached to your network). You only need to install drivers once on each machine to which devices are connected.

Repeat these steps for all devices. To set up your DL devices in viewLinc, see "Discovering Networked Devices" on page 31.

DL Data Loggers connected with USB or Serial Cables

1.4.6 Using Serial Ports

Connect DL data loggers and 300-series transmitters to a viewLinc ES or Device Host server using a serial port.

Connect a Serial Port

1. Connect the device to a Vaisala serial port cable.
2. Connect the serial port cable to your viewLinc ES or Device Host server (ensure the computer is attached to your network).

To set up a DL device in viewLinc, see "Discovering Networked Devices" on page 31.

To set up a 300-series transmitter in viewLinc, see "Adding Devices Manually" on page 32.

DL Data Loggers connected with USB or Serial Cables

1.5 About the viewLinc User Guide

The *viewLinc User Guide* is intended for both viewLinc administrators and users.

- **Administrators**: Learn how to install and configure viewLinc Enterprise Server software and its associated components, and support users with ongoing system administration tasks.
- **Users**: Learn how to complete common viewLinc tasks, such as viewing and monitoring device readings across your network.

1.5.1 How this Manual is Organized

The Vaisala viewLinc User Guide includes the information you need to install, configure and operate the viewLinc system, and step-by-step procedures for the standard tasks performed using viewLinc.
Chapters 2 to 8: Important system setup information for administrators.
Chapter 9: Description of how to perform common user activities.
Chapter 10: Description of ongoing administrator-level system maintenance tasks.
Chapter 11: Reference for users and administrators.

1.5.2 Conventions Used in this Document

This document uses the following conventions:

- Menu options, items you select, and the names of tabs, windows, and buttons are shown in **bold**.
- A sequence of menu item selections is indicated by a list separated by an arrow. For example: "In viewLinc, select **Help > Tours**"
- Keys on the keyboard are shown in [square brackets].
- Vaisala data loggers, device hosts and access points are all devices.

The lock icon indicates the rights required to perform a viewLinc task.

Note highlights important information on using the product.

Tip gives information for using the product more efficiently.

CAUTION
Warns of potential impact to others.

1.5.3 Related User Documentation

Table 7 Reference Manuals

Document Code	Name
M211820EN	Vaisala viewLinc Monitoring System Setup Guide
B211708EN	Vaisala viewLinc Enterprise Server Software Datasheet
M211822EN	RFL100 Quick Guide
M211861EN	RFL100 User Guide
M211820EN	AP10 Quick Guide
M211860EN	AP10 User Guide

1.5.4 Contact Us

viewLinc technical support:	helpdesk@vaisala.com
Vaisala product support/service centers:	www.vaisala.com/support
eLearning:	www.vaisala.com/en/viewlinc-elearning
Calibration:	www.vaisala.com/calibration
Sales:	www.vaisala.com/contact

1.5.5 Need Training?

For new users of viewLinc , or those who might need to refresh their knowledge, Vaisala provides both remote or onsite training, and access to a series of eLearning videos you can view at your convenience.

For customers with active support plans please follow this link to the eLearning portal, www.vaisala.com/viewLinc-elearning.

Contact Vaisala Technical Support to learn more about Vaisala Services.

2. Setup and Installation

Each viewLinc monitoring system installation is unique. Use the setup checklist to identify your specific site requirements and ensure an efficient and successful installation of the viewLinc monitoring system components.

2.1 Setup Checklist

viewLinc Server	
☐	I have a system administrator or IT support available to help me with network and server configuration.
☐	A network server has been allocated to run viewLinc Enterprise Server 24x7. I know its IP address and hostname, and it meets minimum viewLinc server requirements.
☐	I know the address of the Network Time Protocol (NTP) server in the network.
☐	My laptop or workstation has a supported web browser (Google Chrome™, Microsoft® Internet Explorer version 11, or Microsoft® Edge™) and a PDF reader application installed (such as Adobe Acrobat®).
☐	I know where the program files and viewLinc database should be stored. A backup system is in place to make sure the files are recoverable in case of server failure.
☐	I know if the local network security policy requires me to use a trusted TLS certificate. If yes, I have located my company's signed security certificate and key files, or have the information required to create a private certificate and key during installation (hostname, alias, number of years certificate will be valid for).
☐	I have the USB drive that contains the viewLinc setup files and license key.
Devices	
☐	I have a plan that lists the serial number and installation location of each device.
☐	The plan includes information on how each device will be mounted (magnets, screws, etc.).
☐	IP addresses have been allocated for my HMT330 series transmitters and data loggers' network connections (DHCP address reservations or static IPs).
☐	Planned locations of wired devices are within 180cm (6 feet) distance of power outlets.
☐	I know if drilling or door access is required for probes (for example, freezer installation).

Network	
☐	RJ45 Ethernet network drops with jacks have been installed and tested at each location where a wired network connection is needed.
☐	A Power over Ethernet (PoE) injector or switch provides operating power at network drops where a PoE powered device will be installed.

2.2 viewLinc Enterprise Server Configuration

After installing and adding devices to viewLinc, there are many ways to configure viewLinc to meet site-specific monitoring needs. It is recommended that you complete the viewLinc planning worksheet to ensure you consider all your site monitoring needs (see "Plan your viewLinc Configuration" on the facing page).

1. viewLinc Enterprise Server configuration:
   - Create Zones and Locations
   - Add Groups and Users
   - Define Alarm Templates
   - Set System Preferences
2. Additional tasks:
   - Permissions
   - Schedules
   - Predefined Comments
   - Views
3. Installation verification

Online tours are available for each configuration step (see **Help > Tours**).

2.3 Plan your viewLinc Configuration

Taking the time to evaluate and define your company's monitoring needs will provide you and your team with a more secure and easy to maintain monitoring system.
Review this worksheet to make sure you have the information required to configure viewLinc , then complete the viewLinc Enterprise Server setup steps.

viewLinc Planning Worksheet

Zones and Locations (Sites Manager)	
☐	Define a naming convention for each area being monitored with one device channel. (1 device channel = 1 Location)
	1.
	2.
	3.
	4.
☐	Create Zones to organize areas with many Locations (optional)
	1.
	2.

Groups and Users	
☐	Name your groups, and identify the rights to be assigned to each group.
	Group name/rights:
	Group name/rights:
☐	List your users and the group(s) to which they will be assigned
	Users in viewLinc default Administrators group (all rights):

Groups and Users	
	Users in Everyone group (Manage Events right):
	Users in _____ group:
	Users in _____ group:

Threshold Alarms	
☐	Record the threshold settings needed for each Location. (High-High, High, Low, Low-Low, Rate of Change, Alarm Off Margin)
	Location 1:
	Location 2:
	Location 3:

Alarm Notification Settings (Alarm Templates)	
Threshold Alarm Notifications	
☐	Identify the users or groups to be notified in the event of a threshold alarm, when the notification should be issued, how it will be delivered (email, SMS, or a command).
	Name:
	Delay:
	1st notice sent via:
	2nd notice sent via:
	Repeat?
	Frequency:

General Settings (System Preferences)	
☐	Determine whether to use device and channel descriptions in viewLinc , or create longer descriptions (aliases) in viewLinc .
☐	If using an access point, determine data logger lock settings (automatic or disabled).
☐	Enable and then create pre-configured comments for your users to add when responding to alarm conditions.
☐	Enable and then create schedules if Location monitoring/alarm acknowledgement is required for certain time periods, or if different groups will receive different alarm notifications.
☐	Define how to display measurement units.
☐	For multilingual companies, determine the language to use for system notifications.

Email Notification Settings (System Preferences)	
☐	Required: Your IT network manager's email address to **receive** all system alarm email notifications.
☐	An available email address that will be used to **send** viewLinc notifications.
☐	SMTP server address, port number, account user name, and password.
☐	POP3 server address, port number, account user name, and password (optional).

SMS Notification Settings (System Preferences)	
☐	If SMS notifications are enabled, identify your IT network manager's mobile number to **receive** all system alarm SMS notifications.
☐	SMS modem SIM card PIN.
☐	SMS COM port number.
☐	SMS modem baud rate.

2.4 Install viewLinc

All viewLinc monitoring systems require the installation of viewLinc Enterprise Server software on a local or remote dedicated server. If you are setting up a medium or large monitoring system using several devices, it is recommended that you install viewLinc Device Host software on additional dedicated servers for greater network stability and flexibility.

- **viewLinc Enterprise Server software**: This installation software is required on the dedicated Windows server, to monitor and administer all devices connected to it, wired and wireless. It defines the system language, data storage paths, and monitoring conditions.
- **viewLinc Device Host software**: This installation software can be installed on additional, dedicated servers. It allows automatic communication with the viewLinc Enterprise Server computer while offering protection from bandwidth and network communication issues. It provides you with greater flexibility when managing device configuration across a large network.

Refer to the Device Host and Enterprise Server requirements for different installation sizes, to determine if your system is better suited to one or both software installations (see "Hardware Requirements" on page 1).

2.4.1 Installing viewLinc

If you have an older version of viewLinc software on your network, see "Installing viewLinc as an Upgrade" on page 24.

Install viewLinc for the First Time

1. Ensure you have completed the Setup Checklist and have recorded the serial number from your viewLinc USB.
2. On the dedicated viewLinc ES server, insert the viewLinc USB and run viewLincInstall.exe, if it does not start automatically.

> To install viewLinc software on a remote server (and not the local computer), copy **viewLincInstall.exe** file from the USB drive to the destination server.

3. Select the installation language. This language setting is used in the wizard and is used as the viewLinc browser, report and notification default language. The default language can be changed after installation is complete..

> Users can change the browser language at log in. The language used in their reports and notifications is set in each user's profile.

4. Start the Installation Wizard.
5. Enter your license key.

6. Select the installation package. All viewLinc monitoring systems require Vaisala viewLinc Enterprise Server. If your system will support a large installation with several devices, rerun the install wizard to install viewLinc Device Host package on additional dedicated servers (see "Hardware Requirements" on page 1).
7. Accept the Vaisala General License Conditions and BerkleyDB License Agreement.
8. Accept the default installation path for the viewLinc software, or specify a new destination folder (location must have at least 2 GB of free disk space).
9. Accept the default installation path for viewLinc data, or specify a new destination folder (location must have at least 10 GB of free disk space).
10. Choose your certificate and security key files:
    - Choose the option, **Upload a purchased certificate and key (trusted)**, if you already have the files and they are available on your network.
    - If you choose the option, **Generate a certificate and key (self-signed)**, enter your site and company details. The install wizard automatically generates self-signed files as part of the installation process. The files are installed on the server the first time the admin user logs into viewLinc.

    To learn more about certificate and key files, see "Installing viewLinc" on page 181.

11. Select **Install** to complete the installation wizard.

When installation is complete you can set up your devices or begin viewLinc configuration (for reference, see *Vaisala viewLinc Monitoring System Setup Guide*).

You can also set up additional computers as Device Hosts. This option allows for greater flexibility when managing devices, reduces the bandwidth required to communicate from server to device, and reduces the chance of network interference (see "Installing viewLinc on a Device Host Server" below).

If you are ready to start viewLinc configuration, double-click the viewLinc shortcut icon on your desktop.

2.4.2 Installing viewLinc on a Device Host Server

You may need to adjust your firewall settings to specify public/private domain exceptions. Contact Vaisala customer support if you require assistance.

Install viewLinc Device Host Software

1. Insert the viewLinc USB and run viewLincInstall.exe.
2. Select the installation language.
3. Start the Installation Wizard.
4. Accept the Vaisala and BerkleyDB license agreements.
5. Enter the license key number, found on the USB package.
6. Choose a destination for the viewLinc program files.
7. Select **Device Host**.

8. Select **Install**.
9. When the application is finished installing, select **Finish**.

With all necessary viewLinc components installed, you can now use any machine on the network to log in to viewLinc to monitor conditions.

All users can access viewLinc from their own PC or mobile device, without having to install any software; however, their PC must be running a supported Internet browser, they require the IP address where viewLinc is installed, and must be set up as a user in viewLinc.

2.4.3 Installing viewLinc as an Upgrade

To ensure a successful upgrade of your viewLinc software, make sure your system meets the viewLinc 5 system requirements (see "Hardware Requirements" on page 1), and review the new features and functional changes introduced in viewLinc 5 (see "What's New for Upgrade Users" on page 5).

Before you start the viewLinc software upgrade, export a copy of your event log. After upgrade, export the event log again to become familiar with messaging improvements in viewLinc 5.

Install viewLinc Enterprise Server Software

Follow these steps to install viewLinc on an existing server, or on a new server.

1. Ensure you have completed the Setup Checklist and have recorded the license key number from the viewLinc USB.
2. If upgrading on an existing server, verify that the current installation of viewLinc is version 3.6.1 or higher.
3. Back up the current application data directory. The default directory is: C:\Users\Public\Documents|Vaisala\Vaisala viewLinc.
4. If your backup application does not support open database backup, stop viewLinc Watchdog and viewLinc Enterprise Server services:
   a. On your Windows server, select **Start > Control Panel > Administrative Tools > Services** (this path may vary depending on your Windows version and settings).
   b. Right-click on the service (viewLinc Enterprise Server, viewLinc Watchdog), then select **Stop**.
5. On the current or new server, insert the viewLinc USB and run viewLincInstall.exe, if it does not run automatically.
6. Select the installation language. This language setting is used in the wizard and is used as the viewLinc browser, report and notification default language. The default language can be changed after installation is complete..
7. Accept the Vaisala and BerkleyDB license agreements.
8. Enter the viewLinc license key number.

9. Select your security certificate and key files. You can choose to keep the currently installed certificate and key files, upload new certificate and key files, or automatically generate new self-signed certificate and key files (to learn more about security files, see "Installing viewLinc" on page 181).
10. Review the install settings and click **Install**.
11. Click **Finish**.
12. Reboot. Wait 20 minutes to an hour for viewLinc to upgrade the database. viewLinc will not be available during this time. Please do not stop or restart services during this period. There will be a gap in the Events log reflecting the duration of the upgrade.
13. If installing on a new server, copy the backup data from the old server to the new data destination directory:
    - \db folder to Vaisala\Vaisala Veriteq viewLinc\db
    - \log folder to Vaisala\Vaisala Veriteq viewLinc\log (exclude the \debug folder and any files named log\watchdog*.*
    - Reports and transfer folders to Vaisala\Vaisala Veriteq viewLinc\
14. Open the Vaisala\Vaisala Veriteq viewLinc\config\viewLinc.cfg file and set the level = debug ([logging] section).
15. Double-click the desktop icon to start viewLinc. It may take a few minutes to start.
16. Log in with your administrator credentials, such as **admin/admin**, and then select **System Preferences**.
17. In the **System Preferences** window, set the **System log** to **Detailed**.
18. If you have installed viewLinc Device Hosts, run the install wizard to install Device Host software on each device host server.
19. Open **Sites Manager** to verify your Location data is available.

There will be a gap in the events log reflecting the duration of the upgrade.

2.5 Log in to viewLinc

You can log in to viewLinc from any PC with a supported Internet browser.

Log in to viewLinc

1. Double-click the desktop icon or enter the server's IP address and port in a web browser address field. Your administrator provides the correct IP address. For example, https://computername:[portnumber]. If no port number is specified, 443 is used by default.

Save this address to your browser favorites list or set it up as your homepage to easily access viewLinc from your browser.

2. On the viewLinc login screen, select the language you want to use for viewLinc display. When a new language is selected, the page will automatically refresh and update accordingly.

To save your display language setting, ensure that your browser is not set to automatically delete cookies upon exit. To set a default language for reports and notifications that are sent to you, set your preferred language in your user profile (see "Users" on page 59).

3. Enter your username and password.
   - The first time the viewLinc system administrator logs in, enter the default administrator user name and password, **admin**/**viewL!ncAdm1n**.

     For security purposes, it is important to change the default admin user password as soon as possible (see "Groups and Users" on page 159).

   - If you are a member of the Administrators group and this is the first time you are logging in to viewLinc, a brief setup tour starts automatically. Complete the tour to familiarize yourself with the main setup requirements.
   - If you are not an Administrator's group member and this is the first time you are logging in to viewLinc, watch the Welcome tour, **Using viewLinc**, to familiarize yourself with viewLinc.

After you complete or exit a tour, the viewLinc **Overview** window displays the **Getting Started** page.

2.6 System Test

After all viewLinc configuration and device setup activities are complete, follow these simple steps to ensure your system is running smoothly and securely:

- Verify email and SMS functionality (see "Email and SMS Settings" on page 96).
- Ensure all devices are calibrated (see "Device Calibration" on page 174).
- Generate a Location History report to verify that linked Locations are reporting data (see "Creating Location History Reports" on page 146).
- Review the Events window to verify that changes to the system generate an event in viewLinc (see "Track Events" on page 132).

If you are running viewLinc in a GMP environment, you may require validation testing (see "Validate your System" on the facing page).

2.7 Validate your System

viewLinc is ideal for GxP/FDA-regulated applications and environments that contain high-value products. If you are required to maintain bullet-proof environmental monitoring methods and documentation, a viewLinc validation can ensure you receive a stamp of approval during the most stringent audits and inspections.

A GxP-compliant Installation Qualification and Operation Qualification protocol document (IQOQ) is available for purchase from Vaisala. It is used to ensure your system is installed correctly, and performs as expected. IQOQ testing must be performed by a qualified technician or Vaisala Field Services. Learn more at www.vaisala.com/contact-us.

Table 8 Protocol Test References

Test Procedure	References
Email Configuration Verification	System Preferences
SMS Configuration Verification	System Preferences
Event Log and Audit Trail Verification	Events
User Creation and Password Verification	Groups and Users
Group Creation and Assignment Verification	Groups and Users
Security Preferences Verification	System Preferences
Security Rights Verification	Rights and Permissions
Access Permissions Verification	Rights and Permissions
Notification and Threshold Template Verification	Alarm Templates
Email Alarm Notification Verification	Alarm Templates
SMS Alarm Notification Verification	Alarm Templates
Low Threshold Alarm Verification	Threshold Alarm Templates
High Threshold Alarm Verification	Threshold Alarm Templates
Multi-Threshold Verification	Threshold Alarm Templates
RFL-Series Local Threshold Verification	Device Management, Threshold Alarm Templates
140-Series Local Threshold Verification	Device Management, Threshold Alarm Templates
User Schedule Verification	Schedules, Users and Groups
Threshold Schedule Verification	Schedules

Test Procedure	References
Communication Alarm Verification	Device Alarms
Configuration Alarm Verification	Device Alarms
Host Communication Alarm Verification	Device Alarms
Data Presentation Verification	Reports
Calculation Verification	Reports
Time Zone Verification	System Preferences, Reports
System Watchdog Verification	Alarm Templates

3. Device Management

Data is collected in viewLinc from Vaisala devices connected to your network. When new data loggers or transmitters are connected to your network, they are automatically identified by viewLinc. Different devices are then added to viewLinc in a variety of methods:

- RFL100-series data loggers: Automatically identified, manually accepted.
- vNet devices: Automatically identified and automatically added (if on the same subnet), or added manually.
- DL data loggers: Automatically identified and added automatically or manually.
- HMT140-series data loggers: Automatically identified and added automatically or manually.
- 300-series transmitters: Added manually.

Devices and hosts can be managed by users assigned **Manage Devices** right. Some configuration tasks can only be performed by members of the Administrators group.

3.1 Device Hosts

For larger viewLinc system installations, viewLinc provides the option of adding multiple servers to act as device hosts. Connecting groups of devices to device hosts provides you with greater control over specific devices (group management for devices connected to a single host), and ensures greater network stability. You can also set up an additional access points (AP10) as device hosts to manage your RFL100-series data loggers.

For example, you may want to monitor devices in multiple offices. Rather than connecting all devices at each office location to the Vaisala viewLinc Enterprise Server machine, set up additional device hosts at each office for local devices.

This setup allows you to:

- Manage devices more effectively. You may find it easier to pause alarming on all devices at one office, rather than trying to pause alarming on specific devices.
- Ensure even distribution of network traffic. Device hosts help manage the flow of device data to the Vaisala viewLinc Enterprise Server.

3.1.1 Adding Server Hosts

Manage Devices

Add additional servers as device hosts to help manage groups of devices. Before adding a device host, first install viewLinc Device Host software on the Windows server (see "Install viewLinc" on page 22).

Add a Device Host

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. In the **Hosts and Devices** tree, select **Configure > Add Host**.
3. Enter the hostname or IP address.
4. Select **OK**. The viewLinc system automatically discovers the new host and all devices connected to it. Discovery of all devices on the new host may take a few seconds to several minutes to complete. You can continue with other activities during the discovery process. You are notified when the process is complete.
5. Select **Yes** when prompted to refresh.

3.1.2 Adding Access Point Hosts

Manage Devices

Add additional access points as device hosts to help manage groups of wireless devices. Once connected, access points are automatically recognized in viewLinc.

Add an Access Point Host

1. Make sure the access point is configured and connected to your network (refer to the *AP10 User Guide* for instructions).
2. In **Sites Manager** select the **Hosts and Devices** tab and then select Refresh.
3. If the new access point does not appear automatically in the **Hosts and Devices** tree, add the AP manually:
   a. Select **Configure > Add Host**.
   b. Enter the hostname or IP address.
   c. Select **Save**.
   d. Select **Yes** if prompted to refresh viewLinc.

viewLinc automatically accepts the access point, but it may take a few seconds to several minutes to connect all of its RFL data loggers. You can continue with other activities until you receive notification the process is complete. If RFL data loggers are connected to the access point, the **New Devices** prompt appears at the top of the viewLinc desktop. To accept new RFL data loggers, see "Accepting Wireless Devices" on the facing page.

3.2 Ways to Add Devices

As your network monitoring needs increase, it's easy to expand your monitoring capabilities with the addition of new devices.
Depending on the type of devices you are adding to the network, the following options are available to you:

- Automatic detection of new RFL100-series or HMT140-series devices (Accept Devices).
- Automatic detection of new DL devices connected via vNet, USB or multi-port Ethernet device (Discover Devices).
- Manual addition, when you want to add several devices of various types at one time, or you want to add 300-series transmitters (Add Devices).

3.2.1 Discovering Networked Devices

Manage Devices

Use the Device Discovery feature to identify DL data loggers using USB or serial connection cable, or a non-Vaisala single or multi-port Ethernet device connector. Device Discovery can also be used if any DL devices connected using vNet devices are not detected by the viewLinc Aware function.
To learn about viewLinc Aware, see "viewLinc Aware" on page 92.

viewLinc does not recognize 300-series transmitters with the Discover Devices function. Add transmitters manually if they are not detected by viewLinc automatically (see "Adding Devices Manually" on the next page).

Discover DL Data Loggers

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select the host machine to which the device is connected, then select **Configure > Discover Devices** (or right-click and select Discover Devices).

This process may take several minutes, depending on the number of devices and/or components in your network.

3.2.2 Accepting Wireless Devices

Manage Devices

When a new RFL100-series data logger is added to your network, it is identified by the nearest access point. When the access point is paired to an RFL100-series data logger it sends a message to viewLinc that a new device is available. HMT140-series data loggers are also automatically identified by viewLinc. Both RFL100-series and HMT140-series data loggers are added to viewLinc using the New Devices window.

Once a data logger is accepted by your viewLinc system, it is visible in Sites Manager in the Hosts and Devices tree.

Refer to the device user guides for more information about setting up data loggers and access points in your facility.

Accept a Wireless Data Logger

1. Open **Sites Manager**.
2. If viewLinc detects new RFL100-series or HMT140-series devices, **New Devices** text appears at the top of the Sites Manager window. Select the New Devices prompt.

If the New Devices prompt does not appear, see "Ways to Add Devices" on the previous page.

3. In the **New Devices** window in the **Accept** column, select the devices you want to add to your viewLinc system. You can accept a device later (select Leave Pending), or flag a device as available for acceptance by another access point host or viewLinc device host (select Reject).

Rejecting a device prevents it from connecting to the selected host. When a device is rejected it becomes available to connect with another host. A rejected device continues to appear in the New Devices window until it connects with the correct host and is accepted in viewLinc.

4. Select **Accept**.
5. Select **Save**.
6. Open **Sites Manager** to verify that all accepted devices are available in viewLinc:
   a. Select the **Hosts and Devices** tab.
   b. Locate new devices on the **Hosts and Devices** tree.

3.2.3 Adding Devices Manually

Manage Devices

You may need to add a device manually to your system if:

- Discovering DL devices or wireless data loggers is taking too long.
- You are adding a 300 Series Transmitter.
- You want to add a variety of device types at one time (see "Adding Multiple Device Types" on page 34).

Add Vaisala DL Data Loggers

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree select the Vaisala viewLinc or a device host, then select **Configure > Add Device**.
3. In the **Add Device** window, in the **Device Class** list, enter the COM Port number (to view available COM port numbers, go to the Windows start menu and open Device Manager).
4. Select **Save**.

Add 300 Series Transmitters

1. Ensure no other users are logged on to the transmitter you want to add (from a command prompt on the connected PC, type telnet <IP address>).
2. In **Sites Manager** select the **Hosts and Devices** tab.
3. On the **Hosts and Devices** tree, select the Vaisala viewLinc or a device host, then select **Configure > Add Device**.
4. In the **Add Device** window, in the **Device Class** list, select **300 Series Transmitter**.
5. Enter the following:
   - **Timeout**: To ensure continuous monitoring, do not change (default 30 seconds).
   - **Connection Type**: If the transmitter has a LAN or WLAN module, select Network. If you use an external single or multi-port Ethernet device, choose COM Port.
   - **IP Address**: Enter the IP address.
   - **Sample Rate**: Choose 90 (recommended, but you can modify the rate if you need more or less recorded data).
6. Select **Save**.

Add HMT140 Series Data Loggers

1. Ensure no users are logged on to the HMT140 you want to add.
2. In **Sites Manager** select the **Hosts and Devices** tab.
3. On the **Hosts and Devices** tree select the Vaisala viewLinc or a device host, then select **Configure > Add Device**.
4. In the **Add Device** window, in the **Device Class** field, select **HMT140**.
5. Enter the following:
   - **Timeout**: To ensure continuous monitoring, do not change (default 30 seconds).
   - **Serial number**: Enter the HMT140 serial number.
   - **UDP Port**: Can be modified if required.
   - **Max blocks per beacon**: Accept the default number of data blocks (64) transferred between viewLinc and the device to maximize network efficiency, or modify as required (256 max).

   Do not change the **Max blocks per beacon** value for HMT140 data loggers without first consulting your technical support department. Changes to this setting may adversely impact battery life.

6. Select **Save**.

3.2.4 Adding Multiple Device Types

Manage Devices

To save time, you can add several types of devices to viewLinc at one time using a definitions file.

Add Multiple Devices at One Time

1. Create a .txt definitions file that identifies the device class and device properties (see "Managing Devices" on page 183).
2. In **Sites Manager** select the **Hosts and Devices** tab.
3. On the **Hosts and Devices** tree, select a host, then select **Configure > Add Device**.
4. In the **Add Device** window, in the **Device Class** list, select **Upload Definitions File** then browse to the correct file.
5. Select **Save**.

3.3 Configure Hosts and Devices

After devices are connected to your network and visible in viewLinc (Sites Manager > Hosts and Devices), you are ready to configure your devices to work with your viewLinc monitoring system. Configuration activities you can complete in viewLinc for most devices include:

- Modify device description or add an alias
- Set sample intervals
- Enable or disable channels
- Modify device and channel descriptions
- Designate file storage location for historical data backup

If you were using DL data loggers prior to installing viewLinc 5, you may have set them up on your system with vLog software. You can continue to use vLog or use viewLinc for new configuration activities. To ensure configuration with viewLinc, see "Lock/Unlock DL Data Loggers" on page 177.

3.3.1 Viewing Host and Device Properties

In **Sites Manager** select the **Hosts and Devices** tab to view device or host properties. Select the top viewLinc folder in the **Hosts and Devices** tree to include all devices in the Properties grid.

To sort, view or hide grid columns see "Working with Columns" on page 118.

Table 9 Device and Host Properties - Columns

Properties	
Device Properties	
Description	System Preference in use - description or alias.
Description in Device	Description preconfigured in device or modified in viewLinc.
Device Alias	Long description configured in viewLinc.
Device ID	ID assigned by viewLinc when device was added.
Device Status	Connection status with viewLinc.
Serial Number	Serial number associated with the device.
Probe Serial Number	Displays the serial number of the probe if one is connected to the channel.
Sample Interval	Interval between samples taken from device.
Log Capacity	Estimated time remaining for data collection. For information on storing data, see "Editing Device Properties" on page 39.
Device Address	Address of device recognized in viewLinc.
Device IP Address	The IP address of the device.
MAC Address	MAC address of the channel's device, if available.
Security Status	Only DL data loggers will display as Not secure. If a DL data logger indicates Tampered, see "Lock/Unlock DL Data Loggers" on page 177.
Next Calibration Date	Displays next calibration date, if one is set in the device.
Calibrated By	Company which completed most recent calibration service. 300-series and SP data logger calibration information can only be found on the calibration certificate shipped with the device.

Properties	
Channels	Number of available channels for the selected device.
Device Alarming	Indicates whether device alarming is paused.
Hardware Model	Hardware model information for the channel's device.
Hardware Revision	Latest hardware revision number for the channel's device.
Firmware Version	Latest revision number of the firmware in the channel's device.
Transmit Period	Time between each transmission.
Battery Status	Estimated battery life remaining.
RSSI (Signal Strength)	For wireless devices, displays the device signal strength (dBm)
Signal Quality	For wireless devices, displays current signal quality,
SNR	Signal to Noise ratio for wireless devices (dB).
Lock Status	DL data loggers are either locked to viewLinc (Locked) and cannot be modified outside of viewLinc, are locked to vLog or another instance of viewLinc (Remote Lock), or are not yet locked to any software (Unlocked).
Realtime Only	Yes indicates that the data logger only sends real-time data to viewLinc. It does not store data history.
Communication Alarm Template	Name of alarm template in use for channel's device.
Configuration Alarm Template	Name of alarm template in use for channel's device.
Validation Alarm Template	Name of alarm template in use for channel's device.
Calibration Alarm Template	Name of alarm template in use for channel's device.
Channel Index	Index number that the channel has assigned on its device.
Channel Description	System Preference in use - description or alias.
Channel Description in Device	Description provided with the device. Refer to the Location name.
Channel Alias	Displays the alias, if one has been created in viewLinc.
Channel Alarming	Indicates whether device alarming is paused.

Properties	
Channel ID	Unique channel identifier.
Device Units	Units measured (such as RH, C, mA, mV).
Editable	Indicates whether the device has properties that can be modified in viewLinc.
Location	Displays the Location name linked to the channel (if linked).
Host Properties	
Hostname	Displays the host name for the selected device or channel.
Resolved Name	For administrative purposes.
Description	System Preference in use - description or alias.
Status	Connection status with viewLinc.
Host IP Address	Host IP address.
Host Type	Indicates whether the selected host is the Vaisala viewLinc machine.
Number of Devices	The number of devices connected to the host.
Version	viewLinc version running on the host.
Status	Indicates whether the host is currently connected to the viewLinc monitoring system.
viewLinc Aware	Indicates whether the viewLinc Aware Service is enabled on the host.
Host Alarming	Indicates that host alarms are currently enabled.
Installation Mode	If host is a VaiNet access point, indicates whether status is enabled or disabled.
VaiNet Channel	Indicates the channel being used for the VaiNet access point, if applicable.
Host ID	Unique host identifier.

3.3.2 Editing Host Properties

Manage Devices

Depending on the type of host you use, various properties can be modified:

- On the viewLinc ES server all properties are editable.
- On an access point host you can modify the description, and enable or disable installation mode when pairing new RFL data loggers.
- On a device host server you can modify the description, and enable or disable automatic recognition of vNet devices (viewLinc Aware).

Edit Host Properties

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select a host.
3. Select **Configure > Edit Properties**.
4. In the **Edit Host Properties** window, edit available properties.

Enterprise Server properties:

- **Alternate viewLinc server name**: If the viewLinc ES is behind a firewall, add a server name to ensure that device hosts are recognized, even if the IP address of the viewLinc ES changes.
- **viewLinc Enterprise Server port**: This is the port that device hosts use when connecting to the viewLinc ES (refer to your IT port policy to determine if it needs to change).
- **viewLinc Aware**: Disable this function if you have another viewLinc ES or device host running on the same subnet (to ensure vNets connect to the correct viewLinc ES or device host).
- **viewLinc system ID (64-bits)**: The auto-generated system ID is used by devices to recognize the viewLinc ES. If you need to change this number, contact Vaisala Technical Support for assistance.

Access Point properties:

- **Description**: Enter a description (up to 64 alpha-numeric characters) to help identify this host. On the Hosts and Devices tree the host name appears in addition to the description. For example, "My Host (AP10-X###)".
- **Installation mode**: Enable this function to pair new RFL data loggers with the access point.

RFL data loggers can only be paired with an access point that has installation mode enabled. Once paired, installation mode can be disabled. You can enable or disable installation mode in viewLinc or in the access point web UI. For more information refer to the *AP10 User Guide*.

- **VaiNet channel (1-8)**: If your viewLinc system supports several access points on the same wireless frequency, each access point requires a unique channel number to ensure uninterrupted wireless communication.
- **AP display**: Set the panel display on or off.
- **AP display brightness**: Select the panel display brightness level.
- **AP LED**: Set the device signal light on or off.
- **AP LED brightness**: Select the device signal light brightness level.

Device Host properties:

- **Description**: Enter a description (up to 64 alpha-numeric characters) to help identify this host. On the Hosts and Devices tree the host name appears in addition to the product-supplied name. For example, "My Host (van10-X###)".
- **viewLinc Aware**: Disable this function if enabled on the viewLinc ES or other device host running on the same subnet. This is to ensure vNets connect to the correct viewLinc ES or device host.

5. Save your changes.

3.3.3 Editing Device Properties

Manage Devices

You can view and edit device properties, such as the description, alias, timeout seconds, UDP port, password, and data transfer parameters.

Depending on the devices you have installed, you can modify most properties in viewLinc . If you have a DL device already linked to a vLog audit trail, you can either edit the device properties with your vLog software, or first disable the link to the audit trail to modify properties in viewLinc .

> CAUTION
> Editing DL data logger properties automatically clears data history (sample interval, sample warmup time, enable/disable channels, calibration settings). To ensure all device data is up-to-date in viewLinc, view the linked Location trend graph to see the timestamp of the last data transfer.

Edit Device Properties

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select the device you want to edit.
3. Select **Configure > Edit Properties**.
4. Use the **Edit Device Properties** window to edit the following properties:

Vaisala RFL Data Loggers:

- **Device alias**: Optional. Enter a longer, more detailed device description (up to 64 alpha-numeric ASCII characters, less if using UNICODE characters). The alias is

displayed in viewLinc and in reports instead of the description, if the option to use aliases is set up in System Preferences.

- **Device description**: Enter a short device description (up to 16 alpha-numeric characters) to help identify this device. On the Hosts and Devices tree the device description appears in addition to the product-supplied name. For example, "My Device (van10-X###)".
- **RFL LED**: Set the device signal light on or off.
- **RFL display panel**: Set the device panel display on or off.
- **RFL units**: Display metric or standard units.

Vaisala DL Data Loggers:

- **Device alias**: Optional. Enter a longer, more detailed device description (up to 64 alpha-numeric ASCII characters, less if using UNICODE characters). The alias is displayed in viewLinc and in reports instead of the description, if the option to use aliases is set up in System Preferences.
- **Device description**: Enter a short device description (up to 16 alpha-numeric characters) to help identify this device. On the Hosts and Devices tree the device description appears in addition to the product-supplied name. For example, "My Device (van10-X###)".

It is recommended that you use the device description field to identify the model and serial number of the device.

- **COM Port**: Modify if a new COM Port is required.
- **Sample interval**: Select the frequency of data sample collection. Depending on the sample interval selected, the Log Capacity field will update the estimated log time available before overwriting historical data on the device (all data history continues to be stored in viewLinc).
- **Sample warm up time**: Set the time required to prepare for collection of data (option available if function supported by the data logger).
- **Channel [#]**: Allow a channel to start collecting data (Enabled), or prevent a channel from collecting data (Disabled).
- To modify calibration settings, see "Editing Device or Probe Calibration Properties" on page 175.

Vaisala 300 Series Transmitters:

- **Device alias**: Optional. Enter a longer, more detailed device description (up to 64 alpha-numeric ASCII characters, less if using UNICODE characters). The alias is displayed in viewLinc and in reports instead of the description, if the option to use aliases is set up in System Preferences.
- **Timeout (s)**: Specify the number of seconds to wait for data before canceling a transmission.
- **IP address**: If using DHCP, enter a new IP address.

- **TCP port**: Modify if the selected TCP port number is already in use.
- **Sample interval**: Adjust the sample rate depending on how frequently data samples are required from the monitored Location.
- To modify calibration settings, see "Editing Device or Probe Calibration Properties" on page 175.

Vaisala HMT140 Wi-Fi Data Loggers:

- **Device alias**: Optional. Enter a longer, more detailed device description (up to 64 alpha-numeric ASCII characters, less if using UNICODE characters). The alias is displayed in viewLinc and in reports instead of the description, if the option to use aliases is set up in System Preferences.
- **Device description**: Enter a short device description (up to 16 alpha-numeric characters) to help identify this device. On the Hosts and Devices tree the device description appears in addition to the product-supplied name. For example, "My Device (van10-X###)".
- **Timeout (s)**: Number of seconds to wait for data before canceling a transmission.
- **UDP port**: Auto-generated, can be modified if required.
- **Password**: Enter the device password, if this device is password-protected. The password is not saved.
- **Max blocks per beacon**: The maximum size permitted for historical data retrieval. Entering a lower number helps to conserve battery life.

> Do not change the Max blocks per beacon value for HMT140 devices without first consulting your technical support department. Changes to this setting may adversely impact battery life.

- **Retry count**: Number of times data transmission is attempted by the device if it fails to receive an acknowledgement.
- **Transmit period (min)**: Set the frequency of data transmissions, in minutes.
- **Sample interval (min)**: Set the frequency that data samples are saved to the device, in minutes.
- To modify calibration settings, see "Editing Device or Probe Calibration Properties" on page 175.

5. Save your changes.

3.3.4 Editing Channel Properties

Manage Devices

To easily identify a specific channel in viewLinc , you can edit a channel's description, alias, and preferred temperature units, if applicable.

Depending on the device you use, different properties can be modified in viewLinc. Refer to the specific device user's guide for more information.

Edit Channel Properties

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select a device channel to edit.
3. Select **Manage > Edit Properties**.
4. In the **Edit Channel Properties** window, modify the fields as required.
   - **Channel alias**: Optional. Enter a longer, more detailed channel description (up to 64 alpha-numeric ASCII characters, less if using UNICODE characters). The alias is displayed in viewLinc and in reports instead of the description, if the option to use channel aliases is set up in System Preferences.
   - **Channel description**: (DL and HMT140 series data loggers) Enter a short channel description (up to 16 alpha-numeric characters) to help identify this channel in the Hosts and Devices tree. For example, "Temperature".

Use the channel description to identify what is being measured, such as temperature, humidity, voltage, or pressure, and use the linked Location name to identify what is being monitored, such as a refrigerator reference code or laboratory name.

RFL Data Loggers:

Only the channel alias can be modified in viewLinc. All other channel properties are defined by the linked Location threshold alarm settings.

Vaisala DL Data Loggers - voltage or current channels:

- **First/Second input value**: To convert data input, set the first and second input range scaling values.
- **First/Second output value**: To convert data output, set the first and second output range scaling values.
- **Output units**: Specify the type of units to display converted input values in viewLinc.

Vaisala DL Data Loggers - Boolean channels:

- **Value when closed**: Set the value to display in viewLinc.
- **Output units**: Editable when the channel is not linked to a Location. Specify the channel units to display in viewLinc.

HMT140 Series Wi-Fi Data Loggers (with HMP110 probes):

- **Password**: If passwords are enabled on an HMT140 device (using the HMT140 Utility software) enter the password to ensure changes to HMT140 properties are updated on the device.
- **Decimal Places**: Enter the number of decimal places to display on the device.
- **High/Low Alarm Value**: High and low range alarm values that initiate a data transmission.
- **High/Low Alarm Time**: High and low alarm time specifies the number of seconds the probe is in alarm state before transmitting a beacon. The default setting, 255, disables the transmission.
- **Presentation Scale/Offset**: Editable based on channel type. Refer to the Vaisala *HMT140 Wi-Fi Data Logger User's Guide*.
- **Engineering Scale/Offset**: Editable based on channel type. Refer to the Vaisala *HMT140 Wi-Fi Data Logger User's Guide*.
- **Calibration Scale/Offset**: The primary calibration scaling (x = Scale* V + Offset). If the calibration scale or offset are modified, device calibration dates appear. Before you can save the new calibration scale or offset values, update the device calibration settings (see "Editing Device or Probe Calibration Properties" on page 175).

5. Save your changes.

4. Sites Management

The areas you monitor with devices are identified in viewLinc as Locations, and several Locations can be organized into Zones. Members of the Administrators group or other groups assigned the right, Manage Sites, can create and modify Zones and Locations in the **Sites Manager** window.

Locations are created independent of the device being used to collect data to ensure that each Location retains its assigned threshold and permission settings no matter which device is used being used to monitor conditions. If you swap a device out for calibration, or pause device alarming during a maintenance cycle, the Location retains the assigned threshold and permission settings.

4.1 Zones and Locations

When creating new Zones, first think about the areas you want to monitor (your buildings, floors, storage rooms, testing labs), then identify all the specific Locations within those areas where your devices are installed and channels record data (cabinets, refrigerators, storage racks).

For organizations with several devices installed, Zones help you identify the areas where data is collected from multiple devices or device channels. You can also create sub-zones if you monitor several areas at multiple sites.

By identifying Locations in Zones you can also:

- Swap a device easily from one Zone to another (perhaps when sending a data logger out for calibration).
- Ensure that reporting is consistent for a specific Zone, regardless of the data logger used to monitor that Location.

A fully configured viewLinc desktop provides you with an online representation of your monitored areas.

4.2 Create Zones and Locations

Sites Manager is where you set up the areas you monitor as Locations, organize them into Zones, link Locations to device channels, apply threshold alarm templates, set group access permissions, and assign schedules.

viewLinc provides you with one top-level Zone automatically, viewLinc . It can be renamed at any time, perhaps with your company name, or the name of one of the buildings you monitor.

Additional Zones and sub-zones can be set up to help identify monitored floors, rooms, warehouses, cooling or warming facilities). You can easily create Locations from device channels and add them to Zones.

For a demonstration of how to create a Zone or a Location, tours are available on the Help menu.

For more information about connecting devices and enabling or disabling channels, refer to your device-specific user's guides.

4.2.1 Creating Zones

Manage Sites

Create Zones to help organize groups of Locations.

Create a new Zone

1. In **Sites Manager**on the **Zones and Locations** tree, select the top-level folder. You can also select an existing Zones to create a sub-zone.
2. Select **Manage > Create Zone**, or right-click a Zone folder and select **Create Zone**.
3. On the **Create Zone** window, enter a unique name for the Zone, then specify:
   - **Dashboard icon**: Select an icon you want used to represent the type of Zone when displaying on the dashboard.
   - **Description**: For additional clarification, you can enter a description of this Zone (optional).
4. Select **Create**.
5. Select **Save**, or **Undo** to cancel.

If a Zone was added to an incorrect tree position, you can use your mouse to drag it to a new tree position.

4.2.2 Creating Locations

Manage Sites

Create Locations to monitor device data in viewLinc. After Locations are created, link Locations to device channels. You require Manage Devices right to link Locations to your device channels.

Use your mouse to drag a device channel from the Hosts and Devices tree to a Zone, automatically creating a new linked Location (see "Creating Linked Locations Automatically" on page 49).

Add a Location

1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Zone or Location.
2. Select **Manage > Create Location**, or right-click a Zone folder and select **Create Location**.
3. On the **Create Location** window, enter a name for the Location.

Use the Location name to describe the area being monitored. If a device is swapped out or re-located, the Location description is retained.

4. Enter Location properties:
   - **Measurement type**: Select the value being measured. If the type is Temperature, select the preferred temperature unit to display in browser windows (°C or °F, or the system default, set in the System Preferences window) .
   - **Decimal places**: Enter the number of decimal places to display.
   - **Description**: For additional clarification, you can enter a description of this Location (optional).
5. Select **Create**.
6. Select **Save**, or **Undo** to cancel.

To enable data reporting and alarm monitoring in viewLinc, link this Location to a device channel.

4.3 Link Device Channels to Locations

Link device channels to Locations to monitor recorded device data in viewLinc . Linking a device channel to a Location also allows you to maintain consistent data and alarm history for a monitored area, even if the devices used for monitoring change (a device may be swapped out to monitor another area, or sent for calibration or repair).

Only device channels linked to Locations can generate alarms.

When data monitoring for a specific area is no longer required, you can easily unlink a device channel and link it to a different Location (see "Unlinking/Relinking Locations and Channels" on page 163).

For audit trail security, you cannot delete a Location that was linked to a device channel; however, unused Locations can be unlinked and hidden from view (see "Deactivating Locations" on page 167).

4.3.1 Linking Channels to Locations

Manage Sites

Before you can start monitoring conditions with viewLinc , device channels must be linked to viewLinc Locations. To create a new Location automatically from a new channel, see "Creating Linked Locations Automatically" on the facing page.

Full Control permission is required for all Locations being linked.

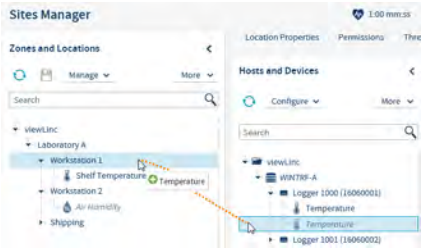
Link a New Channel to a New Location

1. In **Sites Manager** on the **Zones and Locations** tree, select an unlinked Location (displayed in *italicized* text.
2. Select the **Hosts and Devices** tab.
3. In the **Hosts and Devices** tree, select an unlinked channel (it is displayed in *italicized* text) with a matching measurement type.
4. Select **Configure > Link Channel**.
5. In the **Link Channel to Location** window, choose when you want this new Location to start monitoring data.
   - **Start now**: Data is recorded starting from the next available sample time.
   - **Start from earliest available link time**: Include all channel data history recorded by the device. This option is useful if the channel has been in use but unlinked for a period of time.
   - **Start from a specified time**: Set a specific time to start recording data history. You may want to use this option to delay the start of recorded history.
6. Select **Link**.
7. Select **Save**.

4.3.2 Creating Linked Locations Automatically

Manage Sites

Use the drag and drop feature to create new Locations that are automatically linked to device channels.



Full Control permission is required for the Zone where the new Location will be created.

Create a Location from an Unlinked Device Channel

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. In the **Hosts and Devices** tree, select the new device.
3. Select an unlinked device channel, then drag it over to the Zone where the new Location will be created. The icon changes to ⊕ when the position is valid.
4. In the **Link Channel to Location** window, choose when you want this new Location to start monitoring data:
   - **Start now**: Data is recorded starting from the next available sample time.
   - **Start from earliest available link time**: Include all channel data history recorded by the device. This option is useful if the channel has been in use but unlinked for a period of time.
   - **Start from a specified time**: Set a specific time to start recording data history. You may want to use this option when you want to delay the start of recorded history.
5. Select **Link**.
6. To define a unique Location name, select the new Location and right-click to select **Edit Properties**.
7. Select **Update**, then select **Save**.

4.3.3 Viewing Channel Link History

Manage Devices

You require at least View permission to see Zones and Locations in Sites Manager (see "Applying Group Permission to Zones" on page 103).

View Link History

1. In **Sites Manager**, navigate the **Zones and Locations** tree to select a linked Location.
2. On the **Location Properties** tab select the Location on the grid.
3. Select the **Channel History** tool bar button, .

4. Review historical details the **Linked Channel History** window:
   - **Link Start**: Unlimited indicates this channel has remained linked and has continuously monitored data at the linked Location since the channel started monitoring data.
   - **Link End**: Unlimited indicates this channel is still linked to the Location and is monitoring data continuously.

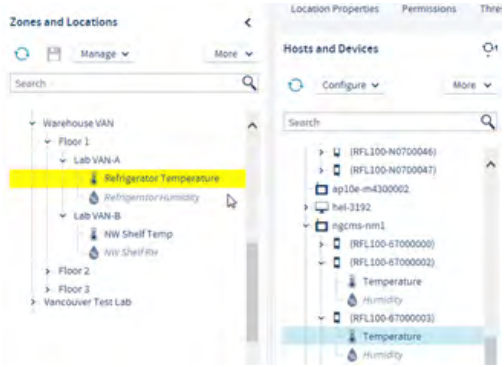
4.3.4 Finding Linked Channels/Linked Locations

Manage Sites

If you have a large installation with many devices and channels, try viewLinc 's Find in Tree feature. You require View permission for all linked Locations.

Find a Location's Linked Channel - Sites Manager

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. Navigate to a Location in the **Zones and Locations** tree.
3. Select **Configure > Find Linked Channel** or right-click and select **Find Linked Channel**. A yellow highlight bar appears temporarily in the **Hosts and Devices** tree to indicate the linked channel.



Find a Channel's Linked Location - Sites Manager

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. Navigate to a channel in the **Hosts and Devices** tree.
3. Select **Configure > Find Linked Location** or right-click and select **Find Linked Location**. A yellow highlight bar appears temporarily in the Zones and Locations tree to indicate the linked Location.

If the yellow highlight does not appear, you do not have permission to view the linked Location/channel.

Find a Location's Linked Channel - Sites

1. In **Sites** navigate to a Zone in the **Zones and Locations** tree.
2. On the **Status** tab select a Location.
3. Select the **Find in Tree** toolbar button, , or right-click on the Location and select **Find in Tree**. A yellow highlight bar appears temporarily in the Zones and Locations tree to indicate the corresponding Location.

4.4 Build Dashboards

Create a dashboard to help your team become familiar with the physical location of data points (viewLinc Locations). A dashboard can be a facility map, a drawing, photo, or other image file (.png or .jpg) representing a specific area.

After you add an image, select and place sub-zones or individual Locations on the dashboard.
You can create dashboards to display Location data without a background image, for larger, more remote screen displays.

Dashboard tours are available on the Help menu.

4.4.1 Building Dashboards

Manage Sites

Upload a dashboard image file from any desktop or network location, in .png or .jpg format.
You can add a dashboard image to a Zone or a Location, or to a view (a view you created or are permitted to edit).

You require Full Control permission to add a Zone or Location dashboard image, or to add dashboard images to views created by others.

Add a Dashboard Image

1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone or a Location (or in **Views Manager** on the **Views** tree, select a view).
2. Select the **Dashboard** tab, then select **Add Dashboard Image**.
3. Browse to find an image, then select **Add**. The image automatically resizes to fit the screen. If it is necessary to resize the image, adjust the borders with your mouse, starting from the bottom right corner.
4. Select **Save**.

Add Zones and/or Location Data Points

Only sub-zones and child Locations of a Zone can be added as data points on the dashboard image.

1. In **Sites Manager** on the **Zones and Locations** tree, or in **Views Manager** on the **Views** tree, select a Zone or Location you want to display on the dashboard.
2. Click and drag the Zone or Location to the dashboard. When you drag the Zone or Location, an icon appears to indicate when it can be added to the dashboard, .
   - When a sub-zone is added to the dashboard, it displays with its assigned dashboard icon, or, if one was not assigned, the default folder icon. Double-click the icon to view Location data.
   - When a Location is added to the dashboard, it displays the current numeric data reading, with the icon color indicating current condition severity (as set in the threshold alarm template).
3. Select **Save**.

4.4.2 Changing Dashboard Display Settings

Manage Sites

Modify the contents of the dashboard and the appearance of Zone and Location data points.

You require Full Control permission to modify the dashboard display for a selected Zone, Location, or view.

Change the Dashboard Image

Changing the dashboard image does not delete your data points (but you may need to adjust their position on the new image).

1. In **Sites Manager** on the **Zones and Locations** tree, select the Zone or Location you want to modify (or in **Views Manager** select a view).
2. Select the **Dashboard** tab, then select **Add Dashboard Image**, .

3. Enter the file location or use the **Browse** button to navigate to the image you wish to use, then select **Add**.
4. Save your changes.

Change Zone Font

You may want to apply the same settings to all Zones on a dashboard, or modify settings for specific Locations that are important to you.

Change the font size for all Zones on the selected dashboard:

1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone.
2. On the **Dashboard** tab, select **Settings > Dashboard Zone Settings**.
3. In the **Dashboard Zone Settings** window, select the font size in the **Value** column.
4. Save your changes.

Change the font size on an individual dashboard Zone:

1. In **Sites Manager** on the **Dashboard** tab, right-click on a Zone and select **Edit Display Settings**.
2. In the **Edit Zone Display Settings** window, choose a font size from the drop-down list, or select **Set to default** to change it to use dashboard preferences.
3. Save your changes.

Change Location Font Size, Icon, or Color

You may want to apply the same settings to all Locations on a dashboard, or modify settings for specific Locations that are important to you.

To set Location preferences for all Locations on the selected dashboard:

1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone with Locations set on a dashboard.
2. On the **Dashboard** tab, select the **Settings > Dashboard Location Settings**.
3. In the **Dashboard Location Settings** window, select a property to modify. Select a row in the **Value** column to see available options.
4. Save your changes.

To set Location preferences for an individual Dashboard Location:

1. In **Sites Manager** on the **Dashboard** tab, right-click on a Location to modify, and select **Edit Display Preferences**.
2. In the **Edit Location Display Preferences** window, select a property to modify. Select a row in the **Value** column to see available options.
3. Save your changes.

Change Location Description Display Options

To set Location description display options for all Locations on the dashboard:

1. In **Sites Manager** on the **Dashboard** tab, select **Settings > Dashboard Location Settings**.
2. In the **Dashboard Location Settings** window, modify the description display options:
   - **Description**: Choose to display the Location description (as specified in Location Properties) above, below, or beside the data reading.
   - **Description format**: Display only the Location name or Location and Zone name.
3. Save your changes.

To set Location Description display options for an individual Location on the dashboard:

1. In **Sites Manager** on the **Dashboard** tab, right-click on a Location to modify, and select **Edit Display Settings**.
2. In the **Edit Location Display Settings** window, modify the description display options.
   - **Description**: Choose to display the Location description (as specified in Location Properties) above, below, or beside the data reading.
   - **Description format**: Display only the Location description or Location and Zone descriptions.
   - **Set to Default**: Select to accept all globally-set dashboard preferences (see step).
3. Save your changes.

Set up a Dashboard for Wall-mounted Monitors

1. In **Sites Manager** on the **Dashboard** tab, select **Settings**.
2. Choose to display Location data in 1-, 2-, 3-, or 4-columns of tiles. A greater number of Locations may require a greater number of columns. Test each option to determine which display option suits your needs most effectively.

> When a column tiling option is selected, the uploaded dashboard image fades into the background.

3. Save your changes.

4.4.3 Deleting Dashboard Images or Data Points

Manage Sites or Manage Views

You can keep dashboards up-to-date with changes to the number of facilities monitored or the addition of more monitored areas. Any user can modify the dashboard images they add in **Views Manager**, or for the views they are permitted to edit.

> Users belonging to groups with Manage Sites right and Full Control permission can modify dashboards in Sites Manager. Users belonging to groups with Manage Views right and Full Control permission can modify dashboards in Views Manager.

Delete a single dashboard data point

1. In **Sites Manager** on the **Zones and Locations** tree (or in **Views Manager** on the **Views** tree), select the Zone or Location dashboard you want to modify.
2. On the **Dashboard** tab, right-click a dashboard data point then select **Delete**.
3. At the prompt, select **Delete**.
4. Save the change, or select Undo to cancel.

Delete a dashboard image and/or all data points

1. In **Sites Manager** on the **Zones and Locations** tree (or in **Views Manager** on the **Views** tree), select the dashboard you want to delete.
2. On the **Dashboard** tab select **Clear Dashboard**.
3. Choose to delete either the Zones and Locations or the dashboard image, or both, then select **Clear**.
4. Save the change, or select **Undo** to cancel.

5. Groups and Users

All viewLinc users must be assigned to one or more groups. Each group is assigned rights that define the viewLinc windows the users in the group can access.

Users can belong to more than one group. To help get you started, there are two default groups available:

Administrators: A user added to the viewLinc Administrators group has all rights assigned. They can access all windows and perform any function within viewLinc .

Everyone: All new users are automatically assigned to the Everyone group. This group has access to the Overview, Sites, Reports, Alarms, Views Manager, and Events windows.

The Zones and Locations users are permitted to view and/or modify within a window are set with permission levels (see "Applying Group Permission to Zones" on page 103).

Members of the Administrators group are automatically granted Full Control permission to all Zones and Locations. They can also perform system-level changes, such as restart viewLinc Enterprise Server or a device host, acknowledge system alarms, acknowledge all off alarms, permanently delete Zones or Locations, and fix the validation status or remote lock on DL data loggers.

Watch these tours: Rights and Permissions, Create a Group, and Create a User, available on the Help menu.

5.1 Rights

Rights are assigned to groups, and give all users in a group access to functional areas in viewLinc. Groups can be given one or more rights, and users can be members of one or more groups. By default all new users are automatically assigned to the Everyone group with the right, Manage Events.

Users created in an earlier version of viewLinc retain any rights that were assigned in the earlier version. To manage access to different functional areas of viewLinc more effectively, remove legacy user rights and assign the user to a group with the same rights.

Once removed, legacy user rights cannot be reapplied.

CAUTION
Users assigned to the viewLinc Administrators group are automatically granted these additional system-level functions:

- Undo remote-lock on DL data loggers
- Restart viewLinc
- Test network communications
- Acknowledge inactive alarms
- Acknowledge system alarms
- Correct security status
- Pause host alarms
- Add users to the Administrators group
- Edit user profiles of Administrators group members

Table 10 Rights Definitions

Name	Access to	Description
Manage Alarm Templates	Alarm Templates	Add or edit alarm templates (threshold alarms, device alarms, notifications, email and SMS content, schedules).
Manage Devices	Sites Manager, Hosts and Devices tab	Add, edit, deactivate, or lock devices; Modify host alarm settings. Requires Full Control permission on linked Locations.
Manage Events	Overview, Sites, Reports, Alarms, Views Manager, and Events	View, add events and event comments; Create personal views.
Manage Reports	Reports	View, print, copy, or edit reports created by others (all users can add, edit or delete their own reports).
Manage Sites	Sites Manager, Hosts and Devices tab	Add, edit, or deactivate Zones and Locations; Swap devices with linked Locations; Add threshold alarms and schedules; Assign group permission to Zones; Unlink channels from Locations.
Manage System	System Preferences	Set or edit system-wide preferences; Add predefined comments; Add or modify users and groups.
Manage Views	Views Manager	Add, edit, or share personal or other user's views.

Group rights are refined by permissions. While rights allow groups to complete specific tasks in viewLinc windows, permissions control the Zones and/or Locations a group can view, configure or manage (see "Permissions" on page 101).

5.2 Groups

5.2.1 Adding Groups

Manage System

Groups define the areas of viewLinc you want specific users to access.

To allow users in a group to view or manage Zones and Locations, assign group permission to the Zone (see "Permissions" on page 101).

Add a Group

1. In the **Users and Groups** window, select the **Groups** tab, then select **Add**.
2. In the **Add Group** window on the **Properties** tab, enter a name for the group. You can use the **Description** field to describe the rights you will assign to the group, or the primary job function of the group.
3. Select the **Rights** tab, then select **Add Right**. The users in the group are automatically given the right, Manage Events.
4. To add users to this group, select the **Members** tab then select users to add the group.
5. Select **Save**.

To make changes to groups, see "Groups and Users" on page 159.

5.3 Users

5.3.1 Adding Users

Manage System

Before you add users to your system, determine which rights the user will need. Users are given rights through the group or groups to which they are assigned.

Only members of the Administrators group can add new users to the Administrators group.

Add a User

1. In the **Users and Groups** window select the **Users** tab.
2. To avoid adding a duplicate user account, check that the user does not already exist
   a. In the **Search** field, enter the user name or full name, then select the search icon, .
   b. Select the 'x' to clear the field and display the full list of users.
3. Select **Add**.

4. On the **Properties** tab, complete the following:
   - **User name** and **Full name**: Enter a user name to use on the login page, and a full name, for internal reference (your company may use abbreviated names for login credentials). If this user will log in with Windows authentication, enter their Windows user name then select **Windows** as the Authentication method.
   - **Email**, **Mobile number**: Add the user's contact details to receive reports and alarm notifications, and send alarm acknowledgements. Enter a mobile number which includes the '+' sign, the country code and area code. For example, +44 604 273 6850 (dashes, spaces or periods can be included, but are not required).
   - **Send alarm notifications**: (available if schedules functionality is enabled) Choose a schedule to define when to send alarm notifications to this user.
     - **Always**: This user will receive notifications at any time of day or night.
     - **According to schedule**. If this user is a member of a group set up to receive alarm notifications, select the schedule which defines when this user should receive notifications.
     - **Never**: This user will not receive alarm notifications, even if they are assigned to a group set up to receive alarm notifications.
   - **viewLinc PIN**: Enter a unique PIN number, using 4 to 6 digits between 1000 and 999999. This number is required by viewLinc when receiving email or SMS alarm acknowledgements from the user's email address or mobile device.
   - **Preferred language**: Choose the language to use when user generates a report or viewLinc sends this user reports and alarm notifications. If no language selected, the system default language is used. Users can select any language.

     The language selected when logging in to viewLinc applies to the viewLinc display only.

     - **Audible alarms**: Choose to enable audible alarms on the user's device (desktop PC) when logged in to viewLinc. Audible alarms must be enabled in System Preferences (see "Audible Alarming" on page 89).

       Only the most recently generated alarm initiates a sound. The user can turn off an audible alarm in the main viewLinc window by clicking the audible alarm icon 🔊.

5. Choose the method of **Authentication**:
   - **viewLinc**: Select this option to set a unique viewLinc password, then enter a new password in the **Password** and **Confirm Password** fields.
   - **Windows**: Select this option to allow user to log into viewLinc with their current Windows password. Check that the Windows user name is entered in the **User name** field (see step 4), and then specify the **Domain**.

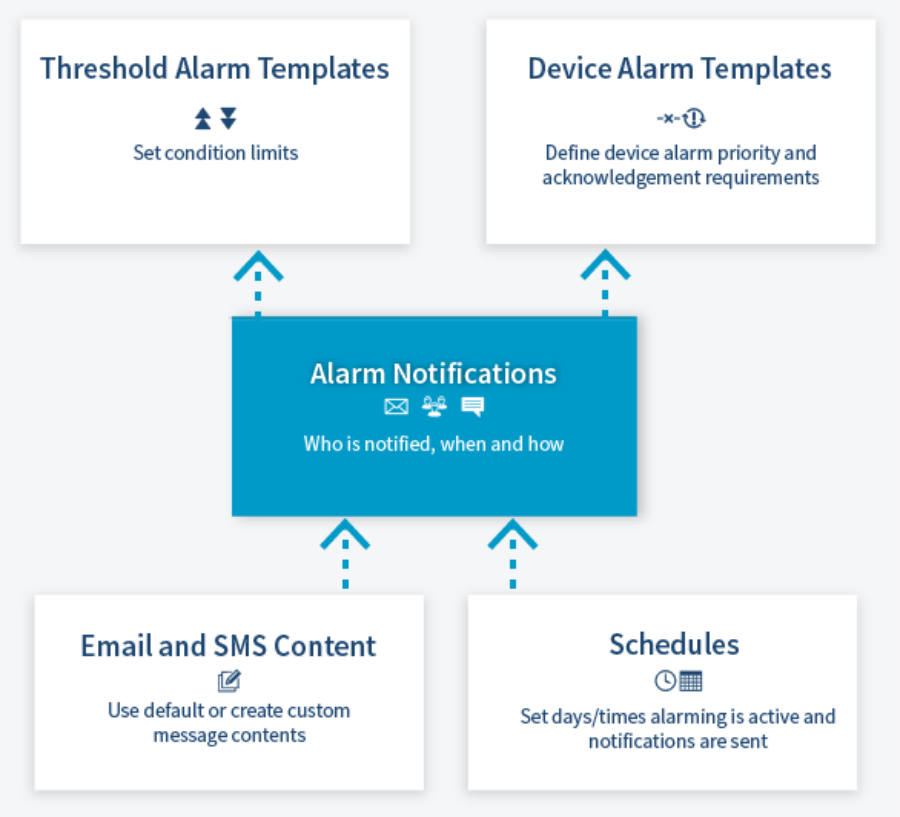
You can require that users re-confirm their identity (re-enter their user name and password) whenever a change is made in viewLinc, or after a set number of minutes. See "Authenticate System Changes" on page 93.

6. On the **Groups** tab, assign the user to a group. In the **Selected** column check all the groups you want the user to belong to. Review the **Rights** column to ensure you are giving this user the rights they need.
7. Select **Save**.

To make changes to the user profile at a later time, see "Groups and Users" on page 159.

6. Alarm Templates

Alarm templates are used to define the alarm condition and notification requirements for Locations and devices.



- Create **threshold alarm templates** to specify the conditions that should trigger an alarm, then apply the template to one or more Locations.
- Default **device alarm templates** are provided and assigned to each new device connected to your viewLinc system. They specify how and when you want to be notified of device status. The default templates can be modified, or you can create new device alarm templates.
- Create **alarm notification templates** to define who should be notified in the event of a threshold or device alarm, the information that should be distributed in email and SMS messages, whether other visual or auditory cues should run to notify a general audience (flashing lights or sounds),

and whether the notified individual must acknowledge an alarm. Alarm notification templates are applied to Locations using threshold alarm templates.

- Default **email and SMS templates** are provided. They contain standard information issued from viewLinc about different alarm conditions in your network. The default content can be modified.
- (Optional) Create **schedules** to define when Location thresholds should be monitored, and when you want alarm notifications sent. You can set up a day schedule and an evening schedule to send notifications to different teams, or set schedules to prevent users on holiday from receiving alarms. Schedules functionality must be enabled, see "Schedules Functionality" on page 89.

Alarm Templates can be added/modified by users assigned to groups with **Manage Alarm Templates** right.

6.1 Types of Alarms

Alarms indicate issues that may require immediate resolution, provide notification about interruptions in communication between devices or hosts and the viewLinc Enterprise Server, updates about system status or configuration changes, and reminders about upcoming maintenance requirements.

Alarms are viewable in the Alarms window (device and system alarms and threshold alarms for Locations you have permission to view), the Sites window (device and threshold alarms for the Locations you have permission to view), or in the Overview window (device and threshold alarms for the Locations assigned to your views).

All alarm events are recorded in the event log, to ensure a secure audit trail.

Table 11 Alarm Descriptions

Alarm Type	Description
System	• Event log validation alarms indicate whether changes have been made to the event log from outside the viewLinc system. • Database validation alarms indicate database corruption or configuration changes made to the historical database originating outside viewLinc. • System alarm settings are configured in System Preferences.
Threshold	• Threshold alarms indicate excessive condition changes in a monitored environment. • Threshold alarm settings are defined in threshold alarm templates and are then applied to Locations.
Device	• Device configuration alarms indicate interruptions collecting device data. • Host configuration alarms indicate synchronization errors between a device host or access point and the viewLinc Enterprise Server. • Device validation alarms indicate corruption in the device memory.

Alarm Type	Description
	• Device calibration alarms indicate upcoming calibration service requirements • Host communication alarms occur when a device host or access point loses connection with the viewLinc Enterprise Server. • Device communication alarms indicate a communication error between a host computer, access point or viewLinc Enterprise Server, and its connected devices. • Device alarm settings are defined in templates.

6.2 System Alarms

System alarms occur automatically when viewLinc detects changes made outside standard desktop operation. It is issued to warn of possible database tampering.

If you receive a system alarm notification (email or SMS), investigate possible causes, acknowledge the alarm notification, and, if required, follow your company's standard operating procedures (SOPs) to resolve the issue.

Critical system errors and warnings are automatically sent to the IT Network manager, and you have the option of sending additional email or SMS system alarm notifications to members of the default Administrators group.

You can modify the content of system alarm email and SMS messages (see "Email and SMS Content" on page 85).

Types of System Alarms

- Database Validation: This alarm indicates device tampering such as a change to the configuration database, data modifications (a possible external script), or data corruption.
- Event Log Validation: This alarm indicates database security interruptions, such as a change made to the event log from outside the viewLinc system.

To define system alarm settings, see "System Alarm Preferences" on page 97.

6.3 Threshold Alarms

Thresholds define the accepted condition limits required to preserve the quality of your inventory or production environment. Threshold condition limits are saved as threshold alarm templates, and can be applied to one or more Locations (see "Creating Threshold Alarm Templates" on the next page).

If condition limits are exceeded, viewLinc can activate an alarm, and, optionally, send one or more alarm notifications (see "Alarm Notifications" on page 79).

Threshold alarm templates define:

- Values associated with one or more conditions (Low-Low, Low, High, High-High, RoC, Alarm off margin).
- Color codes to reflect condition severity.
- One or more threshold alarm activation delays.
- Whether the alarm needs to be acknowledged.

You can apply one or more threshold templates to a Location, depending on how often you need to change threshold values, or how frequently you want to know about changing conditions.

You can also specify the alarm off margin so viewLinc will ignore condition changes within a specified temperature range and persist sending alarm notifications while conditions remain in this range.

Up to 5 threshold settings can be saved as a single template and then assigned to one or more Locations. If the settings are modified, the new settings apply to all Locations to which they have been assigned.

Example

If you have a monitored area that should remain between 10°C and 12°C, you could set up one or all of these levels:

- Low threshold set at 10.5 °C to warn when the temperature is close to the Low-Low threshold
- Low-Low threshold set at 10 °C lasting for more than 1 minute to trigger specific alarm settings for the breach of the lower threshold.
- High threshold set at 11.5 °C to warn when the temperature is close to the High-High threshold.
- High-High threshold set at 12 °C lasting for more than 5 minutes to trigger specific alarm settings when upper threshold exceeded.
- Rate of Change set to 0.25 °C/min to warn when temperature increases or decreases rapidly.

6.3.1 Creating Threshold Alarm Templates

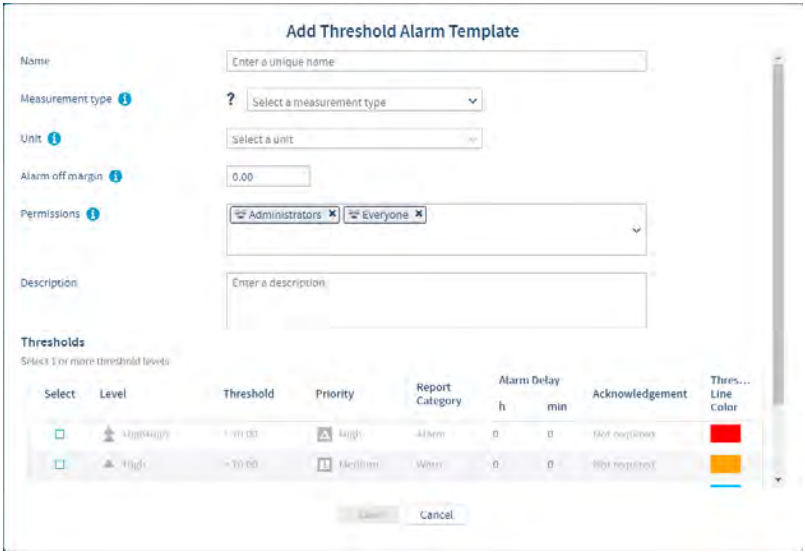
Manage Alarm Templates

Threshold settings (high and low condition limits) are stored in reusable templates which can be applied to one or more Locations. These threshold settings define the conditions that you want to trigger alarms at a specific Location.

To learn more about threshold alarm templates, see "Threshold Alarms" on the previous page.

Create a Threshold Alarm Template

1. In the **Alarm Templates** window select the **Threshold Alarms** tab.
2. Select **Add > Add Threshold Alarm Template**. To copy settings from an existing template, select the template, then **Add > Copy Selected Threshold Alarm Template**.



3. In the **Add Threshold Alarm Template** window, enter a unique name for the new template and then set the template details:
   - **Measurement type**: Select the type of measurement monitored at selected Location(s).
   - **Unit**: Choose the units you want used to record the measurement type.
   - **Alarm off margin**: Specify an active alarm range. If an alarm condition fluctuates within the active alarm range, the alarm does not turn off. For example, if the high threshold is 10 °C, and the alarm off margin is 1 °C, the alarm will not turn off until the temperature falls to or below 9 °C.
   - **Permissions**: Select the groups authorized to modify or apply this template to Locations.
   - **Description**: (optional) Provide more details about the threshold template settings.
4. Enable one or more threshold levels:
   - **Select**: Select the threshold levels you want to activate.
   - **Level**: 5 threshold levels are available, but you only enter values for the levels that are selected.
   - **Threshold**: Set a numerical value manually or with the up/down arrows.
   - **Priority**: Set the response priority for the threshold value. Priority value provides users a visual clue about the severity of conditions in the Alarms window.
   - **Report Category**: This setting defines whether alarms triggered by the threshold level appear on reports as Alarms or Warnings. You can set report options to include or exclude these categories, depending on your reporting requirements.
   - **Alarm Delay** : Set a delay if you want to prevent a threshold alarm from triggering immediately after threshold is exceeded. You may want to set a delay if you want an alarm triggered only if the condition persists beyond a delay period.

5. Select **Save**.

To apply a threshold alarm template to a Location, see "Applying Threshold Alarm Templates to Locations" below.

6.3.2 Applying Threshold Alarm Templates to Locations

Manage Alarm Templates

After creating threshold alarm templates, you can apply the templates to Zones or to specific Locations. You can apply and enable up to 6 threshold alarm templates on one Location, to accommodate different monitoring needs at different times.

To create a threshold alarm template, see "Creating Threshold Alarm Templates" on page 66.

To apply a threshold alarm template to a Location, you require Configure Alarms permission or higher for the selected Location.

Apply a Threshold Alarm Template to a Location

1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone or a Location (hold the [Ctrl] key to select multiple Zones/Locations).

Threshold alarm levels are ignored if they fall outside the Location's linked device measurement range.

2. Select **Manage > Add Threshold Alarms**. Complete the fields in the **Add Threshold Alarm** window:
   - **Location**: Verify that you are adding a threshold alarm template to the correct Location(s). If you selected a Zone, the threshold alarm template is applied to all Locations in the Zone.
   - **Status**: Set status to Enabled to actively monitor thresholds on selected Location(s). If you do not want the threshold alarm settings activated on this Location until a later time (you may have more configuring to do), set as Disabled.
   - **Send to device**: Choose whether to send threshold level information to an RFL100-series or HMT140-series data logger. Select the threshold levels to display using the checkboxes in the **Alarm on Device** column. Only 2 levels can display on an HMT140 data logger (1 high and 1 low).
   - **Device password**: If the selected Location is linked to an HMT140 device with password functionality enabled, enter the password to apply threshold settings.
   - **Measurement type**: Select the type of conditions being measured at this Location.
   - **Threshold alarm template**: Select an available threshold alarm template. The threshold template details appear in the grid.

3. For each alarm level, update threshold alarm settings:
   - **Alarm on Device**: For RFL100 and HMT140 series data loggers. Choose which threshold level(s) to display (an HMT140 can accept 2 levels, one high and one low; RFL can accept 4 levels). For areas with several devices, you may want to display only the most critical threshold levels. If the device is moved, threshold levels remain enabled on the device.

     The **Send to device** option must be enabled to allow threshold levels to alarm on a device.

   - **Alarm Notification Template**: Select an alarm notification template to use if this threshold is exceeded. Alarm notification templates define who is notified and when. See "Alarm Notifications" on page 79.
   - **Message or Comment**: All threshold alarm notifications use content specified in viewLinc's default email and SMS content templates. Use this field to insert custom text in place of the [AlarmMessage] and [Comment] macros embedded in the content templates. To learn more about message content, see "Email and SMS Content" on page 85.
4. Select **Save**.

To copy a threshold template to other Locations using the same measurement type:
1. On the **Threshold Alarm Settings** tab, select a threshold.
2. Select **Copy selected threshold alarm settings**.
3. On the **Zones and Locations** tree, select a Zone or Location.
4. On the **Threshold Alarm Settings** tab, select **Paste to the selected Zone or Location**.

6.3.3 Editing Threshold Alarm Templates

Manage Alarm Templates

Adjust threshold levels for all Locations using the same threshold alarm template.
To learn more about threshold alarm templates, see "Threshold Alarms" on page 65.

CAUTION
Changes to a threshold alarm template affect all Locations using the template.

Edit a Threshold Alarm Template

1. In **Alarm Templates** select the **Threshold Alarms** tab.
2. Select the template you want to modify, then select **Edit**.
3. Select **View Locations** to verify that changes can be applied to all Locations currently using the template.
4. Modify the editable settings. For information on all field options, see "Creating Threshold Alarm Templates" on page 66.
5. Select **Save**.

6.3.4 Editing Location Threshold Alarm Settings

Manage Alarm Templates

Modify threshold alarming status, threshold alarm template or alarm notification template used for individual or multiple Locations.

To modify threshold alarm settings you require Configure Alarms permission or higher for the selected Location(s).

Edit Threshold Alarm Settings

1. In **Sites Manager** in the **Zones and Locations** tree, select the Zone or Location you want to modify ([Ctrl]+click to select multiple Zones and Locations).
2. Select the **Threshold Alarm Settings** tab, and then select one or more threshold alarm rows .
3. Select **Edit threshold alarm settings**. For information on editable options see, "Applying Threshold Alarm Templates to Locations" on page 68.

CAUTION
If modifying settings for multiple Locations with different settings applied, indicated with the icon, , it is recommended that you leave mixed settings unchanged.

4. Select **Save**.

6.3.5 Deactivating/Reactivating Threshold Alarms

Manage Alarm Templates

Threshold alarm settings cannot be deleted, but they can be deactivated. Once deactivated, the threshold alarm settings row is hidden from view. Deactivated threshold alarm settings can be reactivated on the Location at any time.

To prevent a Location from using applied threshold alarm settings temporarily (useful if you need to store more than 6 threshold alarm settings with a Location), simply disable a threshold alarm setting (see "Disabling/Enabling Threshold Alarm Settings" on page 169).

Deactivate Location Threshold Alarming

1. In **Sites Manager** select a Location in the **Zones and Locations** tree.
2. On the **Threshold Alarm Settings** tab, select the threshold you want to deactivate.
3. Select **Deactivate**.
4. At the prompt, select **Deactivate**.

To view a deactivated threshold, select **View > Include Deactivated Threshold Settings**.

Reactivate Location Threshold Alarming

1. In **Sites Manager** select a Location in the **Zones and Locations** tree.
2. On the **Threshold Alarm Settings** tab select **View > Include Deactivated Threshold Settings**.
3. From the list of threshold alarm templates that appear, highlight the threshold you want to reactivate, then select **Activate**.
4. At the prompt, select **Activate**.

6.4 Device Alarms

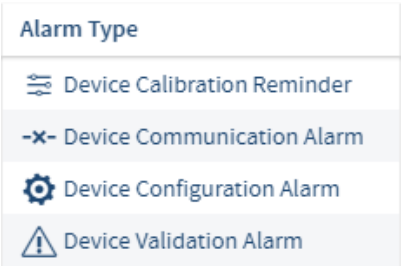
Communication between devices and the viewLinc Enterprise Server is essential for continuous monitoring of conditions. To ensure you are notified of any issues that require attention, configure the default host and device alarm templates according to your company's notification requirements.
In Sites Manager, the Device Alarms tab displays a list of the device alarm templates applied to your devices. You can modify the default device alarm templates, or create new device alarm templates in the Alarm Templates window.

6.4.1 Types of Device Alarms

Four (4) device alarm templates are automatically applied to each monitoring device connected to the viewLinc Enterprise Server (data loggers and transmitters). Two alarm templates are applied to hosts (Device Host computers and access points).
Device alarm templates contain default (and modifiable) settings which define:

- Alarm priority
- Alarm notification delay
- Acknowledgement requirements
- Group authorized to modify device alarm settings

The default device alarm templates assigned to devices can be modified. You can also create new device alarm templates with unique settings for specific Locations.



Device or Host Communication Alarms

Device communication alarms occur when communication is interrupted between a host computer, access point or viewLinc Enterprise Server, and its connected devices.

Host Communication Alarms occur when a device host or access point loses its connection to the viewLinc Enterprise Server. Communication alarms are like a system health test, alerting you if there is a problem that might disrupt viewLinc monitoring and alarming.

By default, there is one communication alarm template preconfigured for each host and each device.

Communication alarm templates control:

- How alarm notification displays
- Who is notified
- When alarm notification is initiated
- Whether alarm acknowledgement is required

If a device host computer or access point host goes offline, only a host communication alarm is generated. Connected devices do not generate device communication alarms.

Device or Host Configuration Alarms

If you receive a device configuration alarm, this indicates that your device is configured incorrectly or has stopped recording data history. Host configuration alarms are triggered when there is a synchronization error between a host and it's connected devices.

Here are a few examples:

- An internal device error is preventing data history from recording.
- viewLinc detects a device's stop mode is not set to Wrap when full (DL Loggers).
- viewLinc cannot retrieve historical samples because a device is configured with a delayed data recording start (DL Loggers).
- viewLinc detects a device that is locked to another system.
- A device may have a disabled channel that is linked to Location.
- IR sensor sending too many transmissions which may drain battery.

The default delay before viewLinc sends a device configuration alarm notification is 60 seconds You can adjust the notification delay and other device configuration settings in viewLinc .

Device Validation Alarms

If the validation memory in a device is corrupted or has been modified, this alarm notification will advise that you contact your Vaisala technical support representative for assistance.

Device Calibration Alarms

A device calibration alarm is an intermittent notification sent when a Vaisala data logger or probe is due for calibration.

By default, you receive notifications at the following intervals: 3 months and 1 month before the calibration due date, then again on the scheduled recalibration date (auto-generated for 1 year from last calibration date). This alarm remains active, even after acknowledgement, until the device is recalibrated (for more information contact Vaisala Calibration Service Center).

You can set the default calibration duration for all data loggers in **System Preferences**, or, if you have Manage Devices right, modify the calibration duration for a specific data logger or probe in Sites Manager (**Hosts and Devices > Configure > Edit Properties**).

6.4.2 Host Communication Alarm Settings

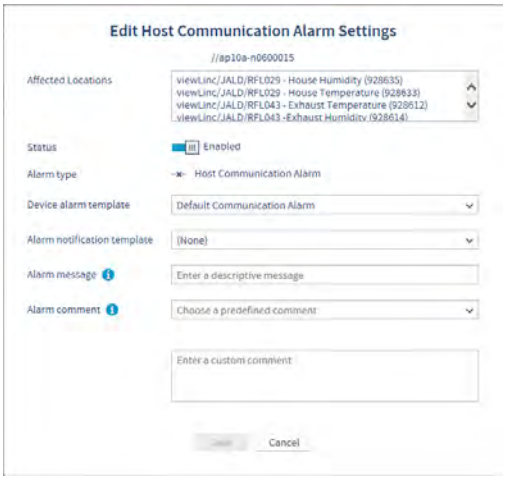
Manage Alarm Templates

By default, viewLinc assigns a host communication alarm template to all new hosts added to the viewLinc monitoring system. Host communication alarm settings can be modified, and an alarm notification template can be added. Together, these templates define when a host communication alarm is activated, who is notified, and what alarm priority should be assigned (for reporting purposes).

To view the properties of default or custom device alarm templates, see "Editing Device Alarm Templates" on page 78.

Edit Host Communication Alarm Settings

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree select one or more hosts.
3. Select **Configure > Host Communication Alarm Settings**.



4. Set properties:
   - **Status**: Host communication alarms can only be generated when status is enabled.
   - **Device alarm template**: Accept the default template, Default Communication Alarm, or select a custom template from the drop-down list. Template selection applies to all selected hosts.
   - **Alarm notification template**: Select a custom template from the drop-down list. Notifications are not sent if no alarm notification selected (alarms are always indicated on the Location Alarms tab in Sites or Overview, or in the Alarms window).
   - **Alarm message**: (Optional) Enter a descriptive message to include in email or SMS notifications. This text is used in place of the [AlarmMessage] macro in the related default email templates, or can be added to a custom email or SMS template.
   - **Alarm comment**: (Optional) Select from the list of available predefined comments, or enter a custom comment to include in email or SMS notifications. This text is used in place of the [Comments] macro in the related default email templates, or can be added to a custom email or SMS template.
5. Save your changes.

6.4.3 Host Configuration Alarm Settings

Manage Alarm Templates

By default, viewLinc assigns a host configuration alarm template to all new hosts added to the viewLinc monitoring system. Host configuration alarm settings can be modified, and an alarm notification template can be added. Together, these templates define when a host configuration alarm is activated, who is notified, and what alarm priority should be assigned (for reporting purposes).

To view the properties of default or custom device alarm templates, see "Editing Device Alarm Templates" on page 78.

Edit Host Configuration Alarm Settings

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree select one or more hosts.
3. Select **Configure > Host Configuration Alarm Settings**.
4. Set properties:
   - **Status**: Host configuration alarms can only be generated when status is enabled.
   - **Device alarm template**: Accept the default device alarm template, Default Host Configuration Alarm, or select a custom template from the drop-down list. Template selection applies to all selected hosts.
   - **Alarm notification template**: Select a template from the drop-down list. Notifications are not sent if no alarm notification selected (alarms are always indicated on the Location Alarms tab in Sites or Overview, or in the Alarms window).
   - **Alarm message**: (Optional) Enter a descriptive message to include in email or SMS notifications. This text is used in place of the [AlarmMessage] macro in the related default email templates, or can be added to a custom email or SMS template.

- **Alarm comment**: (Optional) Select from the list of available predefined comments, or enter a custom comment to include in email or SMS notifications. This text is used in place of the [Comments] macro in the related default email templates, or can be added to a custom email or SMS template.

5. Save your changes.

6.4.4 Creating Device Alarm Templates

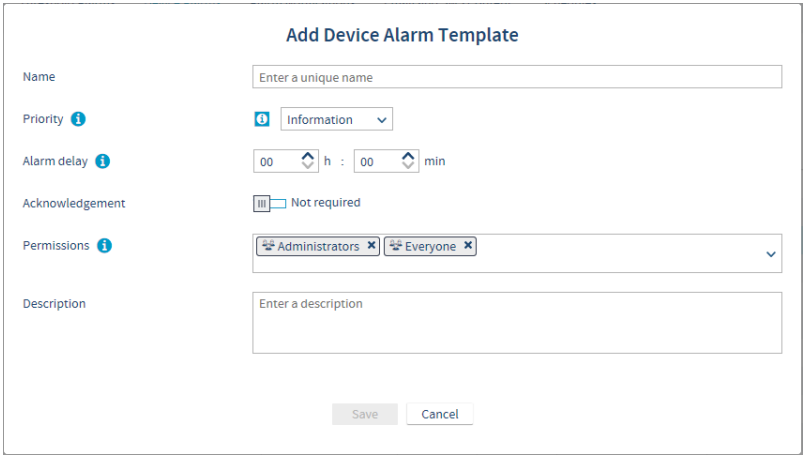
Manage Alarm Templates

Create a copy of a device alarm template when you want to replicate most template properties, or create a new template when you want to define all new properties.

To learn more about device alarms, see "Types of Device Alarms" on page 71.

Create a Device Alarm Template

1. In **Alarm Templates** select the **Device Alarms** tab.
2. Select **Add > Add Device Alarm Template**. To copy settings, select an existing template, then select **Add > Copy Selected Device Alarm Template**.



3. In the Add Device Alarm Template window, enter a unique name for the new template and then set the template properties:
   - **Priority**: The priority level is used as a visual indication of issue severity, to help you determine how quickly to respond to the issue.
   - **Alarm delay**: When viewLinc identifies a device alarm condition, the delay is the time period starting from the moment an issue is detected and when the device alarm is triggered. It is recommended that you set the delay according to the priority.

- **Acknowledgement**: Indicate whether user acknowledgement of this device alarm is required. When an alarm is acknowledged, the action is tracked in the event log.
- **Permissions**: Select the groups permitted to modify or apply this template. The group requires Configure Alarms permission to apply the template to Locations.
- **Description**: (optional) Provide more details about the device alarm template.

4. Select **Save**.

You can now apply this device alarm template to a Location.

When you apply a device alarm template to a Location, it remains in effect on the Location, even if the Location is linked to a different device.

6.4.5 Applying Device Alarm Templates

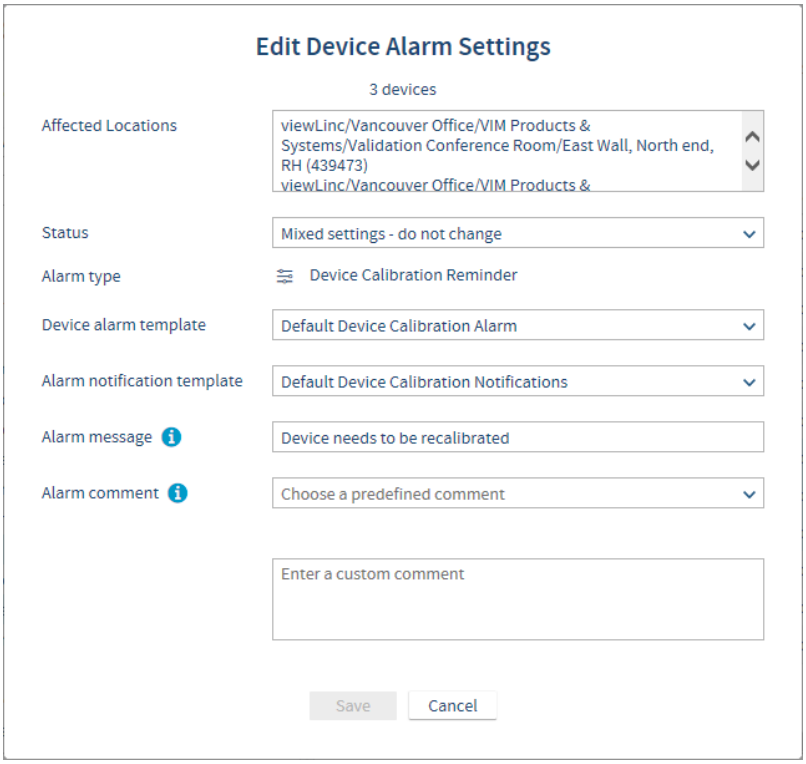
Manage Alarm Templates

Default device alarm templates are automatically applied to linked Locations and template settings can be modified. You can also create and apply custom device alarm templates.

To apply a custom device alarm template to a Location, you require Configure Alarms permission or higher for the selected Location.

Apply a Custom Device Alarm Template to a Location

1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Zone or a Location.
2. Select the **Device Alarm Settings** tab.
3. Select the row for each device alarm type you want to modify, then select Edit (or use the right-click menu). Sort the **Alarm Type** column in ascending or descending order to select a group of the same device alarm types.
4. On the **Edit Device Alarm Settings** window, verify you have selected the correct Location(s).



5. Edit device alarm settings:
   - **Status**: Device alarms are only generated when status is enabled.
   - **Device alarm template**: Select the template to use for the alarm type. If multiple templates are in use, it is recommended not to change the current template selections.
   - **Alarm notification template**: Select an available alarm notification template to use for device alarms at selected Location. If multiple templates are in use, it is recommended not to change the current template selections.
   - **Alarm message** and **Alarm comment**: All device alarm notifications use content specified in viewLinc's default email and SMS content templates. Use these fields to insert custom text in place of the [AlarmMessage] and [Comment] macros embedded in the content templates. To learn more about message content, see "Email and SMS Content" on page 85.
6. Select **Save**.

6.4.6 Editing Device Alarm Templates

Manage Alarm Templates

Modify device alarm template settings for all Locations using a default viewLinc device alarm template. To learn more about device alarm templates, see "Types of Device Alarms" on page 71.

Edit a Device Alarm Template

1. In **Alarm Templates** select the **Device Alarms** tab.
2. Select the template you want to modify, then select **Edit**.
3. Select **View Locations** to verify that changes can be applied to all Locations currently using the template.
4. Modify editable settings. For information on all field options, see "Creating Device Alarm Templates" on page 75).
5. Select **Save**.

6.4.7 Editing Location Device Alarm Settings

Manage Alarm Templates

Device alarm settings can be set for individual devices, or applied to several devices at one time.

To modify device alarm settings you require Configure Alarms permission or higher for the selected Location(s).

Edit Device Alarm Settings

1. In **Sites Manager** in the **Zones and Locations** tree, select the Zone or Location you want to modify ([Ctrl]+click to select multiple Zones and Locations).
2. Select the **Device Alarm Settings** tab, and then select one or more device alarm rows in the grid.
3. Select **Edit device alarm settings**, then adjust settings in the **Edit Device Alarm Settings** window:
   - **Affected Locations**: Verify that all Locations linked to this device can be updated with new device alarm settings. If a device has multiple Locations linked to its channels, make sure that new alarm template settings are applicable to all affected Locations.
   - **Status**: If the status is disabled, viewLinc will not initiate the specified device alarm or device notifications.
   - **Device alarm template**: Select a device alarm template or accept the default option provided. Device alarm templates set the priority level for the device alarm condition, when it is issued, and if it needs to be acknowledged. If multiple device alarms selected, it is recommended not to change the current template selections.
   - **Alarm notification template**: Select an alarm notification template or accept the default option provided. Alarm notification templates specify who is notified, when and how. If multiple device alarms selected, it is recommended not to change the current template selections.

- **Alarm message**: (Optional) Enter a descriptive message to include in email or SMS notifications. This text is used in place of the [AlarmMessage] macro in the related default email templates, or can be added to a custom email or SMS template.
- **Alarm comment**: (Optional) Select from the list of available predefined comments, or enter a custom comment to include in email or SMS notifications. This text is used in place of the [Comments] macro in the related default email templates, or can be added to a custom email or SMS template.

4. Select **Save**.

6.5 Alarm Notifications

Alarm notification templates define:

- When an alarm notification is sent.
- Who receives notification.
- How the notification is delivered.
- If a visual external alarm command is initiated.
- If a notification delay is required after an alarm is triggered, and if the notification will repeat at timed intervals.

The content of a notification is defined by the email or SMS template associated with the alarm (see "Email and SMS Content" on page 85).

Audible alarms are enabled in System Preferences on the General tab (see "System Preferences" on page 87), and then users must be set up to receive audible alarms (see "Groups and Users" on page 57).

Alarm notification templates can be assigned to Locations using a threshold alarm template, to a linked Location's device alarm templates, or can be assigned to system alarms (see **System Preferences > System Alarms**).

Example

If you want a notification sent to an on-site supervisor, you could create an email notification for the first recipient with a short delay period, perhaps 1 minute, and an SMS notification to be issued at 20 minutes.

You may also want another email notification issued to someone else with a different delay period, for example 20 minutes. If the first notification is not acknowledged within 20 minutes, the second notification is automatically sent.

6.5.1 Creating Alarm Notification Templates

Manage Alarm Templates

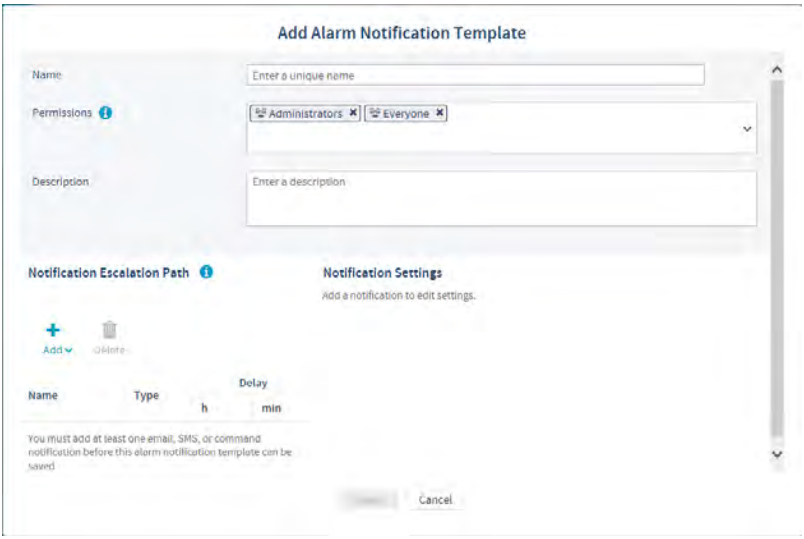
An alarm notification template defines who should be notified in the event of a threshold, device, or system alarm. You can set up an email, SMS, a local visual notification (command), or an escalation path using a combination of notification types, recipients, and delivery times.

Command notifications do not initiate for system alarms.

The content generated for alarm notifications is provided in over 40 default email/SMS templates. Message content can also be customized to send specific information to select groups (see "Email and SMS Content" on page 85).

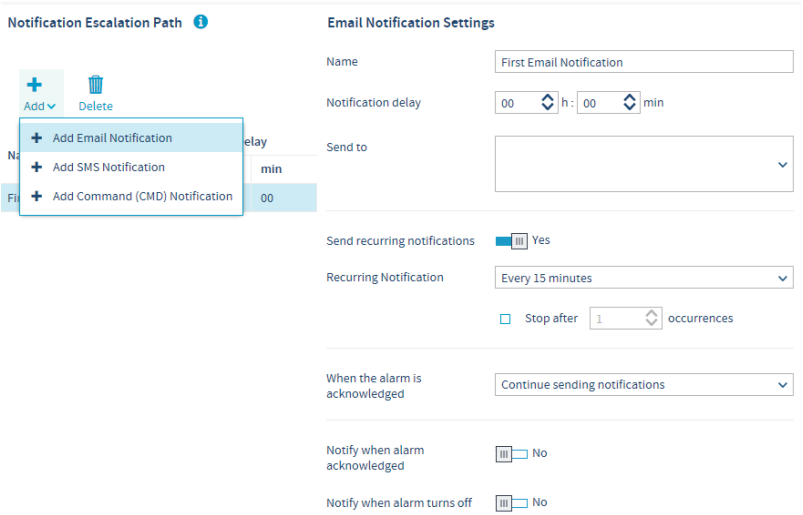
Create an Alarm Notification Template

1. In **Alarm Templates**, select the **Alarm Notifications** tab.
2. Select **Add > Add Alarm Notification Template**. To copy settings, select an existing template, then select **Add > Copy Selected Alarm Notification Template**.



- **Permissions**: Select the groups authorized to modify or apply this template to Locations.
- **Description**: (optional) Provide more details about the alarm notification template.

3. In the **Notification Escalation Path** area, select **Add**, then select an email or SMS alarm notification, or a command notification.



4. To create an email or SMS notification, complete the fields in the **Email/SMS Notification Settings** pane:
   - **Name**: Enter a unique name for each notification. You may want to indicate whether it is an initial or followup notification, or identify the group it goes to.
   - **Notification delay**: Specify a delay in hours and/or minutes from when an alarm is triggered and you want an alarm notification message sent. Alarm activation delays can also be added to threshold alarms.

     If you enter a time delay before a notification message is sent, ensure the combined threshold alarm activation delay and alarm notification delay meets your alarm notification requirements.

   - **Send to**: Select a user or select a group containing all the users you want notified. All users in the group will receive the default alarm notification message. The default template used varies based on the type of alarm (see "Email and SMS Content" on page 85).
   - **Send recurring notifications**: Turn this option on to send the default repeat notification at set intervals while the alarm condition exists, or after a specific number of notification messages are sent.
   - **When the alarm is acknowledged**: Specify whether to stop or continue sending notifications after an alarm is acknowledged, and whether to send the default acknowledgement notification message and/or alarm off notification message.

To modify the content of default alarm notification messages, see "Email and SMS Content" on page 85.

5. To create a command notification, complete the following fields in the **Command Notification Settings** window:
   - **Name**: Enter a unique name to describe the command.
   - **Notification delay**: Specify a delay in hours and/or minutes from when an alarm is triggered and you want the command to run. Alarm activation delays can also be added to threshold alarms.

     If you enter a time delay before a command runs, ensure the combined threshold alarm activation delay and command run delay meets your alarm notification requirements.

   - **Main command to run**: Enter the first command you want to run when an alarm is triggered. Additional commands can be set to run in the recurring command area. Here is an example of a Python script specific to a digital relay I/O device. Different parameters apply to different commands or scripts:

     ```
     C:\Program Files\Vaisala\viewLinc\python\python" -m
     viewLinc.scripts.SwitchBbRelay [COM port number]
     ```

   - **Run recurring commands**: Choose to send the same or different command at repeating intervals while the condition still exists; specify whether you want the commands to stop running after the alarm is acknowledged, or after a specific number of commands are run.
   - **When the alarm is acknowledged**: Choose to continue or block recurring commands.
   - **Run command when alarm acknowledged/when alarm turns off**: Choose a different command to run when an alarm is acknowledged or when the alarm turns off.
6. Select **Save**. You can now apply this alarm notification template to one or more Locations (Sites Manager > Manage), or assign it for use with system alarms (System Preferences > System Alarms).

6.5.2 Applying Alarm Notification Templates

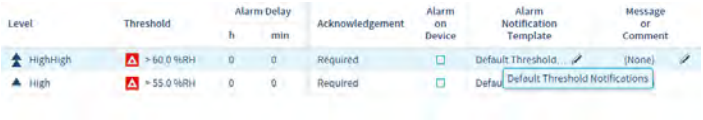
Manage Alarm Templates

After creating alarm notification templates, apply the template to Locations currently using enabled threshold alarm templates, add them to specific device alarm templates, or assign them for use with system alarms.

To apply an alarm notification template, you require Configure Alarms permission or higher for the selected Location.

Apply an Alarm Notification Template to a Location Threshold Alarm

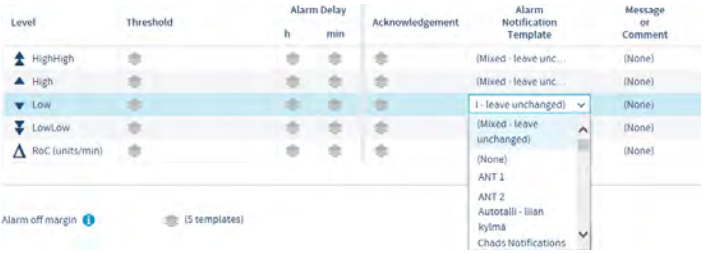
1. In **Sites Manager** on the **Zones and Locations** tree, select a Location.
2. Select the **Threshold Alarm Settings** tab.
3. Select a threshold alarm settings row on the grid, then select **Edit Threshold Alarm Settings**. If no templates are available, you must add a threshold template to the Location (**Manage > Add Threshold Alarms**).
4. On the **Edit Threshold Alarm Settings** window, select an enabled threshold level.



5. In the **Alarm Notification Template** column, use the drop-down list to select an available alarm notification template.
6. Select **Save**.

Apply an Alarm Notification Template to Multiple Location Threshold Alarms

1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Zone or several Locations ([Ctrl] + click).
2. On the **Threshold Alarm Settings** tab, select one or more threshold setting rows.
3. Select **Edit threshold alarm settings**.
4. On the **Edit Threshold Alarm Settings** window in the **Alarm notification template** column, select a template for one or more enabled threshold levels.



5. Select **Save**.

Apply an Alarm Notification Template to a Location Device Alarm

1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Location.
2. Select the **Device Alarm Settings** tab.
3. Select the device alarm type from the list, then select **Edit Device Alarm Settings**.
4. On the **Device Alarm Editor** window, in the **Alarm notification template** field, select an alarm notification template.
5. Select **Save**.

Apply an Alarm Notification Template to Multiple Location Device Alarms

1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Zone or multiple Locations ([Ctrl] + click).
2. Select the **Device Alarm Settings** tab.
3. Select the same device alarm types (use the Alarm Type column header to sort the grid in ascending or descending order), then select **Edit device alarm settings**.
4. On the **Edit Device Alarm Settings** window, in the **Alarm notification template** field, select an alarm notification template.
5. Select **Save**.

Apply Alarm Notification Templates for System Alarms

1. In **System Preferences** select the **System Alarms tab**.
2. Select an alarm notification template for Database Validation Alarms and/or Event Log Validation alarms.
3. Select **Save**.

6.5.3 Editing Alarm Notification Templates

Manage Alarm Templates

Before making changes to an alarm notification template, check which Locations and system alarms are using the template. To learn more about alarm notification templates, see "Alarm Notifications" on page 79.

Edit an Alarm Notification Template

1. In **Alarm Templates** select the **Alarm Notifications** tab.
2. Select the template you want to modify, then select **Edit**.
3. Modify the editable settings . For information on all field options, see "Creating Alarm Notification Templates" on page 80).
4. Select **Save**.

6.6 Email and SMS Content

Threshold, device and system alarm notifications contain default email and SMS content to inform your team about alarm conditions occurring on your network.

viewLinc provides more than 40 default email and SMS content templates. There are templates for the initial notification of an alarm condition, templates for each alarm type if recurring notifications are required, and templates for notification that an alarm condition is no longer present.

Default email and SMS templates can include predefined or custom alarm comments and alarm messages, if specified. Alternatively, you can compose new template content (see "Creating Custom Email or SMS Content" below).

To see a list of all available templates, go to **Alarm Templates > Email and SMS Content**.

6.6.1 Creating Custom Email or SMS Content

Manage Alarm Templates

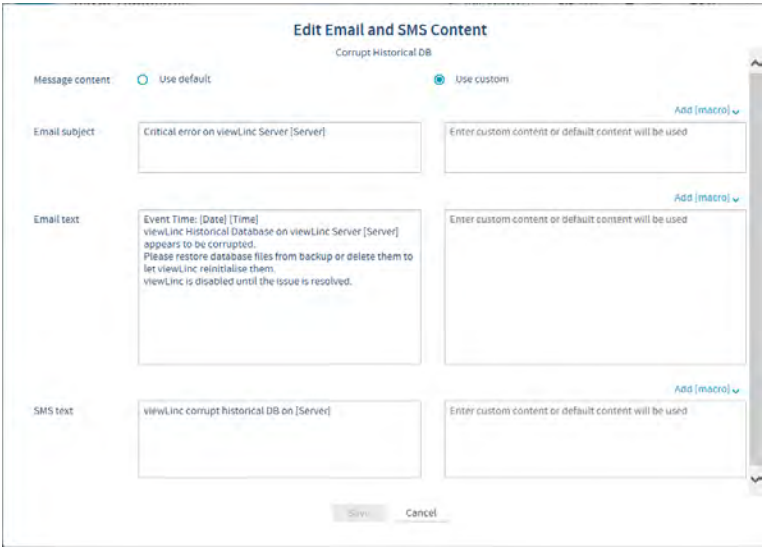
You can modify email and/or SMS message content issued from viewLinc.

Custom alarm messages and/or comments can be included in email and SMS templates:

- "System Alarm Preferences" on page 97
- "Editing Location Device Alarm Settings" on page 78
- "Applying Threshold Alarm Templates to Locations" on page 68

Create Custom Email or SMS Message Content

1. In **Alarm Templates** select the **Email and SMS Content** tab.
2. Select a template to modify, then select **Edit**. In the **Edit Email and SMS Content window**, default content is displayed but it cannot be modified.



3. Select **Use custom**.
4. Enter new content in the active custom text areas:
   a. In the **Email subject**, **Email text** or **SMS text** areas, enter new content.

   SMS messages are limited to 70 characters in length. Message length can increase if your network supports longer SMS messages. Please contact Vaisala Technical Support for assistance.

   b. To insert system-generated content, such as a timestamp or viewLinc alarm message, move the cursor where you want to add the content, then select an option from the **Macros** dropdown. For a complete of list of macro definitions see "Email and SMS Content Macros" on page 185.
5. Save your changes.

7. System Preferences

viewLinc defines system options that affect the behavior and display of your data and devices. System preferences can be modified by users who are assigned to groups with Manage System right.

7.1 General Preferences

Modify General System Settings

Manage System

1. In **System Preferences** on the **General** tab, set **General** options:
   - **System language**: Set the default system language for reports and notifications. You can also enable additional languages to allow users to set preferred language output for reports, notifications and their viewLinc desktop display. To learn more, see "Language Preferences" on page 94.
   - **Scheduling**: Enable this option to control when users receive notifications, and when Location alarming should be active. After enabling this option, create schedules. See "Creating Schedules" on page 105.
   - **Email and SMS alarm acknowledgement** : Allow users to acknowledge alarms by responding to email and/or SMS messages on mobile devices. To learn more, see "Remote Acknowledgement" on the next page.
   - **Audible alarm notification**: Enable audible alarm notification, then set up each user to receive audible alarming. To learn more, see "Audible Alarming" on page 89.
   - **Audible alarm sound**: Choose the sound for audible alarms. Select the ▸ to start/stop a sound test.
2. Set default units and values. These values are used wherever units display (trend graphs, reports). These values can be modified for specific Locations.
   - **Default temperature units**: By default all devices monitoring temperature display in Celsius.
   - **Default MKT activation energy**: Set the MKT value according to your GxP requirements. To learn more see "MKT Activation Energy" on page 90.
3. Specify device options:
   - **Device description**: Choose to display the device alias (a longer description) in viewLinc. To learn more, see "Device or Channel Alias" on page 91.
   - **Channel description**: Choose to display the channel alias (a longer description) in viewLinc. To learn more, see "Device or Channel Alias" on page 91.
   - **Device calibration duration**: Set default data logger and probe calibration cycle length in months. To learn more, see "Device Calibration Duration" on page 91.

- **Automatically lock DL devices**: Enable auto-locking to ensure all newly connected DL data loggers can only be modified by viewLinc. To learn more, see "Lock/Unlock DL Data Loggers" on page 177.
- **DL data logger timebase synchronization**: When the logger timebase synchronization feature is enabled, the time clock in a logger is continuously compared with the viewLinc clock and adjusted, if required. To learn more, see "Timebase Synchronization" on page 92.
- **viewLinc Aware functionality**: Enable viewLinc Aware to ensure faster setup for vNet devices. To learn more, see "Lock/Unlock DL Data Loggers" on page 177.

4. Set security options:
   - **License key**: The viewLinc license key defines the number of devices you can connect to your system. To learn more about licensing options, see "License Key" on page 93.
   - **Comments on changes**: Indicate whether comments are required when users acknowledge alarms or modify the system. To create predefined comments, see "Adding Predefined Comments" on page 99.
   - **Confirm identity on changes**: Require user authentication when making system changes. To learn more, see "Authenticate System Changes" on page 93.
5. Adjust technical support log settings (optional).
   - **System log**: Record different amounts of system activity.
   - **Device driver log:** Record different amounts of device activity.
   - **Log maximum age**: Specify how long to store technical support files. Once the limit is reached, old log files are deleted. "Technical Support Logs" on page 93.

It is recommended that you change support log settings only when directed by Vaisala Technical Support.

6. Save your changes.

7.2 Remote Acknowledgement

Manage System

Alarm acknowledgement can be completed in a browser on a monitor or mobile device on the Overview, Sites or Alarms windows, anytime.
viewLinc must be set to allow remote acknowledgement if you want users to acknowledge alarm notifications via email or SMS.

Each user who is permitted to acknowledge alarms remotely must include a mobile number and unique PIN on their profile (see "Users" on page 59).

Allow Remote Acknowledgement

1. In **System Preferences** on the **General** tab, select the **Remote acknowledgements** row.
2. In the **Value** column choose your acknowledgement preference:
   - **Email**: To allow email acknowledgement, make sure your email server is set up to receive email acknowledgements (see "Setting Up Email Server Preferences" on page 96).
   - **SMS**: To allow SMS acknowledgements, make sure your SMS modem is set up to receive SMS acknowledgements (see "Setting Up SMS Modem Preferences" on page 97).
3. Select **Save**.

7.3 Schedules Functionality

Manage System

Set specific times of day or days of the week when you want a user or group to be notified of alarm conditions. Schedules can also be used to specify the times when you want Location threshold alarming active. By default, this option is disabled.

Enable or Disable Schedules

1. In **System Preferences** on the **General** tab, select the **Scheduling Functionality** row.
2. In the **Value** column enable or disable scheduling.
3. Save your changes.

To learn how to create and apply schedules, see "Schedules" on page 105.

7.4 Audible Alarming

Manage System

Audible alarming activates a sound on a user's computer in the event of an alarm condition. An audible alarm icon displays on the viewLinc desktop UI, **Alarms (21)** .

- To hear an audible alarm, the user must be logged into viewLinc on their computer and have audible alarms enabled on their user profile (see "Users" on page 59).
- To turn off an active audible alarm, the user can click the alarm icon. See "Responding to Audible Alarms" on page 129.

CAUTION
Audible alarms are not heard if the user is not logged in, or is using a browser with audio turned off.

Enable or Disable Audible Alarms

1. In **System Preferences** select the **General** tab.
2. On the **Audible alarm notification** row, select **Enable** or **Disable**.
3. If audible alarms are enabled, use the **Audible alarm sound** row to select a sound. Select the ▸ to start/stop a sound test.
4. Select **Save**.

7.5 Temperature Measurement Units

Manage System

When viewLinc is first installed, temperature values are set to display in degrees Celsius. You can configure viewLinc to show temperatures in either Celsius or Fahrenheit, a setting that is applied globally.

This setting does not alter how a device measures temperature, it simply alters the units in which temperature is displayed (except for channels which already have preferred unit settings assigned).

You can set measurement units on individual device channels. See "Editing Device Properties" on page 39.

Set Temperature Units

1. In **System Preferences**, on the **General** tab, select the **Default temperature units** row.
2. Set the **Value** field.
3. Select **Save**.

7.6 MKT Activation Energy

Manage System

The default value for MKT Activation Energy is used when generating reports and trends.

Mean Kinetic Temperature (MKT) is considered useful for understanding temperature excursions in GDP-compliant applications. See MKT Application Note.

Set MKT Value

1. In **System Preferences** on the **General** tab, select the **MKT Activation Energy** row.
2. Set the **Value** field.
3. Select **Save**.

7.7 Device or Channel Alias

Manage System

Vaisala devices have descriptions stored inside them that have a maximum length of 16 alpha-numeric characters (300-series transmitters do not store descriptions). These descriptions can be defined and modified using viewLinc or device configuration software (vLog or HMT140 Utility).

For easier reference, you can configure viewLinc to display a longer, more informative description for a device or a channel, up to 64 alpha-numeric characters. This longer description is called an alias.

Events-, Alarms-, Reports windows, and email messages all use the selected description for channels and devices.

Set Alias Preference

1. In **System Preferences** on the **General** tab, select the **Channel Description** or **Device Description** row.
2. Set the **Value** field to use alias.
3. Select **Save**.

7.8 Device Calibration Duration

Manage System

A device calibration alarm is an intermittent notification sent when a Vaisala data logger or probe is due for calibration.

By default, you receive notifications at the following intervals: 3 months and 1 month before the calibration due date, then again on the scheduled recalibration date (auto-generated for 1 year from last calibration date). This alarm remains active, even after acknowledgement, until the device is recalibrated (for more information contact Vaisala Calibration Service Center).

You can set the default calibration duration for all data loggers in **System Preferences**, or, if you have Manage Devices right, modify the duration for a specific data logger or probe in Sites Manager (**Hosts and Devices > Configure > Edit Properties**).

Set System-Wide Default Calibration Duration

1. In **System Preferences** select the value column beside the option, **Default calibration duration**.
2. Enter a time period in months.

Calibration duration set on a data logger or a probe overrides the system preference.

3. Select **Save**.

7.9 Timebase Synchronization

Manage System

Synchronized data collection timing between viewLinc and your data loggers ensures more accurate data collection by automatically correcting time drift. When the logger timebase synchronization feature is enabled, the time clock in a data logger is continuously compared with the viewLinc clock and adjusted, if required.

Minor time drift is expected over long data monitoring periods, and can be a result of the impact of temperature on a device collecting data (such as a data logger in a cold area) and where the data is sent (computer in a controlled server room).

Enable data logger timebase synchronization only on one viewLinc Enterprise Server. Logger timebase synchronization only corrects time drift up to 15 minutes. If the drift is greater than 15 minutes, clear data logger history (see "Clearing Historical Samples" on page 178).

Enable/Disable Timebase Synchronization

1. In **System Preferences** on the **General** tab, select the **DL data logger timebase synchronization** row.
2. Set the **Value** field to **Enabled** or **Disabled**.
3. Select **Save**.

7.10 viewLinc Aware

Manage System

This function automatically permits viewLinc to search for and communicate with vNet devices on your network or subnet. The latest Firmware must be installed on each vNet device (v1.4 or higher).

Only enable this option on one viewLinc Enterprise Server installation per subnet.

Enable/Disable viewLinc Aware

1. In **System Preferences** select the **General** tab.
2. Select the **viewLinc Aware functionality** row, then select Enable or Disable.
3. Select **Save**. New devices are automatically discovered in viewLinc within five minutes. If the auto-discovery process is taking too long, you can force discovery. See "Discovering Networked Devices" on page 31.

To learn more about how to set up vNet devices with viewLinc, refer to the *vNet User's Guide*.

7.11 License Key

Manage System

This number specifies how many devices can be managed by your licensed viewLinc product; it does not monitor how many users can access the system. You are required to enter your license key during installation, or when upgrading your system size.

Enter a New License Key

1. In **System Preferences**, select the **General** tab
2. On the **License key** row, enter your license number in the **Value** field .
3. Select **Save**.

7.12 Authenticate System Changes

Manage System

To ensure more robust system security, you can require that users reenter their password to make changes in viewLinc. This setting is applied universally to all viewLinc users.

Set an Authentication Requirement

1. In **System Preferences** select the **General** tab.
2. Select **Confirm identity on changes**, then choose an authentication option:
   - **Never**: Logged-in users are not required to confirm their identify when making changes.
   - **Always**: Logged-in users are required to enter their password each time they try to make a change.
   - **After 1 - 30 minutes/After 1 hour**: Logged-in users are required to re-enter their password if the selected time period has passed since their last authenticated change.
3. Select **Save**.

7.13 Technical Support Logs

Manage System

If you require viewLinc technical support, your Vaisala Technical Support representative may ask you to change the technical support log settings temporarily, to help them better understand the issue you may be encountering.

These options specify the amount of information detail included in the support log file, for viewLinc and for data logger drivers, and for how long data will be stored before it is deleted (your technical support representative will advise which settings should be applied).

Change Support Log Settings

1. In **System Preferences** select the **General** tab.
2. In the **System log**, **Device driver log**, and **Log maximum age** rows, set the amount of technical detail required, as directed by Vaisala Technical Support.
3. Select **Save**.

Vaisala Technical Support will remind you to reset default values after completing their analysis.

7.14 Language Preferences

Manage System

The system language setting is used for reports and notifications. By default it is the language selected during viewLinc Enterprise Server installation. If your company operates in countries where other languages are spoken, you may want to provide users the option to receive notifications and reports, and display the viewLinc desktop, in their native language.

Enable support for additional languages on the **System Preferences > Languages** tab, and then set the user language preference on each users' profile (see "Users" on page 59).

Important notes about system language setting and user language preference:

- Quick reports: When a user generates a Quick Report, the content is generated according to the user's logged in language, even if it is different from their language preference.
- Scheduled reports: Sent to recipients according to their language preference.
  - If no user language preference is specified, report content is generated in the report language.
  - If no user language preference or report language specified, the content is generated according to the default system language.
- User-generated reports: Report content is generated in the system language.

Languages supported:

English (EN)
Chinese (Simplified - ZH)
French (FR)
German (DE)
Japanese (JA)
Swedish (SV)
Spanish (International - ES)
Portuguese (Brazilian - PT)

Set System Language

1. In **System Preferences** select the **General** tab.
2. On the **System language** row select the system language in the **Value** field.
3. Select **Save**.

Make Additional Languages Available

1. In **System Preferences** select the **Languages** tab.
2. Enable the language choices you want displayed when users log in.
3. Select **Save**.

7.15 Unit Display Preferences

Manage System

Channel measurement units are preset in your devices. However, you can display device measurement units differently in viewLinc . For example, if a channel tracks voltage in MilliAmps, you could change the viewLinc display text to, mA.

Set Unit Descriptions

1. In **System Preferences** select the **Units** tab.
2. Select a unit type row, then select **Edit**.
3. Update the unit properties:
   - **Name**: Modify the name of the unit type.
   - **Device units**: Ent Enter a maximum of 6 CAPITAL letters per unit of measurement. Use a comma (,) to separate unit types.
   - **Display Text**: Enter the format to display for each unit. For example, if a temperature unit is C, you may want to display Celsius.
   - **Min**: Set the minimum value permitted for this unit.
   - **Max**: Set the maximum value permitted for this unit.
4. To add new device units, select **Add**. In the **New Unit** window make sure you enter the unit properties as they are set in your device.

See your device user's guide to determine current unit properties and min/max values.

5. Select **Save**.

Delete Units

You can delete any unit types that were manually added and are not currently used by a Location or threshold alarm template.

7.16 Email and SMS Settings

System alarm notifications are issued via email or SMS. viewLinc administrators define the default email server and SMS modem settings, such as the issuing and receiving mail server and delivery addresses.
To complete the setup of system notification preferences, define the users or groups that you want to receive system alarm notifications (see "System Alarm Preferences" on the facing page).

7.16.1 Setting Up Email Server Preferences

Manage System

Define your company's outgoing email account information used for sending system alarm email notifications, and incoming email server requirements used to receive system alarm email acknowledgements (if remote acknowledgment is permitted).

Set Email Server Preferences

1. In **System Preferences** select the **Email Settings** tab.
2. In the **Outgoing Server** area, enter a valid send from address (email notifications from viewLinc are sent from this address, so the email address must exist within your company), then enter:
   - **SMTP server**: Mail server address. For example, smtp.company.com.
   - **Port**: Outgoing mail server port number (between 1-65535, default is 25). Your IT network administrator has this information.
   - If your outgoing mail server requires authentication, select **SMTP Authentication** and enter the user name or email address, and password required to send email.

viewLinc automatically uses secure SMTP if it is supported by the SMTP server.

3. Select **Send Test Email** to verify the test email is sent successfully.
4. In the **Incoming Server** area, configure the required mail server settings for your connection type:
   a. **Connection type**: **POP3**.
      - **POP3 server**: Enter the incoming POP3 mail server name (for example, pop.company.com).
      - **Port**: Enter the incoming mail server port number (default is 110).
      - Enter the user name (or address) and password for a valid POP3 account, required to receive email.
   b. **Connection type**: **IMAP**.
      - IMAP server: Enter the incoming IMAP mail server name (for example, imap.company.com).
      - **Port**: Enter the incoming IMAP mail server port number.
      - Enter the user name (or address) and password for a valid IMAP account, required to receive email.
5. Select **Save**.

7.16.2 Setting Up SMS Modem Preferences

Manage System

SMS settings define your SMS modem configuration when sending system alarm SMS notifications and receiving system alarm SMS acknowledgements (as required by your cellular provider).

SMS messages are limited to 70 characters in length. Message length can increase if your network supports longer SMS messages. Please contact Vaisala Technical Support for assistance.

Set SMS Modem Preferences

1. In **System Preferences** select the **SMS Settings** tab.
2. Complete the **SMS Modem** section:
   - **SMS COM port**: Your SMS modem's port number.
   - **Baud rate**: Select the rate which is best supported by your modem.
   - **SIM Card PIN number**: Enter the PIN number, required to receive incoming messages.
3. Select **Send Test SMS**. If an SMS message is not sent to the correct mobile phone, adjust the settings until the test SMS is sent successfully.
4. Select **Save**.

7.17 System Alarm Preferences

Manage System

System alarms are generated automatically to indicate general system issues, database history integrity, and event log tampering. They are always high priority, are issued immediately, and always require acknowledgement. Acknowledgement of system alarms can be performed in viewLinc (see "Receive Alarm Notifications" on page 125) or remotely via email or SMS.

To allow remote acknowledgement of system alarms via email or SMS, see "Remote Acknowledgement" on page 88.

Set System Alarm preferences

1. In **System Preferences** select the **System Alarms** tab.
2. In the **IT Network Manager** area, enter the mobile number and email address you want to receive viewLinc system notifications. You can also choose whether to send copies of system alarm notifications to members of the Administrators group.
3. In the **Database Validation Alarm** area, the **Priority**, **Delay** and **Acknowledgement** options cannot be modified. You can modify the following options:
   - **Alarm notification template**: Choose an alarm notification template to use with the system alarm notification. The alarm notification template defines whether an email or SMS

notification is issued, how soon after the alarm is triggered the notification is sent, and how often it is repeated.

Only email and SMS settings set in the selected alarm notification template apply to system alarms. Commands are not initiated for system alarms. See "Creating Alarm Notification Templates" on page 80.

- **Alarm Message**: Alarm message text replaces the [AlarmMessage] macro in database validation alarm email templates (see "Email and SMS Content" on page 85).
- **Alarm Comment**: Choose to include a predefined comment (if available), or enter a custom comment. Comments text replaces the [Comments] macro in database validation email templates (see "Email and SMS Content" on page 85).

4. In the **Event Log Validation Alarm** area, the **Priority**, **Delay** and **Acknowledgement** options cannot be modified. You can modify the following options:
   - **Alarm notification template**: Choose an alarm notification template to use with the system alarm message. The alarm notification template defines whether an email, SMS or command notification is issued, how soon after the alarm is triggered the notification is sent, and how often it is repeated. See "Creating Alarm Notification Templates" on page 80.
   - **Alarm Message**: Alarm message text replaces the [AlarmMessage] macro in event log alarm email templates (see "Email and SMS Content" on page 85).
   - **Alarm Comment**: Choose to include a predefined comment (if available), or enter a custom comment. Comments text the [Comments] macro in event log email templates (see "Email and SMS Content" on page 85).
5. Select **Save**.

7.18 Comments

Manage System

User-entered comments can provide valuable reference information about changes made to your system, or in response to network events.

You can specify whether users are required to enter comments manually, or if they should select a predefined comment. Comments can be used in several places: added to events, included in reports and email notification templates, or added during acknowledgement of alarm notifications.

To set up predefined comments, see "Adding Predefined Comments" on the facing page.

Set Comments Preference

1. In **System Preferences** select the **General** tab.
2. In the **Comments on changes** row, select an option from the list available in the in the **Value** column.

- **Not required**: Users will not be prompted to enter a comment when system changes are made.
- **Optional**: The comments window will appear for system changes, and users have the option to enter a comment or select a predefined comment.
- **Required**: The comments window will appear and users must enter a comment or select a predefined comment.
- **Only predefined comments required**: The comments window will appear with a list of available predefined comments. This option requires predefined comments to be available.

3. Select **Save**.

7.18.1 Adding Predefined Comments

Manage System

Predefined comments are a quick way for users to describe standard, repeatable actions taken when responding to alarms, or to provide common rationale for system changes.

The viewLinc administrator may want to include a predefined comment in outgoing system or threshold alarm notifications to provide guidance on actions required. To save time, users can add a predefined comment when responding to alarm notifications to describe a common action performed. Predefined comments can also be used to describe events in the event log.

Add a Predefined Comment

1. In **System Preferences** select the **Comments** tab.
2. Select **Add**.
3. Enter a new comment (up to 300 characters).
4. Select **Save**.

If you require that your users add a comment for all system changes/additions/deletions, set the comment preference in **System Preferences > General**.

Predefined comments can be added to:

- System alarms (see "System Alarm Preferences" on page 97).
- Location threshold alarm settings (see "Applying Alarm Notification Templates" on page 82).
- Alarm acknowledgements (see "Acknowledge Alarms in the Alarms Window" on page 127).
- Events (see "Adding Comments to Events" on page 133).

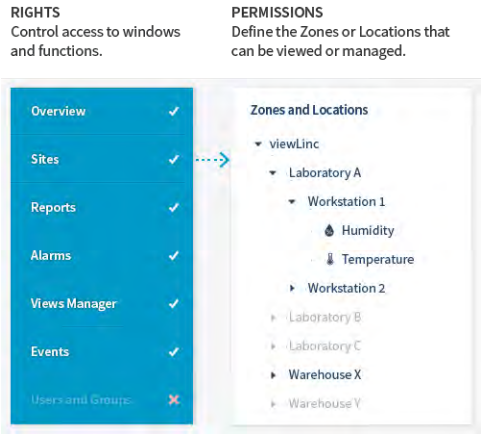
8. Additional Setup Tasks

After all primary viewLinc configuration tasks are complete, you can take advantage of more viewLinc features:

- Add group **permissions** to Zones and Locations. Permissions are used to control the groups which can view, configure or manage different viewLinc Zones and associated Locations.
- Create **schedules** to define active periods for alarming and notifications. Schedules can ensure users who are not on shift do not receive notifications, or prevent unnecessary alarming during maintenance periods.
- Build **views** to help users more easily identify Locations of importance. For larger installations, views can help organize different categories of Locations.
- Set up a **remote display** to broadcast live conditions on a large monitor in a warehouse.

8.1 Permissions

Four levels of permission define the Zones and Locations group members can view and access, and, depending on the permission level granted, which functions a user can perform. Even if a group has Manage Sites right, members of the group can only modify settings for the linked Locations their group is permitted to access.



Permission levels are applied to Zones and can include or exclude sub-zones and Locations. By default, all users in the viewLinc Everyone group have View permission to view the top system Zone, viewLinc, but must be given View permission to see Zones or Locations that are added. Members of the viewLinc Administrators group have the highest permission level, Full Control, and can see and manage all new Zones and Locations that are added.

To manage permissions most effectively, apply group permission levels to specific Zones, and allow the permission to be inherited all sub-zones.

Important Notes about Permissions

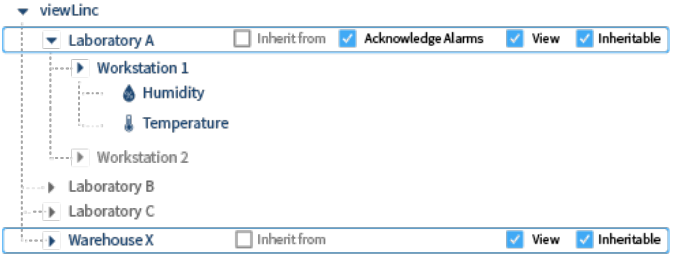
- Permissions granted to a Zone apply to all sub-zones and Locations (inherited).
- An individual user's permission is based on the highest group permission available for the Zone.
- If you upgraded from an earlier version of viewLinc, permissions assigned to users are preserved; however, if you remove a user's permission it cannot be reapplied.

Before assigning permissions to groups, make sure each group has the rights required to complete tasks associated with the Zone or Location (see "Rights" on page 57).

Example

Francis is responsible for generating and distributing alarm reports created by the teams working in Zone: Laboratory A and Zone: Warehouse X. Francis is also responsible for acknowledging threshold alarms on all Locations in the sub-zone Workstation 1. Francis does not need to see the sub-zone Workstation 2, or the Zones Laboratory B or Laboratory C.

1. Add Francis to a group with Manage Reports right.
2. Assign the group View permission to Warehouse X, and make the permission inheritable to all sub-zones and Locations.
3. Assign the group Acknowledge Alarms permission to Laboratory A and make the permission inheritable to all sub-zones and Locations.



8.1.1 Permission Levels

The most basic permission level, View, allows a group to see a Zone and its Locations in various viewLinc windows. Higher permission levels allow a group to perform different actions on the Zone and the Locations in the Zone.

Table 12 Permission Levels

Name	Actions Allowed
Full Control	View, acknowledge alarms, configure alarm templates, apply alarm schedules, and assign permissions for all Locations in a Zone.
Configure Alarms	View, acknowledge alarms, and apply or modify threshold alarm templates for all Locations in a Zone.
Acknowledge Alarms	View and acknowledge alarms for all Locations in a Zone.
View	View all Locations in a Zone.

8.1.2 Applying Group Permission to Zones

Manage Sites

Before groups can view any Zones or Locations in viewLinc, groups must be granted View permission or higher to specific Zones.

Full Control permission is required to grant other groups permission to the selected Zone.

Add Permission

1. In **Sites Manager** navigate the **Zones and Locations** tree to select a Zone or sub-zone.
   - To check currently applied permissions, select the **Permissions** tab and open the **Permissions Viewer** (see "Using Permissions Viewer" on the next page).
2. Select **Manage > Edit Permissions**.

To see which users are included in a group, select **Properties**.

3. Add permissions in the **Edit Permissions** window:
   - To apply the same group permissions for the selected Zone to all sub-zones and Locations, select the group then select **Inherit from**.
   - To change the group permission level, de-select **Inherit from** then choose a permission level in the **Permissions** columns.

- To ensure a group has a permission level passed on to all current and future sub-zones and Locations in the selected Zone, ensure the **Inheritable** option is selected.

4. Select **Save**.

Edit Permission

For a group with inherited permissions, you can remove inherited permission to a specific sub-zone.

You cannot modify a user's inherited permissions granted from an earlier version of viewLinc. User permissions can only be removed.

1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone.
2. Select **Manage > Edit Permissions**.
3. In the **Edit Permissions** window, de-select the group's **Inherit from** checkbox, then choose a new permission level in the **Permissions** columns. If all permission levels are de-selected, sub-zones are not visible (the **Permission** column will read **Hide**).
4. Select **Save**.

Delete Permission

Before permission can be deleted, inherited permission must be removed (see Edit Permission).

CAUTION
Deleting group permission may disable the group's permission levels applied to sub-zones.

1. In **Sites Manager** on the **Zones and Locations** tree, select a Zone.
2. Select **Manage > Edit Permissions**.
3. In the **Edit Permissions** window, select the group.
4. Select **Delete**. If the Delete button is not active, you first need to disable inherited permissions.
5. Select **Save**.

8.1.3 Using Permissions Viewer

Manage Sites

For large organizations with multiple Zones or Locations and specific access control requirements, the Permissions Viewer provides you with a quick way to view currently applied group permissions.

Look Up Permissions

1. In **Sites Manager** select a Zone on the **Zones and Locations** tree.
2. Select the **Permissions** tab. The highest available permission level assigned to groups or upgraded users appears in the **Permission** column. If no group permissions are available on a Zone, the group permission level is **Hide**.
3. To view all permissions for a specific group or user, select the **Permissions Viewer** button.

4. In the **Permissions Viewer** window, choose to **Show groups** or **Show users**.
5. Select a group or user to view all assigned permissions.

To modify permissions, see "Applying Group Permission to Zones" on page 103.

8.2 Schedules

By default, Location threshold alarming is always active and alarm notifications are always sent. Schedules are used to help manage network traffic when a Zone or Location does not require monitoring or when specific users are not required to receive alarm notifications. For example, you could set up a schedule for notifications to be sent to users on day shift, between 6 am and 4 pm, another schedule for users on night shift, 4 pm to 2 am, and a threshold alarm schedule for active alarming between 6 am to 2 am.

You can temporarily turn off all threshold alarming and prevent notifications from being sent, perhaps during a system maintenance period. See "Pausing Threshold Alarming" on page 129.

8.2.1 Creating Schedules

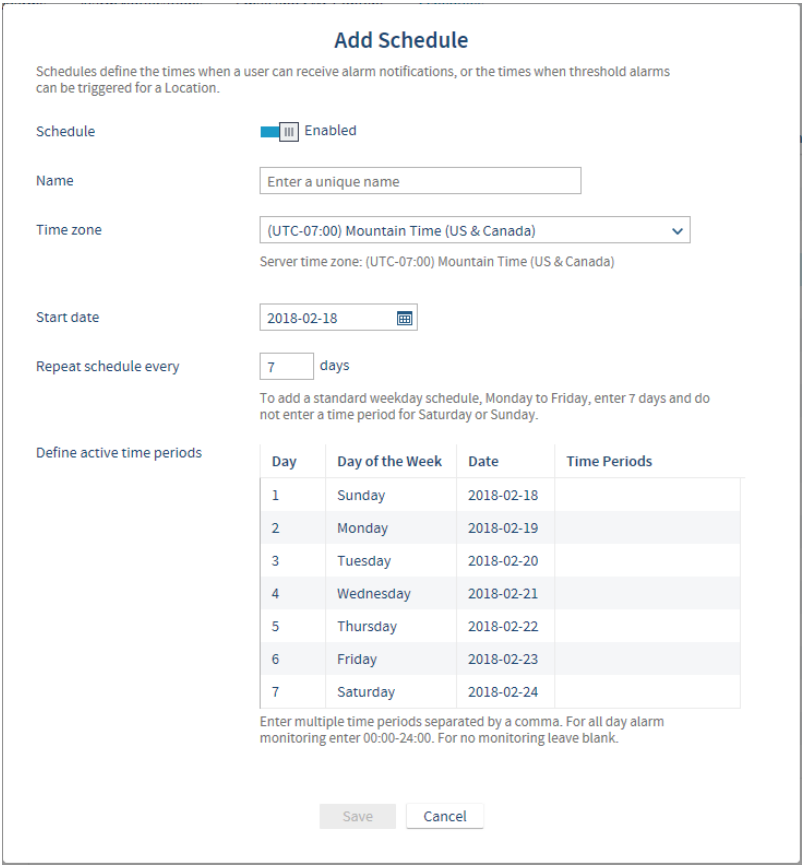
Manage System

Schedules define the times when a user can receive alarm notifications, or the times when threshold alarms can be triggered for a Location.

Before you can apply schedules to users or Locations, make sure scheduling functionality is enabled (see "Schedules Functionality" on page 89).

Create a Schedule

1. In **Alarm Templates** select **Schedules > Add**.



2. On the **Add Schedule** window enter schedule settings:
   - **Schedule**: You can create a schedule before setting it to Enabled. Once the schedule is applied to users or Locations, you can quickly enable or disable it here. If a schedule is disabled, thresholds are always monitored and notifications always sent for threshold excursions.
   - **Name**: Enter a unique name for the schedule.
   - **Time zone**: Select the time zone you want the schedule to use. If your company monitors conditions in multiple time zones, you may want to create schedules for each time zone.
   - **Start date**: Choose a start date by typing in the text box or choosing a date from the calendar. This date defines the day of the week to start the schedule.

- **Repeat schedule every**: To set the schedule for a standard work week that repeats every 7 days, enter **7** and do not enter time periods for non-work days. For a continuous week (no days off), enter **9**. The maximum value is 99 days.
- **Define active time periods**: Enter the time period for each day in the cycle, in 24-hour time. Use the following format: **xx:xx-yy:yy**, where **xx:xx** is the start time and **yy:yy** is the end time. This is when threshold alarming and alarm notifications will be active.

3. Select **Save**.

You can now apply this schedule to Locations and/or users (see "Adding User Schedules" below and "Setting Threshold Alarm Schedules" below).

8.2.2 Setting Threshold Alarm Schedules

Manage Sites

Apply a schedule to a Zone or a Location to define when threshold excursions should trigger an alarm notification. Schedules are created in the Alarm Templates window (see "Creating Schedules" on page 105).

Before adding a schedule, make sure you have enabled the scheduling function (see "Schedules Functionality" on page 89).

Set a Location Threshold Alarm Schedule

Configure Alarms permission is required for all Locations or Zones.

1. In **Sites Manager** in the **Zones and Locations** tree, select a Location.
2. Select **Manage > Set Threshold Alarm Schedule**.
3. In the **Set Threshold Alarm Schedule** window, select **According to schedule** and select a schedule from the dropdown list.

   CAUTION
   viewLinc does not monitor threshold limits outside scheduled times (no threshold alarms are activated and notifications are not sent). Choose Always to ensure alarm monitoring continues 24x7.

4. Select **Save**.

8.2.3 Adding User Schedules

Manage System

Apply a schedule to a user to define when they should receive alarm notifications. Schedules are created in the Alarm Templates window (see "Creating Schedules" on page 105).

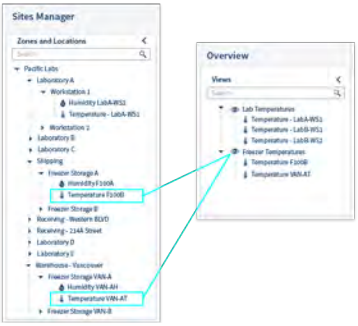
Before adding a schedule, make sure you have enabled the scheduling function (see "Schedules Functionality" on page 89).

Add a User Schedule

1. In the **Users and Groups** window select the **Edit** toolbar button.
2. On the **Edit User** window in the **Send alarm notifications** field:
   - By default, the schedule is set to **Always**, to indicate that this user should always receive an alarm notification 24x7.
   - To make sure this user never receives alarm notifications, select **Never**. This is a useful option when a user is away on holiday.
   - Select **According to schedule** and then choose a schedule from the dropdown list.
3. Select **Save**.

8.3 Views

Views are an easy way for users to monitor important Locations, or group Location data according to job function.



Views can be set up to display Location status on a new dashboard image, or to display a trend graph for select Locations (useful when presenting a view on a remote display terminal). Create new views in **Views Manager** and access them in the **Overview** window.

8.3.1 Your Views

Each time you log in to viewLinc, the **Overview** window displays your views. Views are your custom collections of Locations created in Views Manager. You may also see views created by others that you are permitted to access (see "Views" above).

Use views to:

- Monitor current conditions at the Locations in a view (Status tab).
- Display a dashboard representing a view (Dashboard tab).
- Respond to alarms or generate alarm reports for all Locations in a view (Location Alarms tab).
- Create a trend based on data collected at all Locations in a view (Trend tab).

8.3.2 Creating Views

The Zone and Location tree structure in Sites and Sites Manager can only be modified by a viewLinc Administrator (with Manage Sites right). All other viewLinc users can create views to customize the display of important Locations.

Create a View

1. In **Views Manager** select **+ Add > Add View**.
2. In the **Add View** window, enter a name for the view.
3. Select **+ Add > Add Locations**.
4. Select Locations you want to include in the view:
   - Select all Locations in a Zone (select the Zone checkbox), or select individual Locations in one or more Zones.
   - Only the Locations within a selected Zone are included in a view. You can organize Locations within a view using folders.
5. Select **Add**.
6. Save the **View**.

If you are a member of a group with Manage Views right, you can also share your view (see "Sharing Views" on the next page).

Organize Locations in a View

1. In **Views Manager** on the **Views** tree, select a saved view.
2. Select **+ Add > Add Folder**. The menu is not active if there are unsaved changes in the tree.
3. In the **Add Folder** window, enter a name for the folder.
4. Select an icon to display on a dashboard.
5. Select **Add**.
6. On the **Views** tree, drag Locations into the new folder.

Set a Default View

Each time you log in your default view appears automatically.

1. In **Overview** on the **Views** tree, select a view.
2. Select **Options > Set as Default View**.

A different default view can be specified by each user.

8.3.3 Sharing Views

Manage Views

Allow other users to access a view you create. When a user logs in, new shared views display automatically in the **Overview** window. Sharing views is an easy way to customize a remote display (see "Creating Views for Remote Display" below).

Only the Locations the group has permission to view will be visible in the view.

Share a View

1. In **Views Manager** in the **Views** tree select a view.
2. On the **Permissions** tab select **Add**. The **Add Permissions** window appears.
3. Select one or more groups and then select the permission level you wish to give:
   - **View**: Allow group to see this view in their **Overview** window.
   - **Full Control**: Allow group to modify the view in **Views Manager**, or share the view with others.
4. Select **Save**.

8.3.4 Choosing a Default View

If you have been assigned views by others or have set up your own views, you can identify one as the default view. The default view opens automatically each time you log in, and displays the current dashboard (if one has been added).

Choose a Default View

1. In **Overview** in the **Views** tree, select a view.
2. Select **Options > Set as Default View**. A star icon appears on your default view, ☆.

To quickly find your default view, click the **Select Default View** toolbar icon, ☆.
To change the default view, simply select a new view in the **Views** tree, and select **Options > Set as Default View**.

8.3.5 Creating Views for Remote Display

Manage System, Manage Views

Create a view to control the content displayed on a stand-alone or wall-mounted display terminal.

Set Up a Remote Display View

1. Create a new view which includes the Zones and/or Locations you want to see on the display terminal (see "Views" on page 108).

2. Create a new group with Acknowledge Alarms permission for the Zones and/or Locations in the view (see "Groups" on page 59).
3. Share the view with the group (see "Sharing Views" on the previous page).
4. Ensure there is at least one user in the group. This user will be used to log in to the remote display. You can create a remote display-only user and add the user to the new group (see "Users" on page 59).
5. Set up the view as the user's default view (see "Choosing a Default View" on the previous page).

If remote display power is interrupted, the logged in user's default view automatically reconnects without requiring another log in.

8.4 Access viewLinc via Remote Display or Mobile Device

It is easy to set up viewLinc on a remote display terminal, or access the application on a mobile device.

- **Remote Display**: Set up a conveniently located visual display for a specific monitoring environment. A large monitor is best for areas requiring a larger visual display, without having to set up a complete workstation (with tower or keyboard). The remote display screen contains the **Overview** window tabs, with a collapsed **Views** navigation tree. Location information is defined by the default view assigned to the logged in user account.

If remote display power is interrupted, the logged in user's default view automatically reconnects without requiring another log in.

- **Mobile Device**: Monitor and acknowledge alarms from your smartphone or tablet.

viewLinc supports Point-of-Sale (POS) terminals. Please contact Vaisala Technical Support for assistance.

8.4.1 Remote Display Requirements

Before setting up a remote display terminal, ensure the following:

- The display hardware meets viewLinc System Requirements (see "Hardware Requirements" on page 1).
- The display can connect to a wired keyboard, or has a touchscreen keypad.
- A remote display view is available to the logged in user (see "Creating Views for Remote Display" on the previous page).

Any viewLinc user can log in to the remote display; however, the displayed data is defined by the view settings available to the logged in user.

8.4.2 Setting up a Remote Display

Set up a Remote Display Terminal

Only users assigned to the default viewLinc Administrator group can set up a remote display. Contact your IT network administrator if you require assistance.

1. Set up a remote display view (see "Creating Views for Remote Display" on page 110).
2. On the remote display terminal, create a Windows account and set it up for automatic log on (for example, http://support.microsoft.com/kb/324737).
3. In the Windows Startup folder, create a desktop shortcut to open a supported browser (see "Hardware Requirements" on page 1). This ensures the browser launches automatically when a user logs in.
4. Disable Windows updates to prevent popups on the display screen.
5. Launch the terminal browser and set the default home page to your viewLinc address, followed by **/display** (for example, **http://viewLinc.com/display**).
6. Set the remote terminal browser to work in full screen mode (press **[F11]**).
7. Log in to the viewLinc remote display application with the remote user account name and password. The user's default view opens automatically. These settings are remembered until a user logs out from the display application.

If the display reboots for any reason, the Windows auto logon setting automatically relaunches the browser and logs in as the last user.

8.4.3 Using viewLinc Mobile

If you have team members working away from your viewLinc network, they can continue to access viewLinc data with viewLinc Mobile. Requires a supported Android browser, or supported iOS Mobile Safari browser.

Open viewLinc Mobile

1. Open the Internet browser on your mobile device.
2. Enter your viewLinc IP address followed by **/mobile**. For example, **##.###.##.##/mobile**.

3. Select the language you want to display. When changing to a language other than English, the page automatically refreshes to display the new language.
4. Log in with your viewLinc user name and password.
5. Tap **Login**.

For more information, see "Viewing Data with viewLinc Mobile" on page 153.

9. Daily Tasks

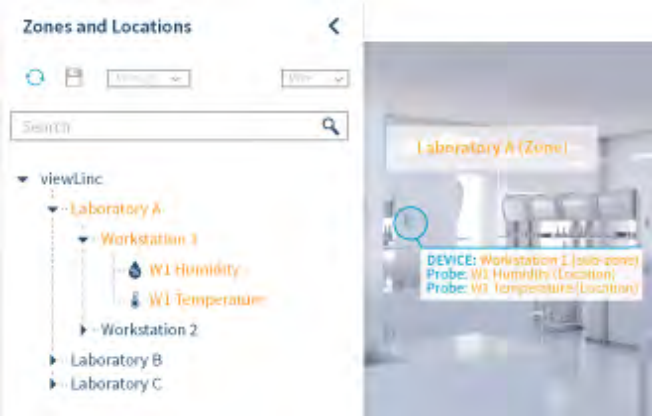
To help you become more familiar with the viewLinc workspace, it is recommended that you watch the tour, Using viewLinc (available on the viewLinc toolbar, under the Help menu).
For most viewLinc users, common daily tasks include:

- Monitoring conditions (see "Monitor Conditions" on page 119).
- Receiving and responding to alarms (see "Receive Alarm Notifications" on page 125).
- Temporarily pausing alarms (see "Pause Alarms" on page 129).
- Reviewing event log activities (see "Track Events" on page 132).
- Analyzing historical data (see "Building Trends" on page 137).
- Generating different types of reports (see "Reporting" on page 142).

Several tours are available and demonstrate how to perform daily tasks (Help > Tours).

9.1 Desktop Orientation

viewLinc is designed for easy identification of the monitored areas of your company—Zones and Locations. All the Zones and Locations you are permitted to view are visible in the **Sites** window, on the **Zones and Locations** navigation tree.



Tabs in the Sites and Overview windows are used to look at data in different ways:

Status	Dashboard	Location Alarms	Trend
View and monitor Zone and Location threshold and configuration status	Display an imported image to help you identify the physical environment being monitored.	View active alarm events for Zones and Locations in the tree.	Combine, contrast and compare Location history in visual graphs with real-time data.

The **Zones and Locations** tree can be expanded or collapsed to reduce visual clutter, and can be further customized into views. Views can be set up to contain only the Locations that are most important to you. To learn more about views, see "Your Views" on page 108.

9.1.1 Icons

Table 13 Icon Glossary

Home Screen Icons	
	Amount of time that has passed since receiving the last data transmission from any device. When view is regularly updating, icon is green. When view has not been able to update, icon is red
	Number of alarms currently active, on Locations user is permitted to view. Click to open the Alarms window and acknowledge alarms.
	An audible alarm is active. Click to cancel the sound and open the Alarms window.
	Open online Help or watch a tour.
	Log out or open the Users and Groups window to edit your personal details. Requires Manage System right.
UTC+7	Time zones in viewLinc are expressed in terms of an offset from UTC (Coordinated Universal Time). UTC is the time standard used to synchronize the clocks of computers over the internet.
Window Icons	
	Refresh - View the most current system modifications or data updates.
	Find in Tree - Highlight the selected Location in the Zones and Locations navigation tree.
	Quick Reports - Generate an Alarm-, Location History-, or System report for the selected Zone or Location.
	Measurement type: Temperature
	Measurement type: Humidity

◇	Measurement type: Other
10 01	Measurement type: Boolean
Lab A	An unlinked channel or Location displays in gray, italicized text.
~~Lab A~~	A deactivated Location displays in red, strike-out text.
	Vaisala device icon: RFL100-series
	Vaisala device icon: DL device
	Vaisala device icon: HMT140-series
	Vaisala device icon: 300-series
	Host icon: Access point
	Host icon: Device Host server
	viewLinc ES server
	Alarming paused
	Group
	Calibration alarm
	Communication alarm
	Configuration alarm
	Validation alarm

9.1.2 Search for Zones and Locations

If you have a long list of Zones and Locations, finding a specific Location may be time-consuming.

Full search

All users have access to the Search field at the top of the Zones and Locations navigation tree:

- In **Sites** on the **Zones and Locations** tree, enter your search criteria, then click the magnifying glass icon to activate the search (use the 'x' to clear the search field).

Search tips

- To search for a Location containing the word 'South', enter **South** (viewLinc searches for Zones or Locations containing the word South, or combination phrases, such as South-West or Fridge: South Corner).
- To search for a Zone starting with the term, 'Room', enter: **Room***.

- To search for a Zone starting with the term, 'Room', and all Locations starting with the term, 'Temp', enter: **Room*/Temp***.
- To search for a term with a single character difference, such as 'temperature' or 'température', enter: **temp?rature**.

See also, "Finding Linked Channels/Linked Locations" on page 50.

9.1.3 Working with Columns

Several viewLinc windows present Location details in tables, with a customizable set of columns.

Sort Column Content

Depending on the column contents, you can automatically sort alphabetically or numerically.

1. Hover your mouse over a column heading, then click the down arrow, ⌄.
2. On the menu that appears, select **Sort Ascending** or **Sort Descending** (you can also click on any column header to sort all the rows alphabetically in ascending or descending order).

Change Column Order

Use your mouse to move columns further left or right.

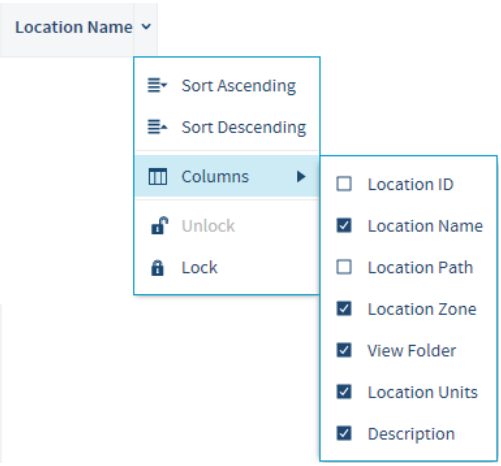
1. Open a window with movable columns: Overview, Sites, Alarms, Views Manager, Events, Users and Groups, and Sites Manager.
2. Select a column header name and click and hold to drag it right or left
3. Release the column and drop it when the drop indicator appears:

If the drop indicator does not appear, the column is in a fixed position and cannot be moved.

Show/Hide Columns

1. Hover your mouse over a column heading, then click the down arrow, ⌄.

2. On the menu that appears, select **Columns**, then select columns to display or deselect columns to hide.



3. Click outside the column list, or press **[Esc]** to close the list.

9.2 Monitor Conditions

To help you monitor only those Locations which are important to you, open the Sites or Overview window to view active threshold and device alarms. Alarms display only for the Locations or Zones you have permission to view.

You may be required to act upon an alarm in one of several ways:

- Threshold alarms can be acknowledged if you have acknowledge alarms permission on the Location.
- Device alarms can be acknowledged if you have acknowledge alarms permission for at least one Location linked to the device.

All active alarm types, including system alarms, display in the Alarms window. Alarms display only for the Locations or Zones you have permission to view. To learn more about alarm types, see "Types of Alarms" on page 64.

9.2.1 Identifying Active Alarms

All active alarm types display in the Alarms window—threshold alarms, device alarms, and system alarms; however, only the alarms for the Locations you are permitted to view are visible.
Use the Alarms window to acknowledge alarms, and print or export alarm reports.

You can view and acknowledge threshold and device alarms in the Sites or Overview windows, on the Location Alarms tab.

Active and Inactive Alarms

- Check the **Status** column to determine if an alarm is in an active alarm state, or was in an alarm state and is now inactive.
- Both active and inactive alarms that require an acknowledgement display in the grid.
- Inactive alarms that do not require acknowledgement do not display in the grid.
- The option to acknowledge all inactive alarms is restricted to members of the default viewLinc Administrator's group.

Alarm Acknowledgement

- Check the **Acknowledgement** column to determine if an alarm requires acknowledgement, and if it has been acknowledged.
- Threshold alarms can be acknowledged if you have acknowledge alarms permission for the Location.
- Device alarms can be acknowledged if you have acknowledge alarms permission for at least one Location linked to the device.
- System alarms can only be acknowledged by members of the default viewLinc Administrators group.

9.2.2 Sites or Overview Window: Status Tab

In the Sites or Overview window select the Status tab to review the severity levels of active threshold and device alarms.

Table 14 Status Tab Columns

Column	Definition
State	Current threshold condition (this column cannot be removed)
Type	Value being measured (this column cannot be removed)
Threshold Status	Summary of all active threshold alarms
Device Status	Connection status with viewLinc
Value	Current measured value

Column	Definition
Timestamp	Time of most recent recorded value
Threshold Summary	Description of threshold measurement criteria
Location ID	System-generated ID for reference purposes.
Location Path	Folder
Location Description	User-defined description
Device ID	System-generated ID for reference purposes.
Device Serial Number	Device-specific serial number
Device Address	Device Host location
Device Description	User-defined description
Sample Interval	Device-configured sample timing
Battery Level	Estimated remaining battery life
Signal Quality	Wireless reception quality
Channel ID	Device-configured channel ID
Channel Number	Device-configured channel number recording data for this Location
Channel Description	User-defined channel description

9.2.3 How does viewLinc identify threshold alarms?

When Location conditions (such as temperature and relative humidity) fall outside set threshold limits (specified in a threshold alarm template) a threshold alarm is triggered. When you apply a threshold alarm template to a Location, you can also add an alarm notification template to define who should be notified in the event of an alarm condition.

viewLinc can be configured to issue a notification at the first sign of a problem, sending an alert to a mobile device or computer display, as an SMS text or email notification. These notifications can also be scheduled for delivery on a specific day, time period, or according to a user's work schedule.

You can also set up threshold alarm color settings to provide a visual indication in the viewLinc display that an alarm condition is a mild concern or an extreme concern (colors are preset according to low to extreme concern).

9.2.4 What Happens When an Alarm is Triggered?

The alarms icon on the viewLinc header bar indicates the number of active alarms, . To view all active alarms, click the icon to open the Alarms window.

If you are set up to receive audible alarms, click the active alarm sound icon to turn off, .
Once an alarm condition is present, viewLinc can be configured to send different types of notifications to designated users or groups:

- **Email or SMS**: An email or SMS notification can be sent once or repeatedly, based on the alarm notification template being used for the Location, and according to a user's work schedule. An email or SMS message can automatically be sent to the users in a specific group.
- **Command**: An application can be launched to activate an external device or emit an audible alarm. For example, when an alarm condition occurs a command could activate a light or buzzer, or a have a computer page or phone a particular number.

You can configure viewLinc to send alarm notification to designated users or groups at different times, define the message content, require an email or SMS acknowledgement of an alarm, and set up predefined comments that make it easier for your team to respond.

- Create threshold alarm templates to define the conditions that will trigger an alarm (see "Creating Threshold Alarm Templates" on page 66).
- Create alarm notification templates to define who is notified in the event of threshold, device or system alarms (see "Creating Alarm Notification Templates" on page 80).

9.2.5 Viewing Conditions on Dashboards

Dashboard images are added to Zones and/or Locations by users with Manage Sites right and Full Control permissions. Dashboard images are added to views by users with Manage Views right.
All users can see site dashboards in the Sites window, and see view dashboards in the Overview window. Locations on a dashboard may display alarm status with color coded icons or background color (see "Changing Dashboard Display Settings" on page 53).

No alarm condition detected	Green	
High priority alarm	Red icon, or	
	with red background	
Medium priority Alarm	Orange	

Low priority alarm	Yellow	
Information priority alarm	Blue	

Dashboard Navigation Tools	
	Refresh/Undo: Update data readings, or if there are unsaved changes to the dashboard, the icon changes to allow you to undo all unsaved changes.
	View Trend: View a Location's historical data as a trend in a new browser window.
	Find in Tree: Highlight the selected Location in the Zones and Locations navigation tree.

9.2.6 Viewing Dashboard Location Trends

View Location History Trend

1. In the **Sites** window or the **Overview** window, select a Zone or Location using a dashboard image.
2. On the **Dashboard** tab, select a current data reading.
3. Select the **View Trend** toolbar button (or right-click on the data reading and select **View Trend**). In the open trend window, you can modify the trend start and end times, and the graph contents.

For more information about modifying the trend view, see "Create Trends" on page 136.

9.2.7 Finding Linked Dashboard Location

On any dashboard tab (Sites, Sites Manager, Overview, Views Manager), you can use the Find Linked Location tool help you identify your dashboard Locations in the Zones and Locations tree, or the Views tree.

Find a Linked Dashboard Location

1. In **Sites** select a Zone or Location which is using a dashboard image (or in **Views Manager** on the **Views** tree, select a view).
2. On the **Dashboard** tab, select a current data reading.
3. Select the **Find in Tree** toolbar button (or right-click on the dashboard data reading). A yellow highlight bar appears temporarily in the Zones and Locations tree (or Views tree) to indicate the corresponding Location.

9.2.8 Printing or Exporting Current Alarm Data

For historical record-keeping purposes, you may want to print a hard copy of active alarm conditions. To print an alarm report for a specific time period, see "Alarm Period Reporting" on page 145.

In the Alarms, Sites or Overview window, you can print current alarm data directly to your printer, or export the data to a spreadsheet (.tsv). In the spreadsheet format, you can modify how you want the information to display, to meet your company's reporting requirements.

To learn how to generate alarm reports for specific alarm types or specific time periods, see "Creating Alarm Reports" on page 150.

Print Current Alarm Data

- In the **Alarms** window, select **Print**. Choose your desired print settings and then print.
- In the **Sites** or **Overview** window on the **Location Alarms** tab, select one or more active alarms, then select **Print**. Choose your desired print settings and then print.

Export Current Alarm Data

1. To export active data in the **Alarms** window:
   - Select **Export to Excel**. A list of all active alarms export to a .tsv format file in a spreadsheet program (default spreadsheet software is set on user PC).
2. To export active data in the **Sites** window:
   a. On the **Zones and Locations** tree, select one or more Locations or Zones with currently active alarm conditions.
   b. On the **Location Alarms** tab select **Export to Excel**. A list of all active alarms export to a .tsv format file in a spreadsheet program.
3. To export active data in the **Overview** window:
   a. On the **Views** tree, select one or more views containing Locations with currently active alarm conditions.
   b. On the **Location Alarms** tab select **Export to Excel**. A list of all active alarms export to a .tsv format file in a spreadsheet program.
4. The file download (.tsv) appears in the status bar at the bottom of the display window. Double-click the file icon to open the **activealarms.tsv** file in the spreadsheet program of your choice.
5. At the prompt, select **Save** (the file is saved to your default downloads folder) or **Open**. If Windows does not recognize the file format, select Excel from your Programs folder to view the file and make changes.

9.3 Receive Alarm Notifications

If you are a member of a group that is responsible for responding to alarms, you may be notified of an alarm condition or event in a number of ways, such as:

Receive an email or SMS notification

See a visual indicator in viewLinc or on an external device

Hear an audible alarm

You can respond to an alarm by acknowledging the alarm in viewLinc. If your system is set up to accept remote acknowledgement, you can reply to an email or SMS alarm notification.

9.3.1 Ways to Acknowledge Alarms

An acknowledgement indicates to the viewLinc system and others that an alarm condition is recognized. Details provided during acknowledgement about the steps taken to correct the alarm condition, and any comments, are tracked as an event in the Events window.

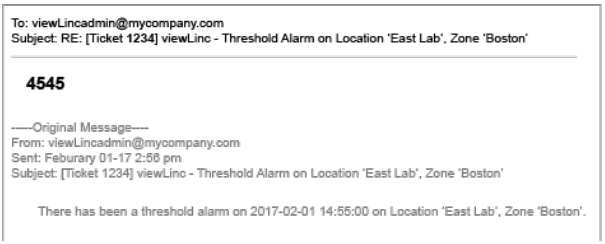
If you work remotely, alarms can be acknowledged with a mobile device. See "Acknowledging an Alarm with viewLinc Mobile" on page 155.

Only viewLinc users with Acknowledge Alarms permission (or higher) for the Locations where an alarm is occurring can acknowledge alarms (see "Applying Group Permission to Zones" on page 103).

Acknowledge Alarms via Email or SMS

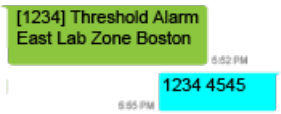
Alarm notifications may be received and acknowledged by email or SMS text, if your viewLinc system supports remote acknowledgement (see "Email and SMS Settings" on page 96).

1. Open the alarm notification.
   - Email notifications are sent from the viewLinc server administrator account (for example, viewLinc.boulder@companyemail.com).
   - SMS notifications are sent from the viewLinc SMS modem number.
2. To acknowledge an email, send a reply which includes the default subject line (with ticket number), and enter your PIN in the body of the message. For example:



Sending a reply without a PIN in the email message body area or the ticket number in the subject line does not acknowledge the alarm.

3. To acknowledge an SMS notification, send a reply from your phone which includes the ticket number and your PIN.



Only SMS replies sent from your recognized phone number and PIN will acknowledge an alarm.

Acknowledge Alarms in Sites or Overview

1. In the **Sites** or **Overview** window select the **Location Alarms** tab.
2. Review the list of all active alarms (**Status** column).
3. Use the **Acknowledgement** column to identify alarms that require acknowledgement. To acknowledge multiple alarms, press the **[Ctrl]** or **[Shift]** keys while you select multiple alarms.
4. Select **Acknowledge** (or right-click and select Acknowledge).

5. In the **Acknowledge Alarms** window, enter a description of the actions taken to correct the alarm condition and any additional comments. You can select a comment from the predefined comments drop-down list, if there are any available, or enter your own comment in the text box.

For example, if you receive a high temperature alarm for a refrigeration facility and notice that a refrigerator door has been left open, close the door and describe this action in the Acknowledge Alarms window.

6. Select **Acknowledge**. Your comments and actions are added to the event log and the **Acknowledge Alarm** prompt closes. Locations are updated with this change in status, as well as the **Acknowledgement** column in the Alarms window.

Acknowledge Alarms in the Alarms Window

The Alarms window displays all alarm types, listed in priority order. Device and system alarms are visible to all users, only alarms for Locations you are permitted to view are visible.

Only a member of the default viewLinc Administrators group can acknowledge system alarms.

1. In the **Alarms** window, review the list of all active alarms (**Status** column).
2. Use the **Acknowledgement** column to identify alarms that require acknowledgement. To acknowledge multiple alarms, press the **[Ctrl]** or **[Shift]** keys while you select multiple Alarms.
3. Select **Acknowledge** (or right-click to select Acknowledge).
4. In the **Acknowledge Alarms** window, enter the actions taken and enter a comment. You can select a comment from the predefined comments drop-down list, if available, or enter your own comment in the text box.
5. Select **Acknowledge**. Your comments and actions are added to the event log. Locations are updated with this change in status, as well as the Acknowledgement column in the Alarms window.

Acknowledge System Alarms

System alarms (database or event log validation alarms) can only be acknowledged in the Alarms window. System alarms remain in the Alarms window until they are acknowledged.

You must be a member of the viewLinc Administrators group to use the Acknowledge all system alarms function.

1. In the **Alarms** window on the alarms grid, right-click on a system alarm and select **Acknowledge**.
2. In the **Acknowledge Alarms** window indicate any action taken, select a predefined comment, if available, or enter any additional comments about why you are acknowledging an inactive alarm.
3. Select **Acknowledge**.

Acknowledge All System Alarms

1. In the **Alarms** window select **Acknowledge > Acknowledge All System Alarms**. Multiple Location selection is not required.
2. In the **Acknowledge Alarms** window indicate any action taken, select a predefined comment, if available, or enter any additional comments about why you are acknowledging inactive alarms.
3. Select **Acknowledge**.

9.3.2 Acknowledging Inactive Alarms

Some companies may require you to acknowledge inactive alarms. Inactive alarms indicate that an alarm was triggered, but the alarm condition is no longer present.
To acknowledge inactive threshold or device alarms, you can use the Alarms, Sites or Overview windows.

Only a member of the default viewLinc Administrators group can acknowledge inactive alarms.

Acknowledge an Inactive Alarm - Alarms Window

1. In the **Alarms** window on the alarms grid, right-click on an inactive alarm and select **Acknowledge**.
2. In the **Acknowledge Alarms** window indicate any action taken, select a predefined comment, if available, or enter any additional comments about why you are acknowledging an inactive alarm.
3. Select **Acknowledge**.
   - Acknowledged inactive device communication alarms remain listed in the grid.
   - Acknowledged device calibration due notifications remain listed in the grid.
   - Acknowledged inactive threshold alarms disappear from view.

Acknowledge All Inactive Alarms - Alarms Window

1. In the **Alarms** window select **Acknowledge > Acknowledge All Inactive Alarms**. Multiple Location selection is not required.
2. In the **Acknowledge Alarms** window indicate any action taken, select a predefined comment, if available, or enter any additional comments about why you are acknowledging inactive alarms.
3. Select **Acknowledge**.

Acknowledge an Inactive Alarm - Sites Window

1. In the **Sites** window on the **Zones and Locations** tree, select a Zone.
2. On the **Location Alarms** tab in the alarms grid, right-click on an inactive alarm and select **Acknowledge**.
3. In the **Acknowledge Alarms** window indicate any action taken, select a predefined comment, if available, or enter any additional comments about why you are acknowledging an inactive alarm.
4. Select **Acknowledge**.

Acknowledge an Inactive Alarm - Overview Window

1. In the **Overview** window on the **Views** tree, select a view.
2. On the **Location Alarms** tab in the alarms grid, right-click on an inactive alarm and select **Acknowledge**.
3. In the **Acknowledge Alarms** window indicate any action taken, select a predefined comment, if available, or enter any additional comments about why you are acknowledging an inactive alarm.
4. Select **Acknowledge**.

9.3.3 Responding to Audible Alarms

If your system generates audible alarms, they are only received by users logged in to viewLinc with the audible alarm preference enabled in their user profile. The user PC must have volume turned on.
When an audible alarm is turned off, it is not recognized in viewLinc as an acknowledgement of the alarm. Audible alarm activation and cancellation are not tracked in the events log.

Turn off an Active Audible Alarm

1. To cancel an active audible alarm, select the red audible alarm icon at the top of the viewLinc screen, .
2. To cancel an active audible alarm and acknowledge the alarm:
   a. Select the red audible alarm icon at the top of the viewLinc screen, . The icon changes to an alarm icon, .
   b. Select the alarm icon to open the **Alarms** window.
   c. Locate the alarm in the alarms table and then select **Acknowledge > Acknowledge Alarm**.
3. Complete the **Acknowledge Alarms** window. To learn more about acknowledging alarms, see "Acknowledge Alarms in the Alarms Window" on page 127.

9.4 Pause Alarms

To avoid receiving unnecessary threshold or device alarm notifications when moving devices, or if a known situation will result in conditions exceeding set thresholds, you can pause threshold alarming on one or more Locations, or device alarming on a single device or all devices connected to a host.
Paused alarms reactivate automatically after 24 hours, if not resumed manually before that time. Data collection continues during a pause period at all linked Locations.

You require Configure Alarms permission for the Locations you want to pause. Only members of the Administrators group can pause host alarms.

How is this different from disabling an alarm?

Threshold and device alarms remain disabled until manually set back to enabled (see "Types of Device Alarms" on page 71).

9.4.1 Pausing Threshold Alarming

Pause threshold alarming to avoid triggering unnecessary threshold alarms. For example, if you are moving monitored inventory out of one facility and moving it to another, or are bringing in additional inventory and the activity will impact device readings.
When you pause threshold alarming, viewLinc continues to monitor your Location, but ignores all threshold levels. Data continues to be logged on your devices, and device alarming is still active.

You can pause threshold alarms on one or more Locations in the Sites window, or pause all threshold alarms for Locations assigned to a view in the Overview window.

If you work remotely, alarms can be paused from a mobile device. See "Pause or Resume Alarming with viewLinc Mobile" on page 155.

You require Configure Alarms permission for each Location you want to pause alarming.

Pause Threshold Alarming on a Location

1. In **Sites** on the **Zones and Locations** tree select one or more Locations or Zones (Ctrl+click).
2. Select **Options > Pause Threshold Alarms** (or right-click to select **Pause Threshold Alarms**).
3. In the **Pause Threshold Alarms** window, specify:
   a. **Duration**: Enter the length of time you want alarming paused (1 to 24 hours).
   b. **Add comments**: If required, enter a reason for pausing threshold alarms using a predefined comment (if available), or enter your own notes in the text box.
4. Select **OK**. The active alarms list on the Location Alarms tab refreshes automatically.

Pause Threshold Alarming in a View

1. In the **Overview** window on the **Views** tree, select one or more views ([Ctrl]+click).
2. Select **Options > Pause Threshold Alarms** (or right-click to select **Pause Threshold Alarms**).
3. In the **Pause Threshold Alarms** window, specify:
   a. **Duration**: Enter the length of time you want alarming paused (1 to 24 hours).
   b. **Add comments**: If required, enter a reason for pausing threshold alarms using a predefined comment (if available), or enter your own notes in the text box.
4. Select **OK**. The active alarms list on the Location Alarms tab refreshes automatically.

9.4.2 Pausing Device or Host Alarming

Pause device or host alarming to avoid unnecessary alarms (for example, if you are renovating a controlled space and need to shut down power temporarily). When you pause alarming, viewLinc continues to monitor your Location(s), but ignores all device and host communication interruptions. Pausing device or host alarms does not interrupt data collection for any linked Locations.

You can pause alarms on one or more Locations in the Sites window, or pause all Locations assigned to a view in the Overview window.

If you work remotely, alarms can be paused from a mobile device. See "Pause or Resume Alarming with viewLinc Mobile" on page 155.

You require Configure Alarms permission for the Locations you want to pause. Only members of the Administrators group can pause host alarms.

Pause Device Alarming on a Single Location

1. In the **Sites** window on the **Zones and Locations** tree, select a Location.
2. Select **Options > Pause Device Alarms** (or right-click to select **Pause Device Alarms**).

3. In the **Pause Device Alarms** window, ensure you have selected the correct data logger channel, then select **Yes** to continue.
   - **Duration**: Enter the length of time you want alarming paused (1 to 24 hours).
   - **Add Comments**: If required, enter a reason for pausing device alarming. Select a predefined comment, if available, or enter your own notes in the editable text box.
4. Select **OK**.

Pause Device Alarming on Multiple Locations

1. In the **Sites** window on the **Zones and Locations** tree, select multiple Locations or Zones ([Ctrl]+click), then select **Options > Pause Device Alarms** (or right-click to select **Pause Device Alarms**).
2. In the **Pause Device Alarms** window review the selected data logger channels, then select **Yes** to continue.
   - **Duration**: Enter the length of time you want alarming paused (1 to 24 hours).
   - **Add Comments**: If required, enter a reason for pausing device alarming using a predefined comment (if available), or enter your own notes in the editable text box.
3. Select **OK**.

Pause Device Alarming in a View

1. In the **Overview** window on the **Views** tree, select one or more views ([Ctrl]+click).
2. Select **Options > Pause Device Alarms** (or right-click to select **Pause Device Alarms**).
3. In the **Pause Device Alarms** window select **Yes** to continue.
   - **Duration**: Enter the length of time you want alarming paused (1 to 24 hours).
   - **Add Comments**: If required enter a reason for pausing host alarming using a predefined comment (if available), or enter your own notes in the text box.
4. Select **OK**.

Pause Host Alarming

1. In the **Sites** window on the **Zones and Locations** tree, use your mouse to select a Location then select **Options > Pause Host Alarms** (or right-click to select **Pause Host Alarms**).
2. In the **Pause Host Alarms** window select **Yes** to continue.
   - **Duration**: Enter the length of time you want alarming paused (1 to 24 hours).
   - **Add Comments**: If required enter a reason for pausing host alarming using a predefined comment (if available), or enter your own notes in the text box.
3. Select **OK**.

9.4.3 Resuming Threshold, Device or Host Alarming

You can resume alarming on one or more Locations in the Sites window, or resume alarming for Locations assigned to a view in the Overview window.

Resume Alarming

You require Configure Alarms permission for each Location you want to pause alarming.

1. In the **Sites** window on the **Zones and Locations** tree, select the Location or Zone which currently has alarming paused. Or, in the **Overview** window on the **Views** tree, select a view which currently has alarming paused.
2. Select **Options > Resume [...] Alarms** (or right-click to select Resume [...] Alarms).

9.5 Track Events

Use the Events window to analyze events and determine when and where particular problems occurred, or to diagnose a situation that requires troubleshooting.

All viewLinc system activity is treated as an event, and all events are tracked in the events log. Data tracked as an event is different from monitored data logged in a device. Here are some key differences:

- Events occur within the viewLinc system: alarms, alarm acknowledgements, system configuration changes, general system notifications.
- Devices track the changes within the environment being monitored: temperature, relative humidity, air pressure, or voltage.

To ensure viewLinc continuously monitors and stores event log history, event validation alarms notify you if the viewLinc event log has been tampered with externally.

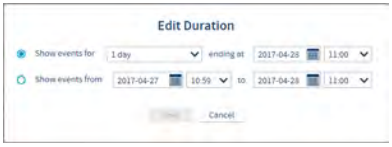
9.5.1 Viewing Events

The Events window displays the event log, a text-based listing of all event types—alarms, device changes, system updates—occurring with the software or affecting devices on your system.

To ensure no tampering has been recorded, check the Event Log Status in the top right corner of the Events window.

View Events

1. Open the **Events** window.
2. To view events during a specific period, select **Edit Duration**.
3. Specify the time frame.



- **Show events for/ending at**: Choose a time frame with an end date.
- **Show events from/to**: Enter a specific date and time, or use the calendar buttons to make your selection.

4. To refine the displayed events, select **Show Advanced Filters**.

5. Select from the available filters.
   - **Category**: Select one or more types of events to include in the export.
   - **Locations**: Select the Zones and/or Locations to include.
   - **Groups** and **Users**: Show events recorded by selected groups or users.
6. Select **Apply Filters**. To reset filters, select **Clear**.

After setting filters, you can use the Search field to display only events acknowledged by specific users or groups, or only events occurring at a specific Location.

7. To view additional event information, such as comments and details added to custom events, double-click an event to open the **Event Details** window.

Event details can be used to review more specific information about why an alarm event occurred, or to see comments entered.

9.5.2 Adding Comments to Events

You may want to add comments to an event log entry to provide details about why an event occurred or what was done in response to an event or problem.

Add an Event Comment

1. In the **Events** window, select an event, then select **Add Comment**.
2. In the **Add Comment** window, select from the list of predefined comments (if available), or enter your own comment.
3. Select **Save**.

View an Event Comment

1. In the **Events** window, select a row containing an event (a comment icon (🗨) appears in the **Comments** column).
2. Double-click the event row.
3. In the **Event Details** window, comments appear on the last line of the grid.

Comments also appear in the Event Log Report.

9.5.3 Adding Custom Events

When you create a custom event (perhaps to indicate a system upgrade), the new event appears at the top of the Events window.

Add an Event

1. In the **Events** window, select **Add Custom Event**.
2. Fill in the custom event message and details, then select **Save**.
   - **Event message**: Enter a short description that will display in the Events window **Message** column.
   - **Details**: Enter a full description of the custom event (required). This information is included when printing the Event Log report.
3. Save the new event. It appears at the top of the events grid.

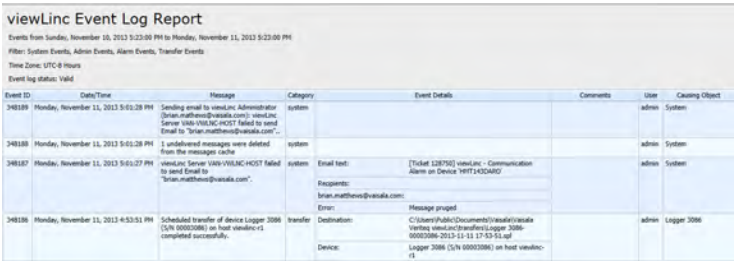
9.5.4 Printing and Exporting Event Logs

For record-keeping purposes, you may need to generate a printed record of events. You can generate a standard viewLinc Event Log Report, or export the record details to a spreadsheet (using .tsv format), for custom reporting.

Print an Event Log

1. In the **Events** window, specify parameters for the report:
   a. To choose a preset or custom timeframe select **Edit Duration**:
      - **Show events for/ending at**: Choose a timeframe with end date.
      - **Show events from/to**: Enter a specific date and time, or use the calendar buttons to make your selection.
   b. To refine the report contents, select **Show Advanced Filters**:
      - **Category**: Check the types of events to include in the report.
      - **Locations**: Show events occurring at one or more selected Zones and/or Locations.
      - **Groups/Users**: Show events recorded by selected groups or users.
2. Select **Apply Filters**. To reset filters, select **Clear**.

3. Select **Print**. In a new browser window, a printer-friendly event log report opens.


viewLinc Event Log Report

Events from Sunday, November 10, 2013 5:23:00 PM to Monday, November 11, 2013 5:23:00 PM

Filter: System Events, Admin Events, Alarm Events, Transfer Events

Time Zone: UTC-8 Hours

Event log status: Valid

Event ID	Date/Time	Message	Category	Event Details		Comments	User	Causing Object
348189	Monday, November 11, 2013 5:01:28 PM	Sending email to viewLinc Administrator (brian.matthews@vaisala.com): viewLinc Server VAN-VWLNC-HOST failed to send Email to "brian.matthews@vaisala.com"...	system				admin	System
348188	Monday, November 11, 2013 5:01:28 PM	1 undelivered messages were deleted from the messages cache	system				admin	System
348187	Monday, November 11, 2013 5:01:27 PM	viewLinc Server VAN-VWLNC-HOST failed to send Email to "brian.matthews@vaisala.com".	system	Email text: Recipients: brian.matthews@vaisala.com: Error:	[Ticket 128750] viewLinc - Communication Alarm on Device 'HMT143DARO' Message pruged		admin	System
348186	Monday, November 11, 2013 4:53:51 PM	Scheduled transfer of device Logger 3086 (S/N 00003086) on host viewlinc-r1 completed successfully.	transfer	Destination: Device:	C:\Users\Public\Documents\Vaisala\Vaisala Veriteq viewLinc\transfers\Logger 3086-00003086-2013-11-11 17-53-51.spf Logger 3086 (S/N 00003086) on host viewlinc-r1		admin	Logger 3086

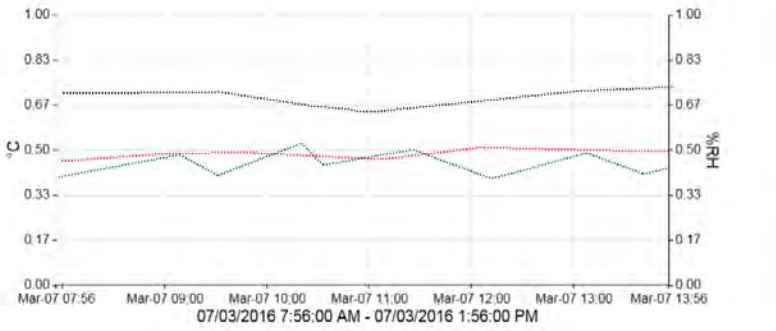
4. Set your print parameters and print the report (**File > Print**).

Export an Event Log

1. In the **Events** window, specify parameters for the export:
   a. To choose a preset or custom timeframe select **Edit Duration**:
      - **Show events for/ending at**: Choose a timeframe with an end date.
      - **Show events from/to**: Enter a specific date and time, or use the calendar buttons to make your selection.
   b. To refine the export contents, select **Show Advanced Filters**:
      - **Category**: Check the types of events to include in the export.
      - **Locations**: Show events occurring at one or more selected Zones and/or Locations.
      - **Groups** and **Users**: Show events recorded by selected groups or users.
2. Select **Apply Filters**. To reset filters, select **Clear**.
3. Select **Export**.
4. To open the file, specify the spreadsheet program to use for .tsv files. Exported .tsv files open in read-only mode.

9.6 Create Trends

To better understand condition fluctuations at your Locations, create a trend. Trends display current or historical data readings for one or more Locations in a graphical format.



Multi-Location trends can be created in the Sites window or Views Manager window, on the Trend tab. Each trend graph can contain data for up to 16 Locations and up to 4 measurement types.

Use the View Trend toolbar button, , available in the Overview window (Status and Dashboard tabs), Sites window (Status tab), and Sites Manager window (Location Properties and Dashboard tabs) for a quick view of a single Location trend.

Table 15 Key Elements in a Trend Graph

Item	Description
Graph area	A graphical representation of Location data history.
Left and right Y-axis measurement scales	Shows the range of data displayed in the graph. You can modify the scale minimum and maximum values (see "Modifying Trends" on page 139).
X-axis time scale (bottom)	Shows the reporting time frame. Use the forward and back arrows below the graph to adjust the reporting timeframe (see "Trend Navigation" on page 138).
Location lines	Indicate path of historical measurement readings based on a specific date or time frame. Move your mouse and hover over a specific point to show the specific X- and Y-axis values.

Item	Description
Threshold lines	Color-coded line (based on threshold setting) to show historical threshold values. Move your mouse and hover over a specific point to show the specific X- and Y-axis values.
Locations / Group Statistics	View Location details in separate rows, or group statistics for all Locations.

9.6.1 Building Trends

Compare live data for multiple Locations, and display the data in a graph. You require view permission for all Locations you want to include in the trend graph.

You can build trends in the Sites, Overview or Views Manager windows.

Build a Trend

1. In the **Sites**, **Overview** or **Views Manager** window, navigate the **Zones and Locations** tree and select a Location you want added to the trend. Or, in **Views Manager** on the **Views** tree, select a view that contains the Location(s) you want to view as a trend.
2. Select the **Trend** tab.
3. Use your mouse to drag the selected Location or view to the **Trend** pane. You can continue to build upon and modify your trend at any time by simply dragging more Locations onto the graph (up to 16 Locations, up to 4 measurement units).
4. To modify the trend start date, select **Edit Trend**:
   - **Show trend for [time] ending at [date/time]**: Trends only display data logged up to the current time. You can select a set trend time period up to 1 month prior to the current date/time.
   - **Show trend from [date/time] to [date/time]**: If you want to see more historical data, select a specific time period to show (you cannot select a future date).
   - **Include real-time samples**: When checked, this option includes more frequent real-time samples alongside with the logged device data (based on the device sample rate).
   - **Show data markers**: When checked, this option adds small markers on the trend graph, indicating exactly when the readings took place.
   - **Vertical Axis Scale**: For each measurement value, you can set the minimum or maximum range you want included in the trend, or choose Auto to include all values.

When you create a trend in Sites or Views Manager window, you can save the trend as a view and share it with team members, or save the graph as a Location history report for future reference (see "Saving Trends" on page 140).

9.6.2 Trend Functions

The Trend tab is available in the Overview and Sites windows. Most functions are the same, except where indicated:

- **Refresh**: Retrieve most recent data readings from server. If **Updates on** is enabled, the trend graph automatically retrieves data readings every minute.
- **Open trend in new window**: (Overview window) Opens the trend in a new window.
- **Save As**: (Sites window) Save the current trend graph as a single page Location history report or as a view. To save as a report requires Manage Reports right. To save as a view requires Manage Views right.
- **Edit Trend**: Modify the trend start or end date, set the time duration, select line properties, and specify axis scale values.
- **Clear Trend**: (Sites window) Clear all Location data lines from the trend graph, or clear lines and reset trend graph settings to default.

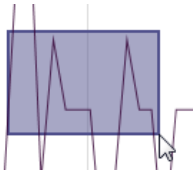
Use the Locations grid below the trend graph to remove individual Location lines (see "Modifying Trends" on the facing page).

- **Updates on/off**: Update real-time data readings, to a maximum trend duration of 7 days.

9.6.3 Trend Navigation

The Trend tab contains navigation controls which allow you to navigate historical data trends and refresh the view as required:

▶ ◀	Adjust the trend time frame by increments of 1/4. For example, if you are viewing 6 hours of data, the frame moves forward or back 1.5 hours; if you are viewing 1 month of data, the frame moves forward or back 1 week. The frame can only move forward up to the current time.
◀◀ ▶▶	Adjust the trend time frame by a full increment. For example, if you are viewing 6 hours of data, the frame moves forward or back 6 hours; if you are viewing 1 month of data, the frame moves forward or back 1 month. The frame can only move forward up to the current time.
▶|	Show the most recent data (up to current date/time).
Updates on	Select this option to continuously update the trend with most current readings (this option has the same effect as pressing the ▶| button).
	To see close-up trend details, click and drag across a trend line. Drag right to zoom in/drag left to zoom out.



Navigating or zooming within the trend graph automatically unchecks the **Updates on** option. As you navigate within the trend graph, you are then viewing historical data.

9.6.4 Modifying Trends

You can change both the content and the display settings of a trend graph in either the Sites window or the Views Manager window. You can only modify trend display settings in the Overview window.

Trends modified in the Sites or Views Manager windows can be saved and shared with others (see "Saving Trends" on the next page).

Show/Hide selected Locations

1. In **Sites** on the **Trend** tab, select **Locations** below the graph.
2. In the **Show** column, select or deselect the Locations to include on the graph. Select **Delete** to remove the Location data from the graph completely.

View Trend Max/Min Statistics

1. In **Sites** on the **Trend** tab, select **Group Statistics** below the graph.
2. In the **Group Statistics** tab to see the max/min ranges for all Locations together.

Change Trend Duration/Data/Scale

1. Select **Edit Trend**.
2. To modify trend duration:
   - Select a preset time range. Graph will display data for the selected time range, prior to the specified end time (default is 6 hours ending at current time).
   - Select a time period based on specific calendar dates.
3. To modify line properties (by default these options are not selected):
   - **Include real-time samples**: Update Location trend lines to include both data collected in viewLinc based on viewLinc scan rate, and data reported by a device based on device sample rate.
   - **Show data markers**: Add points on Location trend lines to indicate when a data sample was recorded.
4. Define the vertical axis scale min/max graph range:
   - For each measurement type included in a graph, you can set the minimum and/or maximum value automatically based on actual readings, or set specific min/max values to include in the graph (by default, the min/max settings are automatically generated).

Clear Trend - Sites Window

- To remove all Location graph lines select **Clear Trend > Delete all Lines**. Trend settings remain intact.
- To remove all graph lines and return to the default trend settings, select **Clear Trend > Reset to Defaults**.

Refresh Trend Data

- Select **Show most current data**, or select **Updates on** to refresh the graph with most recent data collected by the viewLinc Enterprise Server.
- **Refresh**: Force retrieval of the most recent data collected by the viewLinc Enterprise Server. If **Updates on** is enabled, the trend graph automatically retrieves real-time data readings every minute.
- **Updates on/off**: Update trend with real-time data readings, up to a maximum trend duration of 7 days. If the trend duration is set for more than 7 days, the **Updates on** setting is automatically disabled.

9.6.5 Saving Trends

Manage Views, Manage Reports

There are 2 ways to save a trend:

- In the Sites window, save a trend as a view, and share it with other users or groups. Requires Manage Views right.
- In the Sites or Views Manager window, save a trend as a Location History report. Requires Manage Reports right.

Save a Trend as a View

1. In the **Sites** window, create a trend (see "Building Trends" on page 137).
2. Select **Save As > View**.
3. Enter a name to identify the view, then select **Save**.

Notify your team that the view is available in the **Overview** window.

Save a Trend as a Report

1. In the **Sites** window or **Views Manager** window, create a trend (see "Building Trends" on page 137).
2. Select **Save As > Location History Report**.
3. Enter a name to identify the report, then select **Save**.

Notify your team that the report is available in the **Reports** window.

9.7 Viewing Quick Trends

To quickly view Location data in a trend graph use the View Trend toolbar button, , available in Sites, Sites Manager and Overview windows.
You can view multiple, individual Location trends at once by opening multiple trend view windows. If you use Internet Explorer, ensure your browser is set up to open new links in a new window or tab (**Tools > Internet options > General**).

Configure an alarm to automatically display a trend in response to an alarm condition (see "Alarm Notifications" on page 79).

Quick Trend - Sites Window

1. In the **Sites** window on the **Zones and Locations** tree, select a Zone.
2. On the **Status** tab select a Location, then select the **View trend** toolbar button (or right-click to select **View trend**).
3. In the open **Trend** window, you can modify the trend start and end times, and the graph contents.

Quick Trend - Sites Manager Window

1. In the **Sites Manager** window on the **Zones and Locations** tree, select a Zone.
2. On the **Location Properties** tab select a Location, then select the **View trend** toolbar button (or right-click to select **View trend**).
3. In the open **Trend** window you can modify the trend start and end times, and the graph contents.

Quick Trend - Overview Window

1. In the **Overview** window on the **Views** tree, select a view.
2. On the **Status** tab select one or more Locations, then select the **View trend** toolbar button (or right-click to select **View trend**).
3. In the open **Trend** window, you can modify the trend start and end times, and the graph contents.

For more information about modifying trends, see "Create Trends" on page 136.

9.8 Reporting

Using the historical data collected by Vaisala devices, you can automatically create reports to analyze changes in data over a specific period of time, or compare conditions recorded by different devices. Reports can be used to:

- Review data readings for specific monitored areas over selected time periods.
- Obtain summary or detailed alarm history values for one or more Locations, including alarm duration, acknowledgements and corrective actions taken.
- Produce presentation-ready materials, including data, statistics and graphs.
- Deliver data by email on a schedule to specific personnel.

9.8.1 Types of Reports

viewLinc provides a set of default reports to help you easily view data trends or alarm statistics. Users with Manage Reports right can create custom reports to set specific content parameters, and make them easily accessible by others from the Sites and Overview windows (see "Sharing Quick Reports" on the facing page).

No specific rights are required to generate reports – any user can generate a report for a Zone or Location to which they have View permission.

- **Alarm reports**: Provide an overview of alarm events over a period of time. Events related to every alarm are grouped together and presented in a readable form.
- **Location History reports**: Provide a detailed history of Location data values presented in both graphical and tabular format.
- **System reports**: Provide overall snapshots of specific system information, such as system configuration, and lists of available templates. You can also generate a system report to list current users and groups, Locations, and permission details.

9.8.2 Generating Reports

All available reports are listed in the Reports window. The reports available are either default viewLinc reports, reports you have created, or reports that others have shared with you (see "Generating Quick Reports" on page 144).

Reports are templates, waiting to be populated with generated data. Once a report is generated, open the Downloads tab to find out when the report is ready to print (a generated .pdf file) or export to a spreadsheet (a generated .tsv file). See "Viewing Report Downloads" on page 144.

You can also automatically generate and send a report to an email recipient (.pdf) on a regular schedule. Any sent report can also be downloaded from the Downloads tab.

Generated report content is limited to the Zones and/or Locations you have permission to view. If you require additional Location information in a report, request view permission for the Zone/Location, or ask to receive reports by email.

Generate Report Data

1. In **Reports** select a report, then select **Generate**.
2. Choose a report option:
   - **PDF**: This option is available for Alarm and Location History reports. Choose this option to generate the report according to PDF settings specified in the Scheduled Generation parameters.
   - **Excel (.tsv)**: Generate the report in .tsv format.
   - **Email**: Generate and send report to predetermined list of users or groups, as a .pdf attachment (system reports are only .xls attachments). Once generated, the report is sent according to the report's scheduled generation parameters.

   Automatically generated and emailed report content is generated according to the recipient's language preference.
   - If no language preference is specified for the recipient, the content is generated in the language specified for the report (language can be specified for reports that are automatically generated and saved).
   - If no language is specified for the recipient or the report, the content is generated in the system default language (System Configuration > Preferences).
3. On the **Downloads** tab, the most recently generated report appears at the top of the list. Once report generation is complete, open or save the report by clicking the link in the **Progress** column.

Manually generated and scheduled reports are available to download for 24 hours, to ensure that any reports auto-generated during off-peak hours remain available in regular work hours.

9.8.3 Sharing Quick Reports

Manage Reports

Allow other users to quickly generate a report from the Sites and Overview windows. Report content is limited to the Zones or Locations a user or group has permission to view.

Administrators, users who are part of groups assigned Manage Reports right, and report owners can specify which of their reports can be made available as a quick report.

Quick report content is generated according to the user's logged in language.

Add a Quick Report

1. In the **Reports** window, select a report, then select **Edit**.
2. In the **Available as quick report** field, select **Yes**.
3. Save the change.

9.8.4 Generating Quick Reports

A quick report is a report made available to others to generate easily from the Sites or Overview windows. The structure of the report adheres to the structure defined by the report owner, but the content of the report (data) is limited to the Zones and Locations the user is permitted to view.
If you have Manage Reports right, you can make a report available to others as a quick report (see "Sharing Quick Reports" on the previous page).

When a user generates a Quick Report, the content is generated according to the user's logged in language, even if it is different from their language preference.

Generate a Quick Report

1. In the **Sites** window or **Overview** window, select one or more Locations or Zones.
2. Select **Options > Quick Reports**, choose a report type (Alarm, Location History, or System), then select an available quick report.
3. To create a .pdf output of the report, select **Generate Report (*.pdf)**.
4. To create a report you can manipulate in a spreadsheet, select **Generate for Excel (*.tsv)**.
5. To send the report to another user, select **Generate and Email Report**:
   a. Choose the report format.
   b. Enter the email address of the recipient, and any additional viewLinc users or groups to whom you want the report sent.
   c. Optional: Modify the **Subject** and **Body** fields for the email message.
   d. Select **Send**.
6. To find out when the report is ready to download and print, open **Reports > Downloads**.

9.8.5 Viewing Report Downloads

Each time a report is generated the **Downloads** tab updates to show when the report is available to download and print.

View Downloaded Reports

1. In the **Reports** window, select the **Downloads** tab.
2. To check the report status, locate your report in the list:
   - **Generated By**: Identifies the person who initiated the report generation (username), or if it was automatically generated (System).
   - **Generated As**: Indicates whether the report owner generated the report (report includes all source data), or, if another user generated it as a quick report (report only includes data for the Locations user has permission to view).
   - **Generated**: When report content was generated, seen as the user's local time.
   - **Available For**: Indicates remaining time the generated report will be available to download and print. Manually generated and scheduled reports remain available for 24 hours.

> To save a report permanently, download and save it before available download time runs out, or edit the report properties to **Autogenerate and save** (requires Manage Reports right).

- **Timezone**: The server time zone. If a report you want to see is generated by a server in a different timezone, select your time zone to see reporting details in local time.
- **Progress**: Indicates when the report is available to download, queue status, or report generation errors.
- **Status**: Indicates whether a scheduled report was saved to a network location or sent to a recipient.

3. To download and/or print a generated report, in the **Progress** column select the report link and open your downloads folder (or follow the prompt to open or save the file).

9.8.6 Deactivating/Activating Reports

When you deactivate a report, you prevent it from being used or auto-generated for a specific period of time. When you want to use it again, simply reactivate the report. If you no longer need a report, delete the report ( ).

> You cannot delete a deactivated report.

Deactivate a Report

1. In the **Reports** window, select the report you want to delete.
2. Select **Deactivate**.

Activate a Report

1. In the **Reports** window, select **View > Include Deactivated Reports**.

> To sort all deactivated reports to display at the top of the list, select the **Active** column heading.

2. Select the report you want to reactivate, then select **Activate**.

9.8.7 Alarm Period Reporting

Default viewLinc alarm reports—Last 8 hours, Last day, Last week—can be generated by all users from the Sites or Overview windows. Additional custom alarm reports are available from these windows if they are set up as Quick Reports (see "Create Custom Reports" on the next page).

To print out only currently active alarm data, see "Printing or Exporting Current Alarm Data" on page 124.

Generate an Alarm Report for Specific Zones or Locations

1. In the **Sites** window on the **Zones and Locations** tree, select a Zone or a Location. Hold the [Ctrl] key to select multiple Zones/Locations.
2. Select **Options > Quick Reports > Alarm Reports**, then select the report type and the output format: .pdf (standard presentation format), .tsv (modifiable format with a spreadsheet program), or send the report as an email attachment (.pdf).
3. To generate and send the report to an email recipient:
   a. Enter the email address of the recipient, and any additional viewLinc users or groups to whom you want the report sent.
   b. Optional: Modify the **Subject** and **Body** fields for the email message.
   c. Select **Send**.
4. To find out when the report is ready to download and print, or when it was sent, open **Reports > Downloads**.

9.9 Create Custom Reports

Create a new Location History, Alarm or System report to include the reporting information you need.

You can also specify:

- A user or group authorized to modify the report
- The time zone to use when generating data
- The groups who can receive the report by email
- A schedule to generate the report automatically
- Availability as a quick report

You require Manage Reports right to create or modify reports.

9.9.1 Creating Location History Reports

Manage Reports

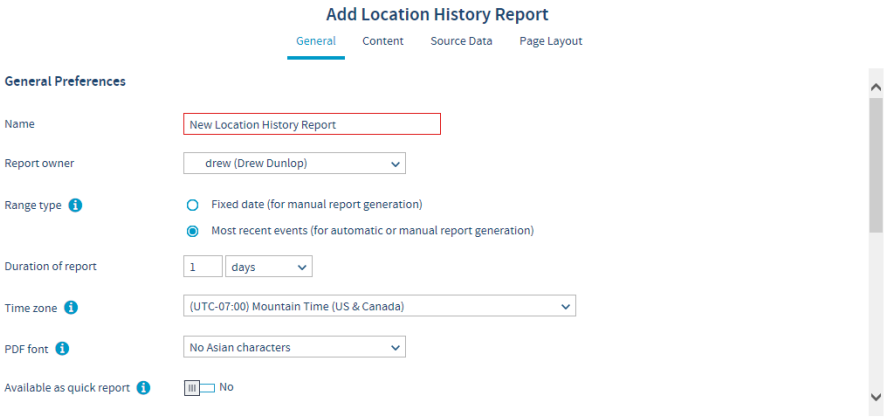
Location History reports identify specific information about condition values over a period of time.

Create a new Location History Report

1. In **Reports** select **Add > Location History Report**.

To reuse settings from an existing Location history report, select the report, then select **Add > Copy Selected Report**.

2. Complete the **General** tab.



- **Name**: Enter a unique name for the new report.
- **Report owner**: Your viewLinc user name appears automatically, as the report owner. If you have Manage Reports right, you can select a different or additional user to modify this report.
- **Range type**: Specify the period of time you want the report to include. A fixed date sets duration according to specific dates, or choose a period in hours/days/weeks/months.
- **Duration of report**: Specify the time period you want included in the report. If you want to include only the last 8 hours of data, enter **8** and then choose **hours** from the drop-down list.
- **Time zone**: Change this value if reporting time zone is not the same as the server time zone.
- **PDF font**: Choose the format for the report output. If you want to generate a report in Chinese, select **Chinese character support**.
- **Available as quick report**: Allow users to generate this report from the Sites and Overview windows. Quick reports generate data for the user's selected Location(s) or view(s).

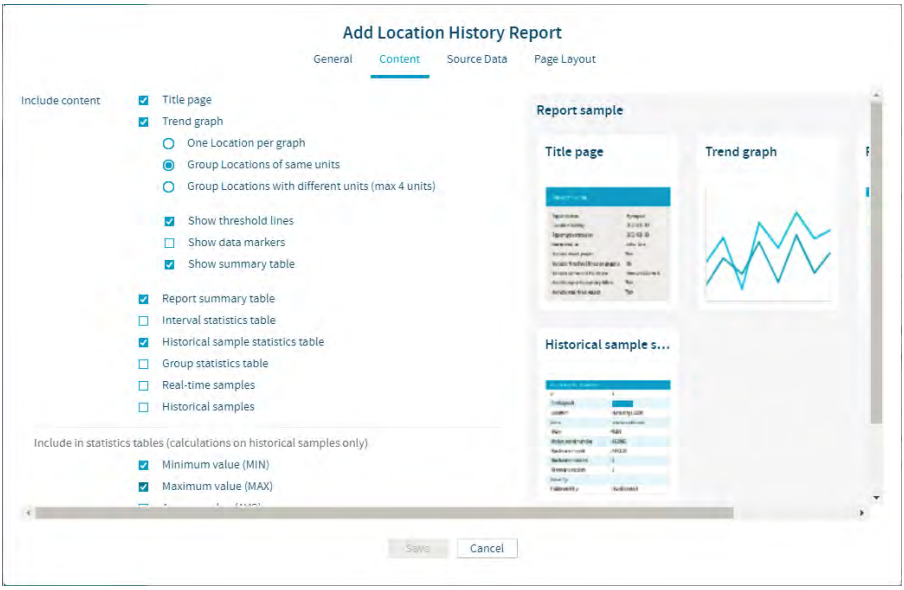
3. If you selected the range type **Most recent events**, you can choose to generate the report automatically. Complete the **Automatic Generation** section:

For large reports, we recommend that you schedule report generation at a time when few users are using the system, such as after business hours.

- **Generate and email**: Generate and then send the report directly to specific viewLinc users and groups.
- **Generate and save**: Generate and then save the report to a specific file location.
  - **Save To**: Specify an accessible network server or restricted file location where you want the report saved.
  - **Language**: Saved reports are automatically generated in the system default language unless a report language is specified.

- **Start generating**: Set the data generation start date and time.
- **Generate report every**: Enter the start date and time you want the report generated.
- **Report format**: Specify whether you want the report generated hourly, daily, weekly, or monthly.

4. On the **Content** tab, identify the data you want included in the report.

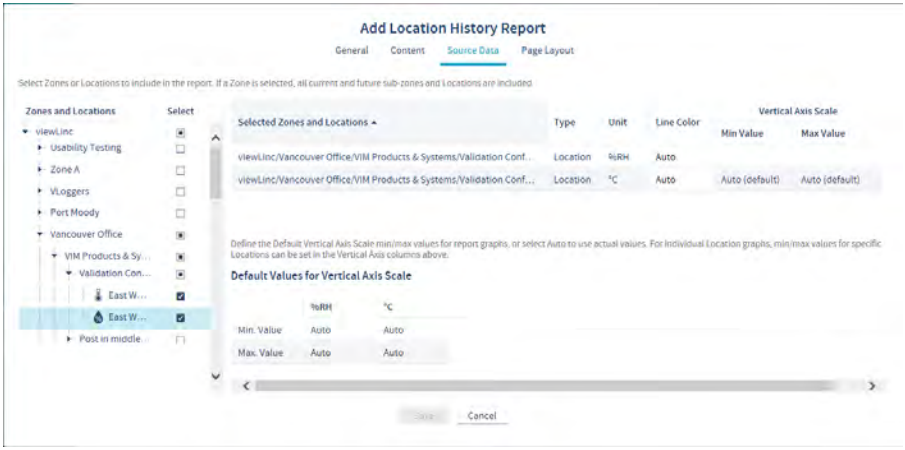


- **Title page**: Include content overview.
- **Trend graph**: Generate a graphical display of the report data. You can choose to include separate graphs for each Location, compile all Location data on a single graph (the default option, limited to a maximum of 16 Locations), or choose to group measurement units together on the same graph (up to 4 measurement types per graph). If you choose to include a statistics summary, a statistics summary table is included in the report. Choose samples in the section, **Include in statistics tables**.
- **Report summary table**: This option can be deselected independent of the statistics summary table.
- **Interval statistics table**: Select a timeframe measured in days/hours, or on a calendar month. If the **General** tab setting for the **Duration of report** is set on a weekly interval and you want to daily interval statistics, specify **1 day, 0 hours**. Choose **Show graph** to include an additional graphical representation of the statistics. Choose samples in the section, **Include in statistics tables**.

Interval statistics table will only appear if the duration is less than the report duration.

- **Historical sample statistics tables** : Include statistics calculated by Location (ordered according to measurement type). Choose samples in the section, **Include in statistics tables**.
- **Group statistics table**: Generate one statistics table for all Locations with the same measurement type. For example, the maximum temperature of all the temperature recording Locations included in the report. Choose samples in the section, **Include in statistics tables**.
- **Real-time samples** and/or **Historical samples**. If you choose to include historical samples, select a set data period (every 5, 15, 30, or 60 minutes) and indicate whether the last sample reflects the closest reading to the period interval timestamp. This option is useful when reporting Locations have different sample rates.
- **Include in statistics tables**: Select the historical sample data to include in all statistics tables.

5. On the **Source Data** tab, use the Zones and Locations navigation tree to select the Zones and/or Locations you want to include in the report



- **Zones and Locations**: To select all Locations in a Zone, select the checkbox corresponding to the Zone name. When a Zone is selected, all current and future Locations are automatically included in the report. To select or deselect a specific Location in a Zone, expand the Zone.
- **Line Color**: Specify a color to identify Locations (color not available for Zones). Auto chooses the next available color (see page "Q: How does viewLinc select colors for reports?" on page 185 for the color spectrum sequence).

- **Vertical Axis Scale Min/Max Values**: If trend graphs will be generated (Content tab, Trend graph - One Location per graph) each Location graph can have specific min/max values, or accept the default values.
- **Default Values for Vertical Axis Scale**: Enter the minimum and maximum values to define the upper and lower limits for the graph measurement range. Auto

6. Modify report output display options on the **Page Layout** tab:
   - **Paper**: Choose the report page size and orientation.
   - **Page Header/Page Footer**: For header or footer options, choose to display on all pages, on the first page only, on the last page only, or on the first and last page.
   - To define the content of your header or footer, enter text in the **Left header**, **Center header** or **Right header** fields. You can also use the Footer field to include a Signature box or Comments boxes.
   - To include an image instead of text in **Left header**, select **Image**, then choose a .jpg image file from the drop-down (for previously used images) or upload a new .jpg image file using **Upload new** button.

   Only .jpg files can be used in reports. The image file must not exceed 154 x 48 pixels.

7. Save the new report.

To generate your new Location history report, see "Generating Reports" on page 142.

9.9.2 Creating Alarm Reports

Manage Reports

Alarm reports identify alarm event patterns over a period of time.

Create an Alarm Report

1. In **Reports** select **Add > Alarm Report**.

   To reuse settings from an existing alarm report, select the report, then select **Add > Copy Selected Report**.

2. Complete the **General** tab:
   - **Name**: Enter a unique name for the new report.
   - **Report owner**: Your viewLinc user name appears automatically, as the report owner. If you have Manage Reports right, you can select a different or additional user to modify this report.
   - **Range type**: Specify the period of time you want the report to include. A fixed date sets duration according to specific dates, or choose a period in hours/days/weeks/months.
   - **Duration of report**: Specify the time period you want included in the report. If you want to include only the last 8 hours of data, enter **8** and then choose **hours** from the drop-down list.

- **Time zone**: Change this value if reporting time zone is not the same as the server time zone.
- **PDF font**: Choose the format for the report output. If you want to generate a report in Chinese, select **Chinese character support**.
- **Available as quick report**: Allow users to generate this report from the Sites and Overview windows. Quick reports generate data for the user's selected Location(s) or view(s).

3. If you selected the range type, **Most recent events**, you can choose to generate the report automatically. Complete the **Automatic Generation** section:

For large report data sets, we recommend that you schedule report generation at a time when few users are using the system, such as after business hours.

- **Generate and email**: Generate and then send the report directly to specific viewLinc users and groups.
- **Generate and save**: Generate and then save the report to a specific file location.
  - **Save To**: Specify an accessible network server or restricted file location where you want the report saved.
  - **Language**: Saved reports are automatically generated in the system default language unless a report language is specified.
- **Start generating**: Set the data generation start date and time.
- **Generate report every**: Enter the start date and time you want the report generated.
- **Report format**: Specify whether you want the report generated hourly, daily, weekly, or monthly.

4. On the **Content** tab, identify the data you want included in the report:
   - **Include content**: Include a summary of all active, activated, deactivated and acknowledged alarms by Location.
   - **Report detail level**: Choose to group all alarm details in shortened form or expand the length of the report to include all alarm details. Depending on the number of alarms, this can increase the size and time required to generate the report significantly.
   - **Alarm content**: Choose to report on specific types of device alarms.
5. On the **Source Data** tab, use the navigation tree to select the Zones and/or Locations you want to include in the report:
   - **Zones and Locations**: To select all Locations in a Zone, select the checkbox corresponding to the Zone name. When a Zone is selected, all current and future Locations are automatically included in the report. To select or deselect a specific Location in a Zone, expand the Zone.
6. Modify report output display options on the **Page Layout** tab:
   - **Paper**: Choose the report page size and orientation.
   - **Page Header/Page Footer**: For header or footer options, choose to display on all pages, on the first page only, on the last page only, or on the first and last page.
   - To define the content of your header or footer, enter text in the **Left header**, **Center header** or **Right header** fields. You can also use the Footer field to include a Signature box or Comments boxes.

- To include an image instead of text in **Left header**, select **Image**, then choose a .jpg image file from the drop-down (for previously used images) or upload a new .jpg image file using **Upload new** button.

Only .jpg files can be used in reports. The image file must not exceed 154 x 48 pixels.

7. Save the new report.

To generate your new Alarm report, see "Generating Reports" on page 142.

9.9.3 Creating System Reports

Manage Reports

System reports provide an overall snapshot of select system information.

Create a System Report

1. In the **Reports** window, select **Add > System Report**.

To reuse settings from another system report, select the report on the grid, then select **Add > Copy of Selected Report**.

2. Complete the **General** tab:
   - **Name**: Enter a unique name for the new report.
   - **Report owner**: Your viewLinc user name appears automatically, as the report owner. If you have Manage Reports right, you can select a different or additional user to modify this report.
   - **Duration of report**: Specify the time period you want included in the report. If you want to include only the last 8 hours of data, enter **8** and then choose **hours** from the drop-down list.
   - **Time zone**: Change this value if reporting time zone is not the same as the server time zone.
   - **PDF font**: Choose the format for the report output. If you want to generate a report in Chinese, select **Chinese character support**.
   - **Available as quick report**: Allow users to generate this report from the Sites and Overview windows. Quick reports generate data for the user's selected Location(s) or view(s).
3. (Optional) Complete the **Automatic Generation** section:

For large report data sets, we recommend that you schedule report generation at a time when few users are using the system, such as after business hours.

- **Generate and email**: Generate and then send the report directly to specific viewLinc users and groups.
- **Generate and save**: Generate and then save the report to a specific file location.
  - **Save To**: Specify an accessible network server or restricted file location where you want the report saved.

- **Language**: Saved reports are automatically generated in the system default language unless a report language is specified.
- **Start generating**: Set the data generation start date and time.
- **Generate report every**: Enter the start date and time you want the report generated.

4. On the **Content** tab, identify the data you want included in the report:
   - **Server**: Include viewLinc Enterprise Server configuration details.
   - **System preferences**: Include the currently selected viewLinc system preferences.
   - **Alarm templates**: Include details for selected templates (active and deactivated).
   - **Users and groups**: Include all users and/or groups, and their assigned permissions to Locations.

     The report shows the highest available permission for each Location, listed alphabetically by user or group. To learn more about permissions, see "Applying Group Permission to Zones" on page 103.

   - **Sites**: Include Location details about current threshold and device alarm templates, and permission levels granted to users/groups for each Location (active and deactivated).

     The report lists highest available permission for the user or group, listed alphabetically by Location. To learn more about permissions, see "Applying Group Permission to Zones" on page 103.

   - **Devices**: Include a list of all linked system hosts, data loggers and transmitters (active and deactivated).
5. Save the new report.

To generate your new System report, see "Generating Reports" on page 142.

9.10 Viewing Data with viewLinc Mobile

Several viewLinc functions are accessible via mobile device. To log in, open a device browser and enter the IP address/mobile (**##.###.##.##/mobile**). The initial screen that appears after you log in is the **Sites** window navigation tree. Tap the name of a Zone to reveal the Locations below it. Select a Location and then tap the **Options** button to view available options:

- **Refresh**: Update display to show most recently collected data.
- **Pop-up Trend**: Display selected Location data in trend graph.
- **Pause/Resume Threshold Alarming**: Pauses threshold alarming temporarily on all Locations in the selected Zone for 1 hour.

Ways to Display Mobile Data

Sites View: Display trends, change trend graph settings, pause threshold alarming. When a Zone is selected, the view expands to display sub-zones and Locations.

- To go up a folder, tap the previous screen button, viewLinc (do not use your device Back button, it closes the active tab and ends the browsing session).

Table View: Displays detailed Location information for whichever Location was selected from the Sites view. Pause threshold, host or device alarming.

- To view Location information, select the Location, then double-tap to view details. Click the ✖ to return to view previous screen.
- To go up a folder, select the **Sites View** icon, (do not use your device Back button, it closes the active tab and ends the browsing session).

Alarm View: Displays alarm information for whichever Location was selected from the Locations pane view (or all Location alarms, if none selected).

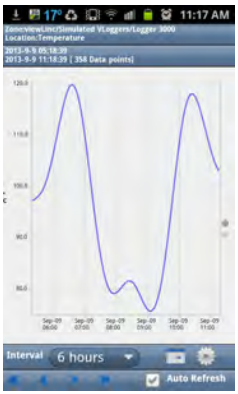
- To view Alarm information, select the Location, then double-tap to view details. Click the ✖ to return to view previous screen.
- To go up a folder, select the **Sites View** icon, (do not use your device Back button, it closes the active tab and ends the browsing session).

Only Locations that have active alarms display on the mobile device. For example, if you are at the system level when you press the alarm grid, it displays all active alarms in the system, if any.

Open a Pop-up Trend

Before you can view pop-up trends on a mobile device, ensure the device browser is not set to block pop-ups. Refer to your device-specific user guide for more information.

1. Tap the **Sites** button, then navigate to a specific Location.
2. Tap **Options > Pop-up Trend**. The pop-up trend window appears in a new browser tab.



- **Interval**: Trends display up to 1 month of data logged up to the current date.
  - Tap the calendar button to set the end date.
  - Tap the settings icon to include real-time samples or threshold lines on the graph.
- **Auto Refresh**: Select this option to update the trend with real-time data readings. Only available for trends set to a maximum duration of 7 days.
- Use the arrows to scroll the trend forward and back (see"Trend Navigation" on page 138).

9.10.1 Pause or Resume Alarming with viewLinc Mobile

You can pause or resume alarms on a mobile device for the Locations you have permission to view on your desktop display. To learn more about pausing alarms, see "Pause Alarms" on page 129.

Pause or resume alarming

1. Open **Table** view ( ).
2. Select the Location you want to pause or resume alarming, then select **Options**.
3. Tap **Pause X Alarming** or **Resume X Alarming** (where X is the type of alarm you'd like to control, Threshold, Host or Device.)

- Once alarming is paused, it remains paused for one (1) hour.
- To resume alarming within the hour, repeat these steps and select **Resume X Alarming**.

9.10.2 Acknowledging an Alarm with viewLinc Mobile

If you are authorized to acknowledge alarms for the Locations you can view, you are authorized to acknowledge those alarms remotely. To learn more about acknowledging alarms, see "Ways to Acknowledge Alarms" on page 125.

Acknowledge an Alarm

1. Tap the **Alarms** button.
2. Select the alarm you want to acknowledge.
3. Tap **Options > Acknowledge**. At the prompt, enter the action taken, select a predefined comment (if required) and add extra comments (optional).
4. Fill in the required information and then tap **Acknowledge**.

9.10.3 Viewing Data on a Remote Display

Several viewLinc functions are available on a remote display.

If the display terminal does not have touch-screen capability, a connected keyboard is required.

Open viewLinc on a Remote Display Terminal

1. Open the Internet browser on the display terminal.
2. Enter your viewLinc IP address followed by **/display** (for example, **##.###.##.##/display**).
3. Select the language you want to display. When changing to a language other than English, the page automatically refreshes to display the new language.
4. Log in as the remote display user. The content displayed is defined by the default view for the signed in user. These settings are remembered until the user logs out.
5. Select display options:
   - Open the Dashboard tab to display a graphic of monitored Locations in the view (dashboards for views are set up in Views Manager).
   - Open the Trend tab and select a view. The graph automatically loads data for all Locations in the view.
   - To view multiple Location trends on a single monitor, open multiple browser windows. In each browser window, log in to viewLinc as a different user, each with a different default view.

If a browser reboots unexpectedly, viewLinc automatically relaunches the browser and logs in as the last user. The browser opens the user's default view with the last open tab displayed.

9.10.4 Changing a Display Terminal View

To change the view displayed on a display terminal, you can either select a different view assigned to the user currently logged in, or log in as a new user with different views available.

Change the Display View

1. On the viewLinc remote display, expand the **Views** pane.
2. In the **Views** tree, select another available view. The display updates automatically.

Log In as a New User

1. On the viewLinc remote display, select **User > Logout**, then select **Yes**.
2. At the viewLinc log in prompt, enter the new user name and password.
3. Expand the **Views** pane to select an available view.

10. Administrator Tasks

After the viewLinc system is set up and system monitoring is active, ongoing system maintenance tasks can be performed by members of the Administrators group, or users assigned the required rights.

10.1 Groups and Users

As your team grows or responsibilities change, you can quickly adjust user profile and group properties.

For information on adding groups and users, see "Groups and Users" on page 57.

10.1.1 Editing User or Group Details

Manage System

Edit a User or Group

1. In the **Users and Groups** window, select the user or group you want to edit, then select **Edit** (or right-click and select **Edit**).
2. Edit settings as needed (for information on user or group properties see "Groups and Users" on page 57).
   - Only members of the Administrator's group can modify a user's group assignments.
   - Only viewLinc passwords can be modified.
3. Select **Save**.

10.1.2 Deactivating/Reactivating Users

Manage System

Users cannot be deleted from the viewLinc database; however, you can use the deactivate function to ensure users who have moved to other positions or left the company are no longer included in group alarm notifications and/or group report distribution (this is easier than removing groups from individual alarm templates or reports).

Deactivate a User

1. In the **Users and Groups** window select the **Users** tab.
2. Select the user you want to deactivate. If your user list is long, use the Search tool to locate a user, or click the top column header to sort names in alphabetical order.

3. Select ✖ **Deactivate** .
4. To confirm, select **Deactivate**.

The user row is automatically hidden.

To show all deactivated users, select **View > Include Deactivated Users**.

Reactivate a User

1. In the **Users and Groups** window select the **Users** tab.
2. Select **View > Include Deactivated Users** .
3. Select a deactivated user row (greyed out text row).
4. Select ✓ **Activate** .

The user row reappears in the table.

10.1.3 Deactivating/Reactivating Groups

Manage System

Groups cannot be deleted from the viewLinc database; however, you can use the deactivate function to ensure that the group is no longer used for alarm notifications or group report distribution (this is easier than removing the group from multiple alarm notification templates and/or reports).

All users in a group must be deactivated before a group can be deactivated.

Deactivate a Group

1. In the **Users and Groups** window select the **Groups** tab.
2. Select the group you wish to deactivate.
3. Select ✖ **Deactivate** .
4. To confirm, select **Deactivate**.

The group row is automatically hidden.

To show all deactivated groups, select **View > Include Deactivated Groups**.

Reactivate a Group

1. In the **Users and Groups** window select the **Groups** tab.
2. Select **View > Include Deactivated Groups**.
3. Select a deactivated group row (greyed out text row).
4. Select ✓ **Activate** .

The group row reappears in the table.

10.2 Zones and Locations

Manage Sites

Modification to Zones and Locations is performed in the Sites Manager window. Common administrator activities include changing a Zone or Location name, unlinking and moving a Location to a different zone, applying different permissions, creating schedules, and/or applying different threshold templates.

Full Control permission is required to make changes to Zones or Locations.

Edit Zone Display Properties

1. In **Sites Manager** on the **Zones and Locations** tree, select the Zone you want to edit.
2. Right-click to select **Edit Properties** or select **Manage > Edit Properties**.
3. In the **Edit Zone** window, modify the information viewLinc uses to display the Zone: name, dashboard folder icon, description.
4. Save the changes.

Edit Location Display Properties

1. In **Sites Manager** on the **Zones and Locations** tree, select the Location you want to edit.
2. Right-click to select **Edit Properties** or select **Manage > Edit Properties**.
3. In the **Edit Location** window, modify the information viewLinc uses to display the Location: name, description, units and decimal places. These settings control the way the Location appears throughout viewLinc . If you enter a smaller number of decimal places than your device reads, viewLinc automatically rounds the data it receives from the device to the nearest decimal point.
4. Save the changes.

10.2.1 Viewing Location Properties

In the **Sites Manager** window use the **Location Properties** tab for at-a-glance review of important Location details. Access to the Sites Manager window requires Manage Sites right.

View Trend: View a Location's historical data as a trend in a new browser window.

Find in Tree: Highlight the selected Location in the Zones and Locations navigation tree.

Show Linked Channel History: Find out how long a specific device channel has been linked to a selected Location, when the link first began, and for how long it has been linked.

Table 16 Location Properties Columns

Column	Contains
Type	The Location Type icon. This column cannot be moved. For icon descriptions, see "Icons" on page 116.
Zone	Full path of the parent Zone.
Location	Location name as displayed in the navigation tree.
Location ID	Number assigned by viewLinc to a new Location. It can never be changed. Used to avoid confusion if more than one Location is given the same name.
Description	User-entered device description.
Device Description	Name of a device, as defined by a user.
Device Serial Number	Device serial number automatically stored in viewLinc .
Channel Description	Description provided by a user.
Device ID	A number assigned to a new device, generated by viewLinc , and can never be changed. Used to avoid confusion if more than one device is given the same name.
Channel ID	A number assigned to a new channel, created by viewLinc , and can never be changed. Used to avoid confusion if more than one channel is given the same name.
Channel Index	Channel number assigned to the linked Location.
Location Units	Unit display format set in viewLinc , often modified for reporting purposes (for example, American sites may want to see readings in standard measurement units, Fahrenheit, while Canadian operations may prefer them in metric, Celsius).
Preferred Units	Unit display option (such as C or F), for the specific Location (units can be set differently for different Locations).
Device Units	Data logger or transmitter units, such as C, DEGC, TDC, set by Vaisala. These can be changed in viewLinc to display in a more meaningful way (Location or Preferred Units).
Measurement Type	The value being measured (temperature, humidity, boolean, pressure).
Decimal Places	System-defined preference.

Column	Contains
Device Address	System folder path to this Location.
Link Start	Date the Location started recording data (Unlimited indicates this Location has remained linked to the current channel since it started monitoring data).
Link End	Date the Location stopped recording data (Unlimited indicates the Location is still linked to the current channel, and continuously recording data).
Permission	The permission a user has been granted for this Location.
Threshold Alarm Schedule	The name of the threshold alarm schedule set for this Location, if one has been assigned.

10.2.2 Renaming a Location or Zone

Manage Sites

Renaming Zones edits the Zone name only; it does not change the Locations assigned within it.

1. In **Sites Manager** on the **Zones and Locations** navigation tree, select the Location or Zone you want to rename.
2. On the **Manage** menu, select **Edit Properties**, or right-click and select **Edit Properties**.
3. Enter a new unique name, then select **Update**.
4. Select **Save** or **Undo** to cancel the change.

10.2.3 Unlinking/Relinking Locations and Channels

Manage Sites

As your company's monitoring needs change, perhaps due to a change in monitored spaces or a facility move, you may want to link a device channel to a different viewLinc Location. This is an easy change with viewLinc 's unlink/relink function.

Full Control permission is required for all Zones where Locations are being linked or unlinked.

Channels can be unlinked individually, or you can unlink all channels within a Zone at one time. This option saves you time when you want to deactivate a Zone that is no longer being monitored.
For some organizations, the list of Locations and Zones is lengthy, and the first step is to identify the Location to which a channel is linked (see "Finding Linked Channels/Linked Locations" on page 50).

Unlink a Location from a Channel

When a device channel is unlinked from a viewLinc Location, data history is retained in the Location History report.

1. In **Sites Manager** navigate the **Zones and Locations** tree to the linked Location.
2. Select **Manage > Unlink Channel** (or right-click and select **Unlink Channel**).
3. Select **Unlink**. The device channel is now available to link to another Location.
4. Select **Save**.

Unlink all Locations in a Zone

These steps are required if you want to delete a Zone (see "Removal of Zones and Locations" on page 167).

1. In **Sites Manager**, navigate the **Zones and Locations** tree to find the Zone with the Locations you want to unlink.
2. Select **Manage > Unlink Channels**(or right-click and select **Unlink Channels**).
3. Select **Unlink** to confirm the change.
4. Select **Save**.

Link a Previously Linked Channel to a New Location

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. In the **Zones and Locations** tree, navigate to a new, unlinked Location.
3. In the **Hosts and Devices** tree select an unlinked channel (the channel may have been linked before, but is now in the unlinked state, displaying *italicized* text).
4. Select **Configure > Link Channel**.

5. In the **Link Channel to Location** window, choose when you want this new Location to start monitoring data:
   - **Start now**: Data is recorded at this Location starting from the next available sample recorded on the channel.
   - **Start from earliest available link time [ ]**: New channel data starts recording to the Location based on last time the channel was linked.
   - **Start from a specified time**: Set the time to start recording data history.

6. Select **Link**.
7. Select **Save**.

Link a New Channel to an Previously Linked Location

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. In the **Zones and Locations** tree, navigate to an unlinked Location (the Location may have been linked previously to another channel, but is currently in the unlinked state, displaying *italicized* text).
3. In the **Hosts and Devices** tree select the unlinked channel.
4. Select **Configure > Link Channel**.

5. In the **Link Channel to Location** window, choose when you want this new Location to start monitoring data:
   - **Start now**: Data is recorded at this Location starting from the next channel reading.
   - **Start from the earliest available link time [ ]**: New channel data starts recording to the Location based on last time the Location was linked.
   - **Start from a specified time**: Set a specific time to start recording data history.
6. Select **Link**.
7. Select **Save**.

Link Previously Linked Channel to a Previously Linked Location

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. In the **Zones and Locations** tree, navigate to an existing, unlinked Location.
3. In the **Hosts and Devices** tree, select an existing, unlinked channel.
4. Select **Configure > Link Channel**.

5. In the **Link Channel to Location** window, choose when you want this Location to start monitoring data:
   - **Start now**: Data is recorded at this Location starting from the next available sample time.
   - **Start from the earliest available link time [ ]**: This option automatically selects the most recently linked time, the Location or the channel linkage. This prevents data duplication and invalid alarms.
   - **Start from a specified time**: Set a specific time to start recording data history.
6. Select **Link**.
7. Select **Save**.

Location data and alarm history is preserved when unlinking/relinking devices.

10.2.4 Moving Locations

Manage Sites

viewLinc recognizes devices regardless of their assigned Zone, which allows you to move devices and channels from one Zone to another, without losing data history.

For example, if you need to move a monitored refrigeration unit to another physical location, in viewLinc, simply move the device Location data point to a different refrigeration Zone. Full Control permission for the Location is required.

Move a Location to another Zone

1. In **Sites Manager** make sure you have a destination Zone created for the Location.
2. On the **Zones and Locations** tree, select the Location you want to move.
3. To move the Location with your mouse, in the **Zones and Locations** tree select a Location and drag it to the new Zone.

If the new Location has the same name as another Location in the Zone, at the prompt modify the Location name.

4. To move the Location manually, in the **Zones and Locations** tree select a Location:
   a. Select **Manage > Cut** (or right-click and select **Cut**).
   b. Select the Zone where the Location will be moved and then select **Manage > Paste**.
5. Select **Save**, or **Undo** to cancel the move.

10.3 Removal of Zones and Locations

As your company grows, or monitoring needs change, you may find that you no longer need a Zone or Location displayed on your desktop. To ensure complete audit trail records, Locations can be deleted only if they have never been linked to a channel to collect data. Any Locations that cannot be deleted can still be prevented from appearing on the viewLinc desktop, with the deactivate function.

- **Deactivate**: The Location is hidden from view (Zones and Locations tree) and can be reactivated at a later time.
- **Delete**: The Zone or Location can no longer be used. This option is a good way to remove the visual clutter associated with deactivated Zones or Locations.

You cannot delete the top-level Zone or a Zone with Locations that have been used to collect data. Zone deletion is only available when all child Locations are deleted or moved to another Zone.

10.3.1 Deactivating Locations

Manage Sites

When you no longer want to record data or monitor a Location, deactivate the Location so it is no longer visible on the Zones and Locations tree. All previously recorded history is saved.

Deactivate a Location

1. In **Sites Manager** on the **Zones and Locations** tree, select a Location to deactivate.
2. Select **Manage > Deactivate** (or right-click and select **Deactivate**).
3. At the prompt, select **Deactivate**. The Location is hidden from view.
4. Select **Save**, or **Undo** to cancel the change.

To show or hide all deactivated Zones or Locations, select **More > Include Deactivated Locations**.

10.3.2 Reactivating Locations

Manage Sites

Only deactivated Locations which were never linked to a device channel may be reactivated.

Reactivate a Deactivated Location

1. In **Sites Manager** on the **Zones and Locations** tree, select **More > Include Deactivated Locations**.
2. Select the deactivated Location (appears as ~~red strikeout~~ text), then select **Manage > Activate** (or right-click to select **Activate**).
3. At the prompt, confirm activation.
4. Select **Save**.

10.3.3 Hiding/Showing Deactivated Locations

Manage Sites

When you deactivate a Location, it is hidden from view in the Zones and Locations tree.

To make them visible again open **Sites Manager**, then select or deselect **More > Include Deactivated Locations**.

10.3.4 Deleting Zones or Locations

Manage Sites

Unlinked Locations which have never been linked to a device channel can be deleted. Once deleted, they are no longer available in the Zones and Locations tree.

If a Location has been linked to a device channel, the Location can only be deactivated. Deactivated Locations are hidden from view and can be reactivated (see "Deactivating Locations" on the previous page).

Zones can only be deleted if all child Locations are deleted.

Delete a Location

1. In **Sites Manager** select an unlinked Location.
2. Select **Manage > Delete** (or right-click to select **Delete**). If the option to delete is not available, the selected Location was previously linked to a channel and cannot be deleted, only deactivated.
3. Select **Save**.

Delete a Zone

1. In **Sites Manager** select an empty Zone to delete. To verify that the Zone does not contain any hidden deactivated Locations, select **More > Include Deactivated Locations**.

> If the Zone you want to delete contains any deactivated Locations, you can drag them to another unused Zone.

2. Select **Manage > Delete** (or right-click and select **Delete**).
3. Select **Save**.

10.4 Disable/Enable Alarming

Manage Devices

To prevent unnecessary alarming during system maintenance periods, which may take more than 24 hours, disable device alarms.

- Disable/enable device alarming
- Disable/enable threshold alarm settings
- Disable/enable threshold alarm template level (affects all Locations using the template)

To disable alarming on devices for a temporary period of up to 24 hours, see "Pause Alarms" on page 129.

To stop device alarming and data logging until further notice or even permanently, you must deactivate a device or host, see "Deactivating/Reactivating Hosts or Devices" on page 172.

10.4.1 Disabling/Enabling Threshold Alarm Settings

Manage Alarm Templates

Disabling threshold alarm settings is useful when you want to temporarily prevent threshold alarming on one or several Locations . You can also disable individual levels in a threshold alarm template (see "Disabling/Enabling Threshold Alarm Template Levels" on the next page).

Disabled threshold alarm settings remain visible on your viewLinc screen and can be enabled at any time.

When you no longer want threshold settings used, use the deactivate option (threshold alarm settings cannot be deleted). Deactivated threshold alarms are hidden from view, but can be reactivated at any time. See "Deactivating/Reactivating Threshold Alarms" on page 70.

Enable/Disable Threshold Alarm Settings

1. In **Sites Manager** navigate to a Location in the **Zones and Locations** tree.
2. On the **Threshold Alarm Settings** tab, select one or more rows ([Ctrl]+click to select multiple), then select **Edit threshold alarm settings**(or use the right-click menu).
3. On the **Edit Threshold Alarm Settings** window, enable or disable the **Status** setting.
4. Select **Save**.

10.4.2 Disabling/Enabling Threshold Alarm Template Levels

Manage Alarm Templates

When creating a threshold alarm template, you may not want to enable all levels. You may want to apply the threshold alarm template to several Locations, then enable specific levels at different times.

Enabling or disabling a threshold alarm template level affects all Locations using the template.

Enable/Disable a Threshold Alarm Level

1. In **Alarm Templates** select the **Threshold Alarms** tab.
2. Select the threshold alarm template you want to modify, then select **Edit**.
3. On the thresholds grid in the **Enabled** column, enable or disable threshold levels. At least one threshold level must remain enabled.
4. Select **Save**.

10.4.3 Disabling/Enabling Device Alarming

Manage Devices

To prevent unnecessary alarming during system maintenance periods, which may take more than 24 hours, disable device alarms. You can also disable all alarming on a device for a temporary period, up to 24 hours (see "Pause Alarms" on page 129).

Alternatively, to stop all device alarming and data logging until further notice or even permanently, you can deactivate a device or host (see "Deactivating/Reactivating Hosts or Devices" on page 172).

Enable/Disable a Device Alarm Assigned to a Location

1. In **Sites Manager** select a Location in the **Zones and Locations** tree.
2. On the **Device Alarm Settings** tab select the device alarm type you want to enable or disable.
3. Select **Edit device alarm settings**.
4. In the **Edit Device Alarm Settings** window set the **Status** option to **Enabled** or **Disabled**.
5. Select **Save**.

Enable/Disable Multiple Device Alarms

1. In **Sites Manager** select one or more Zones or Locations in the **Zones and Locations** tree ([Ctrl]+click).
2. On the **Device Alarm Settings** tab, select the alarm types you want to enable or disable.
3. Select **Edit device alarm settings**.
4. In the **Edit Device Alarm Settings** window select the status option: **Enabled** or **Disabled**, or, if multiple alarm types are selected, leave the default option selected, **(Mixed - leave unchanged)**.
5. Select **Save**.

10.4.4 Disabling/Enabling Host Alarming

Manage Devices

Disable host alarms to prevent continuous alarming during maintenance periods.

Enable/Disable Host Alarms

1. In **Sites Manager** on the **Hosts and Devices** tree, select a host.
2. Select **Configure > Host Communication/Host Configuration Alarm Settings**.
3. Set the **Status** option to **Enabled** or **Disabled**.
4. Select **Save**.

10.5 Device Maintenance

Users who are part of the default Administrators group, or are part of a group assigned Manage Devices right, use the Sites Manager window to manage and maintain hosts and devices.
To complete host and device configuration tasks, see "Configure Hosts and Devices" on page 34.

10.6 Device Removal

Manage Devices

Before you remove a device from your network, or transfer it to a new monitoring area on the same network, the device must be deactivated. A deactivated device stops logging data and disables all device and threshold alarming.
You may want to remove a device when:

- a device requires maintenance (such as recalibration)
- a device is no longer required

To deactivate a host or a device, see "Deactivating/Reactivating Hosts or Devices" on the next page.
To remove an RFL data logger from an access point, see "Releasing RFL Data Loggers" on the next page.

When a device is swapped it is automatically deactivated. See "Swap Devices" on page 173.

10.6.1 Deactivating/Reactivating Hosts or Devices

Manage Devices

You can deactivate a single device or all devices connected to a host. This action will stop all alarming and all data collection until you reactivate the device or host.

Deactivate a Host or a Device

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select the host or device you want to deactivate.
3. Select **Configure > Deactivate** (or right-click and select **Deactivate**).
4. A message appears, asking that you confirm deactivation of the host or device. Select **Deactivate**.

The host/device is no longer visible on the Hosts and Devices tree, but the network connection is still intact, allowing you to reactivate the host/device at a later time.

Reactivate a Host or a Device

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select **More > Include Deactivated Devices**.
3. Select the deactivated host/device (indicated by a ~~red strikeout~~), then select **Configure > Activate**(or right-click and select **Activate**).

Hide or Show Deactivated Hosts or Devices

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree select **More**, then check or uncheck the option, **Include Deactivated Devices**.

10.6.2 Releasing RFL Data Loggers

Manage Devices

Before moving or removing RFL data loggers on your network, they must be released from their access point to prevent unnecessary alarming.

Refer to the device user guides for more information about managing data loggers and access points in your facility.

Release an RFL Data Logger

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. Select one or more RFL data loggers in the **Hosts and Devices** tree.
3. Select **Configure > Release Device from Access Point**.

After releasing an RFL data logger, it can be accepted later by the same or by another access point host.

4. At the prompt, select **Release**.

10.7 Swap Devices

The swap device function allows you to exchange a device that is currently linked to a Location, while retaining the threshold and device alarm settings which are currently applied to the Location.
A swap may be required for maintenance purposes, such as calibration of the device or probe, an update of the data logger firmware, or to change to a wireless device.
When a device is swapped (see "Swapping Devices" below), the change is noted on the Location History report (the report shows the device serial number for a reporting period). If, during the reporting period, the device was swapped, this event is listed in the report summary.

10.7.1 Swapping Devices

Manage Sites

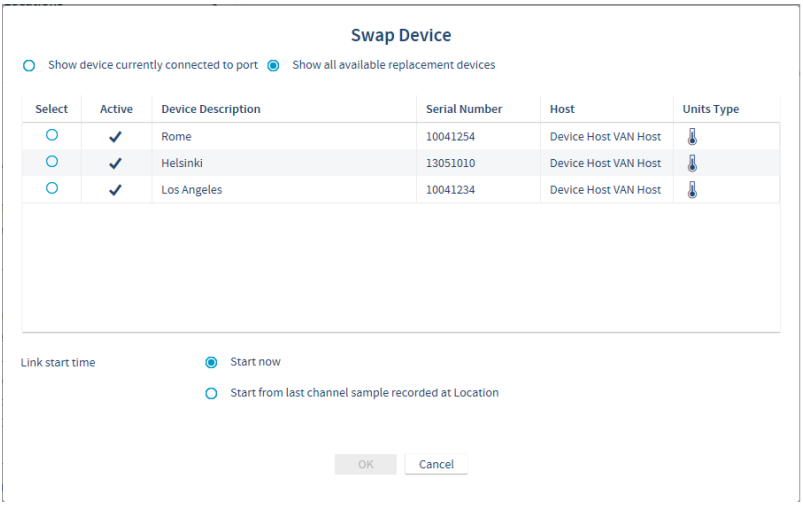
Any device linked to a Location can be swapped without interruption to threshold monitoring or causing a device alarm.

Only a device with the same settings may be swapped (for example, a device with 3 channels cannot be swapped for a device with 2 channels, and the channels must record the same type of data).

Swap a Device

1. Make sure the replacement device is:
   - connected to your network
   - on the same host as the device to be swapped
   - has the same sample rate
   - has the same channel indexes and measurement types
2. In **Sites Manager** select the **Hosts and Devices** tab.
3. On the **Hosts and Devices** tree, select the device to be swapped.
4. Select **Configure > Swap This Device With**.

Only compatible and available replacement devices are displayed.



5. In the **Swap Device** window, select the replacement device.
   - **Show device currently connected to port**: If you are swapping a DL logger and the new device is already connected, enable this option to help locate a specific device.
   - **Link start time**: Select **Start now** to associate all channel data starting from this point forward with the linked Location.
   - **Start from last channel sample recorded at Location**: This option automatically starts from the most recently linked time. This option prevents data duplication and invalid alarms.

To ensure gap-free data, if the data logger was offline while still connected to viewLinc , viewLinc will not try to restore the data history during the offline period.

6. Select **OK**.

10.8 Device Calibration

Calibration ensures that data recorded by the measurement equipment (data loggers, transmitters, probes) is reliable and accurate.

For example, most people are used to adjusting their watches to the correct time. Working standards (clocks) are visible and almost everywhere, and making a comparison–calibration–is easy. If the time on the watch differs from the trusted reference, make an adjustment. The measured data (the time) shown on the trusted reference (the clock) can be can be relied upon as a reference point.

Use viewLinc to update your device, probe and channel calibration values. To make sure your devices are calibrated on schedule, set up viewLinc calibration reminders for your devices and their probes.

Refer to the *HMP110 Series User's Guide* for information about calibrating HMP110 Humidity/Temperature probes.

10.8.1 Editing Channel Calibration Properties

Manage Devices

Channel calibration settings are the reference values used for testing measurement accuracy on Vaisala data loggers.

Edit Channel Calibration Properties

Ensure that the initial calibration values have been downloaded from the device to viewLinc (automatically discovered when device detected by viewLinc).

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. In the **Hosts and Devices** tree, select a data logger channel to edit.
3. Select **Configure > Edit Properties**.
4. In the **Edit Channel Properties** window, edit the properties, **Calibration scale** and **Calibration offset** using information provided by Vaisala or collected from on-site calibration testing.
5. If you are changing calibration settings on an HMT140 device, you are prompted to reset the device calibration settings (see "Editing Device or Probe Calibration Properties" below).
6. Select **OK**.

10.8.2 Editing Device or Probe Calibration Properties

Manage Devices

When you set calibration dates for devices and their probes, viewLinc automatically issues calibration reminder notifications at 3 months and 1 month before to the due date, and again on the due date. You can set the properties for calibration notifications (priority, delay, acknowledgement) in Alarm Templates (see "Device Calibration Duration" on page 91), and define the notification message content (see "Email and SMS Content" on page 85).

Calibration duration can be set for all devices in **System Preferences** by selecting the value column beside the option, **Default Calibration Duration**; however, the calibration duration set on a data logger or a probe overrides the system preference.

Edit Device or Probe Calibration Properties

Calibration information on some devices is set automatically and cannot be modified.

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. In the **Hosts and Devices** tree, select a device.
3. Select **Configure > Edit Properties**.
4. In the **Edit Device Properties** window, calibration fields are available for the device and any attached probes. Enter calibration details:
   - **Calibration date**: Enter the last calibration date, unless preset by Vaisala Calibration Services.
   - **Calibrated by**: Name of person who last calibrated the device, unless preset by Vaisala Calibration Services.
   - **Next calibration date**: Enter the date for next calibration. If no date entered, the system automatically sets the date to one year after last calibration date.
5. Select **OK**.

10.8.3 Off-site Calibration

To maintain the high accuracy measurement of the viewLinc system, Vaisala offers calibrations and complete functional testing in our own ISO 17025 accredited lab, which meets the standards of ISO/IEC 17025 & ANSI/NCSL Z540-1-1994.

Calibration services include:

- Verification of specifications against the original calibration
- Battery check and replacement if necessary
- Update firmware if necessary

10.8.4 On-site Calibration

When sending devices in for recalibration is impractical, Vaisala's on-site calibration team is ready to assist. On-site calibration includes a NIST-traceable certificate and reminders of recalibration due dates.

To reduce the costs of calibration Vaisala offers optional 3 or 5-year pre-paid plans that not only provide protection from price increases, but also offer significant savings on calibration costs. For convenience, rental devices are available.

10.9 Lock/Unlock DL Data Loggers

If your viewLinc monitoring system includes DL data loggers, viewLinc can be set to prevent other software (such as other installations of viewLinc or vLog) from being used to make changes to DL data loggers.

Lock DL data loggers to ensure other software cannot be used to:

- Modify data logger or channel description
- Enable or disable a channel
- Set sample interval
- Clear data logger
- Set channel scaling
- Change warmup time

Remote Lock

DL data loggers that are linked to vLog or Spectrum software prior to being connected to viewLinc are remote locked. You can unlink data loggers in vLog (refer to your vLog user guide for instructions), or undo the remote lock in viewLinc.

10.9.1 Locking/Unlocking DL Data Loggers

Manage Devices

Lock a DL Data Logger to viewLinc

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. Select a device or multiple devices ([Ctrl]+click).
3. Select **Configure > Lock Device**.
4. Select **Save**.

Unlock a DL Data Logger from viewLinc

DL data loggers with a pre-existing link to other software, a remote lock, can only be unlocked by a member of the Administrators Group.

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select a device or multiple devices ([Ctrl]+click).
3. Select **Configure > Unlock Device**.
4. Select **Unlock**.

10.10 Clearing Historical Samples

If your system includes DL data loggers, use the clear history function to:

- Remove collected data on a DL data logger prior to sending it out for calibration or repair.
- Remove data collected on the DL data logger during calibration (you can also choose to ignore the interim data when you relink the device channel to a Location in viewLinc).
- Set DL data logger sampling to Wrap When Full (the required device setting for continuous data collection in viewLinc).

Editing DL data logger properties (sample interval, sample warmup time, enable/disable channels, calibration settings) automatically clears data history.

- If you use older models of Vaisala DL data loggers (with gray case) which do not support timebase synchronization, clearing history automatically synchronizes the data logger clock with the viewLinc clock to correct any time drift.

Over time, the clock time in a data logger begins to differ from the clock time in viewLinc; this is called time drift. Some time drift is expected over long data monitoring periods and is corrected through synchronization. Synchronized timing ensures more accurate data collection results. See "Timebase Synchronization" on page 92.

10.10.1 Clearing Historical Samples in DL Data Loggers

Manage Devices

If your DL data loggers are already set to Wrap When Full (by a calibration team or using vLog), clearing of historical samples is not required.

Clear Historical Samples

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select one or more DL data loggers ([Ctrl]+click).
3. Select **Configure > Clear Historical Samples**.
4. At the warning prompt, select **Clear**.
5. At the confirmation prompt, select **OK**.

10.11 Correct Security Status

Only a member of the default viewLinc Administrators group can perform this task.

If a DL data logger security status indicates tampered (in **Sites Manager** on the **Hosts and Devices** tab, **Properties** table, **Security Status** column), it is advised that a member of the Administrators group investigate the issue to determine the cause. For assistance, contact Vaisala Technical Support. Once the issue is identified and/or corrected (according to your company security policy) you can complete the following steps to reset the security status.

Change to the security status does not interrupt continuous monitoring.

Clear Tampered Security Status

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select the device or multiple devices ([Ctrl]+click) you want to edit.
3. Select **Configure > Correct Security Status**.
4. At the warning prompt, select **Yes**.
5. At the completion prompt, select **OK**.

10.12 Testing Network Communications

Only a member of the default viewLinc Administrators group can perform this task.

If you are receiving communication alarms, you may want to verify the stability of network communications.

Test Host Communications

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select a host.
3. Select **Configure > Ping Host**. This may take up to a minute, depending on network traffic.
4. The **Ping Results** window indicates whether any communication failures were detected. Select OK to close the window.

10.13 Restarting viewLinc

Only a member of the default viewLinc Administrators group can perform this task.

Occasionally, you may want to take viewLinc offline, or complete a reboot of your system (this does not affect the data collection). You can choose to restart or stop viewLinc temporarily.
You can also restart a device host or an access point host to return it to factory settings.
Restarting a device host or access point does not interrupt data collection on connected devices.
A system or host restart is recorded in the Event Log.

Restart viewLinc Enterprise Server

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select the viewLinc Enterprise Server, then select **Configure > Restart viewLinc Enterprise Server**.
3. Select **Yes** to confirm restart. An event message is generated and an email is sent to the IT Network Manager (specified in System Preferences > System Alarms).

Restart viewLinc Device Host or Access Point

1. In **Sites Manager** select the **Hosts and Devices** tab.
2. On the **Hosts and Devices** tree, select a device host or access point, then select **Configure > Restart [Device Host/Access Point]**. A system-wide message alerts all logged in users that viewLinc is about to restart.

11. Frequently Asked Questions

This section contains answers to frequently asked setup questions and information for troubleshooting common problems with viewLinc, Vaisala devices, and vNet or Digi networking devices. It also contains more technical information for viewLinc administrators and your network support staff.

11.1 Installing viewLinc

Q: How does viewLinc upgrade data for use in viewLinc 5.0?

A: viewLinc automatically detects and converts your data. This is done transparently when you install viewLinc .

Upgrading from v3.6.1 to 5.0:

1. New top-level Zones are created based on the Zone structure you set up in the earlier version. In addition, a top-level Zone called 'Unassigned' is created for any unassigned Zones.
2. Locations are created for all active channels. The Location name is copied from the channel's preferred description (the assigned alias or device description, depending on the system preference). Duplicate channels assigned to multiple Zones are ignored.
3. If the earlier version of viewLinc has restricted users configured, viewLinc 5.0 permissions are applied, according to the following procedure:
   a. All users are assigned to the group **Everyone**.
   b. The group **Everyone** is assigned View permission to the top-level Zone, without inheriting View permission to the Locations in the top-level Zone.
   c. Users have their historical permission level automatically assigned to Zones.
   d. If previously granted permission to a channel, users have their historical permission level automatically assigned to the linked Location.
   e. Users are assigned to groups according to their historical permissions.
   f. Users with Full Control permission are automatically added to the default Administrators group.
4. Thresholds configured on active channels are applied to linked Locations.
5. Reports are upgraded to retrieve data from the new Locations/Zones.
6. POS displays are upgraded to retrieve data from the new Locations.

For more about upgrade changes, see "What's New for Upgrade Users" on page 5.

Q: How do I configure a firewall for viewLinc?

A: viewLinc will have exceptions added in the Domain and Private networks. Exceptions will not be added to Public networks. If this is required, they must be added manually. Please contact Vaisala Technical Support if you require assistance.

Q: Why am I receiving a certificate error? Will it go away?

A: viewLinc uses a certificate and security key to establish a secure connection between network PCs and the viewLinc Enterprise Server. A certificate is used to encrypt data and authenticate the viewLinc Web Server. If your system uses a self-signed security certificate you may see this error. To remove it, set each user's browser to trust the certificate. Alternatively, you can purchase a trusted certificate from a Certificate Authority. Replacing the self-signed certificate with a trusted certificate automatically prevents certificate errors from appearing.

Q: How do I update my security certificate and key files?

A: viewLinc stores the certificate and key files uploaded or generated during installation in the viewLinc installation directory. You can update the files at any time:

1. Copy new files to the viewLinc Enterprise Server data directory (<data folder>\config\keys\).
2. If the filenames are different from the original filenames, update the viewLinc.cfg file (<data folder>\config\viewLinc.cfg):

```
[web]
privatekeyfile = <newname>.key
certificatefile = <newname>.crt
```

3. Restart viewLinc Web Server (see "Restarting viewLinc" on page 180).

11.2 Managing Data

Q: I want to back up all files associated with viewLinc, where are they?

A: Before completing a backup, it is recommended that all viewLinc services be stopped. Then backup the files in these folders:

- Configuration files: **app_data_root\config***
- Historical data files, repository files, uploaded images: **app_data_root\db***
- Event logs: **app_data_root\log***

Q: What happens with the sampling in viewLinc when I attach a USB cable to a device for configuration etc.?

A: If a USB cable is attached to a device (i.e. the HMT140), the sampling is interrupted. When the USB cable is removed, sampling resumes. The sample timestamps start when the cable is removed, and are not an integral number of sample rate seconds since the previous sample. This should not affect operation. If the USB cable is attached for a long time, greater than twice the transmit rate, configuration alarms occur for missing historical data. They will clear once the sampling resumes.

Q: My upload keeps failing when using a file to upload logger info. How do I upload successfully?

A: Check that you have separated your parameters with tabs, not spaces, commas, etc. Only parameters entered as tab-separated lines (.tsv format) work.

11.3 Managing Devices

Setting Up Devices

Q: How do I create a definitions file to add multiple device types at one time?

A: Create a .txt definitions file that identifies the device class and device properties (separating each field with a tab):

Table 17 Definitions File Fields

Device Type	Properties to Define
DL	Define the COM Port number to which a device is connected, for example: vcom com_port=101 vcom com_port=102 vcom com_port=103
HMT330	Define the following: sample_rate = the internal sample rate of the device timeout = the timeout for communication events connection = the type of connection, COM Port or TCP com_port = a COM Port number to which your device is connected (values for COM Port connections are user-defined) serialno = the serial number of your device udp_port = UDP Port number ip_port = the TCP Port (values for TCP connections, ip_address and ip_port, are user-defined)
	Common values for both TCP and COM Port connections: sample_rate = 10s 90s (default), 12m, 2h, 2d, or 12d
	Optional values for COM Port connection: baud = 300, 2400, 4800, 9600, 19200 (default), 57600, or 115200 stopbits = 1 (default) or 2 databits = 7 or 8 (default) parity = odd, even or none (default)
HMT140	Define the serial number: hmt140 serial_number

Q: How do I add IP addresses for Vaisala devices using Ethernet devices (such as Digi, Moxa, or vNet devices)?

A: You don't. However you do assign IP addresses to your Vaisala devices. Because viewLinc communicates using COM ports, attaching Vaisala devices to the network using Ethernet/IP addresses requires the use of vNets or other Ethernet interface devices. Ethernet interface devices create virtual COM ports that allow Vaisala devices to communicate with viewLinc using Ethernet.

We recommend that you do not use dynamic IP addresses for your Vaisala devices; instead, use a reserved or static IP address (obtained from your IT department). IP addresses are assigned to Ethernet interface devices during driver configuration.

To learn more about using vNet devices, see www.vaisala.com/products. To learn more about Digi devices, see www.digi.com.

Q: How can I connect via wireless or Ethernet with 300 Series Transmitters?

A: Internal LAN-1 Module (Ethernet): Allows single PTU300*, HMT330, DMT340 or MMT330 transmitter to connect to a viewLinc host computer via standard TCP/IP Ethernet network. LAN-1 Module is internally powered by the transmitter.

- **Internal WLAN-1 Module (802.11b/g Wi-Fi)**: Allows single PTU300*, HMT330, DMT340 or MMT330 device to connect to a viewLinc server via standard 802.11b/g wireless networks. WLAN-1 Module is internally powered by the transmitter.
- **Single Port Ethernet Device**: Allows single PTU300, HMT330, DMT340 or MMT330 device to connect to a viewLinc server via standard TCP/IP Ethernet network. Requires installation of related device drivers and configuration of virtual COM ports on the viewLinc host computer. Requires transmitter configured with DB9 serial cable. Requires DB9-serial cable connection between Ethernet device and transmitter.
- **Multi-port Ethernet Device**: Allows multiple PTU300, HMT330, DMT340 or MMT330 devices to connect to a viewLinc server via standard TCP/IP Ethernet network. Requires installation of Ethernet device drivers and configuration of virtual COM ports on the viewLinc host computer. Allows for multiple PTU300, HMT330, DMT340 or MMT330 to connect to the host computer through a common TCP/IP network interface module. Requires transmitter configured with DB9 serial cable. Requires DB9-serial cable connection between Ethernet device and Vaisala transmitter.
- **Single Port Network Device (802.11b/g Wi-Fi)**: Allows single PTU300, HMT330, DMT340 or MMT330 device to connect to the viewLinc host computer via standard 802.11b/g wireless networks. Requires installation of networking device drivers and configuration of virtual COM ports on viewLinc host computer. Requires transmitter configured with DB9 serial cable.
- **Multi-port Network Device (802.11b/g Wi-Fi)**: Allows multiple PTU300, HMT330, DMT340 or MMT330 devices to be connect to the viewLinc server via standard 802.11b/g wireless networks. Requires installation of networking device drivers and configuration of virtual COM ports on viewLinc host computer. Allows for multiple data loggers to connect to the host server through common 802.11b/g wireless networks. Requires transmitter configured with DB9 serial cable.
- PTU300 can only support WLAN-1 and LAN-1 modules when no data logger modules are installed.

Check COM port assigned to a vNet or other Network Device

1. From the Windows **Control Panel**, open **Device Manager**.
2. Expand **Ports (COM & LPT)** to see which COM ports are connected to which devices. By default, vNet devices are named CDL-VNET-P - model name.
3. For more detail, in Device Manager under Multiport serial adapters, right-click the device in question. Choose **Properties**, select the **Advanced** tab, and click **Properties**. On the left will be a list of the COM ports used for the device. To see which devices are controlled by viewLinc, open the **System** tab.

11.4 Predefined Settings

Q: How does viewLinc select colors for reports?

A: When Location line colors are set to 'Auto' viewLinc assigns the next free color from a built in palette of colors. Colors are selected in the following order/sequence:

a. Black (0, 0, 0)
b. Red (255, 0, 0)
c. Green (0, 128, 0)
d. Orange (255, 165, 0)
e. Blue (0, 0, 255)
f. Yellow (255, 255, 0)
g. Purple (128, 0, 128)
h. Brown (150, 75, 0)
i. Grey (128, 128, 128)
j. Maroon (128, 0, 0)
k. Lime (0, 255, 0)
l. Tomato (255, 99, 71)
m. Azure (30, 127, 255)
n. Amber (255, 204, 0)
o. Byzantium (112, 41, 99)
p. Bronze (205, 127, 50)
q. Silver (192, 192, 192)
r. Crimson (220, 20, 60)
s. Emerald (80, 200, 120)
t. Coral (255, 127, 80)
u. DeepSkyblue (0, 191, 255)
v. Ecru (205, 178, 128)
w. Eggplant (97, 64, 81)
x. Buff (240, 220, 130)

Q: What content variables can I add to an email or SMS notification templates?

A: Auto-generated content can be added to an email or SMS template using macros. Not all macros are available in all email/SMS templates.

Table 18 Email and SMS Content Macros

Macro	Description
Available in All Alarm Templates	
[AlarmMessage]	A custom message is included in the message content, if specified for the corresponding alarm type (threshold, device, or system). If no alarm message specified, no content is generated for the macro.

Macro	Description
[Comments]	A predefined or custom comment is included in the message content, if specified for the corresponding alarm type (threshold, device, or system). If no content specified for the comment, no content is generated for the macro.
[Date]	Date of alarm.
[Server]	Name of the server viewLinc is installed on.
[Time]	Time of alarm event.
Alarm-related Messages	
[AlarmObject]	Description of where alarm was triggered, from a channel, a data logger or host.
[AlarmType]	Type of alarm, Communication or Threshold.
[AlarmTimestamp]	Time alarm occurred.
[AlarmDeactivationTimestamp]	Time alarm turned off.
Alarm Acknowledgement Messages	
[Acknowledger]	Person who acknowledged the alarm.
[AcknowledgerAction]	What was done in response to the alarm.
[AcknowledgerComments]	Comment entered by person acknowledging the alarm.
[AcknowledgeTimestamp]	Time alarm was acknowledged.
[AlarmID]	Alarm ticket ID (used for remote acknowledgements).
Threshold Alarms	
[AlarmValue]	Location value when alarm occurred.
[MinAlarmValue]	Minimum Location alarm value during alarm period.
[MaxAlarmValue]	Maximum Location alarm value during alarm period.
[CalibrationUrl]	Calibration Services website address.

Macro	Description
[LocationValue]	Location alarm value when email issued.
[ThresholdCondition]	Summary of the threshold condition.
[LocationTimestamp]	**Device Communication Alarms**
[DeviceChannelsSummary]	Brief description of all data logger channels associated with the alarm event.
[LocationSummary]	List of data logger channels in alarm state.
Host Communication Alarms	
[DeviceHostDevicesSummary]	Brief description of all data loggers on a host, associated with the alarm event.
[DeviceChannelsSummary]	Brief description of all data logger channels associated with the alarm event.

11.5 Troubleshooting Tips

Q: Why can't I log in to viewLinc using the correct username and password?

A: Ensure the viewLinc Enterprise Server service is running:
If viewLinc is not running, a blue screen and status message appears on your desktop display. If the viewLinc Web service is not running, you will see a browser error message. In Windows Control Panel, choose **Administrative Tools | Services**, then find "viewLinc Enterprise Server" on the list and right-click to select **Start**.

Has your domain name changed? If you are using Windows authentication, ensure your domain name matches your current log in password.

Q: Why can't I see any Zones and Locations?

A: viewLinc Zones and Locations are only visible if a group has been granted permission to view them. viewLinc Administrators set up group permissions on Zones. Permission to a Zone is required before you can view the Zones and Locations in Sites Manager, Sites, Alarms or Events windows.

Q: Why can't I access all viewLinc navigation pane windows?

A: viewLinc Administrators set up group rights to functional areas of viewLinc. If you require additional rights to access another viewLinc window, contact your Administrator.

Q: Why am I receiving a device configuration alarm indicating a low battery alarm when I know the batteries are new?

A: If you are using an older model DL data logger, some low battery alarms are triggered even when the battery is not the issue. Look up the event corresponding to the device configuration alarm in the Events window, and review the event details. For more assistance, contact Vaisala Technical Support.

Q: I'm receiving communication alarms in viewLinc. I think my network device or Vaisala device has stopped responding. What do I do?

1. Make sure your Vaisala data loggers and transmitters are plugged in and/or batteries are full.
2. Make sure your network devices are connected to a power supply and the power supply is plugged in. On a Digi or vNet network device, the power light on the front of the device should be solid red.
3. Ensure each device is connected to and communicating with the network. Try to connect with the device (see "Testing Network Communications" on page 179).
4. If there is communication between the device and the network, check that the Vaisala-supplied cable is connected properly. If the light is solid red, there is a problem with the network device or device cable. Make sure your device has been configured to use RealPort (see http://www.vaisala.com/en/lifescience). If this still doesn't fix the problem, go to step 6.
5. If the light is working correctly but you are still receiving communication alarms, open Windows Device Manager on the viewLinc computer and ensure the device is still installed:
   a. From the Windows Control Panel select **System and Security > Administrative Tools > Computer Management > Device Manager.**
   b. Under the Multiport serial adaptor category in Device Manager, look for duplicate drivers using the same COM port.
6. If the light on the cable is not working properly, open vLog and determine if the cable can communicate with the Vaisala device. If there is a problem with the device communicating with the vLog graphing application, it is likely the device or device cable is not functioning properly. Try connecting the device to a new vNet or Digi networking device, or to a computer using USB, and see if you can connect to it from vLog.

Q: How can I stop alarming while we reconfigure a storage area?

Table 19 Tips for Managing Alarms

What do you want to do?	Function	Description
Stop Location threshold alarming temporarily.	Pause/Resume	You can pause Location threshold alarming for up to 24 hours (threshold alarming resumes automatically after 24 hours). To pause Location threshold alarming for a longer period, disable the threshold alarm template (affects all Locations using the template). **Sites > Zones and Locations > Alarming**

What do you want to do?	Function	Description
Stop device alarming temporarily.	Pause/Resume	Stop device alarming up to 24 hours (device alarming resumes automatically after 24 hours). Affects the device and all device channels (and linked Locations). **Sites > Zones and Locations > Alarming**
Stop host alarming temporarily.	Pause/Resume	Stop host alarming temporarily up to 24 hours (host alarming resumes automatically after 24 hours). Affects the host, all devices connected to the host, and all device channels (and linked Locations). **Sites > Zones and Locations > Alarming**
Stop all threshold alarming for more than 24 hours, at a specific Location or Zone.	Disable/Enable	Stop all threshold alarming for the selected Location or Zone. **Sites Manager > Threshold Alarm Settings > Edit**
Stop all threshold alarming for more than 24 hours, at several Locations.	Disable/Enable	Stop threshold alarming at all Locations using the selected threshold alarm template. **Alarm Templates > Threshold Alarms > Properties**
Ignore one or more threshold levels, at several Locations.	Disable/Enable	Prevent a threshold level from being recognized by all Locations using the template. **Alarm Templates > Threshold Alarms > Edit > Deselect level**
Delete a threshold alarm template.	Threshold alarm templates cannot be deleted. They can be deactivated or disabled at the Locations where they are applied.	
	Deactivate/Activate	**Sites Manager > Threshold Alarm Settings** Deactivated threshold alarm settings are hidden from view, and do not monitor Locations. Threshold data is not included in reports while settings are deactivated.

What do you want to do?	Function	Description
	Disable/Enable	**Sites Manager > Threshold Alarm Settings** Disabled threshold settings remain with the Location, but are not used for monitoring or reporting.
Delete a Location	Deactivate/Activate	**Sites Manager > Zones and Locations > Manage** Current or previously linked Locations cannot be deleted, only hidden from view (for audit trail purposes). Only Locations which have never been linked (used to record data) can be deleted (Manage > Delete).
Delete a device or host.	Deactivate/Activate	**Sites Manager > Zones and Locations > Hosts and Devices** Device continues to record data in viewLinc , but hidden from display in viewLinc UI (you cannot delete devices for audit trail purposes).

Q: My security certificate has expired. Will viewLinc still run?

A: Yes. If your certificate or key file is moved or expires, viewLinc 5.0 will continue to run. To renew a self-signed certificate you will have to create a new certificate manually. Please contact Vaisala Technical Support if you require assistance.

If the URL used to access the server is https://viewLinc.mycompany.com/, then the filenames should be viewLinc.mycompany.com.key and viewLinc.mycompany.com.crt.

Glossary

A

access point (AP)
: A host device that enables communication between wired and wireless parts of a network. Access points typically use specific network standards. Also known as a gateway. Required to connect RFL100-series data loggers to viewLinc.

Acknowledge Alarms permission
: A permission level which allows a group to view Locations and acknowledge Location alarms.

acknowledgement
: User response to an alarm event.

Administrators group
: Members of the Administrator's Group have all rights, plus extra system-level rights which allow them to: undo Remote-lock on DL data loggers; restart viewLinc; test network communications; acknowledge inactive alarms; acknowledge system alarms; correct security status; add users to the Administrator group; edit user profiles of Administrators group members

alarm condition
: Environmental state which initiates an alarm event.

alarm event
: A record of an alarm condition.

alarm notification template
: Defines who is notified, when and how. Can be applied to a Location using a threshold template, or a device using a device alarm template.

Alarm off margin
: Also known as deadband. An active alarm will not turn off if conditions fluctuate within set margin.

Alarm Templates window
: Window used to create threshold, device, and notification alarm templates; Define content for email and SMS alarm messages; Create schedules.

Alarms window
: Window used to monitor active alarms.

ANSI characters
: Keyboard characters for all supported European languages. See https://www.w3schools.com.

audit trail
: A continuous record of all changes made to a device or the viewLinc system. The viewLinc audit trail is recorded in the Event Log.

C

calibration
: The process of checking and correcting the reading of any instrument giving measurements.

channel
: A device data transmission path. A device may have more than one channel available.

child
: A Location which resides within a Zone, or a sub-zone that resides within a Zone.

Communication alarm
: Notification that there is a problem with the transfer of data.

Configuration alarm
: Notification of an internal system error.

Configure Alarms permission
: A permission level which allows a group to view Locations, acknowledge Location alarms, and add or modify Location threshold alarms.

continuous monitoring
: Unbroken record of environmental surveillance.

D

dashboard
: An image file that provides a visual reference to a physical space being monitored.

deadband
: Alarm off margin. An active alarm will not turn off if conditions fluctuate within the set margin.

device
: Data collection hardware connected to your network (data loggers, transmitters).

device hosts
: Additional servers running viewLinc device host software. Allows for easier management of connected devices and greater network stability.

drift
: When data logger time gradually deviates from viewLinc server time.

E

Enterprise Server
: Required Vaisala viewLinc monitoring system software.

Events window
: Window used to record all system activities. Functions include: add comments about events, generate reports on specific event periods.

excursion
: When Location conditions exceed or deviate outside specified threshold limits.

F

Full Control permission
: A permission level which allows a group to view Locations, acknowledge Location alarms, configure Location threshold alarms, and modify or delete Zones and Locations.

I

inherit
: To automatically grant a permission level assigned to a top-level folder to its sub-zones or Locations.

IQOQ
: Installation Qualification / Operation Qualification protocol document used for system validation.

IT network manager
: The person responsible for maintaining your network, including connected software and hardware.

L

Location
: A viewLinc data collection point, such as a freezer or storage shelf, connected to a device channel that is part of the Vaisala viewLinc Monitoring System.

Location alarm
: Notification that a threshold level has been exceeded or communication problem has occured at point of data collection.

M

macros
: Predefined text strings you can add to custom email and sms content templates.

Manage Alarm Templates
: A right assigned to a group to allow configuration of alarm templates (threshold, device, notification, email and sms).

Manage Devices
: A right assigned to a group to allow addition or removal of devices, configure and edit device settings.

Manage Events
: A right assigned to a group to allow addition of custom events, add comments to events, print and export event details.

Manage Reports
: A right assigned to a group to allow addition and configuration of reports created by others (all users can add, edit and delete their own reports).

Manage Sites
: A right assigned to a group to allow addition or modification of Zones and Locations, add threshold alarms, permissions, and schedules.

Manage System
: A right assigned to a group to allow configuration of all system preferences, add users and groups, add schedules and predefined comments.

Manage Views
: A right assigned to a group to create new views, add or rename Zones, define accesss permissions for Zones, add dashboard images, share and manage trends.

MKT Activation Energy
: Mean Kinetic Temperature

O

Overview window
: Window used to display user-defined and shared views, specific collections of Zones and Locations. Set a default view to open automatically at login, generate view-specific reports and trends.

P

parent
: Zone which includes sub-zones or Locations

permission
: An access level which allows groups to view, configure or manage specific Locations and Zones.

PIN
: Personal Identification Number

PoE
: Power over Ethernet. Allows one cable to provide both data and electrical power to devices such as wireless access points. Benefits of PoE include longer cable lengths and elimination of the need for nearby power outlets.

R

real-time data
: viewLinc collects real-time data from devices more frequently than a device's set sample rate (usually in 10 second intervals).

report owner
: Individual who created a report.

Reports window
: Generate and create reports; download user-generated and shared reports.

RFL
: VaiNet wireless data logger.

rights
: Rights allow group access to viewLinc windows and additional window functions. All users have Manage Views right, which allows access to the basic functions in Overview, Sites, Reports, Alarms, Views Manager, and Events windows. Permissions must be granted for groups to see and perform functions on Zones and Locations in these windows.

ROC
: Rate of Change. Measures the amount of variation within one (1) minute. For example, you may want to know how quickly the temperature in a refrigerator rises when the door is opened.

S

sample
: One (1) recorded and time-stamped data logger measurement.

sampling rate
: Frequency of samples recorded over time.

sites
: Term used to refer to a collection of Zones and Locations.

Sites Manager window
: Window used to manage Zones, Locations, devices, and hosts. Functions include: Manage hosts and devices, create Zones and Locations, configure permissions, set Location threshold and notification settings, load dashboard images.

Sites window
: Windows used to display Zones and Locations a group is permitted to view. Functions include: pause alarming, generate quick reports, monitor conditions on the dashboard, build trends.

System alarm
: Notification when viewLinc detects changes made outside standard viewLinc operation (such as possible database tampering).

System Preferences window
: Define global settings, such as: system language, enable remote acknowledgement, set up audible alarming, enable use of schedules, set device default settings, enable comments.

T

threshold
: A level that when exceeded, initiates a threshold alarm.

Threshold alarm
: Notification that a threshold level has been exceeded.

TLS (SSL)
: Transport Layer Security (formerly Secure Sockets Layer). Communications protocol used to secure communications between network servers and web browsers.

V

VaiNet devices
: Vaisala wireless communication devices that use LoRa technology.

Validation alarm
: Notification when a problem with data collection is detected.

view
: User- or group-specific collection of Locations. Created in Views Manager, available in the Overview window.

View permission
: A permission level which allows a group to view Locations, acknowledge Location alarms, configure Location threshold alarms, and modify or delete Zones and Locations.

vLog
: Configuration software shipped with DL data loggers (prior to viewLinc 5).

W

Wrap when full
: This setting ensures a device will continue to record data, overwriting the earliest recorded data with new history when it reaches capacity. No interruption in data recording.

Z

Zone
: A collection of Locations being monitored. Zones can be divided into sub-zones.

Index

1

140-series Wi-Fi data loggers
  adding 31
  alias 41
  timeout 41
  transmit period 41

3

300 series transmitters
  adding 31
  alias 40
  sample rate 40
  timeout 40

A

access
  to Locations 103
  to views 110
access control See permissions
access points
  adding 30
  communication alarms 64
  configuration alarms 64
  releasing devices 172
  restarting 180
Acknowledge Alarms permission 103
acknowledging alarms
  about 125
  inactive alarms 120, 128
  receiving notifications 125
  remote acknowledgement 88
  system alarms 120, 127
  with viewLinc mobile 156
active alarms, viewing 122
adding
  140 series data loggers 31
  300 series transmitters 31
  access point hosts 30
  comments 98
  comments to a report 150-151
  comments to events 133
  custom events 134
  dashboard images 52
  device host server 29
  devices 29, 31-32, 34
  DL data loggers 32
  groups 59
  hosts 29
  Locations 47, 166
  multiple devices 34
  permissions 103
  reports 146
  RFL data loggers 31
  schedules 89, 105
  security certificate 23
  signature to a report 150-151
  sub-zones 46
  thresholds to Locations 66
  units 95
  users 59
  views 108
  Zones 46
adding/removing columns 118
adjusting
  dashboard layout 53
  scale value in a trend 139
Administrators group
  rights 58
  system rights 57
alarm notification templates
  about 64, 79
  adding to device alarms 83
  adding to Location threshold alarms 82

adding to system alarms 97
creating 80
editing 84
alarm notifications
audible 79, 89
command 122
email 122
launching an application or device 122
receiving 125
scheduling 105
sms 122
alarm off margin 67
alarm reports
creating 146, 150
deactivating/reactivating 145
printing current data 124
alarm templates
about 63
alarm notifications 79-80
device alarms 75, 78
email and sms content 85
schedules 105
threshold alarms 65
alarms
about 64
acknowledging 125
audible 60, 79, 89, 129
calibration 72, 91
communication 72-73, 188
configuration 64, 74
deactivating/activating 70
device 71
disable device alarming 169
disabling/enabling 169-171
editing device alarm settings 78
editing threshold alarm settings 70
email and sms message content 64
host 65
identifying 121
inactive 120
low battery 188
monitoring 119-120
multiple notifications 79
pausing 129, 131
remote acknowledgment 88
reporting 124
resume alarming 131
system 97
threshold 63, 65, 70
validation 72
viewing in Overview window 116
viewing in Sites window 116
Alarms window
acknowledging alarms 128
monitoring alarms 120
printing current alarm data 124
aliases
for channels 42
for devices 39
using 87, 91
android phones 1
applying
alarm notification templates to thresholds 82
threshold alarm templates to Locations 68
assigning
permissions 103
rights 57
audible alarms 79
enabling/disabling 89
for a user 60
responding to 129
turning off 129
audit trail 132
availability of generated reports 144

B

backing up 183
blocks per beacon 41

browsers
  opening multiple trends 141
  supported 1-2
building
  dashboards 52
  trends 137
  views 109

C

calibration
  about 174
  alarms 72, 91
  duration, setting 175
  editing channel settings 175
  editing device settings 175
  request off-site service 176
  request on-site service 176
calibration alarms 65
celsius or fahrenheit 90
certificates
  fixing errors 182
  installing with 23
  security 17
changing
  alarm notification templates 84
  dashboard display 54
  default view 110
  device alarm settings 78
  devices 173
  linked Locations 166
  Location alarm settings 70, 78
  monitored areas 166
  threshold alarm settings 70
  trends 139
  unit display 95
channels
  alias 87, 91
  description 42
  enable/disable 40
  finding linked Location 50
  linking to Locations 48-49, 163-164, 166
  naming 49
  unit display 95
  unlinking/relinking to Locations 49, 164
  viewing link history 50
checklist
  for site preparation 17
choosing
  default view, Overview window 110
clearing
  DL data logger history 178
  historical samples 178
color
  default palette 185
  selecting for reports 149
columns
  add/remove 118
  hiding 118
  sort order 118
COM Ports
  viewing 184
command notifications
  adding 80
comments
  about 98
  adding on a report 150-151
  adding to Events 133
  predefined 99
  viewing in event log 132
communication alarms
  device or host 72
  disabling/enabling 171
  pausing 129
  setting for hosts 73
  troubleshooting 188
communications
  network test 179
conditions
  identifying 121

configuration alarms
  device or host 72
  setting on hosts 74
Configure Alarms permission 103
configuring
  devices 34
  viewLinc 18-19
connection type
  IMAP 96
  POP3 96
contact information
  technical support 15
  Vaisala Calibration Services 174
content of email/SMS messages 85
controlling access to Locations/Zones 101
copying
  alarm notification templates 80
  device alarm templates 75
  threshold alarm settings 69
  threshold alarm templates 66
correcting device security status
  DL data loggers 179
creating
  alarm notification templates 80
  alarm report 150
  dashboards 52
  device alarm templates 75
  email and SMS templates 85
  groups 59
  Locations 47
  reports 144, 146
  schedules 89
  sub-zones 46
  threshold alarm templates 68
  trends 137
  user profiles 59
  views 108-110
  Zones 46-47
custom
  email and SMS templates 85
  events 134
  reports 146, 150

D

dashboards
  about 52, 122
  adding data points 53
  adding images 52
  changing font 54
  deleting data points 55
  deleting images 55
  find linked Location 123
  modifying data display 53
  view trend 123
data
  clearing history 178
data loggers
  adding 29
  channel properties 42
  clearing history 178
  configuring with viewLinc 39
  connecting 9
  correcting security status 179
  description and alias 39
  device alarms 71, 78
  setting up 9
  supported 1
  swapping 173
  timebase synchronization 91
data trends 137
database validation alarms 65
deactivating/reactivating
  devices/hosts 172
  groups 160
  Locations 167
  reports 145
  threshold alarm settings 70
  users 159
  Zones 167

decimal places 161
default application file locations 3
default view 109
definitions file 34
delay, alarm notification 80
deleting
  dashboard images or data points 55
  Locations 167-168
  permission to Zones or Locations 104
  reports 145
  units 95
  users 159
  Zones 164, 167-168
device alarm templates
  applying 76
  creating 75, 78
  editing 78
device alarms
  about 63, 71
  applying a notification template 83
  communication 72-73
  configuration 72, 74
  device alarm templates 75-76
  enabling/disabling 169-170
Device Host software 1, 22
device hosts
  adding 29
  alarm types 72
  pause alarming 131
  resume alarming 131
devices
  accepting wireless devices 31
  adding AP hosts 29
  adding data loggers or transmitters 31-32, 34
  adding PC hosts 30
  alarm settings 78
  alarm templates 75
  alarms 71
  alias 87, 91
  calibration 176
  calibration alarms 65, 72, 91
  calibration duration 175
  calibration properties 174-175
  channel calibration properties 175
  channel properties 42
  clearing history 178
  communication alarms 65
  configuration alarms 72
  configuring 34
  connecting 9
  correct security status 179
  deactivating/reactivating 172
  decimal places 161
  definitions file 34
  discovering 31, 34
  editing 39
  installing 9
  license key requirements 93
  locking/unlocking 176-177
  managing 29
  pausing device or host alarms 131
  properties 35
  rejecting 32
  releasing 172
  removing 171
  resume alarming 131
  RFL data loggers 31, 172
  supported 1
  swapping 173
  validation alarms 64
Digi devices
  troubleshooting 183
disabling/enabling
  audible alarms 90
  communication alarms 171
  device alarms 169-170
  schedules functionality 89
  threshold alarm levels 170
  threshold alarms 169

viewLinc Aware Service 92
disconnect after scan 40
discovering
devices 31, 34
displaying viewLinc on a remote terminal 156
DL Data Loggers
adding 32
discovering 31
sample interval 40
warmup time 40
downloading reports 144
drag and drop
to add Locations to a dashboard 52
to create a trend 137
to link Locations 49
drivers
USB cable 13

E

editing
calibration properties 175
channel properties 42
device alarm settings 78
device alarm templates 78
device properties 39
email and SMS templates 85
host properties 38
Location or Zone properties 160
RFL data logger properties 39
threshold alarm settings 70
threshold templates 69
user accounts 159
Zones and Locations 163
eLearning 15
email
custom content 85
default content 85
server settings 96
email notifications
acknowledgement 88, 125
receiving 122
templates 80
email settings
IT network administrator address 96
notification settings 96
enabling/disabling
audible alarms 89
communication alarms 171
device alarms 169-170
schedules functionality 89
threshold alarm levels 170
threshold alarms 169
viewLinc Aware Service 92
Enterprise Server
about 1
security certificate 23
errors
certificate 182
escalation path 80
Ethernet interfaces
installation of viewLinc with 12
troubleshooting 183
event log validation alarms 65
event logs See Events window
Events window
about 132
adding comments 133
adding custom events 134
printing/exporting 134
viewing events log 132
Excel reports 147, 151-152
exporting
alarm data, current 124
event logs 134
Location alarms report 146

F

file locations 3
find
  assigned permissions 104
  dashboard Locations 123
  linked Location 50
  search tool 117
firewall 181
fix security status 179
fonts, changing 53
Full Control permission 103

G

generating reports
  about 142
  download status 144
  quick reports 144
getting help
  eLearning 15
  technical support 15
getting started
  overview 1, 116
  planning worksheet 19
  setup checklist 17
  upgrading 5
  what's new 4
graphing a trend 137
groups
  access to Locations and Zones 103
  access to views 110
  creating 59
  deactivating or reactivating 160
  rights 57
GxP-compliance 90

H

hiding/showing
  columns 118
  deactivated devices/hosts 172
  deactivated groups 160
  deactivated Locations/Zones 168
  deactivated users 159-160
history
  clearing 178
  of linked channel 49
HMP110 probe 43
HMT140 Series Wi-Fi Data Loggers
  adding 31
  max blocks per beacon 41
  properties 43
  sampling in viewLinc 182
  timeout 41
  transmit period 41
host alarms 71
hosts
  adding 29-30
  communication alarms 65, 73
  configuration alarms 64, 74
  deactivating/reactivating 172
  editing properties 38
  installing viewLinc Device Host 23
  rejecting devices 32
  restarting 180
  testing network communications 179

I

identifying alarm conditions 121
image requirements for dashboards 52
IMAP 96
inactive alarms
  acknowledging 128
inherited permissions 102, 104
installation, system test 26
installing
  Device Host software 23
  device hosts 23
  viewLinc as an upgrade 24
  viewLinc Enterprise Server software 22

vNet Devices 12
Internet browsers, versions supported 1
iphone 1
IT network administrator 97
items on the dashboard
display options 53
find linked Location 123
view trend 123

L

language
in reports 143
on screen 26
setting for users 60
supported in viewLinc 94
learning about viewLinc 8
legacy user permissions 6
legacy user rights 5-6, 57
license key, entering 93
link history, viewing 49
linked channel/Location, finding 50, 117
linking/unlinking channels and Locations 47-49, 163
Location data on dashboards 122
Location history reports
creating 146
deactivating/reactivating 145
Locations
about 45
adding alarm notification schedules 107
adding schedules 105
adding threshold alarms 68
alarms status 120
applying alarm notification templates 82
assigning permissions 103
changing linked channel 163
changing threshold alarm settings 70
dashboards 52
deactivating/reactivating 167
deleting 167
editing properties 160
finding 50, 123
linking/unlinking channels 48-49
moving 166
pausing threshold alarming 129
permissions 102
renaming 163
reporting 146
resuming threshold alarming 131
searching for 117
setting up 45, 47
status 161
swapping devices 173
trends 123, 135, 140
locking/unlocking DL data loggers 176-177
log capacity 40
loggers **See also** devices
adding 29
channel descriptions 42
description and alias 39
DL, clear history 178
DL, correct security status 179
editing alarm settings 78
locking 176-177
setting up 9
logging in 25, 112, 187
low battery warning 188

M

maintenance
removing devices 171
restarting or stopping viewLinc 180
swapping a device 173
managing
groups and users 57
hosts and devices 29
sites 45
manually adding devices 32

Mean Kinetic Temperature 90
measurement units
  displaying 95
  temperature 90
message content 85
min/max statistics in trends 139
MKT activation energy
  setting value 90
mobile devices 111-112, 153
modem, SMS 97
monitoring
  alarms 119-120
  events 132
moving
  Locations or Zones 167
multiple alarm notifications 79

N

naming
  device or channel alias 87, 91
  Locations 47, 49
network testing 179
network traffic, balancing load 29
notification templates
  adding to Location device alarm settings 83
  adding to Location threshold alarm settings 82
notifications
  about 122
  audible 89
  commands 122
  email settings 85, 96
  message content 85
  schedules 105
  SMS settings 85, 97

O

off-site calibration 176
on-site calibration 176
organizing
  Locations and Zones 46
  views 109
orientation
  viewLinc desktop 115
Overview window
  about 108
  acknowledging alarms 128
  adding views 108
  default view 110
  pause alarming 130
  printing current alarm data 124
  resume alarming 131

P

passwords
  devices 39
  users 159
pausing/resuming
  alarms 129
  device or host alarming 130
  threshold alarming 129
PC requirements 3
PDF reports 147, 151-152
permissions **See also** access control
  about 102
  assigning to Locations 103
  defined 103
  inherited 104
  upgrading 102
  users, legacy 6
Permissions Viewer 104
PIN
  modem SIM Card 97
  user 60
POP3 96
POS 111
predefined comments 99
preferences
  audible alarms 89

email/SMS 96
language 94
predefined comments 98
schedules 105
system alarms 97
temperature units 90
printing
current alarm data 124
custom reports 146
event logs 134
Location alarms 146
Location history reports 146
quick reports 143-144
reports 142, 144
system reports 152
properties
channels 42
devices 39
Locations 160

Q

quick reports 143-144
generating 144

R

reactivating/deactivating
devices/hosts 172
groups 160
Locations 167
threshold alarms 70
users 160
receiving notifications 125
rejecting wireless devices 31
releasing wireless devices 172
relinking/unlinking channels 164
remote acknowledgment of alarms 88
remote display
about 111, 156
changing screen view 156
creating a view for 110
requirements 111
setting up 112
views 108
remote lock 177
removing
devices 171
Locations or Zones 167
reports
adding signature or comments box 150-151
alarm history 146
color for Location data 149
creating 144, 146, 150
current alarms 124
deactivating/reactivating 145
deleting 145
download progress 143-144
event logs 134
Excel 147, 151-152
generating 142
language 143
Location alarms 146
Location history 146
PDF 147, 151-152
printing 142
quick 143-144
repeating schedule 148, 151, 153
System 152
types 142
user language 60
Reports window 142
requirements
remote display 111
viewLinc setup 2
responding to alarms 125, 129
restarting 180
resume alarming 131
RFL100 Series Data Loggers
adding 31

display panel settings 39
LED settings 39
properties 39
releasing from access point 172
rights
Administrators group 57
assigning to groups 57
defined 58
users, legacy 5-6, 57
roadmap
setting up viewLinc 18

S

sample interval 40
sample rate 41
saving trends 140
scaling 139
schedules
applying to a Location 107
applying to a user 107
creating 105
enabling 89
for generating reports 148, 151, 153
search 117
secure SMTP 96
security
certificate errors 182
certificates 17, 23
self-signed or trusted certificates 182
security status, DL data loggers 179
serial ports 13
Series 11
server
name 38
requirements 2
session expiry 93
setting up
channel calibration properties 175
configuration steps 18
default view, Overview window 110
device calibration properties 175
devices 9, 31-32, 34
email server 96
Locations and Zones 45
planning worksheet 19
remote acknowledgment 125
remote display 112
schedules 105
SMS modem 97
setup checklist 17
sharing
reports 143
views 110
show/hide deactivated
devices/hosts 172
groups 160
Locations/Zones 168
threshold alarm settings 70
users 160
signatures
adding to reports 150-151
SIM Card PIN 97
site map
dashboards 52
sites
about 45
Sites Manager window
about 45
dashboards 52
device alarm settings 71, 76
hosts and devices 29
permissions 103
schedules 107
threshold alarm settings 68
Zones and Locations 45
Sites window
acknowledging alarms 128
building trends 137, 141
generating quick reports 143

monitoring alarms 119
pausing alarms 130
printing current alarm data 124
resuming alarming 131
SMS
message content 85
modem settings 96-97
notification settings 97
SIM Card PIN 97
SMS notification templates 80
SMTP settings 96
sorting columns 118
sounds for audible alarms 89
stopping viewLinc 180
sub-zones 46
support information 15
supported browsers 2
supported devices 1
supported languages 94
swapping devices 173
synchronization
logger timebase 91
system
installation test 26
IT network administrator, notifying 96
SMS modem 97
system alarms
about 65
acknowledging 127
preferences 97
system preferences
comments 98-99
email/sms settings 96
language 94
license key 93
remote alarm acknowledgement 88
schedules 105
session expiry 93
temperature units 90
units 95
viewLinc Aware Service 92
system reports
creating 146, 152
deactivating/reactivating 145
generating 142

T

technical support 15
technical support log 93
temperature
setting measurement units 90
templates
alarm notification 79
device alarm 63, 71, 76, 78
editing 84
email and SMS 64, 85
predefined comments 99
schedules 105
threshold alarm 63, 66, 69
testing
network communications 179
system installation 26
threshold alarm templates
about 63
adding notification templates 82
alarm off margin 67
applying to Locations 68
copying 69
creating 66
editing 69
threshold alarms
about 65
deactivating/reactivating 70
disabling temporarily 169-170
identifying conditions 121
pausing 129
schedules 107
threshold values, reading 137

time synchronization 92
timeout period 39, 93
  300 series transmitters 40
  HMT140 Wi-Fi data loggers 41
TLS (SSL)
  security 17
toolbar icons 116
tours 8
training 15
transmit period 41
transmitters
  adding 29
  setting up 9
trends
  about 135
  building 137
  displaying 135
  duration 139
  functions 138
  modifying 139
  navigation 138
  saving 140
  settings 139
  viewing on dashboard 123
troubleshooting 181
turning off
  audible alarms 129
types of alarms 64
types of reports 142

U

UDP port 38-39
units
  adding or modifying 95
  deleting 95
  preferences 95
unlinking/relinking channels 163-164
upgrading
  difference from earlier versions 5, 102
  installation 24
uploading definitions file 34
users
  access to views 110
  adding 59
  adding a schedule 107
  adding to groups 59, 61
  assigning rights 57
  deactivating/activating 159
  editing 159
  for remote display terminal 110
  legacy permissions 6
  legacy rights 6
  logging in 25
  permissions 101, 103
  preferred language 60
  schedules 105
  setting timeout period 93
  views 108, 110

V

Vaisala devices
  accepting RFL/HMT140 data loggers 31
  adding 31-32
  discovering 31
  setting up 9
validation alarms 64-65, 72
  notification settings 97
View permission 103
viewing
  active alarms 122
  COM ports 184
  device properties 35
  event comments 133
  event logs 132
  Location status 161
  Locations and Zones 116
  measurement units 95
  permissions 104

trends 123, 141
viewLinc
about 1
backing up 184
configuration 18
connecting devices 9
desktop orientation 115
device host requirements 2
Device Host, about 1
end-user PC requirements 3
Enterprise Server, about 1
installation options 9
logging in 25
new features 4-5
planning worksheet 19
remote display 111
restarting 180
security options 93
server requirements 2
SMTP 96
supported Internet browsers 1
tours 8
upgrading from earlier version 24
what's new 4-5
viewLinc Aware 92
viewLinc Mobile
about 111-112
acknowledging alarms 155
pause/resume alarming 155
views
adding folders 109
changing remote display view 156
creating 108-109
default 109-110
for remote display terminal 110
pausing/resuming alarms 130-131
sharing 110
vLog functionality in viewLinc 176-177
vNet devices
installing 9, 12
troubleshooting 183
viewLinc Aware Service 92

W

warmup time
DL data loggers 40
what's new 4-5
wireless devices, connecting 31
worksheet, configuration 19

Y

yellow highlight bar, not appearing 51

Z

Zones
about 45-46
adding 46
adding Locations 47
assigning permissions 103
dashboards 52
deleting 167
device alarms 71
moving Locations 166
pausing/resuming threshold alarming 129
permissions 102
renaming 163
searching for 117
setting up 45-46
viewing data 45

VAISALA

www.vaisala.com